



ArcSight User Behavior Analytics

Software Version: 6.10

User Guide

4/12/2018

Powered by  **SECURONIX**

Legal Notices

Warranty

The only warranties for Micro Focus products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

Micro Focus ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

Restricted Rights Legend

Confidential computer software. Valid license from Micro Focus required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

© Copyright 2018 Micro Focus or one of its affiliates.

Follow this link to see a complete statement of copyrights and acknowledgments: <https://community.softwaregrp.com/t5/ArcSight-Discussions/Third-Party-Copyright-Notices-and-License-Terms/td-p/1589228>

Legal Notice for Open Source Code

vLGPLv3, LGPLv2, EPL 1.0, CDDL

This product includes code licensed under the LGPLv3 licensed-code, LGPLv2 licensed-code, Eclipse Public License 1.0, CDDL-licensed code, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Micro Focus.

To obtain such source code on CD, send a check or money order in the amount of US \$10.00 (for shipping and handling) to:

Micro Focus

Attn: Gordon Lee

1140 Enterprise Way

Sunnyvale, CA 94089

USA

Please specify the product and version for which you are requesting the source code.

Support

Contact Information

Phone	A list of phone numbers is available on the Micro Focus ArcSight Technical Support Page: https://softwaresupport.softwaregrp.com/documents/10180/14684/esp-support-
-------	--

Contact Information, continued

	contact-list
Support Web Site	https://softwaresupport.softwaregrp.com/
Protect 724 Community	https://community.softwaregrp.com/t5/Protect724/ct-p/Protect724

Contents

Introduction	8
Who Should Read This Document?	8
User Interface Elements	9
Using the Documentation	15
Security Command Center	16
Security Dashboards	16
Top Violators	16
Top Threats	19
Top Violations	22
Kill Chain Analysis	25
Violation Timeline	26
Watchlist	27
Entities	29
Threats	49
Policies	59
Actions	59
Chat	59
Policy Details	61
Violators	63
Watchlists	66
Automated Response	72
Configuring Automated Response Framework Connections	75
Enabling Play Books	78
Enabling Play Books in Threat Indicators	78
Exporting CEF Alerts from ArcSight UBA Using Play Books	82
Launching Play Books	84
Customizing Tasks in Play Books	87
Data Insights	89
Creating New Dashboards	94
Configuring Dashboards	98
Customizing Widgets	101

Using Dashboards	130
Example Dashboards	133
Compliance Dashboards	135
PCI Dashboards	135
HIPAA Dashboards	137
Access Outliers Dashboard	143
High Risk Users	143
Rogue Access Detected	147
Access Reviews Dashboard	151
Access Review Details	152
Past Due Access Reviews	157
Investigation Workbench	158
Workbench Overview	158
Launching the Investigation Workbench	158
Simple Search	159
Advanced Search	162
Launching the Investigation Workbench from Other Screens	163
Starting Investigation for Multiple Entities Using Workspaces	163
Pivoting Across Objects	164
Viewing Objects in Detail	164
Viewing Objects Summary	164
Spotter	166
Using Spotter	166
Getting Started	166
Searching Spotter	174
Using Search Queries	175
Exporting Search Results as Reports	181
Viewing Jobs	184
Spotter Search Help	185
Search Operators	185
Reporting Operators	200
Analytical Operators	204
Incident Management	213

Managing Cases	213
Incident Management Dashboard	213
Viewing Case Details	215
Collaborating on Cases	219
Taking Actions on Cases	221
Creating a Case from the Security Command Center	226
Reports	230
Categorized Reports	230
Adding a new report category	233
Editing or Deleting an Existing Report or Report Category	235
Creating a New Report	237
Editing an Existing Report	244
Scheduling and Running an Existing Report	245
Downloading a Report to File	248
Running Reports from Spotter	249
Auditing	252
Configuring Auditing	253
Checking Log Tampering	254
Report Status	255
Scheduling a saved report	257
Merging Spotter Reports	259
Report Templates	261
Views	267
Users	268
Performing User Searches	272
Viewing User Details	273
Editing Users	280
Peers	283
Managing Peers	283
Viewing Peer Groups	286
Editing Peers	287
Resources	289
Watch List	303

Adding Members to a Watch List	305
Removing Members from a Watch List	307
White List	309
Creating a New White List	310
Adding Members to White Lists	311
Managing Policies for Targeted White Lists	314
Lookup Tables	316

Introduction

ArcSight UBA 6.10 is a big data security analytics platform built on Hadoop that utilizes Securonix machine learning-based anomaly detection techniques and threat models to detect sophisticated cyber and insider attacks. ArcSight UBA 6.10 uses Hadoop both as its distributed security analytics engine and long-term data retention engine. Hadoop nodes can be added as needed, allowing the solution to scale horizontally to support hundreds of thousands of events per second (EPS).

Features:

- Supports a rich variety of security data including security event logs, user identity data, access privileges, threat intelligence, asset metadata, and netflow data.
- Normalizes, indexes, and correlates security event logs, network flows, and application transactions.
- Utilizes machine learning-based anomaly detection techniques, including behavior profiling, peer group analytics, pattern analysis, and event rarity to detect advanced threats.
- Provides out-of-the-box threat and risk models for detection and prioritization of insider threat, cyberthreat, and fraud.
- Risk-ranks entities involved in threats to enable an entity-centric (user or devices) approach to mitigating threats.
- Provides Spotter, a blazing-fast search feature with normalized search syntax that enables investigators to investigate today's threats and track advanced persistent threats over long periods of time, with all data available at all times.
- Provides the Investigation Workbench to detect links across disparate data sets to enable quick investigations and hunting for cyber threats.

Who Should Read This Document?

The ArcSight UBA 6.10 User Guide is written for:

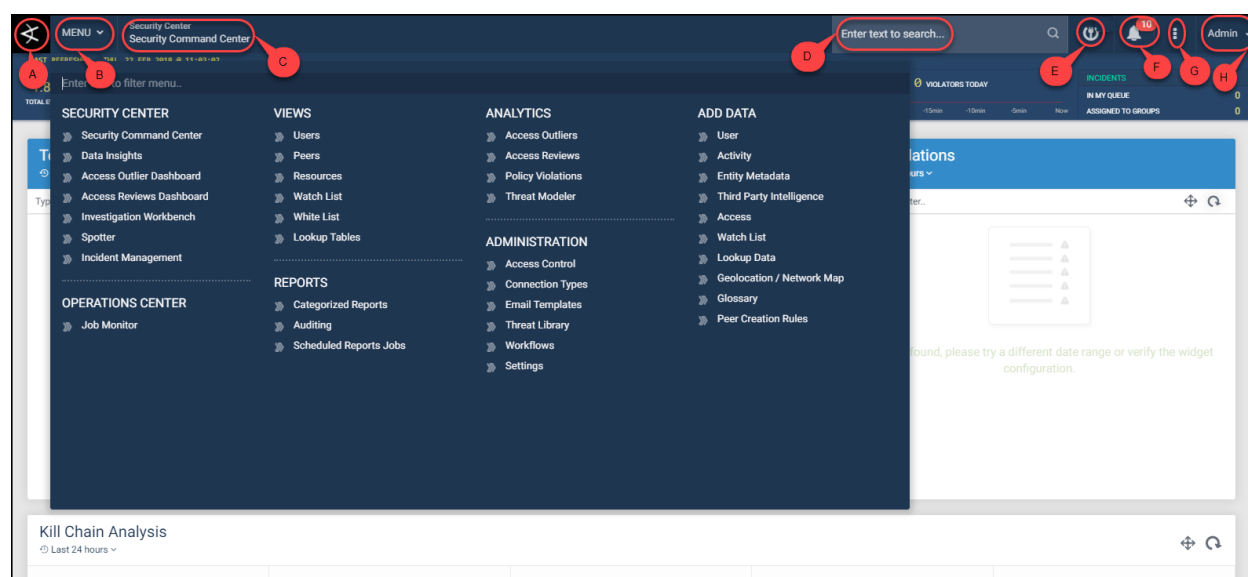
- Information security professionals, security analysts who need to detect and manage threats.
- Risk and compliance officers, and IT specialists who need to use ArcSight UBA's reporting capabilities to monitor and remediate compliance.

If you require additional information, the following documents are available:

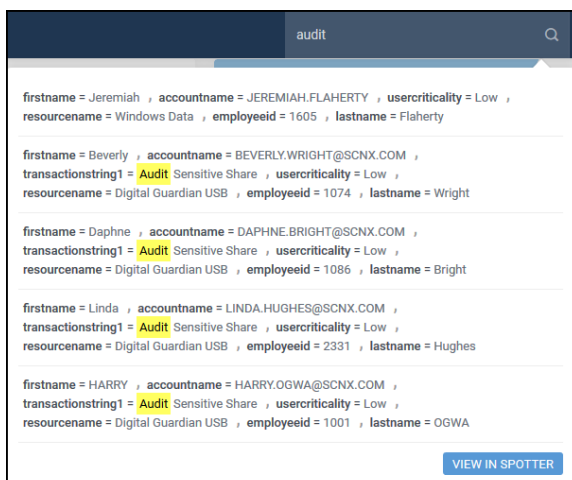
- ArcSight UBA Installation Guide – for system administrators, system integrators, and deployment teams who need to install the application.
- ArcSight UBA Administration Guide – for deployment engineers and service providers responsible for integrating data sources and creating content, compliance officers and IT specialists who need to configure and maintain Risk Management functionality, and system administrators who are responsible for ongoing operations and management, and business managers and other users in a supervisory role who need information about how to use ArcSight UBA to grant employees and partners access to applications, check for policy violations, and manage cases.

User Interface Elements

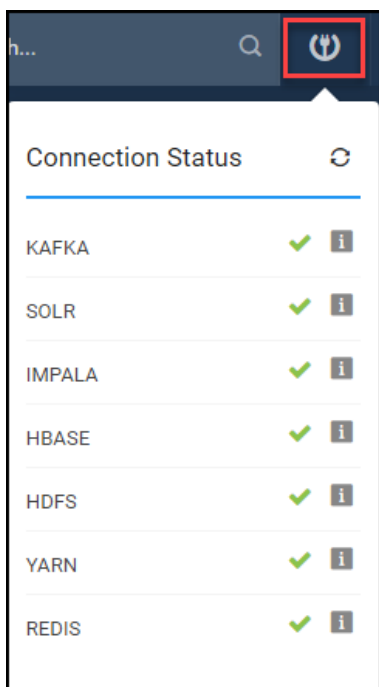
Some of the common elements found throughout the application are shown in the following image:



- A. **ArcSight UBA Logo:** Click from any screen to return to the Security Command Center home screen.
- B. **Main Menu:** Click to expand navigation options.
- C. **Current Screen:** Click to return to the home screen for the current menu item.
- D. **Quick Search:** Enter text to search within ArcSight UBA.

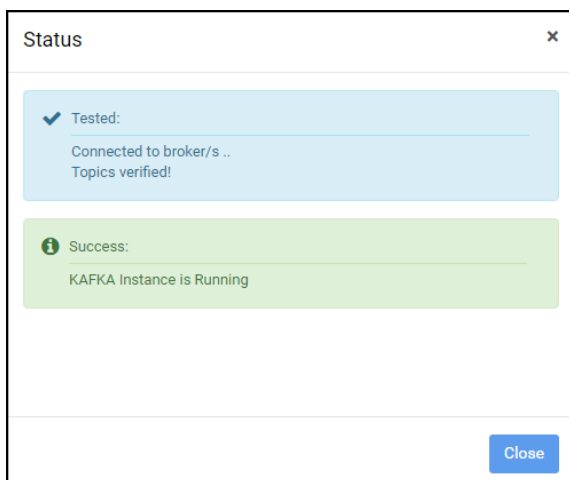


- E. **Connection Status:** Click the to view the **Connection Status** for all Hadoop components running on your environment.



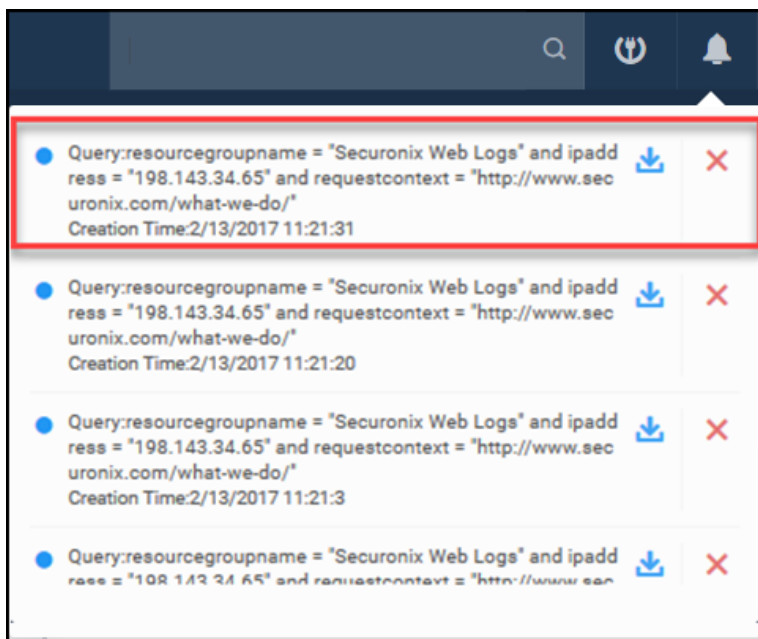
The green check mark indicates the component is running; a red X indicates the component is not running.

Click  to view details of each component.



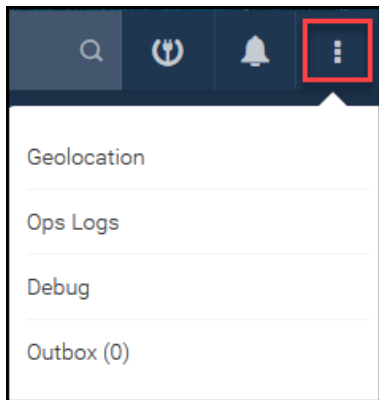
To configure settings for Hadoop components, navigate to **Menu > Administration > Settings > Hadoop** and following the instructions in [Configure Hadoop Settings for ArcSight UBA](#).

- F. **Notifications:** View job failure notifications and download exports including Spotter reports and query results. To delete notifications, click the red X.



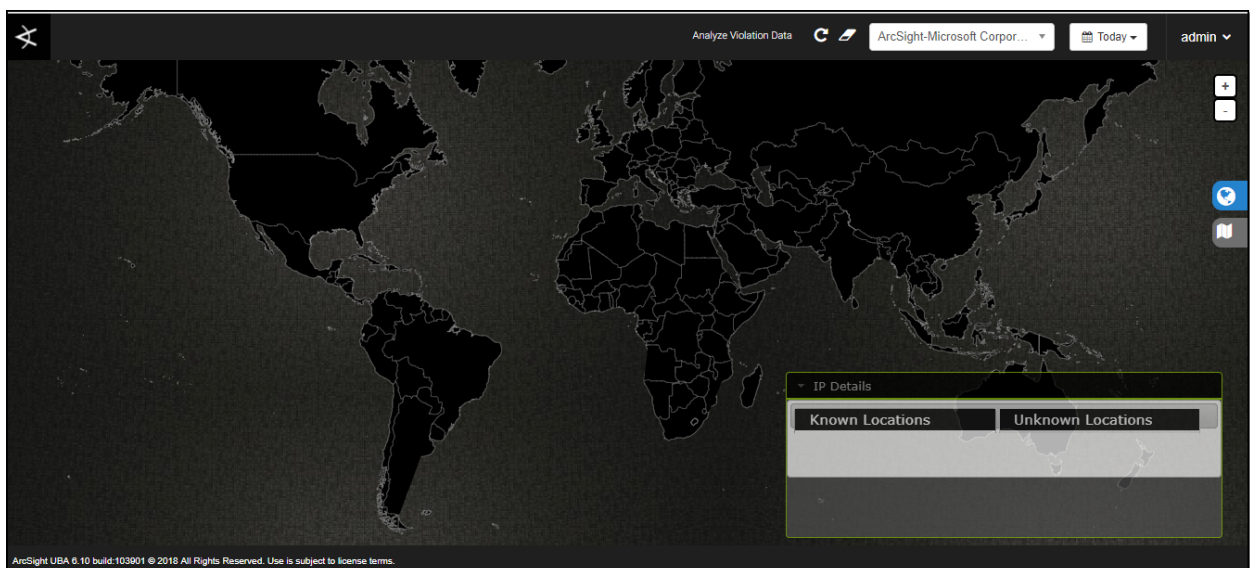
To download reports, click the download icon. For information on how to export Spotter reports, see [Spotter](#).

G. **Collapsed Menu:** Access the following screens:



Geolocation

From this screen, view the geolocation of the network source of specific resources.



You can perform the following actions:

- Toggle **Analyze Violation Data** to Yes to analyze data.
- Click refresh icon to refresh results.
- Click erase icon to clear results

- d. Select a resource from the dropdown.
- e. Select a time range from the dropdown.
- f. Use **+/-** to zoom in/out from the map.
- g. Click and drag mouse around to pan and tilt map view.
- h. Click icons on the right side to switch map view:



Op Logs

From this screen, you can view messages generated while executing Spark jobs.

Operational Messages are generated while executing spark jobs and we can view these messages by starting consumer with appropriate filters.

Datasource	Job	Policy	Source	Max Number Of Messages
GoogleDriveLogs	All	Activity to a Non-Corporate Dom...	All	1000

Stop

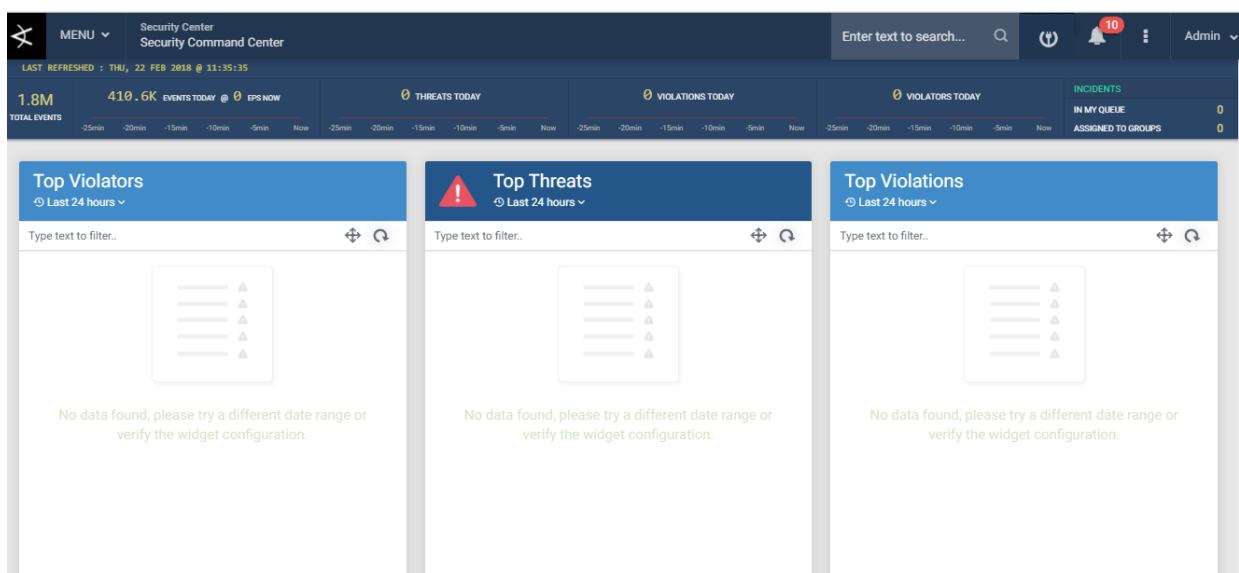
Source	Server Time	Current Time	Message
10-0-0-60.securonix.com	Thu, 13 Apr 2017 18:33:19 GMT	Thu Apr 13 2017 16:29:34 GMT-0500 (Central Daylight Time)	msg=Hadoop configuration obtained!

To view messages, complete the following:

1. Click **+** to start a **Consumer**.
2. Select **Datasource**, **Job**, **Policy**, and **Policy** from dropdowns.
3. Specify the max number of messages. Default 1000.
4. Click Stop to stop retrieving messages.

Debug

From this screen, view error messages and associated data to debug the ArcSight UBA application.



Click an option to see associated data.

Outbox

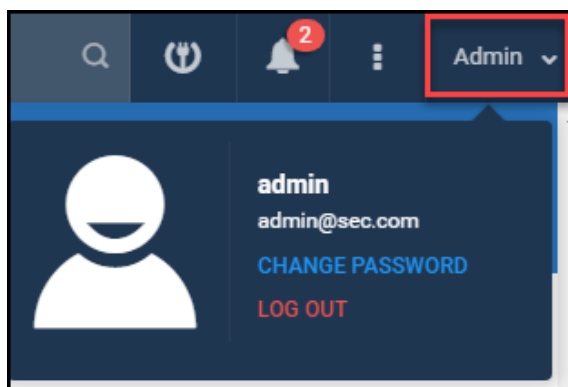
From this screen, view the ArcSight UBA email queue and send or delete messages in the out-box.

Send selected mail(s)		Delete selected mail(s)						
<input type="checkbox"/>	Sender name	From	To	CC	BCC	Subject	Last updated	High Priority
<input type="checkbox"/>	Securonix Admin	admin@mycompany.com	admin@mycompany.com	admin@mycompany.com	-	Case Assigned for review	2017-09-15 20:28:13.0	false
<input type="checkbox"/>	Securonix Admin	admin@mycompany.com	admin@mycompany.com	admin@mycompany.com	-	Case Assigned for review	2017-09-15 20:28:13.0	false

First 1 Last Show 10

Total results : 2 | Total pages : 1

H. **Admin:** View the user name of the current user, change current user password, and log out.



To change the current user's password, click **Change Password**, enter the old and new password, confirm the new password, and click **Update**. To log out, click **Log Out**.

Using the Documentation

The following formatting conventions are used in the documentation:

- **Buttons and keys:** when referring to buttons that must be clicked in the UI and keyboard keys that must be pressed, **bold text** is used.
- **Drop-down list and menu options:** when referring to an option that must be selected from a list or menu, **bold text** is used.
- **Menu navigation:** menu levels are indicated in **bold** and are separated with a right arrow. For example, to navigate to categorized reports, click **Menu > Reports > Categorized Reports**.
- **Folders and folder paths:** folders and folder names are indicated using quotation marks. For example, "C:\Documents\UserGuide".

Security Command Center

The ArcSight UBA Security Command Center is the first screen displayed when you log into the application. The Security Command Center provides a real-time view of threats as they happen. From this screen you can drill down into each user or violation and take action such as launching the Investigation Workbench, creating cases, managing threats, and searching Spotter for more information about the threat. By default, this view provides threats for today's date. You can change the date range, and move and re-size dashboards to customize your display.

The Security Command Center features the following dashboards:

Security Dashboards

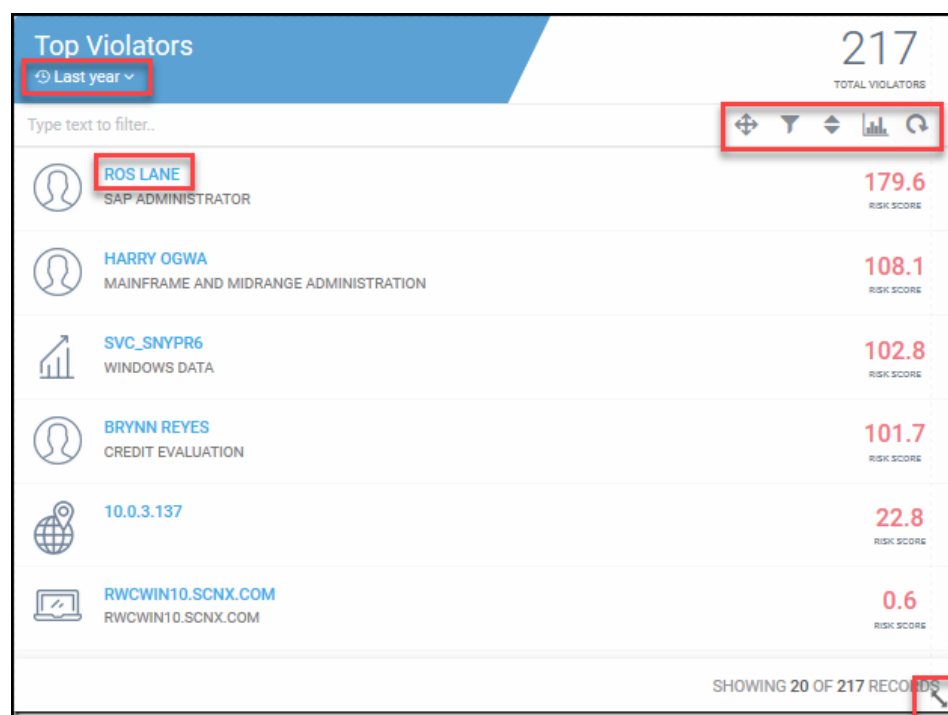
Security Dashboards display summary information about specific areas of concern for the last 24 hours by default. Security Dashboards include the following:

- Top Violators
- Top Threats
- Top Violations
- Kill Chain Analysis
- Violation Timeline
- Watchlist

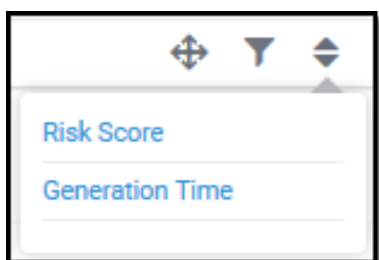
You can perform the following actions from the dashboards:

Top Violators

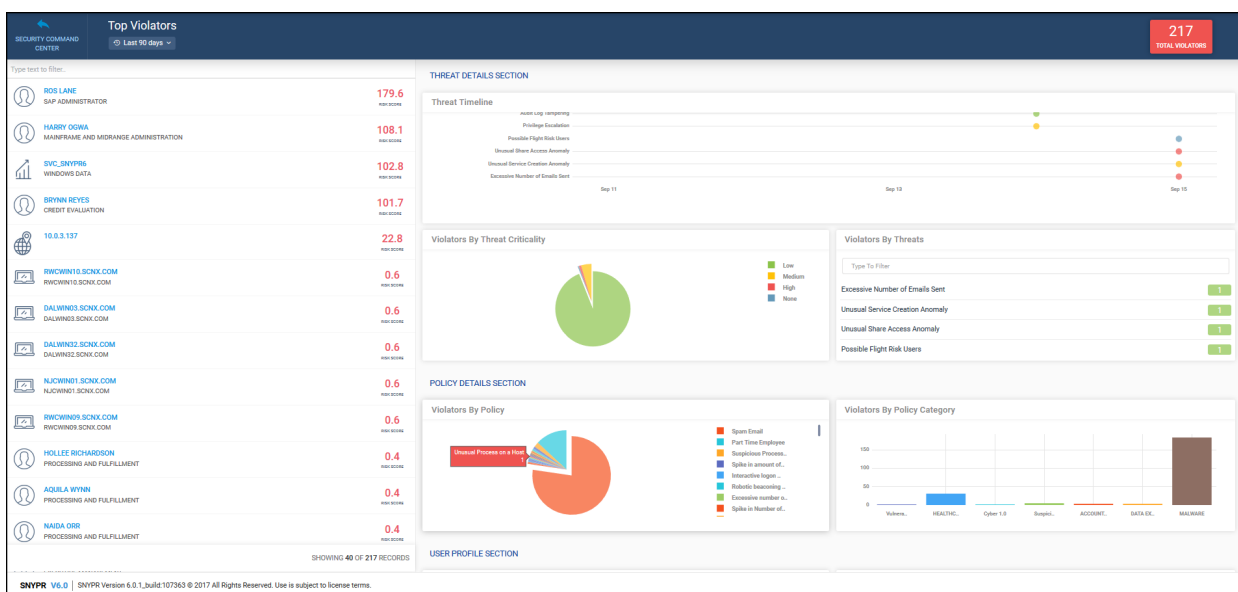
This dashboard displays the top attackers by risk score for the selected time range. Violators can include any entity: users, activity accounts, network addresses, and resources.



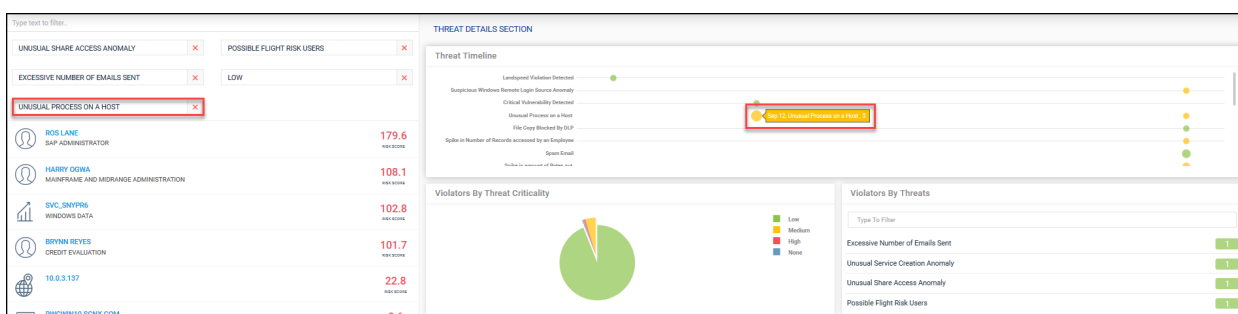
- **Change time range:** Select a time range from dropdown. Default: Last 24 Hours.
- **Type text to filter:** Type a string of text to find specific results.
- **Move:** Click move icon to change the position of the dashboard on the display.
- **Filter:** Click the icon to filter the following:
 - **Users:** A user on the network. Includes HR data and all correlated activity accounts belonging to the user. Example: Ros Lane.
 - **Resources:** An asset on the network. Example: An ATM named CHICAGOBANK_ATM1.
 - **Activity Account:** An account performing activity on a datasource. Example: SVC_ArcSight UBA6 on Windows.
 - **Network Address:** An IP address on the network. Example: 10.0.3.137.
 - **Resource Group Account:** An account performing activity across all datasources in a resource group. **Resource Group** refers to all the data sources imported for a **Device Type**. Example: An account for Resource Group **Blue Coat Proxy** across data sources BlueCoat1, BlueCoat2, and BlueCoatLandspeed.
- **Sort:** Click sort icon to sort by **Risk Score** or **Generation Time**.



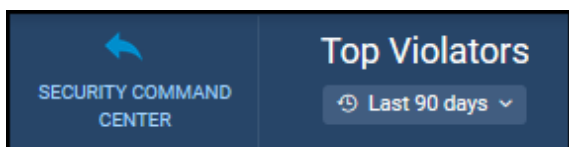
- **Graphical Analysis:** Click graph icon to view graphical summary of the following sections:



On the graphical analysis screen, you can click any data point on a graph to filter results. Click **X** to remove the filter and view all results.



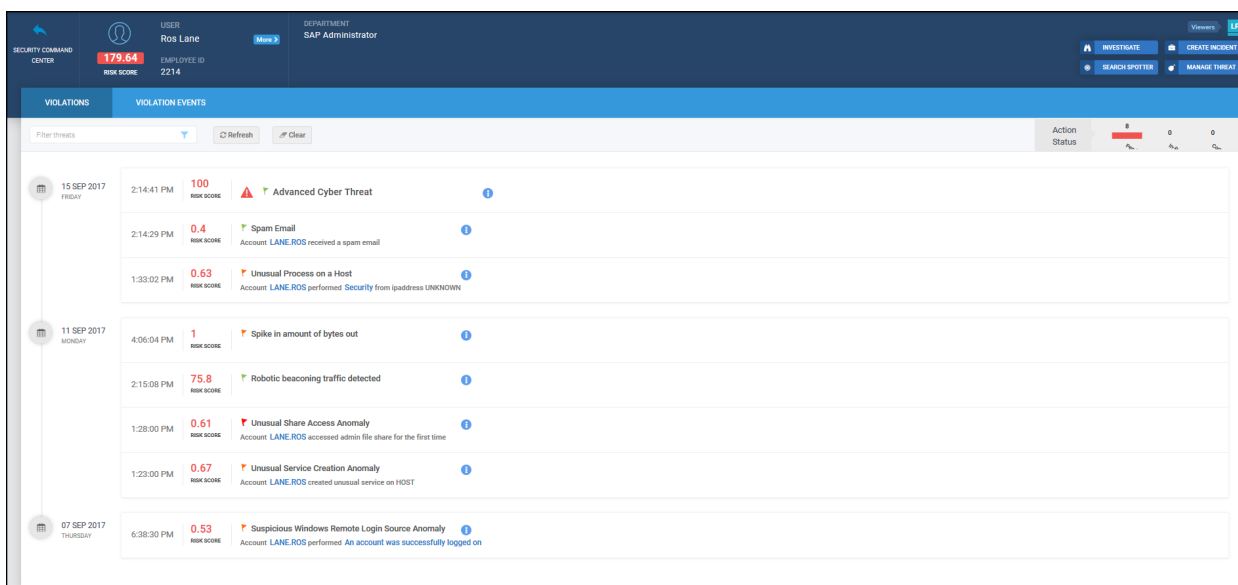
Click **Security Command Center** to return.



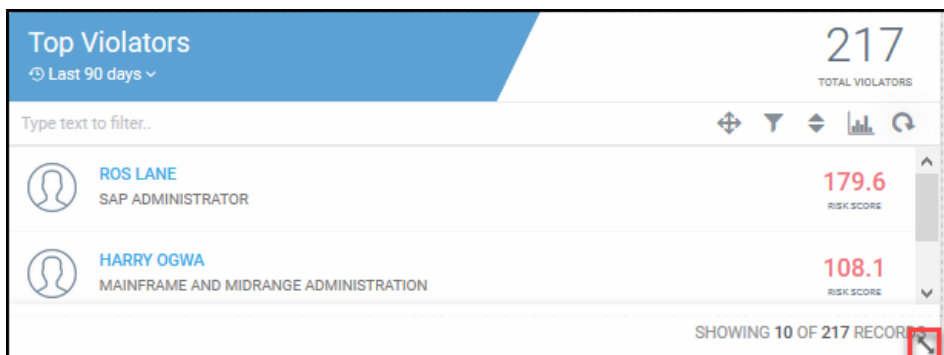
- **Refresh results:** Click refresh icon to refresh the results.



- **Click an Entity Name:** Click entity name to view a Violation Summary from which you can drill down into violations and take actions on the entity, or the violation or threat. For information about how to drill down into violations and take actions, see [Entities](#).



- **Re-size dashboard:** Click the icon to re-size the dashboard.



Top Threats

This dashboard displays the top threats for the time range by the number of violators. See [Threat Modeler](#) in the Administration Guide for information about configuring threat models.

Top Threats

Last 90 days ▾

4 THREATS

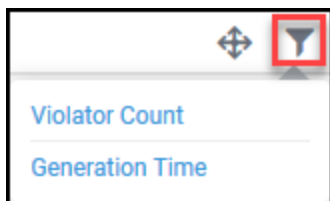
Type text to filter..

25 Days Ago Fri, 15 Sep 2017 @ 19:04:12	PATIENT DATA COMPROMISE NO OF STAGES: 4, RISK SCORING SCHEME:STATIC, WEIGHT:100.0	1 VIOLATORS
25 Days Ago Fri, 15 Sep 2017 @ 14:29:41	INSIDER THREAT NO OF STAGES: 4, RISK SCORING SCHEME:STATIC, WEIGHT:100.0	1 VIOLATORS
26 Days Ago Fri, 15 Sep 2017 @ 14:14:41	ADVANCED CYBER THREAT NO OF STAGES: 6, RISK SCORING SCHEME:STATIC, WEIGHT:100.0	1 VIOLATORS
26 Days Ago Thu, 14 Sep 2017 @ 19:04:11	PRIVILEGE MISUSE NO OF STAGES: 3, RISK SCORING SCHEME:STATIC, WEIGHT:100.0	1 VIOLATORS

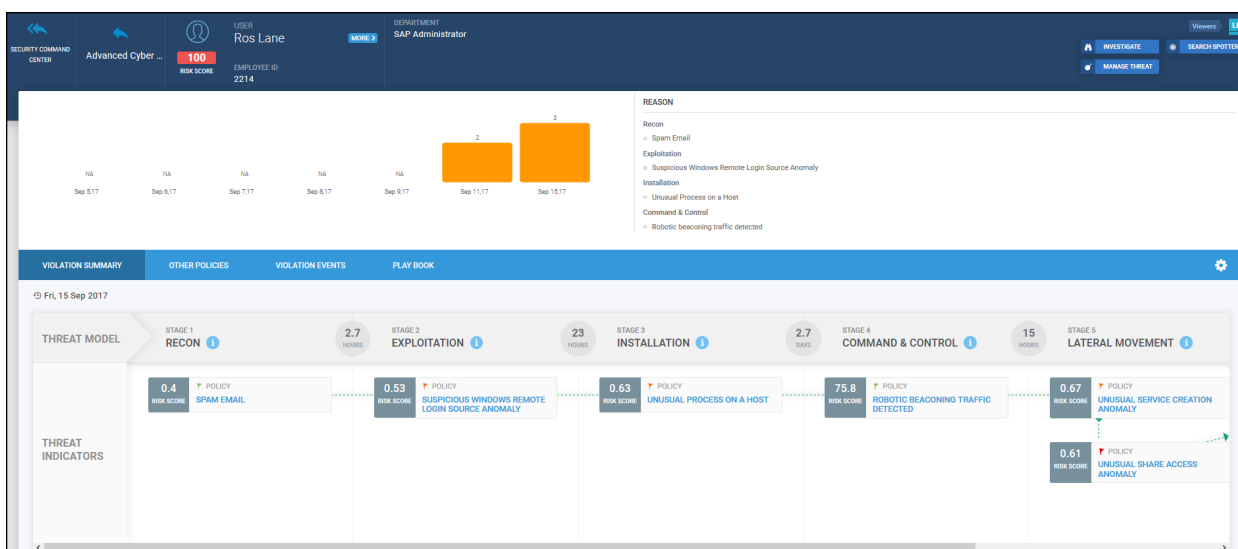
SHOWING 4 OF 4 RECORDS

- **Change time range:** Select a time range from dropdown. Default: Last 24 Hours.
- **Type text to filter:** Type a string of text to find specific results.
- **Move:** Click move icon to change the position of the dashboard on the display.
- **Filter:** Click the icon to filter by criticality:
 - High
 - Medium
 - Low
 - Zero Policy

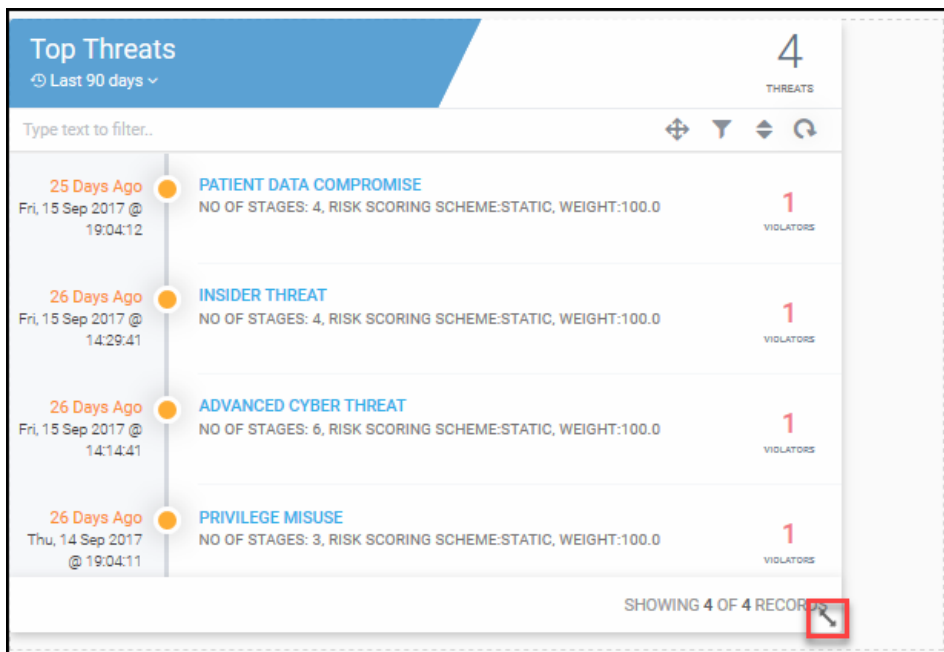
- **Sort:** Click to sort by **Policy Count** or **Generation Time**.



- **Refresh results:** Click refresh icon to refresh the results.
- **Click a Threat Name:** Click a threat name to view a Violation Summary from which you can drill down into violations and take actions on the entity, or the violation or threat. For information about how to drill down into violations and take actions on threats, see [Threats](#).

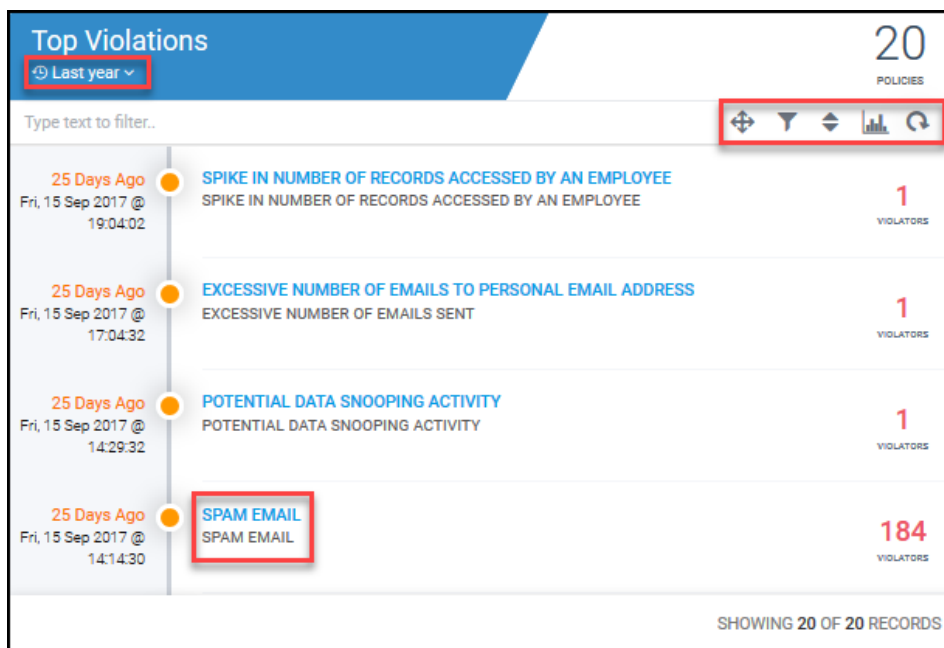


- **Re-size dashboard:** Click the icon to re-size the dashboard.



Top Violations

This dashboard displays the top policy violations for the specified time range by the number of violators.

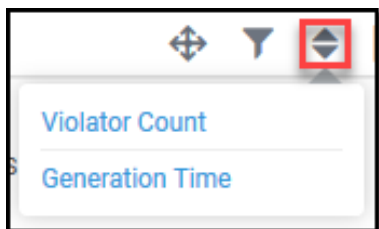


- **Change time range:** Select a time range from dropdown. Default: Last 24 Hours.
- **Type text to filter:** Type a string of text to find specific results.
- **Move:** Click move icon to change the position of the dashboard on the display.
- **Filter:** Click the icon to filter by criticality:

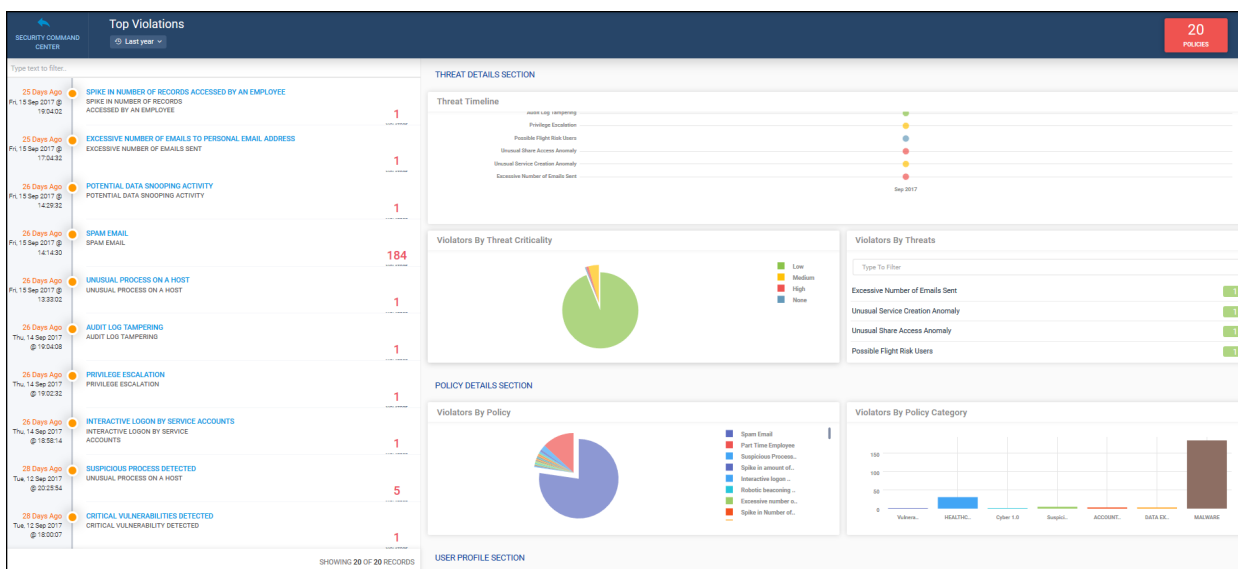


- High
- Medium
- Low
- Zero Policy

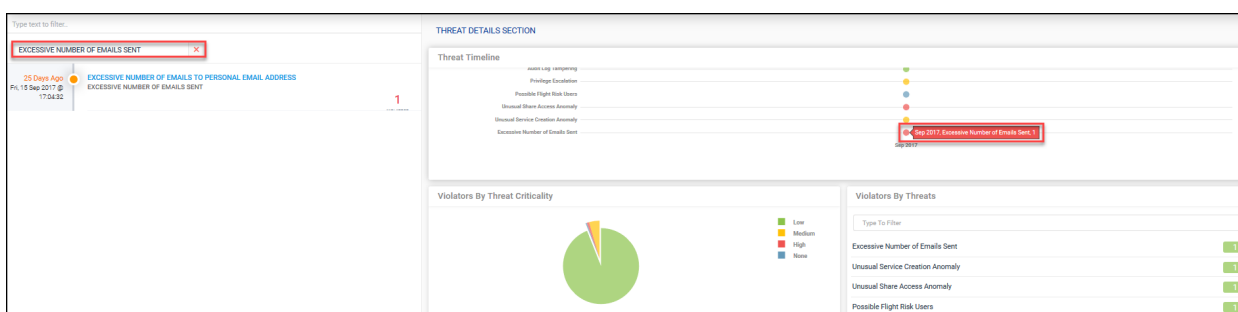
- **Sort:** Click sort icon to sort by **Violator Count** or **Generation Time**.



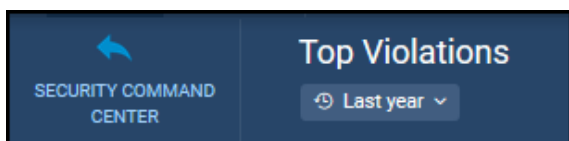
- **Graphical Analysis:** Click graph icon to view graphical analysis of the dashboard summary.



On the graphical analysis screen, you can click any data point on a graph to filter results. Click **X** to remove the filter and view all results.



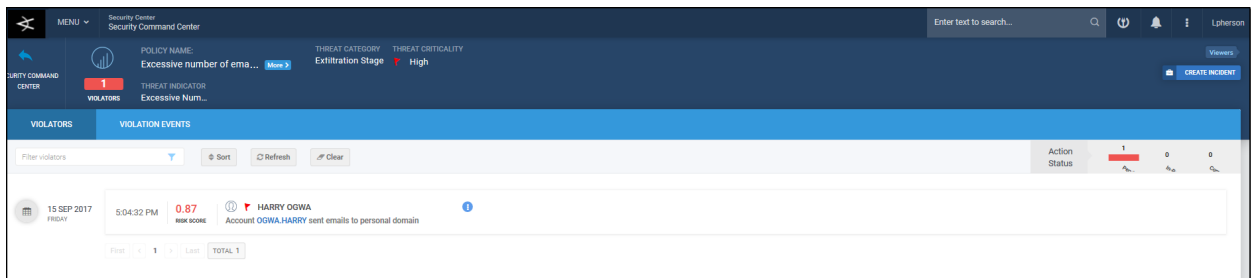
Click **Back to Security Command Center** to return.



- **Refresh results:** Click refresh icon to refresh the results.



- Click a Policy Name:** Click policy name to view a Violation Summary from which you can drill down into the violation and take actions on the violator, or the violation or threat. For information about how to drill down into violations and take actions on policy violations, see [Policies](#).



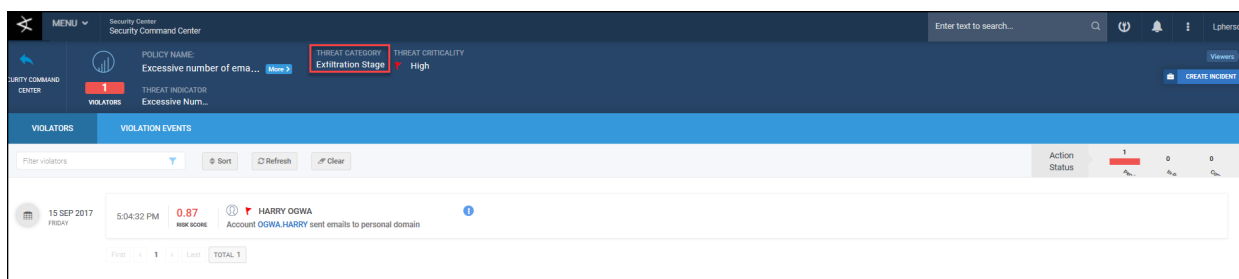
Kill Chain Analysis

This dashboard displays policy violations by Kill Chain stages. The stages include the following:

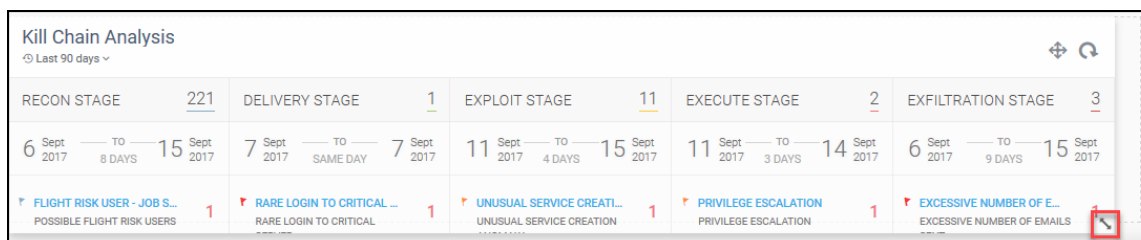
- **Recon Stage:** Stage in which attackers gather information before an attack in an attempt to find a vulnerable point in the network. Example: Phishing emails.
- **Delivery Stage:** Stage in which attackers deliver a malicious package to gain access to a network. Example: User clicks a link within a phishing email and downloads malware from the malicious site.
- **Exploit Stage:** Stage in which attackers find a vulnerable point of entry into the network and gain access. Example: Zero-day attack.
- **Execute Stage:** Stage in which attackers escalate access to execute the attack using admin privileges. Example: Escalating privileges or stealing admin credentials, lateral movement.
- **Exfiltration Stage:** Stage in which the attackers can move freely around the network and access or remove any sensitive data at will. Example: An insider uploading customer information to a personal file sharing/storage site.

Configure the stages of the Kill Chain during **Step 1: Enter Policy Details** when creating Policy Violations.

- **Change time range:** Select a time range from dropdown. Default: Last 24 Hours.
- **Move:** Click move icon to change the position of the dashboard on the display.
- **Refresh results:** Click refresh icon to refresh the results.
- **Click a Policy Name:** Click policy name to view a Violation Summary from which you can drill down into the violation and take actions on the violator, or the violation or threat. For information about how to drill down into violations and take actions on threats, see [Threats](#).

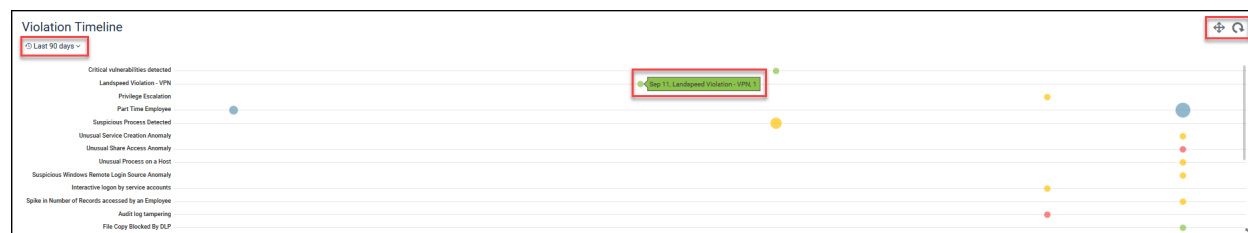


- **Re-size dashboard:** Click the icon to re-size the dashboard.

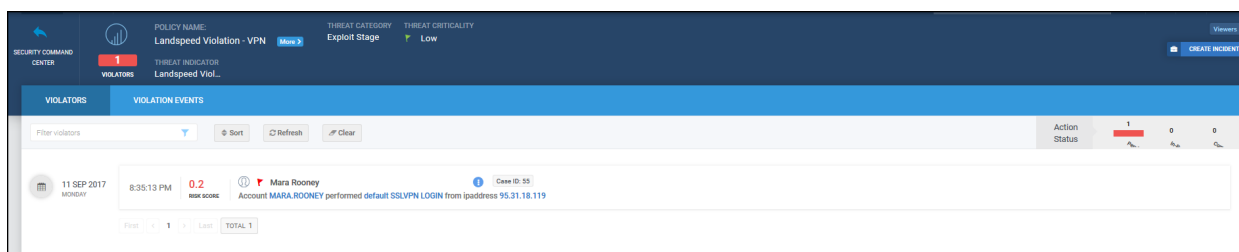


Violation Timeline

This dashboard displays a timeline of policy violations for the specified time range.



- **Change time range:** Select a time range from dropdown. Default: Last 24 Hours.
- **View a data point:** Hover over a data point to view a quick summary of the time, policy violated, and number of violations.
- **Move:** Click move icon to change the position of the dashboard on the display.
- **Refresh results:** Click refresh icon to refresh the results.
- **Click a data point:** Click data point to view a Violation Summary from which you can drill down into the violation and take actions on the violator, or the violation or threat. For information about how to drill down into violations and take actions, see [Policies](#).



- **Re-size dashboard:** Click the icon to re-size the dashboard.



Watchlist

This dashboard displays watch lists with activity within the specified time range. For information about configuring watch lists, see [Watch Lists](#) in the Administration Guide.

Watchlist

Last 90 days

Type text to filter..

WATCHLISTS 5

Watchlist Name	Entities
PART TIME EMPLOYEES	31
FLIGHT RISK USERS	13
PCI ASSET	8
HIPAA SERVERS	7
VULNERABLE HOST	5

SHOWING 5 OF 5 RECORDS

- **Change time range:** Select a time range from dropdown. Default: Last 24 Hours.
- **Move:** Click move icon to change the position of the dashboard on the display.
- **Refresh results:** Click refresh icon to refresh the results.
- **Click a Watchlist Name:** Click a watchlist to view, add or remove members from a watchlist from the Violation Summary screen. For information about how to manage watchlists from this screen, see [Watchlists](#).

SECURITY COMMAND CENTER

WATCHLISTS
flight risk users

TYPE
Users

CRITICALITY
MEDIUM

VIEWERS

TOTAL MEMBERS 13

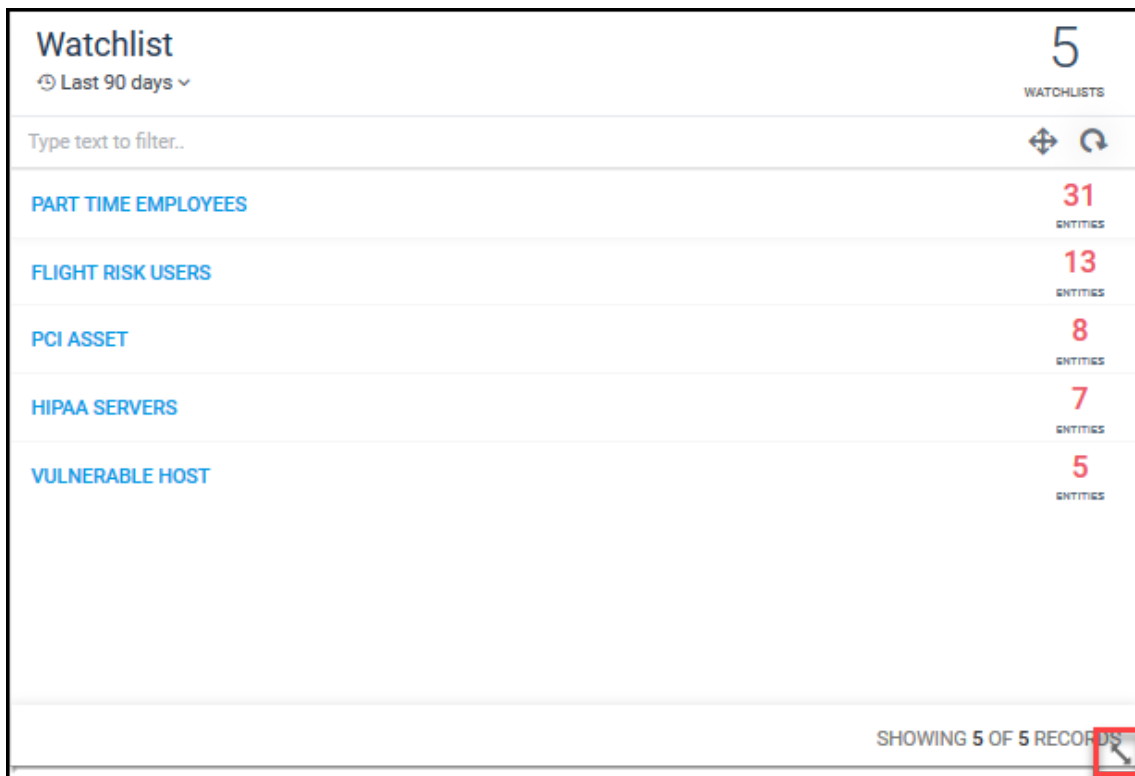
Enter your search criteria

	Entity Name	Watch List Type	Reason	Confidence Level (between 0 to 1)	expirydate	watchlistname	createdate	decayflag
<input type="checkbox"/>	1127	Users		1.0	09/15/2018 20:11:10	Flight Risk Users	09/15/2017 20:11:10	false
<input type="checkbox"/>	1128	Users		1.0	09/15/2018 20:11:10	Flight Risk Users	09/15/2017 20:11:10	false
<input type="checkbox"/>	1129	Users		1.0	09/15/2018 20:11:10	Flight Risk Users	09/15/2017 20:11:10	false
<input type="checkbox"/>	1130	Users		1.0	09/15/2018 20:11:10	Flight Risk Users	09/15/2017 20:11:10	false
<input type="checkbox"/>	1131	Users		1.0	09/15/2018 20:11:10	Flight Risk Users	09/15/2017 20:11:10	false
<input type="checkbox"/>	1132	Users		1.0	09/15/2018 20:11:10	Flight Risk Users	09/15/2017 20:11:10	false
<input type="checkbox"/>	1135	Users		1.0	09/15/2018 20:11:10	Flight Risk Users	09/15/2017 20:11:10	false
<input type="checkbox"/>	1136	Users		1.0	09/15/2018 20:11:10	Flight Risk Users	09/15/2017 20:11:10	false
<input type="checkbox"/>	1138	Users		1.0	09/15/2018 20:11:10	Flight Risk Users	09/15/2017 20:11:10	false
<input type="checkbox"/>	1139	Users		1.0	09/15/2018 20:11:10	Flight Risk Users	09/15/2017 20:11:10	false
<input type="checkbox"/>	1140	Users		1.0	09/15/2018 20:11:10	Flight Risk Users	09/15/2017 20:11:10	false
<input type="checkbox"/>	1142	Users		1.0	09/15/2018 20:11:10	Flight Risk Users	09/15/2017 20:11:10	false
<input type="checkbox"/>	1144	Users		1.0	09/15/2018 20:11:10	Flight Risk Users	09/15/2017 20:11:10	false

First 1 Last Show 15

Total results: 13 | Total pages: 1

- **Re-size dashboard:** Click the icon to re-size the dashboard.










Watchlist		5
🕒 Last 90 days ▾		WATCHLISTS
Type text to filter..		🔍 ↺
PART TIME EMPLOYEES	31	ENTITIES
FLIGHT RISK USERS	13	ENTITIES
PCI ASSET	8	ENTITIES
HIPAA SERVERS	7	ENTITIES
VULNERABLE HOST	5	ENTITIES

SHOWING 5 OF 5 RECORDS

Entities

Entities include Users, Activity Accounts, Resources, and Network Addresses.

Top Violators		217
Last 60 days ▾		TOTAL VIOLATORS
Type text to filter...		
	ROS LANE SAP ADMINISTRATOR	179.6 RISK SCORE
	HARRY OGWA MAINFRAME AND MIDRANGE ADMINISTRATION	108.1 RISK SCORE
	SVC_SNYPR6 WINDOWS DATA	102.8 RISK SCORE
	BRYNN REYES CREDIT EVALUATION	101.7 RISK SCORE
	10.0.3.137	22.8 RISK SCORE
	RWCWIN10.SCNX.COM RWCWIN10.SCNX.COM	0.6 RISK SCORE
	DALWIN03.SCNX.COM	0.6 RISK SCORE
SHOWING 20 OF 217 RECORDS		

The Entities screen displays details about an entity including lists of policy violations and threats. From this screen, you can drill down into the violations and take actions such as launching an investigation, creating a case, searching Spotter, managing the threat, and collaborating with other members of the team who are viewing the entity.

To leave this screen, click **Back to Security Command Center**.

SECURITY COMMAND CENTER

USER

Ros Lane

EMPLOYEE ID

2214

DEPARTMENT

SAP Administrator

179.64

RISK SCORE

More

INVESTIGATE

CREATE INCIDENT

SEARCH SPOTTER

MANAGE THREAT

Views

1P

VIOLATIONS

VIOLATION EVENTS

Filter by type

Refresh

Clear

15 SEP 2017

FRIDAY

2:14:41 PM

100

RISK SCORE

Advanced Cyber Threat

2:14:29 PM

0.4

RISK SCORE

Spam Email

Account LANE.ROS received a spam email

1:33:02 PM

0.63

RISK SCORE

Unusual Process on a Host

Account LANE.ROS performed Security from (ipaddress UNKNOWN)

11 SEP 2017

MONDAY

4:06:04 PM

1

RISK SCORE

Spike in amount of bytes out

2:15:08 PM

75.8

RISK SCORE

Robotic beaconing traffic detected

1:28:00 PM

0.61

RISK SCORE

Unusual Share Access Anomaly

Account LANE.ROS accessed admin file share for the first time

1:23:00 PM

0.67

RISK SCORE

Unusual Service Creation Anomaly

Account LANE.ROS created unusual service on HOST

07 SEP 2017

THURSDAY

6:38:30 PM

0.53

RISK SCORE

Suspicious Windows Remote Login Source Anomaly

Account LANE.ROS performed An account was successfully logged on

Action Status

8

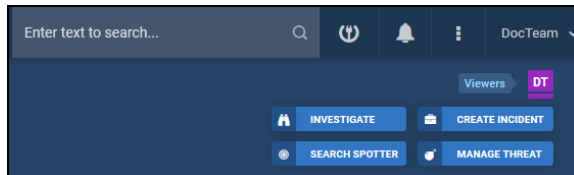
0

0

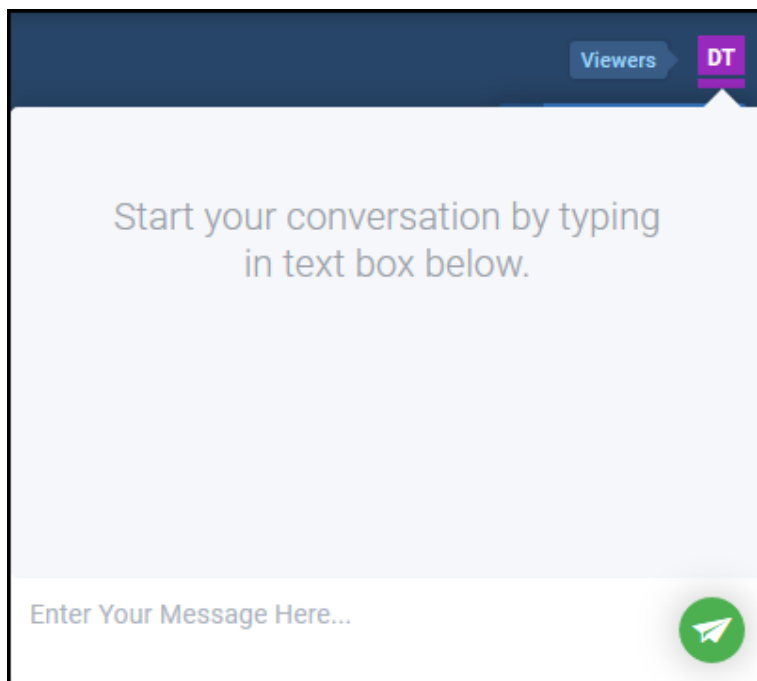
You can perform the following actions from this screen:

Chat

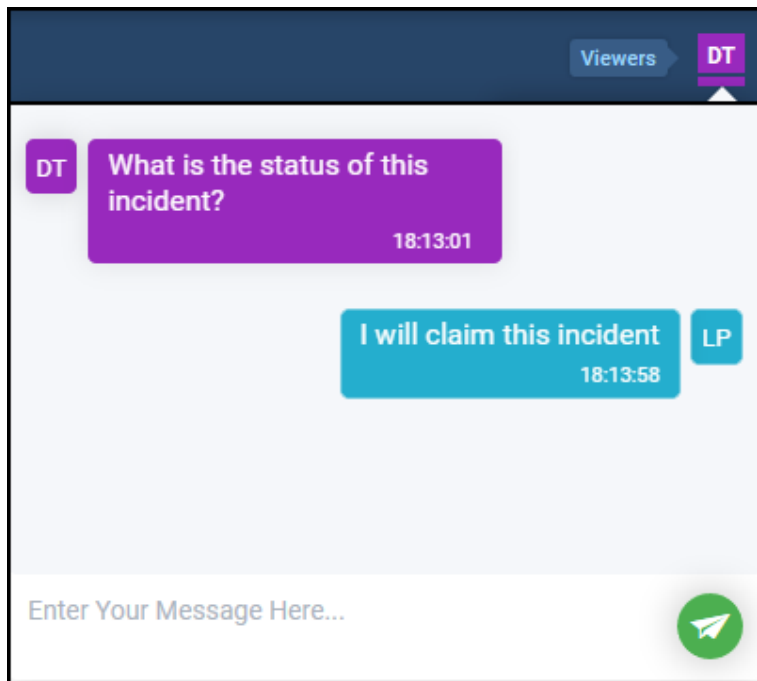
ArcSight UBA 6.10 includes chat capability to allow analysts to easily collaborate on violations and incidents within their groups. The initials of the other users viewing the violation will appear at the top right of the screen.



Click the initials of the user with whom you wish to chat to launch the chat window.

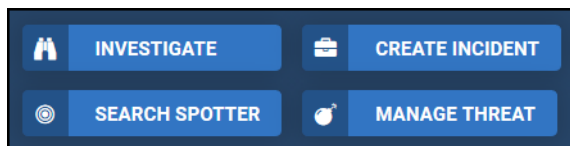


Type text to chat with the other viewers for this incident and click send icon.

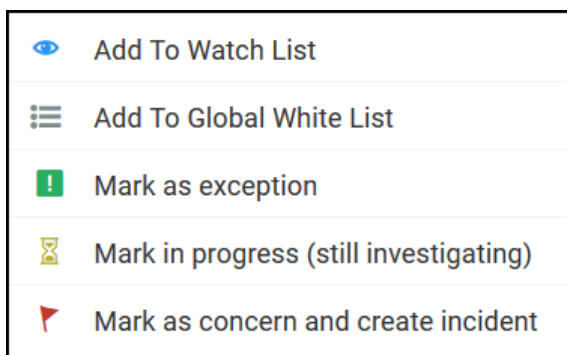


Actions

Click the menu on the right side of the screen to take actions on this entity.



- **Investigate:** Click to launch the Investigation Workbench to drill down into an entity and perform link analysis.
- **Search Spotter:** Click to launch Spotter to search events for this entity.
- **Create Incident:** Click to create a new case for this entity.
- **Manage Threat:** Click to take actions for this entity.



The list of threat actions affect user risk scores in the following ways:

Action	Result
Add to Watch List	Add entity to selected Watch List.
Add to Global White List	Add entity to Global White List to approve activity that would otherwise result in a violation
Mark as Exception	Reduce the entity's risk score to zero.
Mark in Progress (still Investigating)	Retain the entity's existing risk score.
Mark as concern and create incident	Retain the entity's existing risk score and creates an incident on the entity that will include all the violations performed by the entity

Example: Add to Watch List

The following example retains the entity's risk score and adds the entity to a selected Watch List.

To add the entity to a Watch List, click **Manage Threat > Add to Watch List**.

1. Complete the following form:

- **Watchlist:** Select an existing watch list from dropdown. For information about creating watch lists, see [Watch Lists](#) in the ArcSight UBA Administration Guide.
- **Reason:** Enter a reason for adding this entity to the watch list.
- **Expiry Date:** Enter a date on which the entity will be removed from the watch list.
- **Confidence Level:** Indicate a value from 0 to 1 how confident you are the violator should be placed on the selected watch list.

2. Click Add.

The entity will appear in the selected watch list until the expiry date. To view and manage watch lists, see [Views](#).

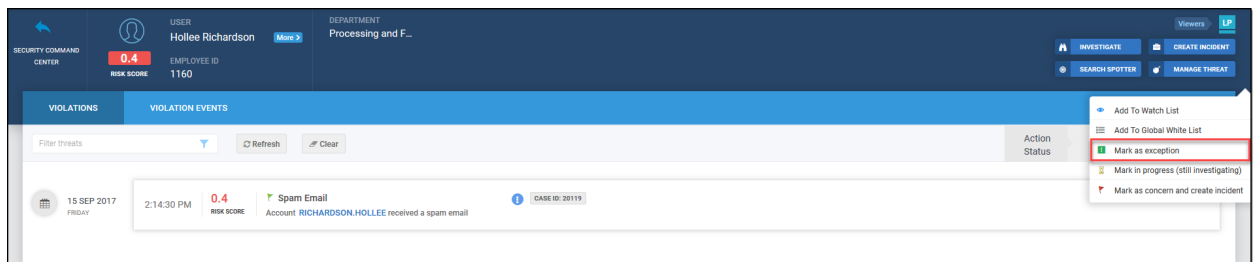
Example: Mark as Exception

The following example reduces the violator's risk score:

In this case, the risk score for this entity is 0.4.



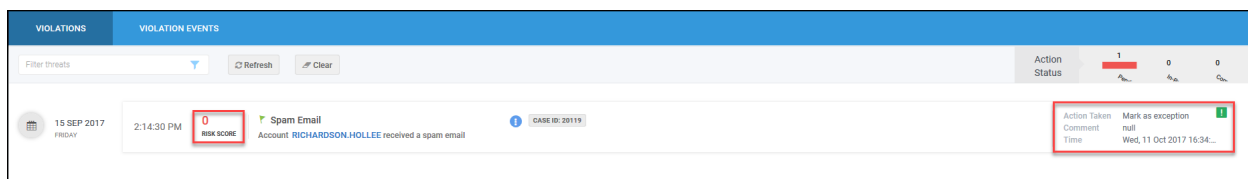
1. Review the violation and determine that it is an exception.
2. Select **Mark as Exception** from the **Manage Threat** menu.



3. (Optional) Provide a comment to indicate why you are marking the entity an exception.

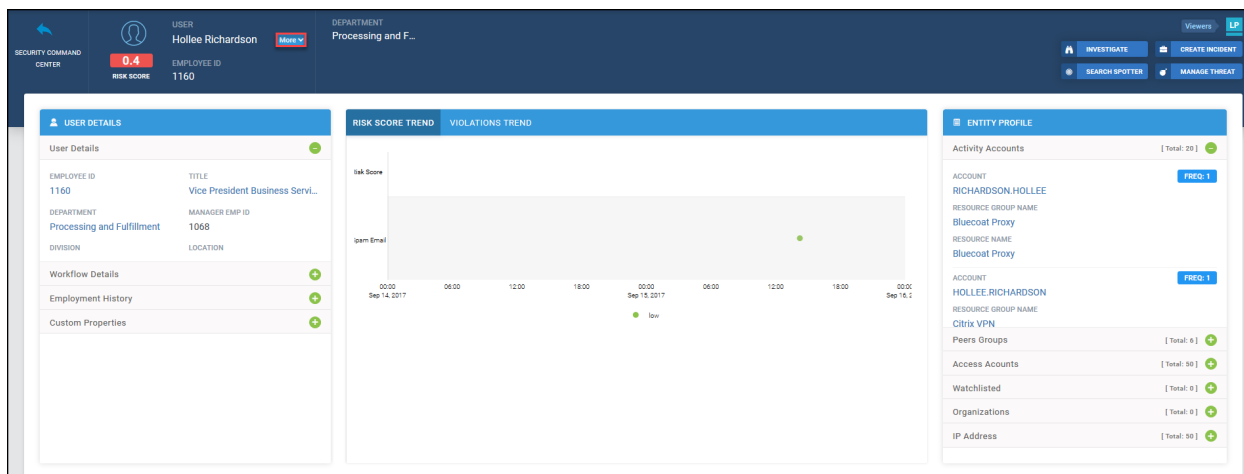
The screenshot shows a dialog box titled 'Action - Mark as exception'. It contains a 'Comments' section with a large text area for input. At the bottom right of the dialog is a 'Submit' button.

The summary for this entity will display **Action Taken** as **Mark as Exception**, and the risk score will be reduced to 0.



Entity Details

Click **+/-** to expand/collapse details about the entity.



Example: User Details



Note: This section will be labeled differently and include different information for the different entity types: Users, Activity Accounts, Resources, and Network Addresses.

Click a value to launch Spotter for that attribute.

USER DETAILS

User Details

EMPLOYEE ID

1160

TITLE

Vice President Business Servi...

DEPARTMENT

Processing and Fulfillment

MANAGER EMP ID

1068

DIVISION

→ Launch Spotter

Workflow Details

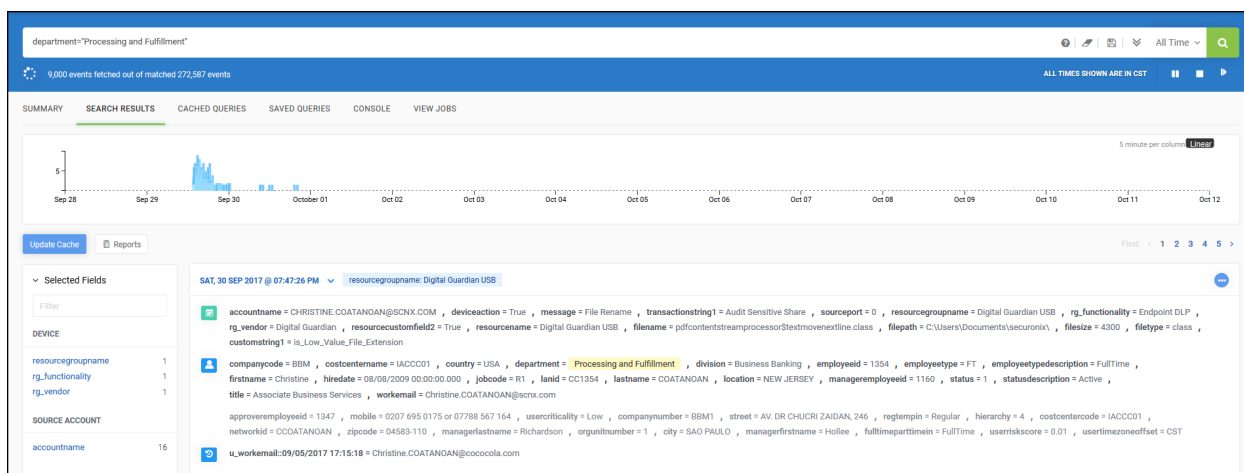
+

Employment History

+

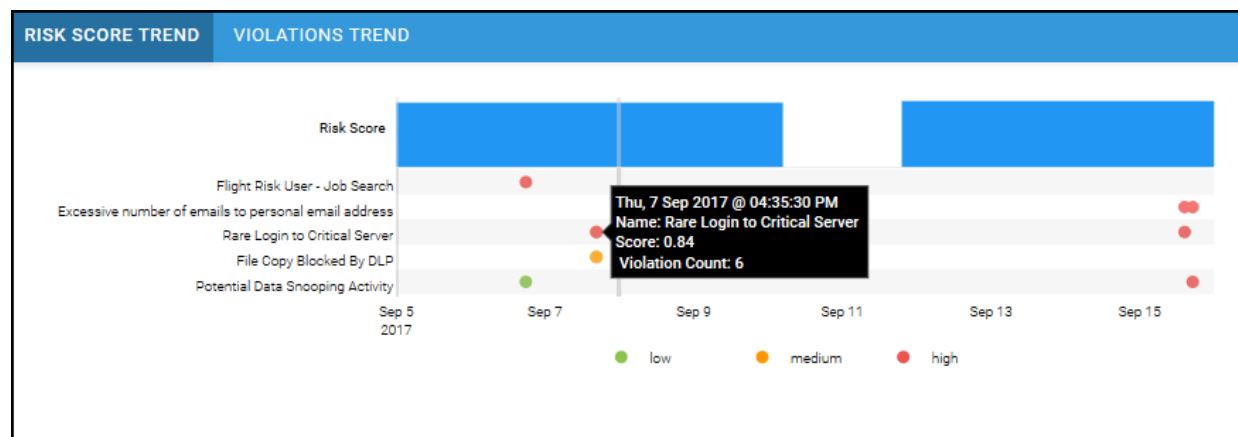
Custom Properties

+



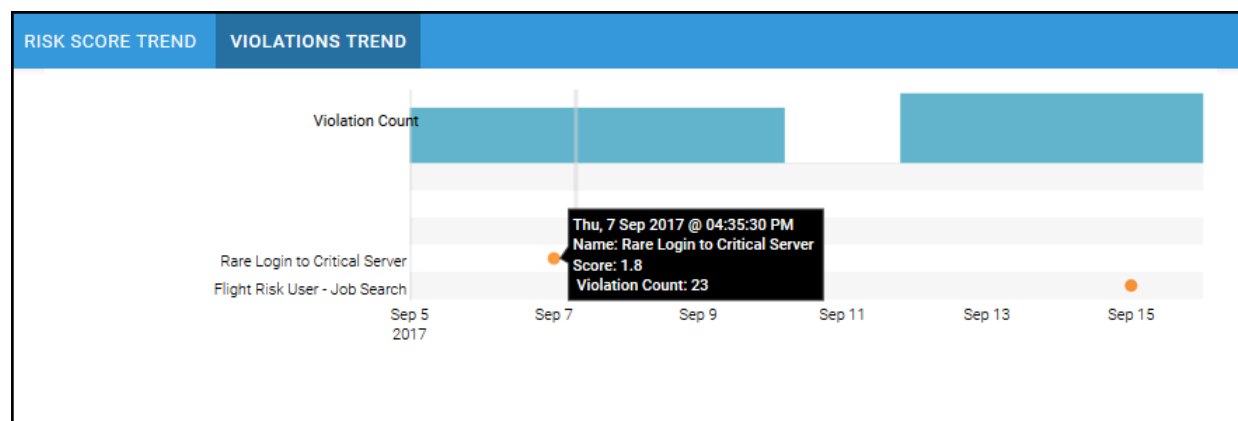
Risk Score Trend

Hover over any data point on the chart to view details.




Violations Trend

Hover over any data point on the chart to view details.




Entity Profile

Click +/- to expand/collapse objects associated with this entity.

 ENTITY PROFILE

Activity Accounts

[Total: 20] 

ACCOUNT

[RICHARDSON.HOLLEE](#)

RESOURCE GROUP NAME

[Bluecoat Proxy](#)

RESOURCE NAME

[Bluecoat Proxy](#)

FREQ: 1

ACCOUNT


[HOLLEE.RICHARDSON](#)

RESOURCE GROUP NAME


[Citrix VPN](#)

FREQ: 1


Peers Groups

[Total: 6] 


Access Accounts

[Total: 50] 


Watchlisted

[Total: 0] 

Organizations

[Total: 0] 

IP Address

[Total: 50] 

Click any object to launch Spotter to view events associated with that object.

ENTITY PROFILE

Activity Accounts [Total: 20]

CITRIX VPN

RESOURCE NAME
Citrix VPN

ACCOUNT **HOLLEE.RICHARDSON** **FREQ: 1**

Launch Spotter

RESOURCE NAME
Citrix VPN

ACCOUNT **FREQ: 1**

Peers Groups [Total: 6]

Access Accounts [Total: 50]

Watchlisted [Total: 0]

Organizations [Total: 0]

IP Address [Total: 50]

Violations

Perform the following actions from this section:

VIOLATIONS **VIOLATION EVENTS**

Filter threats

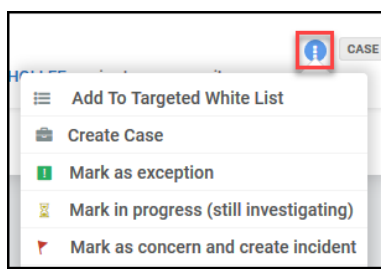
Action Status **1** **0** **0**

15 SEP 2017 **2:14:30 PM** **0.4** **Spam Email** **CASE ID: 20119**

Account RICHARDSON.HOLLEE received a spam email

Click the collapsed menu to take action at the violation level.

See [Actions](#) for more information about taking actions for entities and violations.



Note: Click a violation to view more information about the [Threats](#) or the [Policies](#) violated.

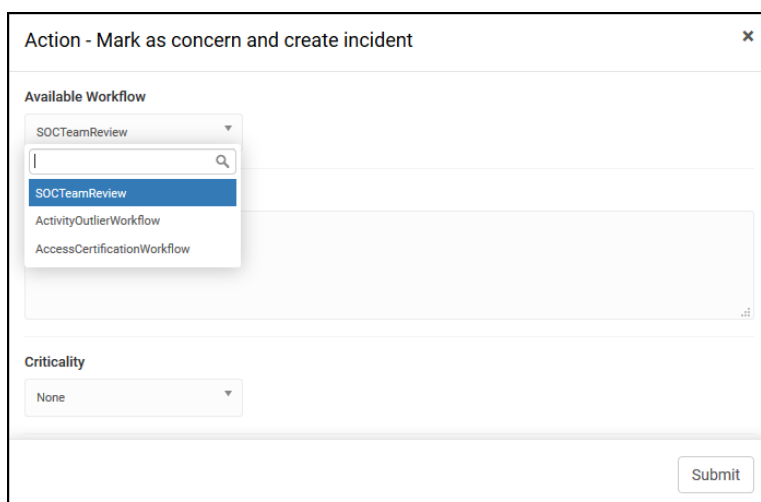
Example: Mark as concern and create incident

The following example retains the entity and violation risk score and creates an incident for the individual violation:

In this case, the risk score for this user is 108.11, and the score for the policy **Potential Data Snooping Activity** is 1.8.

VIOLATIONS	VIOLATION EVENTS
15 SEP 2017 FRIDAY	<p>5:04:32 PM 0.87 RISK SCORE Excessive number of emails to personal email address ⓘ</p> <p>2:29:41 PM 100 RISK SCORE ⚠ Insider Threat ⓘ</p> <p>2:29:32 PM 1.8 RISK SCORE ⚠ Potential Data Snooping Activity ⓘ</p>
07 SEP 2017 THURSDAY	<p>4:35:30 PM 0.84 RISK SCORE ⚠ Rare Login to Critical Account HARRY.OGWA ⓘ</p>
06 SEP 2017 WEDNESDAY	<p>6:14:39 PM 4.6 RISK SCORE 🟢 File Copy Blocked By DLP Account OGWA.HARRY performed File Copy from ipaddress 73.165.233.229 ⓘ</p> <p>5:50:13 PM 0 RISK SCORE ⚠ Flight Risk User - Job Search ⓘ</p>

1. Review the violation and determine that it is a concern.
2. Select **Mark as concern and create incident** from the collapsed menu.
3. Select a workflow to open a case for this violation.



The screenshot shows a modal dialog titled "Action - Mark as concern and create incident". Inside the dialog, there is a section labeled "Available Workflow" which contains a search bar and a list of workflow options. The first option, "SOCTeamReview", is selected and highlighted in blue. Below it are "ActivityOutlierWorkflow" and "AccessCertificationWorkflow". At the bottom of the dialog, there is a "Criticality" dropdown menu currently set to "None", and a "Submit" button.

4. (Optional) Provide a comment to indicate why you are marking the threat a concern and creating an incident.

The risk score for this policy remains 1.8. A new incident has been created for the violation. The case number appears beside the collapsed menu on the violation. For information about managing cases, see [Incident Management](#).

VIOLATIONS		VIOLATION EVENTS	
Filter threats		Refresh	Clear
15 SEP 2017 FRIDAY	5:04:32 PM	0.87 RISK SCORE	Excessive number of emails to personal email address ⓘ
	2:29:41 PM	100 RISK SCORE	Insider Threat ⓘ
	2:29:32 PM	1.8 RISK SCORE	Potential Data Snooping Activity ⓘ CASE ID: 20119
07 SEP 2017 THURSDAY	4:35:30 PM	0.84 RISK SCORE	Rare Login to Critical Server ⓘ Account HARRY.OWA performed An account was successfully logged on
	6:14:39 PM	4.6 RISK SCORE	File Copy Blocked By DLP ⓘ Account OGWA.HARRY performed File Copy from ipaddress 73:165:233:229
06 SEP 2017 WEDNESDAY	5:50:13 PM	0 RISK SCORE	Flight Risk User - Job Search ⓘ

Manage the new case from the [Incident Management](#) dashboard.

Violation Events

Click **Violation Events** view individual events associated with the entity.

For information about the actions you can take from this section, see [Spotter](#).

Violations

VIOLATION EVENTS

index = violation and accountname = "SVC_SNYPR6" and resourcegroupname = "Windows Data" and generationtime between "08/12/2017 17:40:53" "10/11/2017 17:42:18"

4 events fetched out of matched 4 events

ALL TIMES SHOWN ARE IN CST

Show Fields Reports

SUN, 3 SEP 2017 @ 01:15:17 PM resourcegroupname: Windows Data policyname: Audit log tampering

accountname = SVC_SNYPR6, sourceuserprivileges = S-1-5-18, eventoutcome = Log clear, message = The audit log was cleared, sourceprocessname = Microsoft-Windows-Eventlog, transactionstring1 = Security, sourcedomain = ADS-1.scnx.com, devicehostname = DALWIN06, resourcegroupname = Windows Data, devicecustomstring4 = Critical Asset Server, resourcegroupname = Windows Data, baseeventid = null, flowsemid = 0x3e7, categorybehavior = Administration, categoryobject = Device, deviceeventcategory = Creation

category = ACCOUNT MISUSE, policyname = Audit log tampering, riskthreatname = Audit Log Tampering, violator = Activityaccount

SUN, 3 SEP 2017 @ 11:04:55 AM resourcegroupname: Windows Data policyname: Privilege Escalation

accountname = SVC_SNYPR6, sourceuserprivileges = S-1-5-21-205380880-396673830-332456454-500, destinationprivileges = VPN_users, deviceaction = Success, message = A member was added to a security-enabled global group, transactionstring1 = Security, sourcedomain = ADS-1.scnx.com, destinationusername = svc_bkp, destinationuserprivileges = S-1-5-18, resourcegroupname = Windows Data, devicecustomstring4 = Critical Asset Server, resourcegroupname = Windows Data, baseeventid = null, destinationdomain = ADS-1.scnx.com, categorybehavior = Administration, categoryobject = Device, deviceeventcategory = Disabled

category = ACCOUNT MISUSE, policyname = Privilege Escalation, riskthreatname = Privilege Escalation, violator = Activityaccount

SUN, 3 SEP 2017 @ 10:02:00 AM resourcegroupname: Windows Data policyname: Privilege Escalation

accountname = SVC_SNYPR6, sourceuserprivileges = S-1-5-18, deviceaction = Success, message = A user account was created, sourceprocessname = Microsoft-Windows-Security-Auditing, transactionstring1 = Security, sourcedomain = ADS-1.scnx.com, destinationusername = svc_bkp, destinationuserprivileges = S-1-5-21-205380880-396673830-332456454-500, devicehostname = DALWIN06, resourcegroupname = Windows Data, devicecustomstring4 = Critical Asset Server, resourcecustomfield3 = User Account Management, resourcegroupname = Windows Data, baseeventid = null, destinationdomain = ADS-1.scnx.com, categorybehavior = Administration, categoryobject = Device, deviceeventcategory = Disabled

category = ACCOUNT MISUSE, policyname = Privilege Escalation, riskthreatname = Privilege Escalation, violator = Activityaccount

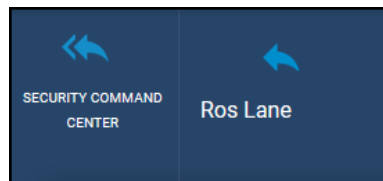
Violation Summary

Click a violation to view a detailed summary of the following:

- Analytics summary
- Violation summary
- Events related to the violation
- Remediation steps to take for a violation
- Automated response playbook selected for the policy

The details displayed on the Violation Summary screen are configured when creating the policy and differ based on the analytical technique. For more information about configuring Violation Summaries, see [Policy Violations](#) in the ArcSight UBA Administration Guide.

To leave this screen, click **Security Command Center** or **[Entity Name]**.

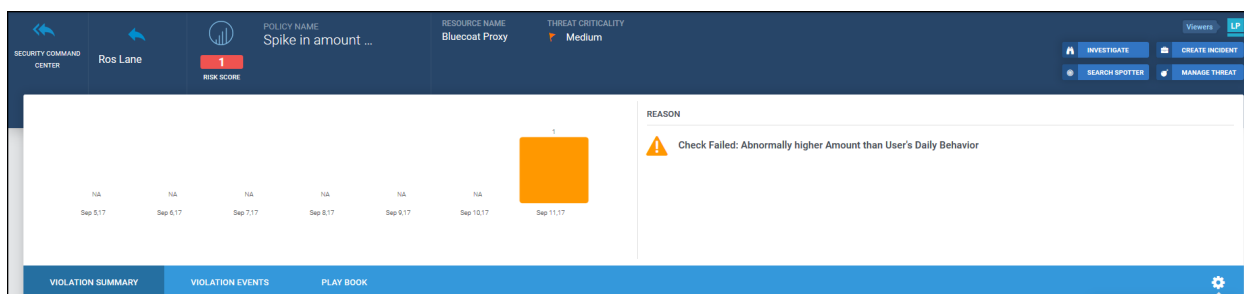


You can perform several actions from the Violations Summary screen:



Note: The views and available actions for each violation differ based on the analytical type and the configurations for the policy.

View a graph of the violations and reason the policy was flagged as a violation.

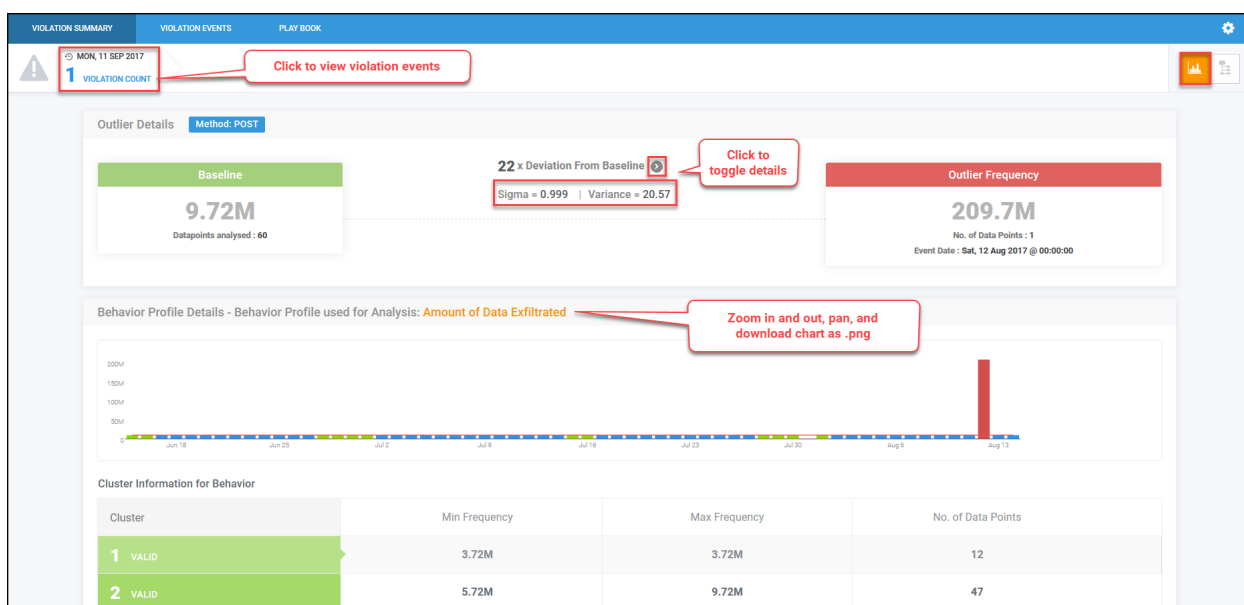


Analytical Summary

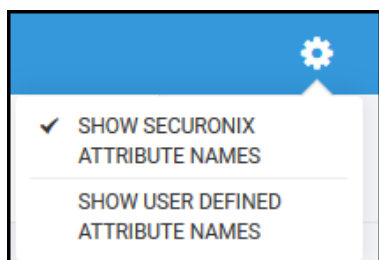
Click bar graph icon to view the Analytical Summary for the violation.



Note: This option will appear for behavior-based violations.



Click the gear icon to view Securonix attribute names or User-defined attribute names. For information about user-defined attributes, see [Activity Data](#) in the ArcSight UBA Administration Guide.

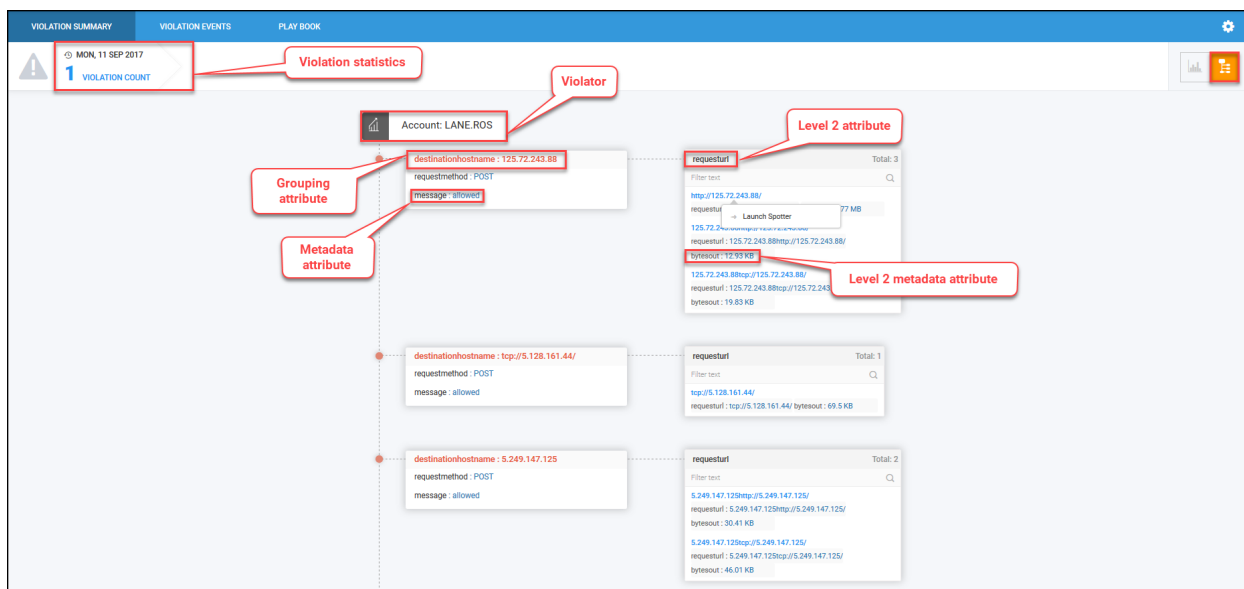


Summary View

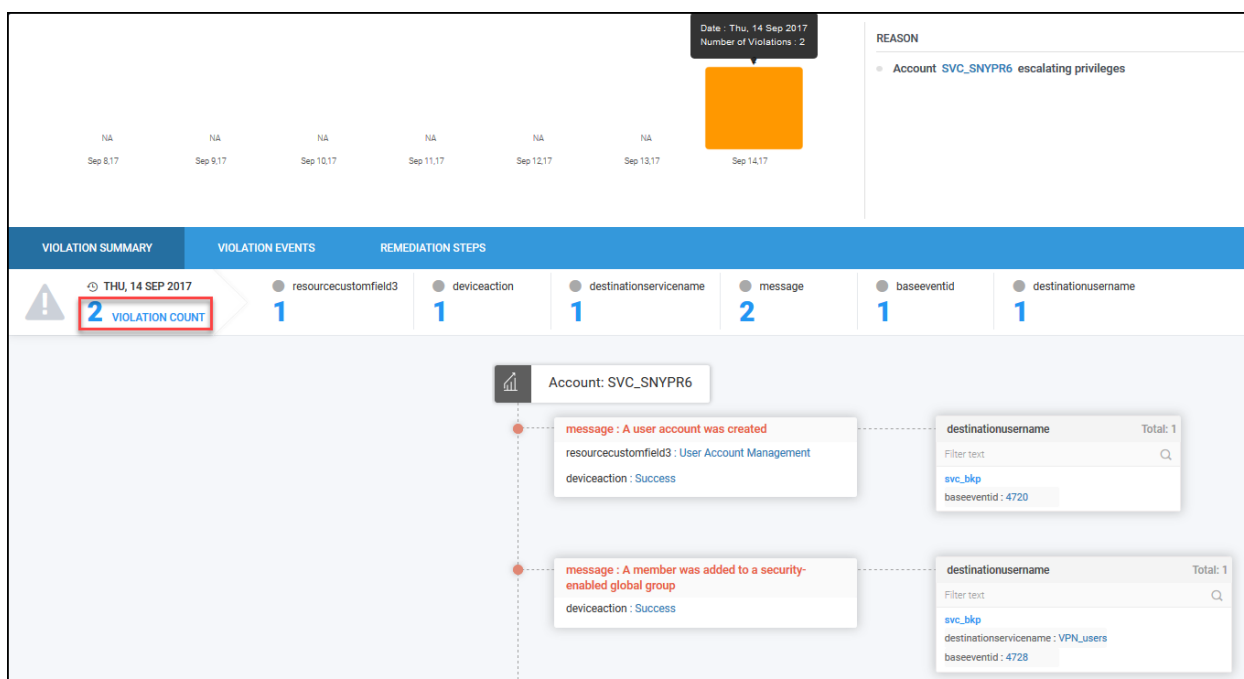
Click tree icon to view the summary of the violation configured during [Policy Violations Step 3: Choose Action for Violation](#).



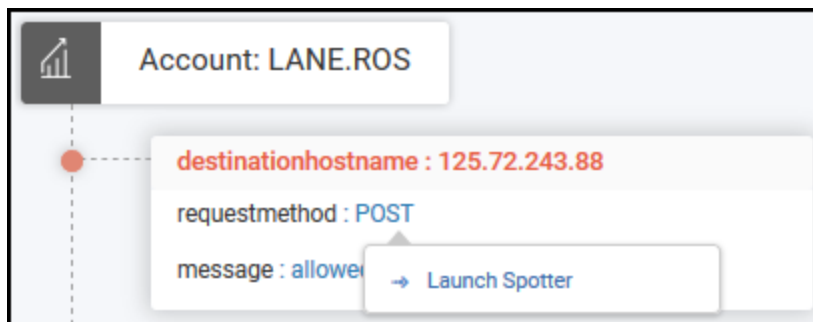
Note: The violation summary will display different information based on the Action Filters enabled in [Activity Data](#) and the analytical technique configured in the Policy. For more information, see the ArcSight UBAA Administration Guide.



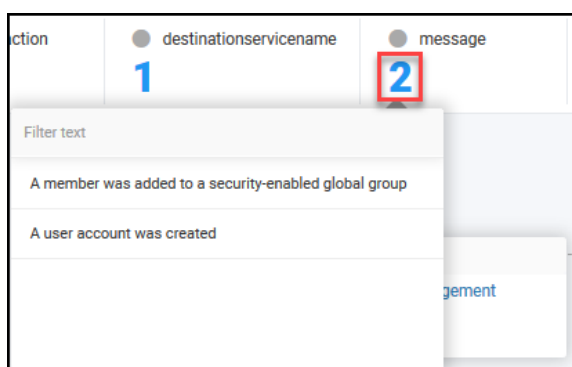
Click a point on the time line to filter Violation Summary to view only those events.



Click any value to launch Spotter.



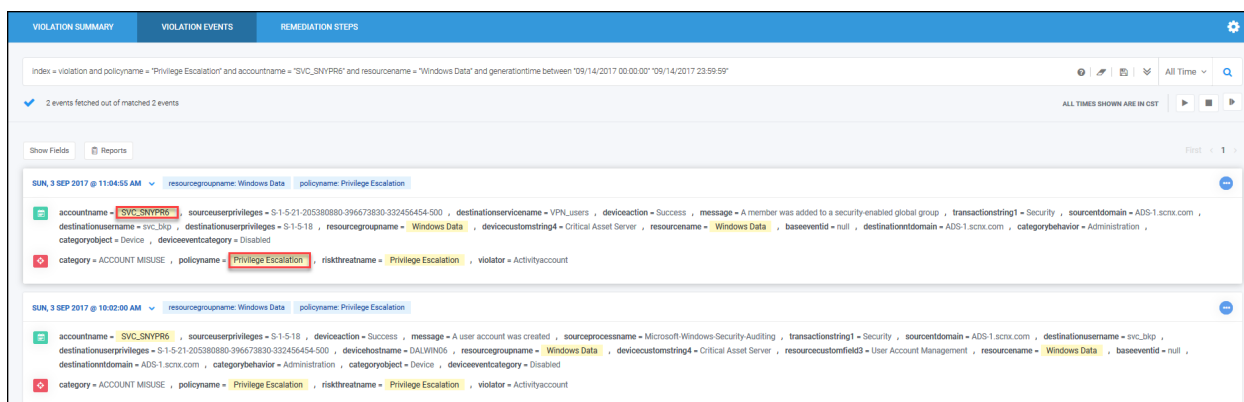
Click an attribute value in violation statistics to filter the summary.



Violation Events

Click **Violation Events** view individual events associated with the policy violation.

For information about the actions you can take from this section, see [Spotter](#).



Remediation Steps

View and complete **Remediation Steps** for this policy. Click links in this section to perform actions such as creating support tickets.



Note: Remediation Steps appear if they are configured for the policy. Configure Remediation Steps during [Policy Violations Step 1: Define Policy](#).

VIOLATION SUMMARY	VIOLATION EVENTS	REMEDIAL STEPS
<ol style="list-style-type: none"> 1 Check the initial level privileges 2 Contact ITops Administrator to get more insight into his privileges 3 Submit a ticket to investigate further 		

Play Book

In ArcSight UBA, play books contain and describe the entire incident and response management lifecycle for a violation by combining automated tasks such as gathering context on the violation and creating support tickets with the manual tasks the analyst must complete when a violation occurs.



Note: Play books appear if they are selected for the policy during policy creation. For more information about using Play Books in ArcSight UBA, see [Automated Response](#).

Automated and completed tasks will appear with a green check mark.

Healthcare Security Breach Playbook

Task #1 Notify
Notify the Privacy Breach Office
Task not executed

Task #2 JIRA : Open Ticket
Open a ticket in JIRA
Task not executed

Task #3 LDAP : Disable Account
Demisto - Disable account in LDAP
Fri, 29 Sep 2017 @ 19:10:23

Healthcare Security Breach Playbook
Handles the security breach by notifying the privacy teams and disables the account

Fri, 29 Sep 2017 @ 19:10:23

Task #1 LDAP : Disable Account
Demisto - Disable account in LDAP

Incident IDs

Indicates the number of times the play book was run and the time and date of the last time the play book launched.

Indicates task status

Indicates the task launched successfully.

Select a play book to launch from the drop down if multiple play books are enabled for this threat indicator.

Disable Account

Disable Account

Open Ticket

Demisto - Disable account in LDAP

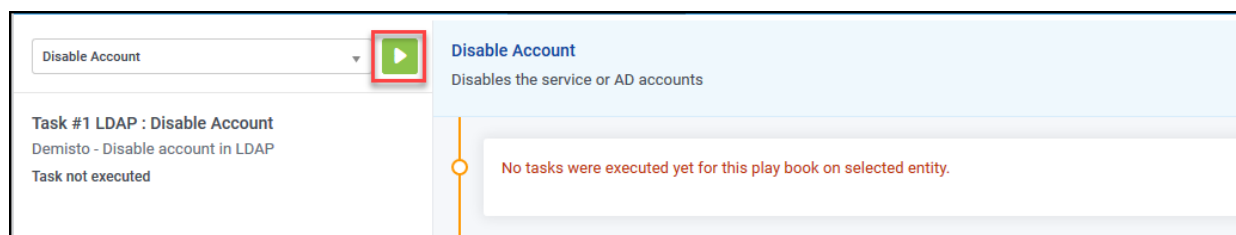
Task not executed

Disable Account

Disables the service or AD accounts

No tasks were executed yet for this play book on selected entity.

Click play icon to launch the play book if **Auto Play** is not enabled or to run automated tasks again.



Disable Account

Task #1 LDAP : Disable Account
Demisto - Disable account in LDAP
Task not executed

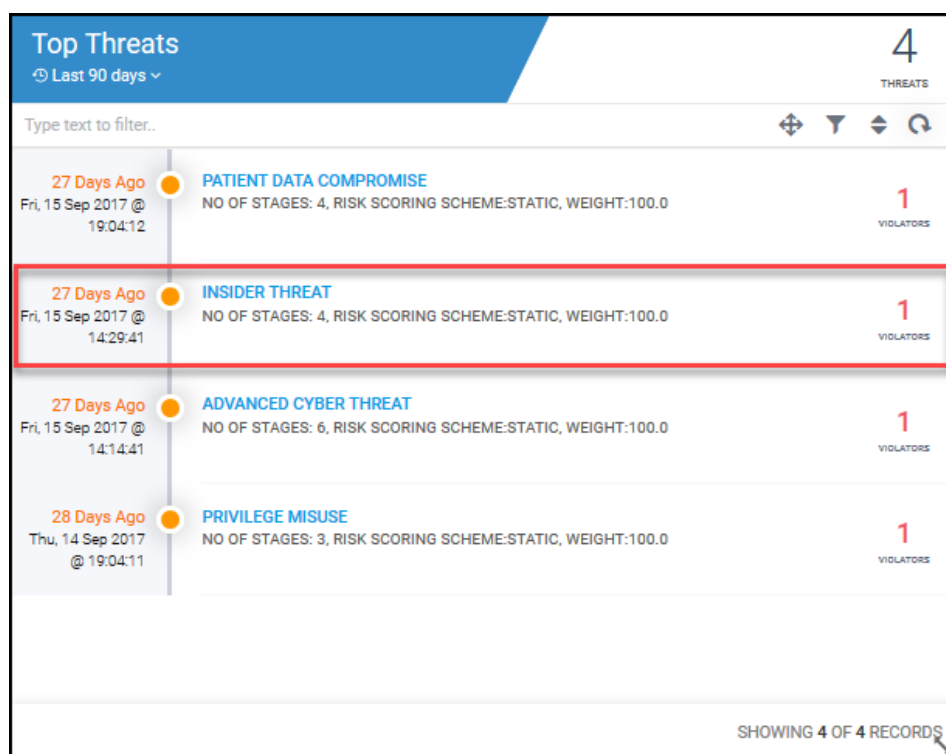
Disable Account
Disables the service or AD accounts

No tasks were executed yet for this play book on selected entity.

Threats

Threat models feature stages that include one or more policy violations to detect a specific type of threat. For more information about Threat Models, see [Threat Modeler](#) in the ArcSight UBA Administration Guide.

To view the threat summary screen, click a threat from one of the dashboards in the Security Command Center. Example: Top Threats.



Top Threats
Last 90 days

Type text to filter...

Time Ago	Threat Name	Details	Violators
27 Days Ago Fri, 15 Sep 2017 @ 19:04:12	PATIENT DATA COMPROMISE	NO OF STAGES: 4, RISK SCORING SCHEME:STATIC, WEIGHT:100.0	1 VIOLATORS
27 Days Ago Fri, 15 Sep 2017 @ 14:29:41	INSIDER THREAT	NO OF STAGES: 4, RISK SCORING SCHEME:STATIC, WEIGHT:100.0	1 VIOLATORS
27 Days Ago Fri, 15 Sep 2017 @ 14:14:41	ADVANCED CYBER THREAT	NO OF STAGES: 6, RISK SCORING SCHEME:STATIC, WEIGHT:100.0	1 VIOLATORS
28 Days Ago Thu, 14 Sep 2017 @ 19:04:11	PRIVILEGE MISUSE	NO OF STAGES: 3, RISK SCORING SCHEME:STATIC, WEIGHT:100.0	1 VIOLATORS

SHOWING 4 OF 4 RECORDS

From this screen you can:

- View information about a threat
- Take action to manage the threat including:
 - Create an incident at the threat level for all violators
 - Manage threat at the entity level for a single violator
- Use chat to collaborate on violations within their groups
- Drill down into the violation to view a detailed summary of the violations

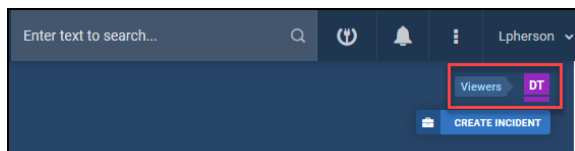
Actions

Click Create Incident on the right side of the screen to create a case at the policy level for all violators.

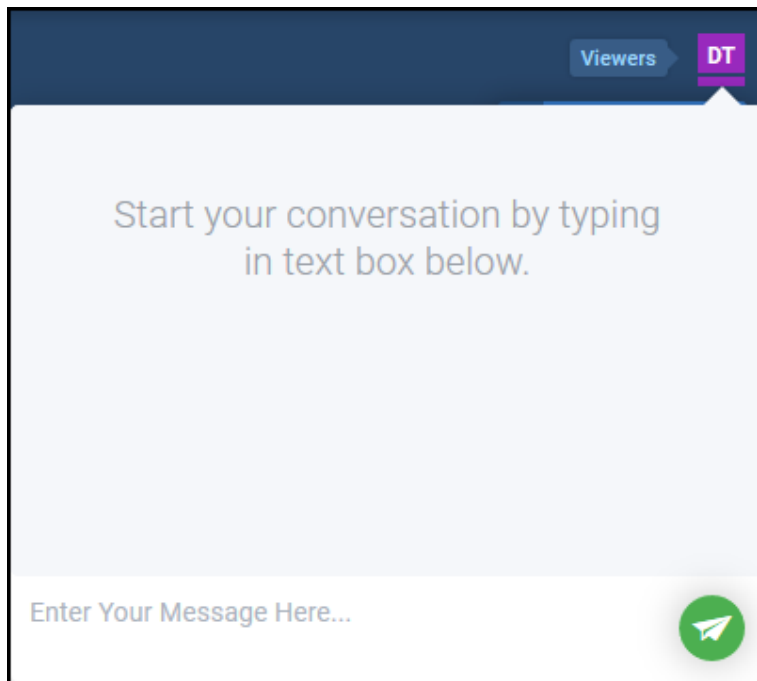


Chat

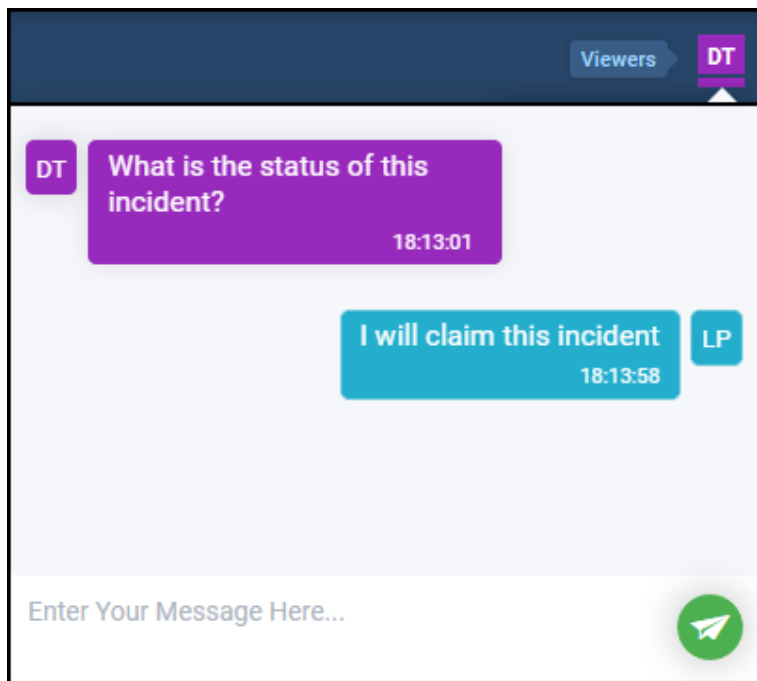
ArcSight UBA 6.10 includes chat capability to allow analysts to easily collaborate on violations and incidents within their groups. The initials of the other users viewing the violation will appear at the top right of the screen.



Click the initials of the user with whom you wish to chat to launch the chat window.

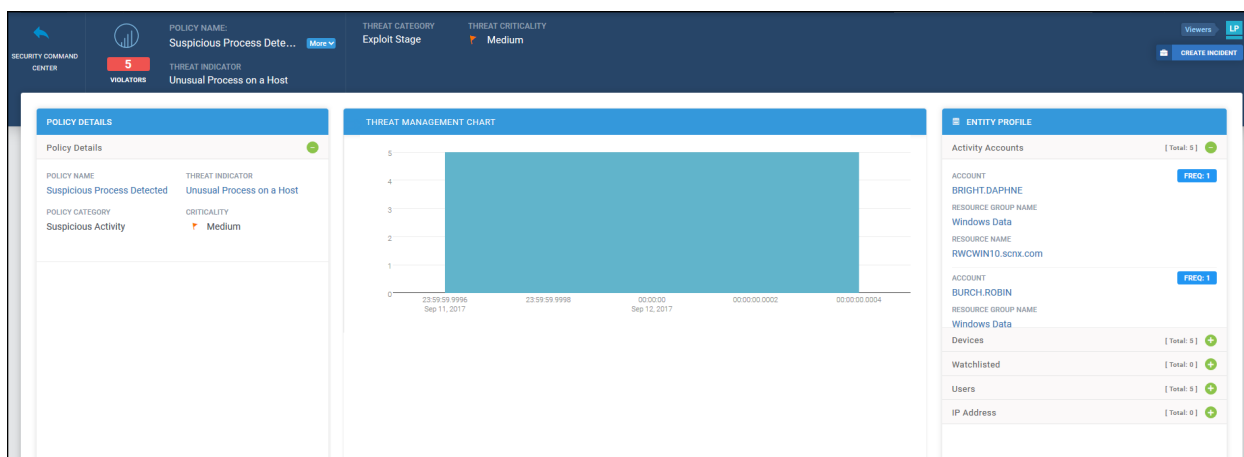


Type text to chat with the other viewers for this incident and click send icon.

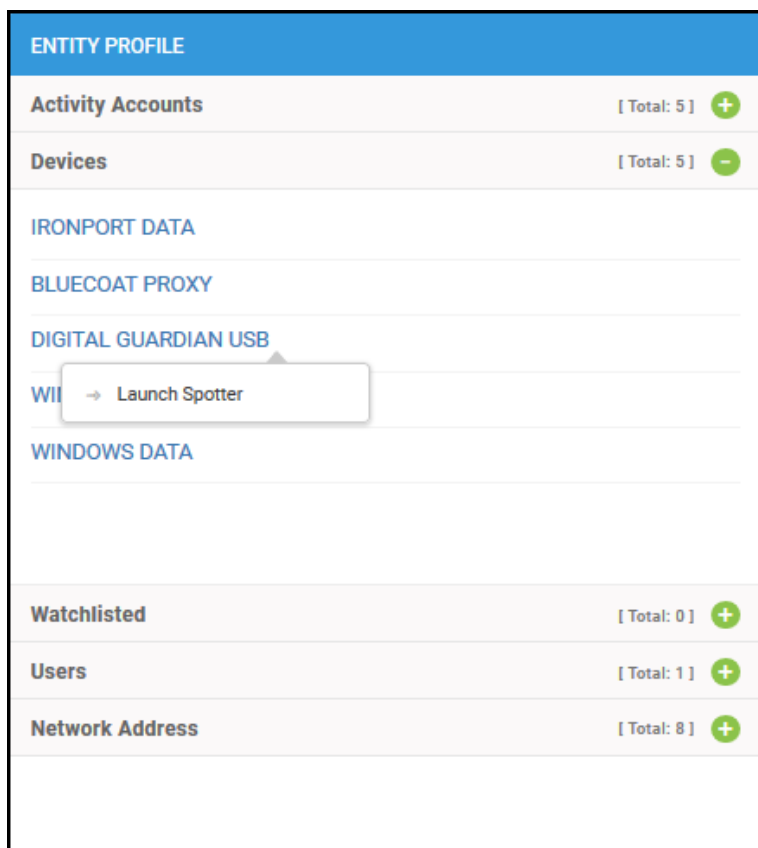


Threat Model Details

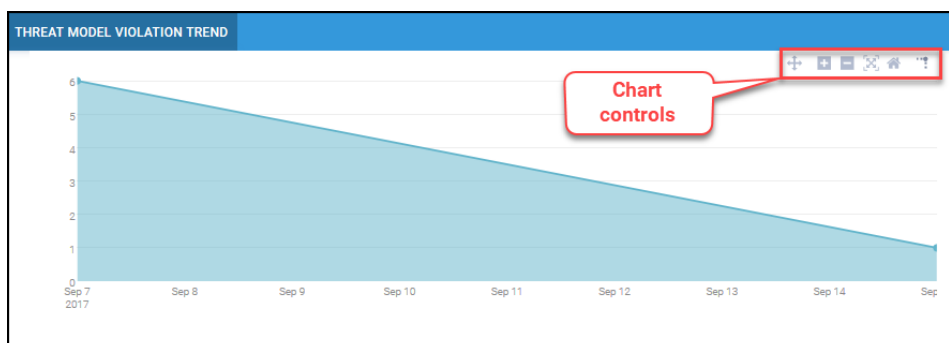
Click **More** to view more details about the threat model.



Click a data point in the details to launch Spotter.



Pan, zoom in, and zoom out of the Threat Model Violation Trend.



Click +/- to expand/collapse details in the Entity Profile.

ENTITY PROFILE	
Activity Accounts	[Total: 5] +
Devices	[Total: 5] +
Watchlisted	[Total: 0] +
Users	[Total: 1] +
Network Address	[Total: 8] -
224.99.147.239	
73:165:233:229	
10.0.1.63	
172.24.78.16	
10.0.1.61	
10.1.5.95	
172.18.114.53	

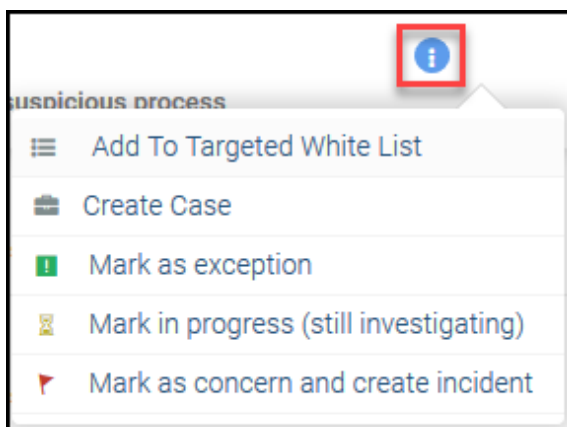
Violators

View the list of entities that have violated the threat model.

VIOLATORS		VIOLATION EVENTS	
Filter violators		Sort Refresh Clear	Action Status 5 0 0
12 SEP 2017 TUESDAY	8:25:54 PM	0.6 RISK SCORE	DALWIN03.scnx.com DALWIN03.scnx.com initiated a suspicious process
	8:25:54 PM	0.6 RISK SCORE	RWCWIN09.scnx.com RWCWIN09.scnx.com initiated a suspicious process
	8:25:54 PM	0.6 RISK SCORE	RWCWIN10.scnx.com RWCWIN10.scnx.com initiated a suspicious process
	8:25:54 PM	0.6 RISK SCORE	DALWIN32.scnx.com DALWIN32.scnx.com initiated a suspicious process
	8:25:54 PM	0.6 RISK SCORE	NJCWIN01.scnx.com NJCWIN01.scnx.com initiated a suspicious process
First 1 Last		TOTAL 5	

You can complete the following actions:

- Enter text to filter violators.
- Click **Sort** to sort by **Generation Time** or **Risk Score**.
- Click **Refresh** to refresh results list.
- Click **Clear** to clear filters.
- View **Action Status** for the Violators.
- Click the collapsed menu to take action on the violator.



See [Entities](#) for more information about taking actions on violators.

Violation Events

Click **Violation Events** view individual events associated with the threat model violation.

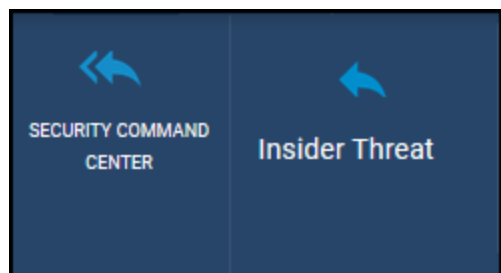
For information about the actions you can take from this section, see [Spotter](#).

The screenshot shows the 'VIOLATIONS' tab in the Security Command Center. It displays a list of violations for the policy 'Excessive number of emails to personal email address'. The first violation is dated 'SUN, 3 SEP 2017 @ 11:21:00 PM' and involves an account named 'OWWA.HARRY' who sent an email to 'harry.ogwall8@gmail.com'. The email subject was 'Revenue Report FY' and the filename was 'FYRevenueReport2017.xlsx'. The violation is categorized as 'ACCOUNT MISUSE, DATA EXFILTRATION' and is associated with the risk 'Excessive Number of Emails Sent'. The user's details include: companycode = TECH, costcentername = INFCCC12, country = USA, department = Mainframe and Midrange Administration, division = Global Technology, employeeid = 1001, employeetype = FT, employeetypedescription = FullTime, firstname = HARRY, hiredate = 08/08/2009 00:00:00.000, jobcode = R1, lastid = H01001, lastname = OOWA, location = DALLAS, manageremployeeid = 1012, middlename = A, status = 1, statusdescription = Active, title = Vice President Mainframe and Midrange, workemail = HARRY.OOWA@scom.com, workphone = 9723451278, approveremployeeid = 1082, mobile = 0151 709 7593, lastperformanceviewdate = 04/01/2014 00:00:00.000, usercriticality = Low, companynumber = TECH12, province = FL, street = 9000 SOUTHSIDE BLVD BLDG 600, reglempin = Regular, lastperformanceviewresult = Poor, costcentercode = INFCCC12, networkid = HOGWA, zipcode = 32256, organnumber = 12, city = JACKSONVILLE, managerfirstname = Joe, fulltimeparttimein = FullTime, usersriskscore = 0.01, userimezoneoffset = CST.

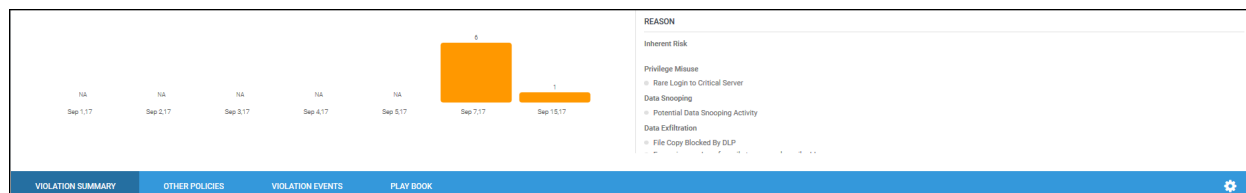
Violation Summary

You can perform several actions from the Violations Summary screen:

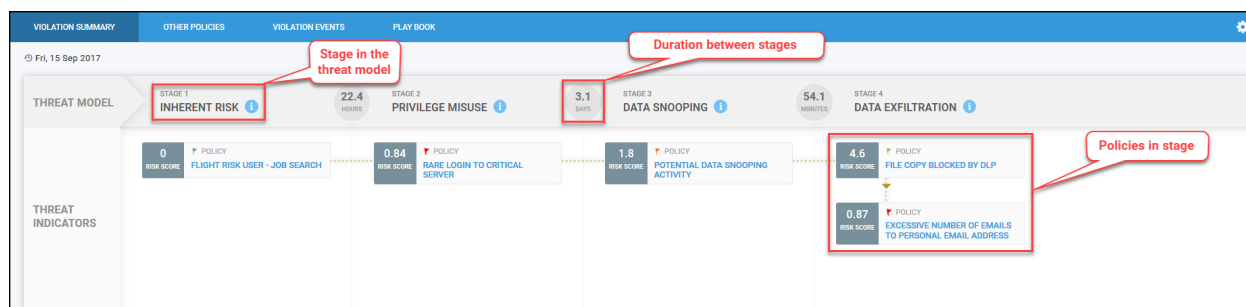
Click Back to **Security Command Center** or Back to **[Threat Name]** to leave this screen.



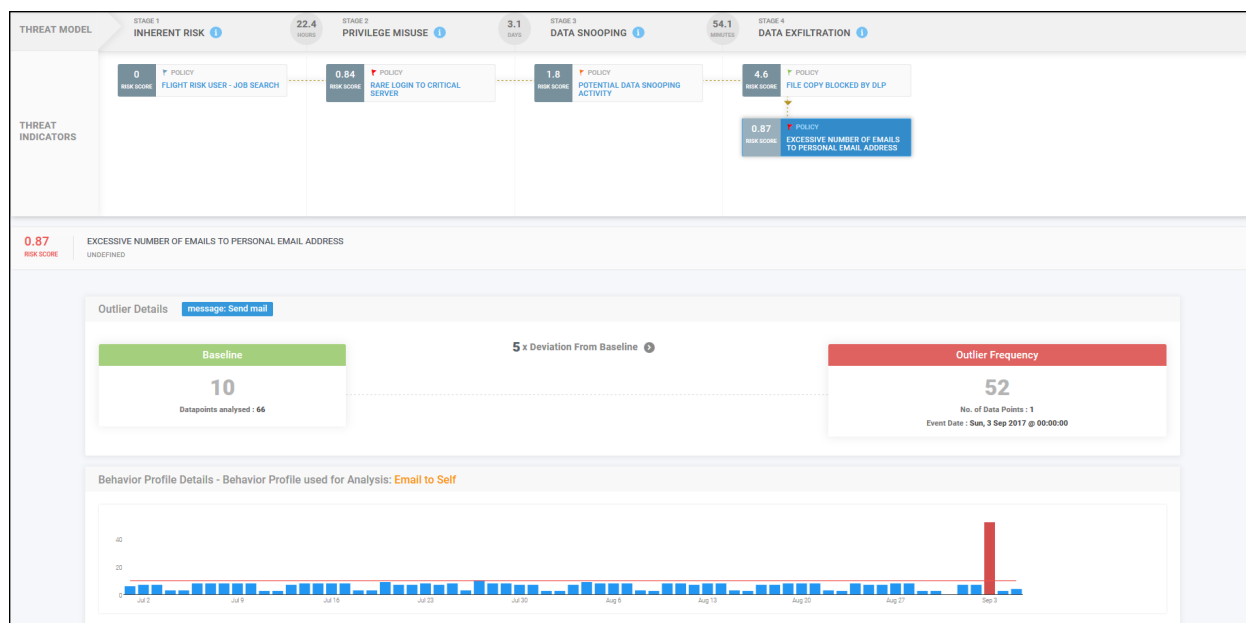
View a graph of the threat model and the list of policies that were violated.



View a summary of the stages of the threat model. This summary includes the Threat Model stages, Threat Indicators (policies within the stages), and the duration of time between each violation.



Click a policy to view a violation summary. See [Entities](#) for more information about Violation Summaries.



Other Policies

View other policies violated by this entity. See [Entities](#) for more information about actions you can take from this section.

VIOLATION SUMMARY	OTHER POLICIES	VIOLATION EVENTS	PLAY BOOK
15 SEP 2017 FRIDAY	5:04:32 PM 0.87 RISK SCORE	Excessive number of emails to personal email address	
	2:29:32 PM 1.8 RISK SCORE	Potential Data Snooping Activity	
06 SEP 2017 WEDNESDAY	6:14:39 PM 4.6 RISK SCORE	File Copy Blocked By DLP Account: OGWA.HARRY performed File Copy from Ipadress 73:165:233:229	
	5:50:13 PM 0 RISK SCORE	Flight Risk User - Job Search	
07 SEP 2017 THURSDAY	4:35:30 PM 0.84 RISK SCORE	Rare Login to Critical Server Account: HARRY.OWGA performed An account was successfully logged on	

Violation Events

Click the **Violation Events** tab to view the events associated with this threat model.

For information about the actions you can take from this section, see [Spotter](#).

Remediation Steps

View and complete **Remediation Steps** for this policy. Click links in this section to perform actions such as creating support tickets.



Note: Remediation Steps appear if they are configured for the policy. Configure Remediation Steps during **Step 1: Define Policy** when creating Policies.

VIOLATION SUMMARY	VIOLATION EVENTS	REMEDIALTION STEPS
<ol style="list-style-type: none"> 1 Check the initial level privileges 2 Contact IT Ops Administrator to get more insight into his privileges 3 Submit a ticket to investigate further 		

Play Book

In ArcSight UBA, play books contain and describe the entire incident and response management lifecycle for a violation by combining automated tasks such as gathering context on the violation and creating support tickets with the manual tasks the analyst must complete when a violation occurs.



Note: Play books appear if they are selected for the policy during policy creation. For more information about using Play Books in ArcSight UBA, see [Automated Response](#).

Automated and completed tasks will appear with a green check mark.

The screenshot shows the 'PLAY BOOK' tab in the Security Command Center. A dropdown menu is set to 'Healthcare Security Breach Playbook'. A red box highlights the play button icon, with an annotation stating: 'Indicates the number of times the play book was run and the time and date of the last time the play book launched.' Below the dropdown, a list of tasks is shown: 'Task #1 Notify', 'Task #2 JIRA : Open Ticket', and 'Task #3 LDAP : Disable Account'. A red box highlights the status 'Task not executed' for Task #2, with an annotation: 'Indicates task status'. Another red box highlights a green checkmark icon, with an annotation: 'Indicates the task launched successfully.' The main area shows a timeline for 'FRI, 29 SEP 2017 @ 19:10:23' with a task 'Task #1 LDAP : Disable Account' and a message 'Demisto - Disable account in LDAP'.

Select a play book to launch from the drop down if multiple play books are enabled for this threat indicator.

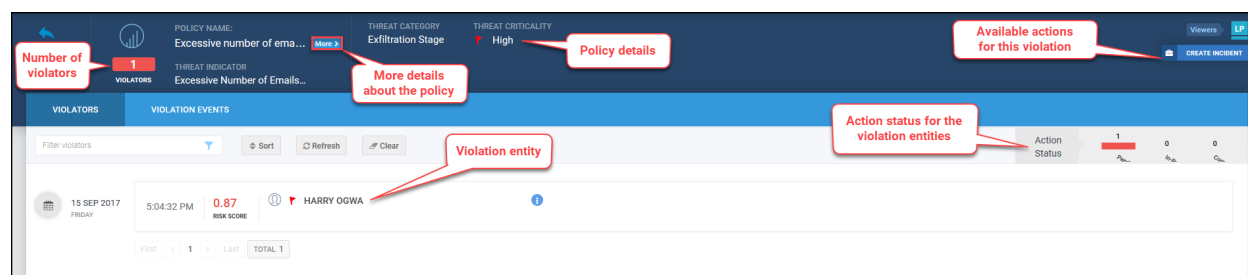
The screenshot shows the 'PLAY BOOK' tab with a dropdown menu open, displaying 'Disable Account' and 'Open Ticket'. A green play button icon is visible next to the dropdown. The main area shows the 'Disable Account' play book with the description 'Disables the service or AD accounts'. A message states: 'No tasks were executed yet for this play book on selected entity.'

Click play icon to launch the play book if **Auto Play** is not enabled or to run automated tasks again.

The screenshot shows the 'PLAY BOOK' tab with the 'Disable Account' play book selected. A red box highlights the green play button icon. The main area shows the 'Disable Account' play book with the description 'Disables the service or AD accounts'. A message states: 'No tasks were executed yet for this play book on selected entity.'

Policies

Click a policy violation from any dashboard on the Security Command Center to view the Violation Summary for a policy and manage the threat.



From this screen you can:

- View information about a policy
- Take action on the violation to manage the threat including:
 - Create an incident at the policy level for all violators
 - Manage threat at the entity level for a single violator
- Use chat to collaborate on violations within their groups
- Drill down into the violation to view a detailed summary of the violations

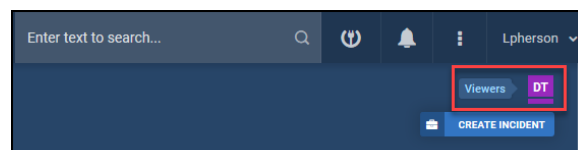
Actions

Click **Create Incident** on the right side of the screen to create a case at the policy level for all violators.

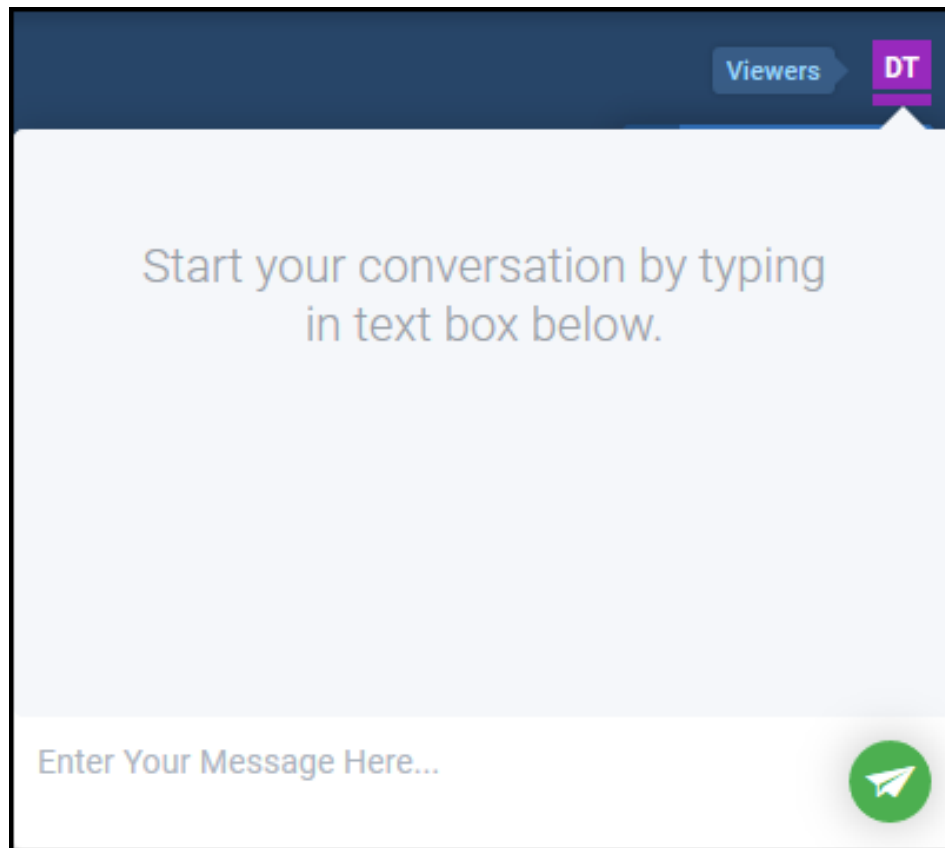


Chat

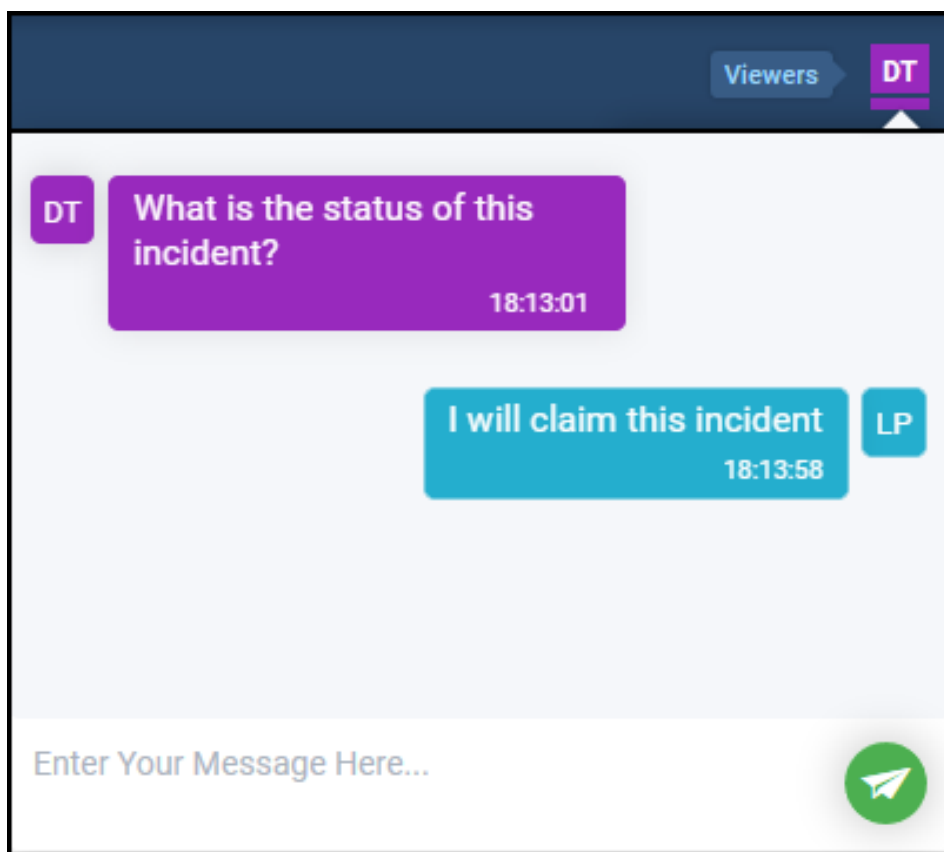
ArcSight UBA 6.10 includes chat capability to allow analysts to easily collaborate on violations and incidents within their groups. The initials of the other users viewing the violation will appear at the top right of the screen.



Click the initials of the user with whom you wish to chat to launch the chat window.

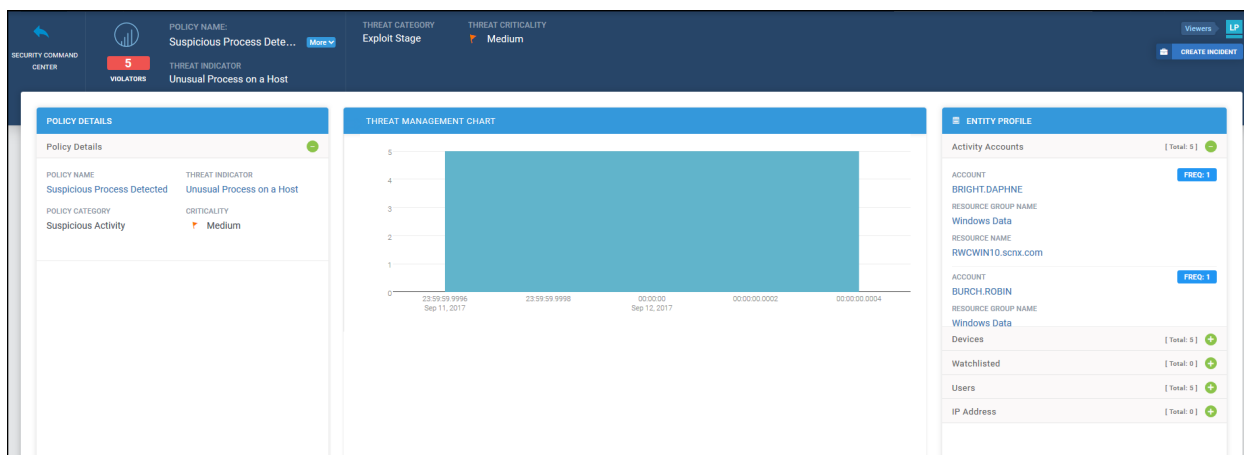


Type text to chat with the other viewers for this incident and click send icon.



Policy Details

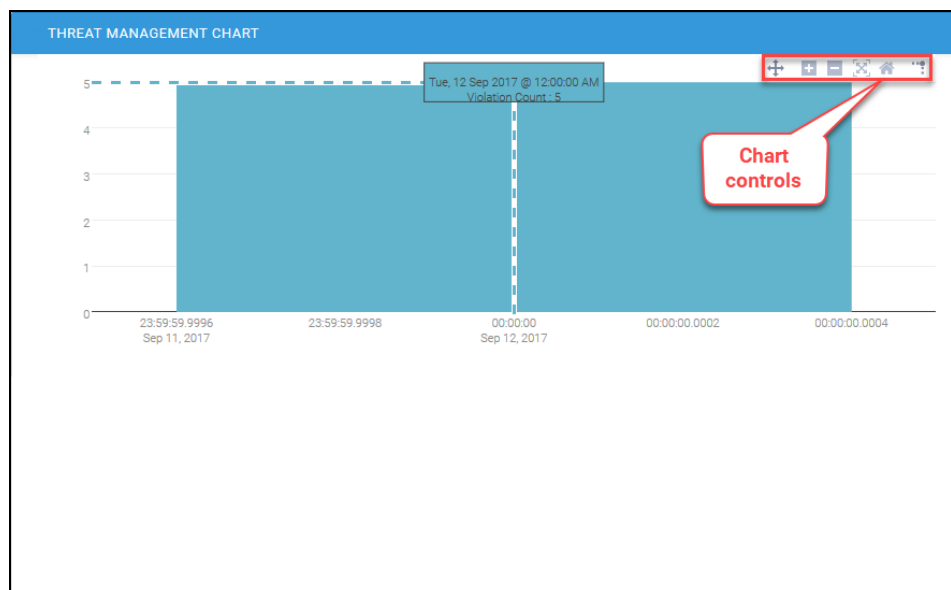
Click **More** to view more details about the policy.



Click a data point in the details to launch Spotter.

The screenshot shows the 'ENTITY PROFILE' page. At the top, there's a blue header with a menu icon and the text 'ENTITY PROFILE'. Below this, a section titled 'Activity Accounts' has a toggle switch set to 'Total: 5' with a minus sign. The main content area lists details for an account named 'BRIGHT.DAPHNE'. It includes fields for 'ACCOUNT', 'RESOURCE GROUP NAME' (Windows Data), and 'RESOURCE NAME' (RWCWIN10.scnx.com). A red box highlights a button labeled 'Launch Spotter' with a right-pointing arrow. To the right of this button is a 'FREQ: 1' button. Below these details, there's a section for 'BURCH.ROBIN' with similar fields. At the bottom, there are several expandable sections: 'Devices' (Total: 5, plus icon), 'Watchlisted' (Total: 0, plus icon), 'Users' (Total: 5, plus icon), and 'IP Address' (Total: 0, plus icon).

Pan, zoom in, and zoom out of the Threat Management Chart.



Click +/- to expand/collapse details in the Entity Profile.

ENTITY PROFILE

Activity Accounts	[Total: 5]	+
Devices	[Total: 5]	+
Watchlisted	[Total: 0]	+
Users	[Total: 5]	-

FIRST NAME

KEVIN

LAST NAME

milton

EMPLOYEE ID

1015

FIRST NAME

Daphne

LAST NAME

Bright

IP Address

[Total: 0]

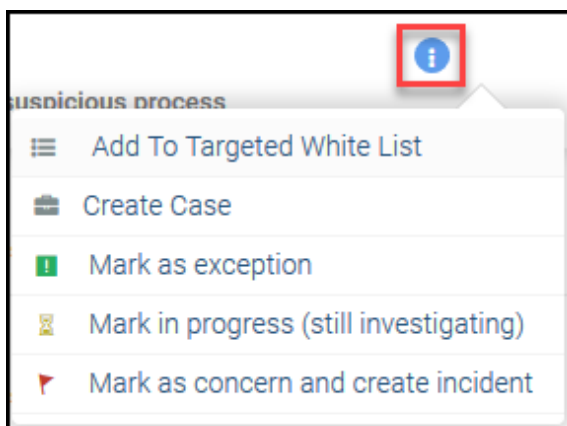
Violators

View the list of entities that have violated the policy.

VIOLATORS		VIOLATION EVENTS			
Filter violators		Sort	Refresh	Clear	Action Status
12 SEP 2017 TUESDAY		8:25:54 PM	0.6 RISK SCORE	DALWIN03.scnx.com DALWIN03.scnx.com initiated a suspicious process	5 0 0
		8:25:54 PM	0.6 RISK SCORE	RWCWIN09.scnx.com RWCWIN09.scnx.com initiated a suspicious process	
		8:25:54 PM	0.6 RISK SCORE	RWCWIN10.scnx.com RWCWIN10.scnx.com initiated a suspicious process	
		8:25:54 PM	0.6 RISK SCORE	DALWIN32.scnx.com DALWIN32.scnx.com initiated a suspicious process	Case ID: 81
		8:25:54 PM	0.6 RISK SCORE	NJCWIN01.scnx.com NJCWIN01.scnx.com initiated a suspicious process	
First		1	LAST	TOTAL 5	

You can complete the following actions:

- Enter text to filter violators.
- Click **Sort** to sort by **Generation Time** or **Risk Score**.
- Click **Refresh** to refresh results list.
- Click **Clear** to clear filters.
- View **Action Status** for the Violators.
- Click the collapsed menu to take action on the violator.



See [Entities](#) for more information about taking actions on violators.

Violation Events

Click **Violation Events** view individual events associated with the policy violation.

For information about the actions you can take from this section, see [Views](#).

Violation Summary

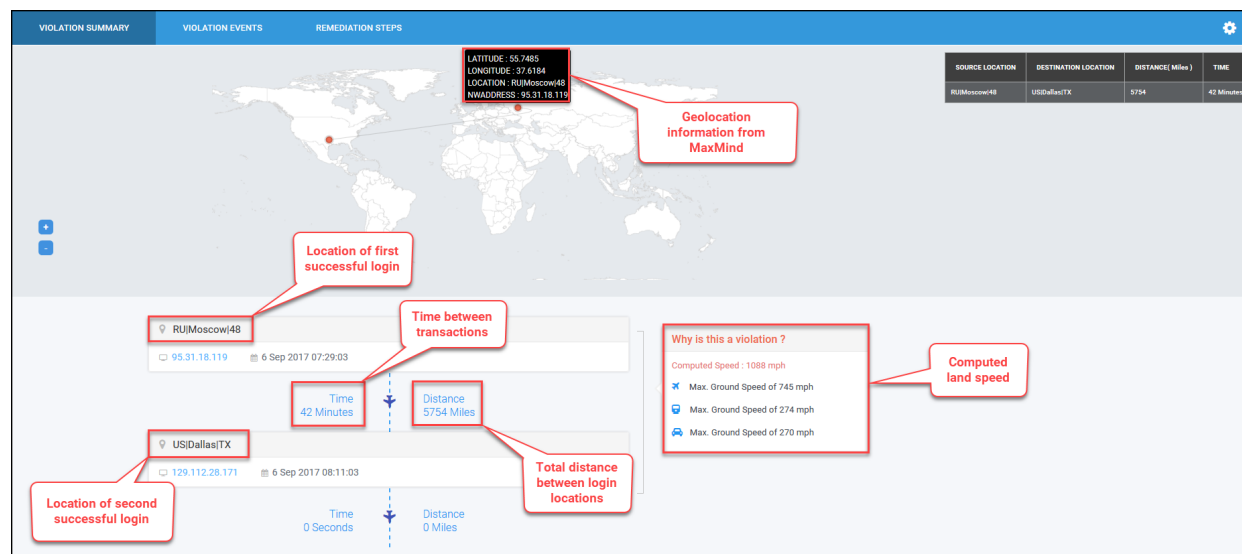
Click the entity name to view a summary of the policy violation for the entity. For information about the actions you can take from this screen, see [Entities](#).



Note: The violation summary will display different information based on the Action Filters enabled in [Activity Data](#) and the analytical technique configured in the Policy. For more information, see the ArcSight UBA Administration Guide.

Click Back to **Security Command Center** or Back to **[Entity Name]** to leave this screen.

The following example displays the violation summary for a land speed violation policy.



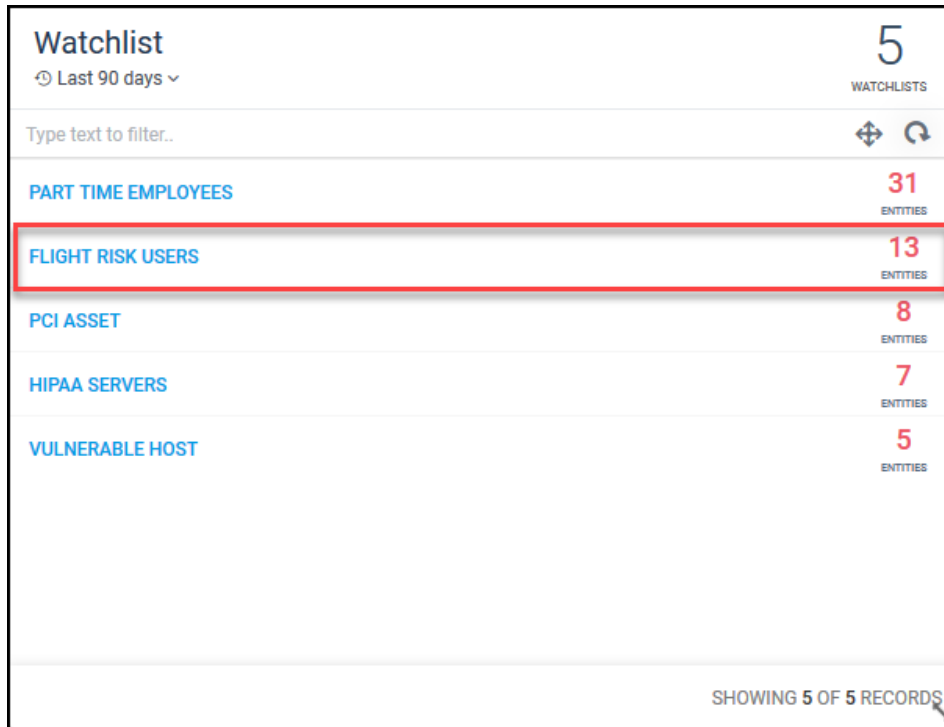
The following example displays a violation summary for a Flight Risk User—Job Search policy.



For information about the actions you can take from this screen, see [Entities](#).

Watchlists

To manage watch lists from the Security Command Center, select a watch list from the Watchlist dashboard.



The screenshot shows the 'Watchlist' dashboard. At the top, there's a header with 'Watchlist' and a dropdown for 'Last 90 days'. To the right, a large number '5' is displayed above the word 'WATCHLISTS'. Below the header is a search bar with the placeholder text 'Type text to filter..'. The main content area is a table with five rows, each representing a watchlist. The first row is 'PART TIME EMPLOYEES' with 31 entities. The second row, 'FLIGHT RISK USERS', is highlighted with a red border and shows 13 entities. The third row is 'PCI ASSET' with 8 entities. The fourth row is 'HIPAA SERVERS' with 7 entities. The fifth row is 'VULNERABLE HOST' with 5 entities. At the bottom right, it says 'SHOWING 5 OF 5 RECORDS'.

Watchlist		5 WATCHLISTS
Type text to filter..		
PART TIME EMPLOYEES	31 ENTITIES	
FLIGHT RISK USERS	13 ENTITIES	
PCI ASSET	8 ENTITIES	
HIPAA SERVERS	7 ENTITIES	
VULNERABLE HOST	5 ENTITIES	

SHOWING 5 OF 5 RECORDS

For information about adding watch lists in ArcSight UBA, see [Watch Lists](#) in the Administration Guide.

You can perform the following actions on this screen:

Manage Watch Lists

SECURITY COMMAND CENTER

WATCHLISTS
flight risk users

TYPE
Users

CRITICALITY
MEDIUM

13
TOTAL MEMBERS

Views

Enter your search criteria

entityname

Add Member(s) Remove Member(s)

<input type="checkbox"/>	Entity Name	Watch List Type	Reason	Confidence Level (between 0 to 1)	expirydate	watchlistname	createdate	decayflag
<input type="checkbox"/>	1127	Users		1.0	09/15/2018 20:11:10	Flight Risk Users	09/15/2017 20:11:10	false
<input type="checkbox"/>	1128	Users		1.0	09/15/2018 20:11:10	Flight Risk Users	09/15/2017 20:11:10	false
<input type="checkbox"/>	1129	Users		1.0	09/15/2018 20:11:10	Flight Risk Users	09/15/2017 20:11:10	false
<input type="checkbox"/>	1130	Users		1.0	09/15/2018 20:11:10	Flight Risk Users	09/15/2017 20:11:10	false
<input type="checkbox"/>	1131	Users		1.0	09/15/2018 20:11:10	Flight Risk Users	09/15/2017 20:11:10	false
<input type="checkbox"/>	1132	Users		1.0	09/15/2018 20:11:10	Flight Risk Users	09/15/2017 20:11:10	false
<input type="checkbox"/>	1135	Users		1.0	09/15/2018 20:11:10	Flight Risk Users	09/15/2017 20:11:10	false
<input type="checkbox"/>	1136	Users		1.0	09/15/2018 20:11:10	Flight Risk Users	09/15/2017 20:11:10	false
<input type="checkbox"/>	1138	Users		1.0	09/15/2018 20:11:10	Flight Risk Users	09/15/2017 20:11:10	false
<input type="checkbox"/>	1139	Users		1.0	09/15/2018 20:11:10	Flight Risk Users	09/15/2017 20:11:10	false
<input type="checkbox"/>	1140	Users		1.0	09/15/2018 20:11:10	Flight Risk Users	09/15/2017 20:11:10	false

- **Add Member(s)**: Click to add members to the watch list.



Note: Members can be users, activity accounts, network addresses, or resources.

Add Member(s)

userid

	Employee ID <small>↓</small>	First Name	Middle Name	Last Name	Manager	Email
<input type="checkbox"/>	10000	DatabaseTestUser		Success		Database.Success@sec.com
<input type="checkbox"/>	1001	HARRY	A	OGWA	1012	HARRY.OGWA@sec.com
<input type="checkbox"/>	1002	HOMER	B	OGWAL	1001	HOMER.OGWAL@sec.com
<input type="checkbox"/>	1003	HILLARY	C	OGWA	1001	HILLARY.OGWA@sec.com
<input type="checkbox"/>	1004	TERRY	D	MERRITT	1005	TERRY.MERRITT@sec.com
<input type="checkbox"/>	1005	TERRY	S	MERRITT	1025	TERRY.MERRITT@sec.com
<input type="checkbox"/>	1006	MEL		GIBSON	1001	MEL.GIBSON@sec.com
<input type="checkbox"/>	1007	RAJESH		RAO	1001	RAJESH.RAO@sec.com
<input type="checkbox"/>	1008	AKON		SHIATSU	1001	AKON.SHIATSU@sec.com
<input type="checkbox"/>	1009	HENRY		PATSUN	1001	HENRY.PATSUN@sec.com

First
<
1
2
3
4
5
>
Last
Show
10

Total results : 999 | Total pages : 100

Add User(s)

1. Select attribute in which to search for entities.
2. Enter a search term to search for a specific entity or enter * to search all entities.
3. Select the check box next to the entities to add.
4. Click **Add User(s)**.
5. Complete the following when **Add Member(s)** dialog window appears:

- a. **Watchlist:** Select from dropdown.

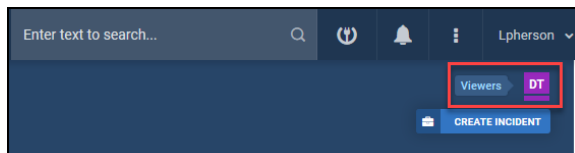


Note: If you select a Watch List that has no entities, the Watch List will be created and will appear in the on the **Security Command Center Watchlist** dashboard as well as **Menu > Views > Watchlist**. The entity you selected will appear in the newly created Watch List. They will NOT be added to the Watchlist from which you click **Add Member(s)** on the Violation Summary screen.

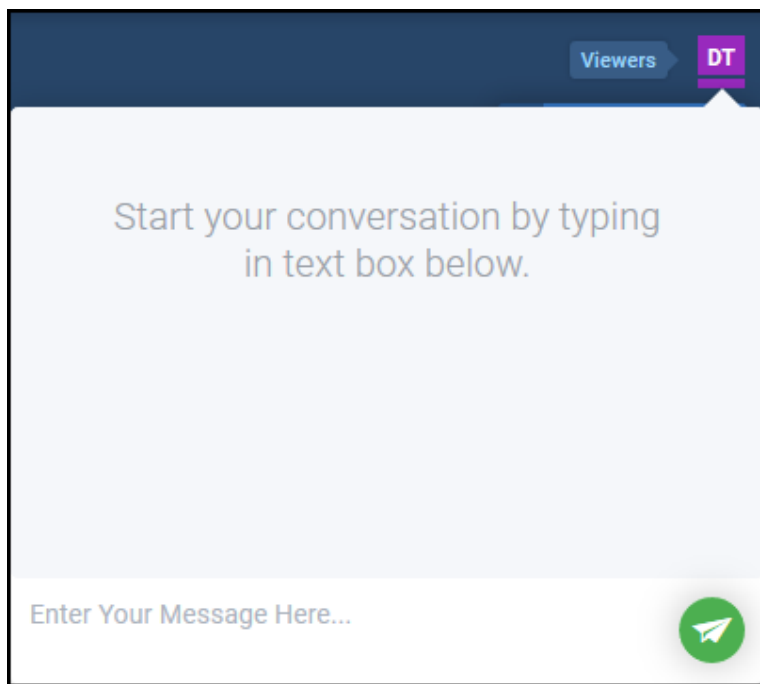
- b. **Reason:** Enter a brief description of the reason you are adding this entity to this watchlist.
 - c. **Expiry Date. Format: MM/dd/yyyy:** Enter the date on which you want to remove this entity from the watchlist.
 - d. **Confidence Level:** Enter a value between 0 to 1 to indicate how confident you are the entity should be added to the watchlist.
 - e. **Location:** Enter the location for the entity.
 - f. **LoginInfo:** Enter any pertinent login information for this entity.
 - g. Click **Add**.
- **Remove Member(s):** Select the check box next to the user you would like to remove and click **Remove Member(s)**.

Chat

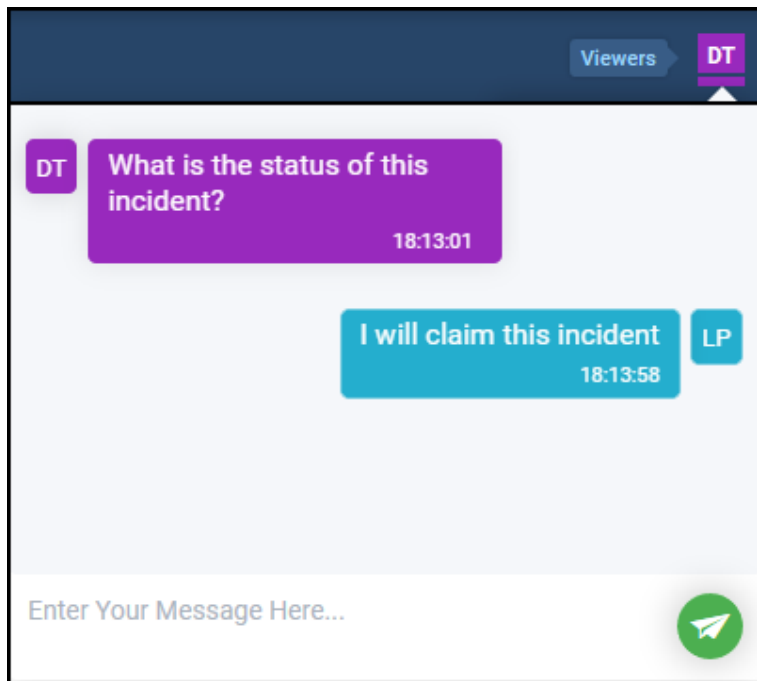
ArcSight UBA 6.10 includes chat capability to allow analysts to easily collaborate on violations and incidents within their groups. The initials of the other users viewing the violation will appear at the top right of the screen.



Click the initials of the user with whom you wish to chat to launch the chat window.



Type text to chat with the other viewers for this incident and click send icon.



Automated Response

ArcSight UBA 6.10 provides the option to apply response orchestration to security violations through actionable play books. In ArcSight UBA, play books contain and describe the entire incident and response management lifecycle by combining automated tasks such as gathering context on the violation and creating support tickets with the manual tasks the analyst must complete when a violation occurs. Automated response reduces the time spent performing simple, repetitive tasks by automating incident triage activities and launching threat and case management functionality automatically.

You can enable play books to launch automated tasks automatically when a violation occurs, or you can manually launch play book tasks from the violation summary screen in the [Security Command Center](#). Play books are enabled when creating Policy Violations.

See [Enabling Play Books](#) for more information about enabling play books when creating policy violations or [Launching Play Books](#) for information about how play books are launched from the [Security Command Center](#).

Automated Response Framework Integrations

With its Automated Response integrations, ArcSight UBA can do the following:

- Launch playbooks in response to different types of threats detected by ArcSight UBA.
- Launch queries or actions on endpoints from the ArcSight UBA console in response to a threat.
- Import critical UEBA alerts in CEF format from ArcSight UBA as incidents along with alerts from different security monitoring systems, and aggregate security alerts by user account into a Security Incident.
- Check the reputation of IPs, domains, URLs, and files.
- Verify if the email sender IP or domain is on a spam list.
- Get Whois and DNS data, and check the validity of Certificates.
- Launch a network vulnerability scan.

Available Play Book Actions

The following table describes the play book actions available with the Automated Response Integrations in ArcSight UBA 6.10:

More actions and integrations are being added regularly.

Integration	Action	Description
Active Directory	BlockUser	Disable an Active Directory User
Active Directory	UnBlockUser	Enable an Active Directory User
Demisto	CreateIncident	Create an incident on Demisto
Email	ArcSight UBA Send Alert Email	Send violation alerts as Email
Nessus	LaunchScan	Launch a Nessus Scan
PassiveTotal	Get Enrichment Data Bulk	Provides enriched data for a given domain
PassiveTotal	Get Host Component	Provides host attribute components for a given domain
PassiveTotal	Get Host Pair	Gets the pair - two domains (a parent and a child) that shared a connection observed from a RiskIQ web crawl for a given domain
PassiveTotal	Get Host Tracker	Extracts tracker details such as website trackers, analytics codes, social network accounts and other unique details for a given domain name.
PassiveTotal	Get Malware Bulk	Provides malware data for a domain
PassiveTotal	Get OSInt Bulk	Provides information gathered from public sources for a particular domain
PassiveTotal	Get Passive DNS	Provides the Passive DNS collection for a particular IP which involves gathering the domain request and IP response from DNS providers across the internet when they happen
PassiveTotal	Get SSL Certificate	Retrieves an SSL certificate by its SHA-1 hash

Integration	Action	Description
PassiveTotal	Get SSL Certificate History	Retrieved SSL history
PassiveTotal	Get Sub-domains	Provides the possible domains associated with the given domain
PassiveTotal	Get Unique DNS	Retrieves the unique passive DNS results from active account source
PassiveTotal	Get Who Is	Retrieves the WHOIS data for the specified domain
PassiveTotal	Search Passive DNS	Searches the Passive DNS data for an IP Address
PassiveTotal	Search SSL By Keyword	Retrieves SSL certificates for a given keyword
PassiveTotal	Search SSL Certificate	Retrieves SSL certificates for a given query
PassiveTotal	Search Who Is	Searches WHOIS data by domain
PassiveTotal	Search Who Is By Keyword	Search WHOIS data for a keyword
Phantom	CreateIncident	Create an incident on Phantom
RSA Archer/RSA Netwitness	ArcSight UBA Send Alert CEF	Send violation alerts as CEF
SpamHaus	Check IP	Verifies if a particular IP is marked spam against Spam Haus repository
SpamHaus	Check Domain	Verifies if a particular domain is marked spam against Spam Haus repository
Tanium	Machine Information	This playbook shows endpoint information from this endpoint
Tanium	Running Processes with MD5	This playbook shows the list of currently running processes with their respective MD5 hashes from this endpoint

Integration	Action	Description
Tanium	Running Applications	This playbook shows the list of currently running applications and their respective versions from this endpoint
Tanium	Non-Approved Established Connections	This playbook shows the list of currently running non approved processes and their target IP addresses from this endpoint
Tanium	User Sessions	This playbook shows the list of currently running user session details from this endpoint
Tanium	Reboot Windows Machine	Deploy action via Tanium to reboot a given Windows endpoint in our network
Tanium	Set USB Write Protect On	Deploy action via Tanium to enable USB write protect on a given Windows endpoint in our network
Tanium	Set USB Write Protect Off	Deploy action via Tanium to disable USB write protect on a given Windows endpoint in our network
VirusTotal	ScanIP	ScanIP and fetch results
VirusTotal	ScanURL	ScanURL and fetch results
VirusTotal	ScanDomain	ScanDomain and fetch results
VirusTotal	ScanFile	ScanFile and fetch results

Note: Taking action such as a Kill action on an endpoint can be dangerous and requires input from VirusTotal (or equivalent) to validate.

Configuring Automated Response Framework Connections

Automated Response Framework integrations are included out of the box with ArcSight UBA 6.10. To use the out of the box integrations, configure the connections in the Properties file located in **securonix/tenants/<tenantname>/securonix_home/response** directory.

To configure the connections in the Properties file for Automated Response Framework integrations, complete the following steps:

Active Directory

1. Navigate to **securonix/tenants/<tenantname>/securonix_home/response/activedirectory**.

2. Complete the following information to establish the connection:

```
username=<username> Example: Securonix
Password=<password>
ldapurl=ldap://<IPAddress>:<port> Example: 10.0.0.25:389
domainname=<activedirectorydomainname> Example: test.securonix.-
com
memberof=
replacepassword=<password>
```

Demisto

1. Navigate to **securonix/tenants/<tenantname>/securonix_home/response/demisto**.

2. Complete the following information to establish the connection:

```
demistoAuthKey=<authkey>
Example: qsrX63xKnJvqrzF8oGI6Gu7DuKItKozIp
demistoURL=https://<IPAddress>:<port> Example: 10.0.0.5:443
```

Nessus

1. Navigate to **securonix/tenants/<tenantname>/securonix_home/response/nessus**.

2. Complete the following information to establish the connection:

```
USERNAME=s<username> Example: Securonix
PASSWORD=<password>
NESSUSURL=https://<IPAddress>:<port> Example: 10.0.0.5:8834
NUMOFRETRIES=5
```

PassiveTotal

1. Navigate to **securonix/tenants/<tenantname>/securonix_home/response/passivetotal**.

2. Complete the following information to establish the connection:

```
USERNAME=<username> Example: amy@sec.com
SECRET_KEY=<secretkey>
Example: 33b3e932a4043e84848c14f2c8856dc1e7ba1b802adc2843b67026a
PT_HOST=api.passivetotal.org
```


Phantom

1. Navigate to **securonix/tenants/<tenantname>/securonix_home/response/phantom**.
2. Complete the following information to establish the connection:

```

USERNAME=<username> Example: admin
PASSWORD=<password>
PHANTOMSERVER=<ipaddress> Example: 10.0.5.20
TOKEN=<token>= Example: tuITaoiBv3fjtFcuQLKciY+niZ87C2l4WcWQf7I

```

SpamHaus

1. Navigate to **securonix/tenants/<tenantname>/securonix_home/response/spamhaus**.
2. Complete the following information to establish the connection:

```

IPREPOSITORY = "pbl.spamhaus.org";
DOMAINREPOSITORY = "db1.spamhaus.org";
PBLLINK = "https://www.spamhaus.org/query/ip/";
DBLLINK = "https://www.spamhaus.org/query/domain/";

```

Tanium

1. Navigate to **securonix/tenants/<tenantname>/securonix_home/response/tanium/src**.
2. Open **ConnectToTanium.py** file.
3. Complete the following information to establish the connection:

```

handler_args['username'] = "<username>" Example: Administrator
handler_args['password'] = "<password>"
handler_args['host'] = "<hostip>"
handler_args['port'] = "<port>" #optional Example: 443

```

VirusTotal

1. Navigate to **securonix/tenants/<tenantname>/securonix_home/response/virustotal**.
2. Complete the following information to establish the connection:

```

apikey-
=3206c1-
1fb600d886ad520bf704d69f64e941665cff4882cd5e0702b9e10328baf

```

RSA Archer

For information about integrating RSA Archer, see Configure [ArcSight UBA] with RSA® Archer® GRC Platform.

RSA Netwitness

For information about integrating RSA Netwitness, see Configure [ArcSight UBA] with RSA® Netwitness®.

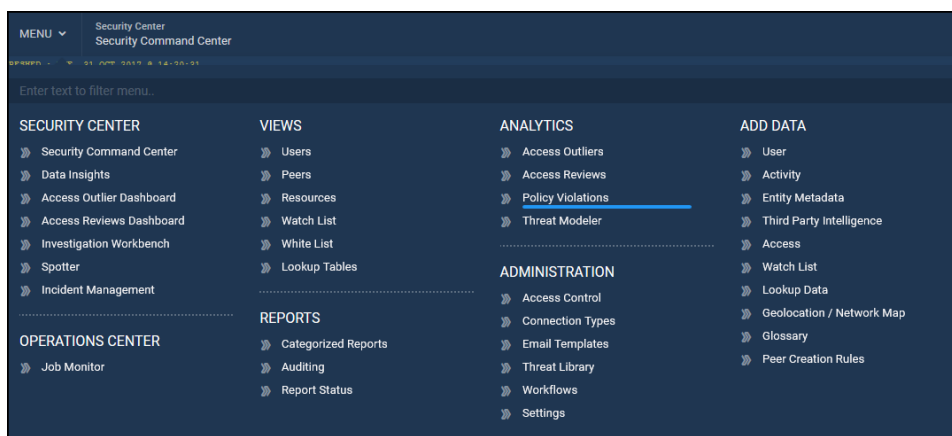
Enabling Play Books

Enable Play Books to automate incident response work flow and launch tasks during **Step 1: Enter Policy Details** when creating Policy Violations.

Enabling Play Books in Threat Indicators

To enable Play Books in threat indicators, complete the following steps:

1. Navigate to **Menu > Analytics > Policy Violations**.



2. Click **+** to create a new policy or click a policy name to edit an existing policy.

Enter your search criteria									
	Type	Analytical Type	Datasource	Datasource Type	Functionality	Last Update Date	Violation Entity	Enabled?	Actions
Create Policy									
Create Identity/Access Policy	Real Time Policy	Tier 2 Behavior Summary	Bluecoat Proxy	Bluecoat Proxy			Activity Account	NO	
Abnormal number of data uploads compared to past behavior NU-1	Real Time Policy	Tier 2 Behavior Summary	Bluecoat Proxy	Bluecoat Proxy			Activity Account	NO	
Accounts that belong to terminated user	Identity Policy	-				2017-10-02 14:11:58.0	Access Account	YES	
Accounts that dont have Users	Identity Policy	-				2015-04-02 22:11:43.0	Access Account	YES	
Accounts where user dont have manager	Identity Policy	-				2015-04-02 22:12:15.0	Access Account	YES	
Accounts with Domain Admin Access	Identity Policy	-				2015-04-02 22:21:56.0	Access Account	YES	

3. Complete the steps on Enter Policy Details screen as described in [Policy Violations](#) in the Administration Guide

4. Proceed to **Define Risk and Threat**.

DEFINE RISK AND THREAT

Category*

Create New Policy Category

None

+

-

Category is displayed on dashboard as a widget and risk will be aggregated for policies with the same category. All violations of the same category will be available in the widget.

Threat Indicator*

Create New Threat Indicator

Edit Threat Indicator

-Select-

Violations detected are indicative of threat

5. Click **Create New Threat Indicator** for a new threat indicator or **Edit Threat Indicator** for an existing threat indicator.
6. Enter **Threat Indicator Name** and select a **Category** from the drop down if appropriate.

Create New Threat Indicator

Threat Indicator Name*

Category*

Recon Stage

Threat Response Playbook

Sample Template: <ul class='remediation-steps-1st'>Response Playbook details go here <a>Use a tag for linkResponse Playbook details go here User strong for bold textResponse Playbook details go here

Select To Associate Playbooks

Save

7. Select play books to associate with the threat indicator under **Select to Associate Playbooks**. Example: VirusTotal ScanIP.

Edit Threat Indicator

Select To Associate Playbooks

☐

SNYPR SendAlertCEF
Send violation alerts as CEF

NO

AUTO PLAY

☒

VirusTotal ScanIP
VirusTotal ScanIP and fetch results

NO

AUTO PLAY

☒

VirusTotal ScanURL
VirusTotal ScanURL and fetch results

NO

AUTO PLAY

☒

VirusTotal ScanDomain
VirusTotal ScanDomain and fetch results

NO

AUTO PLAY

☒

VirusTotal ScanFile
VirusTotal ScanFile and fetch results

NO

AUTO PLAY

☒

Nessus LaunchScan
Launch a Nessus Scan

NO

AUTO PLAY

Save



Note: You may select multiple playbooks for the threat indicator.

8. Enable slider to **YES** to launch **Auto Play** for the play books.

If Auto Play is disabled, you can launch play book tasks manually from the violation summary screen when an incident occurs.

Edit Threat Indicator

Select To Associate Playbooks

<input type="checkbox"/> SNYPR SendAlertCEF Send violation alerts as CEF	<input type="checkbox"/> NO AUTO PLAY
<input checked="" type="checkbox"/> VirusTotal ScanIP VirusTotal ScanIP and fetch results	<input checked="" type="checkbox"/> YES AUTO PLAY
<input checked="" type="checkbox"/> VirusTotal ScanURL VirusTotal ScanURL and fetch results	<input type="checkbox"/> NO AUTO PLAY
<input checked="" type="checkbox"/> VirusTotal ScanDomain VirusTotal ScanDomain and fetch results	<input type="checkbox"/> NO AUTO PLAY
<input checked="" type="checkbox"/> VirusTotal ScanFile VirusTotal ScanFile and fetch results	<input checked="" type="checkbox"/> YES AUTO PLAY
<input checked="" type="checkbox"/> Nessus LaunchScan Launch a Nessus Scan	<input type="checkbox"/> NO AUTO PLAY

Save

9. Click **Save**.
10. Complete the policy configuration as described in [Policy Violations](#) in the Administration Guide.

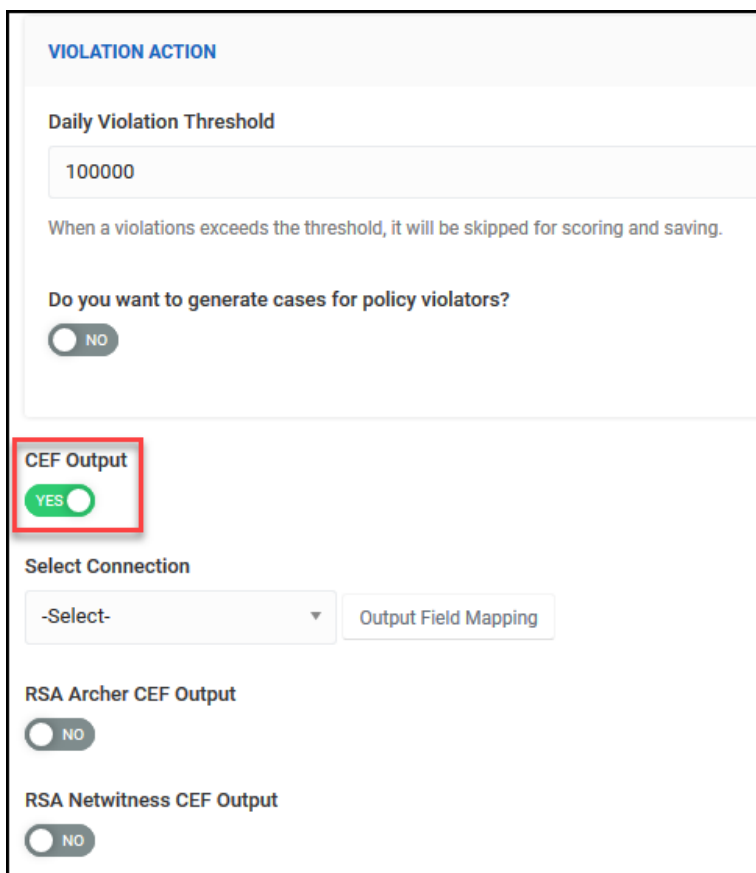
Exporting CEF Alerts from ArcSight UBA Using Play Books

To export CEF alerts through Play Books in ArcSight UBA, complete the following steps:



Note: You must configure your connections for CEF output in [Connection Types](#) before you can export from ArcSight UBA.

1. Complete **Steps 1-6** as described in [Enabling Play Books in Threat Indicators](#).
2. Select one of the following playbooks for **Select to Associate Playbooks**:
 - **SendAlertCEF**
 - **RSA Archer Playbook**
 - **RSA Netwitness Playbook**
3. Click **Save**.
4. **Provide Conditions** for the policy as described in Policy Violations.
5. Proceed to **Choose Actions for Violations**.
6. Configure **Violation Summary** as described in Policy Violations.
7. Proceed to **Violation Action** and complete appropriate fields.
8. Enable **CEF Output** slider to **YES**.



VIOLATION ACTION

Daily Violation Threshold

100000

When a violations exceeds the threshold, it will be skipped for scoring and saving.

Do you want to generate cases for policy violators?

☐ NO

CEF Output

☒ YES

Select Connection

-Select-

RSA Archer CEF Output

☐ NO

RSA Netwitness CEF Output

☐ NO

1. Select **Connection** from dropdown.



Note: Only connections you have enabled in [Connection Types](#) will appear in the drop-down.

9. Enable **RSA Archer CEF Output** slider to **YES**.

1. Select **Connection** from dropdown.



Note: You must configure your connections for RSA Archer CEF output before you can export from ArcSight UBA.

10. Enable **RSA Netwitness CEF Output** slider to **YES**.

1. Select **Connection** from dropdown.



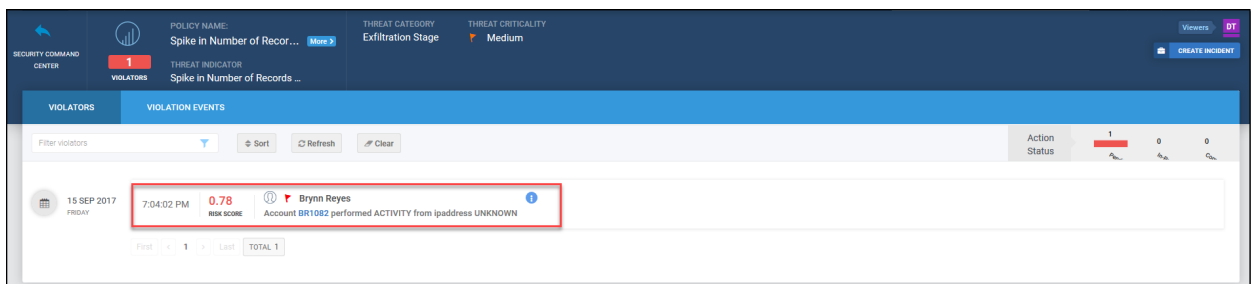
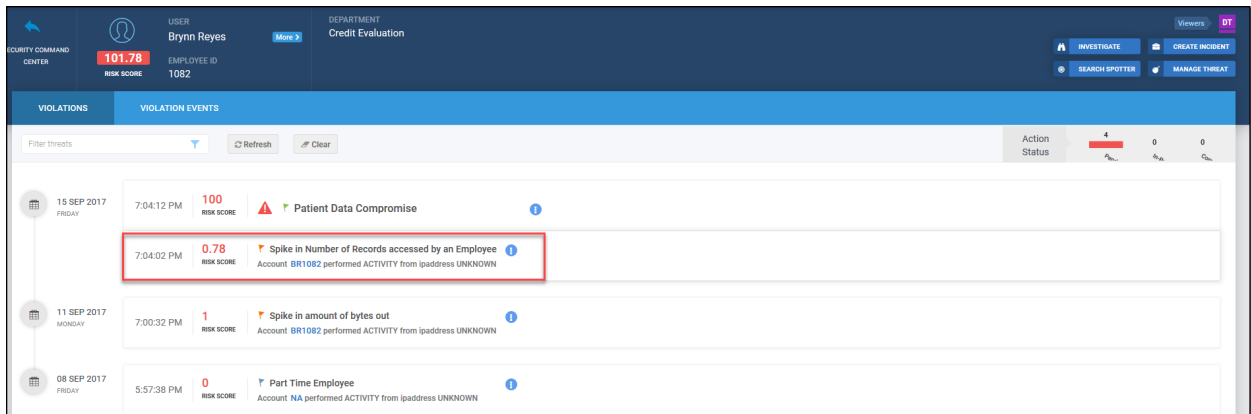
Note: You must configure your connections for RSA Netwitness CEF output before you can export from ArcSight UBA.

Launching Play Books

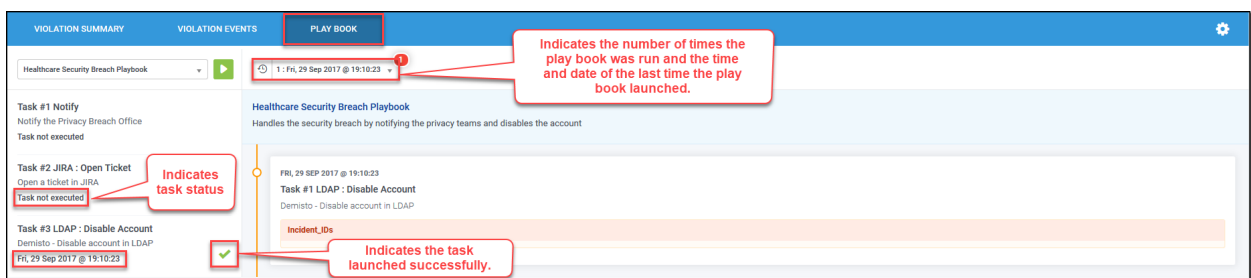
When a violation occurs, ArcSight UBA launches the play books enabled for the threat indicator and runs the automated tasks specified in the play book. You can view play books and manually launch tasks from the violation summary of the [Security Command Center](#).

To view and launch play books, complete the following steps:

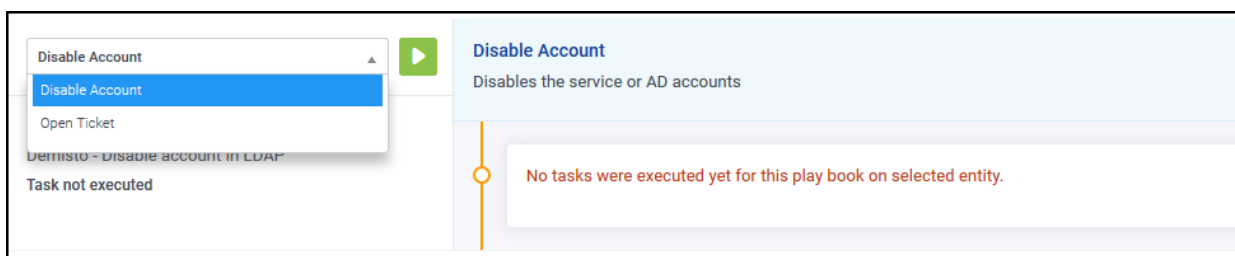
1. Navigate to **Menu > Security Center > Security Command Center** or click the ArcSight UBA logo.
2. Select an entity, or policy or threat violation from a dashboard. Example: Top Violations.
3. Click a violation for an entity or a violator for a violation to view the violation summary.



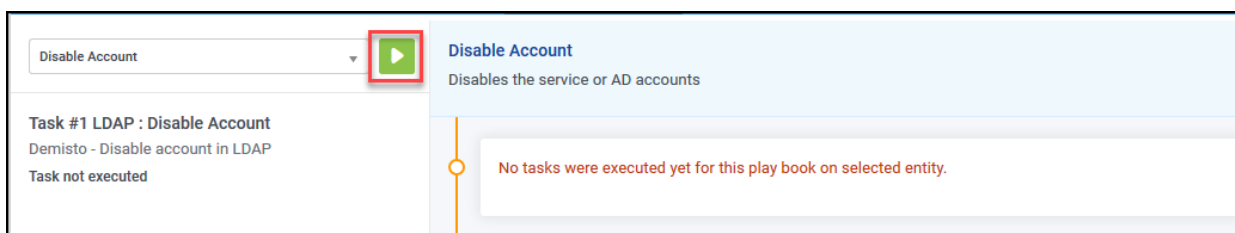
4. Click **Play Book** on the violation summary screen.
Automated and completed tasks will appear with a green check mark.



5. Select a play book to launch from the drop down if multiple play books are enabled for this threat indicator.

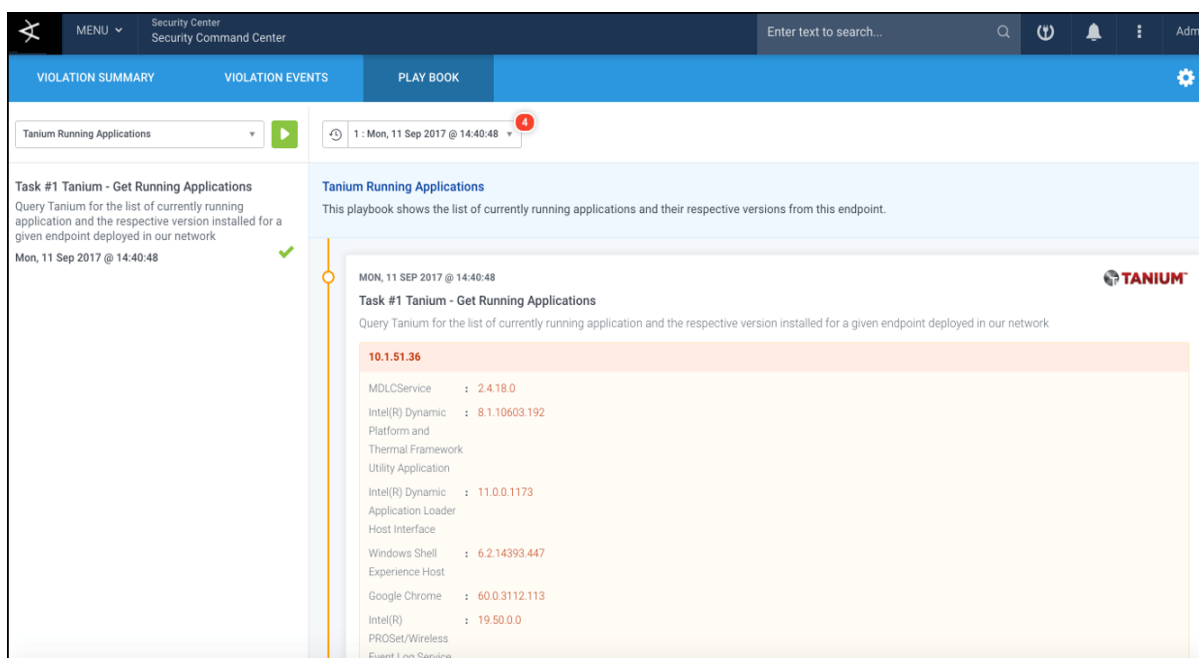


6. Click play icon to launch the play book if **Auto Play** is not enabled or to run automated tasks again.



Sample Play Books

Tanium Get Running Applications



Advanced Cyber Threat Incident Playbook

The screenshot displays the 'Advanced Cyber Threat Incident Playbook' interface. On the left, a sidebar lists tasks: 'Task #1 Demisto: Create Incident' and 'Task #2 VirusTotal: Get Context'. The main panel shows the execution of these tasks. Task #1, 'Create Incident', is completed successfully, creating an incident with ID 1484. Task #2, 'Get Context', is also completed, showing details for IP address 125.72.243.88, including ASN, VLink, and other metadata.

Customizing Tasks in Play Books

Note: This procedure is not recommended. Contact support@securonix.com for assistance.

From the database workbench, you can customize the tasks in the out-of-the-box play books included in ArcSight UBA. You can launch tasks based on the result of previous tasks as in the following example:

Enter the following query: `select * from pbplaybook;`

The list of playbooks tasks will appear:

Example

```
<PlaybookConfig>

<PlaybookName>Demisto Incident playbook ipaddress</PlaybookName>
<version>1.0</version>
<StarttaskId>3</StarttaskId>
<Task idDB="3" name="" Version="1.0" enabled="true" PausePlay-
bookAfterTask="false">
<taskClass>-
com.securonix.de-
mistoIntegrationConnector.action.ActionCreateDemistoIncident</taskClass>
<TaskOutput ResponseCode="-1" TaskId="-1"/>
<TaskOutput ResponseCode="1" TaskId="5"/>
<TaskOutput ResponseCode="2" TaskId="6"/>
</Task>

<Task idDB="5" name="" Version="1.0" enabled="true" PausePlay-
bookAfterTask="false">
```

```

<taskClass>-
com.securonix.de-
mistoIntegrationConnector.action.DemistoTaskStatus</taskClass>
<TaskOutput ResponseCode="-1" TaskId="-1"/>
<TaskOutput ResponseCode="1" TaskId="6"/>
</Task>
<Params type="DISTINCT">
<key>incident.ipaddress</key>
</Params>

```

```

<Task idDB="6" name="" Version="1.0" enabled="true" PausePlay-
bookAfterTask="false">
<taskClass>-
com.securonix.de-
mistoIntegrationConnector.action.DemistoTaskStatus</taskClass>
<TaskOutput ResponseCode="-1" TaskId="-1"/>
</Task>
<Params type="DISTINCT">
<key>incident.ipaddress</key>
</Params>

```

```

</PlaybookConfig>

```

Configure tasks to launch based on the response of previous tasks as in the following example from the highlighted text above:

`<TaskOutput ResponseCode="-1" TaskId="-1"/>` : If Task Response is equal to -1, the playbook will terminate. Example: If URL is not categorized as malicious, no further action is taken.

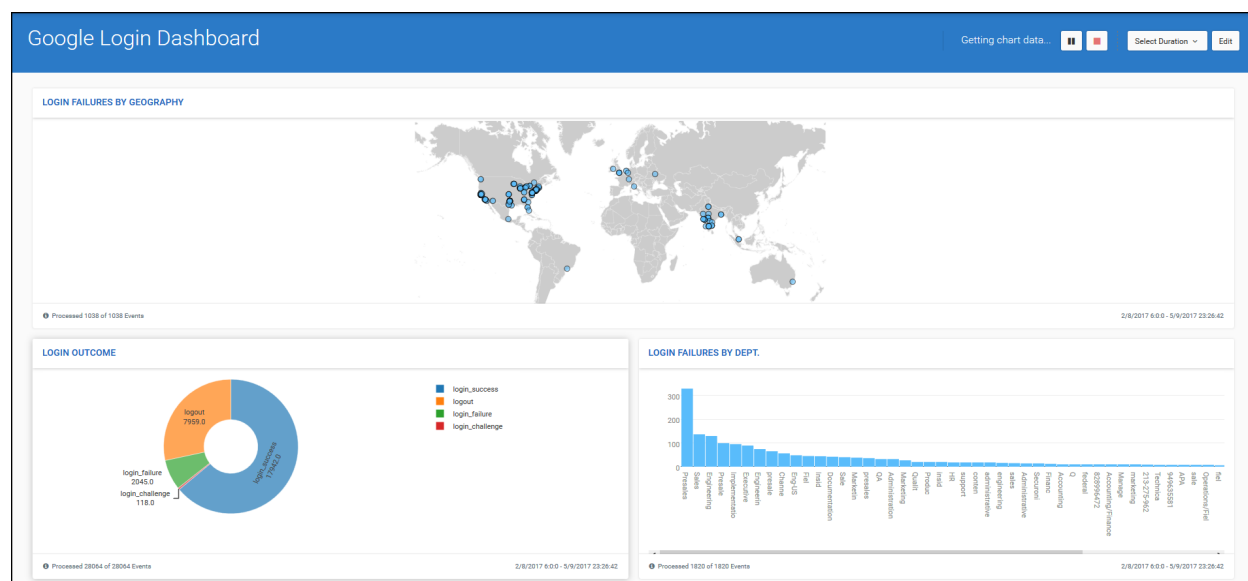
`<TaskOutput ResponseCode="1" TaskId="5"/>` : If Task Response is equal to 1, launch Task 5. Example: If URL is categorized as malicious, block the URL.

`<TaskOutput ResponseCode="2" TaskId="6"/>` : If Task Response is equal to 2, launch Task 6. Example: If URL appears in Alexa's 1 Million Safe Domains, whitelist the URL.

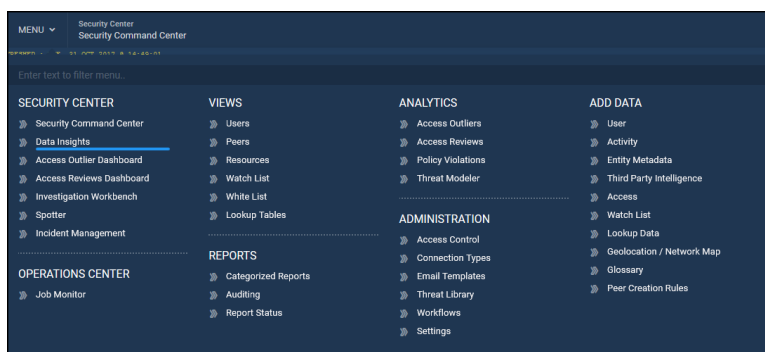
Data Insights

Data Insights allow you to create, modify, save, and share custom dashboards to gain data insights for your organizations with the My Dashboards feature. Each dashboard can contain multiple charts to view data in the following formats:

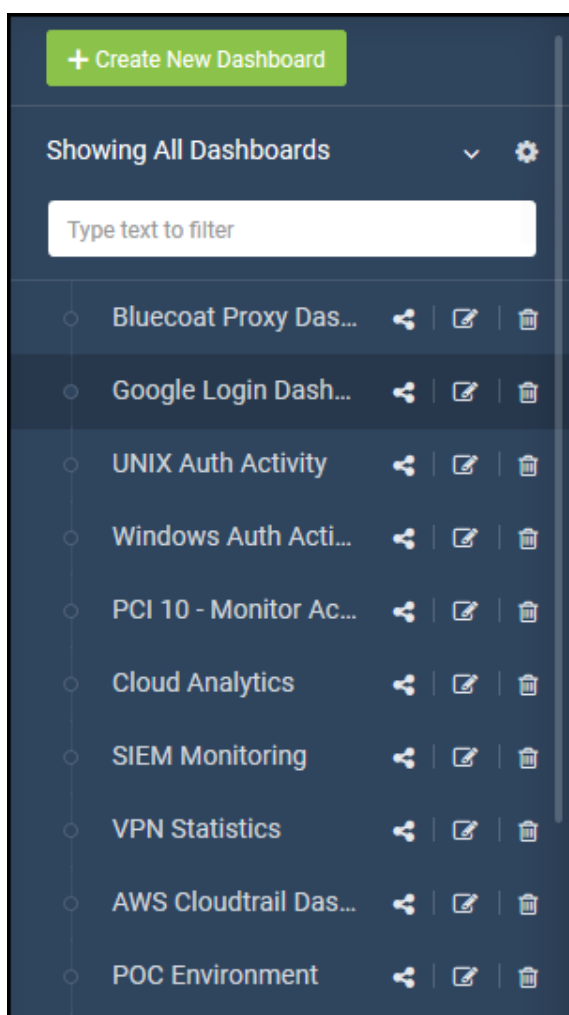
- Line Chart
- Area Chart
- Bar Chart
- Geolocation Map
- Tabular Data
- Donut Chart
- Stacked Bar Chart
- Top N Results
- Bubble Chart
- Source Destination Chart



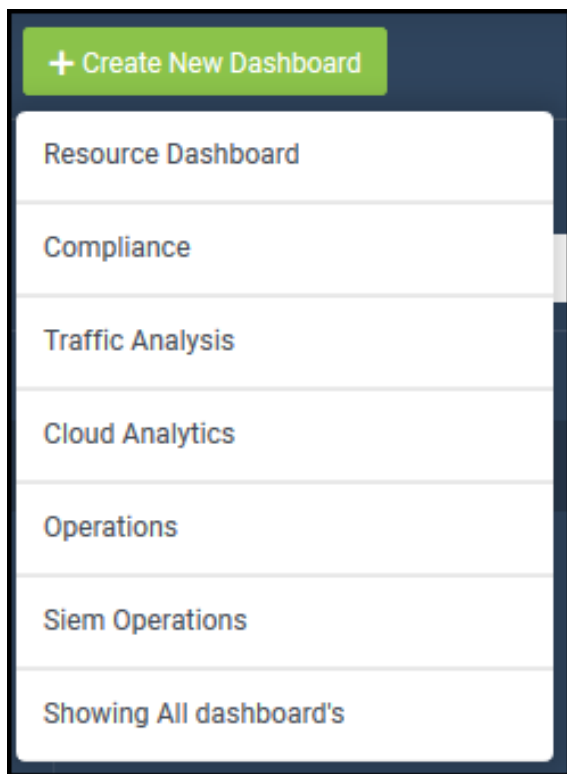
To access My Dashboards, navigate to **Menu > Security Center > Data Insights**.



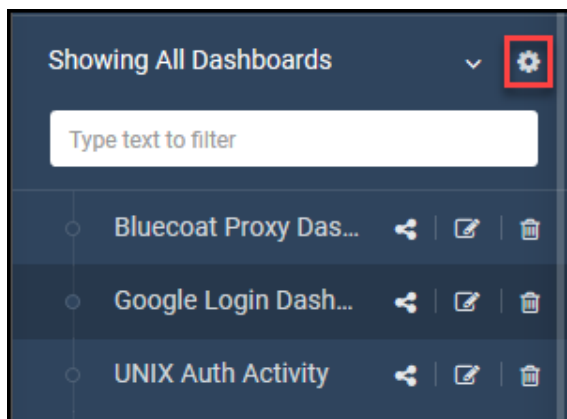
Click  to expand the left navigation panel and select a dashboard to view.



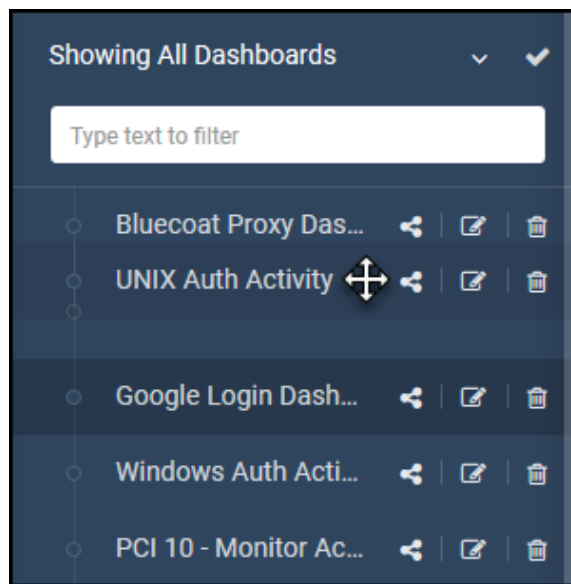
To filter the list, click the down arrow icon. Select a category (configured during [Creating New Dashboards](#)) to filter results.



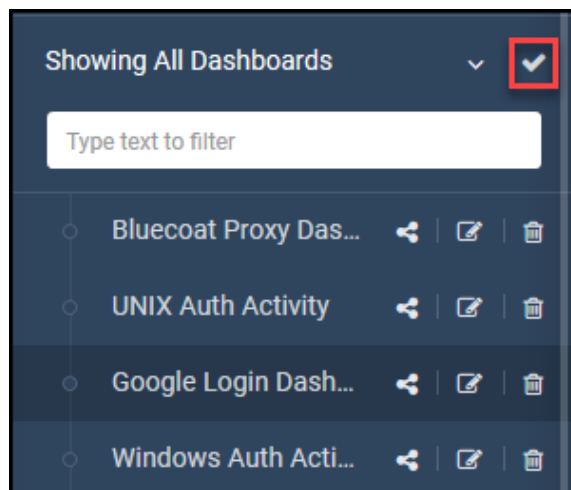
Reorder the list by clicking the cog icon.



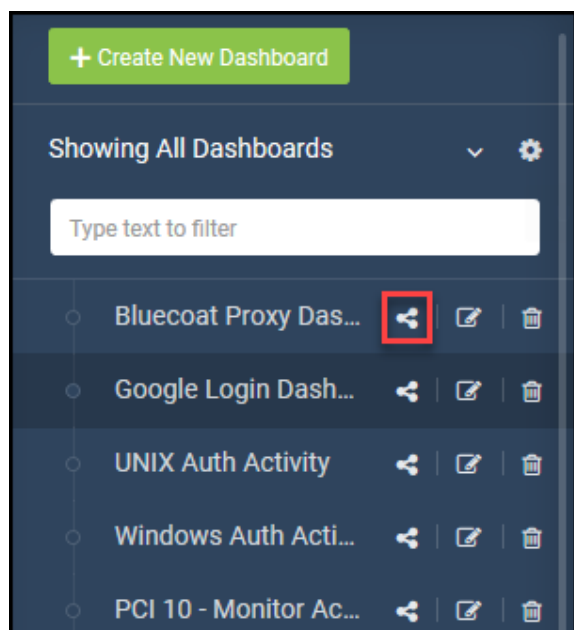
Use mouse to drag the list items into the preferred order.



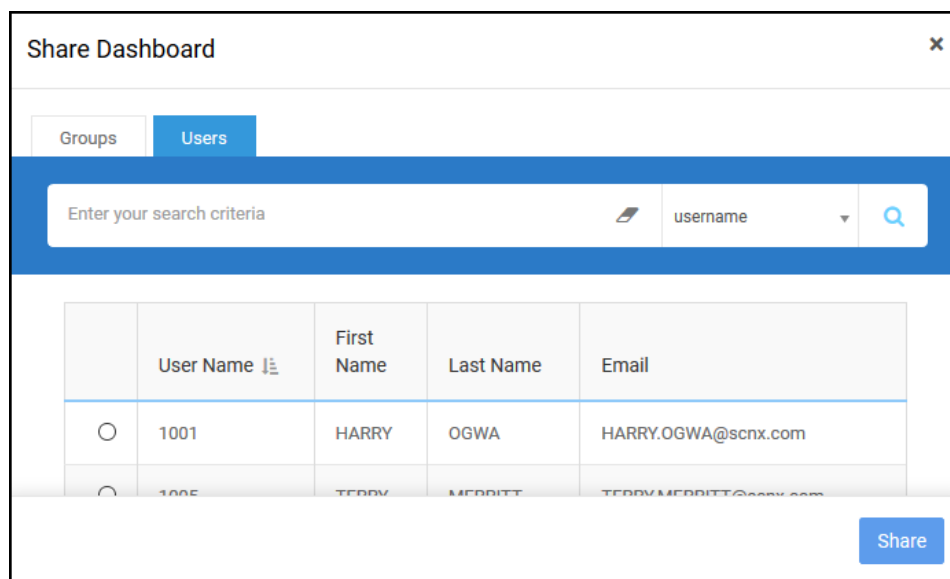
Click the check mark to save the changes.



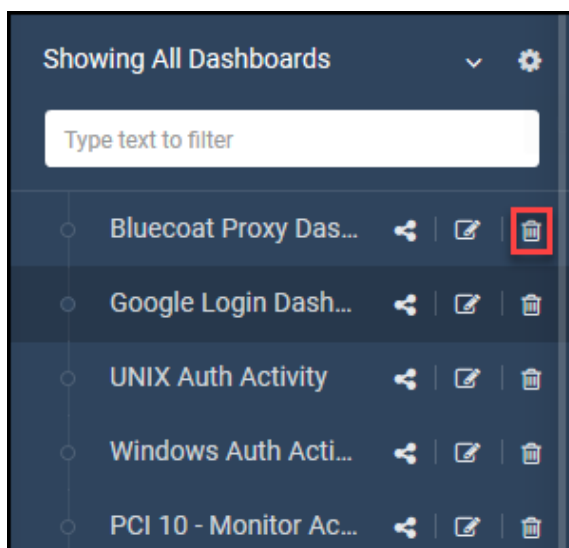
Click share icon to share a dashboard with another user.



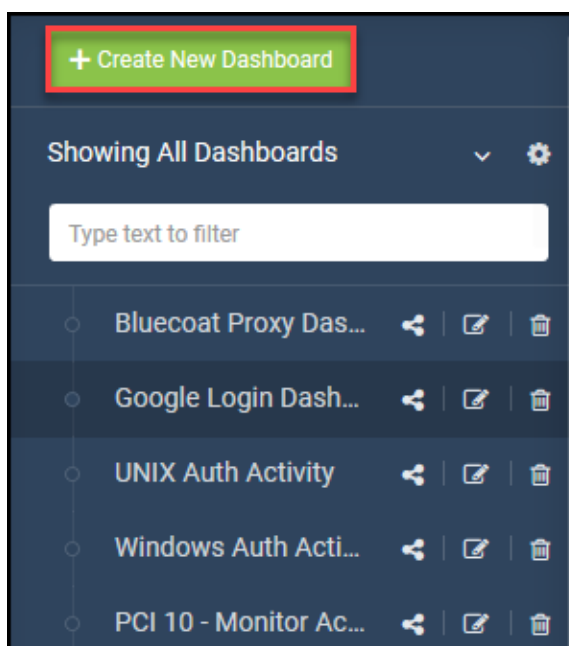
Select users or groups with whom to share the dashboard and click **Share**.



Click the trash icon to delete a dashboard.

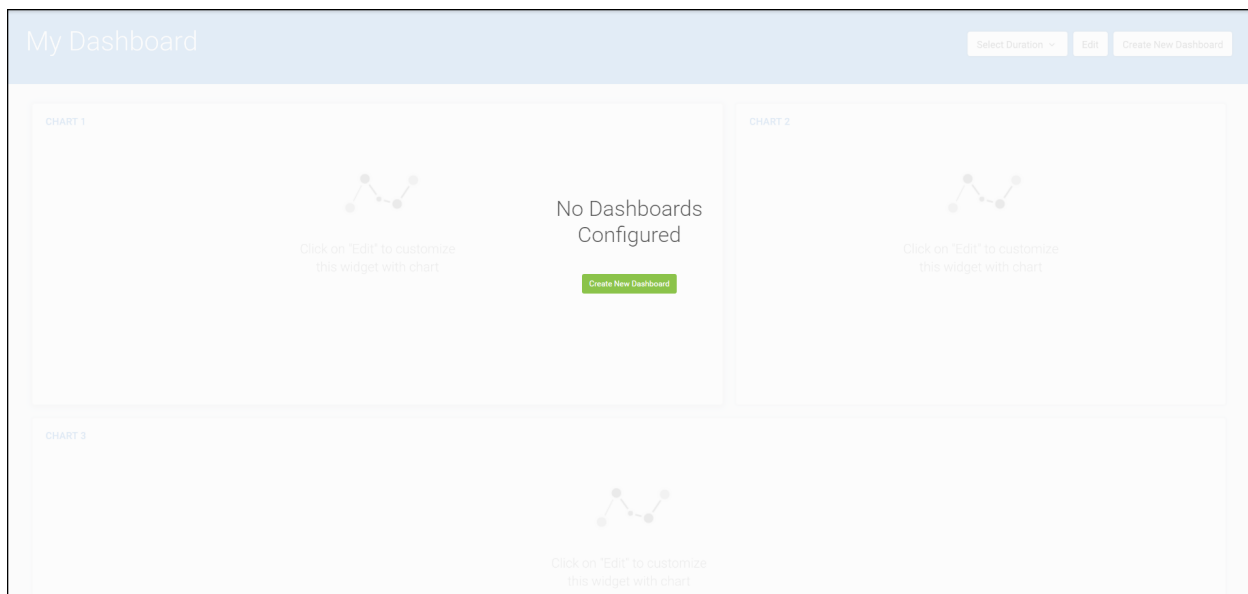


Click **Create New Dashboard** to add a new dashboard.



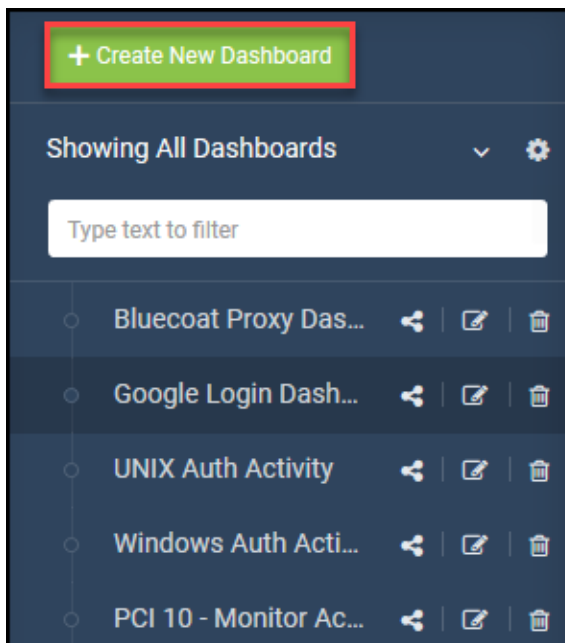
Creating New Dashboards

The first time you access **Data Insights**, you will be prompted to create a new dashboard.



To create a new dashboard, complete the following steps:

1. Click **Create New Dashboard** from the previous screen or by clicking **Create New Dashboard** from the left navigation panel.



2. Complete the following information:

CREATE DASHBOARD

Dashboard Name:*

Provide new dashboard name.

Dashboard description:

Provide new dashboard description.

Select a category for your dashboard








None

Choose a dashboard category

Share Dashboard

Please specify the group/user name to share the dashboard

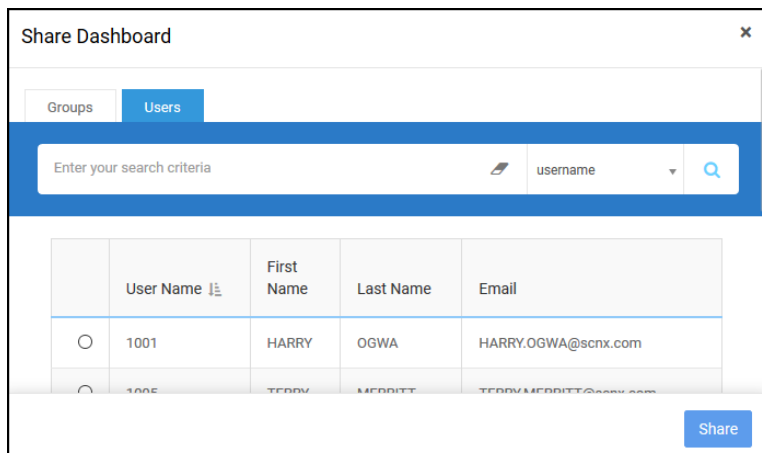
Select Any One Template :*

Select any template layout which will specify the grid structure for the widgets placement in your Dashboard.

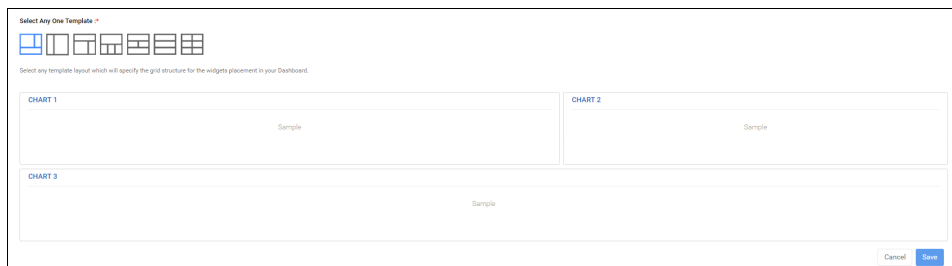
- Dashboard Name:** Provide a unique name for your dashboard.
- Dashboard Description:** Provide a brief description your dashboard.
- Select a category for your dashboard:** Select a category from dropdown or **Create New Category**.
 - Create New Category:** Provide a category name.
- Share Dashboard:** Click search icon to select a user or group with which to share the dash-

board.



- e. **Select Any One Template:** Select a template for the dashboard to specify the grid structure for the placement of widgets on your dashboard.


A preview of the template is displayed:

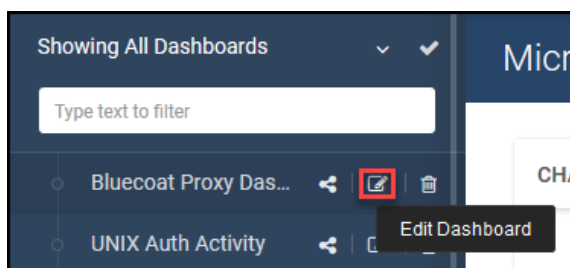


3. Click **Save**.

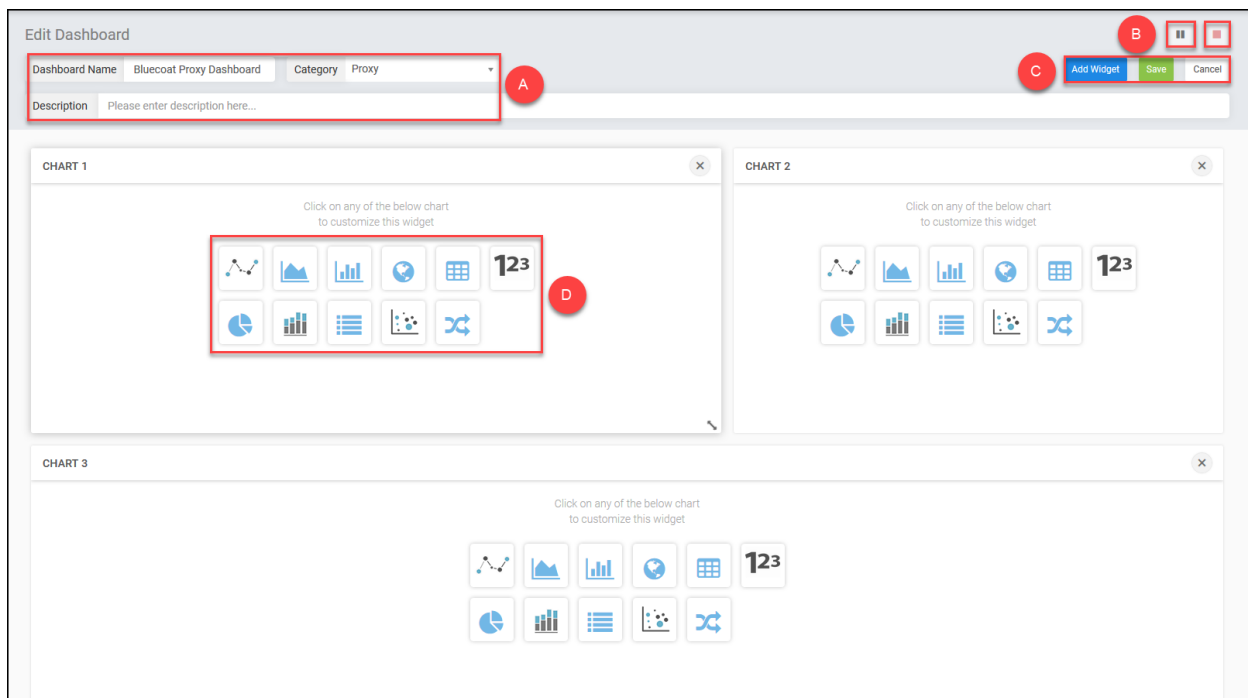
Configuring Dashboards

You can customize the charts you see on your dashboard

To configure and edit dashboards, click the edit  icon beside the dashboard name on the left navigation panel.



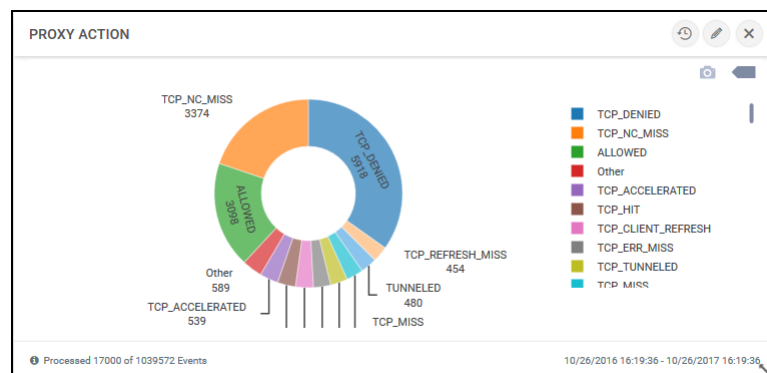
From this screen, you can complete the following actions:









Actions

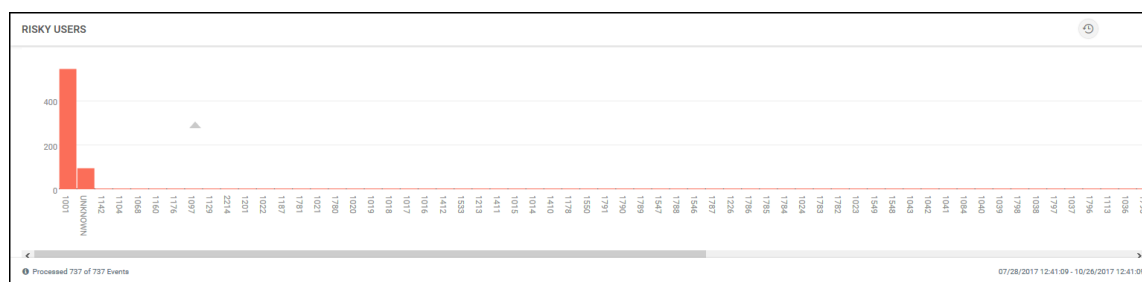
A	Edit dashboard details
B	Use VCR controls to play, pause, or stop updating dashboard
C	<p>Take Dashboard actions:</p> <ul style="list-style-type: none"> • Add new Widget: Add a widget to the template • Cancel: Cancel Editing and return to View mode. • Save: Save the current dashboard.
D	<p>Click on a chart icon to customize the widget. Available charts include:</p> <ul style="list-style-type: none"> • Line Chart • Area Chart • Bar Chart • Gelocation Map • Tabular Data • Number • Donut Chart • Stacked Bar Chart • Top N Results • Bubble Chart • Source Destination Chart

You can take the following actions on widgets:



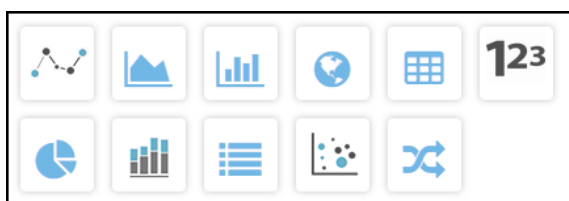
	Select duration for widget
	Edit widget
	Close graph
	Download plot as a PNG
	Toggle to show closest data on hover
	Resize widget

Customizing Widgets



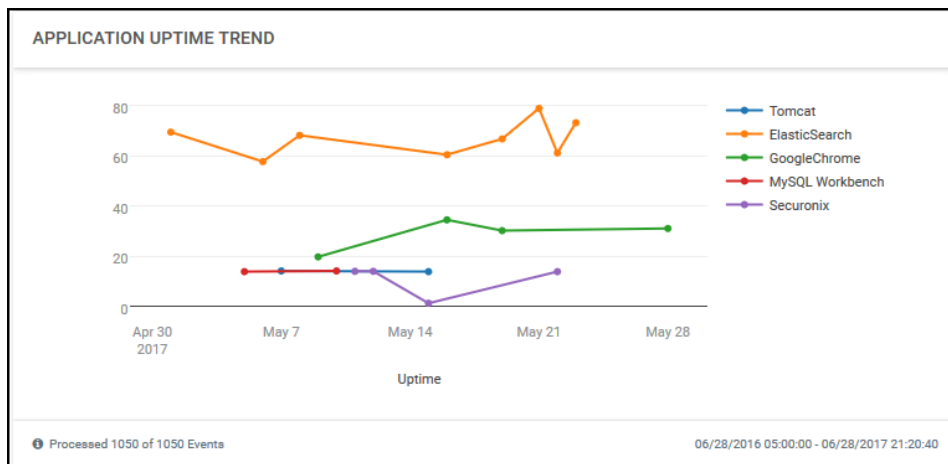
To customize widgets on your dashboard, complete the following steps:

1. Click an icon to select a chart type.



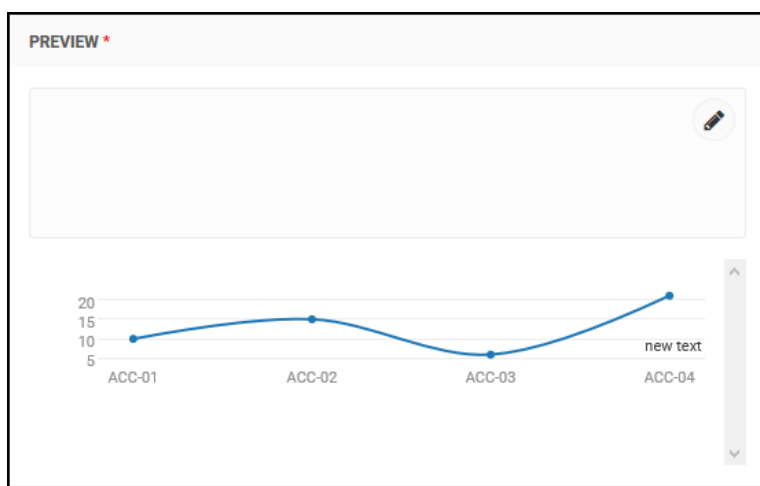
2. Configure charts as described below.
3. Click **Create Chart**.

Line Chart



Preview

Preview input you will enter in the proceeding steps:



General Details

Complete the following information:

GENERAL DETAILS

Chart Label: *

Enter new chart label

Chart Orientation:

Vertical | Horizontal

Select Chart Orientation

Chart Color

Select color of chart

- Chart Label:** Provide a unique name for the chart.
- Chart Orientation:** Select an orientation for the chart.
- Chart Color:** Use color picker and click **Choose** to select a color.

Chart Details

Provide the following information:

CHART DETAILS

Datasource:

Google Login

Select the datasource you would like to create the chart for (Optional)

What type of data you want to use*

Event Data

Select the type of data you would like to run query on.

Time Range*

Last 7 days

Select date range you would like to run the query for

- (Optional) **Datasource:** Select a datasource from the dropdown.
- Time Range:** Select the time range to display in chart results.
- What type of data you want to use:** Select the type of data on which to run the query from the dropdown.

X-Axis


Provide the following information:

X - AXIS

X-Axis Label:




Enter x-axis label

Field*

Select an Option 

Select x axis field

Label Rotation

☒ Horizontal  ☐ Vertical  ☐ Slant 

Enter new chart label

- Field:** Select an attribute from the dropdown. Available attributes are based on the datasource if one has been selected for this chart.
- Label:** Provide a descriptive label for the X-Axis.
- Label Rotation:** Select the rotation for the label: Horizontal, Vertical, or Slant.

Y-Axis


Provide the following information:

Y - AXIS

Y-Axis Label:




Enter y-axis label

Field*

Frequency 

Select y axis field.

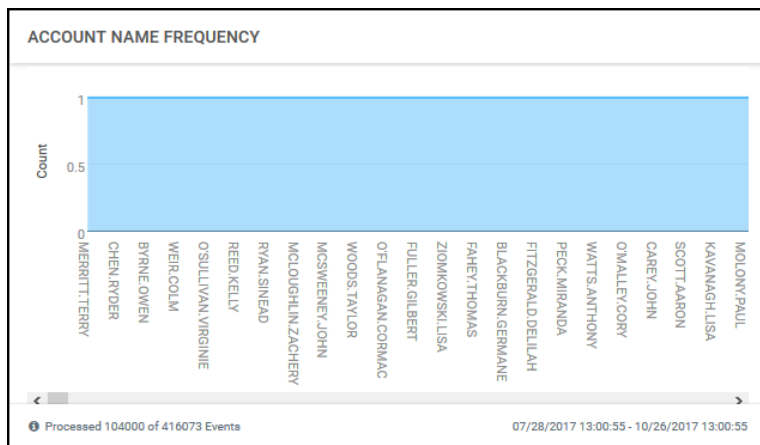
Label Rotation

☒ Horizontal  ☐ Vertical  ☐ Slant 

Enter new chart label

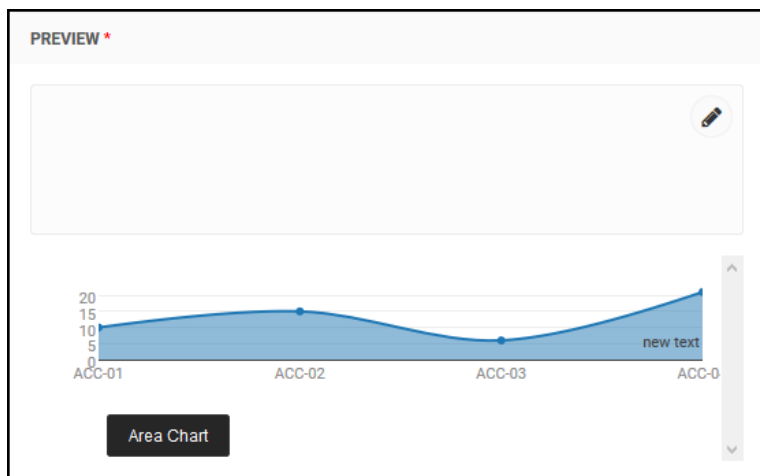
- Field:** Select a field from the dropdown.
- Label:** Provide a descriptive label for the Y-Axis.
- Label Rotation:** Select the rotation for the label.

Area Chart



Preview

Preview input you will enter in the proceeding steps:



General Details

Complete the following information:

GENERAL DETAILS

Chart Label: *

Enter new chart label

Chart Orientation:

Vertical | Horizontal

Select Chart Orientation

Chart Color

Select color of chart

- Chart Label:** Provide a unique name for the chart.
- Chart Orientation:** Select an orientation for the chart.
- Chart Color:** Use color picker and click **Choose** to select a color.

Chart Details

Provide the following information:

CHART DETAILS

Datasource:

Google Login

Select the datasource you would like to create the chart for (Optional)

What type of data you want to use*

Event Data

Select the type of data you would like to run query on.

Time Range*

Last 7 days

Select date range you would like to run the query for

- (Optional) **Datasource:** Select a datasource from the dropdown.
- What type of data you want to use:** Select the type of data on which to run the query from the dropdown.
- Time Range:** Select the time range to display in chart results.

X-Axis

Provide the following information:

X - AXIS

X-Axis Label:

Enter x-axis label

Field*

Select x axis field

Label Rotation

Enter new chart label

- Field:** Select an attribute from the dropdown. Available attributes are based on the datasource if one has been selected for this chart.
- Label:** Provide a descriptive label for the X-Axis.
- Label Rotation:** Select the rotation for the label.

Y-Axis

Provide the following information:

Y - AXIS

Y-Axis Label:

Enter y-axis label

Field*

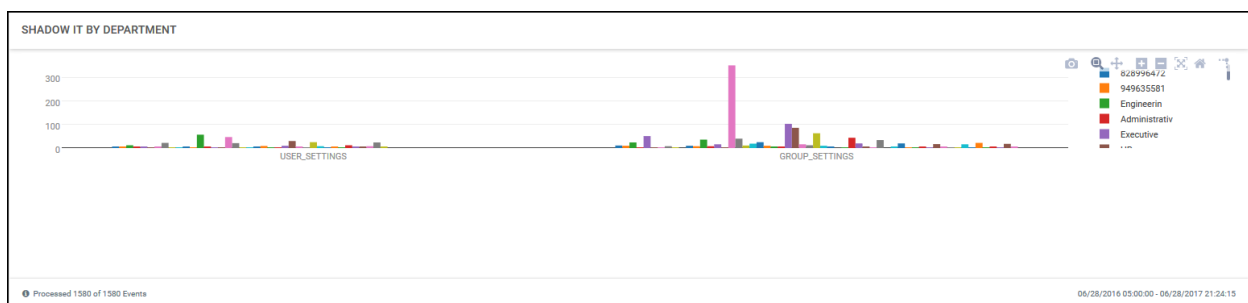
Select y axis field.

Label Rotation

Enter new chart label

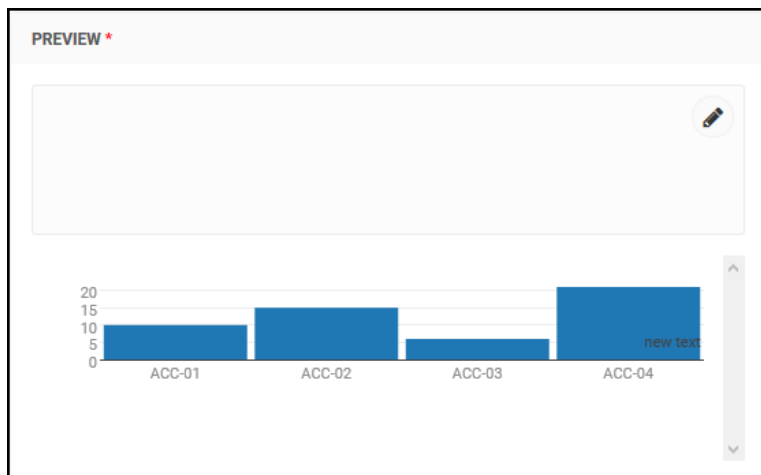
- Label:** Provide a descriptive label for the Y-Axis.
- Field:** Select a field from the dropdown.
- Label Rotation:** Select the rotation for the label.

Bar Chart



Preview

Preview input you will enter in the proceeding steps:



General Details

Complete the following information:

GENERAL DETAILS

Chart Label: *

Enter new chart label

Chart Orientation:

☒ Vertical ☐ Horizontal

Select Chart Orientation

Chart Color

Select color of chart

- Chart Label:** Provide a unique name for the chart.
- Chart Orientation:** Select an orientation for the chart.
- Chart Color:** Use color picker and click **Choose** to select a color.

Chart Details

Provide the following information:

CHART DETAILS

Datasource:
 Google Login
 Select the datasource you would like to create the chart for (Optional)

What type of data you want to use*
 Event Data
 Select the type of data you would like to run query on.

Time Range*
 Last 7 days
 Select date range you would like to run the query for

- (Optional) **Datasource:** Select a datasource from the dropdown.
- What type of data you want to use:** Select the type of data on which to run the query from the dropdown.
- Time Range:** Select the time range to display in chart results.

X-Axis

Provide the following information:

X - AXIS

X-Axis Label:
 Enter x-axis label

Field*
 Select an Option
 Select x axis field

Label Rotation
 ✓ Horizontal Vertical Slant
 Enter new chart label

- Field:** Select an attribute from the dropdown. Available attributes are based on the datasource if one has been selected for this chart.
- Label:** Provide a descriptive label for the X-Axis.
- Label Rotation:** Select the rotation for the label.

Y-Axis

Provide the following information:

Y - AXIS

Y-Axis Label:

Enter y-axis label

Field*

Select y axis field.

Label Rotation

Enter new chart label

- Label:** Provide a descriptive label for the Y-Axis.
- Field:** Select a field from the dropdown.
- Label Rotation:** Select the rotation for the label.

Geolocation Map



Preview

Preview input you will enter in the proceeding steps:

PREVIEW *

General Details

Provide the following information:

- a. **Chart Label:** Provide a unique name for the chart.
- b. **Chart Color:** Use color picker and click **Choose** to select a color.

Chart Details

Provide the following information:

- a. (Optional) **Datasource:** Select a datasource from the dropdown.
- b. **What type of data you want to use:** Select the type of data on which to run the query from the dropdown.
- c. **Time Range:** Select the time range to display in chart results.

Fields

Provide the following information:

The screenshot shows a configuration interface with two sections, FIELD 1 and FIELD 2. Each section contains a 'Field*' label, a dropdown menu with a downward arrow, and the text 'Select geomap field'. An 'Add Line' button is located to the right of each section.

- Field 1:** Select a field from dropdown. Available attributes are based on the datasource if one has been selected for this chart.
- Field 2:** Select a field from dropdown. Available attributes are based on the datasource if one has been selected for this chart.

Group

Provide the following information:

The screenshot shows a configuration interface for a 'GROUP'. It contains a 'Group By Field' label, a dropdown menu with a downward arrow, and the text 'Select group by field'.

- Group by Field:** Select an option under which to group fields from the dropdown.

Tabular Data

ACCOUNT LOCKOUTS	
Lockout	Count
GRAINNE.NI CHEARBHAILL	45
ANNE MARIE.VILLEMAGNE	42
MICHAEL.SAMUEL.KOK	35
ELIZABETH.HOUGHTON	2
ABE.WOOD	1
AINE.MOORE	1

Processed 140 of 140 Events 07/28/2017 13:30:32 - 10/26/2017 13:30:32

Preview

Preview input you will enter in the proceeding steps:

PREVIEW *	
X	Y
ACC-01	20
ACC-02	56

General Details

Complete the following information:

GENERAL DETAILS

Chart Label: *

Enter new chart label

Chart Orientation:

Vertical | Horizontal

Select Chart Orientation

Chart Color

Select color of chart

- Chart Label:** Provide a unique name for the chart.
- Chart Orientation:** Select an orientation for the chart.
- Chart Color:** Use color picker and click **Choose** to select a color.

Chart Details

Provide the following information:

CHART DETAILS

Datasource:

Google Login

Select the datasource you would like to create the chart for (Optional)

What type of data you want to use*

Event Data

Select the type of data you would like to run query on.

Time Range*

Last 7 days

Select date range you would like to run the query for

- (Optional) **Datasource:** Select a datasource from the dropdown.
- What type of data you want to use:** Select the type of data on which to run the query from the dropdown.
- Time Range:** Select the time range to display in chart results.

Column 1

Provide the following information:

COLUMN 1

Column 1 Label

Enter column 1 label

Field*

Select an Option

Select x axis field

Label Rotation

✓ Horizontal

Vertical

Slant

Enter new chart label

- Field:** Select an attribute from the dropdown. Available attributes are based on the datasource if one has been selected for this chart.
- Label:** Provide a descriptive label for the X-Axis.
- Label Rotation:** Select the rotation for the label.

Column 2

Provide the following information:

COLUMN 2

Column 2 Label

Enter column 2 label

Field*

Frequency

Select y axis field.

Label Rotation

✓ Horizontal

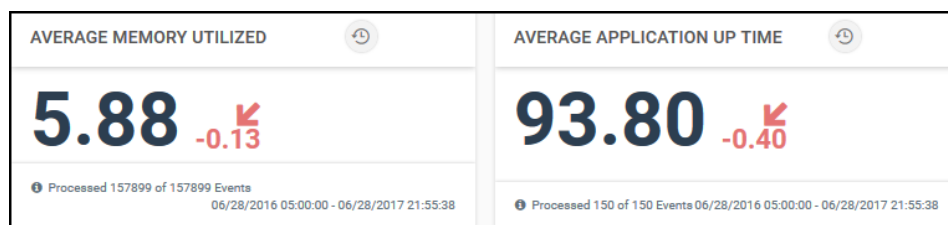
Vertical

Slant

Enter new chart label

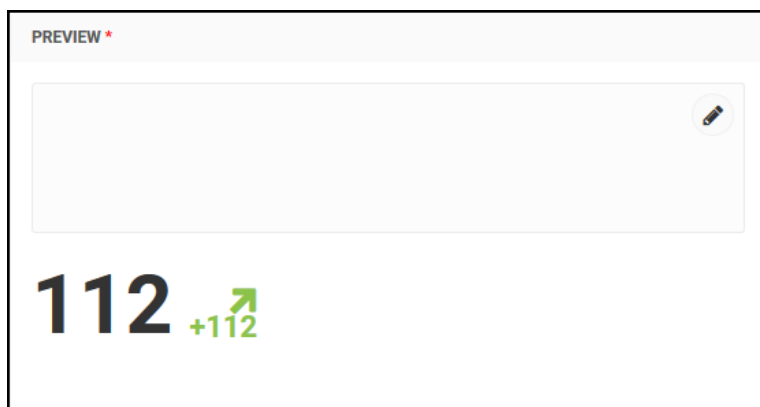
- Column 2 Label:** Provide a descriptive label for the Y-Axis.
- Field:** Select a field from the dropdown.
- Label Rotation:** Select the rotation for the label.

Number Chart



Preview

Preview input you will enter in the proceeding steps:



General Details

Complete the following information:

GENERAL DETAILS

Chart Label:*

Enter new chart label

- a. **Chart Label:** Provide a unique name for the chart.

Chart Details

Provide the following information:

CHART DETAILS

<p>Datasource:</p> <div>Google Login</div> <p>Select the datasource you would like to create the chart for (Optional)</p>	<p>What type of data you want to use*</p> <div>Event Data</div> <p>Select the type of data you would like to run query on.</p>
<p>Time Range*</p> <div>Last 7 days</div> <p>Select date range you would like to run the query for</p>	

- (Optional) **Datasource:** Select a datasource from the dropdown.
- What type of data you want to use:** Select the type of data on which to run the query from the dropdown.
- Time Range:** Select the time range to display in chart results.

Field

Provide the following information:

FIELD

Operator : *

Field*

AVG

Select an Option

Operator

Field

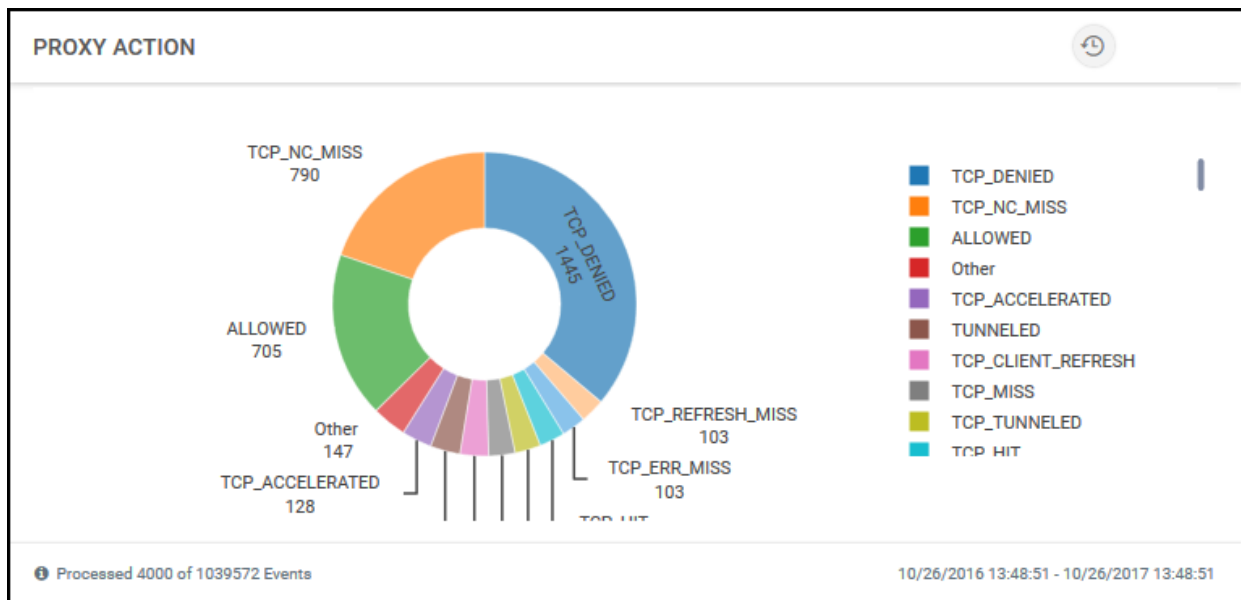
View Based on

Daily

Select the View Based on

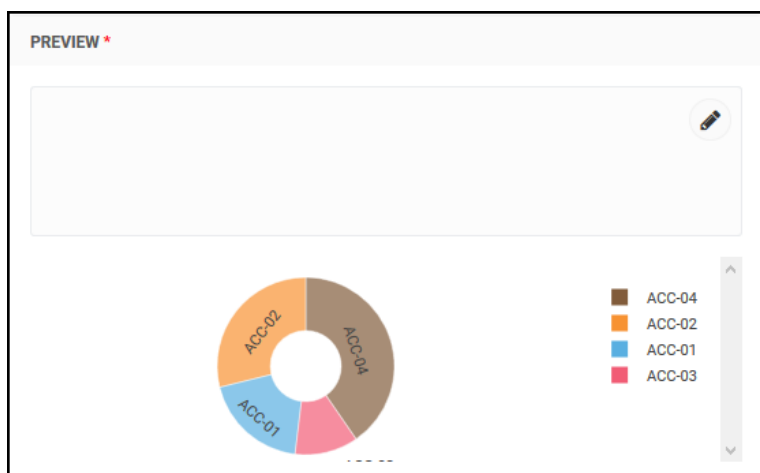
- Operator:** Select from drop down. Example: AVG (Average).
- Field:** Select a field from the dropdown.
- View Based on:** Select from dropdown. Example: Daily.

Donut Chart



Preview

Preview input you will enter in the proceeding steps:



General Details

Complete the following information:

GENERAL DETAILS

Chart Label:*

Enter new chart label

Chart Orientation:

☒ Vertical
 ☐ Horizontal

Select Chart Orientation

Chart Color

▼

Select color of chart

- Chart Label:** Provide a unique name for the chart.
- Chart Orientation:** Select an orientation for the chart.
- Chart Color:** Use color picker and click **Choose** to select a color.

Chart Details

Provide the following information:

CHART DETAILS

Datasource:
Google Login
Select the datasource you would like to create the chart for (Optional)

What type of data you want to use*
Event Data
Select the type of data you would like to run query on.

Time Range*
Last 7 days
Select date range you would like to run the query for

- (Optional) **Datasource:** Select a datasource from the dropdown.
- What type of data you want to use:** Select the type of data on which to run the query from the dropdown.
- Time Range:** Select the time range to display in chart results.

Pie Slice Label

Provide the following information:

PIE SLICE LABEL

Field*
Select an Option
Select x axis field

- Field:** Select an attribute from the dropdown. Available attributes are based on the datasource if one has been selected for this chart.

Pie Slice Size

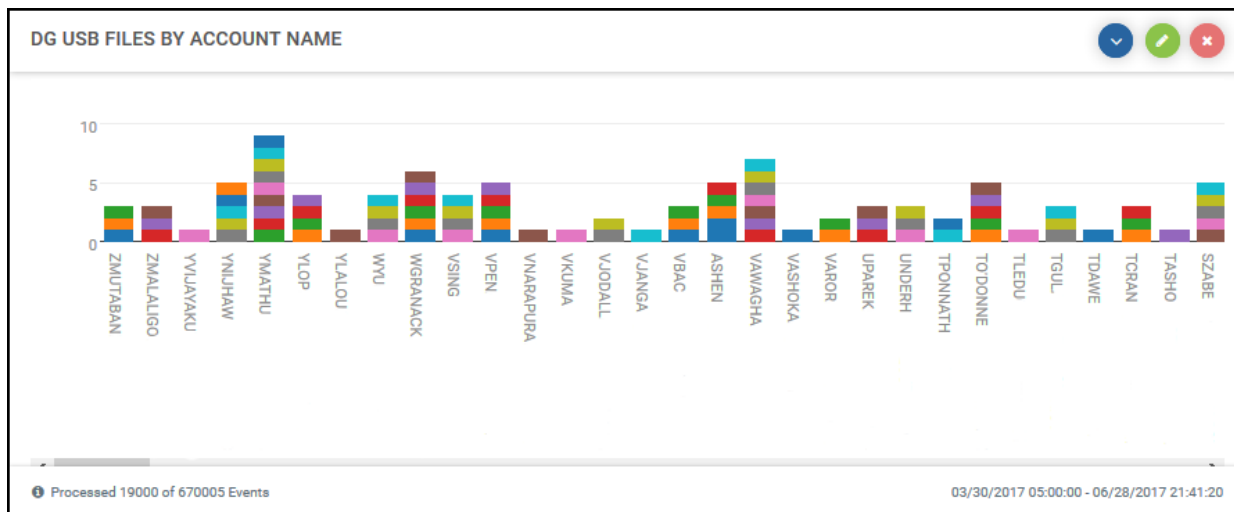
Provide the following information:

PIE SLICE SIZE

Field*
Frequency
Select y axis field.

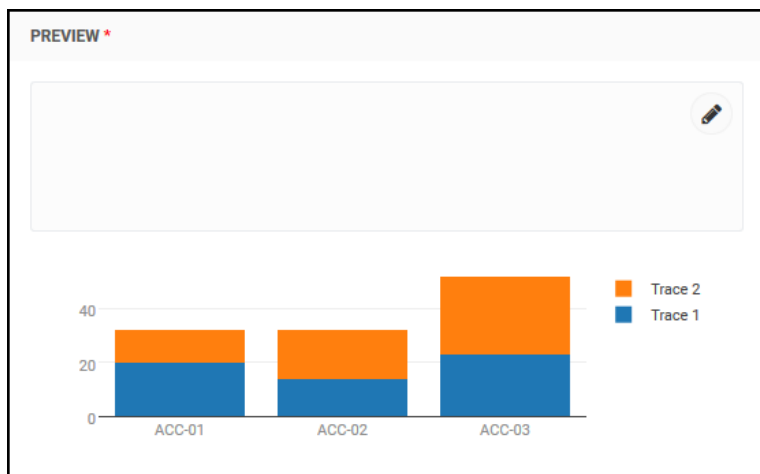
- Field:** Select a field from the dropdown.

Stacked Bar Charts



Preview

Preview input you will enter in the proceeding steps:



General Details

Provide the following information:

GENERAL DETAILS

Chart Label:*

Enter new chart label

Bar Mode:

Stack

Select Bar Mode

Chart Orientation:

✓ Vertical

Horizontal

Select Chart Orientation

- Chart Label:** Provide a unique name for the chart.
- Bar Mode:** Select a bar mode from dropdown.
- Chart Orientation:** Select an orientation for the chart.

Chart Details

Provide the following information:

CHART DETAILS

Datasource:

Google Login

Select the datasource you would like to create the chart for (Optional)

What type of data you want to use*

Event Data

Select the type of data you would like to run query on.

Time Range*

Last 7 days

Select date range you would like to run the query for

- (Optional) **Datasource:** Select a datasource from the dropdown.
- What type of data you want to use:** Select the type of data on which to run the query from the dropdown.
- Time Range:** Select the time range to display in chart results.

X-Axis

Provide the following information:

X - AXIS

X-Axis Label:

Enter x-axis label

Field*

Select an Option ▼
Select x axis field

Label Rotation

✓ Horizontal ... Vertical ! Slant !
Enter new chart label

- Field:** Select an attribute from the dropdown. Available attributes are based on the datasource if one has been selected for this chart.
- Label:** Provide a descriptive label for the X-Axis.
- Label Rotation:** Select the rotation for the label.

Stacks

Provide the following information:

STACKS

Y-Axis Label:

Enter y-axis label

Stacked on*

▼
Select stack field

Label Rotation

✓ Horizontal ... Vertical ! Slant !
Enter new chart label

- Label:** Provide a descriptive label for the stacks.
- Stacked on:** Select attribute from dropdown.
- Label Rotation:** Select the rotation for the label.

Top N Results Chart

RARE USER AGENTS		
	os x) applewebkit/602.4.6 (KHTML,	1
	mozilla/5.0 (linux; android 6.0.1; SAMSUNG SM-G920T Build/MMB29K) AppleWebKit/537.36 (KHTML, like Gecko)	1
	603.1.30	1
	webkit/537.36	1
	/5.0 (macintosh; intel mac os x 10_12_4) AppleWebKit/603.1.30	1

Processed 141000 of 1039572 Events

10/26/2016 15:25:38 - 10/26/2017 15:25:38

Preview

Preview input you will enter in the proceeding steps:

PREVIEW *		
	ACC-01	20
	ACC-02	56
	ACC-03	79
	ACC-04	80

General Details

Provide the following information:

GENERAL DETAILS

Chart Label:*

Enter new chart label

Type:*

▼

Top
Rare

- Chart Label:** Enter a unique name for the chart.
- Type:** Select **Top** or **Rare** from dropdown.

Chart Details

Provide the following information:

CHART DETAILS

Datasource:

Select an Option

▼

Select the datasource you would like to create the chart for (Optional)

What type of data you want to use*

Event Data

▼

Select the type of data you would like to run query on.

Time Range*

Select Duration

▼

Select date range you would like to run the query for

Field:*

Select an Option

▼

Select x axis field

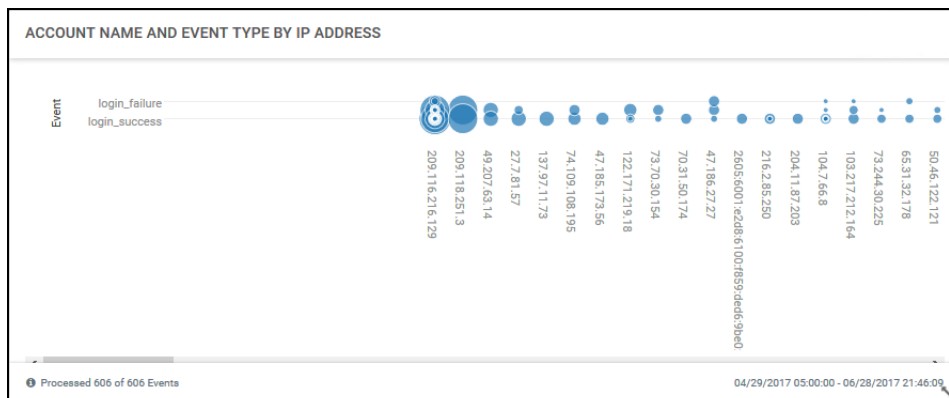
Count :*

5

Total List

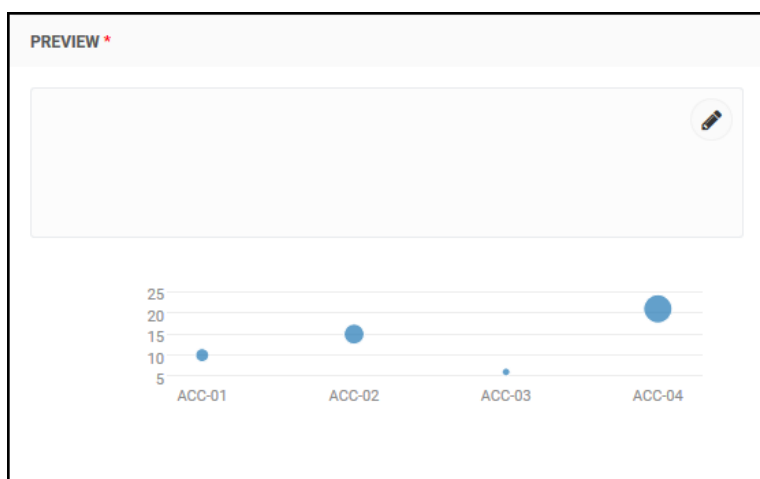
- (Optional) **Datasource:** Select a datasource from the dropdown.
- Time Range:** Select the time range to display in chart results.
- What type of data you want to use:** Select the type of data on which to run the query from the dropdown.
- Field:** Select from dropdown.
- Count:** Specify a count for N. Default: 5.

Bubble Charts



Preview

Preview input you will enter in the proceeding steps:



General Details

Complete the following information:

GENERAL DETAILS

Chart Label: *

Enter new chart label

- Chart Label:** Provide a unique name for the chart.

Chart Details

Provide the following information:

CHART DETAILS

Datasource:

Google Login

Select the datasource you would like to create the chart for (Optional)

What type of data you want to use*

Event Data

Select the type of data you would like to run query on.

Time Range*

Last 7 days

Select date range you would like to run the query for

- (Optional) **Datasource:** Select a datasource from the dropdown.
- What type of data you want to use:** Select the type of data on which to run the query from the dropdown.
- Time Range:** Select the time range to display in chart results.

X-Axis

Provide the following information:

X - AXIS

X-Axis Label:

Enter x-axis label

Field*

Select an Option

Select x axis field

View Based on

Daily

Select x axis field

Label Rotation

✓ Horizontal

Vertical

Slant

Enter new chart label

- Field:** Select an attribute from the dropdown. Available attributes are based on the datasource if one has been selected for this chart.
- Label:** Provide a descriptive label for the X-Axis.
- Label Rotation:** Select the rotation for the label.

Y-Axis

Provide the following information:

Y - AXIS

Y-Axis Label:

Enter y-axis label

Field*

Select y axis field.

Label Rotation

☒ Horizontal ☐ Vertical ☐ Slant

Enter new chart label

- Field:** Select a field from the dropdown.
- Label Rotation:** Select the rotation for the label.
- Label:** Provide a descriptive label for the Y-Axis.

Z-Axis

Provide the following information:

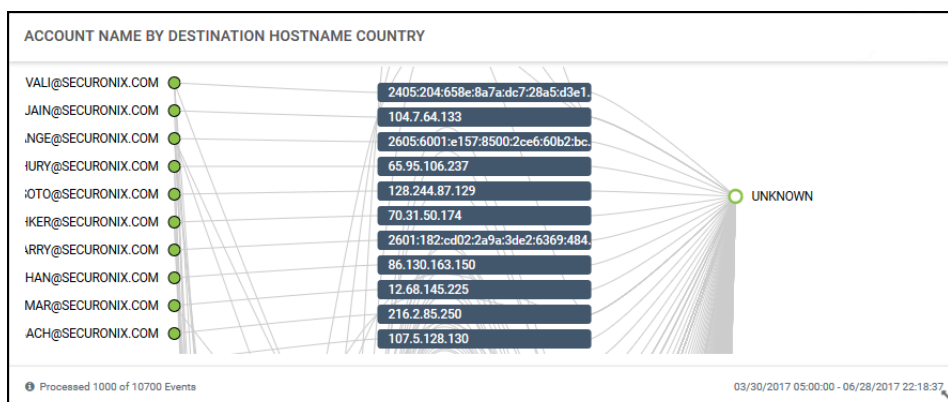
Z - AXIS

Field*

Select z axis field

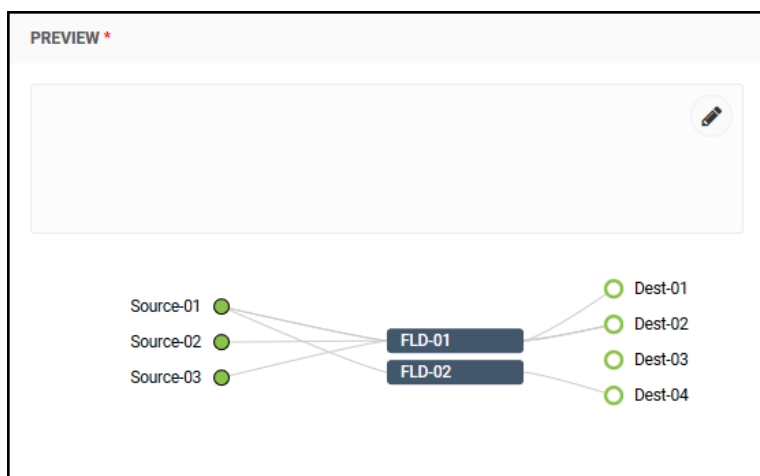
- Field:** Select a Z-axis field from dropdown.

Source Destination Chart



Preview

Preview input you will enter in the proceeding steps:



General Details

Provide the following information:

GENERAL DETAILS

Chart Label:*

Enter new chart label

- a. **Chart Label:** Provide a unique name for the chart.

Chart Details

Provide the following information:

CHART DETAILS

Datasource:
Select the datasource you would like to create the chart for (Optional)

What type of data you want to use*
Select the type of data you would like to run query on.

Time Range*
Select date range you would like to run the query for


- a. (Optional) **Datasource:** Select a datasource from the dropdown.
- b. **Time Range:** Select the time range to display in chart results.
- c. **What type of data you want to use:** Select the type of data on which to run the query from the dropdown.

Source

Provide the following information:

SOURCE

Field*



Select source field.


- a. **Field:** Select a field from dropdown. Available attributes are based on the datasource if one has been selected for this chart.

Field

Provide the following information:

FIELD

Field*



Select y axis field.


- a. **Field:** Select a field from dropdown. Available attributes are based on the datasource if one has been selected for this chart.

Destination

Provide the following information:

DESTINATION

Field*



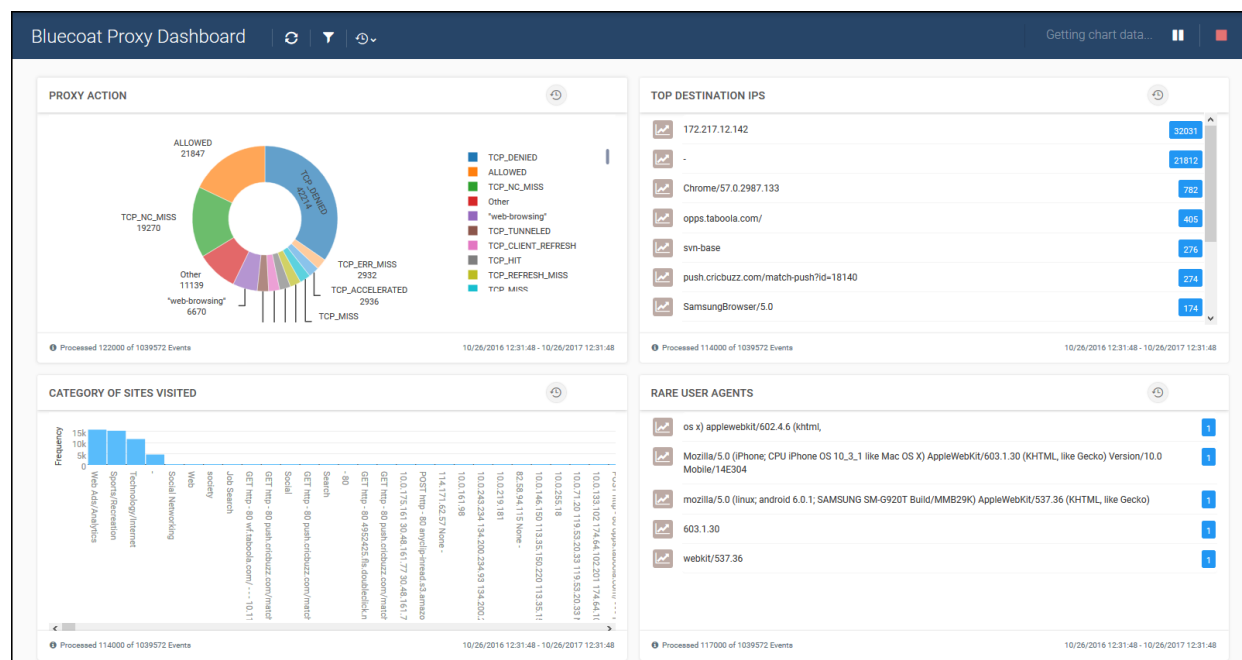
Select destination field.

- a. **Field:** Select a field from dropdown. Available attributes are based on the datasource if one has been selected for this chart.

Using Dashboards

When you have configured the widgets, ArcSight UBA will collect chart data and render the chart. You can filter the information on the dashboard or click data points to launch actions.

From this screen, you can perform the following actions:



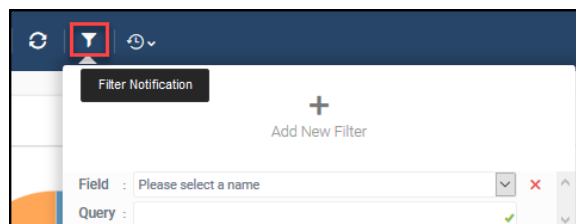
Click Refresh icon to refresh dashboards.



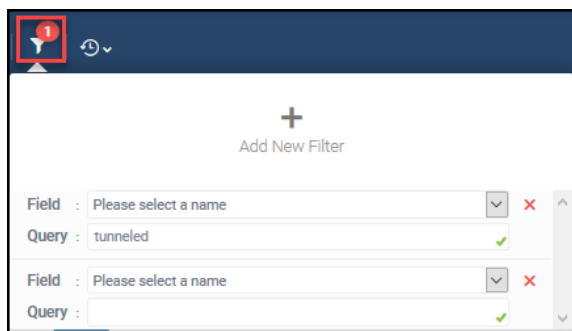
Click Filter icon to add a filter to the chart results.

Click **Add New Filter:**

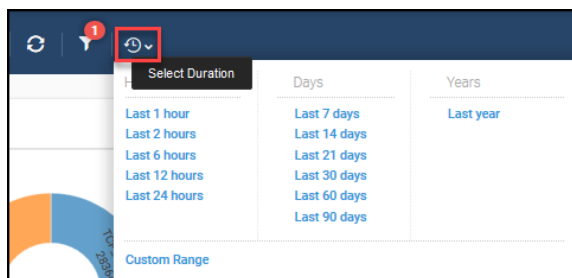
- Select Field from dropdown.
AND/OR
- Enter Query.



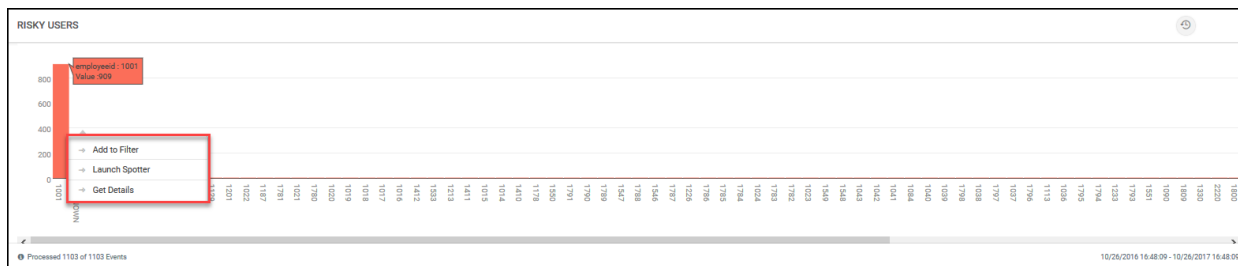
Click the red X to remove a filter.



Click Duration icon to select a time range for the chart.



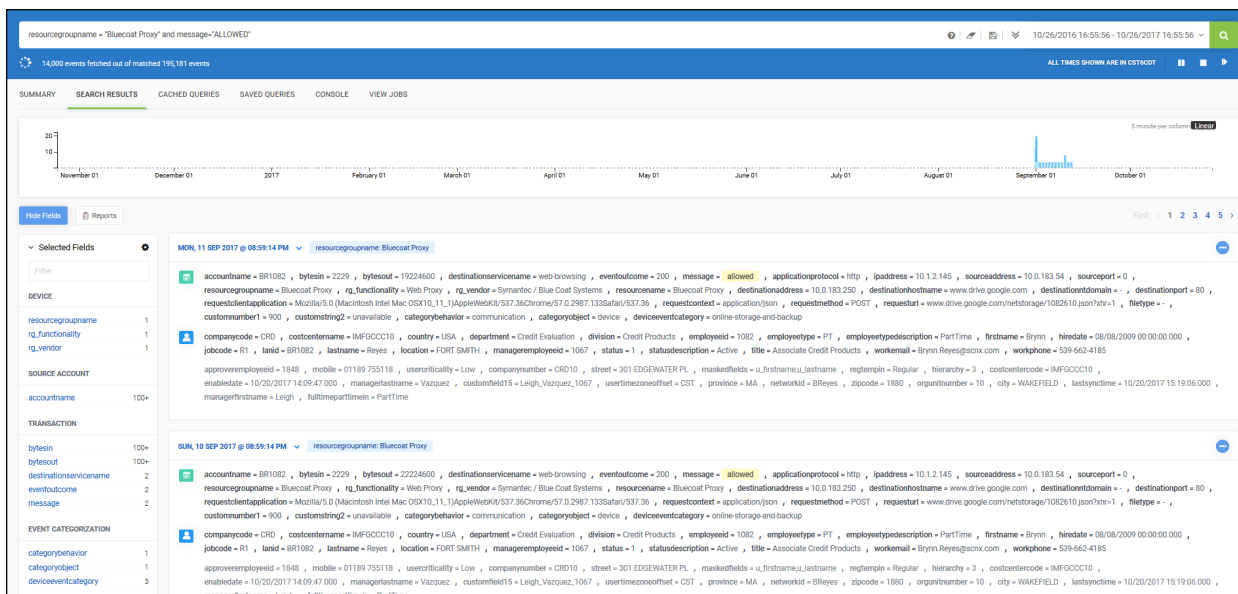
Click a data point to launch actions:





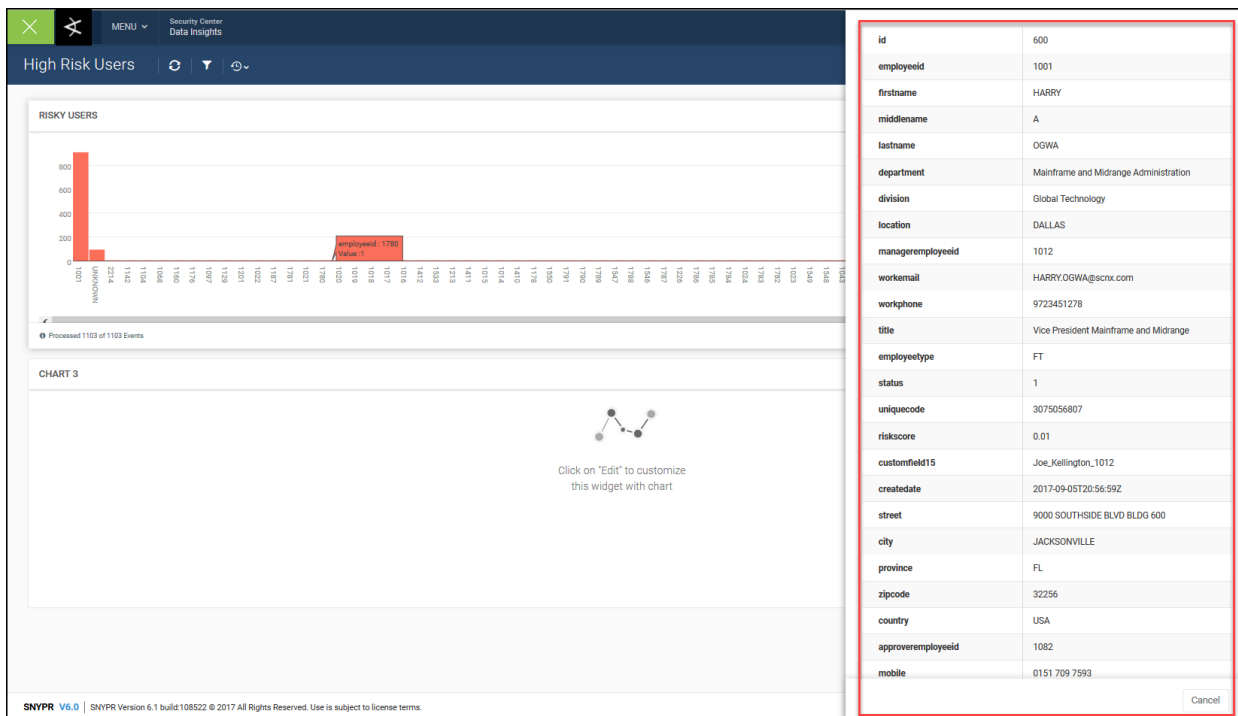
Note: Available actions may vary based on the chart type and data type.

- **Add to Filter:** Filters the chart results based on the data point.
- **Launch Spotter:** Launches a Spotter search based on the data point.



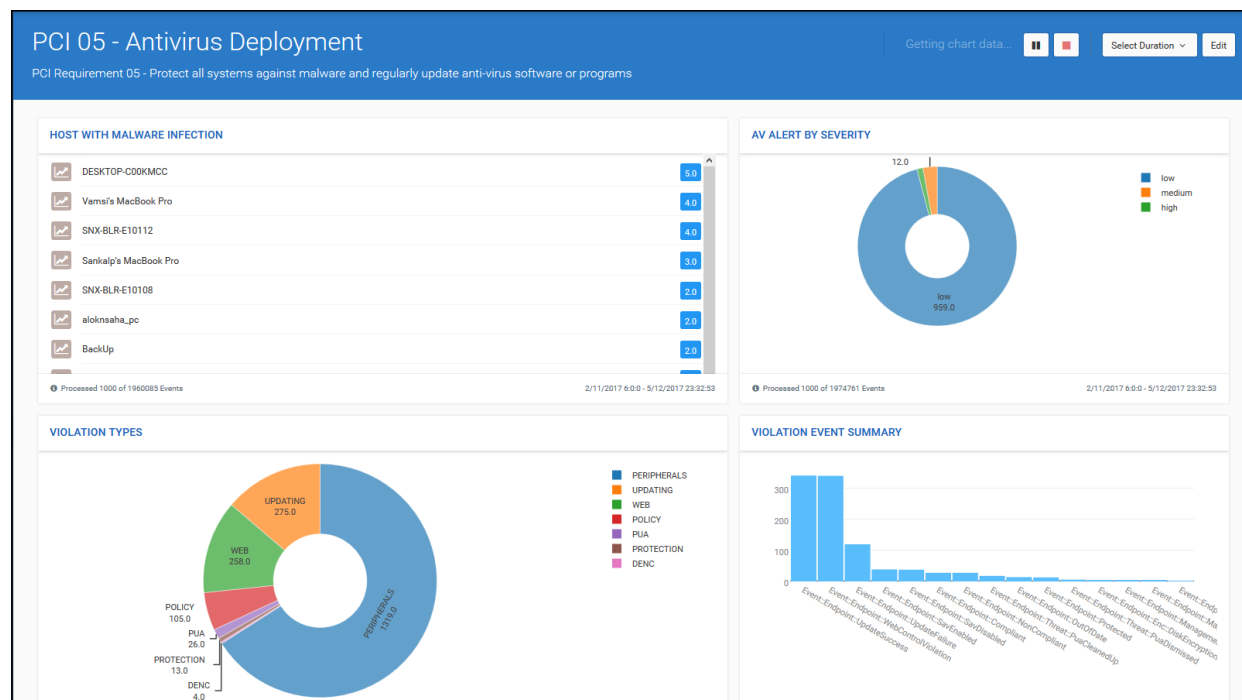
For more information about searching ArcSight UBA, see [Spotter](#).

- **Get Details:** Opens detail panel about the data point.



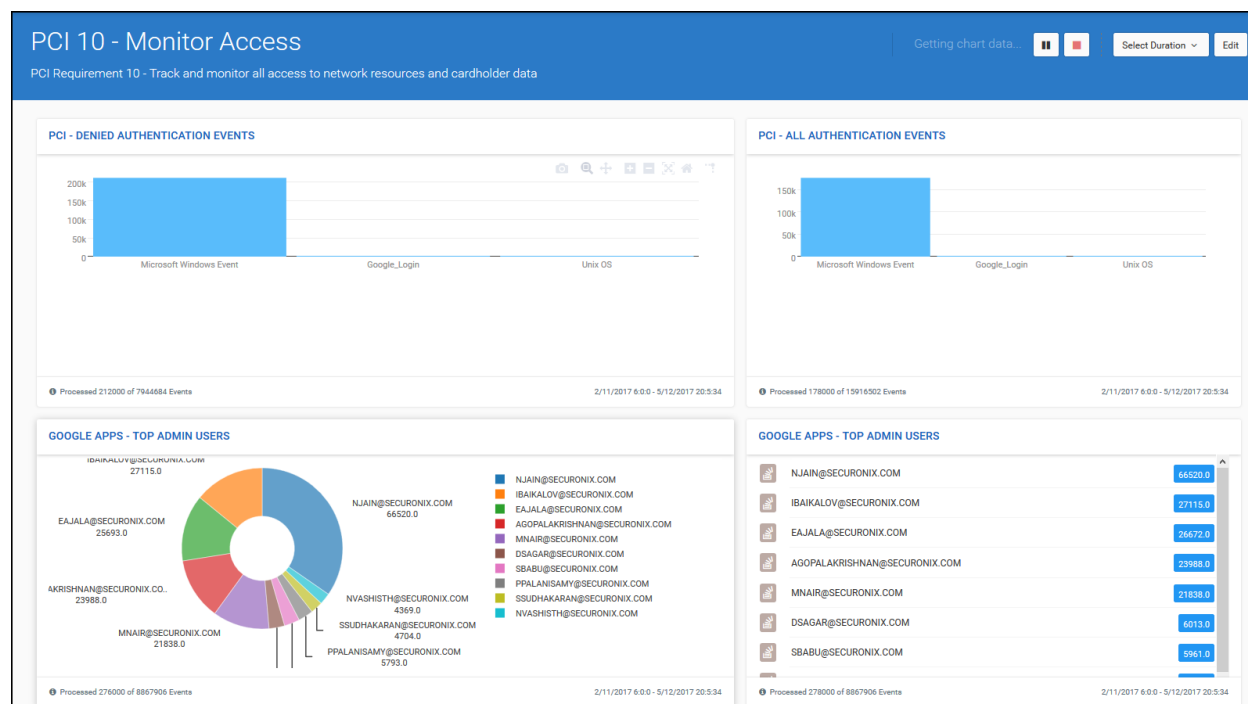
PCI 05 - Anti-virus Deployment

PCI Requirement 05 - Protect all systems against malware and regularly update anti-virus software or programs.



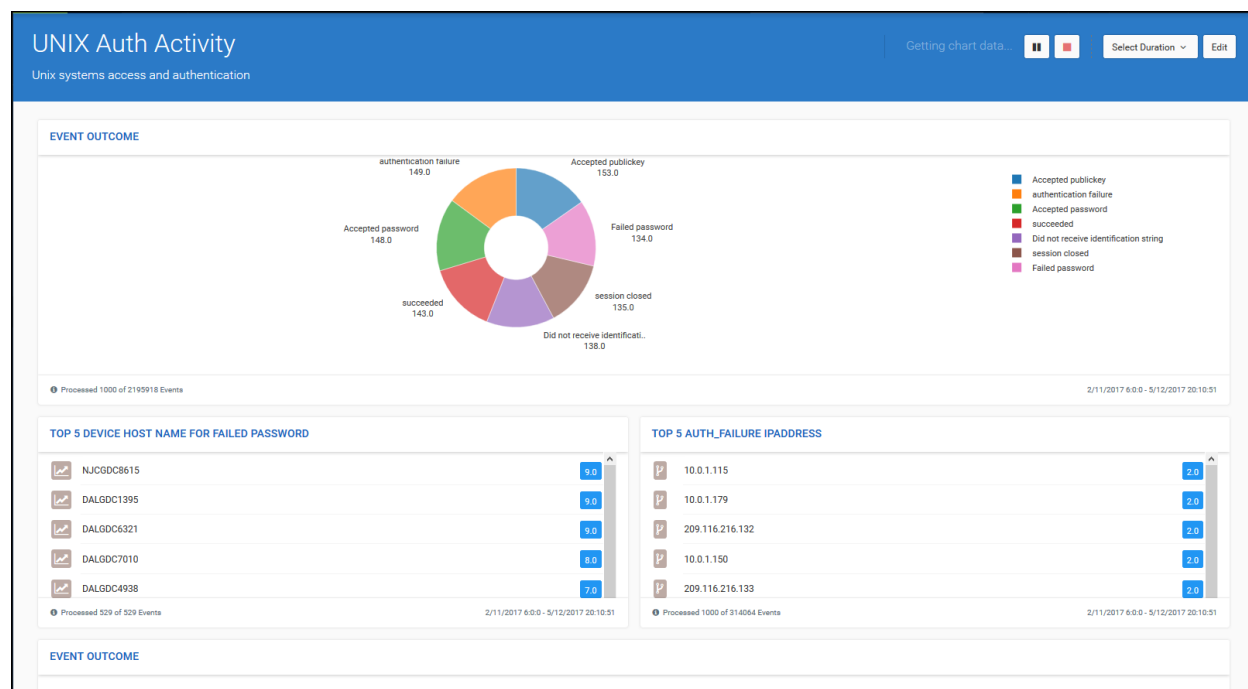
PCI 10 - Monitor Access

PCI Requirement 10- Track and monitor all access to network resources and cardholder data.



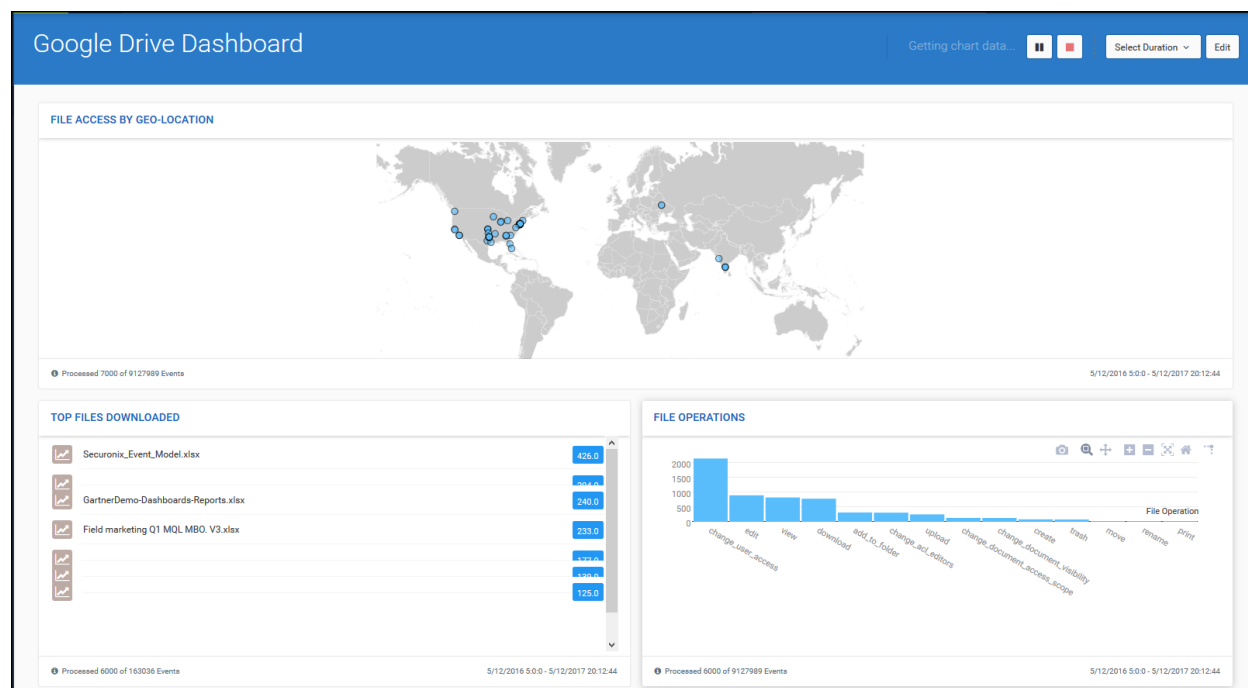
UNIX Auth Activity

Unix systems access and authentication.



Google Drive Dashboard

Activities on Google Drive.



Compliance Dashboards

In Data Insights, you can create, modify, save, and share custom dashboards to gain compliance data insights for your organization with the My Dashboards feature. Examples of dashboards that are available include the following:

- [PCI Dashboards](#)
- [HIPAA Dashboards](#)
- [Compliance Dashboards](#)
- [Compliance Dashboards](#)
- [Compliance Dashboards](#)
- [Compliance Dashboards](#)
- [Compliance Dashboards](#)

PCI Dashboards

The dashboards for PCI requirements are listed in the following table.

PCI Require- metn	Description	Widget Samples	Device Class
01 - Firewall Con- figurations	Install and maintain a fire- wall configuration to pro- tect cardholder data	PCI - All Firewall Con- figuration Events PCI - All Inbound Con- nections PCI - All Outbound Con- nections PCI - Denied Inbound Con- nections PCI - Denied Outbound Connections	Firewall, IDS (Intru- sion Detection Sys- tem)
02 - System Pass- word Man- agement	Do not use vendor-sup- plied defaults for system passwords and other security parameters	PCI - Password Changes and Resets PCI - Account Sharing PCI - Account Lockouts	OS
05 - Antivirus Deployment	Protect all systems against malware and reg- ularly update anti-virus software or programs	PCI - Hosts with AV Pro- tection PCI - Hosts without AV Pro- tection PCI - Hosts with Mal- ware Infection	Malware
08 - Account Man- agement	Identify and authenticate access to system com- ponents	PCI - User Account Creation, Deletion PCI - User Account Priv- ilege Changes PCI - User Group Creation, Deletion PCI - User Group Privilege Changes PCI - DB User Account Creation, Deletion PCI - DB User Privilege Changes	OS and DB

PCI Require- metn	Description	Widget Samples	Device Class
09 - Physical Access	Restrict physical access to cardholder data	PCI - All Authentication Events PCI - Denied Authentication Events PCI - All System Auditing Events PCI - VPN Access Summary PCI - System Admin/Root User Activity PCI - DB Admin Activity PCI - Application Admin Activity PCI - File and Document Management Activity	VPN, OS, Access Privilege, DB, Application and CMS
11-Test Security Systems and Processes	Regularly test security systems and processes	PCI - Critical Vulnerabilities PCI - Top Vulnerable Assets PCI - All Vulnerabilities by Criticality PCI - All Firewall Configuration Events PCI - All Wireless Configuration Events	Scanner, Firewall, IDS, Wireless
12-Security Policy Review	Maintain a policy that addresses information security for all personnel	PCI - All Policy Changes PCI - All Policy Violations	

HIPAA Dashboards

The dashboards for HIPAA are listed in the following table.

HIPAA Requirement	Description	Widget Samples	Device Class
HIPAA - Privacy Safeguards	HIPAA Privacy Rule - 45 CFR Part 164, Subpart E requires appropriate safeguards to protect the privacy of medical records and other personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. For more information visit, https://www.hhs.gov/hipaa/for-professionals/privacy/	HIPAA - All Application Activity HIPAA - Privacy Violations	Application

HIPAA Requirement	Description	Widget Samples	Device Class
HIPAA - Administrative Safeguards	HIPAA Security Rule - Administrative Safeguards - 45 CFR 164.308 requires appropriate administrative safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. For more information visit, https://www.hhs.gov/hipaa/for-professionals/security/	<p>HIPAA - All Policy Changes</p> <p>HIPAA - All Policy Violations</p> <p>HIPAA - File and Document Management Activity</p> <p>HIPAA - Critical Vulnerabilities</p> <p>HIPAA - Top Vulnerable Assets</p> <p>HIPAA - All Vulnerabilities by Criticality</p> <p>HIPAA - All Firewall Configuration Events</p> <p>HIPAA - All Wireless Configuration Events</p> <p>HIPAA - Anti-Malware Deployed</p> <p>HIPAA - Hosts without Anti-Malware Protection (Stopped, Disabled, Not installed)</p> <p>HIPAA - Hosts with Malware Infection</p> <p>HIPAA - Anti-Malware Protection Events</p> <p>HIPAA - Anti-malware Scan Summary</p> <p>HIPAA - Anti-Malware Update Failure, Success</p> <p>HIPAA - Password Changes and Resets</p> <p>HIPAA - Account Sharing</p>	CMS, Scanner, Firewall, IDS, Wireless, Malware, OS, VPN, Application Privilege, DB

HIPAA Requirement	Description	Widget Samples	Device Class
		HIPAA - Account Lock-outs HIPAA - All Authentication Events HIPAA - Denied Authentication Events HIPAA - VPN Access Summary HIPAA - System Admin/Root User Activity HIPAA - DB Admin Activity HIPAA - Application Admin Activity	

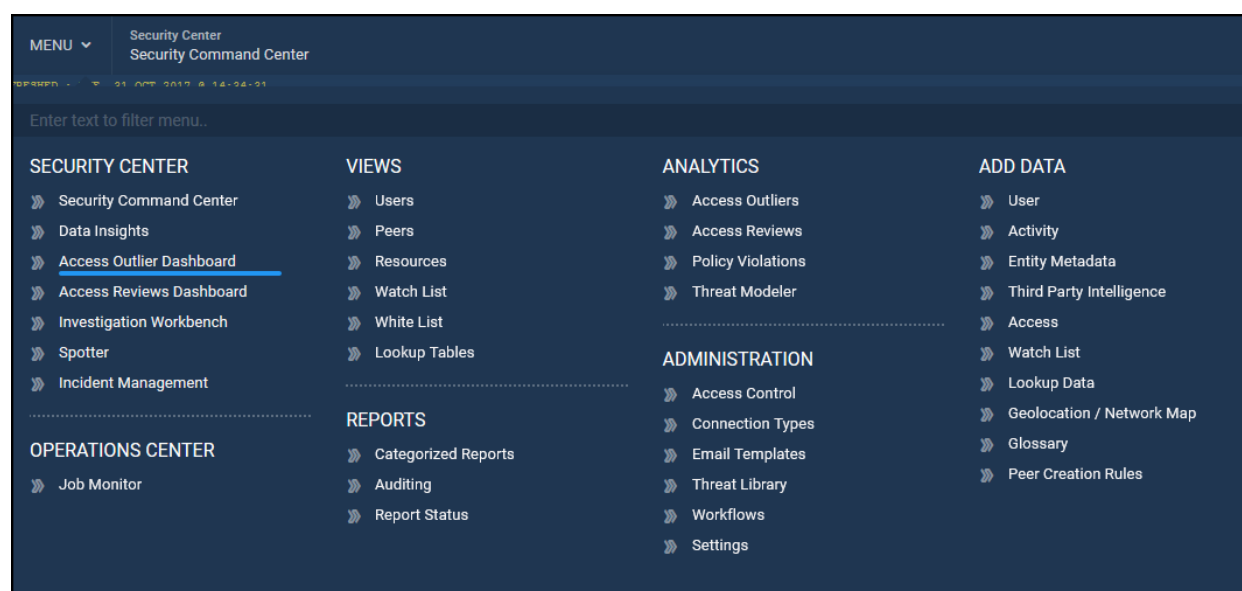
HIPAA Requirement	Description	Widget Samples	Device Class
HIPAA - Technical Safeguards	<p>HIPAA Security Rule - Technical Safeguards - 45 CFR 164.312 requires that only authorized persons have access to electronic protected health information (e-PHI). For more information visit, https://www.hhs.gov/hipaa/for-professionals/security/</p>	<p>HIPAA - User Account Creation, Deletion HIPAA - User Account Privilege Changes HIPAA - User Group Creation, Deletion HIPAA - User Group Privilege Changes HIPAA - DB User Account Creation, Deletion HIPAA - DB User Privilege Changes HIPAA - Account Sharing Summary HIPAA - Automated Logoff of User Account HIPAA - Critical File Changes HIPAA - EMR Access by Admin Users HIPAA - Encryption Events Summary HIPAA - File Integrity Events Summary HIPAA - Logon Attempts (Win) HIPAA - Summary of Database Accessed HIPAA - Summary of File Access HIPAA - User Account Access Summary HIPAA - ePHI Application Audit Events HIPAA - Application Admin Activity</p>	OS and DB

HIPAA Requirement	Description	Widget Samples	Device Class
		HIPAA - All System Auditing Events HIPAA - System Admin/Root User Activity HIPAA - DB Admin Activity	
HIPAA - Physical Safeguards	HIPAA Security Rule - Physical Safeguards - 45 CFR 164.310 - requires facility access be restricted to authorized persons. It extends to proper use of workstations, devices and transfer, removal, disposal, and re-use of electronic media. For more information visit, https://www.hhs.gov/hipaa/for-professionals/security/	HIPAA - Badge Access to Datacenter	Physical

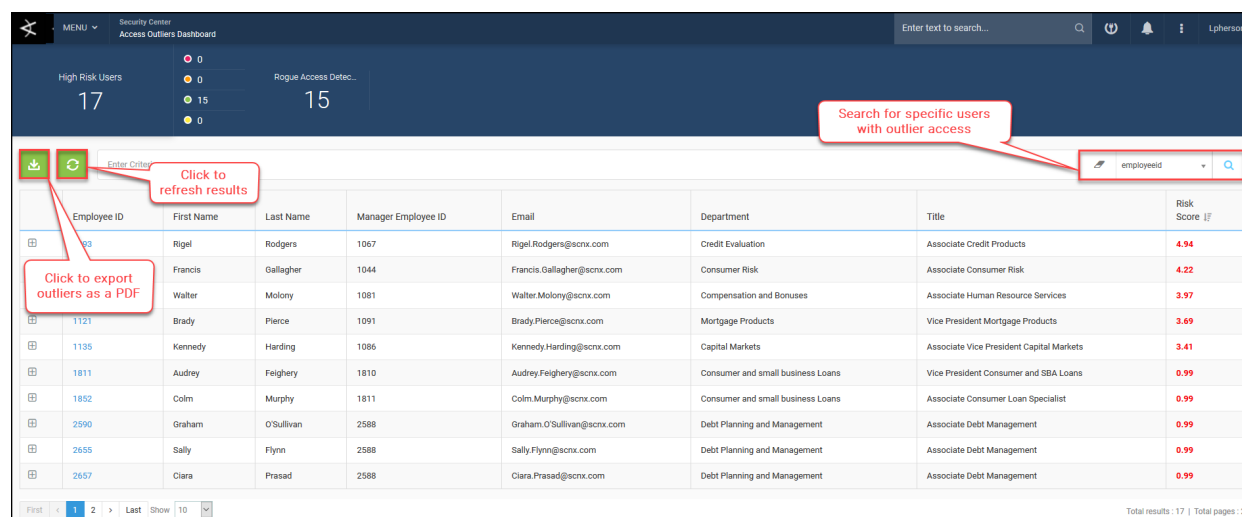
Access Outliers Dashboard

The Access Outliers Dashboard displays the results of Access Outlier jobs. See the ArcSight UBAAdministration Guide for information about how to schedule an Access Outlier job.

To access the Access Outliers Dashboard, navigate to **Menu > Security Center > Access Outlier Dashboard**.



You can perform the following actions from this screen:



High Risk Users

Click **High Risk Users** to view high risk users by risk score.

High Risk Users

42

0

0

141

0

Rogue Access Detec...

141

Enter Criteria

employeeid

	Employee ID	First Name	Last Name	Manager Employee ID	Email	Department	Title	Risk Score <i>if</i>
<div></div>	1993	Walter	Molony	1081	Walter.Molony@scnx.com	Compensation and Bonuses	Associate Human Resource Services	5.46
<div></div>	1852	Colm	Murphy	1811	Colm.Murphy@scnx.com	Consumer and small business Loans	Associate Consumer Loan Specialist	4.98
<div></div>	1093	Rigel	Rodgers	1067	Rigel.Rodgers@scnx.com	Credit Evaluation	Associate Credit Products	4.94
<div></div>	2571	Francis	Gallagher	1044	Francis.Gallagher@scnx.com	Consumer Risk	Associate Consumer Risk	4.78
<div></div>	1811	Audrey	Feighery	1810	Audrey.Feighery@scnx.com	Consumer and small business Loans	Vice President Consumer and SBA Loans	4.0
<div></div>	2442	Kevin	Trimble	1078	Kevin.Trimble@scnx.com	Distressed	Managing Dir. Distressed Assets	3.93
<div></div>	2590	Graham	O'Sullivan	2588	Graham.O'Sullivan@scnx.com	Debt Planning and Management	Associate Debt Management	3.75
<div></div>	1121	Brady	Pierce	1091	Brady.Pierce@scnx.com	Mortgage Products	Vice President Mortgage Products	3.69
<div></div>	2290	Ursula	Maloney	2287	Ursula.Maloney@scnx.com	Credit	Associate Vice President Credit Market	3.68
<div></div>	2332	Darragh	Dyball	2287	Darragh.Dyball@scnx.com	Credit	Associate Vice President Credit Market	3.68

First

<

1

2

3

4

5

>

Last

Show

10

Total results : 42 | Total pages : 5

Click an Employee ID value to view Risk Details for the user. See [Views](#) for more information about Users.

Francis Gallagher [2571] Risk Details ×

General Details
Organizations
Peer Groups
Monitor Access
Monitor Activities
Behavior Profile

employeeid = 2571
1,000 events fetched out of matched 26,242 events
ALL TIMES SHOWN ARE IN CST/CDT

Show Fields Reports

SAT, 30 SEP 2017 @ 06:10:57 AM resourcegroupname: Citrix VPN

accountname = FRANCIS GALLAGHER, bytesin = 0, bytesout = 0, eventoutcome = Success, transactionstring1 = CMD_EXECUTED, applicationprotocol = default GUI, sourceport = 0, devicehostname = 10.0.1.2, resourcegroupname = Citrix VPN, rg_functionality = VPN, rg_vendor = Citrix_VPN_SK, resource = Citrix VPN, destinationaddress = 10.14.117, destinationport = 0, customstring1 = show vpn vsrver vpn.scnx.com

companycode = CSR, costcentername = ISALCCC11, country = USA, department = Consumer Risk, division = Corporate Risk, employeeid = 2571, employeetype = FT, employeetypedescription = FullTime, first name = Francis, hiredate = 08/08/2009 00:00:00.000, jobcode = R1, lanid = FG2571, lastname = Gallagher, location = Chicago, manageremployeeid = 1044, status = 1, statusdescription = Active, title = Associate Consumer Risk, workemail = Francis.Gallagher@scnx.com

approveremployeeid = 2835, usercriticality = Low, companynumber = CSRS, province = CA, street = 300 LAKESIDE DR, maskedfields = u_firstname,u_lastname, regtempin = Regular, hierarchy = 4, costcentercode = ISALCCC11, networkid = FGallagher, zipcode = 94612-3596, enabledate = 10/20/2017 14:09:47.000, managerlastname = Lewis, orgunitnumber = 11, city = OAKLAND, lastsyncntime = 10/20/2017 15:19:06.000, customfield15 = Nora_Lewis_1044, managerfirstname = Nora, fulltimeparttimein = FullTime, userriskscore = 0.01, usertimezoneoffset = CST











Click + to view details and take actions on users with High Risk Access. Click - to collapse details.

Enter Criteria

employeeid

	Employee ID	First Name	Last Name	Manager Employee ID	Email	Department	Title	Risk Score <div></div>
<div></div>	1093	Rigel	Rodgers	1067	Rigel.Rodgers@scnx.com	Credit Evaluation	Associate Credit Products	4.94
<div></div>								
	Detected Date		Threat Name		Policy Name		Account Name	Risk Score
	2017-10-24 15:55:28.0		Rogue Access Detected		High Risk Access		All Accounts	4.94
<div></div>								
<div></div>	2571	Francis	Gallagher	1044	Francis.Gallagher@scnx.com	Consumer Risk	Associate Consumer Risk	4.22
<div></div>	1993	Walter	Molony	1081	Walter.Molony@scnx.com	Compensation and Bonuses	Associate Human Resource Services	3.97

Click **High Risk Access** to view the user's high risk accounts.

	Resource	Account	Access Value	Risk Score (F)	Account Last Used	
	Access Data	 RR1093	memberOf: CN=CRM_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com	0.99	N/A	<div> <div>Select Action</div> <div> <div>Select Action</div> <div>Certify for all</div> <div>Revoke for all</div> <div>Date Extension for all</div> </div> </div>
	Access Data	 RR1093	memberOf: CN=BankSoft_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com	0.99	N/A	
	Access Data	 RR1093	memberOf: CN=HR_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com	0.99	N/A	<div> <div>-Select-</div> </div>
	Access Data	 RR1093	memberOf: CN=Portal_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com	0.99	N/A	<div> <div>-Select-</div> </div>
	Access Data	 RR1093	memberOf: CN=PAY_User,OU=Applications,OU=Corporate,DC=scnx,DC=com	0.99	N/A	<div> <div>-Select-</div> </div>

First 1 Last Show 10

Total results: 5 | Total pages: 1

Use **Select Action** dropdown to take the following actions on ALL high risk accounts for this user:

- **Certify for all:** Certifies access for all accounts.
- **Revoke for all:** Revokes access for all accounts.
- **Date Extension for all:** Extends the date access should be granted for all accounts.

Enter exception time frame to confirm the action.

Confirm Action

Select exception time frame

From

To

Close

Submit

Click + to view details about the high risk access account.

High Risk Access Policy Details						
	Resource	Account	Access Value	Risk Score ¹	Account Last Used	Select Action
	Access Data	RR1093	memberOf: CN=CRM_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com	0.99	N/A	
	Access Data	RR1093	memberOf: CN=BankSoft_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com	0.99	N/A	
	Access Data	RR1093	memberOf: CN=HR_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com	0.99	N/A	
CN=HR_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com is identified as rogue access for User because: <div> <div>1 out of 19 users in Peer Group Associate Credit Products [Type: Title] have access to CN=HR_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com .</div> <div>1 out of 20 users in Peer Group Credit Products [Type: Division] have access to CN=HR_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com .</div> <div>1 out of 10 users in Peer Group FORT SMITH [Type: Location] have access to CN=HR_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com .</div> <div>1 out of 19 users in Peer Group Leigh_Vazquez_1067 [Type: Manager] have access to CN=HR_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com .</div> <div>More Details</div> </div>						

Click **X out of X** value to view Outlier Details.

Outlier Details								
Users With Access		Users Without Access						
Employee ID	First Name	Last Name	Manager Employee ID	Email	Department	Title	Account Name	Resource Name
1093	Rigel	Rodgers	1067	Rigel.Rodgers@scnx.com	Credit Evaluation	Associate Credit Products	RR1093	Access Data
<div> <div>First</div> <div>< 1 > Last</div> <div>Show 10</div> </div> <div>Total results : 1 Total pages : 1</div>								

Click **More Details** to view Peer Name for the account. Click Users with Access value to view Outlier Details. Click **Less Details** to collapse details.

Access Data

RR1093

memberOf: CN=HR_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com

0.99

N/A

Select

CN=HR_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com is identified as rogue access for User because:

1 out of 19 users in Peer Group Associate Credit Products [Type: Title] have access to CN=HR_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com .

1 out of 20 users in Peer Group Credit Products [Type: Division] have access to CN=HR_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com .

1 out of 10 users in Peer Group FORT SMITH [Type: Location] have access to CN=HR_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com .

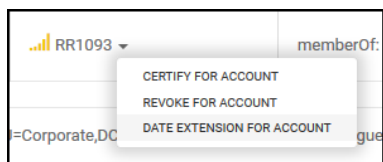
1 out of 19 users in Peer Group Leigh_Vazquez_1067 [Type: Manager] have access to CN=HR_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com .

Less Details

Peer Name (Member Count)	Type	Peer Cohesivenss	Access Outlier Probability	Users With Access
Associate Credit Products (19)	Title	0.975	1	1 / 19
Credit Products (20)	Division	0.975	1	1 / 20
FORT SMITH (10)	Location	0.975	1	1 / 10
Leigh_Vazquez_1067 (19)	Manager	0.975	1	1 / 19

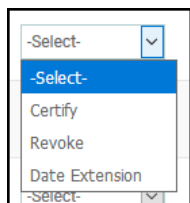
You can take the following actions for each account:

Click arrow beside account to take the following actions on the account:



OR

Use dropdown to take the following actions on the account:



Certify: Certifies access for selected account.

Revoke: Revokes access for selected account.

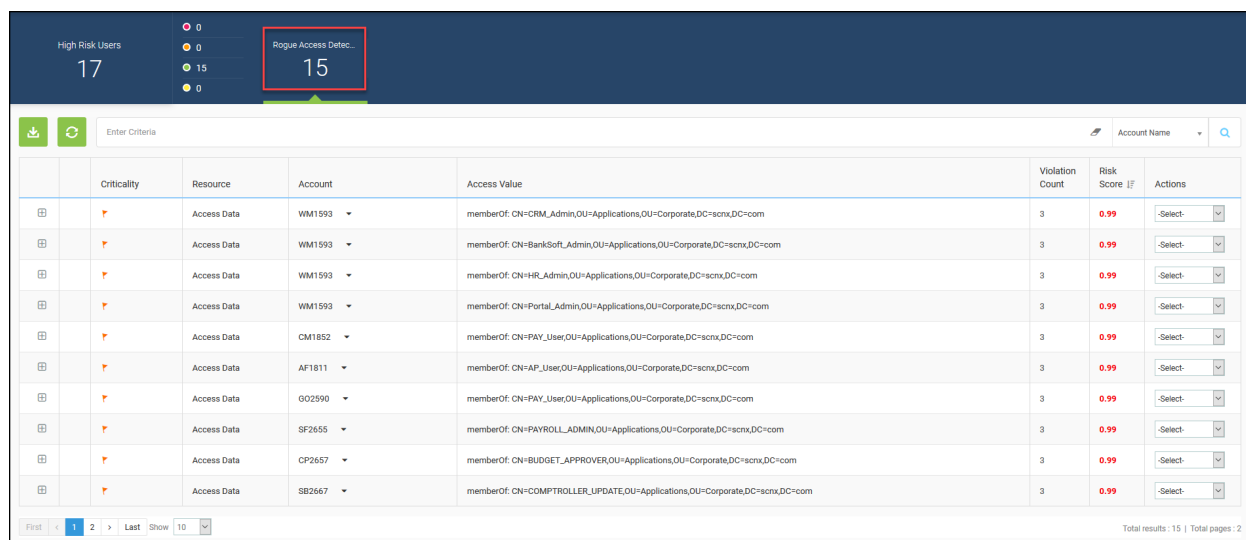
Date Extension: Extends the date access should be granted for selected account.

Enter exception time frame to confirm the action.

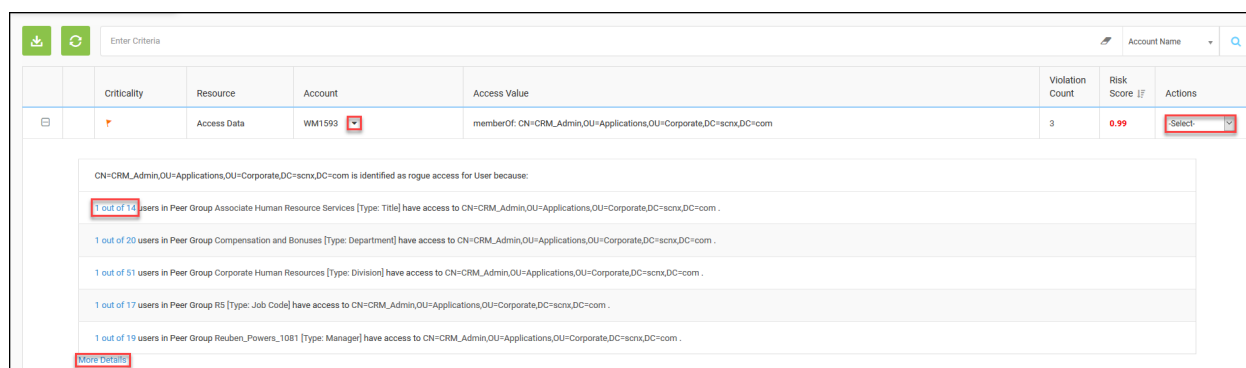
A screenshot of a 'Confirm Action' dialog box. The dialog has a title bar with a close button (X). Inside, there is a large empty text area for notes. Below this, there is a section titled 'Select exception time frame' with 'From' and 'To' input fields. At the bottom, there are 'Close' and 'Submit' buttons.

Rogue Access Detected

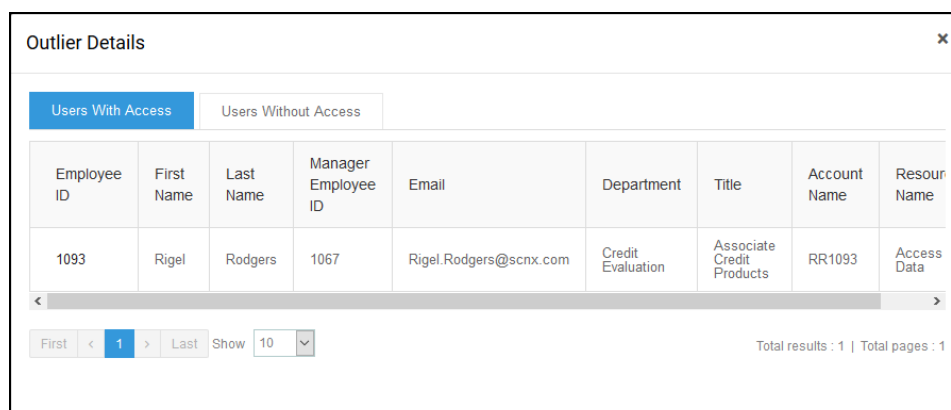
Click **Rogue Access Detected** to view accounts with Rogue Access.



Click + to view details about the rogue access account.



Click **X out of X** value to view Outlier Details.

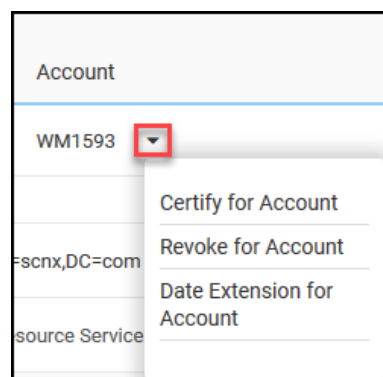


Click **More Details** to view Peer Name for the account. Click Users with Access value to view Outlier Details. Click **Less Details** to collapse details.

	Criticality	Resource	Account	Access Value	Violation Count	Risk Score	Actions
		Access Data	WM1593	memberOf: CN=CRM_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com	3	0.99	
CN=CRM_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com is identified as rogue access for User because:							
1 out of 14 users in Peer Group Associate Human Resource Services [Type: Title] have access to CN=CRM_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com .							
1 out of 20 users in Peer Group Compensation and Bonuses [Type: Department] have access to CN=CRM_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com .							
1 out of 51 users in Peer Group Corporate Human Resources [Type: Division] have access to CN=CRM_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com .							
1 out of 17 users in Peer Group RS [Type: Job Code] have access to CN=CRM_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com .							
1 out of 19 users in Peer Group Reuben_Powers_1081 [Type: Manager] have access to CN=CRM_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com .							
Less Details							
Peer Name (Member Count)		Type	Peer Cohesivness	Access Outlier Probability	Users With Access		
Associate Human Resource Services (14)		Title	0.986	1	1 / 14		
Compensation and Bonuses (20)		Department	0.986	1	1 / 20		
Corporate Human Resources (51)		Division	0.986	1	1 / 51		
RS (17)		Job Code	0.986	1	1 / 17		
Reuben_Powers_1081 (19)		Manager	0.986	1	1 / 19		

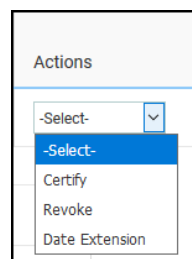
You can take the following actions for each rogue access account:

Click arrow beside account to take the following actions on the account:



OR

Use Actions dropdown to take the following actions on the account:



Certify: Certifies access for selected account.

Revoke: Revokes access for selected account.

Date Extension: Extends the date access should be granted for selected account.

Enter exception time frame to confirm the action.

Confirm Action

Select exception time frame

FromTo

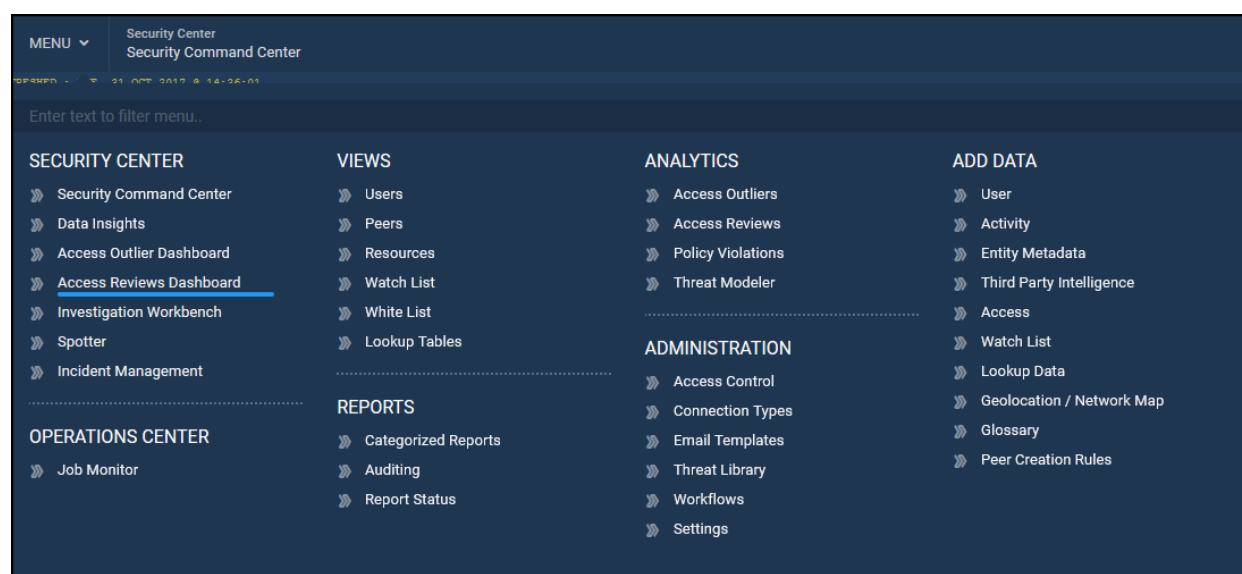
Close

Submit

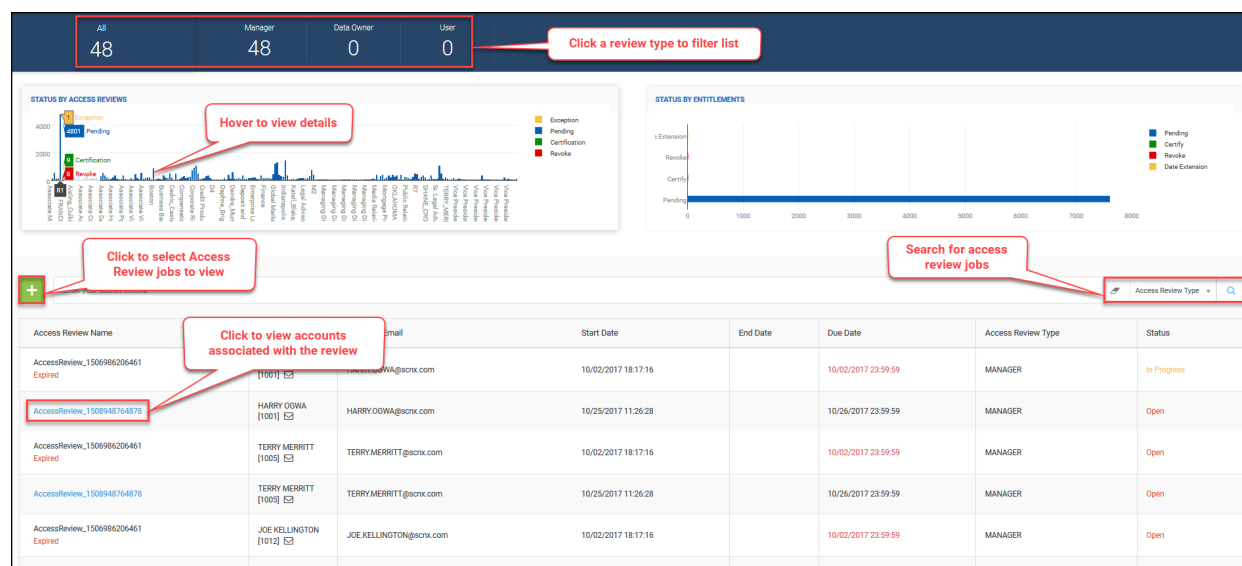
Access Reviews Dashboard

The Access Reviews Dashboard displays the results of Access Review jobs. See the ArcSight UBAAdministration Guide for information about how to schedule an Access Review.

To access the Access Outliers Dashboard, navigate to **Menu > Security Center > Access Reviews Dashboard**.



You can perform the following actions from this screen:



- Click to filter list by the following access review types:
 - Manager
 - Data Owner
 - User
- Hover over data points to view details and statistics about the data point.
- Click **+** to select Access Review jobs to view.
- Search for Access Review jobs
- Click an Access Review job to view users associated with the review.

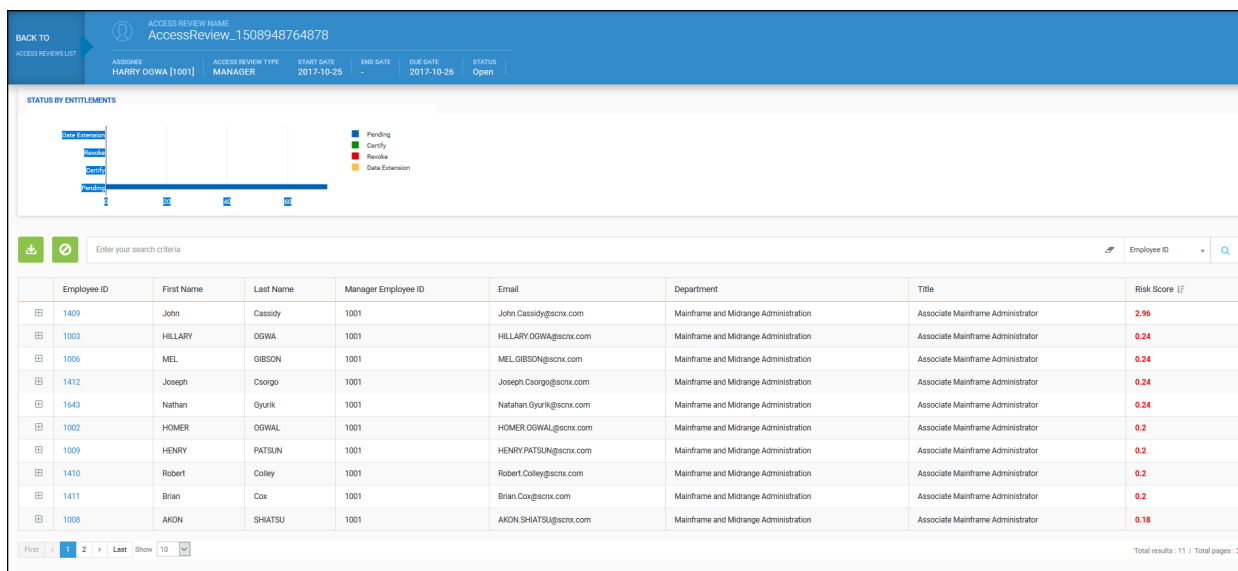


Note: Unless the user is an admin, when the user performing the review is logged on, they will only see the review(s) for which they are responsible.

Access Review Details

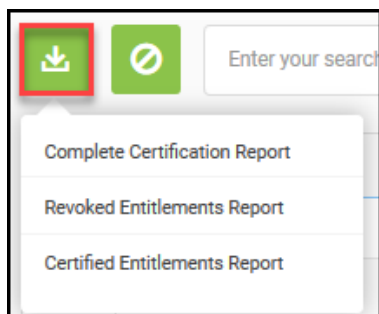
From the Access Review details screen, you can perform the following actions:

Click **Back to Access Reviews List** to return to the previous screen.



Enter query to search for a specific user.

Click download icon to download the following reports as PDF:

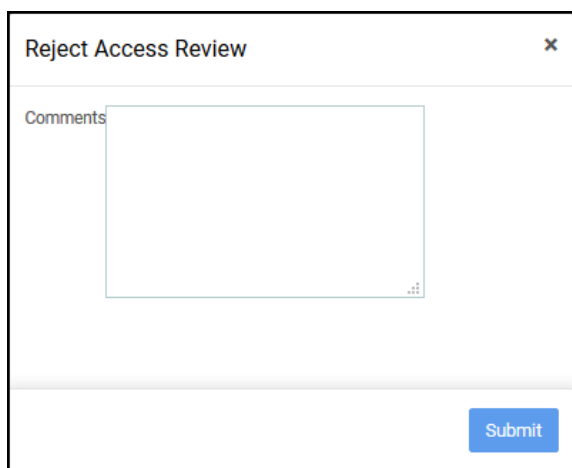


- Complete Certification Report
- Revoked Entitlements Report
- Certified Entitlements Report

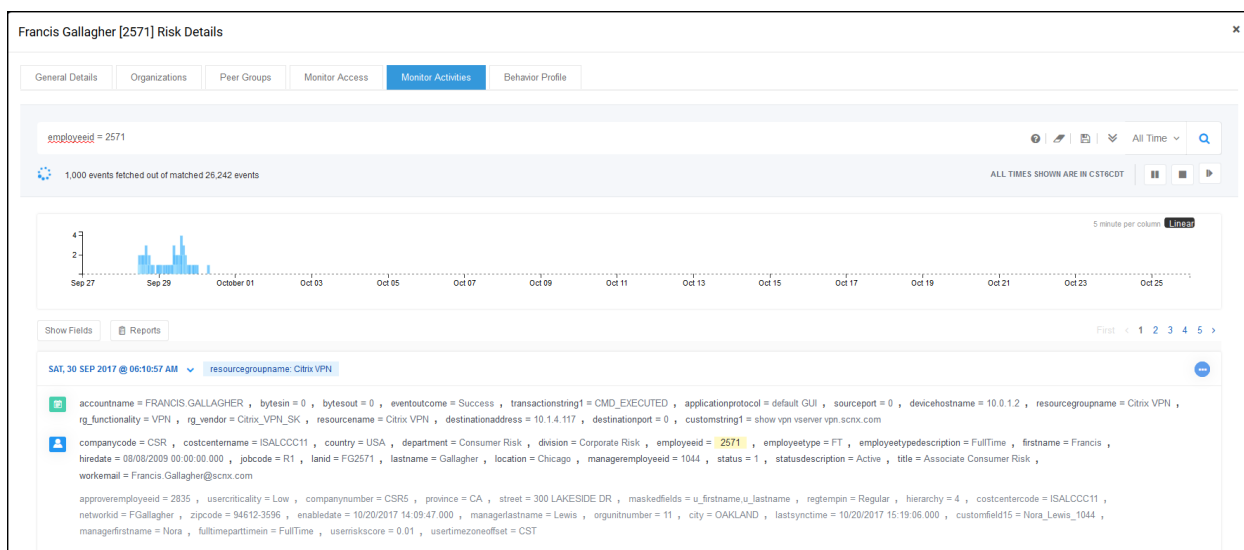
Click Reject icon to reject the Access Review.



Enter comments in the dialogue box and click **Submit** to reject the Access Review:



Click an Employee ID to view Risk Details about the user. See [Views](#) for more information about Users.



Click + to view details and take actions on user accounts. Click - to collapse details.

Employee ID	First Name	Last Name	Manager Employee ID	Email	Department	Title	Risk Score
1059	AARON	SCOTT	1045	AARON.SCOTT@scnx.com	Compliance Risk	Associate Compliance Risk	4.49
1051	HARRY	YOUNG	1045	HARRY.YOUNG@scnx.com	Compliance Risk	Associate Compliance Risk	3.06

Resource	Account	Access Value	Risk Score	Account Last Used	Select Action
Access Data	HY1051	memberOf: CN=POS_User,OU=Applications,OU=Corporate,DC=scnx,DC=com	0.00	N/A	Select-
Access Data	HY1051	memberOf: CN=Remote Desktop Users,CN=BuiltIn,DC=scnx,DC=com	0.00	N/A	Select-
Access Data	HY1051	memberOf: CN=POS_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com	0.15	N/A	Select-
Access Data	HY1051	memberOf: CN=AP_User,OU=Applications,OU=Corporate,DC=scnx,DC=com	0.24	N/A	Select-
Access Data	HY1051	memberOf: CN=CRM_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com	0.28	N/A	Select-
Access Data	HY1051	memberOf: CN=BankSoft_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com	0.28	N/A	Select-
Access Data	HY1051	memberOf: CN=HR_Admin,OU=Applications,OU=Corporate,DC=scnx,DC=com	0.28	N/A	Select-

Use **Select Action** dropdown to take the following actions on ALL accounts for this user:

- **Certify for all:** Certifies access for all accounts.
 - **Revoke for all:** Revokes access for all accounts.
 - **Date Extension for all:** Extends the date access should be granted for all accounts.
- Enter exception time frame to confirm the action.

Confirm Action

Select exception time frame





From

To

Close

Submit

Click **+** to view details about an access account.

	1051	HARRY	YOUNG	1045	HARRY.YOUNG@scrx.com	Compliance Risk	Associate Compliance Risk	3.06
	Resource [1]	Account	Access Value			Risk Score	Account Last Used	Select Action
	Access Data	 HY1051	memberOf: CN=POS_User,OU=Applications,OU=Corporate,DC=scrx,DC=com			0.00	N/A	Select
<div>CN=POS_User,OU=Applications,OU=Corporate,DC=scrx,DC=com is identified as rogue access for User because:<ul style="list-style-type: none">10 out of 13 users in Peer Group Associate Compliance Risk [Type: Title] have access to CN=POS_User,OU=Applications,OU=Corporate,DC=scrx,DC=com.11 out of 11 users in Peer Group Compliance Risk [Type: Department] have access to CN=POS_User,OU=Applications,OU=Corporate,DC=scrx,DC=com.66 out of 66 users in Peer Group Corporate Risk [Type: Division] have access to CN=POS_User,OU=Applications,OU=Corporate,DC=scrx,DC=com.10 out of 10 users in Peer Group Fahad_Walker_1045 [Type: Manager] have access to CN=POS_User,OU=Applications,OU=Corporate,DC=scrx,DC=com.10 out of 10 users in Peer Group R2 [Type: Job Code] have access to CN=POS_User,OU=Applications,OU=Corporate,DC=scrx,DC=com.20 out of 20 users in Peer Group SAN FRANCISCO [Type: Location] have access to CN=POS_User,OU=Applications,OU=Corporate,DC=scrx,DC=com.</div> <div>More Details</div>								

Click **X out of X** value to view Outlier Details for the account.

Outlier Details	
<div> <div>Users With Access</div> <div>Users Without Access</div> </div>	
Account Name	Resource Name
BL1047	Access Data
BH1049	Access Data
HY1051	Access Data
VK1053	Access Data
PK1055	Access Data
JL1057	Access Data
AS1059	Access Data
AW1061	Access Data
JB1407	Access Data
SM1616	Access Data
<div> <div>First</div> <div><</div> <div>1</div> <div>></div> <div>Last</div> <div>Show</div> <div>All</div> <div>▼</div> </div> <div>Total results : 10 Total pages : 1</div>	

Click **More Details** to view Peer Name for the account. Click Users with Access value to view Outlier Details. Click **Less Details** to collapse details.

Access Data	HY1051	memberOf: CN=POS_User,OU=Applications,OU=Corporate,DC=scnx,DC=com	0.00	N/A	Select
CN=POS_User,OU=Applications,OU=Corporate,DC=scnx,DC=com is identified as rogue access for User because:					
10 out of 10 users in Peer Group Associate Compliance Risk [Type: Title] have access to CN=POS_User,OU=Applications,OU=Corporate,DC=scnx,DC=com.					
11 out of 11 users in Peer Group Compliance Risk [Type: Department] have access to CN=POS_User,OU=Applications,OU=Corporate,DC=scnx,DC=com.					
66 out of 66 users in Peer Group Corporate Risk [Type: Division] have access to CN=POS_User,OU=Applications,OU=Corporate,DC=scnx,DC=com.					
10 out of 10 users in Peer Group Fahad_Walker_1045 [Type: Manager] have access to CN=POS_User,OU=Applications,OU=Corporate,DC=scnx,DC=com.					
10 out of 10 users in Peer Group R2 [Type: Job Code] have access to CN=POS_User,OU=Applications,OU=Corporate,DC=scnx,DC=com.					
20 out of 20 users in Peer Group SAN FRANCISCO [Type: Location] have access to CN=POS_User,OU=Applications,OU=Corporate,DC=scnx,DC=com.					
Less Details					
Peer Name (Member Count)	Type	Peer Cohesivness	Access Outlier Probability	Users With Access	
Associate Compliance Risk (10)	Title	0.999	0	10 / 10	
Compliance Risk (11)	Department	0.999	0	11 / 11	
Corporate Risk (66)	Division	0.999	0	66 / 66	
Fahad_Walker_1045 (10)	Manager	0.999	0	10 / 10	
R2 (10)	Job Code	0.999	0	10 / 10	
SAN FRANCISCO (20)	Location	0.999	0	20 / 20	

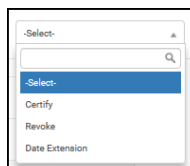
You can take the following actions for each account:

Click arrow beside account to take the following actions on the account:

Account	Access
<div> <div>HY1051</div> <div>memberOf: CN=Corporate,DC=com</div> </div>	
<div> <div>CERTIFY FOR ACCOUNT</div> <div>REVOKE FOR ACCOUNT</div> <div>DATE EXTENSION FOR ACCOUNT</div> </div>	

OR

Use dropdown to take the following actions on the account:



Certify: Certifies access for selected account.

Revoke: Revokes access for selected account.

Date Extension: Extends the date access should be granted for selected account.

Enter exception time frame to confirm the action.

 A screenshot of a "Confirm Action" dialog box. The dialog has a title bar with a close button (X). Inside, there is a large empty rectangular area for a screenshot or image. Below this area, the text "Select exception time frame" is displayed. Underneath, there are two input fields labeled "From" and "To". At the bottom right, there are two buttons: "Close" and "Submit".

The Access Review Dashboard will reflect the actions taken and display the status of individual reviews.

Past Due Access Reviews

When an Access Review is past due, the status shows Expired and you will be unable to take any actions on the review. You must rerun or create a new Access Review Job from **Menu > Analytics > Access Reviews**.

Access Review Name	Assignee	Assignee Email	Start Date	End Date	Due Date	Access Review Type	Status
AccessReview_1506986206461 Expired	HARRY OGWA [1001]	HARRY.OGWA@scnx.com	10/02/2017 18:17:16		10/02/2017 23:59:59	MANAGER	In Progress
AccessReview_1508948764878	HARRY OGWA [1001]	HARRY.OGWA@scnx.com	10/25/2017 11:26:28		10/26/2017 23:59:59	MANAGER	In Progress
AccessReview_1506986206461 Expired	TERRY MERRITT [1005]	TERRY.MERRITT@scnx.com	10/02/2017 18:17:16		10/02/2017 23:59:59	MANAGER	Open
AccessReview_1508948764878	TERRY MERRITT [1005]	TERRY.MERRITT@scnx.com	10/25/2017 11:26:28		10/26/2017 23:59:59	MANAGER	Open
AccessReview_1506986206461 Expired	JOE KELLINGTON [1012]	JOE.KELLINGTON@scnx.com	10/02/2017 18:17:16		10/02/2017 23:59:59	MANAGER	Open
AccessReview_1508948764878	JOE KELLINGTON [1012]	JOE.KELLINGTON@scnx.com	10/25/2017 11:26:28		10/26/2017 23:59:59	MANAGER	Open

Investigation Workbench

The Investigation Workbench enables security analysts to investigate and manage high-risk entities in different dimensions. It provides visualization of connections between users, IP addresses, systems, activities and other relevant data involved in an incident.

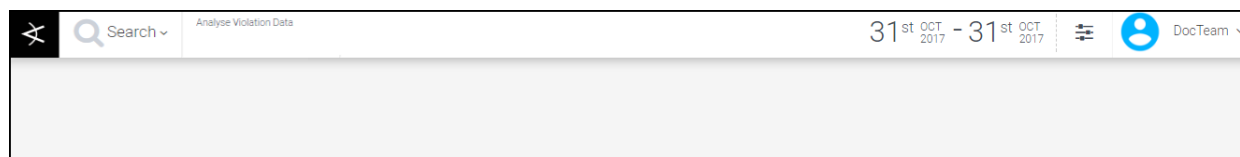
Workbench Overview

The Investigation Workbench provides a quick visualization of multiple data sources and reports. You have the ability to drill down into each and every incident performed by a user.







Use the Investigation Workbench to perform root-cause analysis of a particular violation or breach, providing analysts the ability to view anomalous activities in a chronological order. In the Investigation Workbench, analysts can pivot around any entity. To pivot across various objects, for example, IP address, systems or peer groups, click an entity within the dashboard and from the list of options, select the activity or information you wish to view. You can save and share the investigation results with other analysts.

Launching the Investigation Workbench

To navigate to the Investigation Workbench, click **Menu > Security Center > Investigation Workbench**. The following screen appears.



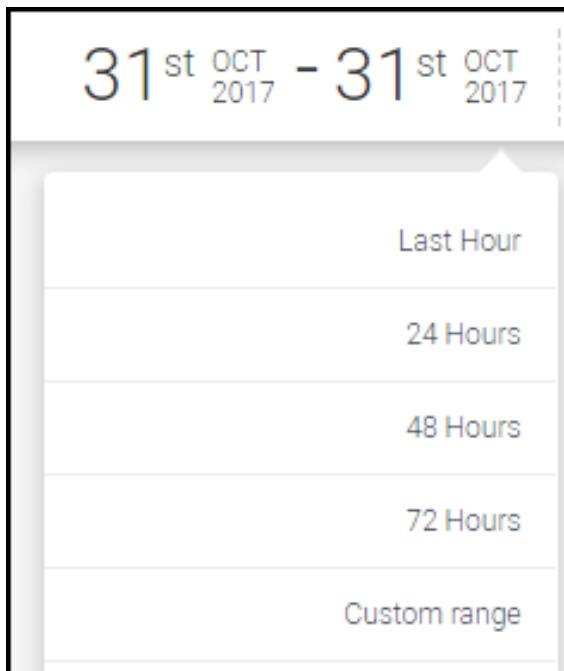
The top navigation bar in Investigation Workbench provides filtering options as listed in the table:

Tool bar option	Function
Analyze Violation Data	<p>NO: By default, the application analyzes all event data.</p> <p>YES: The application limits its analysis to violation data only.</p>
	<p>Click the  dropdown to access this option. Clicking this icon clears all current information from the Investigation Workbench screen and begins a new investigation.</p>
	<p>Click the icon  dropdown to access this option. Click this icon to reset the screen to its default position if you have used the Pan/Zoom feature.</p>
	<p>Click the icon  dropdown to access this option. Click this icon to lock the screen so that you can use your mouse to pan the screen (left-click and drag), and scroll in or out using the mouse scroll wheel.</p>
Search	Use the dropdown to search for an entity.
Date Filter	Use the date filter to choose an hourly range or specify a custom date range.

Simple Search

To do a quick investigation for events in the past hour or for a range, follow these steps:

1. Select the date. By default, the Investigation Workbench displays the current date. To select a different date range, click the date range dropdown menu in the top right area of the screen. Select from the default date ranges, or click **Custom Range** to enter a custom date range.



2. Use the Search dropdown to perform a simple search using a single attribute:

A screenshot of a search form. It contains three dropdown menus: 'Select entity' with 'User' selected, 'Select attributes' with 'employeeid' selected, and 'Enter search text' which is an empty text input field. Below these is a blue 'Search' button and a link that says 'Go to advanced search'.

- Select an entity from the **Select Entity** dropdown, for example, User.
- Select an attribute from the **Select Attribute** dropdown, for example, employeeid. The attributes shown are based on the entity you selected.
- Enter the specific search criteria. For example, 1002. The search string allows you to confine your search to employee id = 1002.
- Click **Search**.

The search results appear as shown in the Investigation Workbench. The search results show all the users in ArcSight UBA when **Analyze Violation Data** is disabled.

Search

Analyze Violation Data

NO

USERS: 666

Showing 1 to 200

06th NOV 2017

-

06th NOV 2017

DocTeam

<div><div></div><div>HARRY ODWA [1001] Vice President Mainframe 117.31</div></div>	<div><div></div><div>HOMER ODWA [1002] Associate Mainframe Admin.</div></div>	<div><div></div><div>HILLARY ODWA [1003] Associate Mainframe Admin.</div></div>	<div><div></div><div>TERRY MERRITT [1004] Managing Dir. Consumer R.</div></div>	<div><div></div><div>TERRY MERRITT [1005] Managing Dir. Compliance</div></div>	<div><div></div><div>MEL GIBSON [1006] Associate Mainframe Admin.</div></div>	<div><div></div><div>RAJESH RAO [1007] Associate Mainframe Admin.</div></div>
<div><div></div><div>AKON SHATSU [1008] Associate Mainframe Admin.</div></div>	<div><div></div><div>HENRY PATSUN [1009] Associate Mainframe Admin.</div></div>	<div><div></div><div>TONY KULSIP [1010] Associate Mainframe Admin.</div></div>	<div><div></div><div>JOE KELLINGTON [1012] Managing Dir. Global Tech.</div></div>	<div><div></div><div>ROBERT WELLINGTON [1013] Vice President Data Serv.</div></div>	<div><div></div><div>JOHN KELLER [1014] Associate Data Services 0.2</div></div>	<div><div></div><div>KEVIN MILTON [1015] Associate Data Services 0.2</div></div>
<div><div></div><div>LARRY ELLISON [1016] Associate Data Services 0.2</div></div>	<div><div></div><div>SEAN CONNERY [1017] Associate Data Services 0.2</div></div>	<div><div></div><div>GILBERT FULLER [1018] Associate Data Services 0.2</div></div>	<div><div></div><div>JOSE MENDOZA [1019] Associate Data Services 0.2</div></div>	<div><div></div><div>JUAN BERRINGER [1020] Associate Data Services 0.2</div></div>	<div><div></div><div>LEE PERRY [1021] Associate Data Services 0.2</div></div>	<div><div></div><div>NEIL DAWSON [1022] Associate Data Services 0.2</div></div>
<div><div></div><div>MICHAEL BLACKWATER [1023] Associate Data Services 0.2</div></div>	<div><div></div><div>KELLY REED [1024] Associate Data Services 0.2</div></div>	<div><div></div><div>TED THOMSON [1025] Chief Executive Officer</div></div>	<div><div></div><div>MELVIN MOORE [1026] Associate Data Services 0.2</div></div>	<div><div></div><div>ALEX TAYLOR [1027] Associate Database Admin.</div></div>	<div><div></div><div>TOM ANDERSON [1028] Associate Database Admin.</div></div>	<div><div></div><div>TERRY THOMAS [1029] Associate Database Admin.</div></div>

Enable **Analyze Violation Data** to view only those users who have a violation. For example a policy violation.

Search

Analyze Violation Data

YES

USERS: 119

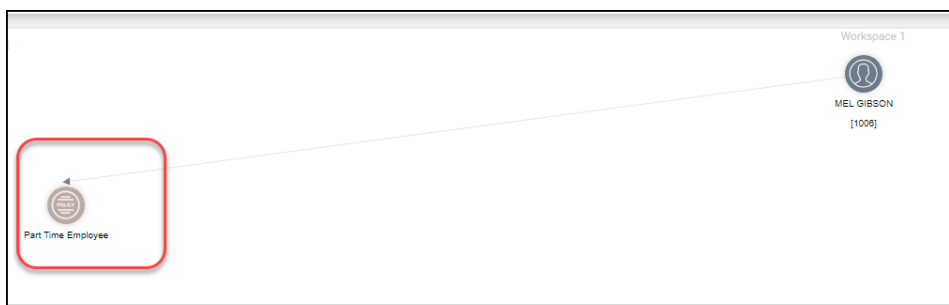
Showing 1 to 119

06th NOV 2017 - 06th NOV 2017

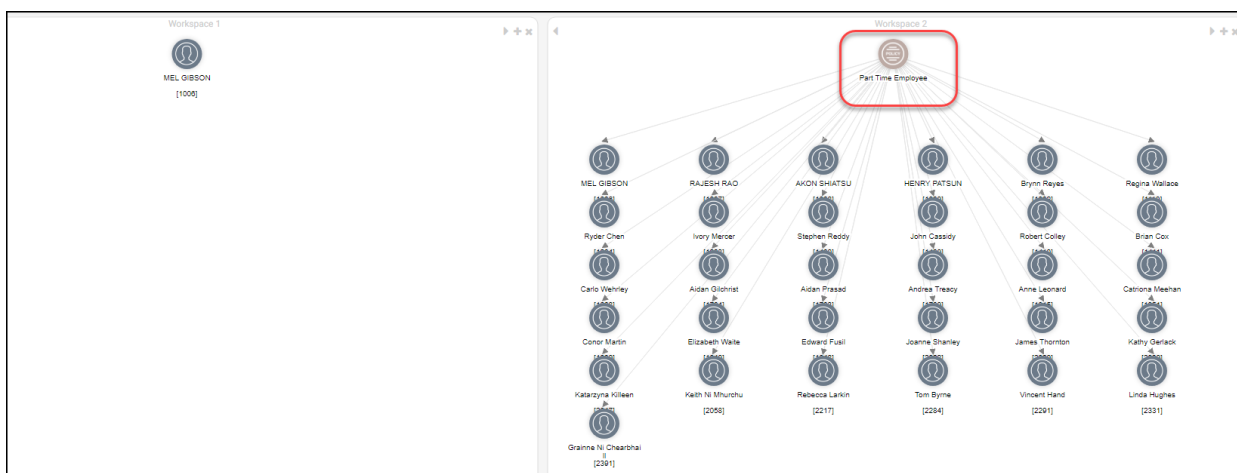
DocTeam

<div><div></div><div>HARRY ODWA [1001] Vice President Mainframe ... 0.01</div></div>	<div><div></div><div>MEL GIBSON [1006] Associate Mainframe Admin...</div></div>	<div><div></div><div>RAJESH RAO [1007] Associate Mainframe Admin...</div></div>	<div><div></div><div>AKON SHATSU [1008] Associate Mainframe Admin...</div></div>	<div><div></div><div>HENRY PATSUN [1009] Associate Mainframe Admin...</div></div>	<div><div></div><div>JOHN KELLER [1014] Associate Data Services 0.01</div></div>	<div><div></div><div>KEVIN MILTON [1015] Associate Data Services 0.01</div></div>
<div><div></div><div>LARRY ELLISON [1016] Associate Data Services 0.01</div></div>	<div><div></div><div>SEAN CONNERY [1017] Associate Data Services 0.01</div></div>	<div><div></div><div>GILBERT FULLER [1018] Associate Data Services</div></div>	<div><div></div><div>JOSE MENDOCZA [1019] Associate Data Services</div></div>	<div><div></div><div>JUAN BERRINGER [1020] Associate Data Services 1.19</div></div>	<div><div></div><div>LEE PERRY [1021] Associate Data Services 0.01</div></div>	<div><div></div><div>NEIL DAWSON [1022] Associate Data Services 0.01</div></div>
<div><div></div><div>MICHAEL BLACKWATER [1023] Associate Data Services 1.19</div></div>	<div><div></div><div>KELLY REED [1024] Associate Data Services 0.01</div></div>	<div><div></div><div>MELVIN MOORE [1026] Associate Data Services 0.01</div></div>	<div><div></div><div>ALEX TAYLOR [1027] Associate Database Admin...</div></div>	<div><div></div><div>TOM ANDERSON [1028] Associate Database Admin...</div></div>	<div><div></div><div>TERRY THOMAS [1029] Associate Database Admin...</div></div>	<div><div></div><div>BART WHITE [1040] Associate Database Admin...</div></div>

Click on the collapsed menu icon for any user, and select **View Policies Violated**. All the policies that the user violated show up in the Investigation Workbench that you can investigate further.



The following screen shows an example of the policy that was violated being investigated.



Advanced Search

To perform an advanced search, click **Search**. From the dropdown, click **Go to Advanced Search**. This option enables you to search using filtering conditions. To add additional filters, click +. In the figure shown, the search has to filter all users whose employeeid contains the value 10.

[Back to basic search](#)


Object	Attribute	Condition	Value	Operator	
User ▼	employeeid ▼	Contains ▼	10	And ▼	+ -

[Search](#)

The following figure shows an example of the search results.

TED THOMSON [1025] Chief Executive Officer 0.01	AMAL WOLFE [1068] Managing Dir. Business De.. 0.01	KATELL BLAKE [1097] Vice President Business D.. 0.01	OLIVIA WILLIAMS [1104] Associate Client Relation.. 0.01	✖ Associated Objects Collapse All
DAQUAN PETTY [1076] Managing Dir. Human Resou.. 0.01	REUBEN POWERS [1081] Vice President Human Reso.. 0.01	HAKEEM CAMPOS [1110] Associate Human Resource.. 0.01	GRIFFIN GUTIERREZ [1083] Associate Payroll Process.. 0.01	No Associated Objects
ANIKA CHARLES [1073] Associate Payroll Process.. 0.01	TERRY MERRITT [1005] Managing Dir. Compliance.. 0.01	FAHAD WALKER [1045] Vice President Compliance.. 0.01	BRYAN LEE [1047] Associate Compliance Risk 0.01	
HARRY YOUNG [1051] Associate Compliance Risk 0.01	VEENA KRISHNAMURTY [1053] Associate Compliance Risk 0.01	PRIYA KING [1055] Associate Compliance Risk 0.01	JUAN LOPEZ [1057] Associate Compliance Risk 0.01	

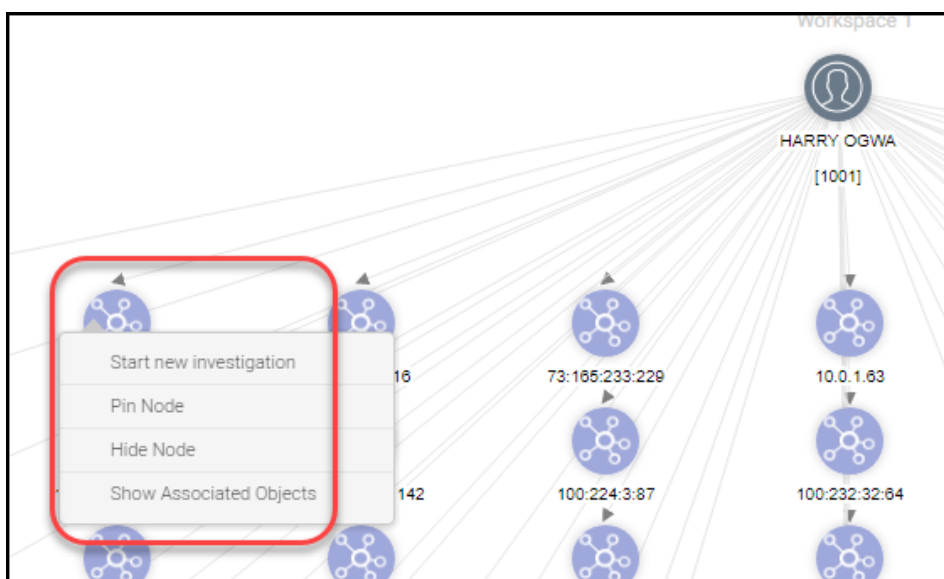
Launching the Investigation Workbench from Other Screens

The Investigation Workbench icon  may appear on other screens. Click the icon to launch investigation into the respective entity. Some screens from where you can launch the Investigation Workbench include:

- The Security Command Center. This is the default overview dashboard that displays the top attackers, threats and violation summary.
- Views for users, peer groups, and resources.

Starting Investigation for Multiple Entities Using Workspaces

- a. Search for an entity using the **Search** dropdown.
- b. Left-click the three-dotted icon to view the associated objects, and pivot on any of them for further investigation. For example, if you selected a user entity, you can view objects associated with it including View Network Address Used.
- c. Click the Network Address Used object. The results appear in a new workspace of the Investigation Workbench as shown.



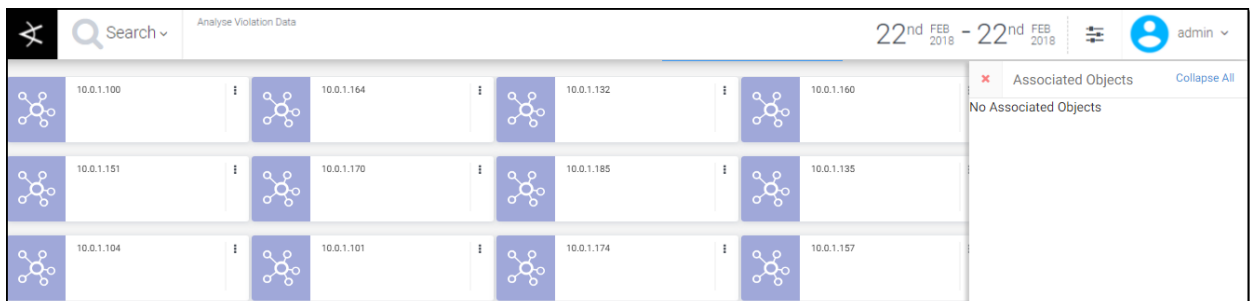
- d. Right-click an IP address to start a new investigation. A new investigation is launched in a second workspace. This feature allows you to investigate multiple entities within the same Investigation Workbench window in their unique workspaces. Scroll to the right as you add more workspaces.

Pivoting Across Objects

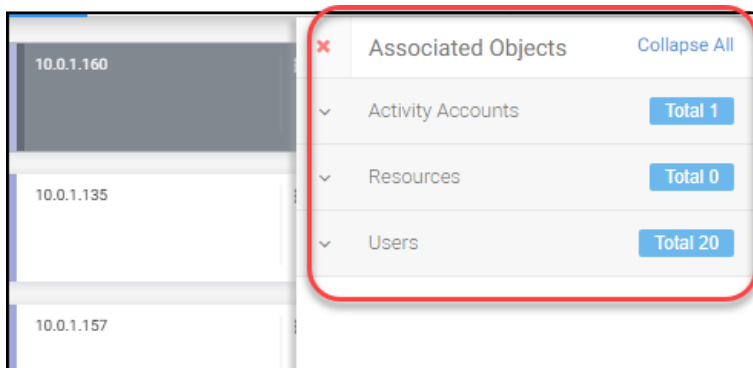
Viewing Objects in Detail

This is another example of how you can view objects associated with an entity. In this example, the entity searched on is the Network Address. When you click a Network address, a summary of the associated objects appears to the right.

- From the Search dropdown, search for Network Address entity. The search results appear with all the network addresses used.



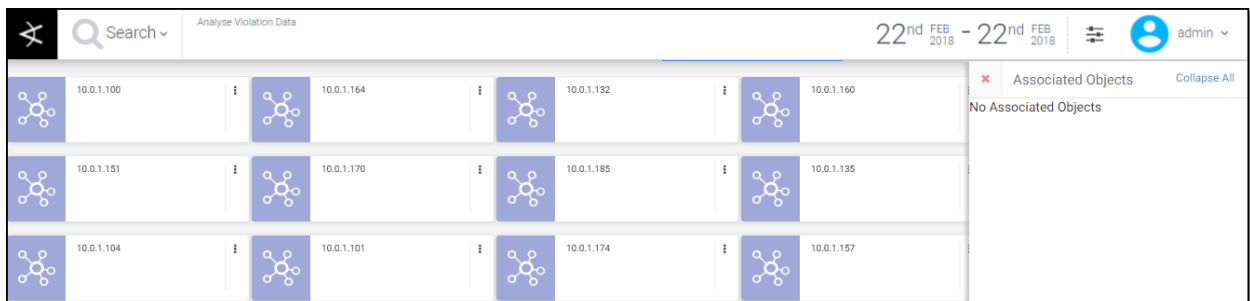
- Right-click an IP address. This launches an **Associated Objects** menu to the right of the screen. You can expand on a menu item to view additional details. Use this menu for a summarization of the associated objects related to the IP address.



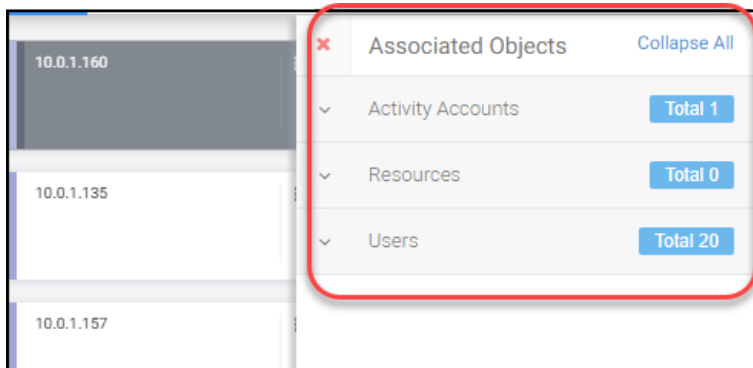
Viewing Objects Summary

This is another example of how you can view objects associated with an entity. In this example, the entity searched on is the Network Address. When you click a Network address, a summary of the associated objects appears to the right.

- a. From the Search dropdown, search for Network Address entity. The search results appear with all the network addresses used.



- b. Right-click an IP address. This launches an **Associated Objects** menu to the right of the screen. You can expand on a menu item to view additional details. Use this menu for a summarization of the associated objects related to the IP address.



Spotter

Spotter is a lightning fast, natural language search engine that uses normalized search syntax and visualization techniques to provide threat hunters the tools they need to investigate current threats and trends, and track advanced persistent threats over long periods of time. Spotter is built on Apache Lucene™, a java-based, high-performance text search engine that provides powerful, efficient, and accurate search capabilities.

Using Spotter

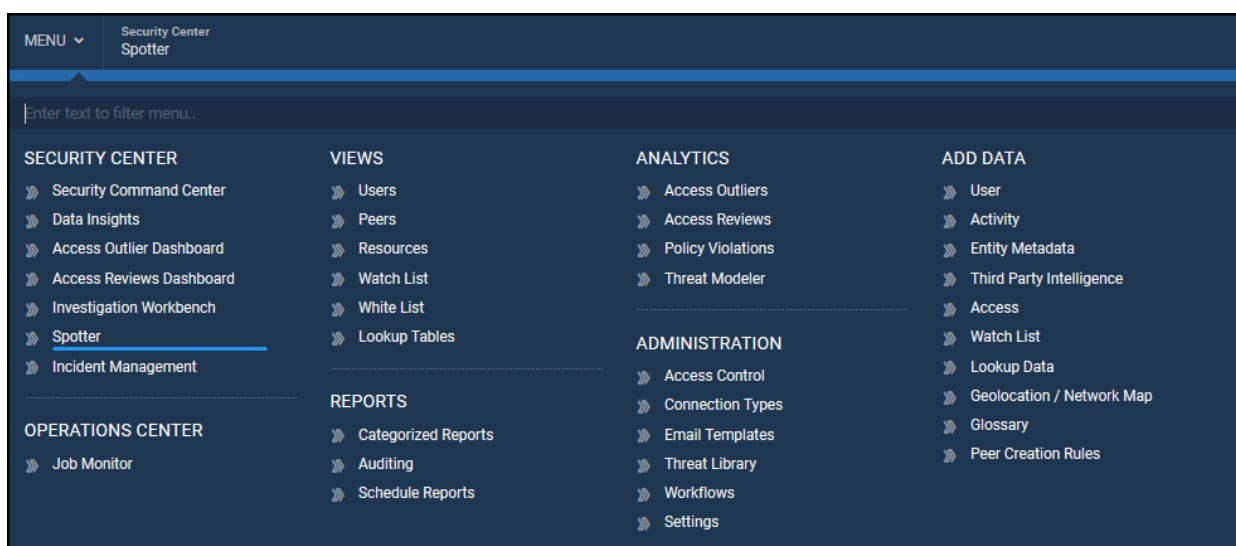
From the Spotter start screen, you can search for and view threats using various search filters. You can specify the report format to display information in tables, as bar charts, bubble charts, and time charts, or view a geographical map.



Note: Click **F2** to redirect to the Spotter start screen from any section of the ArcSight UBA UI.

Getting Started

1. Log in to ArcSight UBA.
2. Navigate to **Menu > Security Center> Spotter**.



Spotter Search Summary View

The Spotter Summary displays the Available Violations and the Available Datasources for a specified time frame. From here you can provide a search query, or enter text to filter the available violations and datasources and sort them by name or total events count.

The screenshot shows the Spotter interface with the following components:

- Search Bar:** Includes a placeholder "Enter search query or click on Datasource below, example: resourcegroupname > Vontu", a "Search controls" button, and a time range selector set to "Last 1 hours".
- Navigation Bar:** Contains tabs for SUMMARY, SEARCH RESULTS, CACHED QUERIES, SAVED QUERIES, CONSOLE, and VIEW JOBS.
- Filter Policies:** A section with a "Filter policies" dropdown and a "Sort results" button.
- Available Violations:** A table listing various violations with their counts. Callouts indicate:
 - "Enter text to filter results" pointing to the filter input.
 - "Click to view violation details" pointing to a violation entry.
 - "Click to view violation results" pointing to a violation entry.
- Available Datasources:** A table listing various datasources with their event counts.

Use the menu on the right side of the search bar to specify a time range.

The screenshot shows the time range selection menu with the following options:

Minutes	Hours	Days	Years
Last 15 minutes	Last 1 hour	Last 7 days	Last year
Last 20 minutes	Last 2 hours	Last 14 days	All Time
Last 25 minutes	Last 6 hours	Last 21 days	
Last 30 minutes	Last 12 hours	Last 30 days	
	Last 24 hours	Last 60 days	
	Last 48 hours	Last 90 days	
	Last 72 hours		

Custom Range

Click on the screen navigation bar to access the following screens at any time:

The screenshot shows the screen navigation bar with the following tabs:

- SUMMARY
- SEARCH RESULTS
- CACHED QUERIES
- SAVED QUERIES
- CONSOLE
- VIEW JOBS

- **Summary:** Displays a summary of the available violations and datasources
- **Search Results:** Displays the results of search queries
- **Cached Queries:** Displays recent queries stored in the cache
- **Saved Queries:** Displays specific queries saved for future use
- **Console:** Displays Spotter activity logs
- **View Jobs:** Displays a list of jobs.

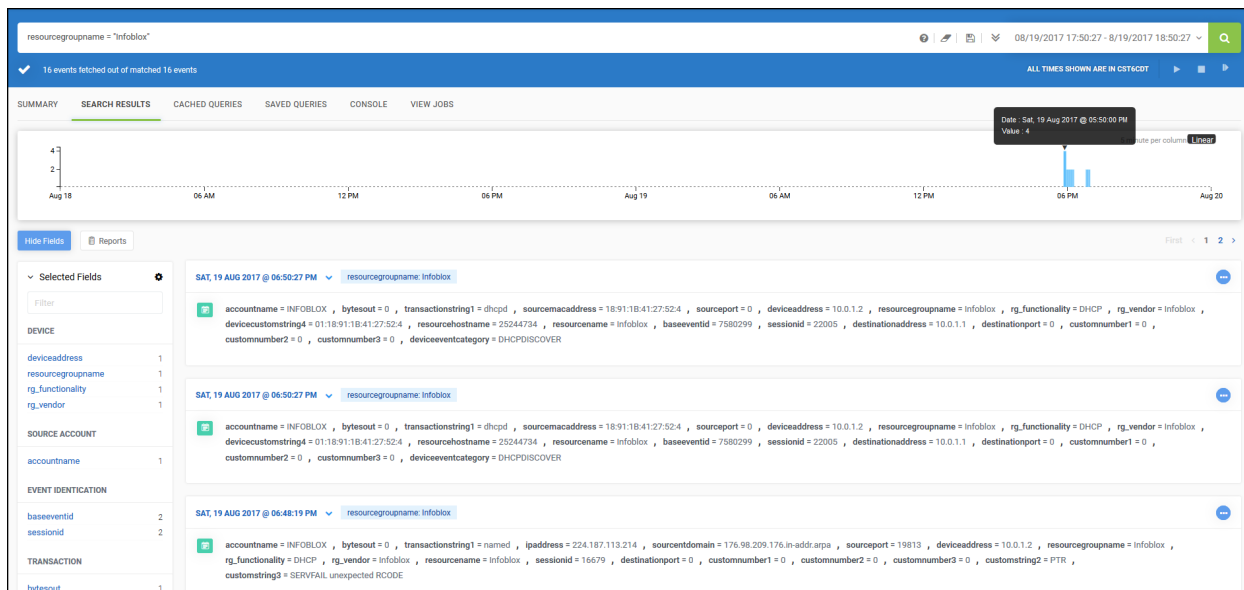


Note: The green bar indicates which screen you are currently viewing.

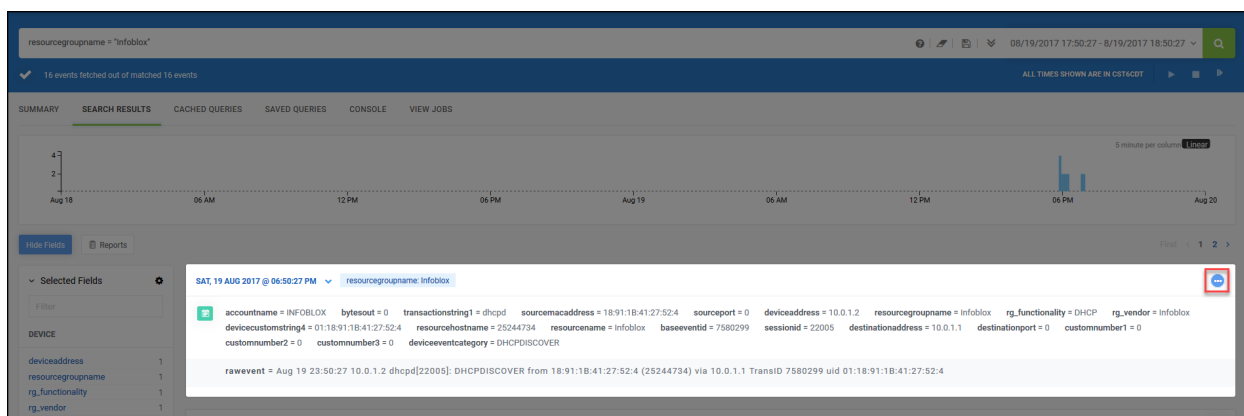
Filter Available Violations and Datasources

From the Summary screen, you can click on any available violation or datasource to filter the results. The view will switch to the Search Results screen.

Spotter Search Results View



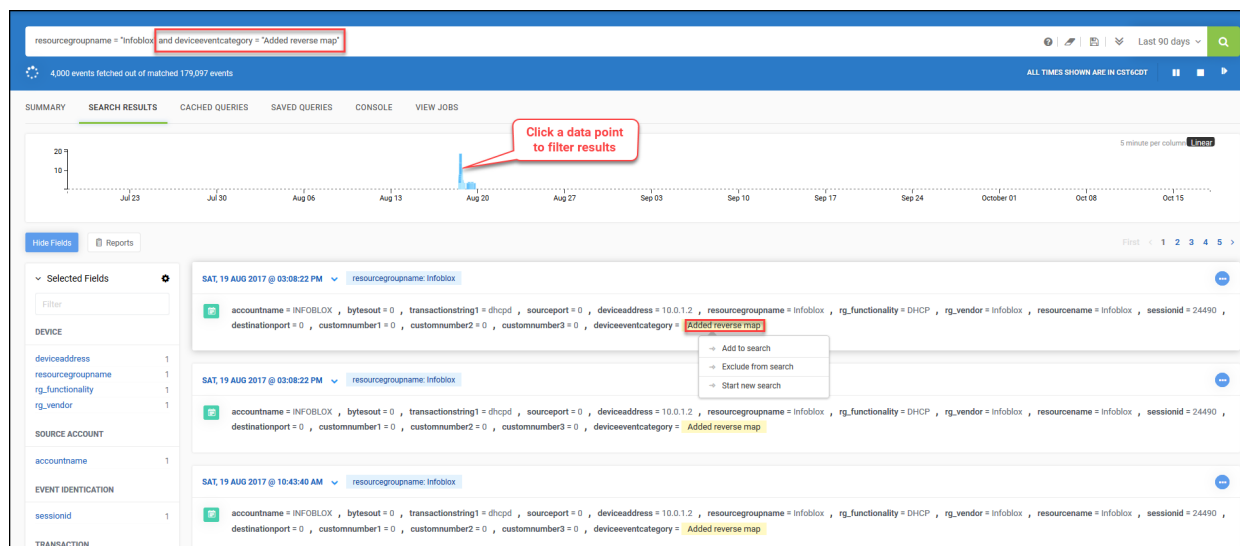
Click the collapsed icon to isolate a single event in the results.



Search Filters

Within the event results, you can click on any field to filter the results. You may select any number of filters to narrow your results.

- Click **Add to search** to apply the filter.
- Click **Exclude from search** to remove the filter.
- Click **Start new search** to clear all results and start a new search.



The field will be added to the search bar with the AND operator, and the field will be highlighted in the events results.

Search Fields

When you import your user, activity, access, watchlist, lookup, and entity metadata, your attributes are mapped to a corresponding attribute within the ArcSight UBA application. These mapped attributes are used as search fields in Spotter.

When you enter a query for a particular data source, the fields that are available and mapped are listed by type in the **Selected Fields** and **Other Fields** panels on the left side of the Search Results screen beside the events. You can select from these fields to add to the search query and filter your results.

In ArcSight UBA 6.10, you can switch your view between the following options:

- **Securonix Attribute Names:** View the attributes in the ArcSight UBA schema to which you have mapped the device or datasource attributes:

TRANSACTION	
bytesin	1
bytesout	1
destination servicename	1
event outcome	1
message	1

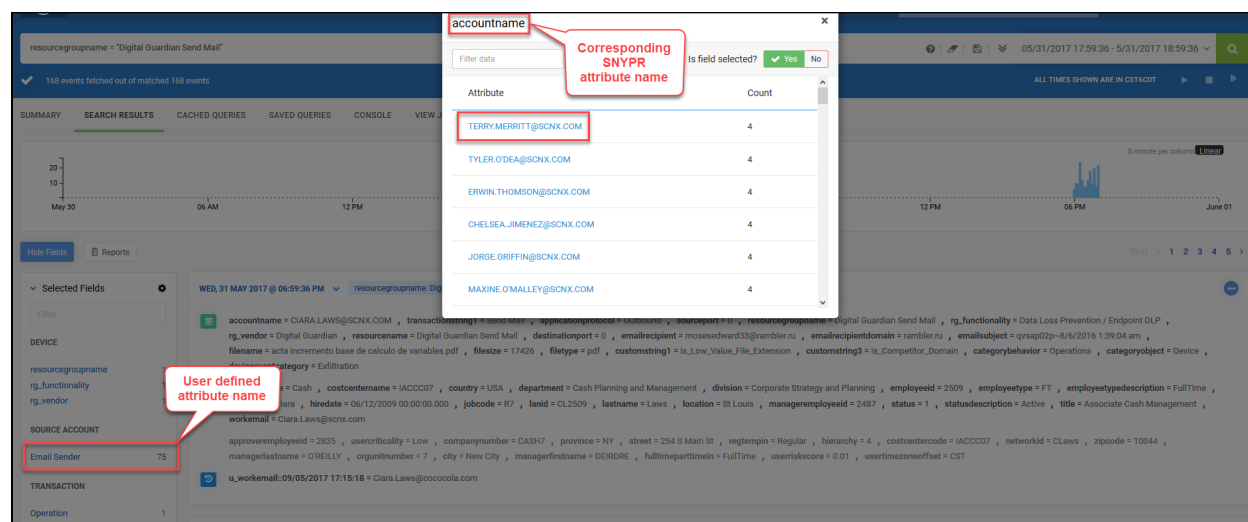
- **User Defined Attribute Names:** View the user-defined names of the attributes mapped during data import. If you have not specified a custom name for an attribute, view the device or data-source attribute name:

TRANSACTION	
Bytes_Received	1
Bytes_Sent	1
Destination Application	1
Response_Code	1
msg	1

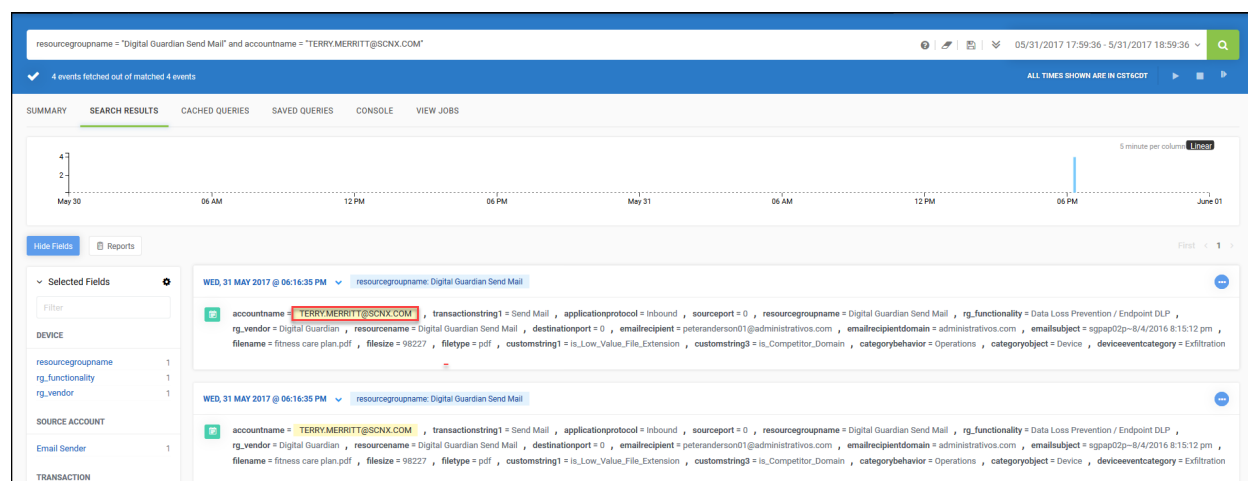
To switch between Securonix Attribute and User Defined Attribute names, click the gear icon and select from dropdown. Click any attribute to filter results. You can also select **Hide Fields** to maximize the event results by hiding the Fields panel.

The screenshot displays the ArcSight User Behavior Analytics 6.10 interface. At the top, there are tabs for SUMMARY, SEARCH RESULTS, CACHED QUERIES, SAVED QUERIES, CONSOLE, and VIEW JOBS. Below the tabs is a timeline view showing data from Sep 10 to Sep 12. A 'Hide Fields' button is visible in the top left of the main content area. On the left side, there is a 'Selected Fields' panel with a gear icon for configuration. Below this panel, there are sections for 'Show Securonix Attribute Names', 'Show User Defined Attribute Names', and 'DEVICE'. The 'TRANSACTION' section is expanded, showing a list of attributes: Bytes_Received, Bytes_Sent, Destination Application, Response_Code, and msg. The main content area displays a detailed view of a transaction event for 'MON, 11 SEP 2017 @ 08:59:14 PM' with resource group name 'Bluecoat Proxy'. The event details include accountname, bytesin, bytesout, destination servicename, event outcome, message, application protocol, ip address, source address, resource group name, rg functionality, rg vendor, destination domain, destination port, request client application, request url, request context, request method, request type, custom number, custom string, category behavior, category object, device event category, company code, cost center name, country, department, division, employee id, employee type, employee type description, hire date, job code, lan id, last name, location, manager employee id, status, status description, title, work email, approve employee id, mobile, user criticality, company number, street, reg temp in, hierarchy, cost center code, manager last name, user time zone offset, province, network id, zipcode, org unit number, city, manager first name, full time part time in, and user risk score.

The number beside the field name represents the number of unique attributes for that particular field. Click on the field to drill down into each attribute to see the number of events associated with it.

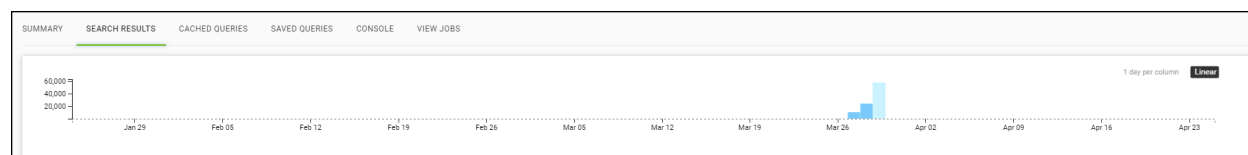


Click on the attribute to see the events associated with it. The selected attribute will appear highlighted in the search results.



Search Results Reports

Spotter displays event information in visual reports. By default, the results are displayed as a linear chart representing the number of events on the y-axis and the date on the x-axis.



Select a point on the chart to view the events for that time.

Use report commands in the search query to change the format of the reports to any of the following types of reports:

Use the following syntax: resourcegroupname = "<name>" | TABLE <field1>, <field2>

resourcegroupname = "Digital Guardian Send Mail" |TABLE ipaddress, accountname

168 events fetched out of matched 168 events

ALL TIMES SHOWN ARE IN CST6CDT

SUMMARYSEARCH RESULTS

CACHED QUERIES

SAVED QUERIES

CONSOLE

VIEW JOBS

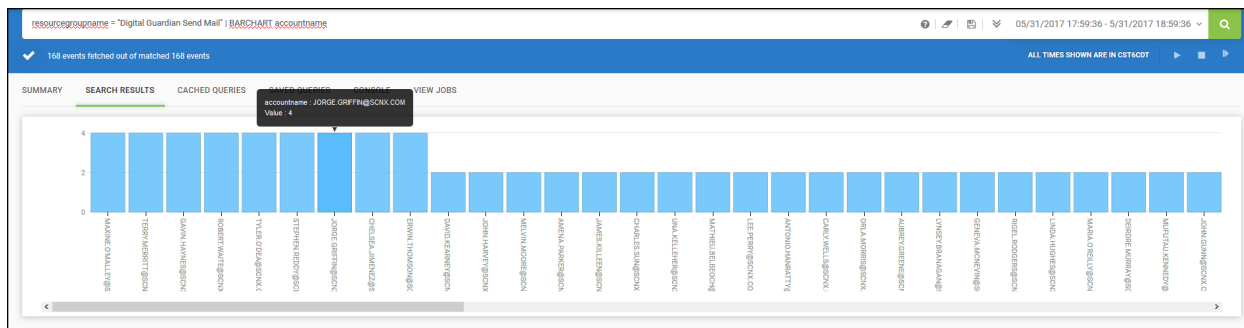
Reports

IPADDRESS	ACCOUNTNAME
-	CIARA.LAWS@SCNX.COM
-	CIARA.LAWS@SCNX.COM
-	DAVID.KEARNEY@SCNX.COM
-	DAVID.KEARNEY@SCNX.COM
-	UNA.KELLEHER@SCNX.COM
-	UNA.KELLEHER@SCNX.COM
-	ORLA.BOYLE@SCNX.COM
-	ORLA.BOYLE@SCNX.COM
-	JAMES.KILLEEN@SCNX.COM
-	JAMES.KILLEEN@SCNX.COM
-	ERWIN.THOMSON@SCNX.COM
-	ERWIN.THOMSON@SCNX.COM
-	MARK.WRISLEY@SCNX.COM
-	MARK.WRISLEY@SCNX.COM
-	JAMAAL.CORLESS@SCNX.COM

First12345>LastTOTAL: 168

Use the following syntax: resourcegroupname = "<name>" | BARCHART <field1>

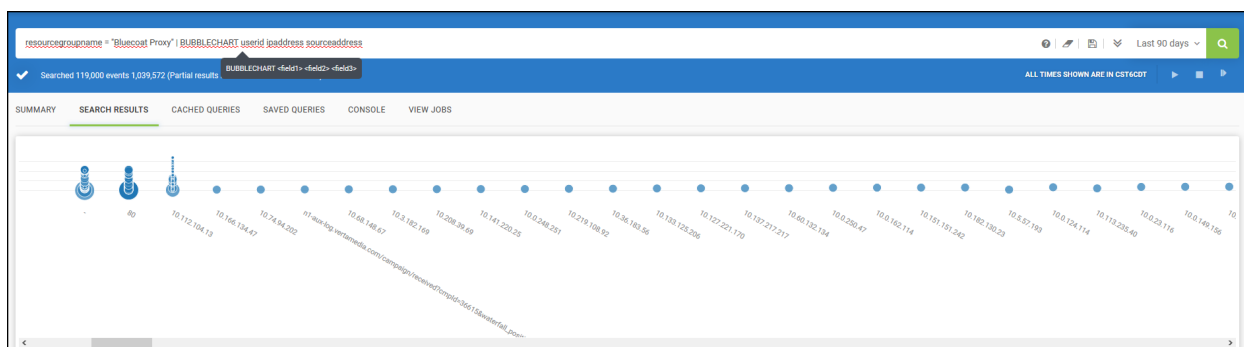
Example: resourcegroupname = "Digital Guardian Send Mail" | BARCHART accountname



Bubble chart

Use the following syntax: resourcegroupname = "<name>" | BUBBLECHART <field1> <field2> <field3>

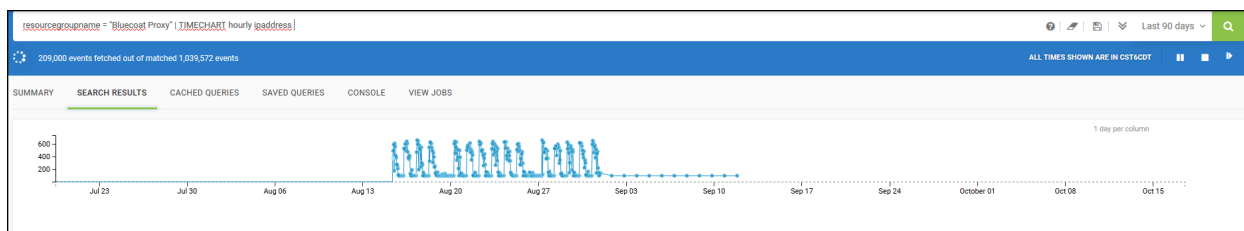
Example: resourcegroupname = "Bluecoat Proxy" | BUBBLECHART userid ipaddress sourceaddress



Time chart

Use the following syntax: TIMECHART <hourly | daily | weekly | monthly> <count by> <field1> <by> <field2> ... <field N>

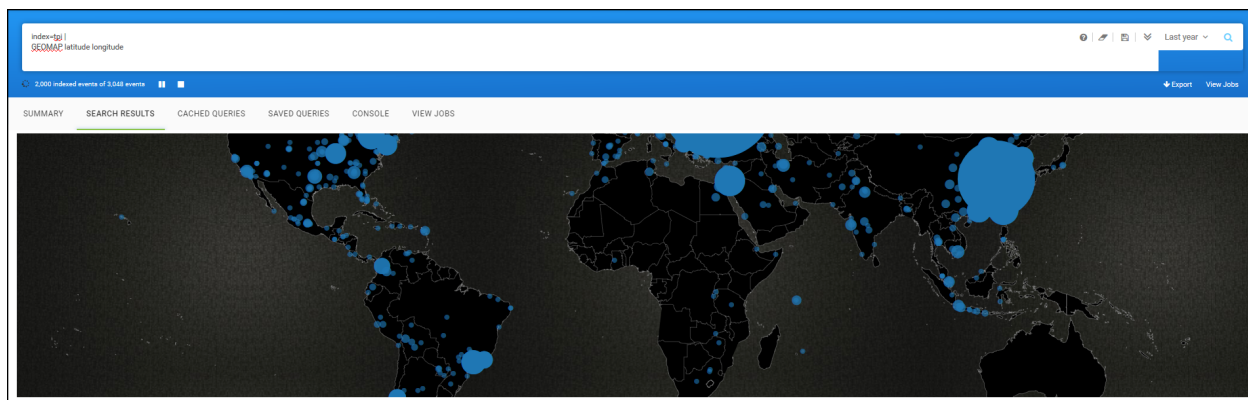
Example: resourcegroupname = "Bluecoat Proxy" | TIMECHART hourly ipaddress



Geomap

Use the following syntax: index=<core> | GEOMAP <field1> <field2>

Example: index=tpi | GEOMAP latitude longitude



Searching Spotter

Indexes

Spotter uses natural language to search within the data indexed in the ArcSight UBA application. You can search within any index into which you have imported data. ArcSight UBA uses the following indexes to store data:

- Activity
- Archive
- Users
- Violation
- TPI
- Watchlist
- Whitelist
- Lookup
- Asset
- Geolocation
- Risk Score
- Risk Score History

By default, Spotter searches the Activity index. You may specify the index you would like to search using the following syntax:

index = < index > <and | or> <field> = <field value>

For example: `index=users`

index:users

666 events fetched out of matched 666 events

ALL TIMES SHOWN ARE IN CST/CDT

SUMMARY SEARCH RESULTS CACHED QUERIES SAVED QUERIES CONSOLE VIEW JOBS

Hide Fields Reports

Selected Fields

Filter

USER IDENTITY

companycode	20
costcentername	19
country	2
department	42
division	14
employeeid	100+
employeeype	2
employeeypedescripion	2
hiredate	100+
jobcode	27
landid	100+
lastname	100+
location	22

companycode = DEP , costcentername = IMFGCC10 , country = USA , department = Deposit and Debit Card Fulfillment , division = Deposit and Card Products , employeeid = 2843 , employeeype = FT , employeeypedescripion = FullTime ,
 firstname = Lars , hiredate = 08/08/2009 00:00:00.000 , jobcode = R1 , landid = LS2843 , lastname = Shah , location = Indianapolis , manageremployeeid = 2835 , status = 1 , statusdescription = Active ,
 title = Associate Deposits and Debit Cards , workemail = Lars.Shah@scnx.com
 networkid = LShah , approveremployeeid = 2835 , zipcode = 2026 , usercriticality = Low , managerlastname = Quinn , companynumber = DEP27 , province = MA , street = 980 WASHINGTON ST , orgunitnumber = 19 , city = DEDHAM ,
 regtempin = Regular , managerfirstname = Joseph , hierarchy = 4 , fulltimeparttimein = FullTime , usersriskscore = 0.01 , costcentercode = IMFGCC10 , usertimezoneoffset = CST

companycode = DEP , costcentername = IMFGCC10 , country = USA , department = Deposit and Debit Card Fulfillment , division = Deposit and Card Products , employeeid = 2842 , employeeype = FT , employeeypedescripion = FullTime ,
 firstname = Monika , hiredate = 08/08/2009 00:00:00.000 , jobcode = R1 , landid = Md2842 , lastname = de Chalendar , location = Indianapolis , manageremployeeid = 2835 , status = 1 , statusdescription = Active ,
 title = Associate Deposits and Debit Cards , workemail = Monika.de.Chalendar@scnx.com
 networkid = Mde Chalendar , approveremployeeid = 2835 , mobile = 020 7695 4169 , zipcode = 66206-2157 , usercriticality = Low , managerlastname = Quinn , companynumber = DEP26 , province = KS , street = 9500 Mission Road ,
 orgunitnumber = 19 , city = Overland Park , regtempin = Regular , managerfirstname = Joseph , hierarchy = 4 , fulltimeparttimein = FullTime , usersriskscore = 0.01 , costcentercode = IMFGCC10 , usertimezoneoffset = CST

Use the fields associated with the indexes to filter results.

index:users and employeeypedescripion = PartTime

31 events fetched out of matched 31 events

ALL TIMES SHOWN ARE IN CST/CDT

SUMMARY SEARCH RESULTS CACHED QUERIES SAVED QUERIES CONSOLE VIEW JOBS

Hide Fields Reports

Selected Fields

Filter

USER IDENTITY

companycode	6
costcentername	8
country	1
department	14
division	6
employeeid	31
employeeype	1
employeeypedescripion	1
hiredate	30
jobcode	1
landid	31
lastname	31

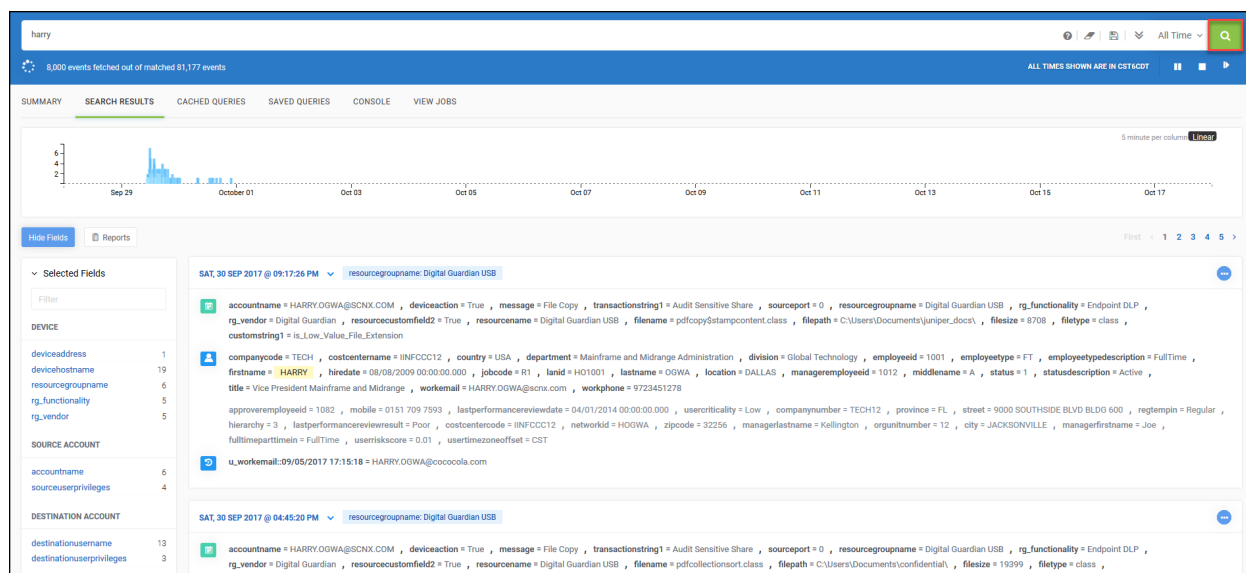
companycode = GMKT , costcentername = ISALCCC11 , country = USA , department = Commodities , division = Global Markets , employeeid = 2391 , employeeype = PT , employeeypedescripion = PartTime , firstname = Grainne ,
 hiredate = 08/08/2009 00:00:00.000 , jobcode = R1 , landid = GN2391 , lastname = Ni Chearbhail , location = Boston , manageremployeeid = 2335 , status = 1 , statusdescription = Active , title = Associate Commodities Market ,
 workemail = Grainne.Ni.Chearbhail@scnx.com
 networkid = GNI Chearbhail , approveremployeeid = 2681 , mobile = + 44 207 695 4469 , zipcode = 92560-7010 , usercriticality = Low , managerlastname = Barry , companynumber = GMKT15 , province = CA , street = 500-c Newport Center Dr ,
 orgunitnumber = 15 , city = Newport Beach , regtempin = Regular , managerfirstname = Donna , hierarchy = 4 , fulltimeparttimein = PartTime , usersriskscore = 0.01 , costcentercode = ISALCCC11 , usertimezoneoffset = CST

companycode = GMKT , costcentername = ISALCCC11 , country = USA , department = Credit , division = Global Markets , employeeid = 2331 , employeeype = PT , employeeypedescripion = PartTime , firstname = Linda ,
 hiredate = 08/08/2009 00:00:00.000 , jobcode = R1 , landid = LH2331 , lastname = Hughes , location = Boston , manageremployeeid = 2287 , status = 1 , statusdescription = Active , title = Associate Vice President Credit Market ,
 workemail = Linda.Hughes@scnx.com
 networkid = LHughes , approveremployeeid = 2534 , mobile = 2076957667 1/58 , zipcode = 94404-1213 , usercriticality = Low , managerlastname = Coughlan , companynumber = GMKT15 , province = CA , street = 1163 Triton Dr ,
 orgunitnumber = 15 , city = Foster City , regtempin = Regular , managerfirstname = Tadeusz , hierarchy = 4 , fulltimeparttimein = PartTime , usersriskscore = 0.01 , costcentercode = ISALCCC11 , usertimezoneoffset = CST

Using Search Queries

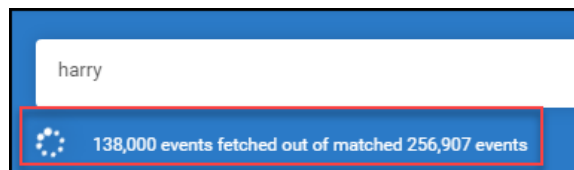
Threat hunters can use simple language to find specific events or information associated with entities, resources, and threats.

To search Spotter, enter the query and hit **Enter** or the use the magnifying glass icon on the right side of the search bar.

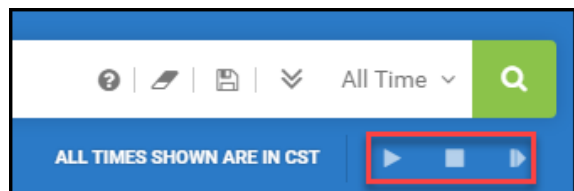


Search Controls

The search controls below the search bar show the progress of your search and identifies any errors with search syntax or invalid parameters.



You can also start, stop, or pause queries.



Spotter Search Help

From the other options section on the right side of the search bar, you can access Spotter Search Help to view the syntax and examples of the available commands, operators, and fields Spotter uses to perform functions such as search within indexes, change the report format, and analyze data.



Search commands

BASIC

POLICY
Queries for Violation Core

Data Sources
Queries for Activity Core

EVAL

EQUALS
Returns true if value matches else returns false

ISDIGIT
Returns true if value is digit , else returns false

to_unixtime
Returns epochtime from a valid date string

ISINT
Returns true if value is int , else returns false

ISNOTNULL
Returns true if value is not null , else returns false.

ISBOOLEAN
Returns true or false if it is boolean

from_unixtime
Returns Valid date String from a epochtime

LEN
Find length of field value

ISNUM
Returns true if value is number , else returns false

POLICY

Description
Queries for Violation Core

Syntax
<resourcegroupname> <=> <value>

Examples
policyname = Logon_Failure

Notes
Date format supported for the date attributes to Query - MM/dd/yyyy HH:mm:ss.SSS

You can also view this complete information in the [Spotter Search Help](#).

Other Search Options

On the search bar, you can access other search options, including:

Clear search query



Use this option to clear the search bar and results to begin a new search query.

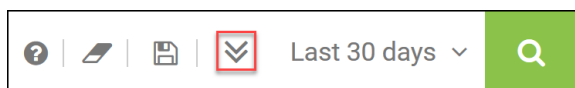
Save search results



Use this option to save the current search on the Saved Queries screen.

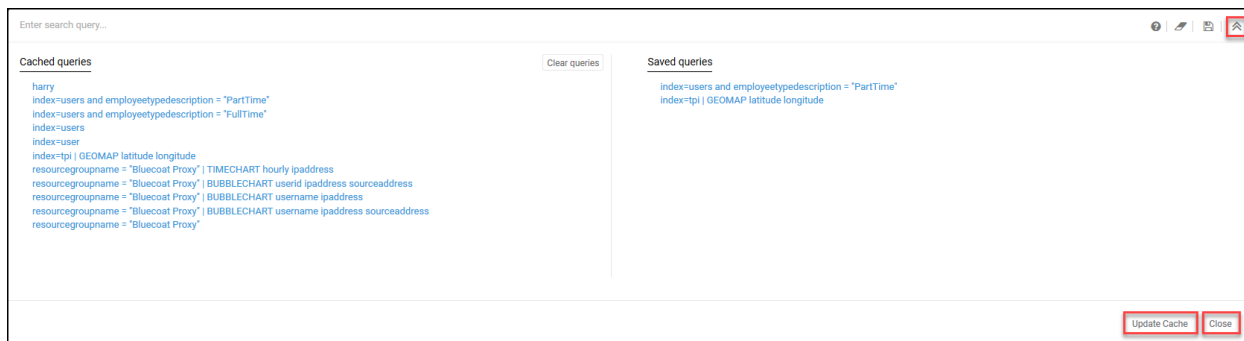
SUMMARY	SEARCH RESULTS	CACHED QUERIES	SAVED QUERIES	CONSOLE	VIEW JOBS
<div> <div>First</div> <div><</div> <div>1</div> <div>></div> <div>Last</div> <div>TOTAL 2</div> </div>					
Name	Query	Action			
Access to Java file	polycname = "Access to Java Files by Non-Engineering Dept [G-DRV]"				
Marketing setting drive permission t	polycname = "Drive Permission Set to Self [G-DRV]" and title = "Marketing associate"				

See more options



Use this option to access more options for searching including the following:

- View Cached queries
- View Saved queries
- **Update Cache**
- Click **Close** to close the window and return to the current screen view



Sample Spotter Search Queries

Example 1: Find Policy Violations

To view all the violations of a particular policy, use the syntax as in the following example:

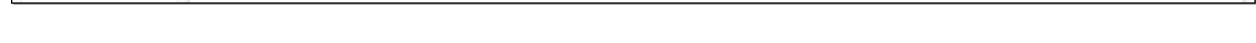
polycname = "Spike in Number of Records accessed by an Employee"



To view check if a user has sent email to a personal email address, the following query uses the

```
resourcegroupname="Digital Guardian Send Mail" | EVAL matchPerc = emailtoSelf(first-
```

© 2013 Pearson Education, Inc. or its affiliate(s). All rights reserved. Pearson Education, Inc., publishing as Pearson Benjamin Cummings, 101 Philip Drive, Assinippi Park, New York, NY 10984-2135



To view all the devices in the asset index, use the following query:

```
index = asset
```

index=asset

782 events fetched out of matched 782 events

ALL TIMES SHOWN ARE IN CST/CDT

SUMMARY SEARCH RESULTS CACHED QUERIES SAVED QUERIES CONSOLE GEOLOCATION MAP VIEW JOBS

Hide Fields Reports

First 1 2 3 4 5

Selected Fields

Filter

OTHER

- key_Serveripaddress 100+
- key_ServerOS 34
- key_Servermacaddress 100+
- key_Id 100+
- key_Servernetworkname 3
- key_Serverfqdn 100+
- entityname 100+
- key_Workstation_MacAddr... 100+
- key_Servercategory 6
- entitytype 1
- key_Workstation_Name 100+
- key_Workstation_Owner 100+
- key_Workstation_OS 2

entityname = 2*-RWC0DC8956 , entityType = Resources , key_ServerOS = Cent-OS 5.6 , key_Servercategory = POS , key_Serverfqdn = RWC-8956.scnx.com , key_Serveripaddress = 10.0.1.164 , key_Servermacaddress = 4:15:4C:96:27:47:47 , key_Servernetworkname = Redwood City Data Center , key_Id = 66

entityname = 2*-RWC0DC8953 , entityType = Resources , key_ServerOS = RHEL 6.8 , key_Servercategory = PCI Assets , key_Serverfqdn = RWC-8953.scnx.com , key_Serveripaddress = 10.0.1.141 , key_Servermacaddress = 3:34:6C:52:12:11:0 , key_Servernetworkname = Redwood City Data Center , key_Id = 43

entityname = 2*-RWC0DC8177 , entityType = Resources , key_ServerOS = Cent-OS 6.2 , key_Servercategory = PCI Assets , key_Serverfqdn = RWC-8177.scnx.com , key_Serveripaddress = 10.0.1.105 , key_Servermacaddress = 11:22:9C:77:3:45:56 , key_Servernetworkname = Redwood City Data Center , key_Id = 7

entityname = 2*-RWC0DC7725 , entityType = Resources , key_ServerOS = Cent-OS 7.2 , key_Servercategory = PCI Assets , key_Serverfqdn = RWC-7725.scnx.com , key_Serveripaddress = 10.0.1.145 , key_Servermacaddress = 1:32:1C:28:1:57:22 , key_Servernetworkname = Redwood City Data Center , key_Id = 47

Example 4: View Top IP Address by Account Name

To view a table with the top IP addresses by account name for a data source, use the following query:

resourcegroupname = "Bluecoat Proxy" | TOP ipaddress by accountname

resourcegroupname = "Bluecoat Proxy" | TOP ipaddress by accountname

3,000 events fetched out of matched 1,039,572 events

ALL TIMES SHOWN ARE IN CST/CDT

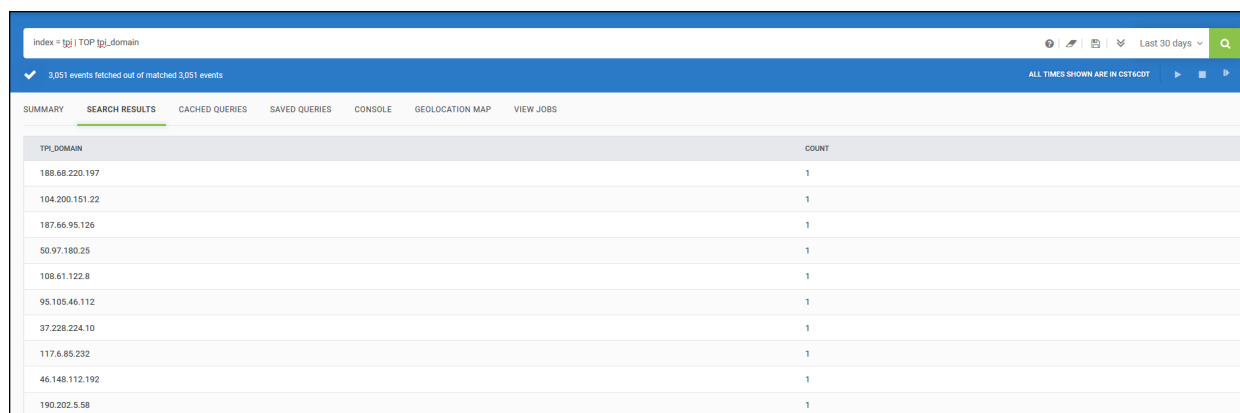
SUMMARY SEARCH RESULTS CACHED QUERIES SAVED QUERIES CONSOLE GEOLOCATION MAP VIEW JOBS

IPADDRESS	ACCOUNTNAME	COUNT
10.1.2.145	BR10B2	19
10.1.4.63	QUINN,JOSEPH	12
10.1.4.98	O'NEILL,RICHARD	11
10.1.4.195	QUINN,BRANDT	11
10.1.2.93	WARNER,ZACHERY	11
10.1.4.115	MCMAHON,LARISSA	11
10.1.1.47	WALSH,LAIDAN	10
10.1.4.44	PEREIRA,KATHRYN	10
10.1.2.70	MCLOUGHLIN,ZACHERY	10
10.1.4.225	HUGHES,LINDA	10

Example 5: Search threat intelligence for top countries of origin

To find the top TPI domains from which threats originate in the Third Party Intelligence index, use the following query:

index = tpi | TOP tpi_domain



index = tpj | TOP tpj_domain

3,051 events fetched out of matched 3,051 events

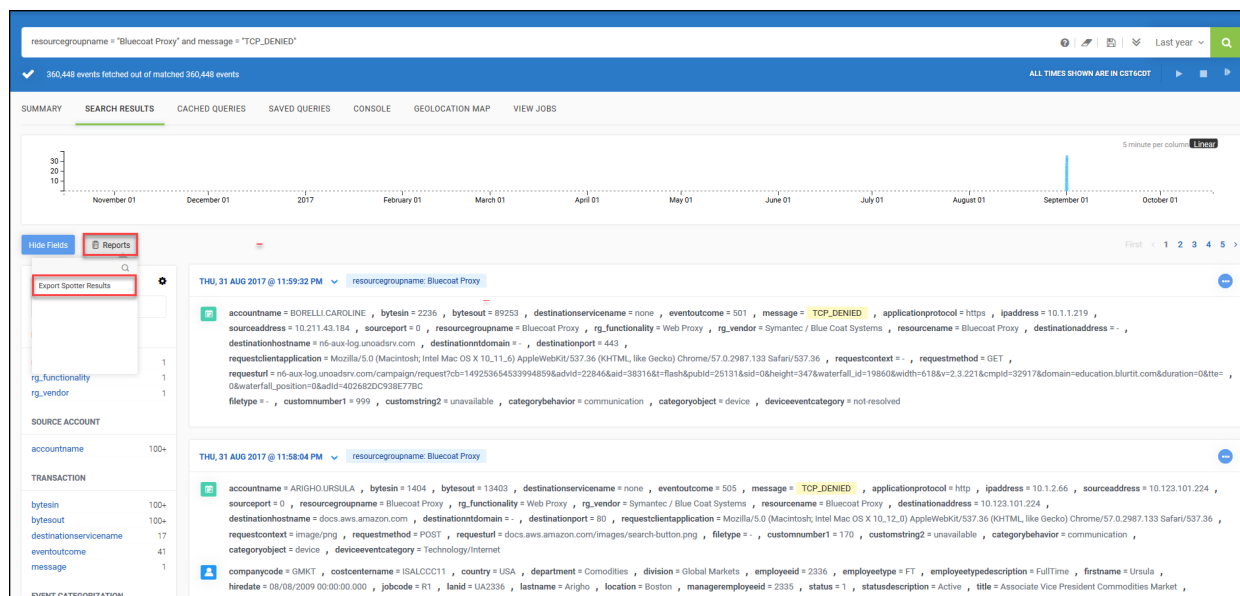
ALL TIMES SHOWN ARE IN CST/CDT

TPJ_DOMAIN	COUNT
188.68.220.197	1
104.200.151.22	1
187.66.95.126	1
50.97.180.25	1
108.61.122.8	1
95.105.46.112	1
37.228.224.10	1
117.6.85.232	1
46.148.112.192	1
190.202.5.58	1

Exporting Search Results as Reports

You can export search results in several file formats. To export Spotter search results, click **Reports** from the Search Results screen above the Selected Fields.

The option to **Export Spotter Results** appears in the dropdown along with any Spotter reports configured under **Menu > Reports > Categorized Reports**. For information about configuring Spotter Reports, see [Reports](#).



resourcegroupname = "Bluecoat Proxy" and message = "TCP_DENIED"

360,448 events fetched out of matched 360,448 events

ALL TIMES SHOWN ARE IN CST/CDT

5 minute per column 1 hour

THU, 31 AUG 2017 @ 11:59:32 PM resourcegroupname: Bluecoat Proxy

accountname = BORELLI CAROLINE , bytesin = 2236 , bytesout = 89253 , destinationservice = none , eventoutcome = 501 , message = TCP_DENIED , applicationprotocol = https , ipaddress = 10.1.1.219 , sourceaddress = 10.211.43.184 , sourceport = 0 , resourcegroupname = Bluecoat Proxy , rg_functionality = Web Proxy , rg_vendor = Symantec / Blue Coat Systems , resource = Bluecoat Proxy , destinationaddress = , destinationhostname = ns-aux-log.unoadsrv.com , destinationdomain = , destinationport = 443 , requestclientapplication = Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133 Safari/537.36 , requestcontext = , requestmethod = GET , requesturl = ns-aux-log.unoadsrv.com/campaign/request?cb=149253654533994859&adid=22846&aid=38316&rt=Flash&pubid=25131&aid=0&height=347&waterfall_id=19860&width=618&v=2.3.221&cmprid=32917&domain=education.blurlit.com&duration=0&tte=0&waterfall_position=5&adid=402682DC93877BC , filetype = , customnumber1 = 999 , customstring2 = unavailable , categorybehavior = communication , categoryobject = device , deviceeventcategory = not-resolved

THU, 31 AUG 2017 @ 11:58:04 PM resourcegroupname: Bluecoat Proxy

accountname = ARIGHO URSULA , bytesin = 1404 , bytesout = 13403 , destinationservice = none , eventoutcome = 505 , message = TCP_DENIED , applicationprotocol = http , ipaddress = 10.1.2.66 , sourceaddress = 10.123.101.224 , sourceport = 0 , resourcegroupname = Bluecoat Proxy , rg_functionality = Web Proxy , rg_vendor = Symantec / Blue Coat Systems , resource = Bluecoat Proxy , destinationaddress = 10.123.101.224 , destinationhostname = docs.aws.amazon.com , destinationdomain = , destinationport = 80 , requestclientapplication = Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.133 Safari/537.36 , requestcontext = image/png , requestmethod = POST , requesturl = docs.aws.amazon.com/images/search-button.png , filetype = , customnumber1 = 170 , customstring2 = unavailable , categorybehavior = communication , categoryobject = device , deviceeventcategory = Technology/Internet

companycode = GMIT , costcentername = ISALCCC11 , country = USA , department = Commodities , division = Global Markets , employeeid = 2336 , employeetype = FT , employeetypedescription = FullTime , firstname = Ursula , hiredate = 08/08/2009 00:00:00.000 , jobcode = RT , lanid = UA2336 , lastname = Arigho , location = Boston , manageremployeeid = 2335 , status = 1 , statusdescription = Active , title = Associate Vice President Commodities Market ,

Click **Export Search Results** or a Spotter Report. The Run Spotter Report window appears.

Run Spotter Report

SPECIFY THE LABEL FOR THE REPORT YOU WANT TO MAP ATTRIBUTE.

Event	Time	Event Time
accountname username	week	eventtime eventtime
bytesin Bytes_Received	month	
bytesout Bytes_Sent	hour	
destinationservername Destination Application	year	
eventoutcome Response_Code	dayofweek	categorizedtime
message msg	dayofweek	categorizedtime
applicationprotocol application	dayofyear	dayofmonth
ipaddress ClientIP	dayofyear	dayofmonth
sourceaddress Device_IP		
sourceport src_port		
resourcegroupname resourcegroupname		
rg_functionality rg_functionality		
rg_vendor rg_vendor		
resource resource		
destinationaddress dst_ip		
destinationhostname Destination Domain		
destinationdomain Referer		
requestclientapplication User_Agent		
requestcontext Query_Response		
requestmethod Method		
requesturl URL		
filetype Filetype		
customnumber1 Duration		
customstring2 Custom Category		
categorybehavior categorybehavior		
categoryobject categoryobject		
deviceeventcategory Category		

Select Report Format

PDF

Run Cancel

Click the attributes to include in the report. Attributes that appear in blue will be included in the report. Attributes that appear in gray are excluded from the report. You can edit the attribute label under which the mapped attribute will appear in the report column.

Click **Save** to save the label and include the attribute in the report.

Click **Remove Mapping** to remove the attribute from the report.

Run Spotter Report

SPECIFY THE LABEL FOR THE REPORT YOU WANT TO MAP ATTRIBUTE.

Event	Time	Event Time
accountname username	week	eventtime eventtime
bytesin Bytes_Received	month	
bytesout Bytes_Sent	hour	
destinationservername Destination Application	year	
eventoutcome Response_Code	dayofweek	categorizedtime
message msg	dayofweek	categorizedtime
applicationprotocol application	dayofyear	dayofmonth
ipaddress ClientIP	dayofyear	dayofmonth
sourceaddress Device_IP		
sourceport src_port		
resourcegroupname resourcegroupname		
rg_functionality rg_functionality		
rg_vendor rg_vendor		
resource resource		
destinationaddress dst_ip		
destinationhostname Destination Domain		
destinationdomain Referer		
requestclientapplication User_Agent		
requestcontext Query_Response		
requestmethod Method		
requesturl URL		
filetype Filetype		
customnumber1 Duration		
customstring2 Custom Category		
categorybehavior categorybehavior		
categoryobject categoryobject		
deviceeventcategory Category		

Select Report Format

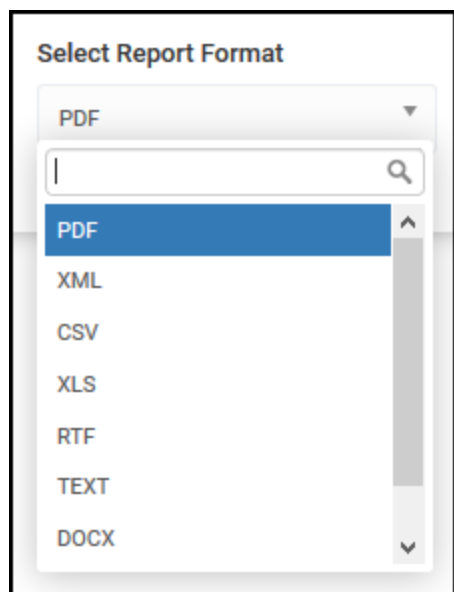
PDF

Map With
resource
Enter The Label For Attribute This Mapped Attribute will reflect as Label in the reports column.
Remove Mapping Save

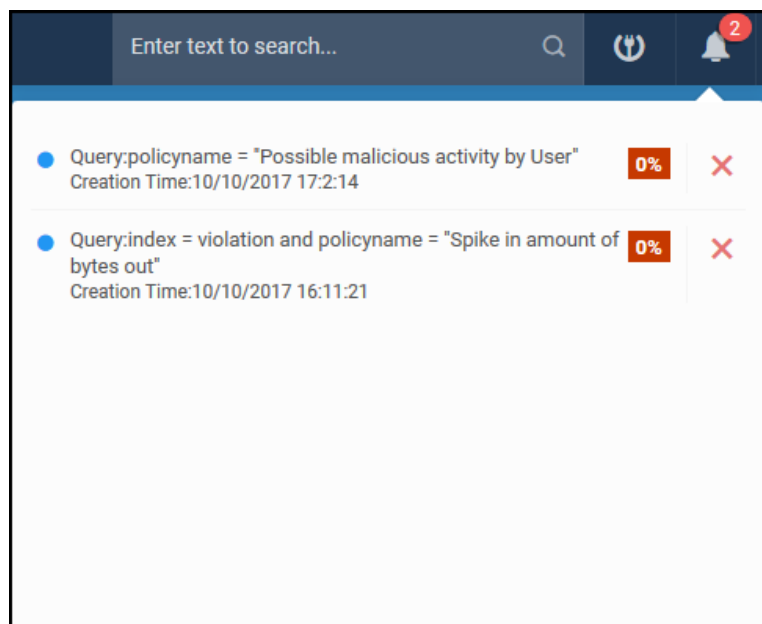
Select from the dropdown to run report in one of the following formats:

- PDF
- XML

- CSV
- XLS
- RTF
- TEXT
- DOCX
- XLSX











Click **Run** to run the report and download the report from the Notifications menu when status is complete:



Viewing Jobs

You may view the jobs in Spotter, including recent search queries and file exports by clicking the **View Jobs** tab. This will display the recent Jobs.

SUMMARY	SEARCH RESULTS	CACHED QUERIES	SAVED QUERIES	CONSOLE	GEOLOCATION MAP	VIEW JOBS
QUERY		RECORDS	START TIME	END TIME	STATUS	ACTIONS
resourcegroupname = "Bluecoat Proxy" and message = "TCP_DENIED"		360.4K	10/17/2017 14:23:58	10/17/2017 14:25:54	FINISHED	
resourcegroupname = "Bluecoat Proxy"		13K	10/17/2017 14:23:48	10/17/2017 14:23:58	FINISHED	
resourcegroupname = "Bluecoat Proxy"		1	10/17/2017 14:23:31	10/17/2017 14:23:32	FINISHED	
index = tpi TOP tpi_domain		3K	10/17/2017 14:17:14	10/17/2017 14:17:14	FINISHED	
index = tpi		3K	10/17/2017 14:16:54	10/17/2017 14:16:54	FINISHED	
index = users		666	10/17/2017 14:16:50	10/17/2017 14:16:50	FINISHED	
index = users TOP statusdescription		666	10/17/2017 14:16:41	10/17/2017 14:16:41	FINISHED	
index = tpi TOP categoryseverity		3K	10/17/2017 14:16:21	10/17/2017 14:16:21	FINISHED	

Click the **Console** tab to view the Spotter activity log.

SUMMARY	SEARCH RESULTS	CACHED QUERIES	SAVED QUERIES	CONSOLE	VIEW JOBS
✓ 24 Apr 2017 16:29:5 resourcegroupname = "GoogleDriveLogs"					
No Results Found					
✓ 24 Apr 2017 16:29:6 resourcegroupname = "GoogleDriveLogs"					
45 found in 0 secs					

Spotter Search Help

This section includes the common natural language search commands for ArcSight UBA 6.10, including search, reporting, and analytical operators.

Search Operators

Basic Commands

Command	Description	Syntax
Policy	Search for a specific policy to find violations Note: Date format supported for the date attributes to Query is MM/dd/yyyy HH:mm:ss.SSS	<policyname> <=> <value>
Example: policyname = "Accounts visiting Algorithmically Generated Domains-1"; policyname = Logon_Failure		
Data Sources	Queries the activity core for specific data sources Note: Date format supported for the date attributes to Query is MM/dd/yyyy HH:mm:ss.SSS	<resourcegroupname> <=> <value>
Example: resourcegroupname = BCP1		
Text	Return all results that include the specified text	<value>
Example: smith		
*	Multiple character wild card searches looks for 0 or more characters	<field1 *> <field2 *> <field n *>
Examples: MM*; With Field : firstname = Ma *		
?	To perform a single character wild card search use the "?" symbol.	<field1 ?> <field2 2> <field n ?>
Example: ??2497		

Index Commands

Command	Description	Syntax
Lookup	Searches within lookup index for all items added in lookup tables	index= < lookup > <and or> <field> Report Commands Field Commands
Examples: index = lookup; index = lookup and lookupname = betaSpotter		
Activity	Searches within the activity index for events. This is the default index for Spotter searches.	index = < activity > <and or> <field> = <field value>
Examples: index = activity; index = activity and accountname = secure; index = activity and deviceaction = 26952 and transactionstring1 = THREAT		
Violation	Searches within the index for policy violations	index = < violation > <and or> <field> = <field value>
Examples: index = violation; index = violation and violator = Users; index = violation and sessionid = 1102		
Riskscore	Searches within the riskscore index that stores all violators and provides riskscore card information	Index = < riskscore > <and or> <field> Report Commands Field Commands
Examples: index = riskscore; index = riskscore and accountname = WHITE.DAVID		
Archive	Searches historical data on HDFS using Impala/Hive Note: You must specify resourcegroupname in query. For Impala queries, resourcegroupname is considered the table name.	index = < archive > <and> <resourcegroupname> <=> <value> <and or> <field> = <field value>
Examples: index = archive and resourcegroupname = Google_login; index = archive and resourcegroupname = Google_login and accountname = AJAIS@SEC.COM		
Whitelist	Searches within the whitelist core for entities in a global or targeted whitelist.	index = < whitelist > <and or> <field> = <field value>
Examples: index = whitelist; index = whitelist and entityname = 1115		

Command	Description	Syntax
TPI	Searches within the TPI index, which stores third party threat intelligence	Index = <tpi> <and or> <field> Report Commands Field Commands
Examples: index = tpi; index = tpi and tpi_addr = zztxdown.com; index = tpi and tpi_srckey = zzshw.net_MalwareDomains		
Asset	Searches within the asset index, which stores device metadata	Index <asset> <and or> <field> Report Commands Field Commands
Examples: index = asset; index = asset and entityname = resource98		
Watchlist	Searches within watchlist index for all watchlisted entities	Index = <watchlist> <and or> <field> Report Commands Field Commands
Examples: index = watchlist; index = watchlist and watchlistitem_item2 = item2		
Users	Searches within the user index	index = < users > <and or> <field> = <field value>
Examples: index = users; index = users and department = marketing		
Riskscorehistory	Searches within the riskscore card history index	Index = <riskscorehistory> <and or> <field> Report Commands Field Commands
Examples: Index = riskscorehistory; index = riskscorehistory and accountname = SWIFT.JOHN		
Geolocation	Searches within the geolocation index for IP Address	index = < geolocation > <and or> <field> = <field value>
Examples: index = geolocation; index = geolocation and longitude = 9.491		

Operators

Command		Syntax
CONTAINS	<p>Checks is a string field contains the specified value</p> <p>Note: Contains does not support Date attributes like hiredate, terminationdate, expirydate and etc. Contains is not case sensitive</p>	<field> CONTAINS <value>
Example: resourcegroupname = BCP1 and accountname contains securonix		
NOT CONTAINS	<p>Checks if a string field does not contain the specified value</p> <p>Note: Not Contains does not support Date attributes like hiredate, terminationdate, expirydate and etc. Contains is not case sensitive</p>	<field> NOT CONTAINS <value>
Example: resourcegroupname = BCP1 and accountname not contains securonix		
AND	Shows the result that fulfills both conditions	<field> <AND> <value>
Example: resourcegroupname = BCP1 and accountname = securonix		
OR	Shows the result which fulfills either one of the specified conditions	<field> <OR> <value>
Example: resourcegroupname = BCP1 OR accountname = TG2277		
BEFORE	<p>Filter the events before date</p> <p>Note: Date format supported for the date attributes to Query is MM/dd/yyyy HH:mm:ss.SSS</p>	<field> BEFORE <value>
Example: policyname = test123 and createdate BEFORE 03/10/2016 06:21:31		

Command		Syntax
AFTER	Filter events after specified date Note: Date format supported for the date attributes to Query is MM/dd/yyyy HH:mm:ss.SSS	<field> AFTER <value>
Example: policyname = test123 and createdate AFTER 03/10/2016 06:21:31		
BETWEEN	Filter the events between value1 and value2 Note: Date format supported for the date attributes to Query is MM/dd/yyyy HH:mm:ss.SSS	<field> BETWEEN <value1><,><value2>
Example: policyname = test123 and week BETWEEN 4,30		
STARTS WITH	Checks if string field value starts with specified value	<field> STARTS WITH <value>
Example: resourcegroupname = BCP1 and accountname STARTS WITH secur		
NOT STARTS WITH	Checks if string field value does not start with specified value	<field> NOT STARTS WITH <value>
Example: resourcegroupname = BCP1 and accountname NOT STARTS WITH secur		
MIN	Provides the MIN value for specified field Note: MIN Operator should be used with following commands: TOP, RARE, STATS and BUBBLECHART	MIN(<field>)
Examples: STATS MIN(bytesout) by ipaddress accountname; resourcegroupname = Email_sent_to_Users BUBBLECHART MIN(bytesout) ipaddress accountname; resourcegroupname = Email_sent_to_Users TOP MIN(bytesout) ipaddress employeeid; resourcegroupname = Email_sent_to_Users RARE MIN(bytesout) ipaddress employeeid		
NULL	Returns the events if the field value is empty	<field> NULL
Example: accountname = securonix AND eventcountry NULL		

Command		Syntax
NOT NULL	Returns the events if the field value is not empty	<field> NOT NULL
Example: accountname = securonix AND eventcountry NOT NULL		
IN	Checks if string field value is present in specified list of comma separated values	<field> IN <value>
Example: resourcegroupname = BCP1 and accountname in TG2277,TG2207		
NOT IN	Checks if string field value is present in specified list of comma separated values	<field> NOT IN <value>
Example: resourcegroupname = BCP1 and accountname not in TG2277,TG2207		
MAX	Provides the MAX value for specified field Note: MAX Operator should be used with following commands: TOP, RARE, STATS and BUBBLECHART	MAX(<field>)
Examples: STATS MAX(bytesout) by ipaddress accountname; resourcegroupname = Email_sent_to_Users BUBBLECHART MAX(bytesout) ipaddress accountname; resourcegroupname = Email_sent_to_Users TOP MAX(bytesout) ipaddress employeeid; resourcegroupname = Email_sent_to_Users RARE MAX(bytesout) ipaddress employeeid		
SUM	Provides the aggregated SUM value for specified field Note: SUM Operator should be used with following commands: TOP, RARE, STATS and BUBBLECHART	SUM(<field>)
Examples: STATS SUM(bytesout) by ipaddress accountname; resourcegroupname = Email_sent_to_Users BUBBLECHART SUM(bytesout) ipaddress accountname; resourcegroupname = Email_sent_to_Users TOP SUM(bytesout) ipaddress employeeid; resourcegroupname = Email_sent_to_Users RARE SUM(bytesout) ipaddress employeeid		

Command		Syntax
AVG	Provides the AVG value for specified field Note: AVG Operator should be used with following commands: TOP, RARE, STATS and BUBBLECHART	AVG(<field>)
Examples: STATS AVG(bytesout) by ipaddress accountname; resourcegroupname = Email_sent_to_Users BUBBLECHART AVG(bytesout) ipaddress accountname; resourcegroupname = Email_sent_to_Users TOP AVG(bytesout) ipaddress employeeid; resourcegroupname = Email_sent_to_Users RARE AVG(bytesout) ipaddress employeeid		
ENDS WITH	Checks if string field value ends with specified value	<field> ENDS WITH <value>
Example: resourcegroupname = BCP1 and accountname ENDS WITH curonix		
NOT ENDS WITH	Checks if string field value does not end with specified value	<field> NOT ENDS WITH <value>
Example: resourcegroupname = BCP1 and accountname NOT ENDS WITH curonix		
=	Finds value that equals operator, tests quality	<field> <=> <value>
Example: resourcegroupname = BCP1		
!=	Finds value that does not equal operator, tests if field is not equal to value	<field> <!=> <value>
Example: resourcegroupname != BCP1		
>	Checks if a numerical field is greater than the specified value	<field> > <value>
Example: resourcegroupname = BCP1 and bytesOut > 200		
<	Checks if a numerical field is less than the specified value	<field> < <value>
Example: resourcegroupname = BCP1 and bytesOut < 200		

Command		Syntax
<=	Less than or equal to	<field> <= <value>
Example: resourcegroupname = BCP1 AND year <= 2017		
>=	Greater than or equal to	<field> >= <value>
Example: resourcegroupname = BCP1 AND year >= 2017		
PCR	<p>Finds changes in traffic flows that indicate exfiltration.</p> <p>Notes:</p> <p>Analysis Techniques: Identify changes in host roles, and investigate. PCR is a normalized metric of traffic ratios and from a host ranging from -1 to 1.</p> $\text{PCR} = (\text{bytesin} - \text{bytesout}) / (\text{bytesin} + \text{bytesout})$ <p>PCR host role:</p> <ul style="list-style-type: none"> • 1.0 pure push - FTP upload, multicast, beaconing • 0.4 70:30 export - Sending Email • 0.0 Balanced Exchange - NTP, ARP probe • -0.5 3:1 import - HTTP Browsing • -1.0 pure pull - HTTP Download <p>DNS is less noisy than HTTP for this metric, and is a possible exfil channel. A positive shift in PCR for DNS traffic may indicate DNS Exfil.</p>	PCR(field1,field2)

Command	Syntax
Examples: TOP PCR(bytesin, bytesout) ipaddress accountname; resourcegroupname = Email_sent_to_Users BUBBLECHART PCR(bytesin, bytesout) ipaddress accountname; resourcegroupname = Email_sent_to_Users BARCHART PCR(bytesin, bytesout) ipaddress accountname; resourcegroupname = Email_sent_to_Users TIMECHART weekly PCR(bytesin, bytesout) ipaddress accountname	

Filter Command

Command	Description	Syntax
FILTER	Query on query on different Solr cores such as: activity, violation, watchlist, riskscore , riskscore-history, users, lookup, geo-location, etc.	Index = <watchlist> <and or> <field> Report Commands Field Commands
Examples: resourcegroupname = BCP1 Filter index = watchlist; WATCHLIST : Filter index = watchlist and entityname = accountname; LOOKUP : Filter index = lookup and value_value2 = accountname; RISKSCORE: FILTER index = riskscore and violator = violator; TPI: Filter index = tpi and tpi_addr = entityid and tpi_criticality = high; ASSET: Filter index = asset and entityname = TG2207;		

Global Search Command

Command	Description	Syntax
Varies (see examples)	Perform a Global Search different cores	index = <core name> <and or> <field> = <field value>
Examples: firstname = Ulla; Activity Core : firstname = Ulla; Violation Core : index = violation and firstname = Ulla; Riskscore Core : index = riskscore and accountname = 1073; Riskscore History Core : index = riskscorehistory and companycode = BBM; TPI Core : index = tpi; Asset Core : index = asset and entityname = sankethApple; Lookup Core : index = lookup and lookupname = test-mar100538; Geolocation Core : index = geolocation and longitude = 5.3735; Watchlist Core : index = watchlist and type = Users; Users Core : index = users and city = DEDHAM		

Field Commands

Command	Description	Syntax
RENAME	Rename the source field to destination field	RENAME < field1> <as> <field2>
Example: Resourcegroupname = BCP1 RENAME ipaddress as hostaddress		
TABLE	Display the specified fields in table format and fields separated by ","(comma)	TABLE <field1><,><field2><,>...<field N>
Examples: resourcegroupname = BCP1 TABLE ipaddress; Multiple Attributes: TABLE ipaddress , accountname, accountstatus		
FIELDS	Display or remove the specified fields from the Results. "+" displays only specified fields."-" removes the specified fields from results.	FIELDS < + or - > <field1><,><field2><,>...<field N>
Examples: resourcegroupname = BCP1 FIELDS + ipaddress; +: FIELDS + ipaddress , accountname; -: FIELDS - ipaddress , accountname		
HEAD	Returns filtered results based on the condition Note: MHEAD Operator should be used with following commands: TOP, RARE, STATS and BUBBLECHART	HEAD <number>
Examples: HEAD 10; With Top: resourcegroupname = OKTA top accountname HEAD 10; With STATS: resourcegroupname = OKTA STATS accountname HEAD 10; With BARCHART: resourcegroupname = OKTA BARCHART accountname HEAD 10		
DELETE	Delete specific events	DELETE <field1 = value> ...<field N = value>
Example: Resourcegroupname = BCP1 DELETE ipaddress = 182.74.60.19 ... DELETE ipaddress = 182.74.60.19 accountname = TG2277		

Command	Description	Syntax
WHERE	Returns filtered results based on the condition Note: WHERE command should be used with the following Operators: > Greater than, >= Greater than or equal to, < Less than, <= Less than or equal to	WHERE <count> <=> <number>
Examples: where count > 10; With Top - resourcegroupname = OKTA top accountname WHERE count > 35; With Top & ORDERBY - resourcegroupname = OKTA top accountname WHERE count > 35 ORDERBY asc; With STATS: resourcegroupname = OKTA stats accountname WHERE count > 35; With STATS & ORDERBY: resourcegroupname = OKTA STATS accountname transactionstring1 WHERE count > 0 ORDERBY desc; With BARCHART: resourcegroupname = OKTA BARCHART accountname ipaddress WHERE count > 5		
GEOLOOKUP	Extract location information such as city, country, latitude, and longitude, based on IP address	GEOLOOKUP <field>
Example: Resourcegroupname = BCP1 GEOLOOKUP ipaddress		
ORDERBY	Sort events by ascending or descending or field. Default asc or desc will sort events by count Note: ORDERBY command should be used with the following commands: TOP, RARE and STATS	ORDERBY <asc or desc or <field asc or desc>>
Examples: ORDERBY asc; Sort Events Descending order: resourcegroupname = Google_Login STATS count by ipaddress firstname ORDERBY desc; Sort Field By Ascending order: resourcegroupname = Google_Login STATS count by ipaddress firstname ORDERBY firstname asc; Sort Field By Descending order: resourcegroupname = Google_Login STATS count by ipaddress firstname ORDERBY ipaddress desc		

Additional Search Examples

Description	Syntax
Get top risk users, activity accounts, activity IP addresses, and resources	Index=riskscore <and> <violation> = <Users Activityip Activityaccount Resources> <top> <violation ID>
Examples: index=riskscore top violatorid; Top Risk Users : index=riskscore and violator= Users top violatorid; Top Activityaccount : index=riskscore and violator= Activityaccount top violatorid; Top Activityip : index=riskscore and violator= Activityip top violatorid; Top Resources : index=riskscore and violator= Activityip top violatorid	
Get flight risk users	Index=riskscore <and> <violation> = <Users> <Filter> <index> <=> <watchlist> <and> <field 1> <=> <field 2>
Example: index=riskscore and violator = Users Filter index = watchlist and entityname = violatorid	
Check if IP address is malicious	Index=riskscore <and> <violation> = <Activityip> <Filter> <index> <=> <tpi> <and> <field 1> <=> <field 2> and <field 3> <=> <field 4>
Examples: Index=riskscore and violator = Activityip Filter; index = tpi and addr = entityid and criticality = high	
Get information about assets on the network	Index = asset <and> <field 1> = <field 2>
Example: Resourcegroupname = BCP1 index = asset and entityname = accountname	
Check if user has sent email to personal email address	resourcegroupname = <value> EVAL X = emailto self (firstname,workemail,0.4)
Examples: resourcegroupname = "ADEvents" EVAL matchPerc = emailto self (firstname,workemail,0.4); resourcegroupname = "ADEvents" eval x = SUBSTRBYINDEX (workemail , "@", "1")	

Reporting Operators

Reporting Commands

Command	Description	Syntax
DISTVALUE	<p>Provides the distinct value group by the field name (ex : firstname)</p> <p>Note: DISTVALUE will calculate the distinct count by the grouped attribute. Example 1: polycname = "IEE for Google login" DISTVALUE ipaddress by accountname, will group the data by the last attribute [accountname] in query. Example 2: polycname = "IEE for Google login" DISTVALUE ipaddress transactionstring1 firstname OR polycname = "IEE for Google login" DISTVALUE ipaddress transactionstring1 by firstname, will group the data by the last attribute [firstname] in query.</p>	DISTVALUE <field1> <by> <field 2> <field N>
Examples: resourcegroupname = Google_login DISTVALUE ipaddress by accountname; resourcegroupname = Google_login DISTVALUE ipaddress transactionstring1 by firstname		
GEOMAP	Displays the events in a GEOMAP	GEOMAP < field 1> <field2> <field-n>
Examples: GEOMAP latitude longitude addr; Activity : resourcegroupname = BCP1 GEOMAP latitude longitude ipaddress; Violation : polycname = Logon_Failure GEOMAP eventlatitude eventlongitude ipaddress; Index : index = tpi GEOMAP tpi_latitude tpi_longitude tpi_addr; GEOLOOKUP: resourcegroupname = BCP1 GEOLOOKUP ipaddress GEOMAP latitude longitude ipaddress; Group By: resourcegroupname = BCP1 GEOMAP eventlatitude eventlongitude ipaddress by eventregion		
BUBBLECHART	Shows a type of chart that displays three dimensions of data (x, y, z)	BUBBLECHART <field1> <count> <by> <field2> <field N>
Examples: resourcegroupname = BCP1 BUBBLECHART ipaddress; STACKED: BUBBLECHART ipaddress by accountid; COUNT: BUBBLECHART count by ipaddress; STACKED with COUNT: BUBBLECHART ipaddress by accountid		
BARChart	Represents grouped data with rectangular bars with lengths proportionate to the values they represent	BARChart <field1> <count> <by> <field2> <field N>

Command	Description	Syntax
Examples: resourcegroupname = BCP1 BARCHART ipaddress; STACKED: BARCHART ipaddress by accountname; GROUP: BARCHART ipaddress accountname; COUNT: BARCHART count by ipaddress; STACKED with COUNT: BARCHART count by ipaddress accountname		
TIMECHART	Displays the data for field(s) in a time series	TIMECHART <hourly daily weekly monthly> <count by> <field 1> <by> <field 2> ... <field N>
Examples: resourcegroupname = BCP1 TIMECHART hourly ipaddress; STACKED: TIMECHART ipaddress by accountname; COUNT: TIMECHART hourly count by ipaddress accountid; STACKED with COUNT: TIMECHART weekly count by ipaddress by accountid; GROUP: TIMECHART hourly count by ipaddress by accountid accountname		
SPAN	Filters group information within a specified time span. Notes: Duration: dur = <ol style="list-style-type: none"> 1. Seconds - s, sec, second, seconds. 2. Minutes - m, min, minute, minutes 3. Hours - h, hr, hour, hours 4. Days - d, day, days 5. Month - mon, month, months 	SPAN dur= (sec min hours days months) (field 1)..(field N)
Examples: SPAN dur = 5min ipaddress accountname; resourcegroupname = Email_sent_to_Users SPAN dur = 5min ipaddress accountname; policyname = afterhours SPAN dur = 5min ipaddress accountname		
DISTCOUNT	Used to return only distinct (different) values	DISTCOUNT <field 1> <by> <field 2> <field N>
Examples: resourcegroupname = BCP1 DISTCOUNT ipaddress; STACKED: DISTCOUNT ipaddress by accountname; GROUP: DISTCOUNT ipaddress accountid; STACKED with GROUP: DISTCOUNT ipaddress by accountname accountstatus		

Analytical Operators

Reporting Commands

Command		Syntax
RARE	Displays the least common values of a field(s). Use this limit to restrict the number of displayed events	RARE <limit = constant> <field 1> <by> <field 2> <field N>
Examples: resourcegroupname = BCP1 RARE ipaddress; STACKED: RARE ipaddress by accountname; GROUP: RARE ipaddress accountname; LIMIT: RARE limit =5 ipaddress; STACKED with LIMIT: RARE limit =5 ipaddress accountid		
TOP	Displays the most common values of a field. Use this limit to restrict the number of displayed events	TOP <limit = constant> <field 1> <by> <field 2> <field N>
Examples: resourcegroupname = BCP1 TOP ipaddress; STACKED: TOP ipaddress by accountname; GROUP: TOP ipaddress accountname; LIMIT: TOP limit =5 ipaddress; STACKED with LIMIT: TOP limit =5 ipaddress accountid		
STATS	Provides statistics for the search field	STATS < field count> <by> <field>
Examples: resourcegroupname = BCP1 STATS ipaddress; STACKED BY: STATS ipaddress by accountname; COUNT BY: STATS count by ipaddress accountname		
LINK	Provide the Graphical tools for organizing and representing events	LINK < field 1> <field2> <field-n>
Examples: LINK emailsender filename emailrecipient; Activity: resourcegroupname = BCP1 LINK ipaddress accountname filename; Violation: policyname = Logon_Failure LINK ipaddress accountname filename		

Eval Commands

Command	Description	Syntax
DEC	Returns the decimal value	EVAL (store-field) = (DEC) (field)
Examples: resourcegroupname = BCP1 EVAL x = DEC (bytesin); resourcegroupname = Email_sent_to_Users EVAL x = DEC (bytesin) EVAL y = HEX(x)		
EQUALS	Returns true is value matches. Returns false if value does not match	EVAL <store-field> = <EQUALS> < field > < field-value >
Examples: resourcegroupname = BCP1 EVAL x = EQUALS (accountname , 2029); LEN: EVAL x = LEN (accountname) EVAL y = EQUALS (x , 6); UPPERCASE: EVAL x = UPPERCASE (accountname) EVAL y = EQUALS (x , TG2277); LOWERCASE : EVAL x = LOWERCASE (accountname) EVAL y = EQUALS (x , tg2277); REPLACE: EVAL x = REPLACE (accountname ,TG2277 , securonix) EVAL y = EQUALS (x , securonix); SUBSTR: EVAL x = SUBSTR (accountname , 0 , 2) EVAL y = EQUALS (x , TG); ISBOOLEAN: EVAL x = ISBOOLEAN (bytesout) EVAL y = EQUALS (x , false); ISNOTNULL: EVAL x = ISNOTNULL (resourcegroupid) EVAL y = EQUALS (x , true); ISNULL: EVAL x = ISNULL (accountname) EVAL y = EQUALS (x , false); ISSTRING : EVAL x = ISSTRING (accountname) EVAL y = EQUALS (x , true); ISNUM : EVAL x = ISNUM (accountname) EVAL y = EQUALS (x , true); ISINT: EVAL x = ISINT (id) EVAL y = EQUALS (x , true); SDIGIT: EVAL x = ISDIGIT (id) EVAL y = EQUALS (x , true)		
ISDIGIT	Returns true if the value is a digit. Returns false if value is not a digit	EVAL <store-field> = <ISDIGIT> < field >
Examples: resourcegroupname = BCP1 EVAL x = ISDIGIT (accountname); LEN: EVAL x = LEN (resourcegroupid) EVAL y = ISDIGIT (x); REPLACE: EVAL x = REPLACE (accountname , - , 1) EVAL y = ISDIGIT (x); SUBSTR: EVAL x = SUBSTR (accountname , 0 , 1) EVAL y = ISDIGIT (x)		
to_unixtime	Returns epoch time from a valid date string	EVAL <store-field> = <to_unix-time> < field Valid String >
Examples: EVAL x = to_unixtime (04/27/2017 15:03:49); EVAL x = to_unixtime (dt_firstseen)		
UNBASE64	Returns the base64 decoding value	EVAL (store-field) = (UNBASE64) (field)
Examples: resourcegroupname = BCP1 EVAL x = UNBASE64 (bytesin); resourcegroupname = Email_sent_to_Users EVAL x = BASE64 (bytesin) EVAL y = UNBASE64(x)		

Command	Description	Syntax
ISINT	Returns true if value is an integer. Returns false if value is not an integer	EVAL <store-field> = <ISINT> <field>
Examples: resourcegroupname = BCP1 EVAL x = ISINT (accountname); LEN: EVAL x = LEN (accountname) EVAL y = ISINT (x); UPPERCASE: EVAL x = UPPERCASE (accountname) EVAL y = ISINT (x); LOWERCASE: EVAL x = LOWERCASE (accountname) EVAL y = ISINT (x); REPLACE: EVAL x = REPLACE (accountname ,TG2277 , securonix) EVAL y = ISINT (x); SUBSTR: EVAL x = SUBSTR (accountname , 0 , 2) EVAL y = ISINT (x)		
ISNOTNULL	Returns true if value is not null. Returns false if value is null	EVAL <store-field> = <ISNOTNULL> <field>
Examples: resourcegroupname = BCP1 EVAL x = ISNOTNULL (accountname); LEN: EVAL x = LEN (accountname) EVAL y = ISNOTNULL (x); UPPERCASE: EVAL x = UPPERCASE (accountname) EVAL y = ISNOTNULL (x); LOWERCASE: EVAL x = LOWERCASE (accountname) EVAL y = ISNOTNULL (x); EQUALS: EVAL x = EQUALS (accountname , -) EVAL y = ISNOTNULL (x); REPLACE: EVAL x = REPLACE (accountname , - , securonix) EVAL y = ISNOTNULL (x); SUBSTR: EVAL x = SUBSTR (accountname , 0 , 5) EVAL y = ISNOTNULL (x); ISBOOLEAN: EVAL x = ISBOOLEAN (bytesout) EVAL y = ISNOTNULL (x); ISSTRING: EVAL x = ISSTRING (accountname) EVAL y = ISNOTNULL (x); ISNUM: EVAL x = ISNUM (accountname) EVAL y = ISNOTNULL (x); ISEMPY: EVAL x = ISEMPY (accountname) EVAL y = ISNOTNULL (x)		
ISBOOLEAN	Returns true or false if field is Boolean	EVAL <store-field> = <ISBOOLEAN> <field>
Examples: resourcegroupname = BCP1 EVAL x = ISBOOLEAN (accountname); LEN: EVAL x = LEN (accountname) EVAL y = ISBOOLEAN (x); UPPERCASE: EVAL x = UPPERCASE (accountname) EVAL y = ISBOOLEAN (x); LOWERCASE: EVAL x = LOWERCASE (accountname) EVAL y = ISBOOLEAN (x); REPLACE: EVAL x = REPLACE (accountname ,TG2277 , securonix) EVAL y = ISBOOLEAN (x); SUBSTR: EVAL x = SUBSTR (accountname , 0 , 2) EVAL y = ISBOOLEAN (x); ISNOTNULL: EVAL x = ISNOTNULL (resourcegroupid) EVAL y = ISBOOLEAN (x); ISNULL: EVAL x = ISNULL (accountname) EVAL y = ISBOOLEAN (x); ISSTRING: EVAL x = ISSTRING (accountname) EVAL y = ISBOOLEAN (x); EQUALS: EVAL x = EQUALS (accountname , securonix) EVAL y = ISBOOLEAN (x)		

Command	Description	Syntax
from_unixtime	Returns Valid date String from an epoch time	EVAL <store-field> = <from_unixtime> < field > < date format >
Example: EVAL x = from_unixtime (eventtime , MM/dd/yyyy HH:mm:ss)		
LEN	Find length of field value	EVAL <store-field> = <LEN> < field >
Examples: resourcegroupname = BCP1 EVAL x = LEN (accountname); LOWERCASE: EVAL y = LOWERCASE (accountname) EVAL x = LEN (y); UPPERCASE: EVAL y = UPPERCASE (accountname) EVAL x = LEN (y); ISEMPTY: EVAL x = LEN (accountname) EVAL y = ISEMPTY (accountname); REPLACE: EVAL y = REPLACE (accountname , - , securonix) EVAL x = LEN (y); SUBSTR: EVAL z = REPLACE (accountname , - , securonix) EVAL y = SUBSTR (z , 0 , 5) EVAL x = LEN (y); ISBOOLEAN: EVAL x = LEN (resourcegroupid) EVAL y = ISBOOLEAN (x); ISINT: EVAL x = LEN (resourcegroupid) EVAL y = ISINT (x); ISNOTNULL: EVAL x = LEN (resourcegroupid) EVAL y = ISNOTNULL (x); ISNULL: EVAL x = LEN (resourcegroupid) EVAL x = ISNULL (x); ISDIGIT: EVAL x = LEN (resourcegroupid) EVAL y = ISDIGIT (x); EQUALS: EVAL x = LEN (accountname) EVAL y = EQUALS (x , 5)		
BASE64	Returns the base64 encoding value	EVAL (store-field) = (BASE64) (field)
Examples: resourcegroupname = BCP1 EVAL x = BASE64 (bytesin); Example 1: resourcegroupname = Email_sent_to_Users EVAL x = BASE64 (bytesin) EVAL y = UNBASE64(x)		
ISNUM	Returns true is the value is a number. Returns false is value is not a number	EVAL <store-field> = <ISNUM> < field >
Examples: resourcegroupname = BCP1 EVAL x = ISNUM (accountname); LEN: EVAL x = LEN (accountname) EVAL y = ISNUM (x); UPPERCASE: EVAL x = UPPERCASE (accountname) EVAL y = ISNUM (x); LOWERCASE: EVAL x = LOWERCASE (accountname) EVAL y = ISNUM (x); EQUALS: VAL x = EQUALS (accountname , -) EVAL y = ISNUM (x); REPLACE: EVAL x = REPLACE (accountname , - , securonix) EVAL y = ISNUM (x); SUBSTR: EVAL x = SUBSTR (accountname , 0 , 5) EVAL y = ISNUM (x)		
UPPERCASE	Converts all characters to uppercase	EVAL <store-field> = <UPPERCASE> < field >

Command	Description	Syntax
Examples: resourcegroupname = BCP1 EVAL x = UPPERCASE (accountname); LEN: EVAL x = UPPERCASE (accountname) EVAL y = LEN (x); LOWERCASE: EVAL x = UPPERCASE (accountname) EVAL y = LOWERCASE (x); ISEMPTY: EVAL x = UPPERCASE (accountname) EVAL y = ISEMPTY (x); EQUALS: EVAL y = UPPERCASE (accountname) EVAL x = EQUALS (y , -); REPLACE : EVAL x = UPPERCASE (accountname) EVAL y = REPLACE (x , - , securonix); SUBSTR: EVAL y = SUBSTR (accountname , 0 , 5) EVAL x = UPPERCASE (y); ISBOOLEAN: EVAL x = UPPERCASE (resourcegroupid) EVAL y = LEN (x) EVAL x = ISBOOLEAN (y); ISNOTNULL : EVAL x = UPPERCASE (resourcegroupid) EVAL y = ISNOTNULL (x); ISNULL : EVAL x = UPPERCASE (accountname) EVAL y = ISNULL (x); ISSTRING : EVAL x = UPPERCASE (accountname) EVAL y = ISSTRING (x)		
ISSTRING	Returns true is value is string. Returns false if value is not string	EVAL <store-field> = <ISSTRING> < field >
Examples: resourcegroupname = BCP1 EVAL x = ISSTRING (accountname); LEN: EVAL x = LEN (accountname) EVAL y = ISSTRING (x); UPPERCASE: EVAL x = UPPERCASE (accountname) EVAL y = ISSTRING (x); LOWERCASE: EVAL x = LOWERCASE (accountname) EVAL y = ISSTRING (x); REPLACE: EVAL x = REPLACE (accountname , - , securonix) EVAL y = ISSTRING (x); SUBSTR: EVAL x = SUBSTR (accountname , 0 , 5) EVAL y = ISSTRING (x)		
ISNULL	Returns true if value is null. Returns false is value is not null	EVAL <store-field> = <ISNULL> < field >
Examples: resourcegroupname = BCP1 EVAL x = ISNULL (accountname); LEN: EVAL x = LEN (accountname) EVAL y = ISNULL (x); UPPERCASE: EVAL x = UPPERCASE (accountname) EVAL y = ISNULL (x); LOWERCASE: EVAL x = LOWERCASE (accountname) EVAL y = ISNULL (x); EQUALS: EVAL x = EQUALS (accountname , -) EVAL y = ISNULL (x); REPLACE: EVAL x = REPLACE (accountname , - , securonix) EVAL y = ISNULL (x); SUBSTR: EVAL x = SUBSTR (accountname , 0 , 5) EVAL y = ISNULL (x); ISBOOLEAN: EVAL x = ISBOOLEAN (byte-sout) EVAL y = ISNULL (x); ISSTRING: EVAL x = ISSTRING (accountname) EVAL y = ISNULL (x); ISNUM: EVAL x = ISNUM (accountname) EVAL y = ISNULL (x); ISEMPTY: EVAL x = ISEMPTY (accountname) EVAL y = ISNULL (x)		
ISEMPTY	Returns true if value is empty. Returns false is value is not empty	EVAL <store-field> = <ISEMPTY> < field >

Command	Description	Syntax
Examples: resourcegroupname = BCP1 EVAL x = ISEMPTY (accountname); LEN: EVAL x = LEN (accountname) EVAL y = ISEMPTY (x); UPPERCASE: EVAL x = UPPERCASE (accountname) EVAL y = ISEMPTY (x); LOWERCASE: EVAL x = LOWERCASE (accountname) EVAL y = ISEMPTY (x); EQUALS: EVAL x = EQUALS (accountname , -) EVAL y = ISEMPTY (x); REPLACE: EVAL x = REPLACE (accountname , - , securonix) EVAL y = ISEMPTY (x); SUBSTR: EVAL x = SUBSTR (accountname , 0 , 5) EVAL y = ISEMPTY (x); ISBOOLEAN: EVAL x = ISBOOLEAN (bytesout) EVAL y = ISEMPTY (x); ISNOTNULL: EVAL x = ISNOTNULL (resourcegroupid) EVAL y = ISEMPTY (x); ISNULL: EVAL x = ISNULL (accountname) EVAL y = ISEMPTY (x); ISSTRING: EVAL x = ISSTRING (accountname) EVAL y = ISEMPTY (x); ISNUM: EVAL x = ISNUM (accountname) EVAL y = ISEMPTY (x)		
HEX	Returns the hexadecimal value	EVAL (store-field) = (HEX) (field)
Examples: resourcegroupname = BCP1 EVAL x = HEX (bytesin); Example 1: resourcegroupname = Email_sent_to_Users EVAL x = DEC (bytesin) EVAL y = HEX(x)		
LOWERCASE	Converts all characters to lower-case	EVAL <store-field> = <LOWERCASE> < field >
Examples: resourcegroupname = BCP1 EVAL x = LOWERCASE (accountname); LEN: EVAL x = LOWERCASE (accountname) EVAL y = LEN (x); UPPERCASE: EVAL x = UPPERCASE (accountname) EVAL y = LOWERCASE (x); ISEMPTY: EVAL x = LOWERCASE (accountname) EVAL y = ISEMPTY (x); EQUALS: EVAL y = LOWERCASE (accountname) EVAL x = EQUALS (y , -); REPLACE: EVAL x = LOWERCASE (accountname) EVAL y = REPLACE (x , - , securonix); SUBSTR: EVAL y = SUBSTR (accountname , 0 , 5) EVAL x = LOWERCASE (y); ISBOOLEAN: EVAL x = LOWERCASE (resourcegroupid) EVAL y = LEN (x) EVAL x = ISBOOLEAN (y); ISNOTNULL: EVAL x = LOWERCASE (resourcegroupid) EVAL y = ISNOTNULL (x); ISNULL: EVAL x = LOWERCASE (accountname) EVAL y = ISNULL (x); ISSTRING: EVAL x = LOWERCASE (accountname) EVAL y = ISSTRING (x)		
REPLACE	Returns a string after replacing all occurrences	EVAL <store-field> = <REPLACE> < field > < field-value > <replace-value>

Command	Description	Syntax
Examples: resourcegroupname = BCP1 EVAL x = REPLACE (accountname ,TG2277 , securonix); LEN: EVAL x = REPLACE (accountname ,TG2277 , securonix) EVAL y = LEN (x); UPPERCASE: EVAL x = REPLACE (accountname ,TG2277 , securonix) EVAL y = UPPERCASE (x); LOWERCASE: EVAL x = REPLACE (accountname ,TG2277 , SECURONIX) EVAL y = LOWERCASE (x); EQUALS: EVAL x = REPLACE (accountname ,TG2277 , securonix) EVAL y = EQUALS (x , securonix); SUBSTR: EVAL x = REPLACE (accountname ,TG2277 , securonix) EVAL y = SUBSTR (x , 0 , 2); ISBOOLEAN: EVAL x = REPLACE (accountname ,TG2277 , securonix) EVAL y = ISBOOLEAN (x); ISNOTNULL: EVAL x = REPLACE (accountname ,TG2277 , securonix) EVAL y = ISNOTNULL (x); ISNULL: EVAL x = REPLACE (accountname ,TG2277 , securonix) EVAL y = ISNULL (x); ISSTRING: EVAL x = REPLACE (accountname ,TG2277 , securonix) EVAL y = ISSTRING (x); ISNUM: EVAL x = REPLACE (accountname ,TG2277 , 123) EVAL y = ISNUM (x); ISINT: EVAL x = REPLACE (accountname ,TG2277 , 123) EVAL y = ISINT (x); ISDIGIT: EVAL x = REPLACE (accountname ,TG2277 , 7) EVAL y = ISDIGIT (x)		
SUBSTR	Returns substring of actual field value	EVAL <store-field> = <SUBSTR> < field > < start-position > <endposition>
Examples: EVAL x = SUBSTR (accountname , 0 , 5); REPLACE: EVAL x = REPLACE (accountname ,TG2277 , securonix) EVAL y = SUBSTR (x , 0 , 3); LEN: EVAL x = SUBSTR (accountname , 0 , 3) EVAL y = LEN (x); UPPERCASE: EVAL x = SUBSTR (accountname , 0 , 3) EVAL y = UPPERCASE (x); LOWERCASE: EVAL x = SUBSTR (accountname , 0 , 3) EVAL y = LOWERCASE (x); EQUALS: EVAL x = SUBSTR (accountname , 0 , 3) EVAL y = EQUALS (x , TG2); ISBOOLEAN: EVAL x = SUBSTR (accountname , 0 , 3) EVAL y = EQUALS (x , TG2) EVAL z = ISBOOLEAN (y); ISNOTNULL: EVAL x = SUBSTR (accountname , 0 , 3) EVAL y = ISNOTNULL (x); ISNULL: EVAL x = SUBSTR (accountname , 0 , 3) EVAL y = ISNULL (x); ISSTRING: EVAL x = SUBSTR (accountname , 0 , 3) EVAL y = ISSTRING (x); ISNUM: EVAL x = SUBSTR (accountname , 0 , 3) EVAL y = ISNUM (x); ISINT: EVAL x = SUBSTR (accountname , 0 , 3) EVAL y = ISINT (x); ISDIGIT: EVAL x = SUBSTR (accountname , 0 , 3) EVAL y = ISDIGIT (x);		
SUBSTRBYINDEX	Returns substring of actual field value by index	EVAL <store-field> = <SUBSTRBYINDEX> < field > < delimiter > <An integer indicating the number of occurrences of delimiter>

Command	Description	Syntax
Examples: EVAL x = SUBSTRBYINDEX (workemail , @, 1); REPLACE: EVAL x = REPLACE (workemail ,TG2277 , securonix) EVAL y = SUBSTRBYINDEX (x , @, 1); LEN: EVAL x = SUBSTRBYINDEX (workemail , @, 1) EVAL y = LEN (x); UPPERCASE: EVAL x = SUBSTRBYINDEX (workemail , @, 1) EVAL y = UPPERCASE (x); LOWERCASE: EVAL x = SUBSTRBYINDEX (workemail , @, 1) EVAL y = LOWERCASE (x); EQUALS: EVAL x = SUBSTRBYINDEX (workemail , @, 1) EVAL y = EQUALS (x , TG2); ISBOOLEAN: EVAL x = SUBSTRBYINDEX (workemail , @, 1) EVAL y = EQUALS (x , TG2) EVAL z = ISBOOLEAN (y); ISNOTNULL: EVAL x = SUBSTRBYINDEX (workemail , @, 1) EVAL y = ISNOTNULL (x); ISNULL: EVAL x = SUBSTRBYINDEX (workemail , @, 1) EVAL y = ISNULL (x); ISSTRING: EVAL x = SUBSTRBYINDEX (workemail , @, 1) EVAL y = ISSTRING (x); ISNUM: EVAL x = SUBSTRBYINDEX (workemail , @, 1) EVAL y = ISNUM (x); ISINT: EVAL x = SUBSTRBYINDEX (workemail , @, 1) EVAL y = ISINT (x); ISDIGIT: EVAL x = SUBSTRBYINDEX (workemail , @, 1) EVAL y = ISDIGIT (x);		

Incident Management

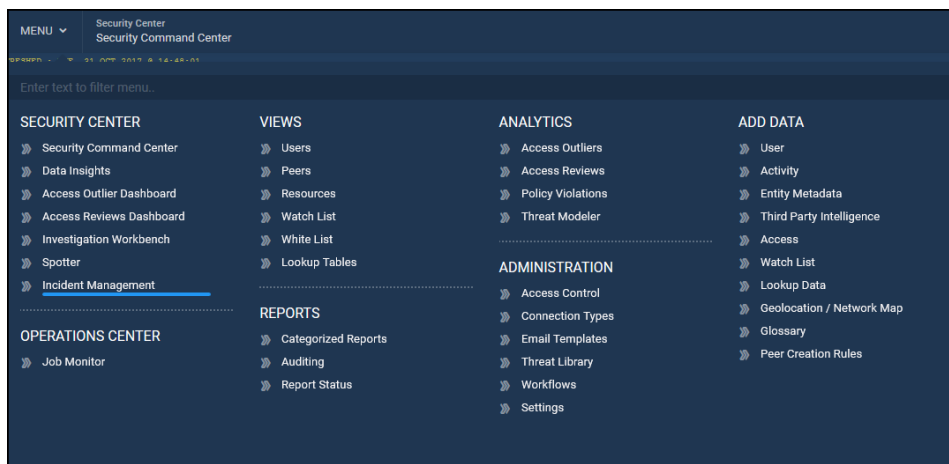
ArcSight UBA includes comprehensive case management capabilities that allow multiple teams to collaborate on investigation and incident response. You can manage and collaborate on cases from Incident Management dashboard.

Managing Cases

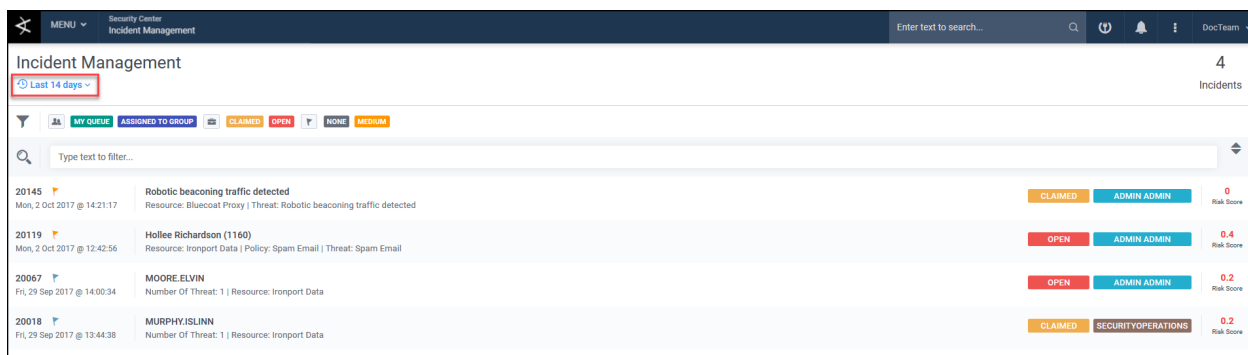
Manage cases from the Incident Management dashboard.

Incident Management Dashboard

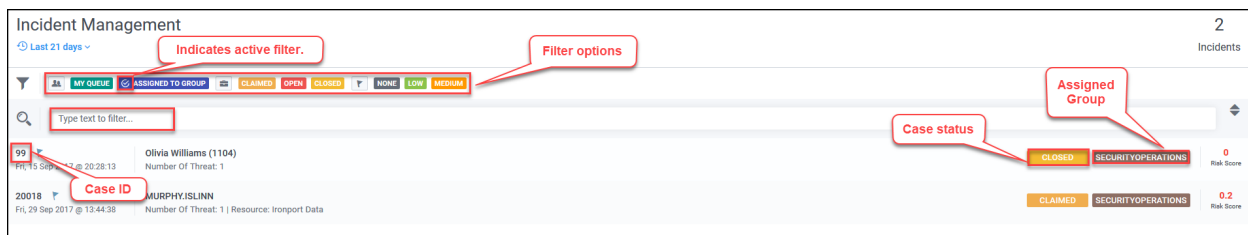
To access case management from the Incident Management Dashboard, navigate to **Menu > Security Center > Incident Management**.



You will see the cases for the last 24 hours by default. Click the time range indicator to change the time range.



You can take the following actions from the Incident Management dashboard:

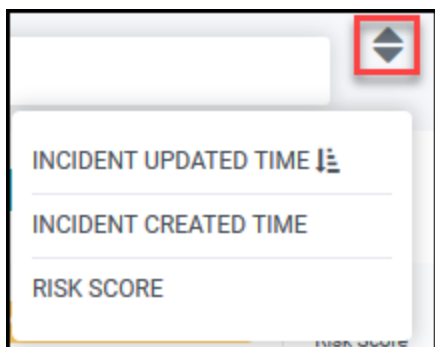


- View the list of cases for the specified time range.
- Click to filter the list of cases by the following options:
 - Current user's queue
 - Assigned to current user's group
 - Case Status
 - Criticality



Note: A check mark appears on active filters.

- Click active filters to remove the filter.
- Type text to filter results.
- Sort list by the following options:



- Incident Updated Time
- Incident Created Time
- Risk Score
- Click the case you want to manage.

The Case Management screen appears. From this screen, you can view details and take actions on the case. The case details are categorized in the following sections of the screen:

- Case Details
- Violator Details
- Threats
- Case Related Violations/Violators
- Play Book
- Activity Stream



Note: The sections that appear for each case vary based on the violation entity and violation type.

The screenshot displays the Incident Management interface. On the left, a list of cases is shown, including 'Mara Rooney (1691)' with a risk score of 0.2. The main panel shows details for Case ID 23, which is 'CLAIMED'. The interface includes a top navigation bar with 'Incidents' and '8' incidents. A sidebar on the left has filters like 'MY QUEUE', 'ASSIGNED TO GROUP', 'CLAIMED', and 'OPEN'. The main content area has a 'VIOLATOR DETAILS' section with fields for First Name, Last Name, Employee ID, Department, Division, and Email. Below this is a 'THREATS' section showing a threat named 'LANDSPEED VIOLATION DETECTED' with a risk score of 0.2. Red callouts point to various UI elements: 'Click to close list of cases' (top left), 'Available actions' (top right), 'Click to close incident' (top right), 'Details about the violation entity' (middle right), and 'Threats associated with this case' (bottom right).

Viewing Case Details

Case Details

View details about the case and take action on the case. The actions you can take from this section are based on the actions defined in the workflow that was assigned to the case. For each action you select, enter comments to explain or justify the action. See [Taking Actions on Cases](#) for more information about the actions you can take from this screen.

The screenshot shows the 'Case Details' section for Case ID 23. It includes a top bar with 'CASE ID : 23' and 'CLAIMED' status. Below this, it shows 'CREATED BY : ADMIN ADMIN' and 'ASSIGNED TO : ADMIN ADMIN'. A sidebar on the left has a 'VIEW' button. The main content area has a 'VIOLATOR DETAILS' section with fields for First Name, Last Name, Employee ID, Department, Division, and Email. Below this is a 'THREATS' section showing a threat named 'LANDSPEED VIOLATION DETECTED' with a risk score of 0.2. Red callouts point to various UI elements: 'View case status' (top right), 'View case details' (middle right), and 'Take actions on the case' (bottom right).

Violator Details

View details about the violation entity, or the threat or policy on which the case was created. Entities can be users, activity accounts, resources, and network addresses.





Note: The details that appear in this section vary based on the type of entity and disposition of the case.

VIOLATOR DETAILS			
RESOURCE NAME DALWIN32.SCNX.COM	RESOURCEGROUP NAME WINDOWS DATA	RESOURCEGROUP TYPE OS	0.5 RISK SCORE

VIOLATOR DETAILS					
FIRST NAME HOLLEE	LAST NAME RICHARDSON	EMPLOYEE ID 1160	DEPARTMENT PROCESSING AND FULFILLMENT	DIVISION BUSINESS BANKING	EMAIL HOLLEE.RICHARDSON@SCNX.COM
					0.01 RISK SCORE

Threats

View the lists of threats associated with the case.

THREATS	ACTIVITY STREAM
<div>  FRI, 15 SEP 2017 @ 20:28:46 FRIDAY </div> <div> RISK SCORE: 0.2 Spam Email  </div> <div> THREAT NAME → SPAM EMAIL ACCOUNT → MINFORD.ACHEL ENTITY → MINFORD.ACHEL </div>	

Click the icon to view a Threat Summary for each threat. View the Violation Summary, Violation Events, and response Play Book.

For more information about the sections of the Threat Summary, see [Threats](#).

CASE ID : 145 OPEN

CREATED BY : ADMIN ADMIN | ASSIGNED TO : ANALYST ANALYST

ACTIONS CLAIM ASSIGN TO ANALYST ASSIGN TO SCOOPS

CREATED ON: FRI, 15 SEP 2017 @ 20:28:45 | UPDATED ON: FRI, 15 SEP 2017 @ 20:28:45 | DUE DATE: -

VIOLATOR DETAILS

ACCOUNT NAME	RESOURCE NAME	RESOURCEGROUP NAME	RESOURCEGROUP TYPE
MINFORD.ACHEL	IRONPORT DATA	IRONPORT DATA	CISCO IRONPORT EMAIL

THREATS ACTIVITY STREAM

FRI, 15 SEP 2017 @ 20:28:46 FRIDAY

RISK SCORE: 0.2 Spam Email

THREAT NAME → SPAM EMAIL | ACCOUNT → MINFORD.ACHEL | ENTITY → MINFORD.ACHEL

Spam Email

REASON

VIOLATION SUMMARY | VIOLATION EVENTS | PLAY BOOK

Advanced Cyber Threat Incident Playbook

Task #1 Demisto: Create Incident
Create a new incident in Demisto
Task not executed

Task #2 VirusTotal: Get Context
Check for IP Address in VirusTotal
Task not executed

Advanced Cyber Threat Incident Playbook
Does a lookup in VirusTotal
Creates an incident in Demisto and blocks malicious IP addresses

No tasks were executed yet for this play book on selected entity.

Case Related Violators

View the list of violators associated with the case.

CASE RELATED VIOLATORS ACTIVITY STREAM

MON, 11 SEP 2017 @ 14:15:08 MONDAY

RISK SCORE: 75.8 **Ros Lane**

EMPLOYEE ID → 2214 | DEPARTMENT → SAP ADMINISTRATOR | DIVISION →

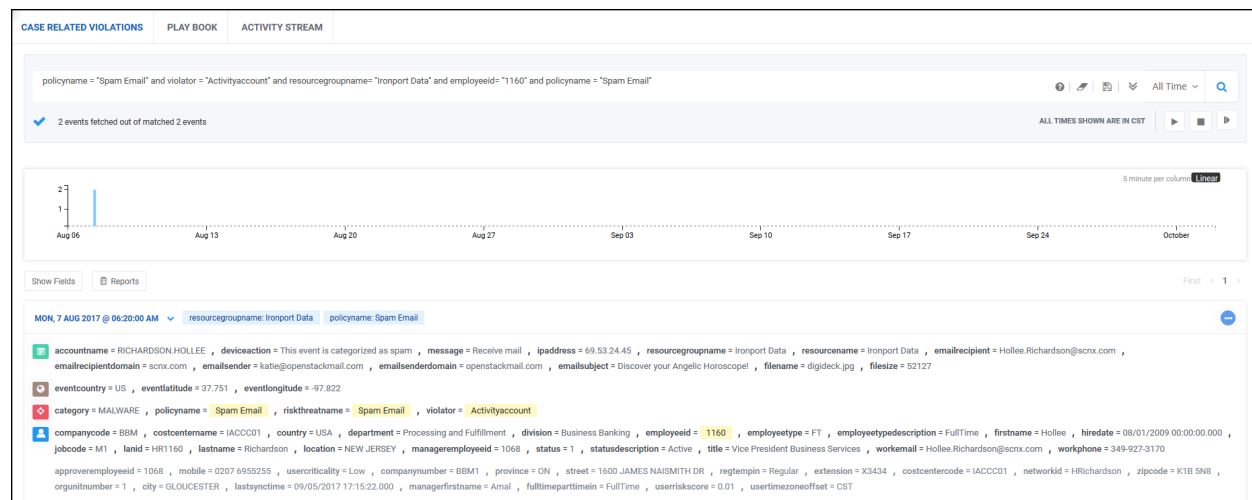
First < 1 > Last TOTAL 1

Click the icon to view the Violation Summary for each violator. View the Violation Summary, Violation Events, and response Play Book.

For more information about the sections of the Violation Summary, see [Policies](#).

Case Related Violations

View the events associated with the case. You can edit the search query to view additional information about the violation. For information on how to perform searches, see [Spotter](#).



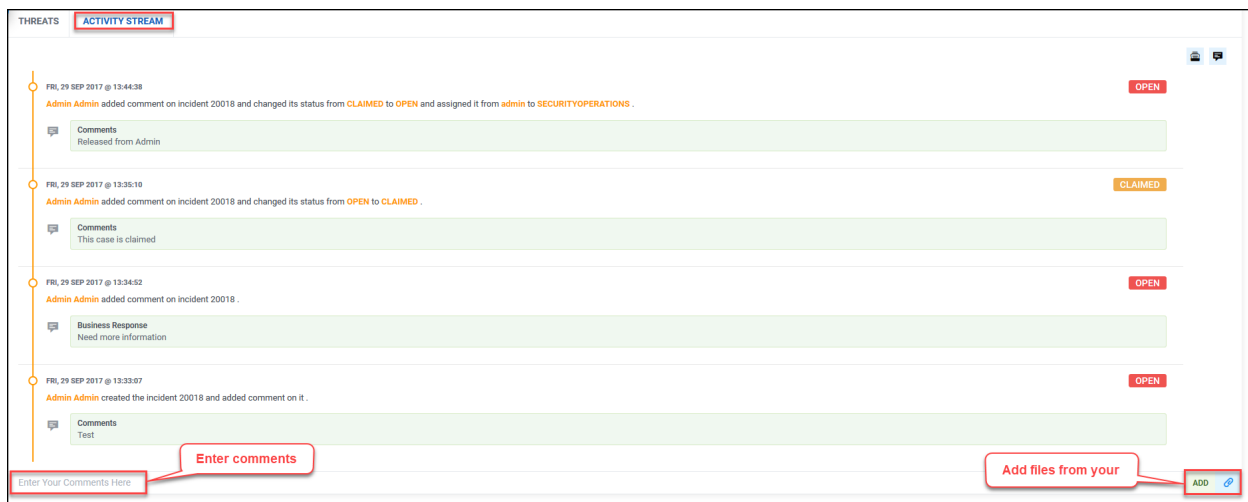
Play Book

View the play book for the violation and take specified steps to remediate the threat. For more information about Play Books in ArcSight UBA, see Response Framework.

CASE RELATED VIOLATIONS	PLAY BOOK	ACTIVITY STREAM
<p>Review if the email contain information that could be obtained from social networking websites</p> <p>Check if the email contains URL link?</p> <p>Check if the URL is suspicious here Virus Total</p> <p>Submit a ticket to block email address/IP.</p>		

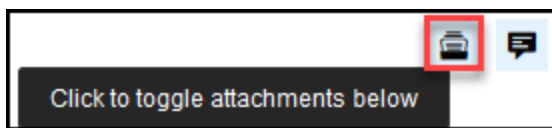
Activity Stream

The Activity Stream displays a real-time stream of case management activity for each case. From the Activity Stream, you can view activity as it happens for the case, enter comments about the case, and add files to the case from your local machine.

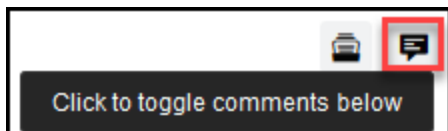


You can take the following actions from this screen:

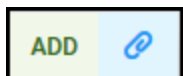
- Toggle to show or hide attachments.



- Toggle to show or hide comments.



- **Add:** Click to add files from your local machine.



Collaborating on Cases

ArcSight UBA 6.10 includes chat capability to allow analysts to easily collaborate on cases within their groups from the case details screen. The initials of the other users viewing the case will appear at the top right of the screen.

CASE ID : 20145

OPEN

VIEWERS DT LP

CREATED BY : ADMIN ADMIN | ASSIGNED TO : ADMIN ADMIN

CREATED ON
MON, 2 OCT 2017 @ 14:03:25

UPDATED ON
TUE, 3 OCT 2017 @ 01:44:51

DUE DATE
-

VIOLATOR DETAILS

POLICY NAME
ROBOTIC BEACONING TRAFFIC DETECTED

POLICY CATEGORY
CYBER 1.0

THREAT NAME
ROBOTIC BEACONING TRAFFIC DETECTED

CASE RELATED VIOLATORS

ACTIVITY STREAM

MON, 11 SEP 2017 @ 14:15:08 MONDAY

RISK SCORE: 75.8

Ros Lane

EMPLOYEE ID ~ 2214 | DEPARTMENT ~ SAP ADMINISTRATOR | DIVISION ~

First 1 Last TOTAL 1



Note: Only users logged in and viewing the case at the same time will appear as available for chat.

Click the initials of the user with whom you wish to chat to launch the chat window.

OPEN

VIEWERS

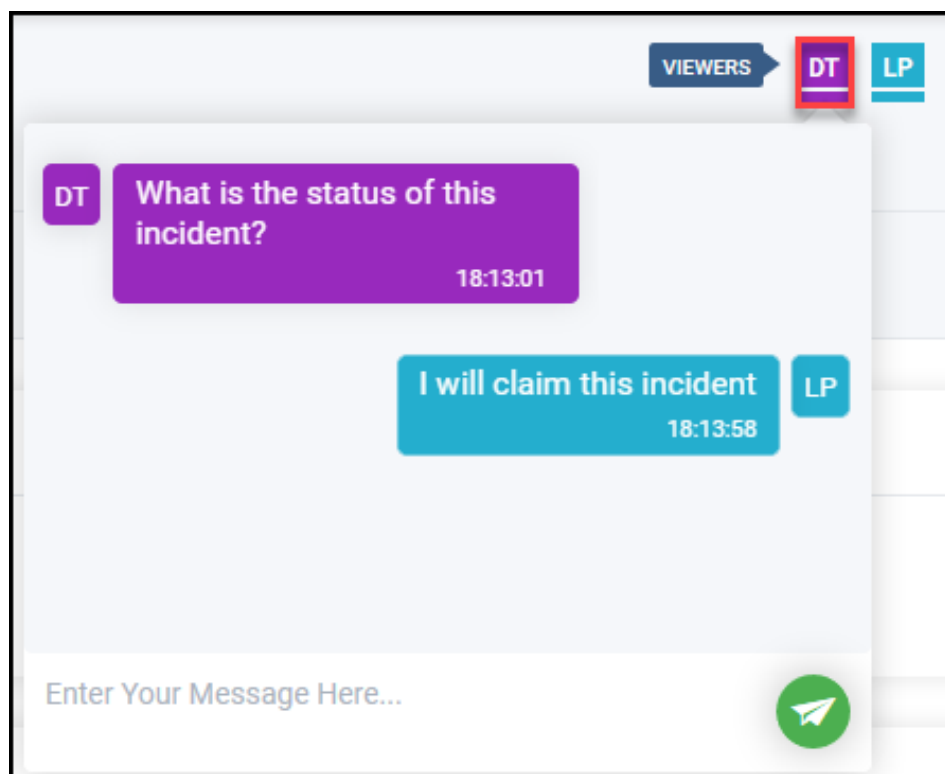
DT

LP

Start your conversation by typing in text box below.

Enter Your Message Here...

Type text to chat with the other viewers for this incident and click send icon.



Taking Actions on Cases

The actions available for each case are based on the workflow selected for the case. For more about configuring work flows, see [Workflows](#) in the ArcSight UBA Administration Guide. Some examples of the actions configured in default work flows include the following:

 **Note:** These actions will not exist for all cases and may be labeled differently for custom work flows.

- **Assign** cases to a specific analyst or group of analysts.
- **Claim** an open case (a case not yet assigned), and begin the investigation process.
- **Accept** the risk.
- Mark as a confirmed **Violation**.
- **Release** the case for another analyst to claim.

To take action on an open case, complete the following steps:

1. Click the action to take from the **Actions** menu.
2. Provide the requested information as in the following examples:

Assign to Analyst

Use this option to assign the case to an individual user or a user group. To assign a case to an analyst, complete the following steps when the Case Action dialog box opens:

ASSIGN TO ANALYST **ASSIGN TO SECOPS**

Business Response
Inaccurate alert-User not a HPA ▼

Business Justification

Remediation Performed

Business Internal Use

Assign To Analyst
Admin Admin [admin] admin... - OR - Select A Group ▼

Select A User

- Admin Admin [admin]
admin@securonix.com
- IT Auditor [auditor]
itauditor@securonix.com
- User Administrator [useradmin]
useradmin@securonix.com
- Access Scanner
[accessscanner]

1. **Business Response:** Select an appropriate business response from the dropdown.
2. **Business Justification:** Enter a comment (optional).
3. **Remediation Performed:** Enter a comment (optional).
4. **Business Internal Use:** Enter a comment (optional).
5. **Assign to Analyst:** Select from dropdown to assign to a single analyst or group.
6. Click **Submit**.
7. The case will display the analyst or group the case is **Assigned To**.

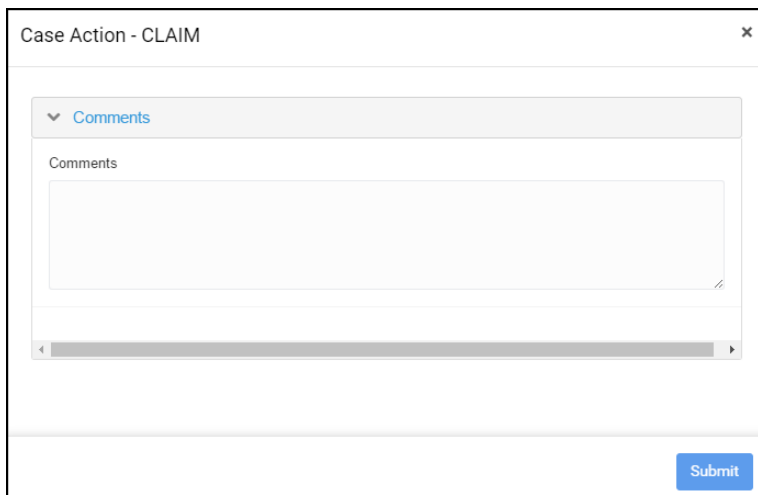
The screenshot displays a case card for 'CASE ID : 20018'. The status is 'CLAIMED' in an orange box. Below the status, it shows 'CREATED BY : ADMIN ADMIN' and 'ASSIGNED TO : SECURITYOPERATIONS', with the latter highlighted by a red rectangle. A blue circular icon with a white 'M' is on the left. The 'ACTIONS' section contains five buttons: 'ACCEPT RISK', 'VIOLATION', 'RELEASE', 'ASSIGN TO ANALYST', and 'ASSIGN TO SECOPS'. At the bottom, a timeline shows 'CREATED ON FRI, 29 SEP 2017 @ 13:33:07', 'UPDATED ON FRI, 29 SEP 2017 @ 13:44:38', and 'DUE DATE -'.

CASE ID : 20018		CLAIMED
CREATED BY : ADMIN ADMIN	ASSIGNED TO : SECURITYOPERATIONS	
ACTIONS		
ACCEPT RISK VIOLATION RELEASE ASSIGN TO ANALYST ASSIGN TO SECOPS		
	CREATED ON FRI, 29 SEP 2017 @ 13:33:07	UPDATED ON FRI, 29 SEP 2017 @ 13:44:38
		DUE DATE -

Claim

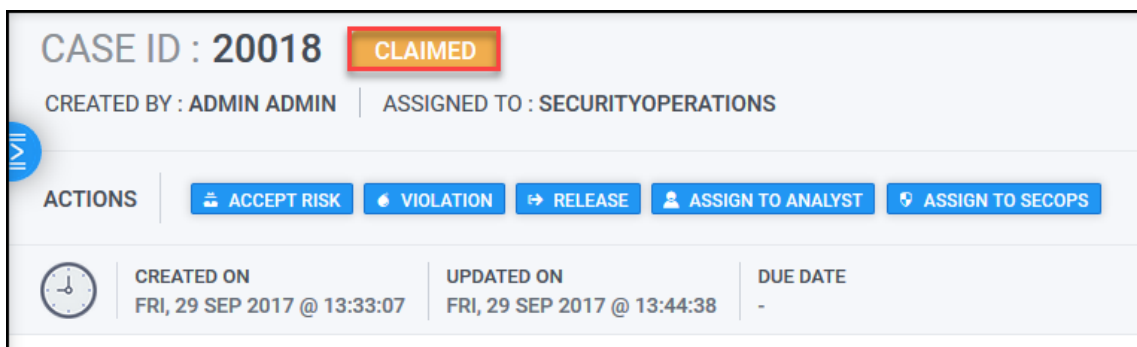
Use this option to claim the case for the current user (you) and start working the investigation. To claim a case, complete the following steps when the **Case Action** dialog box opens:

1. Enter comments to explain or justify the action.



The image shows a dialog box titled "Case Action - CLAIM" with a close button (X) in the top right corner. Inside the dialog, there is a section labeled "Comments" with a dropdown arrow. Below this is a large text area for entering comments. At the bottom right of the dialog is a blue "Submit" button.

2. Click **Submit**.
3. The status will appear as Claimed:



The image shows a case status card for "CASE ID : 20018" with a red "CLAIMED" badge. Below the case ID, it says "CREATED BY : ADMIN ADMIN" and "ASSIGNED TO : SECURITYOPERATIONS". There is a blue "ACTIONS" button on the left. To its right are five buttons: "ACCEPT RISK", "VIOLATION", "RELEASE", "ASSIGN TO ANALYST", and "ASSIGN TO SECOPS". At the bottom, there is a table with case details:

	CREATED ON	UPDATED ON	DUE DATE
	FRI, 29 SEP 2017 @ 13:33:07	FRI, 29 SEP 2017 @ 13:44:38	-



Note: Only the analyst who has claimed the case will have the authority to edit the case. Other analysts in the group will be able to view the case and the case details.

Accept Risk

Use this option to close the case and mark the violation as fixed. To accept risk for a case, complete the following steps when the **Case Action** dialog box opens:

Case Action - ACCEPT RISK

▼ Comments

Business Justification

Accurate alert-Remediated ▼

Accurate alert-Remediated

Accurate alert-Technical issue

Accurate alert-Approved action

Accurate alert-HPA user no longer with the organization

Unable to investigate-Very old ticket

Remediation Performed

Business Internal Use

Submit

1. **Business Response:** Select an appropriate business response from the dropdown.
2. **Business Justification:** Enter a comment (optional).
3. **Remediation Performed:** Enter a comment (optional).
4. **Business Internal Use:** Enter a comment (optional).
5. Click **Submit**.

The case will appear as Completed.



Note: You will not be able to take further action on a case when it has been closed for Accept Risk. You must reopen the case.

Violation

Use this option to close the case and mark the case a confirmed violation. To close a case, complete the following steps when the **Case Action** dialog box opens:

Case Action - VIOLATION

▼ Comments

Business Response

Accurate alert-Violation of policy ▼

Accurate alert-Violation of policy

Accurate alert-Remediated

Business Justification

Business Justification

Remediation Performed

Submit

1. **Business Response:** Select an appropriate business response from the dropdown.
2. **Business Justification:** Enter a comment (optional).
3. **Remediation Performed:** Enter a comment (optional).
4. **Business Internal Use:** Enter a comment (optional).
5. Click **Submit**.

The case will appear as Closed:

CASE ID : 99 **CLOSED**

CREATED BY : ADMIN ADMIN | ASSIGNED TO : SECURITYOPERATIONS

ACTIONS | **CLAIM** | **RELEASE** | **ASSIGN TO ANALYST**

CREATED ON FRI, 15 SEP 2017 @ 20:27:47 | **UPDATED ON** FRI, 15 SEP 2017 @ 20:28:13 | **DUE DATE** -



Note: You will still be able to take actions such as Claim, Release and Assign to Analyst when the case is closed as a violation.

Creating a Case from the Security Command Center

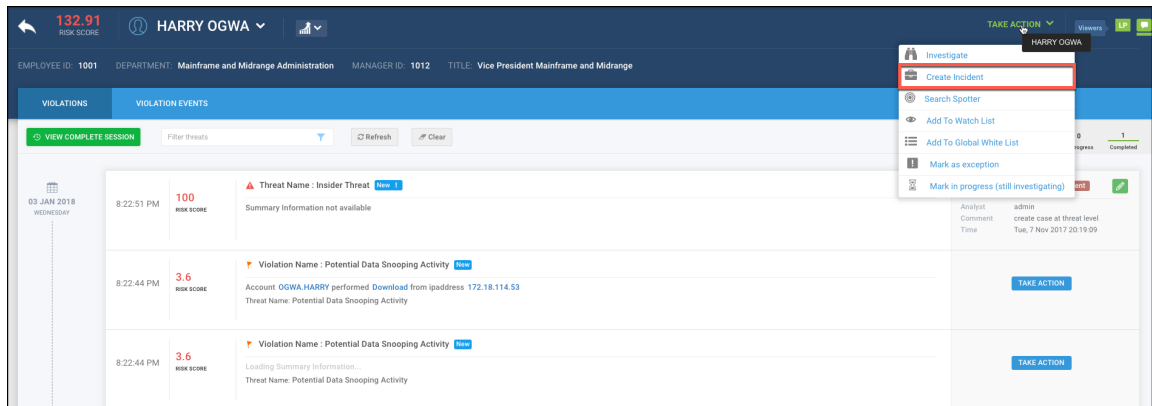
You can create cases from the Security Command Center on the violation or threat summary screen for an entity/violator, or a policy or threat violation:

- **Entity/Violator:** All violations across all jobs will be grouped in one case for an entity.
- **Policy Violation:** All violators of the policy will be grouped under one case for a single policy.
- **Threat Violation:** All violators of the threat will be grouped under one case for a single threat.

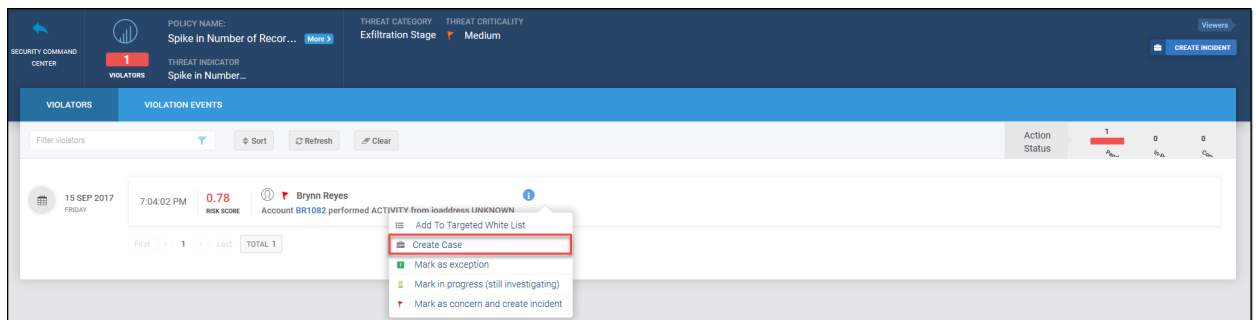
See [Entities](#), [Policies](#), and [Threats](#) for more details about the features available on the Violations Summary screen.

To create a case for an entity, policy or threat from the Security Command Center on the violation or threat summary screen, complete the following steps:

1. Navigate to **Menu > Security Center > Security Command Center**
2. Click an entity, violation, or threat from a dashboard. Example: Top Violators. For more information about the available dashboards, see [Security Command Center](#).
3. Create an incident in one of the following ways:
 - Click **Create Incident** from the **Actions** menu on the right side of the entity or violation view.



- Click **Create Case** to create an incident from the collapsed menu on an entity or violation.



4. Complete the following in the **Action - Create Incident** dialog box:

Action - Create Incident

Available Workflow

SOC Team Review

Comments

Criticality

None

Submit

Criticality

None

Assign To Analyst

Submit

- a. **Select Workflow:** Select a workflow from the dropdown. For more information about configuring work flows, see [Workflows](#) in the ArcSight UBA Administration Guide.
- b. **Comments:** Enter a comment to explain or justify the action.
- c. **Criticality:** Select a criticality from the dropdown.
- d. **Assign to Analyst:** Click search icon to select users or groups to assign to the case and click **Assign**.

Select Assignee

Groups

Users

Enter your search criteria

username

	User Name	First Name	Last Name	Email
	accessscanner	Access	Scanner	info@securonix.com
	admin	Admin	Admin	admin@securonix.com
	auditor	IT	Auditor	itauditor@securonix.com
	breddy@securonix.com	bhanu	reddy	breddy@securonix.com
	HectorR	Hector	Ruiz	hruiz@sec.com
	lpherson@securonix.com	Lindsey	Pherson	lpherson@securonix.com
	useradmin	User	Administrator	useradmin@securonix.com
	zmutabanna@securonix.com	zohra	mutabanna	zmutabanna@securonix.com

First

1

Last

Show

15

Total results : 8 | Total pages : 1

Assign

5. Click **Submit**.

To view the case you created, navigate to **Menu > Security Center > Incident Management**.

Reports

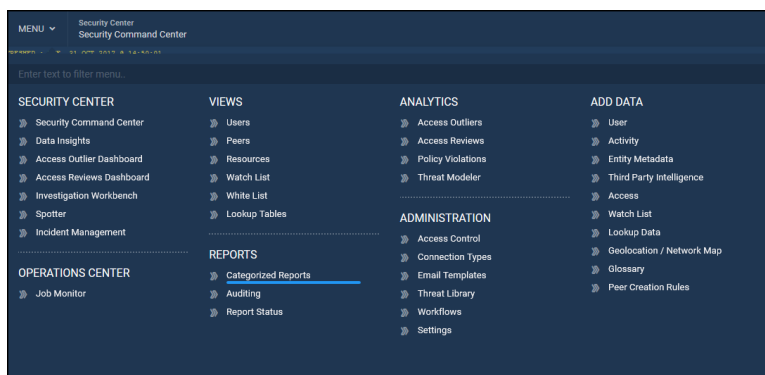
ArcSight UBA has both out-of-the-box standard reports and extensive ad-hoc reporting capabilities. From the **Report** menu, the following options are available:

- [Categorized Reports](#)
- [Auditing](#)
- [Report Status](#)

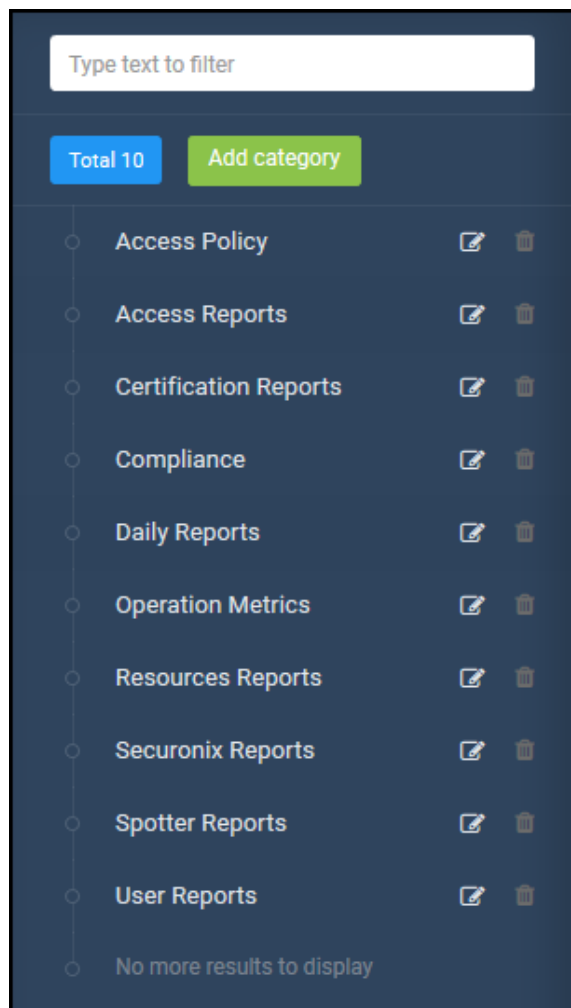
Categorized Reports

This feature allows you to schedule and run default reports, or create custom reports to run on Spotter, database, or archived data.

To access categories reports, Navigate to **Menu > Reports > Categorized Reports**.



Click  to expand the left navigation pane.



Reports are listed and filtered by category. You can add categories and create new reports within an existing category. By default, the following report categories are included:

- Access Policy
- Access Reports
- Certification Reports
- Compliance
- Daily Reports
- Operation Metrics
- Resources Reports
- Securonix Reports
- Spotter Reports
- User Reports

The application creates additional report categories when you import new data sources. For example, if you import activity data from Active Directory, you will see a new “Identity Access Management” category in the Categorized Reports navigation pane, which will contain the Active Directory report.

Click a report category to view the existing default reports available for that category.

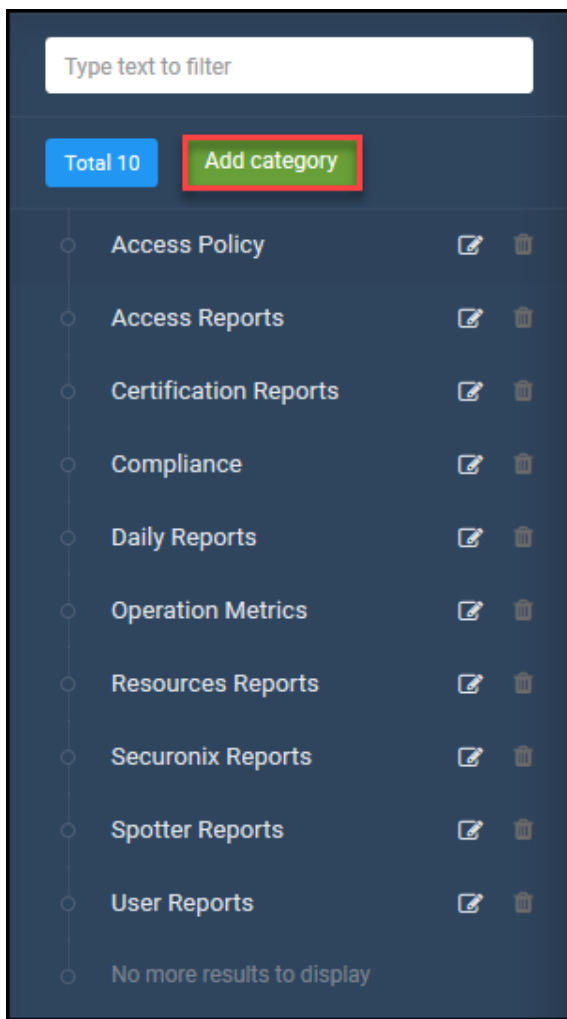
The screenshot displays the 'Categorized Reports' section of the ArcSight User Behavior Analytics 6.10 interface. On the left, a dark blue sidebar lists report categories: Access Policy, Access Reports, Certification Reports (selected), Daily Reports, Identity Access Management..., Incident Management, Resources Reports, Securonix Reports, Spotter Reports, and User Reports. The main content area shows a table of reports under the 'Certification Reports' category. The table has two columns: 'Report Name' and 'Actions'. The reports listed are:

Report Name	Actions
Certification Report - Action Certify <i>Report lists the entitlements certified</i>	[Edit] [Share] [Delete] [Download]
Certification Report - Action Exempt <i>Report lists the entitlement Exempted</i>	[Edit] [Share] [Delete] [Download]
Certification Report By Manager - Action Exempt <i>Report Lists entitlements exempted by Manager</i>	[Edit] [Share] [Delete] [Download]
Certification Report By Manager - Action Revoked <i>Report lists entitlements revoked by Manager</i>	[Edit] [Share] [Delete] [Download]

At the bottom of the table, there is a pagination control showing 'First', '<', '1' (selected), '>', 'Last', and 'Show 10'. To the right, it says 'Total results : 4 | Total pages : 1'.

Adding a new report category

1. Click **Add Category** on the main screen.



2. Enter a unique name in the **Category Name** field when the Add New Category dialog box appears.

Add New Category

Category Name*

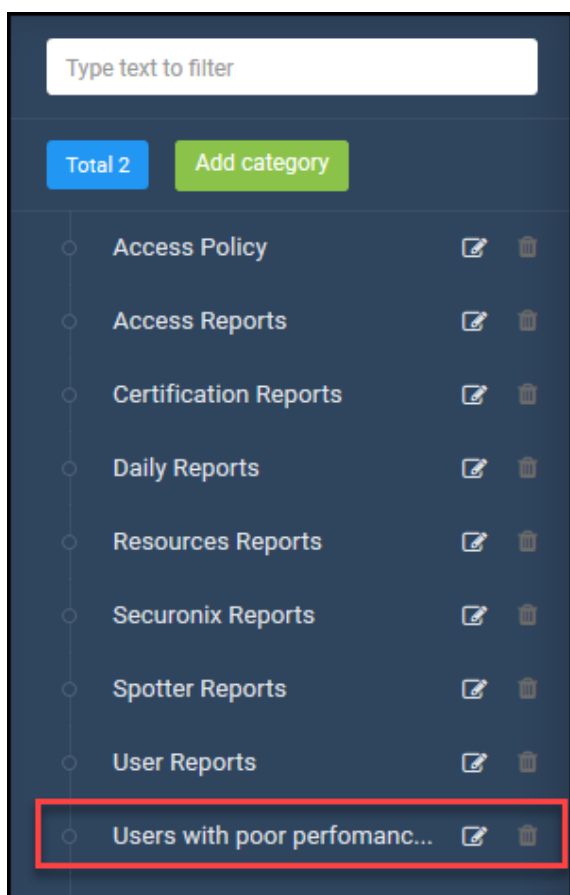
Users with poor performance review

Enter a unique name to identify this category.

Save

3. Click **Save**.


The new category will appear in the left navigation pane.



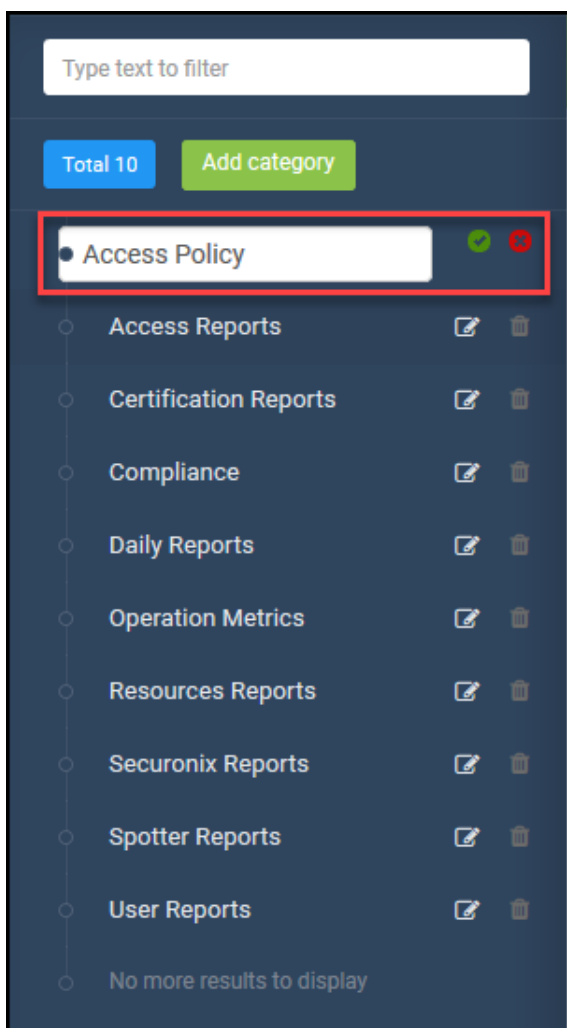
To create new reports for this category, see [Creating a new report](#).


Editing or Deleting an Existing Report or Report Category

You can delete reports by category or a single report within a category.



 **Note:** When you delete a category, the reports associated with that category are not deleted. If you want to retain all of the reports associated with a category that you plan to delete, *you must edit individual reports and change their categories before you delete the category.* To edit or delete an entire **report category**, use the following steps:

1. Click the edit icon:  to edit an existing report category .



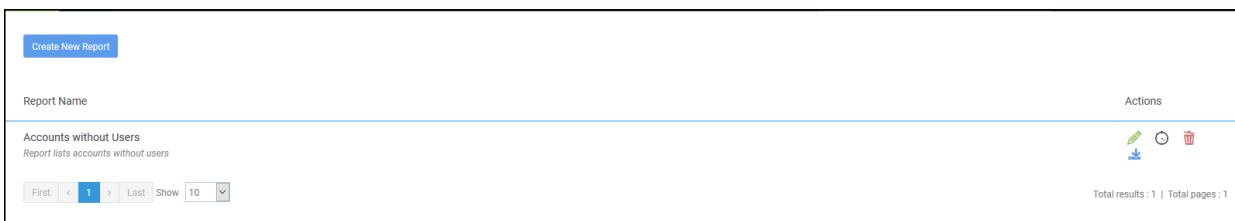
- a. Edit the category information and click green check mark to save.
 - b. Click red **X** to cancel.
2. Click the trash can icon:  to delete an existing report category .

To edit or delete an entire **report**, use the following steps:

1. Click the edit icon:  to edit an existing report .
 - a. Edit the fields described in [Creating a New Report](#).
 - b. Click **Save**.
2. Click the delete icon:  to delete an existing report.

Creating a New Report

1. Click **Create new report** to add a new report.



2. Complete the following information when the **Create new report** dialog box appears:

Basic Report Details

BASIC REPORT DETAILS

Report Name*

Enter a unique name to identify this report.

Owner

Select report owner. Only owners of this report will be able to view it. You can select a group of users or individual user as owner.

Description

Enter report description.

Report Category

User Reports ▼

Select report category.

- Report Name:** Enter a unique name for the report.
- Owner:** Assign this report to a specific group or an individual user. Click the magnifying glass to open a list of available groups and users.

Assign Owner

Groups **Users**

	User Name <input type="text"/>	First Name	Last Name	Email
<input type="radio"/>	accessscanner	Access	Scanner	info@securonix.com
<input type="radio"/>	admin	Admin	Admin	admin@securonix.com

To select a group, click the **Groups** tab. To select an individual user, click the **Users** tab. When you have finished, click **Assign**.



Note: When you assign a report to a specific owner (or group of owners), only the owner(s) of the report can view it.

To remove the owner from a report, click the red **x** located on the right side of the **Owner** field.

- c. **Description:** Enter a brief description for the new report.
- d. **Report Category:** Select an existing report category from the dropdown under which the new report will appear. Example: Access Reports.

Click **Save and Next**.

Connection Types

You can run reports on the following connection types:

- [Database](#): Run report on data stored in database. Select a JRXML file to associate with the report.
- [Archived Data](#): Run report on historical data stored in HDFS. Select a JRXML file to associate with the report.
- [Spotter](#): Run report on data in Solr using Spotter search terms. Select a custom JRXML or select the attributes on which to report to create a custom template.

Database

Complete the following information to run reports on data stored in a database:

FILE AND CONNECTION TYPE DETAILS

Choose the source of your report data*

Database ▼

Select Connection Type

File Name*

Browse

Choose JRXML file to be associated with this report.

- a. **Connection Type:** Database.
- b. **File Name:** Choose the JRXML file of the template associated with this report. To navigate to the appropriate file location, click **Browse**.



Note: ArcSight UBA integrates with Jasper Reports to use the contents and configurations of JRXML files as a template for the report. The securonix_home/reports directory contains over 50 JRXML default files you can use. For more information about Jasper Reports, see <http://community.jaspersoft.com/project/jasperreports-library>. For a complete list of the JRXML files available in **Securonix/tenants/<tenant>/securonix_home/reports**, see [Report Templates](#).

Click **Save and Next** to proceed to **Report Query** to complete the following information:

Parameters (Optional)

Name	Type of parameter	Mapping	Actions
<input type="text"/>	<input type="text"/>	<input type="text" value="-Select-"/>	<input type="text" value="-Select-"/> + -

1. **Parameters:** Complete the following fields:

- **Name:** Enter a name for the parameter.
- **JRXML Parameter:** Enter the JRXML Parameter declared in the Jasper Report file.
Example 1: The value of attribute NAME of the parameter tag from the report file.
Example 2: REPORT_DATA_SOURCE.
- **Type of Parameter:** Select from dropdown. Example: Resource.
- **Mapping:** Select from the dropdown. Example: \$ID.

To add additional parameters, click the green plus (+) sign. To delete parameters, click the red minus (-) sign.

Click **Save**.

Archived Data

Complete the following information to run reports on data stored in HDFS:

File and Connection Type Details

FILE AND CONNECTION TYPE DETAILS

Choose the source of your report data*

Archived Data

Select Connection Type

File Name*

Choose JRXML file to be associated with this report.

- Connection Type:** Archived Data.
- File Name:** Choose the JRXML file of the template associated with this report. To navigate to the appropriate file location, click **Browse**.



Note: ArcSight UBA integrates with Jasper Reports to use the contents and configurations of JRXML files as a template for the report. The securonix_home/reports directory contains over 50 JRXML default files you can use. For more information about Jasper Reports, see <http://community.jaspersoft.com/project/jasperreports-library>. For a complete list of the JRXML files available in securonix/tenants/<tenant>/securonix_home/reports, see Report Defaults.

Click **Save and Next** to proceed to **Report Query** to complete the following information:

Parameters (Optional)

Parameters				
Name	JRXML Parameter	Type of parameter	Mapping	Actions
<input type="text"/>	<input type="text"/>	<div>-Select-</div>	<div>-Select-</div>	<div>⊕ ⊖</div>

- Parameters:** Complete the following fields:
 - Name:** Enter a name for the parameter.
 - JRXML Parameter:** Enter the JRXML Parameter declared in the Jasper Report file.
 Example 1: The value of attribute NAME of the parameter tag from the report file.
 Example 2: REPORT_DATA_SOURCE.
 - Type of Parameter:** Select from dropdown. Example: Resource.

- **Mapping:** Select from the dropdown. Example: \$ID.

To add additional parameters, click the green plus (+) sign. To delete parameters, click the red minus (-) sign.

Click **Save**.

Spotter

Complete the following information to run reports on data in Solr using Spotter search terms:

File and Connection Type Details

FILE AND CONNECTION TYPE DETAILS

ConnectionType*

Spotter

Select Connection Type

Do You want to upload Custom jrxml file.

☒ NO

Toggle to yes if you wish to upload the custom jrxml file for spotter reports.

Default Reports Template*

reportTemplate.jrxml

Browse

Choose JRXML file to be associated with this report.

Do You Want to Keep All Records In Reports.

☒ NO

On Enabling above flag it will fetch all entries for given spotter query in Reports.

Maximum Number Of records*

10000

Maximum Number Of Entries Allowed in Reports.

1. **Connection Type:** Spotter.
2. **Do you want to upload Custom JRXML file:**
 - If **NO: Default Reports Template** is automatically populated with **reportTemplate.jrxml**.
 - If **YES:** Upload a custom JRXML file to be associated with the report.
3. **Do you want to export all records that matched rep:**
 - If **NO:** Specify a **Maximum Number of Records to export**.
 - If **YES:** The report will export all records for the query.

Click **Save and Next** to proceed to **Report Query** to complete the following information:

Enter the Query to Preview Results

ENTER THE QUERY TO PREVIEW RESULTS

Spotter Search Results

Index = Violation and policy = "Flight Risk User - Job Search"

31 events fetched out of matched 31 events

ALL TIMES SHOWN ARE IN CST

WED, 30 AUG 2017 @ 08:35:51 PM resourcegroupname: Bluecoat Proxy policyname: Flight Risk User - Job Search

accountname = OGWA,HARRY , bytesin = 6946 , bytesout = 488 , destinationservername = none , eventoutcome = 200 , message = allowed , applicationprotocol = ssl , ipaddress = 10.0.1.61 , sourceaddress = 10.91.252.94 , resourcegroupname = Bluecoat Proxy , resource = Bluecoat Proxy , destinationhostname = 10.91.252.94 , destinationhostname = https://quintiles.taleo.net , destinationdomain = , destinationport = 8443 , requestclientapplication = Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.112 Safari/537.36 , requestcontext = application/json , requestmethod = POST , requesturl = https://quintiles.taleo.net/careersection/10080/jobdetail.ft?job=1704064&lang=en&src=JB-11S , filetype = , customnumber1 = 16200 , customstring2 = unavailable , categorybehavior = communication , categoryobject = device , deviceeventcategory = Job Search

category = ACCOUNT MISUSE , policyname = Flight Risk User - Job Search , riskthreatname = Possible Flight Risk Users , violator = Activityaccount

companycode = TECH , costcentername = IINFCCC12 , country = USA , department = Mainframe and Midrange Administration , division = Global Technology , employeeid = 1001 , employeetype = FT , employeetypedescription = FullTime , firstname = HARRY , hiredate = 08/08/2009 00:00:00.000 , jobcode = R1 , lanid = H01001 , lastname = OGWA , location = DALLAS , manageremployeeid = 1012 , middlename = A , status = 1 , statusdescription = Active , title = Vice President Mainframe and Midrange , workemail = HARRY.OGWA@scnx.com , workphone = 9723451278

approveremployeeid = 1082 , mobile = 0151 709 7593 , lastperformanceviewdate = 04/01/2014 00:00:00.000 , usercriticality = Low , companynumber = TECH12 , province = FL , street = 9000 SOUTHSIDE BLVD BLDG 600 , regtempin = Regular , lastperformanceviewresult = Poor , costcentercode = IINFCCC12 , networkid = HOGWA , zipcode = 32256 , orgunitnumber = 12 , city = JACKSONVILLE , managerfirstname = Joe , fulltimeparttimein = FullTime , usersriskscore = 0.01 , usertimezoneoffset = CST

1. **Enter the Query to Preview Results:** Enter the Spotter query to populate the report.
Example: index = violation and policyname = "Flight Risk User - Job Search"
For more information about searching Spotter, see [Spotter](#).

Specify the label for the report you want to map attribute

SPECIFY THE LABEL FOR THE REPORT YOU WANT TO MAP ATTRIBUTE.

Event

accountname, bytesin, bytesout, destinationip, eventoutcome, message, applicationprotocol, isid, sourceaddress, resourcegroupname, resource, destinationaddress, destinationhostname, destinationdomain, destinationport, requestclientapplication, requestcontext, requestmethod, requesturl, filetype, customnumber1, customnumber2, categorybehavior, categoryobject, deviceeventcategory, category

Violation

category, policyname, riskthreatname, violator

Identity

companycode, costcentername, country, department, division, employeeid, employeetype, employeepedescription, first, h, jobcode, last, location, manageremployeeid, middlename, status, statusdescription, title, workemail, workplace, workphone

Time

week, month, hour, year, dayofweek, categorycode, dayofyear, dayofmonth

Event Time

eventtime

1. Click to select the attributes to include in the report.
Attributes that appear in blue will be included in the report. Attributes that appear in gray are excluded from the report.

accountname, bytesin, bytesout, username, Bytes_Received, Bytes_Sent

Map With

username

Enter The Label For Attribute. This Mapped Attribute will reflect as Label in the reports column.

Remove Mapping, Save

- Edit the attribute label under which the mapped attribute will appear in the report column. (Optional).
- Click **Save** to save the label and include the attribute in the report.
- Click **Remove Mapping** to remove the attribute from the report.

Parameters (Optional)

Parameters

Field parameter	Label Name	Actions
		● ● ●

1. **Parameters:** Complete the following fields:

- **Name:** Enter a name for the parameter.
- **JRXML Parameter:** Enter the JRXML Parameter declared in the Jasper Report file.
Example 1: The value of attribute NAME of the parameter tag from the report file.
Example 2: REPORT_DATA_SOURCE.
- **Type of Parameter:** Select from dropdown. Example: Resource.
- **Mapping:** Select from the dropdown. Example: \$ID.

To add additional parameters, click the green plus (+) sign. To delete parameters, click the red minus (-) sign.

Click **Save**.

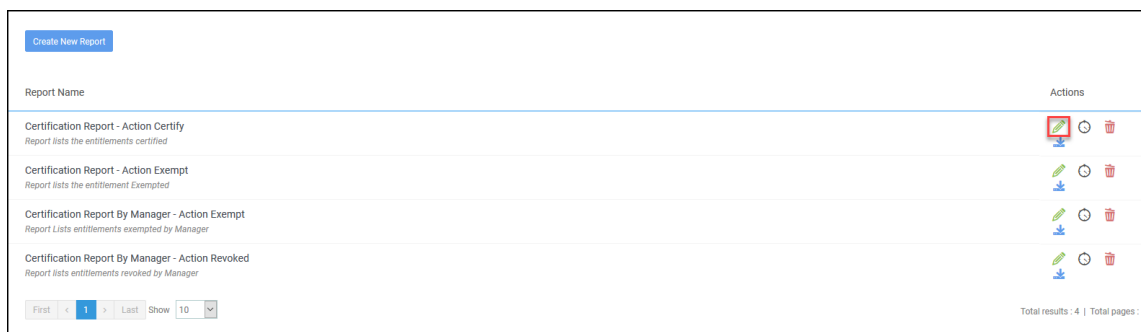
The new report will appear under the category you selected when configuring the [Basic Report Details](#).

Report Name	Actions
Anomalous VIP Break The Glass Activity	
CoWorker Snooping	
Family Snooping	
Neighbor Snooping	
Self Examination	
PCI - Antivirus Deployment <small>PCI Requirement 65 - Protect all systems against malware and regularly update anti-virus software or programs</small>	
PCI - Monitor Access <small>PCI Requirement 10 - Track and monitor all access to network resources and cardholder data</small>	
Base-IH - Account Logon Events (Windows) <small>ISO 17799 Section A.5.5.2</small>	
Base-IH - Control of Collected Evidence <small>ISO 17799 Section A.12.1.7.1</small>	
Base-IH - Control of Human Resources Data <small>ISO 17799 Section A.12.1.9</small>	













Editing an Existing Report

To edit an existing report, complete the following steps:

1. Select a report category from the left navigation pane. The list of reports in that category will appear in the right section of the screen.
2. Locate the report you want to edit. At the end of the report row, you will find a list of **Actions**.



The screenshot shows a web interface for managing reports. At the top left is a blue button labeled 'Create New Report'. Below it is a table with the following structure:

Report Name	Actions
Certification Report - Action Certify <i>Report lists the entitlements certified</i>	  
Certification Report - Action Exempt <i>Report lists the entitlement Exempted</i>	  
Certification Report By Manager - Action Exempt <i>Report Lists entitlements exempted by Manager</i>	  
Certification Report By Manager - Action Revoked <i>Report lists entitlements revoked by Manager</i>	  

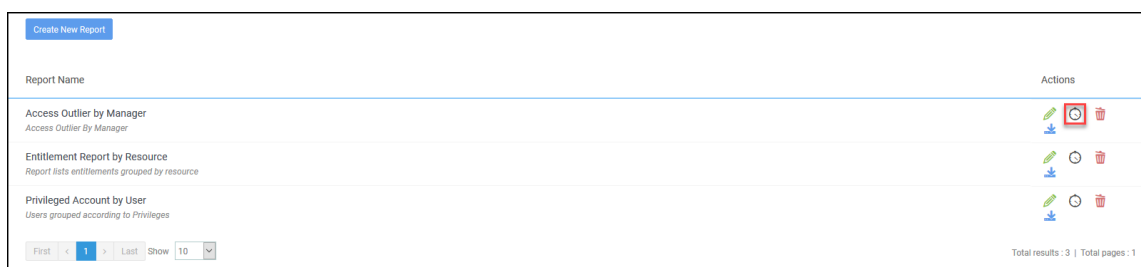
At the bottom of the table, there is a pagination bar with 'First', '<', '1', '>', 'Last', 'Show', '10', and a dropdown arrow. In the bottom right corner, it says 'Total results : 4 | Total pages : 1'.

3. Click the pencil icon to edit the report. The Edit report window opens.
4. Edit the report as needed. For a description of the report fields, see [Creating a New Report](#).
5. Click **Save**.










Scheduling and Running an Existing Report

To schedule a report to run once now or on a schedule, complete the following steps:

1. From the left navigation pane, select a report category. The list of reports in that category will appear in the right section of the screen.
2. Locate the report you want to run. At the end of the report row, you will find a list of **Actions**.
3. Click the **Run** icon to run the report.



The screenshot shows a web interface for managing reports. At the top left is a blue button labeled 'Create New Report'. Below it is a table with the following structure:

Report Name	Actions
Access Outlier by Manager <i>Access Outlier By Manager</i>	  
Entitlement Report by Resource <i>Report lists entitlements grouped by resource</i>	  
Privileged Account by User <i>Users grouped according to Privileges</i>	  

At the bottom of the table, there is a pagination bar with 'First', '<', '1', '>', 'Last', 'Show', '10', and a dropdown arrow. In the bottom right corner, it says 'Total results : 3 | Total pages : 1'.

4. Complete the form to run the report:

Job Name *

Job Description

Report Name*

Select Report Format

pdf

Choose Email Template

-Select-

Run

☒ Do you want to run job Once ?
 ☐ Do you want to schedule this job for future ?

Job will be scheduled according to the server time. Current server time is - 10/10/2017 16:00:22

Schedule



Note: Fields on the form may vary depending on the type of report and resource on which the report is to run.

- Job Name:** Enter a name for the report job.
- (Optional) **Job Description:** Enter a brief description for the job.
- Select Report Format:** Select an option from the dropdown. Example: pdf.
- Choose Email Template:** Select the email template you want to use to send the report via email from dropdown.
- Run:** Select the frequency for the report job:

- **Do you want to run Job Once?:** Select to run the job once now.
- **Do you want to schedule this job for future?:** Select this option to select how often to run the job:

Run

☐ Do you want to run job Once ?

☒ Do you want to schedule this job for future ?

Seconds

Minutes

✓ Hourly

Daily

Weekly

Monthly

Specify Date

Select how often you want the job to run

Start Job At *

05:21:00 PM

NOTE: This is the server time

Stop after

10

Job will be scheduled according to the server time. Current server time is - 10/10/2017 16:25:20

5. Click **Schedule**.

6. Download the report from the **Report Status** screen.

For more information about what you can do from this screen, see [Report Status](#).

Report Status								
<div> <div>BACK TO CATEGORIZED REPORTS</div> <div> <div>Schedule Saved Report</div> <div>Merge Reports</div> </div> </div>								
	Job Name	Create Date	Start Date	Next Trigger Date	End Date	Created By	Status	Actions
✓	SpotterReports_Export Spotter Results_1509635368081	Thu Nov 02 10:09:28 CDT 2017	Thu Nov 02 10:09:28 CDT 2017		Thu Nov 02 10:09:57 CDT 2017	admin	Completed	<div> <div></div> <div></div> <div></div> </div>
✓	SpotterReports_Export Spotter Results_150959976150	Thu Nov 02 00:19:36 CDT 2017	Thu Nov 02 00:19:36 CDT 2017		Thu Nov 02 00:20:03 CDT 2017	admin	Completed	<div> <div></div> <div></div> <div></div> </div>













The report will open in the format selected in **Step 4**.

Activity Monitor		
accountname	transactionstring1	companycode
CIARA.LAWS@SCNX.COM	Send Mail	Cash
CIARA.LAWS@SCNX.COM	Send Mail	Cash
DAVID.KEARNEY@SCNX.COM	Send Mail	GMKT
DAVID.KEARNEY@SCNX.COM	Send Mail	GMKT
UNA.KELLEHER@SCNX.COM	Send Mail	GMKT
UNA.KELLEHER@SCNX.COM	Send Mail	GMKT
ORLA.BOYLE@SCNX.COM	Send Mail	DEBT
ORLA.BOYLE@SCNX.COM	Send Mail	DEBT
JAMES.KILLEEN@SCNX.COM	Send Mail	BAN16
JAMES.KILLEEN@SCNX.COM	Send Mail	BAN16
ERWIN.THOMSON@SCNX.COM	Send Mail	DEP
ERWIN.THOMSON@SCNX.COM	Send Mail	DEP
MARK.WRISLEY@SCNX.COM	Send Mail	DEBT
MARK.WRISLEY@SCNX.COM	Send Mail	DEBT
JAMAAL.CORLESS@SCNX.COM	Send Mail	MKTG
JAMAAL.CORLESS@SCNX.COM	Send Mail	MKTG

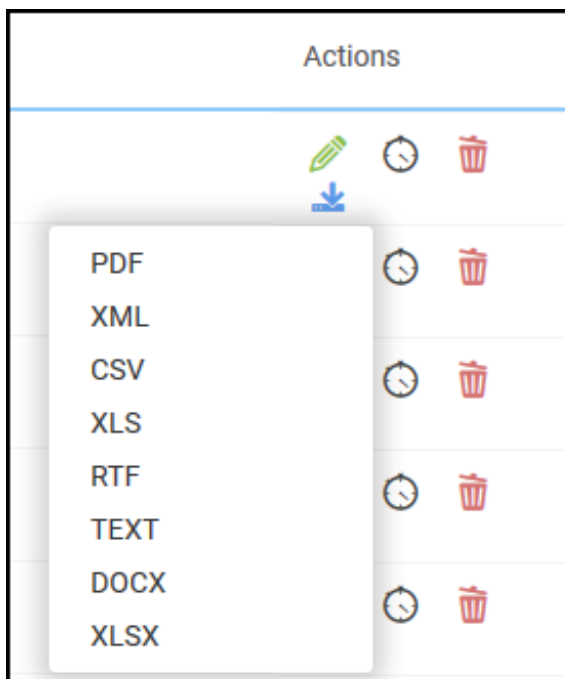
Downloading a Report to File

To download a report to file, complete the following steps:

1. From the left navigation pane, select a report category. The list of reports in that category will appear in the right section of the screen.
2. Locate the report you want to run. At the end of the report row, you will find a list of **Actions**.
3. Click the **Download** icon to run the report.

Create New Report	
Report Name	Actions
Anomalous VIP Break The Glass Activity	  
CoWorker Snooping	  
Family Snooping	  
Neighbor Snooping	  

1. Select the appropriate file format.
The report will download to your local machine.

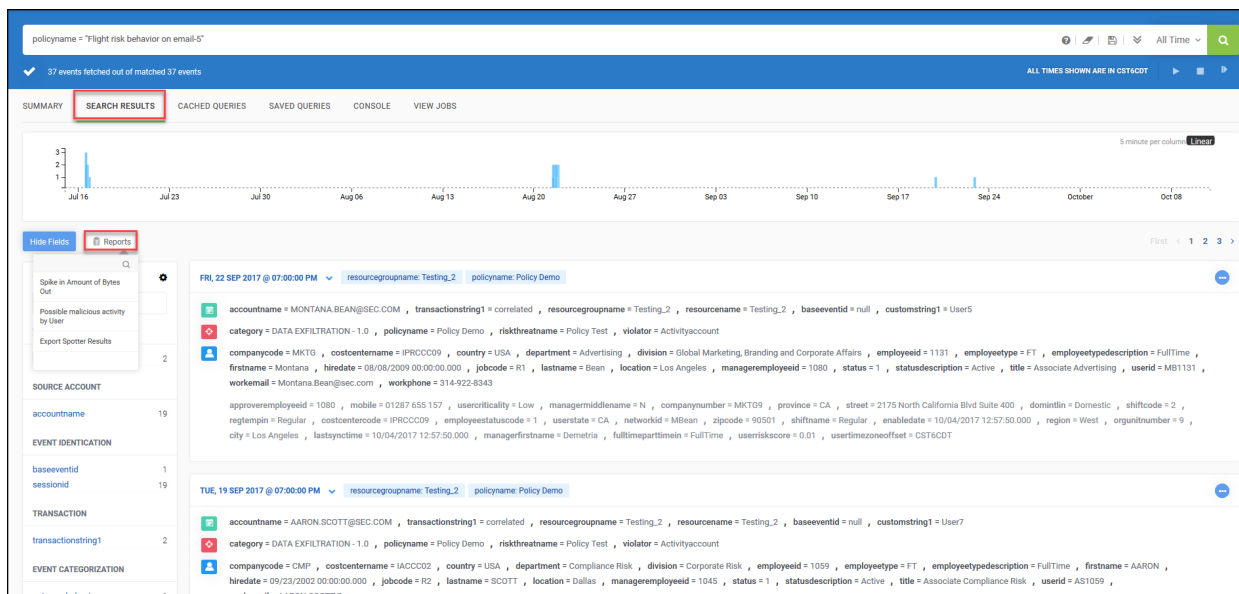


Running Reports from Spotter

In addition to the reports you can configure from the **Menu > Reports > Categorized Reports** screen, you can run reports from Spotter Search Results.

To run reports from Spotter, complete the following steps:

1. Navigate to **Menu > Security Command Center > Spotter** to conduct a search OR click **Launch Spotter** from data points in the **Security Command Center**.
For information about searching Spotter, see [Spotter](#). For information about how to launch Spotter searched from the Security Command Center, see [Security Command Center](#).
2. Click **Reports**.



3. Select a report template from dropdown or click **Export Spotter Results** to create a new report.
4. Click to select the attributes to include in the report.

Attributes that appear in blue will be included in the report. Attributes that appear in gray are excluded from the report.

Run Spotter Report

SPECIFY THE LABEL FOR THE REPORT YOU WANT TO MAP ATTRIBUTE.

Event	Violation	Identity	Time	Event Time
<div>accountname</div> <div>transactionstring1</div> <div>accountname</div> <div>resourcegroupname</div> <div>resourcegroupname</div> <div>resourcegroupname</div> <div>baseeventid</div> <div>baseeventid</div> <div>customstring1</div> <div>customstring1</div>	<div>category</div> <div>category</div> <div>policyname</div> <div>policyname</div> <div>riskthreatname</div> <div>riskthreatname</div> <div>violation</div> <div>violation</div>	<div>companycode</div> <div>companycode</div> <div>costcentername</div> <div>costcentername</div> <div>country</div> <div>country</div> <div>department</div> <div>department</div> <div>division</div> <div>division</div> <div>employeeid</div> <div>employeeid</div> <div>employeetype</div> <div>employeetype</div> <div>employeetypedescription</div> <div>employeetypedescription</div> <div>employeeid</div> <div>employeeid</div> <div>status</div> <div>status</div> <div>status</div> <div>status</div> <div>workphone</div> <div>workphone</div>	<div>week</div> <div>week</div> <div>month</div> <div>month</div> <div>hour</div> <div>hour</div> <div>year</div> <div>year</div> <div>dayofweek</div> <div>dayofweek</div> <div>dayofweek</div> <div>dayofweek</div> <div>categorizedtime</div> <div>categorizedtime</div> <div>dayofyear</div> <div>dayofyear</div> <div>dayofmonth</div> <div>dayofmonth</div>	<div>eventtime</div> <div>eventtime</div>

Map With

employeeid

Enter The Label For Attribute This Mapped Attribute will reflect as Label in the reports column.

Remove Mapping Save

Run Cancel

- a. Edit the attribute label under which the mapped attribute will appear in the report column. (Optional).
 - b. Click **Save** to save the label and include the attribute in the report.
 - c. Click **Remove Mapping** to remove the attribute from the report.
5. Click **Run**.
6. Download the report from the Notifications menu when status is complete:

Enter text to search...

<ul style="list-style-type: none"> Query:policyname = "Possible malicious activity by User" Creation Time:10/10/2017 17:2:14 	0%	✖
<ul style="list-style-type: none"> Query:index = violation and policyname = "Spike in amount of bytes out" Creation Time:10/10/2017 16:11:21 	0%	✖



Note: Merged Reports will not appear on the Report Status screen. You must download the report from the Notifications menu.

Auditing

The Auditing feature allows you to audit activity performed in the ArcSight UBA application and check log tampering.

To access the Auditing screen, on the menu bar, navigate to **Menu > Reports > Auditing**.

Reports Auditing									
Enter Criteria									
Timestamp	User Name	Action	Description	Remote IP Address	Local IP Address	Status	Message	Actions	
2017-10-10 17:11:29.0	admin	DELETED	Delete Policy Job	10.1.52.50	10.1.52.50	SUCCESS	scheduledReports job _admin_2017-10-10 17:02:47.904 is deleted Successfully.	i	
2017-10-10 17:11:21.0	admin	TRIGGERED	Job invoked - New Report_admin_2017-10-10 17:11:16.241	N/A	SNYPR Console	SUCCESS	Job run completed successfully [New Report_admin_2017-10-10 17:11:16.241]	i	
2017-10-10 17:11:21.0	admin	START	Schedule Report	10.1.52.50	10.1.52.50	SUCCESS	Report New Report_admin_2017-10-10 17:11:16.241 runs Successfully.	i	
2017-10-10 17:02:55.0	admin	START	Schedule Report	10.1.52.50	10.1.52.50	SUCCESS	Report _admin_2017-10-10 17:02:47.904 runs Successfully.	i	
2017-10-10 17:02:55.0	admin	TRIGGERED	Job invoked - _admin_2017-10-10 17:02:47.904	N/A	SNYPR Console	SUCCESS	Job run completed successfully [_admin_2017-10-10 17:02:47.904]	i	
2017-10-10 16:46:55.0	admin	SAVED	Creating a New Report	10.1.52.50	10.1.52.50	SUCCESS	Report New Report Saved successfully	i	
2017-10-10 15:49:25.0	admin	LOGIN	Successful Login	10.1.51.110	10.1.51.110	SUCCESS	User authentication successful..	i	
2017-10-10 15:49:20.0	admin	LOGIN	Failed Login	10.1.51.110	10.1.51.110	ERROR	User authentication failed..	i	
2017-10-10 15:41:07.0	System	TRIGGERED	Job invoked - DEE Job	N/A	SNYPR Console	SUCCESS	Job run completed successfully [DEE Job]	i	
2017-10-10 12:58:35.0	admin	DELETED	Delete a Report	10.1.52.50	10.1.52.50	SUCCESS	Report \$reportName deleted successfully	i	
2017-10-10 12:58:25.0	admin	SAVED	Creating a New Report	10.1.52.50	10.1.52.50	SUCCESS	Report Test1 Saved successfully	i	
2017-10-10 12:54:25.0	Trainer1	LOGOUT	Successful Logout	10.1.51.182	10.1.51.182	SUCCESS	User logged out successfully..	i	
2017-10-10 12:53:46.0	Trainer1	LOGIN	Successful Login	10.1.51.182	10.1.51.182	SUCCESS	User authentication successful..	i	

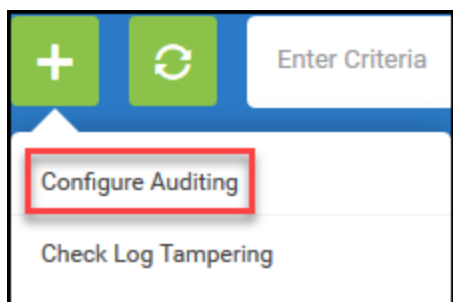
You can take the following actions from this screen:

- Enter search criteria to filter results.
- Click Refresh icon to refresh results.
- Click Info icon ⓘ to view audit details:

Audit Details		✕
User Name ⓘ	mcilento	
Action	LOGIN	
Description	Successful Login	
Timestamp ⓘ	2017-08-03 15:15:51.0	
Remote IP Address ⓘ	10.0.5.42	
Local IP Address ⓘ	10.0.5.42	
Status	SUCCESS	
Message ⓘ	User authentication successful..	
Module	LOGIN_CONTROLLER	
Class	LOGINCONTROLLER	
Type	N/A	

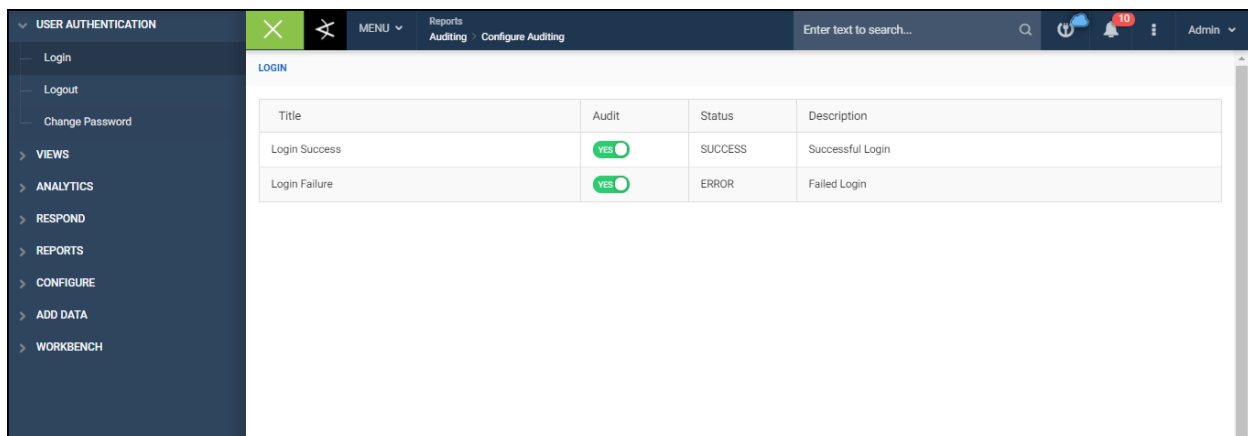
Configuring Auditing

You can configure the types of activity to audit. To configure auditing, click + > **Configure Auditing**:



From the left navigation screen, you can select activity by the following categories:

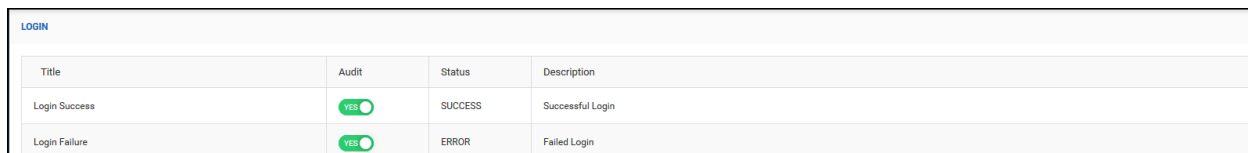
- User Authentication
- Views
- Analytics
- Respond
- Reports
- Configure
- Add Data
- Workbench



The screenshot shows the ArcSight User Authentication interface. On the left is a dark blue sidebar with navigation links: Login, Logout, Change Password, VIEWS, ANALYTICS, RESPOND, REPORTS, CONFIGURE, ADD DATA, and WORKBENCH. The main content area is titled 'LOGIN' and contains a table with the following data:

Title	Audit	Status	Description
Login Success	<input checked="" type="checkbox"/>	SUCCESS	Successful Login
Login Failure	<input checked="" type="checkbox"/>	ERROR	Failed Login

Click an activity type to enable or disable auditing.



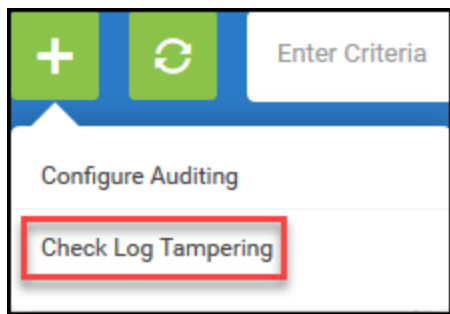
This is a close-up of the 'LOGIN' table from the previous screenshot. It shows the 'Audit' column with green toggle switches for both 'Login Success' and 'Login Failure'.

Title	Audit	Status	Description
Login Success	<input checked="" type="checkbox"/>	SUCCESS	Successful Login
Login Failure	<input checked="" type="checkbox"/>	ERROR	Failed Login

Toggle to **Yes** to enable auditing. Toggle to **No** to disable auditing.

Checking Log Tampering

To check log tampering, click + > **Check Log Tampering**.



From the Tampered Records screen, you can view details of actions performed by users.

Tampered Records							
Timestamp	User Name	Action	Description	Remote IP Address	Local IP Address	Status	Message
2017-05-06 01:18:00.0	admin	TRIGGERED	Job invoked - ResourceData_EntityMetadata_DemoWorkstation1_2017_5_6_1_17_58	N/A	SNYPR Console	SUCCESS	Job run completed successfully [ResourceData_EntityMetadata_DemoWorkstation1_2017_5_6_1_17_58]
2017-05-09 13:09:00.0	admin	LOGIN	Successful Login	10.1.51.42	10.1.51.42	SUCCESS	User authentication successful.
2017-05-09 17:29:00.0	admin	TRIGGERED	Job invoked - PaloAlto_Regex_05_09_2017_05_28_22_PM	N/A	SNYPR Console	SUCCESS	Job run completed successfully [PaloAlto_Regex_05_09_2017_05_28_22_PM]
2017-05-09 18:43:00.0	admin	LOGIN	Successful Login	10.1.51.16	10.1.51.16	SUCCESS	User authentication successful.
2017-05-10 00:33:00.0	admin	TRIGGERED	Job invoked - Bro File_Regex_05_10_2017_12_32_56_AM	N/A	SNYPR Console	SUCCESS	Job run completed successfully [Bro File_Regex_05_10_2017_12_32_56_AM]
2017-05-10 17:34:00.0	admin	LOGIN	Successful Login	10.1.2.1	10.1.2.1	SUCCESS	User authentication successful.
2017-05-10 22:05:00.0	admin	TRIGGERED	Job invoked - Microsoft Windows Event_Regex_05_10_2017_10_02_22_PM	N/A	SNYPR Console	SUCCESS	Job run completed successfully [Microsoft Windows Event_Regex_05_10_2017_10_02_22_PM]
2017-05-17 15:54:00.0	admin	LOGOUT	Successful Logout	10.1.51.7	10.1.51.7	SUCCESS	User logged out successfully.
2017-05-19 11:13:00.0	lpherson@securonix.com	LOGIN	Successful Login	10.1.51.5	10.1.51.5	SUCCESS	User authentication successful.
2017-05-22 22:26:00.0	admin	LOGIN	Failed Login	10.0.5.184	10.0.5.184	ERROR	User authentication failed.
2017-05-24 10:37:00.0	admin	UPDATED	Updating workflow configuration...	10.0.5.182	10.0.0.20	SUCCESS	Workflow Configuration SOCTeamReview saved successfully
2017-05-24 13:14:00.0	Rupali	LOGIN	Successful Login	10.1.51.8	10.1.51.8	SUCCESS	User authentication successful.

Report Status

The Report Status feature allows you to view existing report jobs and schedule new report jobs for saved reports. For more information on creating reports, see [Categorized Reports](#).

To access the Report Status screen, on the menu bar, navigate to **Menu > Reports > Report Status**.

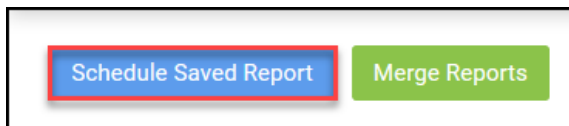
Report Status								
Schedule Saved Report		Merge Reports						
Job Name	Create Date	Start Date	Next Trigger Date	End Date	Created By	Status	Actions	
Test_admin_2017-10-06 09:55:50.012	Fri Oct 06 09:55:55 CDT 2017	Fri Oct 06 09:55:55 CDT 2017		Fri Oct 06 09:56:18 CDT 2017	admin	Completed		
TestReport2_DocTeam_2017-10-05 13:09:05.157	Thu Oct 05 13:09:09 CDT 2017	Thu Oct 05 13:09:09 CDT 2017		Thu Oct 05 13:09:11 CDT 2017	DocTeam	Completed		
TestReport2_DocTeam_2017-10-05 10:06:38.836	Thu Oct 05 10:06:46 CDT 2017	Thu Oct 05 10:06:46 CDT 2017		Thu Oct 05 10:06:48 CDT 2017	DocTeam	Completed		
TestReport2_DocTeam_2017-10-05 10:04:50.191	Thu Oct 05 10:05:11 CDT 2017	Thu Oct 05 10:05:11 CDT 2017		Thu Oct 05 10:05:13 CDT 2017	DocTeam	Completed		
TestReport2_DocTeam_2017-10-05 09:50:08.084	Thu Oct 05 09:50:11 CDT 2017	Thu Oct 05 09:50:11 CDT 2017		Thu Oct 05 09:50:13 CDT 2017	DocTeam	Completed		
TestReport2_DocTeam_2017-10-05 09:46:31.169_renu_9_48_13	Thu Oct 05 09:48:13 CDT 2017	Thu Oct 05 09:48:13 CDT 2017		Thu Oct 05 09:48:15 CDT 2017	DocTeam	Completed		

You can take the following actions on report jobs from this screen:

	Re-run a completed report job.
	Delete existing report jobs.
	Download report.

Scheduling a saved report

1. Click **Schedule Saved Report** from Report Status main screen.



2. Enter the following details:

Job Name *

User Change History_admin_2017-10-10 16:56:19.463

Job Description

Report Name*

User Change History

Select Report Format

pdf

Choose Email Template

-Select-

Run

☒ Do you want to run job Once ?

☐ Do you want to schedule this job for future ?

Job will be scheduled according to the server time. Current server time is - 10/10/2017 16:00:22

Schedule

- a. **Job Name:** Enter a name for the report job.
- b. (Optional) **Job Description:** Enter a brief description for the job.
- c. **Report Name:** Select the name of the report to run from the dropdown. Example: Access Outlier by Manager.
- d. **Select Report Format:** Select an option from the dropdown. Example: pdf.
- e. **Choose Email Template:** Select the email template you want to use to send the report via

email from dropdown.

f. **Run:** Select the frequency for the report job:

- **Do you want to run Job Once?:** Select to run the job once now.
- **Do you want to schedule this job for future?:** Select this option to select how often to run the job:

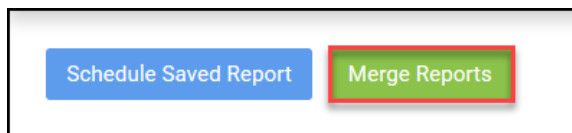
The 'Run' configuration form includes the following elements:

- Two radio buttons: 'Do you want to run job Once ?' (unselected) and 'Do you want to schedule this job for future ?' (selected).
- A row of frequency buttons: 'Seconds', 'Minutes', 'Hourly' (selected with a checkmark), 'Daily', 'Weekly', 'Monthly', and 'Specify Date'.
- A text prompt: 'Select how often you want the job to run'.
- A 'Start Job At *' section with a time input field showing '05:21:00 PM'.
- A note: 'NOTE: This is the server time'.
- A 'Stop after' section with a numeric input field containing '10'.
- An information bar at the bottom: 'Job will be scheduled according to the server time. Current server time is - 10/10/2017 16:25:20'.

3. Click **Schedule**. The report will appear on your list of scheduled reports.

Merging Spotter Reports

To merge Spotter reports, click **Merge Reports**.



Complete the following information:

Job Details

The 'Job Details' form contains two main input fields:

- Job Name ***: A text input field containing 'Report_Ipherson_2017-10-31 14:57:40.919'. Below the field is a small note: 'Enter a unique name to identify this report'.
- Job Description**: A larger, empty text area for providing a description of the job.

a. **Job Name:** Enter a name for the report job.

b. (Optional) **Job Description:** Enter a brief description for the job.

Select Reports to Merge

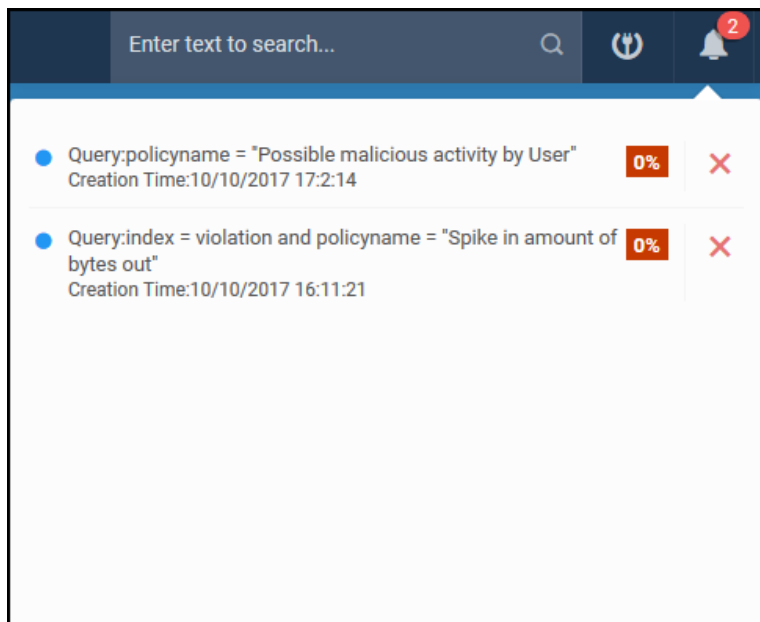
- Drag desired reports from **List of Available Spotter Reports** to **Included Reports for Merge in Sequence**.

Schedule and Email Template Details

- Select Report Format:** Select an option from the dropdown. Example: pdf.
- Choose Email Template:** Select the email template you want to use to send the report via email from dropdown.
- Run:** Select the frequency for the report job:
 - Do you want to run Job Once?:** Select to run the job once now.
 - Do you want to schedule this job for future?:** Select this option to select how often to run the job:

Click **Schedule**.

Download the report from the Notifications menu when status is complete:



Note: Merged Reports will not appear on the Report Status screen. You must download the report from the Notifications menu.

Report Templates

ArcSight UBA includes the following JRXML default files you can use. You can find the default files in your **Securionix/tenants/<tenant>/securionix_home/reports** directory.

Example Report Templates
AccessOrphanAccountsByResourceReport.jrxml
AccessOutlierAnalysisReport.jrxml
AccessOutlierAnalysisReportbyManager.jrxml
AccessOutlierAnalysisReportbyResource.jrxml
Accounts without User2.jrxml
ActivityOrphanAccountsByResourceReport.jrxml
ActivityOutlierAnalysisReport.jrxml
ADOutlierReport.jrxml
BgraphForSelectedRange.jasper
BgraphForSelectedRange.jrxml
BgraphTillNow.jasper
BgraphTillNow.jrxml
BreportSelectedRange.jasper
BreportSelectedRange.jrxml
BreportTillNow.jasper
BreportTillNow.jrxml
CertificationCertifybyDataOwner.jrxml
CertificationCertifybyManager.jrxml
CertificationReport by Certify.jrxml
CertificationReport by Exception.jrxml
CertificationReport_exempted By Manager2.jrxml
CertificationReport_revoked By Manager2.jrxml
CertificationResultsbyDataOwner.jrxml

Example Report Templates
CertificationResultsbyManager.jrxml
CertificationRevokesbyDataOwner.jrxml
CertificationRevokesbyManager.jrxml
DormantAccountsReport.jrxml
Entitlements by Resource.jrxml
EventsGraph.jasper
EventsGraph.jrxml
EventsList.jasper
EventsList.jrxml
ExitReport.jasper
ExitReport.jrxml
GroupOwnerByResourceGroupReport.jrxml
high_risk_selected_users.jasper
high_risk_selected_users.jrxml
high_risk_selected_users_by_category.jrxml
high_risk_users.jasper
high_risk_users.jrxml
high_risk_users_by_category.jasper
high_risk_users_by_category.jrxml
HighRiskAccessByPeer.jrxml
HRE_Template.jasper
HRE_Template.jrxml
HRE_Threats_Template.jasper

Example Report Templates
HRE_Threats_Template.jrxml
HRE_Violations_Template.jasper
HRE_Violations_Template.jrxml
hru_by_category_subreport_risk.jasper
hru_by_category_subreport_risk.jrxml
hru_by_category_subreport_violations.jasper
hru_by_category_subreport_violations.jrxml
hru_subreport_risk.jasper
hru_subreport_risk.jrxml
hru_subreport_violations.jasper
hru_subreport_violations.jrxml
JRMAAnalysisReport.jrxml
logo.gif
logo.jpg
OutlierAnalysisByApplicationPermissionReport.jrxml
PeerBasedActivities.jrxml
PeerBasedActivitiesSubReport.jrxml
PeerBasedActivitiesUserDetails.jrxml
PeerGroupAnalysisReport.jrxml
PolicyGraph.jasper
PolicyGraph.jrxml
PolicyViolators.jasper
PolicyViolators.jrxml

Example Report Templates
Privileged Account by Resource.jrxml
Privileged Account by User.jrxml
RACFOutlierReport.jrxml
reportTemplate.jrxml
ResourceGroupByAccountName.jrxml
ResourceGroupByBytesIn.jrxml
ResourceGroupByBytesOut.jrxml
ResourceGroupByDestinationIP.jasper
ResourceGroupByDestinationIP.jrxml
ResourceGroupByEventOutcome.jrxml
ResourceGroupByInactiveUsers.jrxml
ResourceGroupBySourceIP.jrxml
ResourceGroupByTop10Departments.jrxml
ResourceGroupByTop10PolicyViolators.jrxml
ResourceGroupByTop10Users.jrxml
ResourceGroupByTransaction.jrxml
ResourceGroupByUser.jrxml
UncorrelatedAccessAccountDetails.jrxml
UncorrelatedAccessAccountReport.jrxml
UncorrelatedAccessAccountReportByResource.jrxml
User Change History.jrxml
UserAccessAccountReport.jrxml
UserDetails.jrxml

Example Report Templates
UserPeerAccessReport.jrxml
UserPeerReport.jasper
UserPeerReport.jrxml
Users by Manager.jrxml
Users by Termination.jrxml
Users by TransferredDate.jrxml
Users Entitlement by Resource2.jrxml

For more information about Jasper Reports, see <http://community.jaspersoft.com/project/jasperreports-library>.

Views

The following Views are available in the ArcSight UBA application:

- [Users](#)
- [Peers](#)
- [Resources](#)
- [Watch List](#)
- [White List](#)
- [Lookup Tables](#)

From the Views screen, you can perform the following actions:

- View general details about users and resources
- Drill down into users to view details such as peer groups, access, activity, and behavior profiles
- Modify and delete user identities
- Launch Investigation Workbench for a user
- View and manage Watch Lists
- Create and manage White Lists
- View data in Lookup Tables

Users

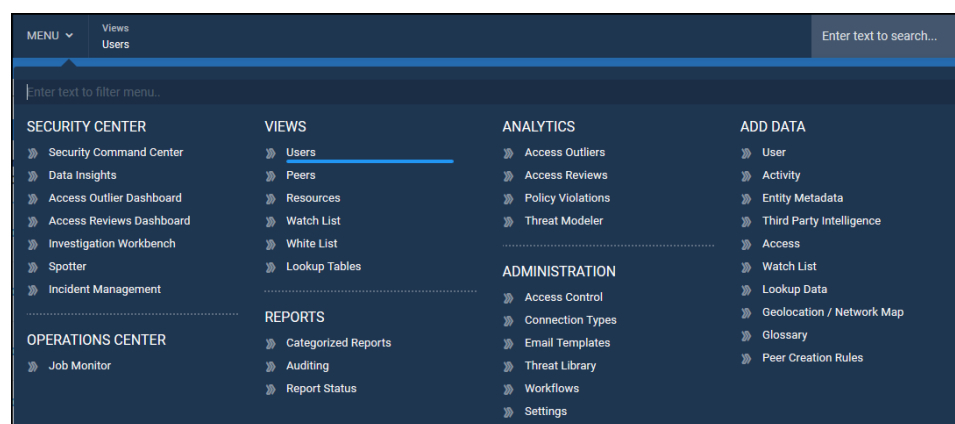
The ArcSight UBA application provides security professionals with relevant intelligence regarding the risk posture of the organization. Users interacting with the organization's IT assets are a cornerstone of the platform. The entire purpose of information security is to detect and prevent rogue users from conducting harmful activities that may damage the well-being of the organization.

Users, in the context of the application, refers to all users interacting with the IT infrastructure of the organization, which may be employees, contractors, temporary workers, partners, vendors, suppliers, and even customers.

This section also allows security administrators to view user identity, access and activity data, peer group memberships, and behavioral profiles of individuals, and to modify imported user identities within the ArcSight UBA application.

Before you can view and manage users, you must import user data into ArcSight UBA. To import user data, refer to [User Data](#) in the ArcSight UBA Administration Guide.

After importing user data, navigate to **Menu > Views > Users** to view and manage user identities.



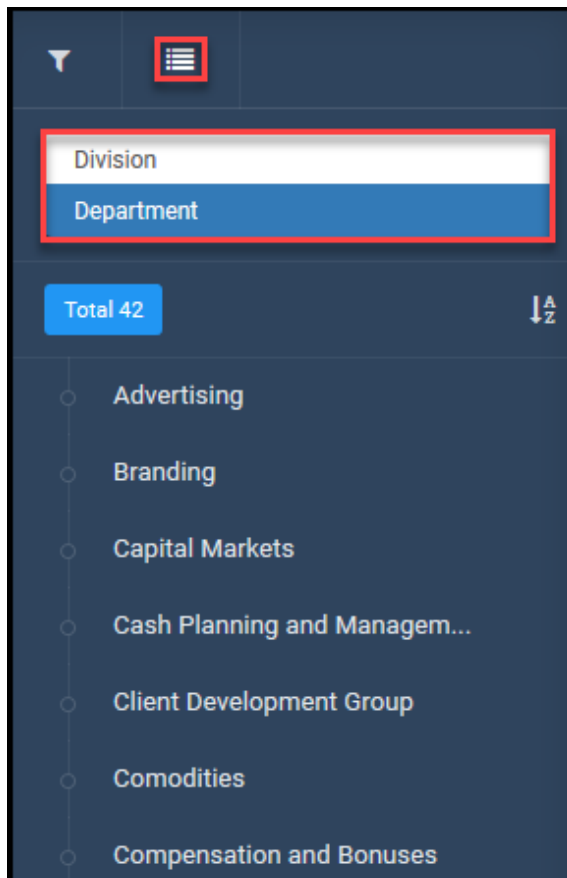
By default, the list is sorted by Employee ID in ascending order. Click a column heading to sort the list in ascending order by that attribute.



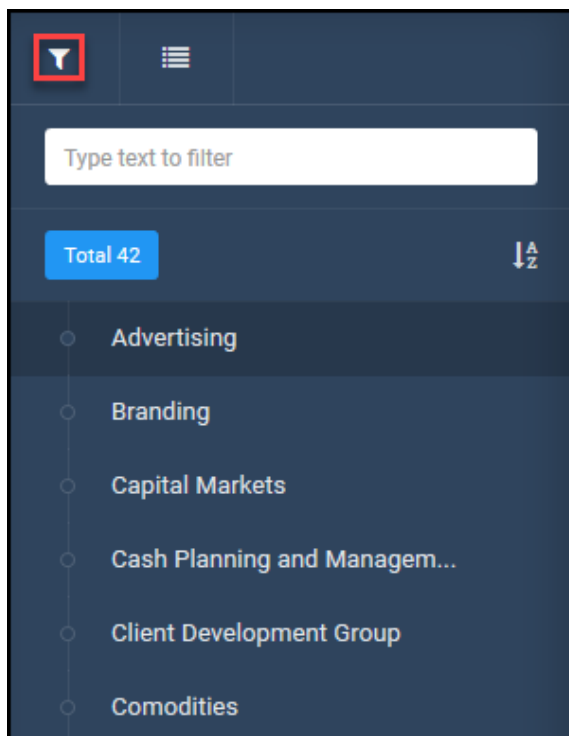
Note: The column headings may vary depending on the attributes mapped when importing user data.


Views Users										
Enter your search criteria										
<input type="checkbox"/>	Employee ID	First Name	Last Name	Manager Employee ID	Email	Department	Division	Title	Employee Type	
<input type="checkbox"/>	1080	Demetria	Bridges	1070	Demetria.Bridges@scnx.com	Advertising	Global Marketing, Branding and Corporate Affairs	Vice President Advertising	FT	
<input type="checkbox"/>	1095	Rosalyn	Harding	1080	Rosalyn.Harding@scnx.com	Advertising	Global Marketing, Branding and Corporate Affairs	Associate Vice President Advertising	FT	
<input type="checkbox"/>	1099	Yeo	Twist	1080	Yeo.Twist@scnx.com	Advertising	Global Marketing, Branding and Corporate Affairs	Associate Advertising	FT	
<input type="checkbox"/>	1130	Amena	Parker	1080	Amena.Parker@scnx.com	Advertising	Global Marketing, Branding and Corporate Affairs	Associate Advertising	FT	
<input type="checkbox"/>	1131	Montana	Bean	1080	Montana.Bean@scnx.com	Advertising	Global Marketing, Branding and Corporate Affairs	Associate Advertising	FT	
<input type="checkbox"/>	1136	Jelani	Charles	1080	Jelani.Charles@scnx.com	Advertising	Global Marketing, Branding and Corporate Affairs	Associate Advertising	FT	
<input type="checkbox"/>	1345	Annie	Wong	1080	Annie.Wong@scnx.com	Advertising	Global Marketing, Branding and Corporate Affairs	Associate Advertising	FT	
<input type="checkbox"/>	1349	Yann	Bernard	1080	Yann.Bernard@scnx.com	Advertising	Global Marketing, Branding and Corporate Affairs	Associate Advertising	FT	
<input type="checkbox"/>	1380	Anh	Tran	1080	Anh.Tran@scnx.com	Advertising	Global Marketing, Branding and Corporate Affairs	Associate Advertising	FT	
<input type="checkbox"/>	1381	Jeanine	Wong	1080	Jeanine.Wong@scnx.com	Advertising	Global Marketing, Branding and Corporate Affairs	Associate Advertising	FT	

You can choose to view users by department or division by clicking the Advanced Options icon in the left navigation panel.



Click the filter icon to type text to filter the list of departments or divisions.



Click the binoculars icon  to launch the Investigation Workbench for a user. For more information, see [Investigation Workbench](#).

Click an Employee ID to view user details.

GENERAL DETAILS			
USER ID	EMPLOYEE ID	FIRST NAME	MIDDLE NAME
-	1080	Demetria	N
LAST NAME	JOB CODE	DOMESTIC/INTERNATIONAL	ORGANIZATION UNIT NUMBER
Bridges	M1	-	9
EMPLOYEE TYPE	PROMOTED	EMPLOYEE TYPE DESCRIPTION	LAST PERFORMANCE REVIEW DATE
FT	-	FullTime	-
FULL TIME/PART TIME	COST CENTER NAME	COST CENTER CODE	SHIFT CODE
FullTime	IPRCC09	IPRCC09	-
ORGANIZATION UNIT NUMBER	MAIL CODE	NAME PREFIX	USER GROUP
9	-	-	-
STANDARD HOURS	DEPARTMENT	LAST PERFORMANCE REVIEW RESULT	REGULAR/TEMPORARY
-	Advertising	-	Regular
CRITICALITY	NETWORK ID	COMPANY CODE	NAME SUFFIX
Low	DBridges	MKTG	-
COMPANY NUMBER	PREFERRED NAME	HIERARCHY	TITLE
MKTG9	-	3	Vice President Advertising
STATUS	DIVISION	STATUS DESCRIPTION	COMMENTS
1	Global Marketing, Branding and Corporate Affairs	Active	-
LAN ID	DATASOURCE		
DB1080	HRFile		

CONTACT DETAILS

See [Viewing User Details](#) for information about what you can do from this screen.

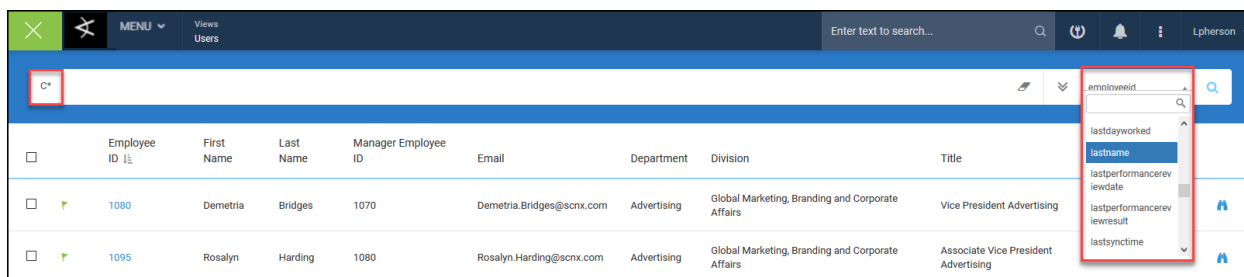
Performing User Searches

Simple User Search

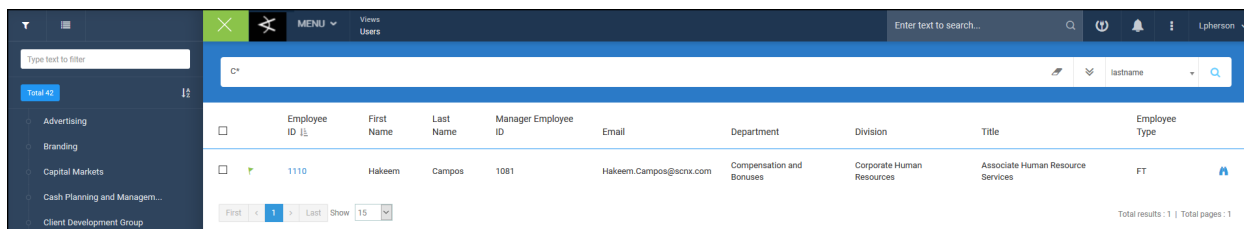
To perform a simple User search, navigate to **Menu > Views > Users**.

In the search bar, select a field on which to search from the dropdown list on which to search. For example, lastname.

Enter the search criteria in the text box. For example, C* to search users whose last name begins with C.



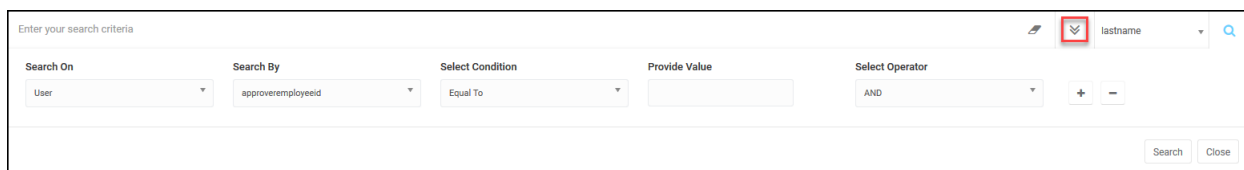
Click the search icon to search. The screen refreshes with the search results.



Advanced User Search

The Advanced search option enables you to use multiple search conditions.

To open the Advanced Search options, click the  icon on the search bar.



Use dropdowns to select the following search parameters:

- **Search on:** Select User or Peer Group.
- **Search by:** Select an available attribute. Example: location.
- **Select Condition:** Select from dropdown. Example: Equal To.
- **Provide Value:** Enter the value on which to search.
- **Select Operator:** Select from dropdown.
- **+/-:** Add/remove search criteria.

When search results appear, click an Employee ID to view user details.

Viewing User Details

Security administrators can view and monitor General Details, Organizations, Peer Groups, Access, Activities, and Behavior Profile for each user.

To view the details of a user, navigate to **Menu > Views > Users**, and then click the Employee ID for the user you wish to view.

By default, the General Details screen appears.

General Details

This screen displays the identity details for the selected user. The information displayed on this screen represents the data collected for the user during the import process.

The screenshot shows the 'General Details' screen for user Demetria Bridges. The interface includes a sidebar with navigation options: General Details, Peer Groups, Monitor Access, Monitor Activities, and Behavior Profile. The main content area displays a table of user information.

GENERAL DETAILS			
USER ID	EMPLOYEE ID	FIRST NAME	MIDDLE NAME
-	1080	Demetria	N
LAST NAME	JOB CODE	DOMESTIC/INTERNATIONAL	ORGANIZATION UNIT NUMBER
Bridges	M1	-	9
EMPLOYEE TYPE	PROMOTED	EMPLOYEE TYPE DESCRIPTION	LAST PERFORMANCE REVIEW DATE
FT	-	FullTime	-
FULL TIME/PART TIME	COST CENTER NAME	COST CENTER CODE	SHIFT CODE
FullTime	IPRCCC09	IPRCCC09	-
ORGANIZATION UNIT NUMBER	MAIL CODE	NAME PREFIX	USER GROUP
9	-	-	-
STANDARD HOURS	DEPARTMENT	LAST PERFORMANCE REVIEW RESULT	REGULAR/TEMPORARY
-	Advertising	-	Regular
CRITICALITY	NETWORK ID	COMPANY CODE	NAME SUFFIX
Low	DBridges	MKTG	-
COMPANY NUMBER	PREFERRED NAME	HIERARCHY	TITLE
MKTG9	-	3	Vice President Advertising
STATUS	DIVISION	STATUS DESCRIPTION	COMMENTS
1	Global Marketing, Branding and Corporate Affairs	Active	-
LAN ID	DATASOURCE		
DB1080	HRFile		

In the lower right corner, a collapsible menu is visible, listing the following options: General Details, Contact Details, Workflow Details, Employment History, and Custom Properties. A green circular icon with a plus sign is located next to the menu. Below the menu, a small text box reads: 'Click here to scroll to a particular section.'

In the lower right corner of the screen is a collapsible menu. When the menu is expanded, you can select from the following options to jump to that section of the user details:

- General Details
- Contact Details
- Workflow Details
- Employment History
- Custom Properties
- Change History

Peer Groups

A user may belong to one or multiple Peer Groups. These Peer Groups are typically based on user HR attributes such as job code, title, manager. The application uses peer groups to compare the user's access and activities and determine outlier behavior or anomalies.

From this screen, you can add peer groups for the user you're viewing or select one or more peer groups to remove.

BACK TO
USERS LIST

USER
Shane Cronin

EMPLOYEE ID
2486

DEPARTMENT
Cash Planning and Management

PEER GROUPS

Add Peer Groups

Remove Peer Groups

<input type="checkbox"/>	Criticality	Peer Name	Member Count
<input type="checkbox"/>		Cash Planning and Management	33
<input type="checkbox"/>		Corporate Strategy and Planning	74
<input type="checkbox"/>		D7	1
<input type="checkbox"/>		Managing Dir. Cash Management	1
<input type="checkbox"/>		St Louis	74
<input type="checkbox"/>		Ted_Thomson_1025	15

First < 1 > Last Show 10

Total results : 6 | Total pages : 1

To add a Peer Group for this user, click **Add Peer Groups**.

Add Peer Groups

Enter your search criteria

name

<input type="checkbox"/>	Criticality	Peer Name	Member Count	Location	Peer Group Type
<input type="checkbox"/>		A1	1		Job Code
<input type="checkbox"/>		Advertising	12		Department
<input type="checkbox"/>		Ainsley_Moses_1065	13		Manager
<input type="checkbox"/>		Aisling_Culkin_2681	4		Manager

Add Peer Groups

Search peer groups, select peer groups to add, and click **Add Peer Groups**.

Monitor Access

Monitor Access option allows you to view the accounts, access privileges, and profiles held by a user on each resource. To view details of an account, click the Account Name.

General Details

Peer Groups

Monitor Access

Monitor Activities

Behavior Profile

BACK TO USERS LIST

USER HARRY OGWA

EMPLOYEE ID 1001

DEPARTMENT Mainframe and Midrange Administration

ACCESS ACCOUNTS

Criticality	Account Name	Resource	Datasource	Account Type
	HO1001	Access Data	Access Data	User

First

<

1

>

Last

Show

15

Total results : 1 | Total pages : 1

The **Account Details** include the following:

- General Details about the account including the type, risk score, criticality, and status.

HO1001 Account Details ×	
General Details	Access Details
Account Name	HO1001
Resource	Access Data
Account Type	User
Risk Score	0.0
Criticality	Medium
Update Date	2017-10-02 17:02:43.0
Status	Active

- Access Details about the account including the values for each attribute mapped to the account. For example, the account employeeID.

HO1001 Account Details

General Details

Access Details

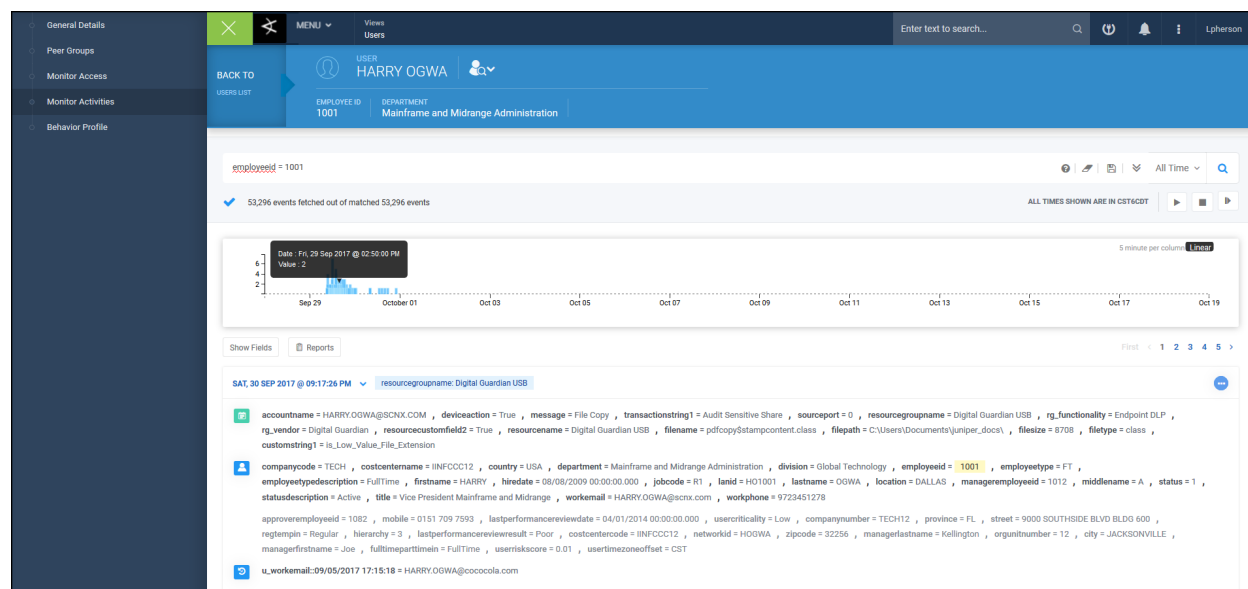
Type to search

Attribute Name	Attribute Value	
accountExpires	AD-LA-DC1	Q
displayName	HARRY,OGWA	Q
employeeID	INTERNAL AUDIT	Q
employeeType	FALSE	Q
homeMTA	CN=pf17664,OU=Retail Workforce,OU=Corporate,DC=scnx,DC=com	Q
lastLogonTimestamp	CN=Mailbox Store (WINDOWS),CN=First Storage Group,CN=InformationStore,CN=WINDOWS,CN=Servers,CN=First Administrative Group,CN=Administrative Groups,CN=First Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=scnx,DC=com	Q
manager	United States	Q
memberOf	CN=HR_User,OU=Applications,OU=Corporate,DC=scnx,DC=com	Q
memberOf	CN=BankSoft_User,OU=Applications,OU=Corporate,DC=scnx,DC=com	Q
memberOf	CN=CRM_User,OU=Applications,OU=Corporate,DC=scnx,DC=com	Q

Monitor Activities

Monitor Activities allows you to view all activities performed by a user across all resources for a selected period.

Click on any data point or field to filter events, enter a custom Spotter query, or export the search results as [Reports](#). For information about how to search events and what actions you can take on this screen, see [Spotter](#).



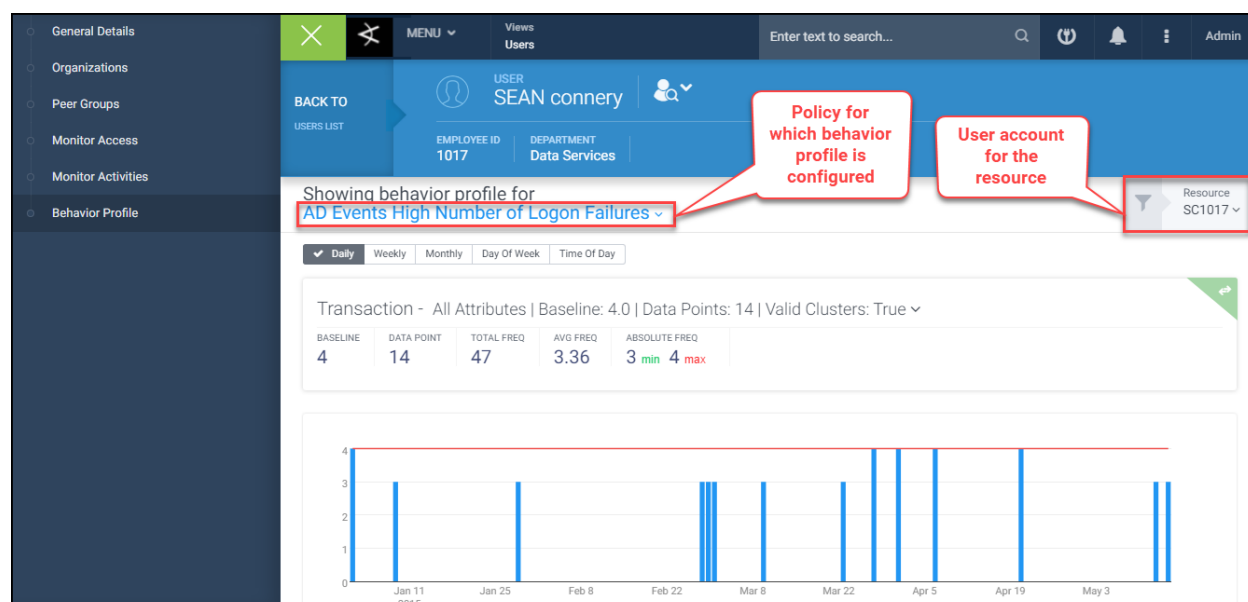
Behavior Profile

ArcSight UBA generates behavior profiles for users. These behavior profiles are very comprehensive and can store up to 120 characteristics for each user. The behavior characteristics include: time slices, activity, and IP address/hostname. Behavior profiles are used to establish a baseline of behavior for a user based on the selected characteristics to determine when the user conducts abnormal or outlier behavior that indicates a threat. For a detailed discussion of Behavior Profiles and why to use them, see [Behavior Profiles](#) in the ArcSight UBA Administration Guide.

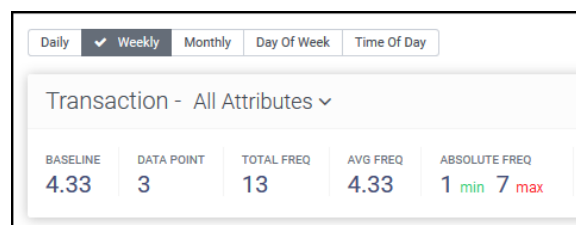
You can perform the following actions on this screen:

Select a policy for which you want to view the Behavior Profile from the dropdown.

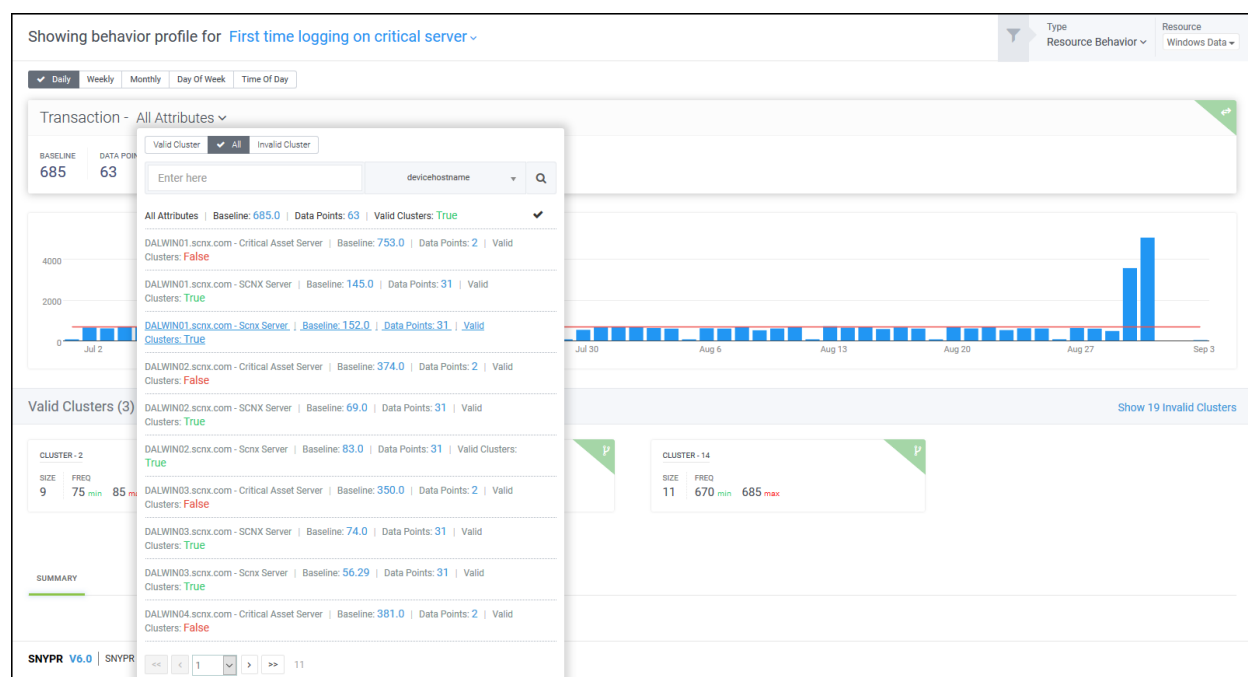
The screen displays activity for the selected account held by the user on the resource. You can view activity for a different account from the **Resource** dropdown.



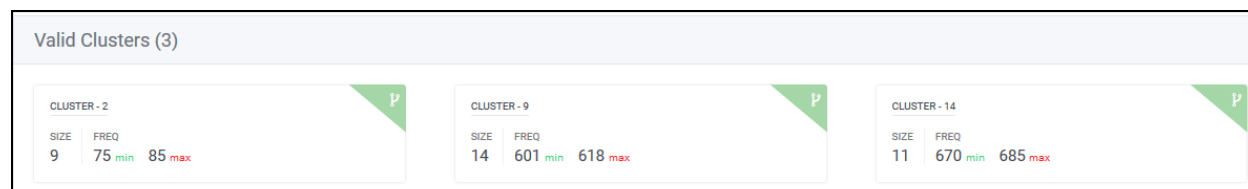
Select a time range in which to view the behavior baseline: daily, weekly, monthly, day of week, or time of day. These options display the number of times the user performed a particular activity within the specified time range.



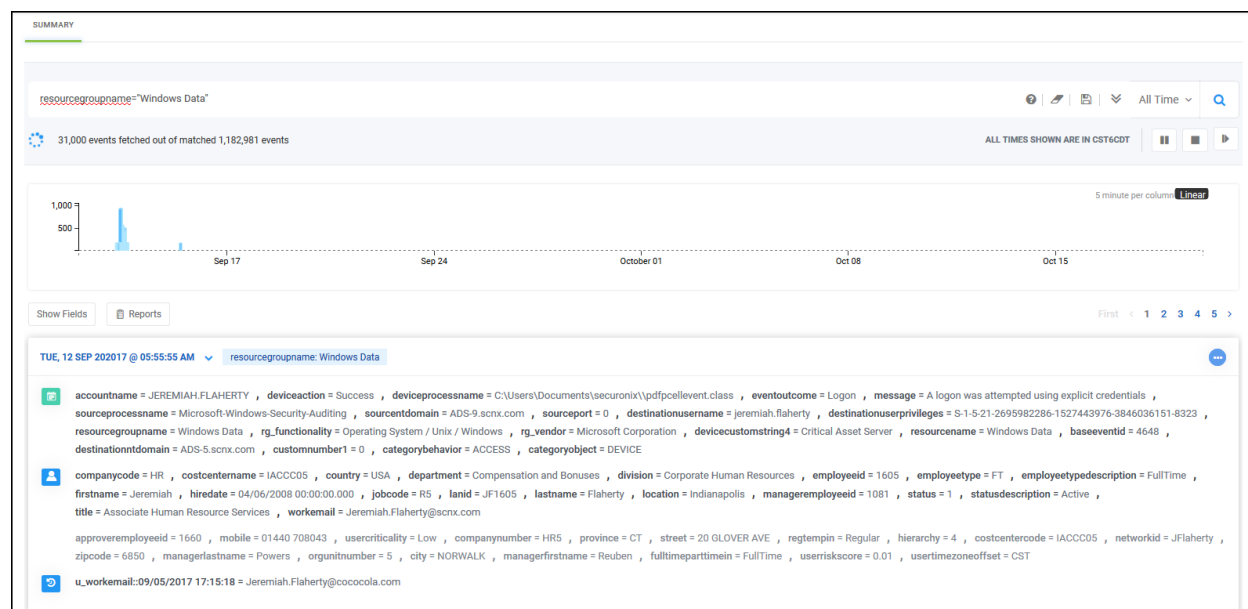
Click **All Attributes** to filter the data points on which to view the baseline. **Baseline** is defined as the maximum value for a valid cluster.



View Valid Clusters on which the profiles are generated. **Valid Clusters** are a numerical measure applied to judge various aspects of cluster validity. Multiple groups of similar data points between minimum frequency and maximum frequency help to create a valid cluster.



View a Summary of the events associated with the behavior profile you are viewing. Click any data point on the baseline to view specific events or enter a custom Spotter query. For more information about what you can do in this section, see [Spotter](#).



Editing Users

Administrative users can make changes to individual users or groups of users.



Manage Bulk Changes to Users

To manage bulk changes to users, navigate to **Menu > Views > Users**.

From the Users screen, you can search for specific users using either a simple or advanced user search. See [Performing User Searches](#) for details.

To select individual users, click the check boxes on the left side of each user you want to edit or click the top check box in the user edit column to select all users. When users are selected, the edit icon appears.

Enter your search criteria									
<input checked="" type="checkbox"/>	Employee ID	First Name	Last Name	Manager Employee ID	Email	Department	Division	Title	Employee Type
<input checked="" type="checkbox"/>	1001	HARRY	OGWA	1012	HARRY.OGWA@scnx.com	Mainframe and Midrange Administration	Global Technology	Vice President Mainframe and Midrange	FT
<input checked="" type="checkbox"/>	1002	HOMER	OGWAL	1001	HOMER.OGWAL@scnx.com	Mainframe and Midrange Administration	Global Technology	Associate Mainframe Administrator	FT
<input checked="" type="checkbox"/>	1003	HILLARY	OGWA	1001	HILLARY.OGWA@scnx.com	Mainframe and Midrange Administration	Global Technology	Associate Mainframe Administrator	FT
<input checked="" type="checkbox"/>	1004	TERRY	MERRITT	1005	TERRY.MERRITT@scnx.com	Consumer Risk	Corporate Risk	Managing Dir. Consumer Risk	FT
<input checked="" type="checkbox"/>	1005	TERRY	MERRITT	1025	TERRY.MERRITT@scnx.com	Executive Management	Corporate Risk	Managing Dir. Compliance Risk	FT
<input checked="" type="checkbox"/>	1006	MEL	GIBSON	1001	MEL.GIBSON@scnx.com	Mainframe and Midrange Administration	Global Technology	Associate Mainframe Administrator	PT
<input checked="" type="checkbox"/>	1007	RAJESH	RAO	1001	RAJESH.RAO@scnx.com	Mainframe and Midrange Administration	Global Technology	Associate Mainframe Administrator	PT
<input checked="" type="checkbox"/>	1008	AKON	SHIATSU	1001	AKON.SHIATSU@scnx.com	Mainframe and Midrange Administration	Global Technology	Associate Mainframe Administrator	PT
<input checked="" type="checkbox"/>	1009	HENRY	PATSUN	1001	HENRY.PATSUN@scnx.com	Mainframe and Midrange Administration	Global Technology	Associate Mainframe Administrator	PT

Click the edit icon to open the Modify Selected Users dialog box.

Modify Selected Users

Criticality

Low

Watchlists

-Select-

Whitelists

-Select-

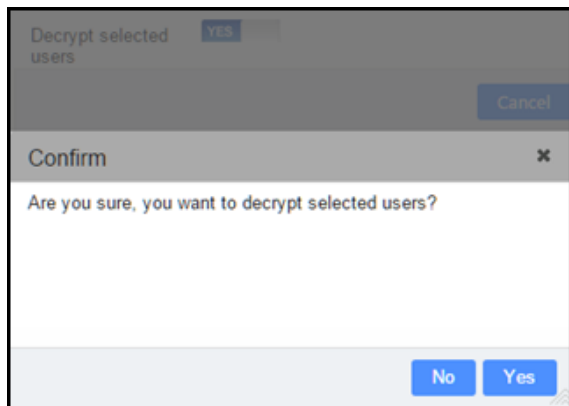
Cancel Save

In the Modify Selected Users dialog box, you can update the following items:

- **Criticality:** Change the criticality level.
- **Watchlist:** Add the users to a watchlist.
- **Whitelist:** Add the users to a whitelist. When you select this option, additional date range fields appear. Enter a **Date From** and **Date To** for the date range that the users should be added to the selected whitelist.

When you have finished modifying the selected users, click **Save**.

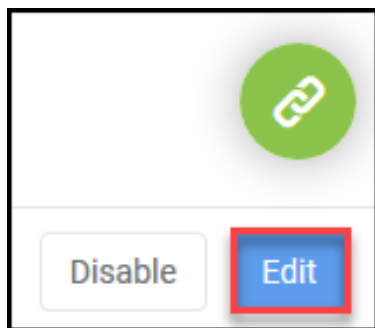
If your system is configured to encrypt user data, you will have an option to decrypt the selected users.



Edit a single user

Navigate to **Menu > Views > Users** and click the **Employee ID** for the user you want to edit.

When the User Details screen appears, scroll to bottom and click **Edit** or click **Disable** to disable to user.



Edit the details for the user and click **Update** or click **Delete** to delete the user.

Peers

A Peer Group is a grouping of users that perform similar job functions. Peer Groups can be created using any of the user attributes. You can define any number of peer groups and assign any number of users to peer groups.

Peer Groups are created to manage access outliers, access logs, and activity logs of the users that belong to a particular peer group. Users are assigned to one or multiple peer groups based on their identity attributes. Each peer group contains additional sets of users with access privileges assigned to each of them. Each access privilege held by a user is compared with all the members of each Peer Group to determine the number of users that hold the same access privilege. The greater the number of users that hold the same entitlement, the lower the probability of the access privilege being an outlier. The entitlement is determined to be an outlier if it crosses a threshold. Each user within the Peer Group may have one or multiple access privileges that are outliers. The greater the number of access privileges that are outliers, the higher the overall access risk for the user.

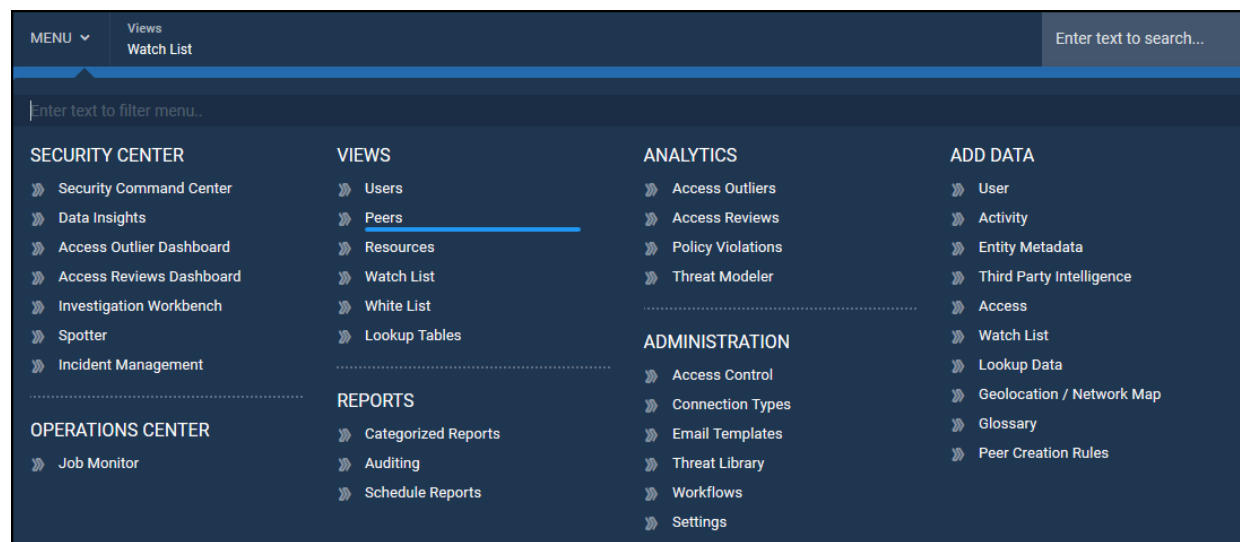
There are three ways to create new peer groups:

- **Peer Creation Rules:** Create Peer Groups using HR attributes and assign users based on selection criteria.
- **Peer Assignment Rules:** Assigns users to the appropriate Peer Groups based on the criteria specified.

For additional information, see [Peer Groups](#) in the ArcSight UBA Administration Guide.

Managing Peers

To manage Peer Groups, navigate to **Menu > Views > Peers**.



The screen displays two tabs:

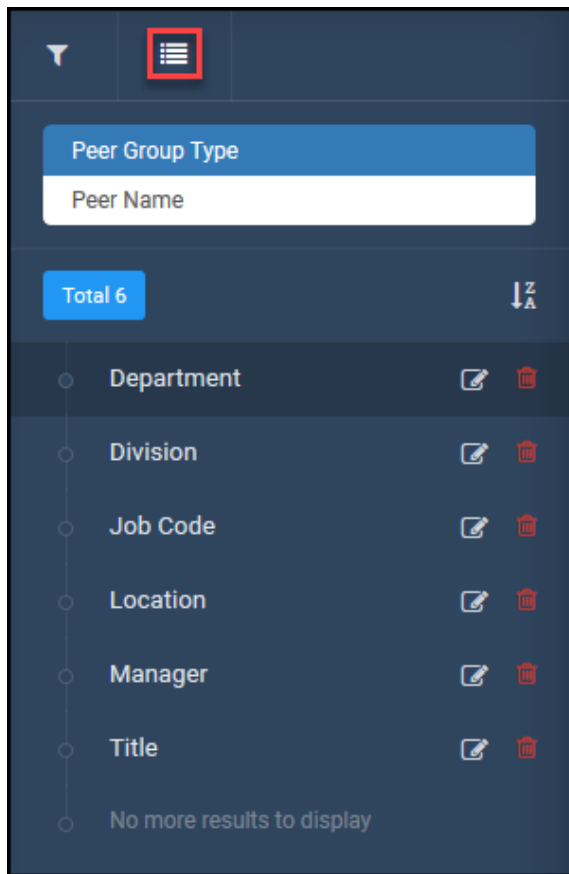
- **User Peer:** View list of peer groups for users
- **Resource Peer:** View list of peer groups for resources

In the left navigation panel, you can select a **Peer Group Type** or **Peer Name** to filter the list.

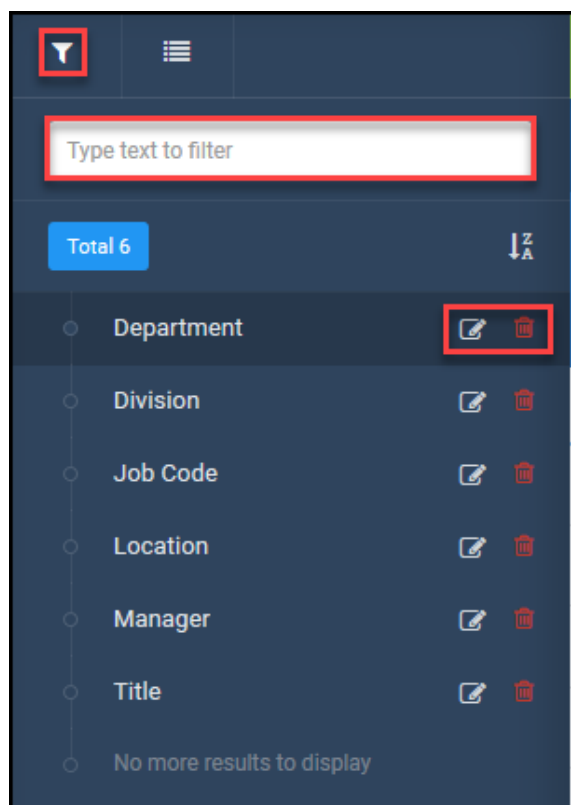
Peer Name	Member Count	Location	Peer Group Type
Advertising	12		Department
Ainsley_Moses_1065	13		Manager
Ainsling_Culkin_2681	4		Manager
Amal_Wolfe_1068	2		Manager
ANNA_Muldowney_2588	39		Manager
Antoinette_Denvir_1810	3		Manager
Audrey_Feighery_1811	14		Manager
Axel_Figueroa_1084	37		Manager
Beverly_Wright_1074	2		Manager

Use the Advanced Options menu to switch the left navigation panel options between **Peer Group Types** or **Peer Names**.

- **Peer Group Types:** Lists all the peer groups of selected Peer Group Type.
- **Peer Name:** Lists all the peers within the selected peer group.



From the left navigation panel, you can type text to filter the list of Peer Group Types and Peer Names.



Click the edit or delete icons to edit or delete a Peer Group Type.

Viewing Peer Groups

Click a peer group to view details about the group.

- On the **User Peer** tab, view information about user peer groups.
- On the **Resource Peer** tab, view details of the resource peers grouped by IP addresses or server names. When you click on a resource, you can view detailed information, such as general information about the resource and who is accessing those resource peers.

General Details

View general details about the peer group. From this screen, you can edit the peer group information and click **Update**.

General Details

Members

BACK TO PEER GROUP LIST

PEER GROUP Advertising

TYPE userpeer

GENERAL DETAILS

Name

Advertising

Provide a name to uniquely identify this connection.

Owner

User that will own the Peer Group.

Criticality

Low

The Criticality affects the risk factor of peer group.

Type

Department

Peer Type.

Cancel Update

Members

View the list of members in the peer group. You can add members or select one or multiple members to remove.

General Details

Members

Members

Add Members Remove Members

	Employee ID	First Name	Middle Name	Last Name	Manager	Email
<input checked="" type="checkbox"/>	1080	Demetria	N	Bridges	1070	Demetria.Bridges@scnx.com
<input type="checkbox"/>	1095	Rosalyn		Harding	1080	Rosalyn.Harding@scnx.com
<input type="checkbox"/>	1099	Yeo		Twist	1080	Yeo.Twist@scnx.com
<input type="checkbox"/>	1130	Amena		Parker	1080	Amena.Parker@scnx.com
<input type="checkbox"/>	1131	Montana		Bean	1080	Montana.Bean@scnx.com
<input type="checkbox"/>	1136	Jelani		Charles	1080	Jelani.Charles@scnx.com
<input type="checkbox"/>	1345	Annie		Wong	1080	Annie.Wong@scnx.com
<input type="checkbox"/>	1349	Yann		Bernard	1080	Yann.Bernard@scnx.com
<input type="checkbox"/>	1380	Anh		Tran	1080	Anh.Tran@scnx.com
<input type="checkbox"/>	1381	Jeanine		Wong	1080	Jeanine.Wong@scnx.com

First 2 Last Show 10

Total results : 12 | Total pages : 2

Click on a member to view details about the member.

Editing Peers

To select peers to edit, click the check boxes on the left side of each peer group you want to edit, or click the top check box in the user edit column to select all users.

Enter your search criteria									
<input checked="" type="checkbox"/>	Employee ID	First Name	Last Name	Manager Employee ID	Email	Department	Division	Title	Employee Type
<input checked="" type="checkbox"/>	1001	HARRY	OGWA	1012	HARRY.OGWA@scnx.com	Mainframe and Midrange Administration	Global Technology	Vice President Mainframe and Midrange	FT
<input checked="" type="checkbox"/>	1002	HOMER	OGWAL	1001	HOMER.OGWAL@scnx.com	Mainframe and Midrange Administration	Global Technology	Associate Mainframe Administrator	FT
<input checked="" type="checkbox"/>	1003	HILLARY	OGWA	1001	HILLARY.OGWA@scnx.com	Mainframe and Midrange Administration	Global Technology	Associate Mainframe Administrator	FT
<input checked="" type="checkbox"/>	1004	TERRY	MERRITT	1005	TERRY.MERRITT@scnx.com	Consumer Risk	Corporate Risk	Managing Dir. Consumer Risk	FT
<input checked="" type="checkbox"/>	1005	TERRY	MERRITT	1025	TERRY.MERRITT@scnx.com	Executive Management	Corporate Risk	Managing Dir. Compliance Risk	FT
<input checked="" type="checkbox"/>	1006	MEL	GIBSON	1001	MEL.GIBSON@scnx.com	Mainframe and Midrange Administration	Global Technology	Associate Mainframe Administrator	PT
<input checked="" type="checkbox"/>	1007	RAJESH	RAO	1001	RAJESH.RAO@scnx.com	Mainframe and Midrange Administration	Global Technology	Associate Mainframe Administrator	PT
<input checked="" type="checkbox"/>	1008	AKON	SHIATSU	1001	AKON.SHIATSU@scnx.com	Mainframe and Midrange Administration	Global Technology	Associate Mainframe Administrator	PT
<input checked="" type="checkbox"/>	1009	HENRY	PATSUN	1001	HENRY.PATSUN@scnx.com	Mainframe and Midrange Administration	Global Technology	Associate Mainframe Administrator	PT

Click the edit icon to open the Modify Selected Peer Groups dialog box.

Modify Selected Peer Groups

Criticality

Low

Save

In the Modify Selected Peer Groups dialog box, you can update the following items:

- **Criticality:** Change the criticality level.

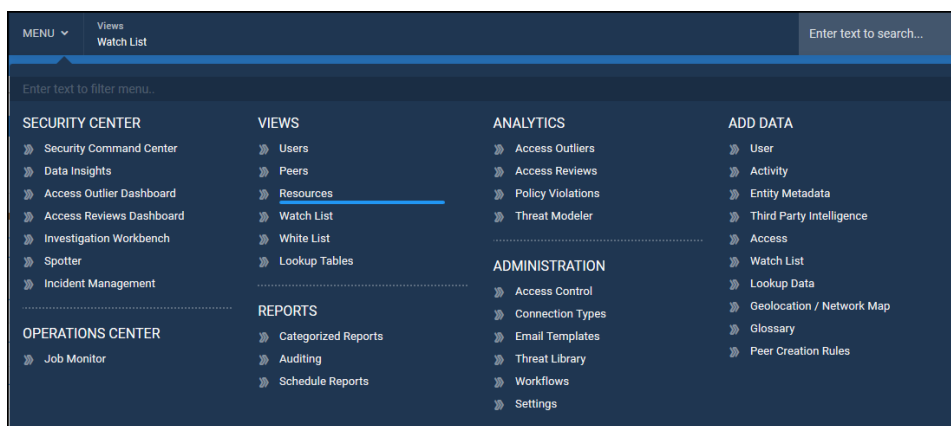
When you have finished modifying the selected peer groups, click **Save**.

Edit the details for the user and click **Update** or click **Delete** to delete the user.

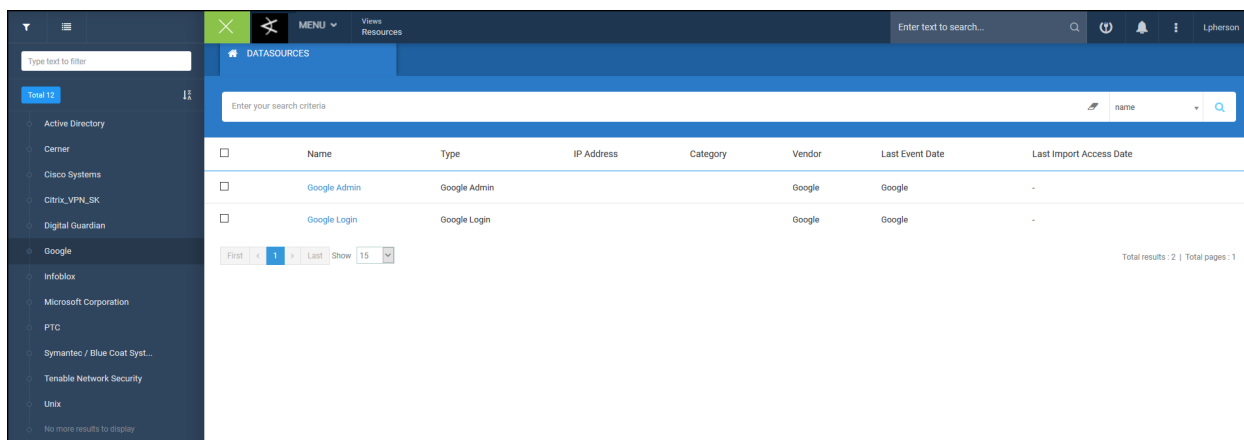
Resources

Resources are the applications, servers, databases, etc. that enable users to perform various tasks. One resource may contain one or more datasources. For example, Google is a resource, and its datasources may include Google Admin and Google Login.

To access the main Datasources screen, navigate to **Menu > Views > Resources**.

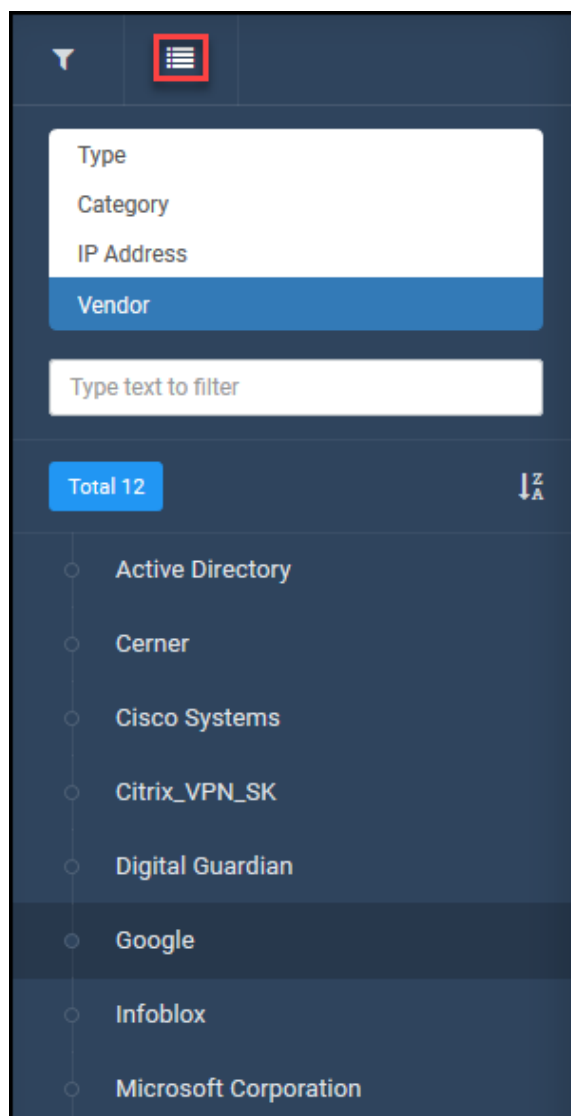


The left navigation panel displays a list of all the resource groups. Click a resource group on the left navigation panel to display a list of all datasources associated with the selected resource group.



Type test or click the Advanced Options menu to filter the list of Resource Groups. You can switch between the following Resource Group options:

- Type
- Category
- IP Address
- Vendor



Click a datasource name to view the details. The left navigation panel shows the available information associated with the selected data source.

General Details

From this screen, view the following for the datasource:

- **Resource Details:** Displays the connection details configured during data import.
- **Associated Resources:** Displays resources associated with the selected data source.
Example: Access Data for Active Directory.
- **Access/Activity Attributes:** Depending on the datasource type, the attributes associated with the datasource.

The screenshot shows the ArcSight User Behavior Analytics 6.10 interface. The sidebar on the left contains navigation options: GENERAL DETAILS, MONITOR ACTIVITIES, MONITOR ACCESS, and BEHAVIOR PROFILE. The main content area is titled 'DATASOURCES' and shows details for a 'Google Login' datasource. A red callout points to a button labeled 'Click to return to main screen'. Another red callout points to a button labeled 'Click to view' in the 'ASSOCIATED RESOURCES' section. The 'ASSOCIATED RESOURCES' table lists one resource: 'Google Login'. The 'ACCESS/ACTIVITY ATTRIBUTES' section shows two tables: '# ACCESS ATTRIBUTES' and '# ACTIVITY ATTRIBUTES'.

Attribute Name	Parent Attribute	High Privileged	Use In Outlier Detection	Mask Attribute Value?
No Access Attributes Defined				

Attribute Name	Mapped Attribute	Format	Include In Analysis?	Include In Peer Based Outliers Analysis	Display on UI?	Tpi enabled?	Mask Attribute Value?	Display Order
devicehostnameregion	devicehostnameregion		false		true		false	
devicehostnameecity	devicehostnameecity		false		true		false	

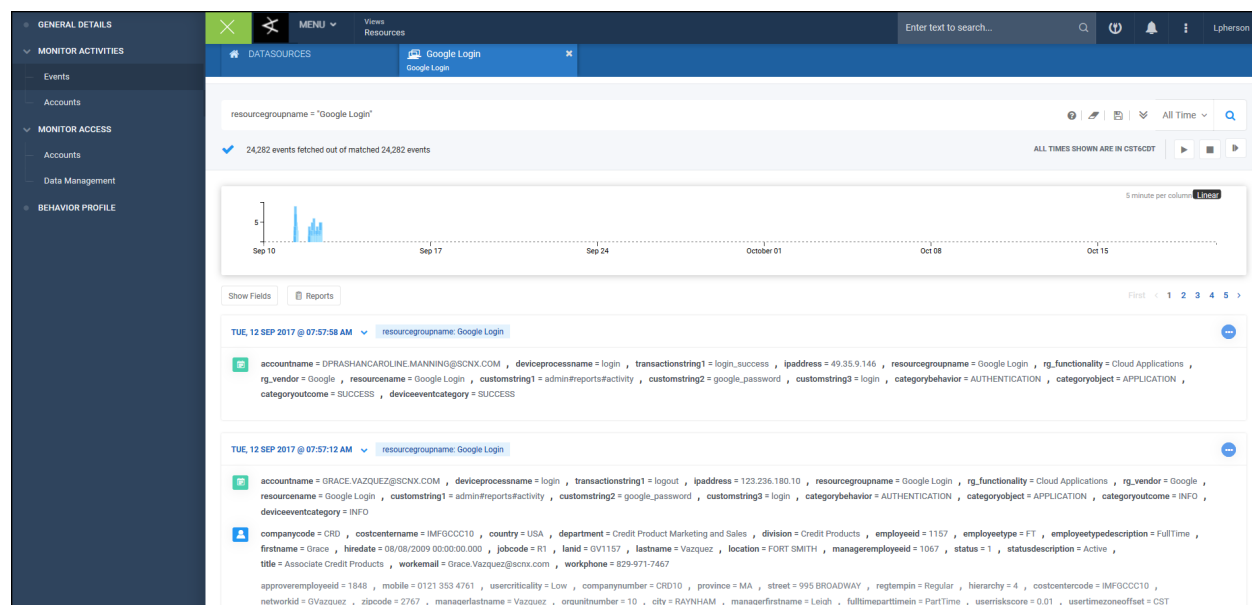
Monitor Activities

The Monitor Activities section allows you to supervise the activity data for different data sources. Within the Monitor Activities section, you can view the following:

Events

View activity events associated with the datasource.

Click on any data point or field to filter events, enter a custom Spotter query, or export the search results as [Reports](#). For information about how to search events and what actions you can take on this screen, see [Spotter](#).



Accounts

From this screen you can view accounts for the datasource. Use the dropdown to switch between viewing Correlated and Uncorrelated accounts.

Correlated Accounts

Correlated Accounts

Uncorrelated Accounts

Account Name	Employee ID	First Name	Last Name	Account Type	Account Status	Create Date
TED.THOMSON@SCNX.COM	1025	Ted	Thomson	Regular	1	2017-09-05 15:56:59.0
NORA.LEWIS@SCNX.COM	1044	NORA	LEWIS	Regular	1	2017-09-05 15:56:59.0
FAHAD.WALKER@SCNX.COM	1045	FAHAD	WALKER	Regular	1	2017-09-05 15:56:59.0
BRIAN.RODRIGUEZ@SCNX.COM	1046	BRIAN	RODRIGUEZ	Regular	1	2017-09-05 15:56:59.0
BRYAN.LEE@SCNX.COM	1047	BRYAN	LEE	Regular	1	2017-09-05 15:56:59.0
BYRON.LEWIS@SCNX.COM	1048	BYRON	LEWIS	Regular	1	2017-09-05 15:56:59.0
BOBBY.HALL@SCNX.COM	1049	BOBBY	HALL	Regular	1	2017-09-05 15:56:59.0
HARRY.YOUNG@SCNX.COM	1051	HARRY	YOUNG	Regular	1	2017-09-05 15:56:59.0
VEENA.KRISHNAMURTY@SCNX.COM	1053	VEENA	KRISHNAMURTY	Regular	1	2017-09-05 15:56:59.0
PRIYA.KING@SCNX.COM	1055	PRIYA	KING	Regular	1	2017-09-05 15:56:59.0

First < 1 2 3 4 5 > Last Show 10

Total results: 239 | Total pages: 24

- **Correlated Accounts:** Displays the Account Name and the user associated with the account. Click an Employee ID to view details about the user.
- **Uncorrelated Accounts:** Displays Account Names that have not been associated with a user. You can use this information to investigate why an account did not correlate, or if the accounts are super user accounts that do not need to be correlated.

Account Name
ACHOUDHARY@SCNX.COM
ADCARLYWELLS@SCNX.COM
AFARHAT@SCNX.COM
AJAISWAL@SCNX.COM
ANH.TRIAN@SCNX.COM
ASURESH@SCNX.COM
AVUYYURU@SCNX.COM
BENEFITS@SCNX.COM
BERNICE.O'HALLORAN@SCNX.COM@SCNX.COM
BRIAN.KING@SCNX.COM

Monitor Access

Access-related data for employees is imported from log files generated by various vendor tools. This section includes the following subsections:

- **Accounts:** Allows you to view a list of correlated, uncorrelated and soft link accounts. For each account, you can view the access-related information for a particular user on the selected data-source.
- **Data Management:** Enables you to view the different categories in your activity feed.

Information in these sections is based on Access Data and may not appear for all datasources.

Accounts

Select from the dropdown to view a list of correlated, uncorrelated, and soft link accounts. For each account, you can view the access-related information for a particular user on the selected data-source.

The screenshot shows the ArcSight User Behavior Analytics interface. The left sidebar contains navigation options: GENERAL DETAILS, MONITOR ACTIVITIES, MONITOR ACCESS, and BEHAVIOR PROFILE. The main content area is titled 'DATASOURCES' and shows a list of accounts. A dropdown menu is open for 'Correlated Accounts', showing options: Correlated Accounts, Uncorrelated Accounts, and Soft Link Accounts. The table below lists accounts with columns: Criticality, Account Name, Description, Employee ID, First Name, Last Name, Account Type, Account Status, Actions, and Create Date.

Criticality	Account Name	Description	Employee ID	First Name	Last Name	Account Type	Account Status	Actions	Create Date
	AB2518		2518	Ashling	Barnett	User	Active	Assign To	2017-10-02 17:02:43.0
	AB2639		2639	Andreas	Baker	User	Active	Assign To	2017-10-02 17:02:43.0
	AC1073		1073	Anika	Charles	User	Active	Assign To	2017-10-02 17:02:43.0
	AC1778		1778	Amy	Coughlan	User	Active	Assign To	2017-10-02 17:02:43.0
	AC1779		1779	Alan	Carter	User	Active	Assign To	2017-10-02 17:02:43.0
	AC2681		2681	Aisling	Culkin	User	Active	Assign To	2017-10-02 17:02:43.0
	AC2785		2785	Andrew	Crean	User	Active	Assign To	2017-10-02 17:02:43.0
	AD1810		1810	Antoinette	Denvir	User	Active	Assign To	2017-10-02 17:02:43.0
	AD2451		2451	Assumpta	Donovan	User	Active	Assign To	2017-10-02 17:02:43.0

Correlated Accounts

Click an Account Name to view the General and Access Details for the account.

The screenshot shows a dialog box titled 'Details for Account AB2518'. It has two tabs: 'General Details' (selected) and 'Access Details'. The 'General Details' tab displays the following information:

Account Name	AB2518
Resource	Access Data
Account Type	User
Risk Score	0.0
Criticality	Medium
Update Date	2017-10-02 17:02:43.0
Status	Active

Click an Employee ID to view details about the user. See [Users](#) for more information about these details.

User Details ✕

General Details | Organizations | Peer Groups | Monitor Access | Monitor Activities | Behavior Profile

GENERAL DETAILS

USER ID -	EMPLOYEE ID 2518	FIRST NAME Ashling	MIDDLE NAME -
LAST NAME Barrett	JOB CODE R7	DOMESTIC/INTERNATIONAL -	ORGANIZATION UNIT NUMBER 7
EMPLOYEE TYPE FT	PROMOTED -	EMPLOYEE TYPE DESCRIPTION FullTime	LAST PERFORMANCE REVIEW DATE -
FULL TIME/PART TIME FullTime	COST CENTER NAME IACCC07	COST CENTER CODE IACCC07	SHIFT CODE -
ORGANIZATION UNIT NUMBER 7	MAIL CODE -	NAME PREFIX -	USER GROUP -
STANDARD HOURS -	DEPARTMENT Cash Planning and Management	LAST PERFORMANCE REVIEW RESULT -	REGULAR/TEMPORARY Regular
CRITICALITY Low	NETWORK ID ABarrett	COMPANY CODE Cash	NAME SUFFIX -
COMPANY NUMBER CASH7	PREFERRED NAME -	HERARCHY 4	TITLE Associate Cash Management
STATUS 1	DIVISION Corporate Strategy and Planning	STATUS DESCRIPTION Active	COMMENTS -
LAN ID	DATA SOURCE		

Click **Assign To** to assign the account to a user.

Assign To User ✕

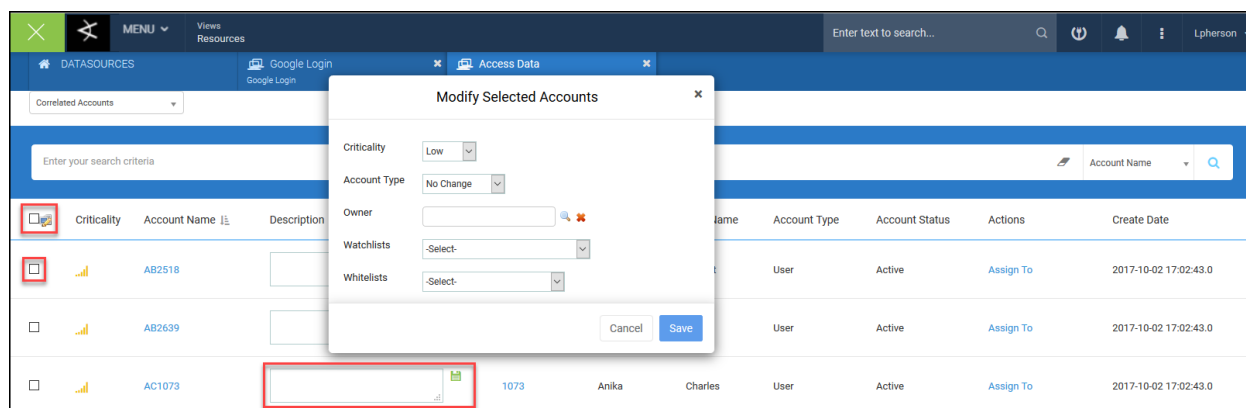
Correlate Account ▾

Enter your search criteria 🔍 employeeid ▾ 🔍

	Employee ID	First Name	Middle Name	Last Name	Manager	Email
<input type="radio"/>	1001	HARRY	A	OGWA	1012	HARRY.OGWA@scnx.com
<input type="radio"/>	1002	HOMER	B	OGWAL	1001	HOMER.OGWAL@scnx.com
<input type="radio"/>	1003	HILLARY	C	OGWA	1001	HILLARY.OGWA@scnx.com
<input type="radio"/>	1004	TERRY	D	MERRITT	1005	TERRY.MERRITT@scnx.com
<input type="radio"/>	1005	TERRY	S	MERRITT	1025	TERRY.MERRITT@scnx.com
<input type="radio"/>	1006	MEL		GIBSON	1001	MEL.GIBSON@scnx.com
<input type="radio"/>	1007	RAJESH		RAO	1001	RAJESH.RAO@scnx.com

Assign

Modify accounts by selecting an one or multiple accounts and clicking the edit icon.



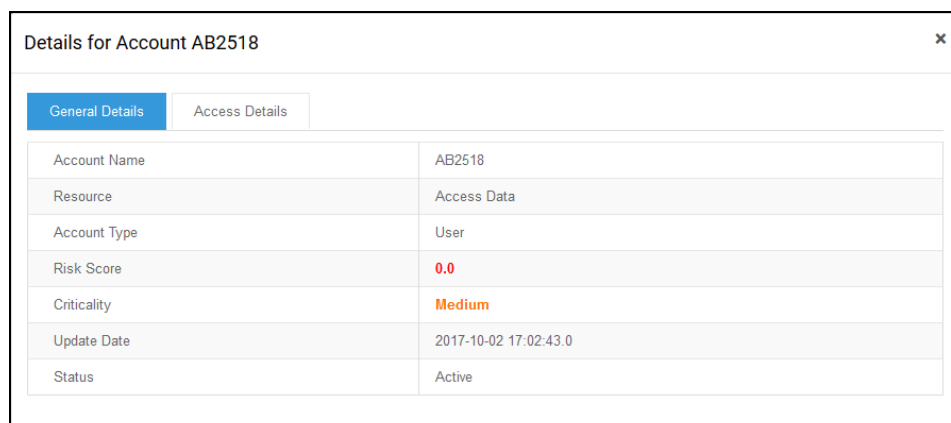
Specify the following and click **Save**:

- Criticality
- Account Type
- Owner
- Watchlists
- Whitelists

Enter a description of the access entitlements and click the green Save icon to add an entry into the ArcSight UBA Glossary of access entitlements. Example: CN=Portal_User, OU=Applications, OU=Corporate, DC=sec.

Uncorrelated Accounts

Click an Account Name to view the General and Access Details for the account.

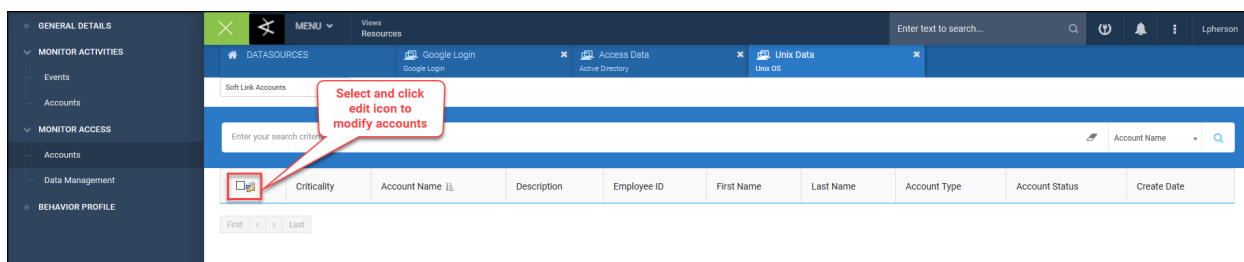


Modify accounts by selecting an one or multiple accounts and clicking the edit icon. Specify the following and click **Save**:

- Criticality
- Account Type
- Owner
- Watchlists
- Whitelists

Soft Link Accounts

View information about soft link accounts, if present.



Modify accounts by selecting an one or multiple accounts and clicking the edit icon. Specify the following and click **Save**:

- Criticality
- Account Type
- Owner
- Watchlists
- Whitelists

Data Management

View and modify Access Value for users, and add definitions into the ArcSight UBA Glossary of access entitlements.

The screenshot shows the ArcSight UBA interface with the 'Access Data' view selected. The table below represents the data shown in the interface.

	Criticality	Access Value	Owner 1 Employee ID [Rank]	Owner 2 Employee ID [Rank]	Owner 3 Employee ID [Rank]	Owner 4 Employee ID [Rank]	Owner 5 Employee ID [Rank]	Exclude In Outlier Analysis	Glossary
		AD-LA-DC1						false	

Navigation controls at the bottom include 'First', '1', '>', 'Last', 'Show 15', and 'Total results'.

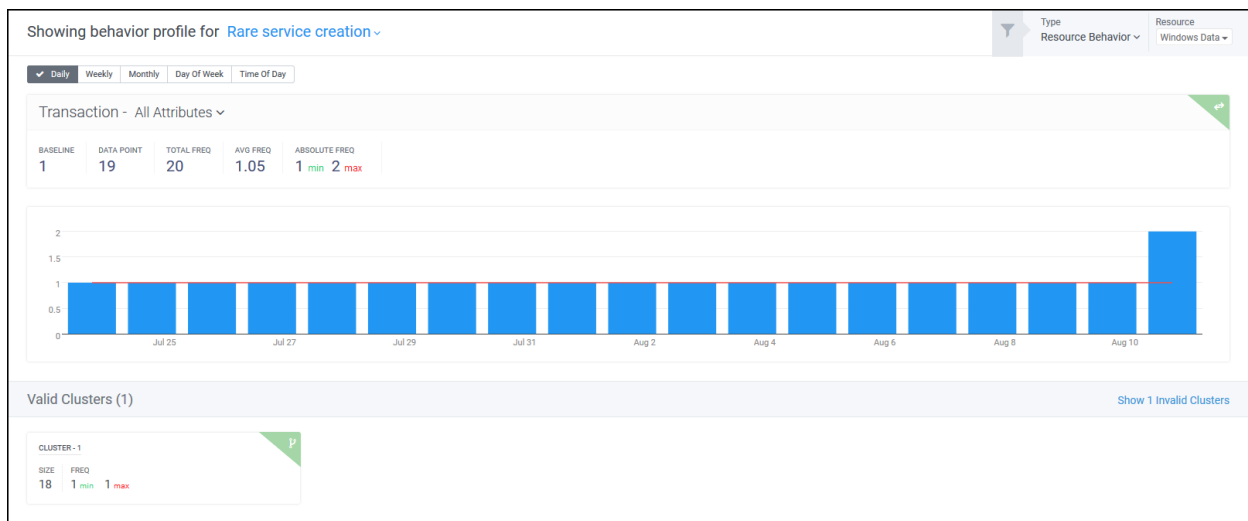
Select an Access Value and click edit icon to modify access data.

Click the green Save icon and enter a definition of the access entitlements to add an entry into the ArcSight UBA Glossary of access entitlements. Example: CN=Portal_User, OU=Applications, OU=Corporate, DC=sec.

Resource Behavior Profiles

Behavior profiling analyzes what users do on a company network by collecting all user privileges, resources, and activities, establishing a baseline of normal behavior, and then identifying the abnormal or outlier behaviors to bring to the attention of security administrators. Behavior profiles are generated based on attributes in the datasource, which are specified during policy creation and selected based on the requirements for the policy.

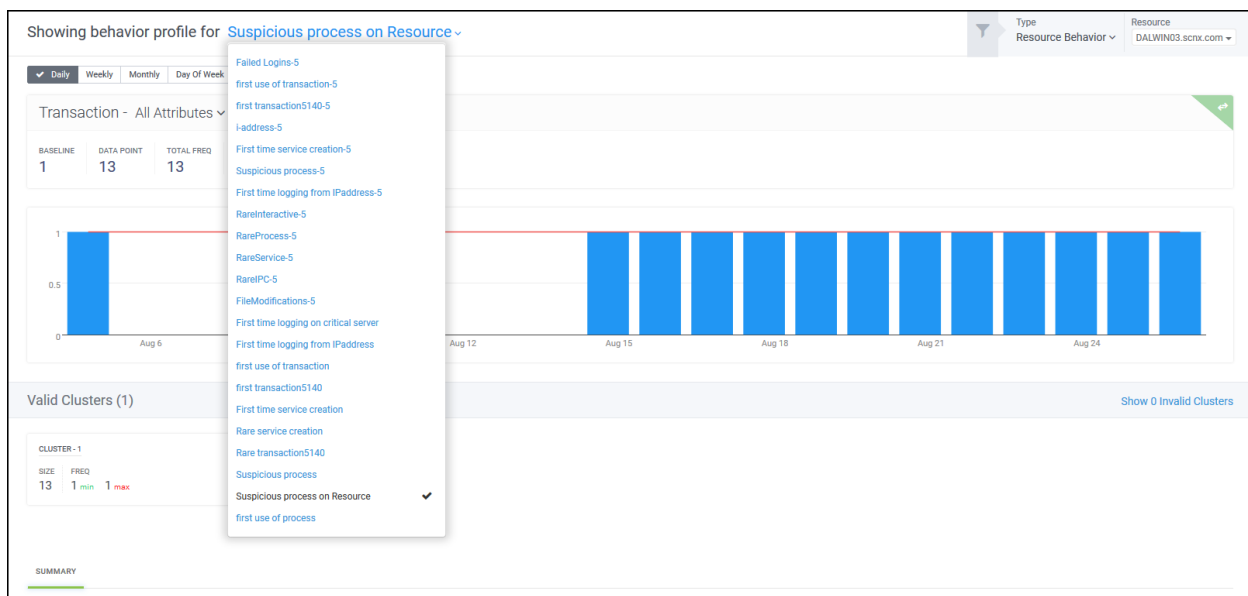
For example, for the policy Rare Service Creation, if one service account is created on Windows per day, ArcSight UBA establishes a baseline of *one, daily* for the resource. If two service accounts are created on Windows in one day, ArcSight UBA detects the rare behavior as an outlier, and a violation is generated.



For more detailed information about how behavior profiles are generated, refer to [Behavior Profiles](#) in the Administration Guide.

On the Behavior Profile screen for a Resource, you can perform the following actions:

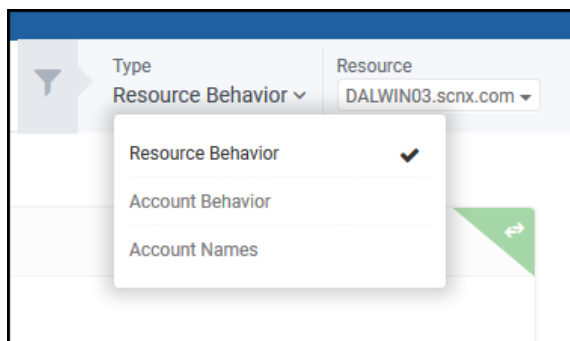
Select a policy that has been configured for the datasource for which to view the behavior profile.



From the **Type** dropdown, select options to view the Resource Behavior, the Account Behavior, and the Account Names.

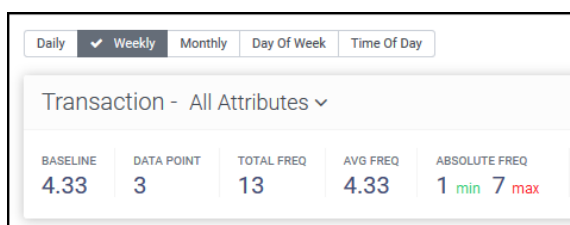


Note: Menu options may vary based on the violation entity selected during policy creation.

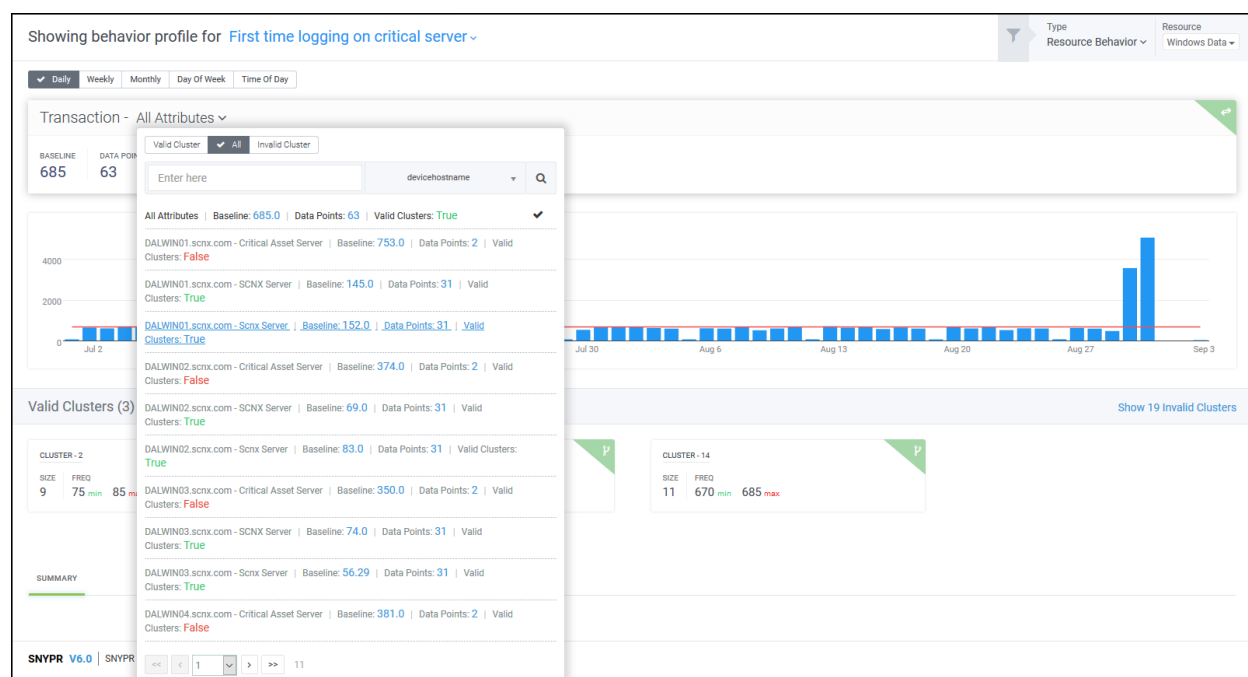


- **Resource Behavior** shows the baseline activities for the selected resource and any anomalies that deviated from the baseline across time line.
 - **Resource:** Select a specific resource from dropdown to view behavior profile for that resource.
- **Account Behavior** shows account behavior across the time line for the selected resource.
 - **Resource:** Select a specific resource from dropdown to view behavior profile for that resource.
- **Account Names** shows the behavior profile for the account across a time line for the selected resource.
 - **Resource:** Select a specific resource from dropdown to view behavior profile for that resource.
 - **Account:** Select an account from the dropdown to view events for that account.

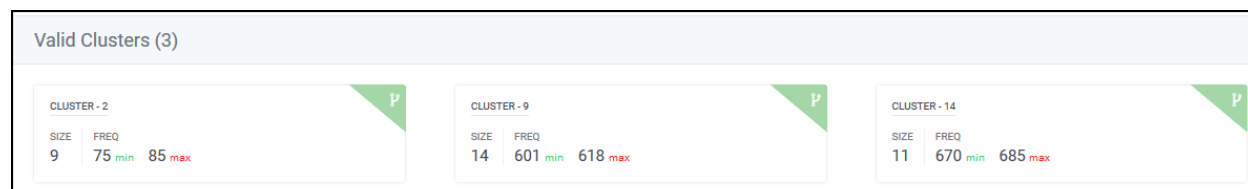
Select a time range in which to view the behavior baseline: daily, weekly, monthly, day of week, or time of day.



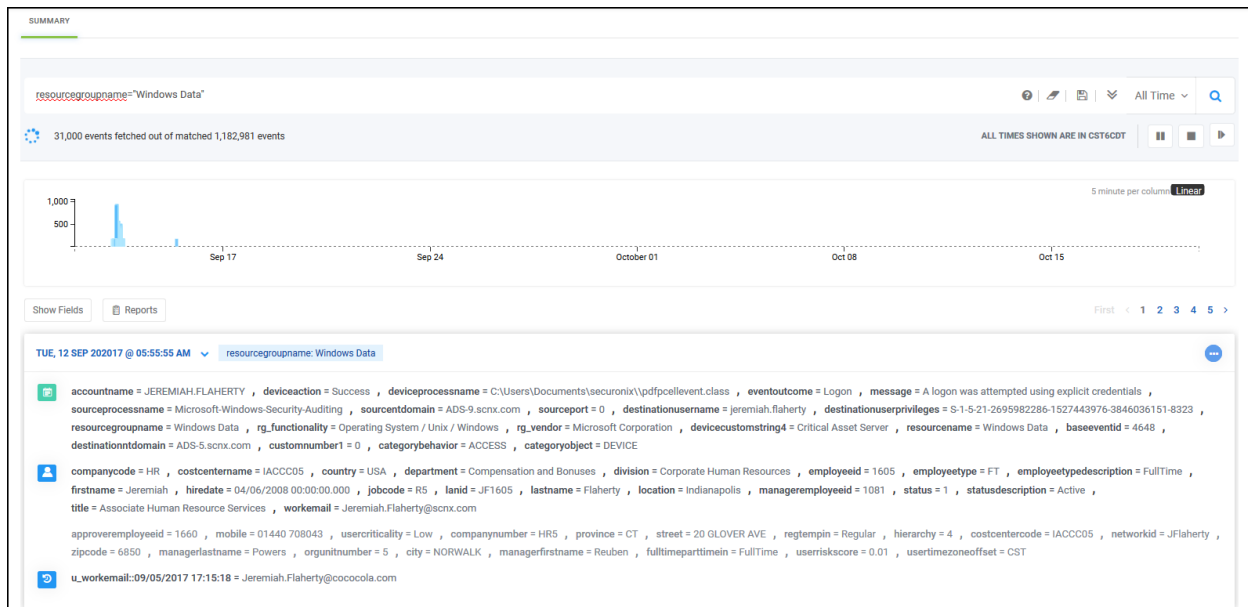
Click **All Attributes** to filter the data points on which to view the baseline. **Baseline** is defined as the maximum value for a valid cluster.



View Valid Clusters on which the profiles are generated. **Valid Clusters** are a numerical measure applied to judge various aspects of cluster validity. Multiple groups of similar data points between minimum frequency and maximum frequency help to create a valid cluster.



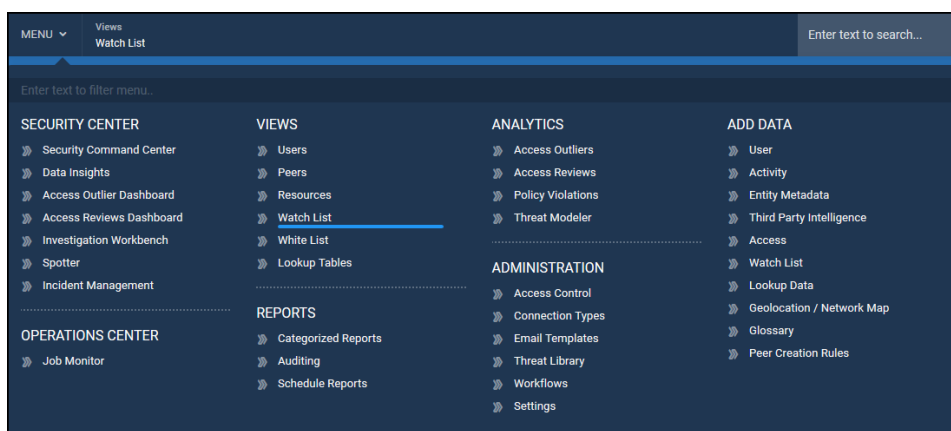
View a Summary of the events associated with the behavior profile you are viewing. Click any data point on the baseline to view specific events or enter a custom Spotter query. For more information about what you can do in this section, see [Spotter](#).



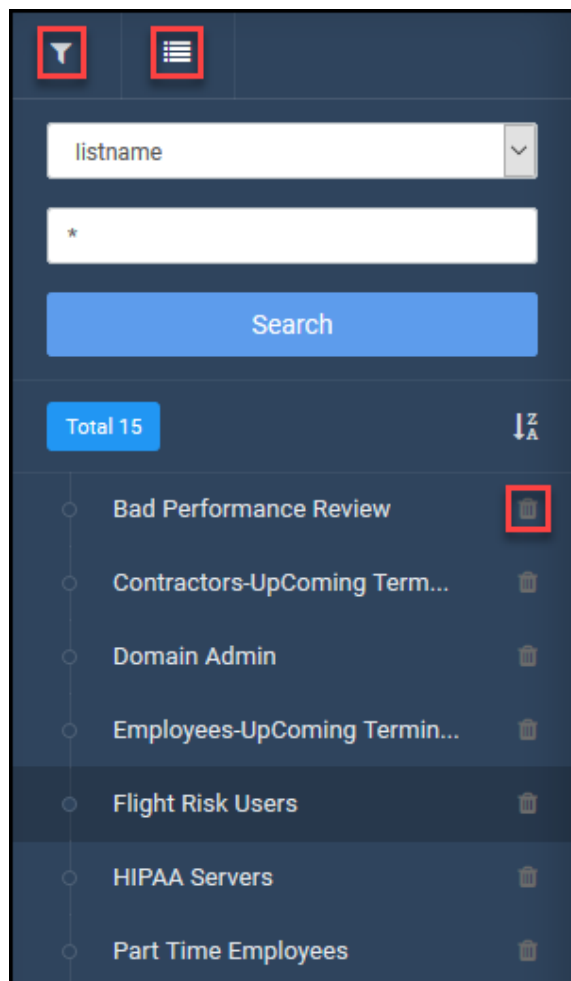
Watch List

A watch list is a means to place entities on a close watch based on inherent risks. This feature helps to monitor a user, account, host, etc. that is deemed problematic and requires special attention. For example, a user who has an upcoming termination event can be put on a watch list to closely monitor the activities that the user performs. Security analysts are notified if the user performs certain actions such as data exfiltration or inappropriate data access. Another example could be a malware infected account that is put on a watch list to closely monitor its activities and detect further activities. For information about how to create a watch list, see [Watch Lists](#) in the ArcSight UBA Administration Guide.

From the Watch List screen, you can view watch lists, manage members in a watch list, and delete watch lists. To access Watch Lists, navigate to **Menu > Views > Watch Lists**.



Select a watch list from the left navigation panel. You can type text to filter the list or click the Advanced Options menu to search for a specific watch list. Click the delete icon to delete a watch list.



When you select a watch list, the list of members appear on the right side of the screen. From here, you can add, remove, or view members in a watch list. Members can be users, activity accounts, network addresses, or resources.

Watch List

Enter your search criteria

entityname

Add Member(s) Remove Member(s) Watch List Type : Users

	Entity Name	Reason	Confidence Level (between 0 to 1)	expirydate	createdate
<input type="checkbox"/>	1127		1.0	09/15/2018 20:11:10	09/15/2017 20:11:10
<input type="checkbox"/>	1128		1.0	09/15/2018 20:11:10	09/15/2017 20:11:10
<input type="checkbox"/>	1129		1.0	09/15/2018 20:11:10	09/15/2017 20:11:10
<input type="checkbox"/>	1130		1.0	09/15/2018 20:11:10	09/15/2017 20:11:10
<input type="checkbox"/>	1131		1.0	09/15/2018 20:11:10	09/15/2017 20:11:10
<input type="checkbox"/>	1132		1.0	09/15/2018 20:11:10	09/15/2017 20:11:10
<input type="checkbox"/>	1135		1.0	09/15/2018 20:11:10	09/15/2017 20:11:10
<input type="checkbox"/>	1136		1.0	09/15/2018 20:11:10	09/15/2017 20:11:10
<input type="checkbox"/>	1138		1.0	09/15/2018 20:11:10	09/15/2017 20:11:10
<input type="checkbox"/>	1139		1.0	09/15/2018 20:11:10	09/15/2017 20:11:10
<input type="checkbox"/>	1140		1.0	09/15/2018 20:11:10	09/15/2017 20:11:10
<input type="checkbox"/>	1142		1.0	09/15/2018 20:11:10	09/15/2017 20:11:10
<input type="checkbox"/>	1144		1.0	09/15/2018 20:11:10	09/15/2017 20:11:10

Click an Entity Name to view details about the entity.

User Details

General Details Organizations Peer Groups Monitor Access Monitor Activities Behavior Profile

GENERAL DETAILS

USER ID	EMPLOYEE ID	FIRST NAME	MIDDLE NAME
-	2518	Ashling	-
LAST NAME	JOB CODE	DOMESTIC/INTERNATIONAL	ORGANIZATION UNIT NUMBER
Barrett	R7	-	7
EMPLOYEE TYPE	PROMOTED	EMPLOYEE TYPE DESCRIPTION	LAST PERFORMANCE REVIEW DATE
FT	-	FullTime	-
FULL TIME/PART TIME	COST CENTER NAME	COST CENTER CODE	SHIFT CODE
FullTime	IACCC07	IACCC07	-
ORGANIZATION UNIT NUMBER	MAIL CODE	NAME PREFIX	USER GROUP
7	-	-	-
STANDARD HOURS	DEPARTMENT	LAST PERFORMANCE REVIEW RESULT	REGULAR/TEMPORARY
-	Cash Planning and Management	-	Regular
CRITICALITY	NETWORK ID	COMPANY CODE	NAME SUFFIX
Low	ABarrett	Cash	-
COMPANY NUMBER	PREFERRED NAME	HERARCHY	TITLE
CASH7	-	4	Associate Cash Management
STATUS	DIVISION	STATUS DESCRIPTION	COMMENTS
1	Corporate Strategy and Planning	Active	-
LAN ID	DATA SOURCE		

Adding Members to a Watch List

Click **Add Member(s)** to select entities to add to the watch list. When all the entities are selected, click **Add User(s)**.

Add Member(s)

*

employeeid

Q

<input type="checkbox"/>	Employee ID <small>1</small>	First Name	Middle Name	Last Name	Manager	Email
<input type="checkbox"/>	1001	HARRY	A	OGWA	1012	HARRY.OGWA@scnx.com
<input type="checkbox"/>	1002	HOMER	B	OGWAL	1001	HOMER.OGWAL@scnx.com
<input type="checkbox"/>	1003	HILLARY	C	OGWA	1001	HILLARY.OGWA@scnx.com
<input type="checkbox"/>	1004	TERRY	D	MERRITT	1005	TERRY.MERRITT@scnx.com
<input type="checkbox"/>	1005	TERRY	S	MERRITT	1025	TERRY.MERRITT@scnx.com
<input type="checkbox"/>	1006	MEL		GIBSON	1001	MEL.GIBSON@scnx.com
<input type="checkbox"/>	1007	RAJESH		RAO	1001	RAJESH.RAO@scnx.com
<input type="checkbox"/>	1008	AKON		SHIATSU	1001	AKON.SHIATSU@scnx.com
<input type="checkbox"/>	1009	HENRY		PATSUN	1001	HENRY.PATSUN@scnx.com
<input type="checkbox"/>	1010	TONY		KULDIP	1001	TONY.KULDIP@scnx.com

First < 1 2 3 4 5 > Last Show 10

Total results : 666 | Total pages : 67

Add User(s)

The **Add Member(s)** screen appears. Complete the following information:

- **Watch List:** Select from dropdown.
- **Reason:** Enter a reason for adding the member to the watch list.
- **Expiry Date:** Enter the date the watch list will expire and the members will be removed from the list. Date Format: MM/dd/yyyy
- **Confidence Level:** Enter a value between 0 and 1 for how confident you are the entity should be added to the watch list.
- (Optional) **Location:** Enter a location for the members of the watch list.

Click **Add**, and the entities will be added to the watch list.



Note: If you have a paginated list of users, select and add users one screen at a time, changing pages may clear any selections. You may change the number of records shown per page to add multiple users.

Removing Members from a Watch List

To remove members from the list, select one or multiple users from the list of members.

<div><div>Add Member(s)</div><div>Remove Member(s)</div></div> Watch List Type : Users					
<input type="checkbox"/>	Entity Name <small>ℹ</small>	Reason	Confidence Level (between 0 to 1)	expirydate	createdate
<input type="checkbox"/>	1127		1.0	09/15/2018 20:11:10	09/15/2017 20:11:10
<input type="checkbox"/>	1128		1.0	09/15/2018 20:11:10	09/15/2017 20:11:10
<input type="checkbox"/>	1129		1.0	09/15/2018 20:11:10	09/15/2017 20:11:10
<input checked="" type="checkbox"/>	1130		1.0	09/15/2018 20:11:10	09/15/2017 20:11:10
<input checked="" type="checkbox"/>	1131		1.0	09/15/2018 20:11:10	09/15/2017 20:11:10
<input type="checkbox"/>	1132		1.0	09/15/2018 20:11:10	09/15/2017 20:11:10
<input type="checkbox"/>	1135		1.0	09/15/2018 20:11:10	09/15/2017 20:11:10
<input checked="" type="checkbox"/>	1136		1.0	09/15/2018 20:11:10	09/15/2017 20:11:10

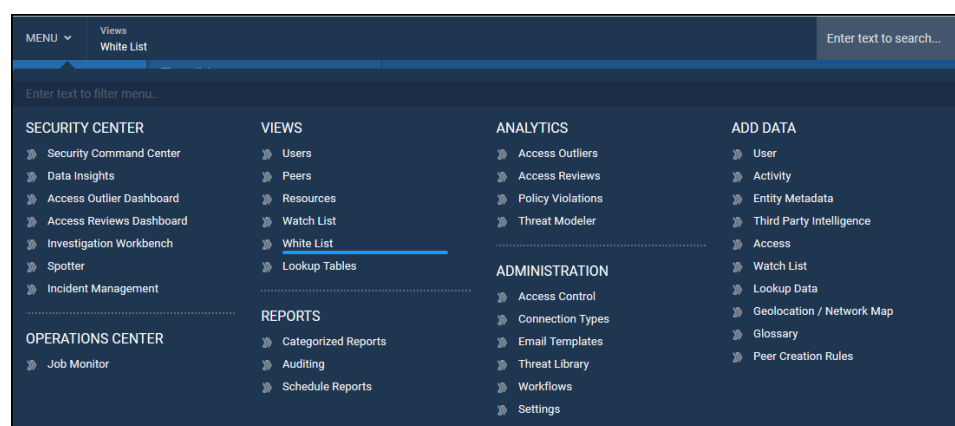
Click **Remove Member(s)**.

White List

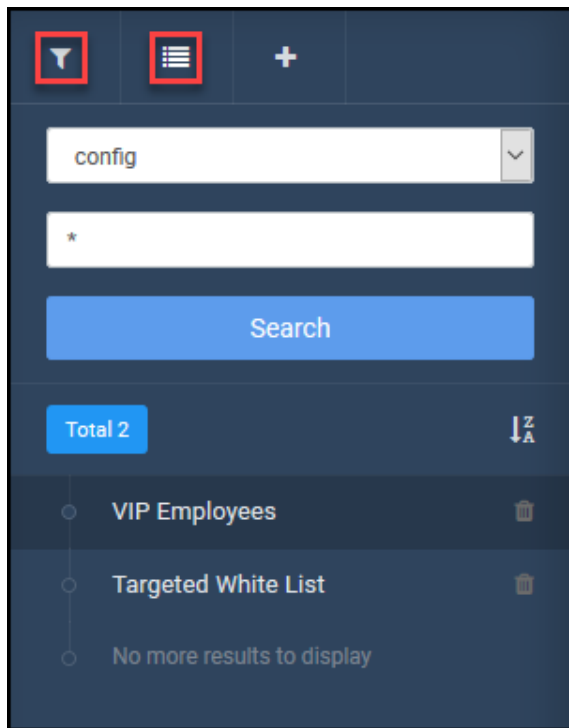
ArcSight UBA uses white lists to specify entities that are exempt from monitoring by the application. You can create the following types of white lists for an entity:

- **Global:** The white list applies to the entity. The application will not flag violations for any policies running in the environment.
- **Targeted:** The white list applies to both the entity and a specific policy or policies. The application will not flag violations for specified policies.

To create and manage global and targeted white lists, navigate to **Menu > Views > White List**.



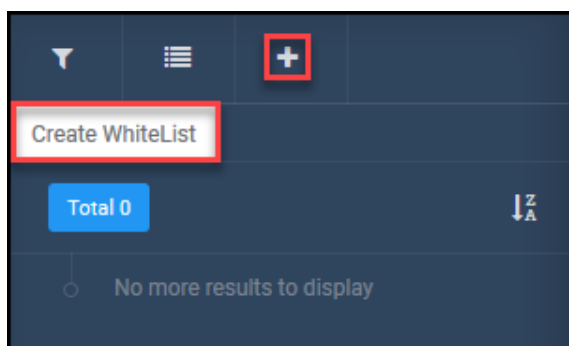
View the list of available white lists in the left navigation panel. You can type text to filter the list or click Advanced Options icon to search.



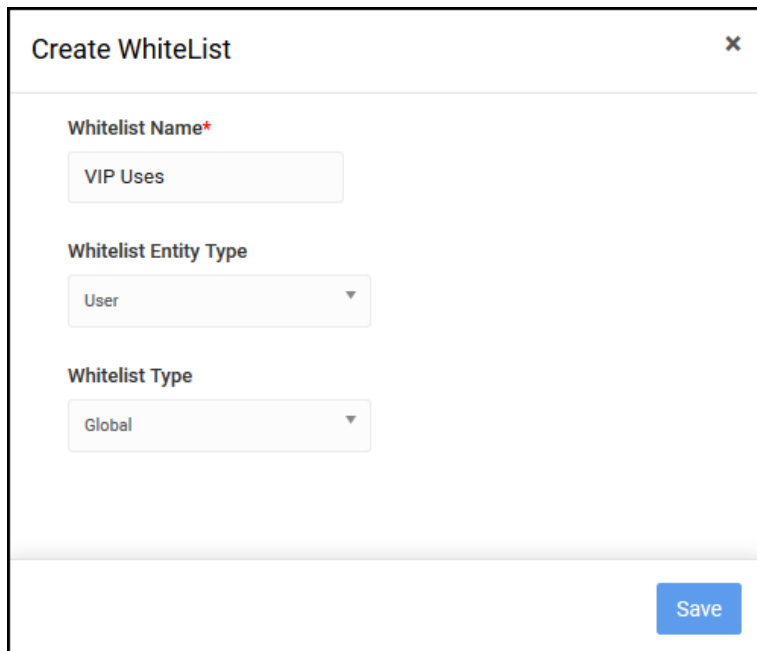
Click a white list to view and manage the list of members on the list. See [Adding New Members to White Lists](#) for information.

Creating a New White List

To create a new white list, click **+** to expand the menu and click **Create WhiteList**.



Complete the following information and click **Save**:



Create WhiteList [X]

Whitelist Name*
VIP Uses

Whitelist Entity Type
User ▼

Whitelist Type
Global ▼

Save

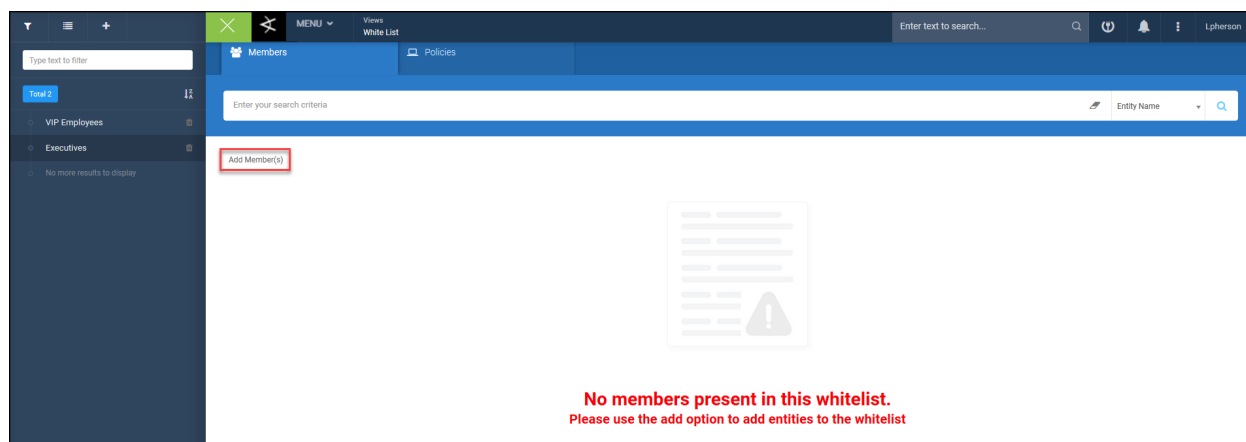
- **Whitelist Name:** Provide a unique name for the white list. Example: VIP Users
- **Whitelist Entity Type:** Select an entity type from the following options:
 - User
 - Activity Account
 - Resources
 - Activityip
 - Violator
- **Whitelist Type:** Select from dropdown:
 - Global: Applies to the entity.
 - Targeted: Applies to a both the entity and a specific policy or policies.

Proceed to Adding Members to White Lists.

Adding Members to White Lists

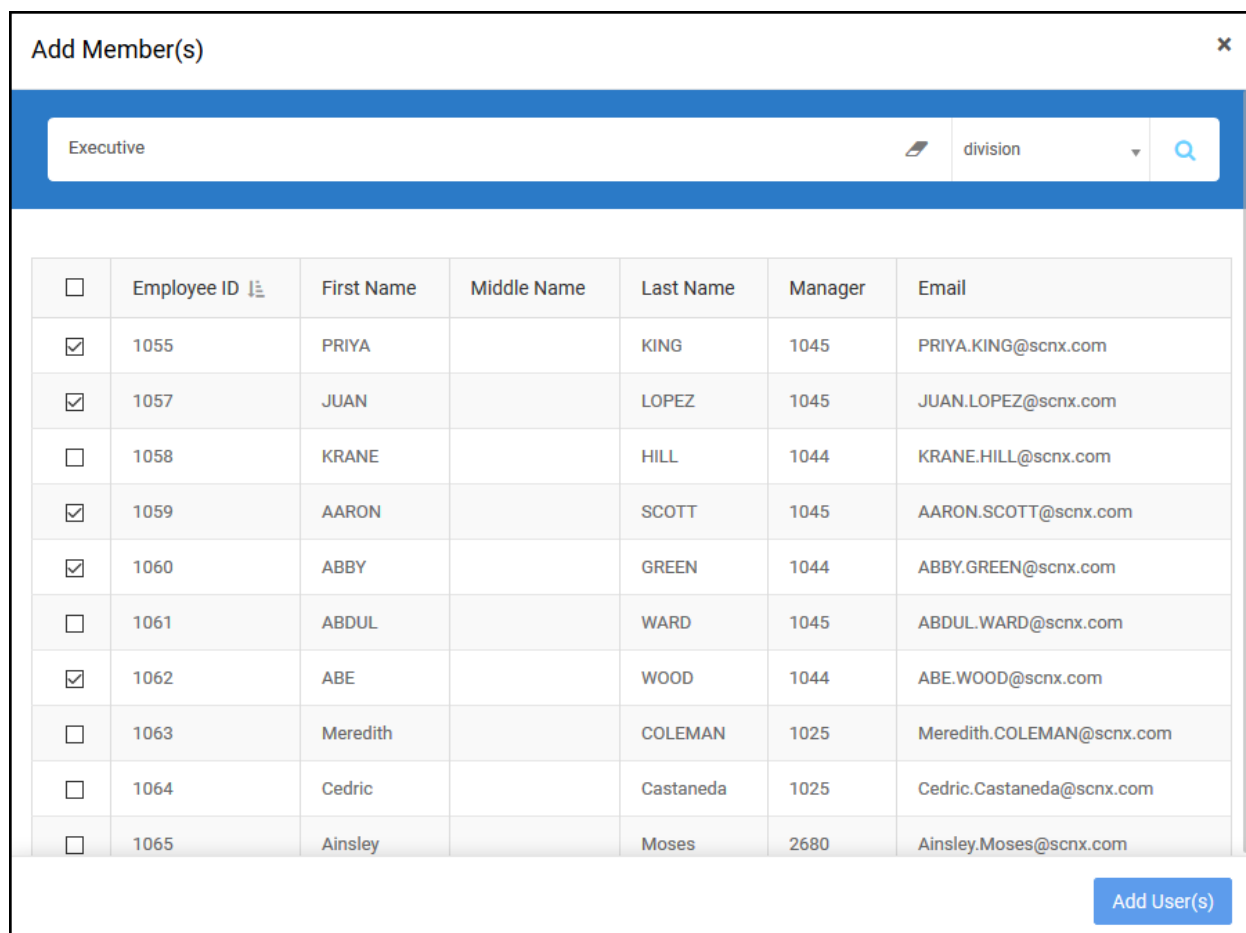
To add members to white lists, complete the following steps:

Select white list from the left navigation panel and click **Add Member(s)**.



Global White Lists

Select the members to add to the global watch list and click **Add User(s)**.



Complete the following information in the **Add Member(s)** dialogue box:

- **Whitelist Name:** Enter a whitelist name or proceed to next step to accept default.
- **Whitelist Forever:** Enable if the members will remain on the whitelist forever. Disable to enter an expiry date for the whitelist.
- **Comments:** Enter comments about the whitelist or members.
- **Do you want to reduce the risk score for selected user to zero?:** Enable to reduce the risk score of the user. The selected user will be skipped next time they violate a policy. Disable to retain user's risk score when they violate a policy.
- **Add:** Click to add the members to the whitelist.

Click **Yes** in the Add Whitelist Confirmation dialogue box to confirm adding members to whitelist.

Targeted White Lists

Select the resource group from which to add entities from the dropdown.

□

Complete steps as described in [Global White Lists](#).

Click **Remove Member(s)** to remove members from the white list.

Managing Policies for Targeted White Lists

Click the Policies tab to specify the policies to include in targeted white lists. ArcSight UBA will not flag violations for members on the white list for the specified policies.


The screenshot displays the ArcSight UBA interface. On the left, a sidebar shows a search bar and a list of categories: 'Total 2', 'VIP Employees', 'Executives', and 'No more results to display'. The main area has a top navigation bar with 'Members' and 'Policies' tabs. Below the tabs is a search bar labeled 'Enter your search criteria' and a dropdown menu for 'Policy Name'. Below the search bar are two buttons: 'Add Policy(ies)' and 'Remove Policy(ies)'. The main content area is a table with a header row 'Policy Name' and 13 rows of policy names, each preceded by a checkbox.

	Policy Name
<input type="checkbox"/>	Accounts that dont have Users
<input type="checkbox"/>	Accounts that belong to terminated user
<input type="checkbox"/>	Accounts where user dont have manager
<input type="checkbox"/>	Contractors with remote login access
<input type="checkbox"/>	SOD Access Violation
<input type="checkbox"/>	Employees with upcoming terminations within 30 days
<input type="checkbox"/>	Terminated Employees
<input type="checkbox"/>	Contractors with upcoming contract end date
<input type="checkbox"/>	Terminated Contractors
<input type="checkbox"/>	Users with Bad Performance Reviews
<input type="checkbox"/>	Users with Sunset Date in next 30 days
<input type="checkbox"/>	Recent Hires
<input type="checkbox"/>	Recent Transfers


Click **Add Policy(ies)** to select policies to add to the target white list.


Add Policy(ies)


*



Policy name





<input type="checkbox"/>	Policy Name 
<input type="checkbox"/>	Accounts that dont have Users
<input type="checkbox"/>	Accounts that belong to terminated user
<input type="checkbox"/>	Accounts where user dont have manager
<input type="checkbox"/>	Contractors with remote login access
<input type="checkbox"/>	SOD Access Violation
<input type="checkbox"/>	Employees with upcoming terminations within 30 days
<input type="checkbox"/>	Terminated Employees
<input type="checkbox"/>	Contractors with upcoming contract end date
<input type="checkbox"/>	Terminated Contractors
<input type="checkbox"/>	Users with Bad Performance Reviews

Add Policy(ies)

Select and click **Remove Policy(ies)** to exclude policies from the whitelist. ArcSight UBA will flag violations for members on the white list for policies excluded from the whitelist.

Type text to filter

Total 2

VIP Employees

Executives

No more results to display

Members

Policies

Enter your search criteria

Policy Name

Add Policy(es)

Remove Policy(es)

	Policy Name
<input type="checkbox"/>	Accounts that dont have Users
<input checked="" type="checkbox"/>	Accounts that belong to terminated user
<input type="checkbox"/>	Accounts where user dont have manager
<input type="checkbox"/>	Contractors with remote login access
<input type="checkbox"/>	SOD Access Violation
<input checked="" type="checkbox"/>	Employees with upcoming terminations within 30 days
<input type="checkbox"/>	Terminated Employees
<input type="checkbox"/>	Contractors with upcoming contract end date
<input type="checkbox"/>	Terminated Contractors
<input checked="" type="checkbox"/>	Users with Bad Performance Reviews
<input type="checkbox"/>	Users with Sunset Date in next 30 days
<input type="checkbox"/>	Recent Hires
<input type="checkbox"/>	Recent Transfers

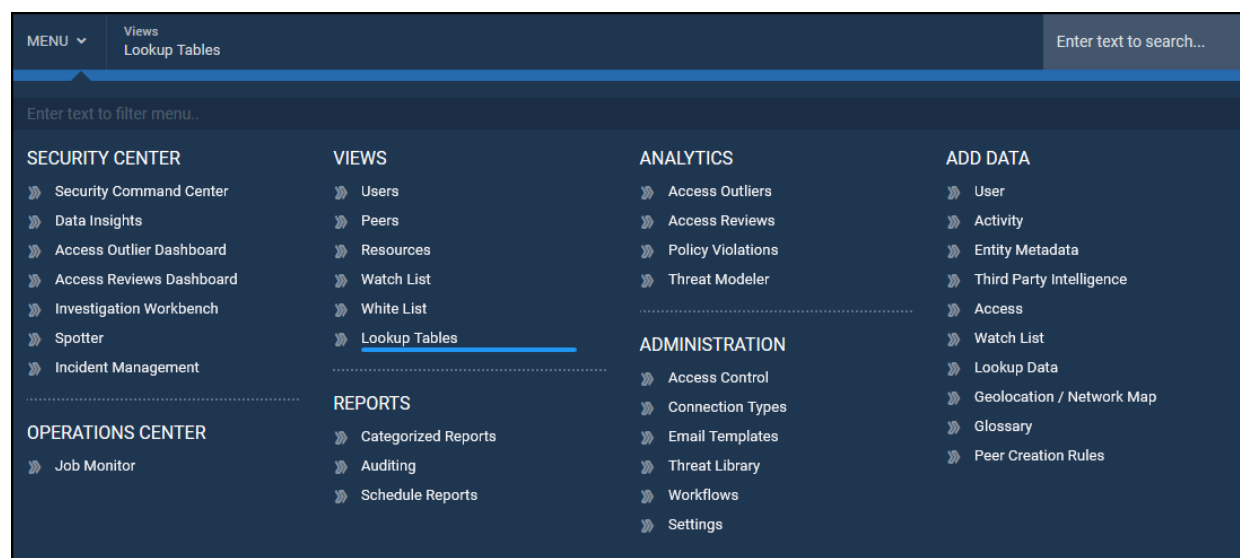
Lookup Tables

A Lookup Table is similar to an Excel table. The Lookup Table functions like an index for faster processing, wherein the lookup function is used to find a one-row or one-column range (known as a vector) for a value. The function then returns a value from the same position in a second one-row or one-column range.

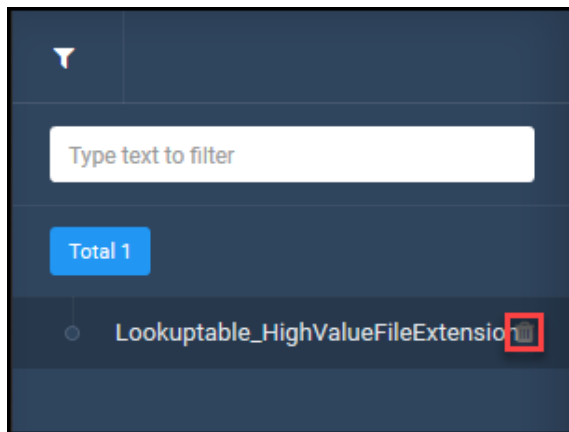
For example, an Excel spreadsheet contains Resources to Business unit mappings required to populate the business unit name against the resources table in the application. You can use a pre-processor or a stored procedure to reference this spreadsheet to obtain the corresponding values for each resource name, and then populate the resource table with the business unit name for each resource. The application provides the Lookup Tables as extra tables that can be used according to individual user needs.

For more detailed information and to import lookup data, see [Lookup Tables](#) in the Administration Guide.

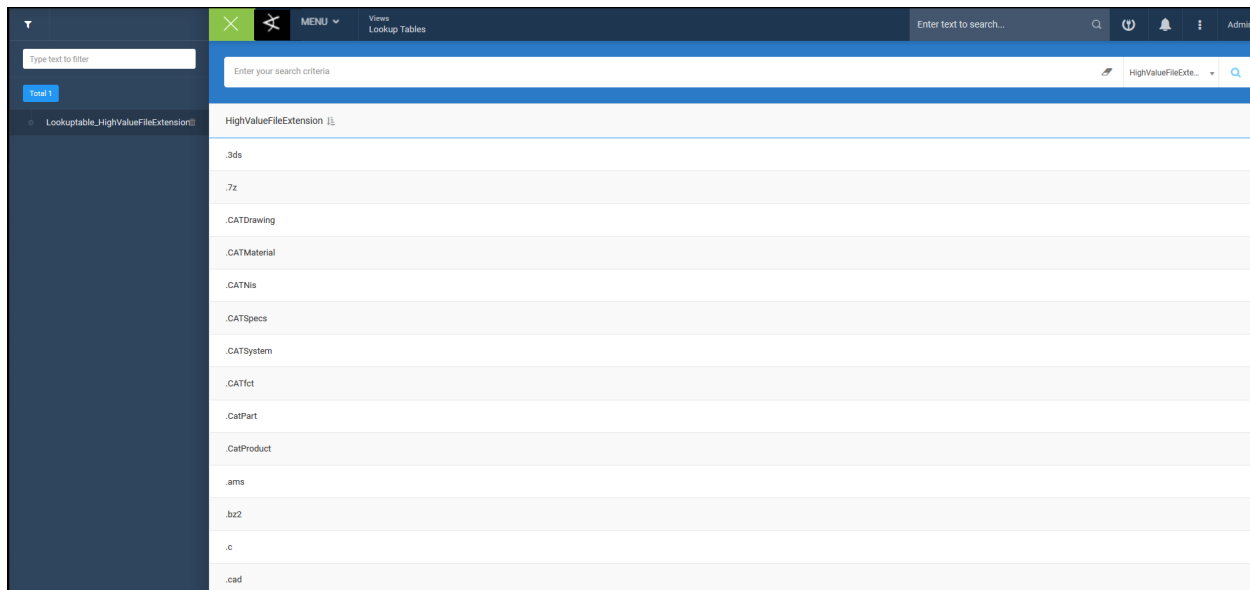
To view data in Lookup Tables, navigate to **Menu > Views > Lookup Tables**.



The left navigation panel displays the imported Lookup Tables. Type text to filter the list. You can also click the delete icon to delete a Lookup Table.



Click the name of the Lookup Table for which you want to view data. The data appears on the right. You can perform a search on the data in any field.



Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Documentation (Micro Focus ArcSight User Behavior Analytics 6.10)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to arst-techpubs@hpe.com.

We appreciate your feedback!