
Micro Focus Security

ArcSight ESM CIP for SOX

Software Version: 4.02

Solutions Guide

Document Release Date: June, 2018

Software Release Date: June, 2018



Legal Notices

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") 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.

Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is 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.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ctp/productdocs

Contents

Chapter 1: Compliance Insight Package for Sarbanes-Oxley Overview	11
Regulatory Compliance for IT Security	11
ISO Family of Standards	11
The NIST Standards	12
Compliance Insight Package for Sarbanes-Oxley 4.0	12
How CIP for SOX4 Works	13
ISO 17799:2005 Use Cases	14
Identity Management Use Cases – New for SOX4	14
User Attribution	14
Role-Based Access Monitoring	15
Executive Report– New for SOX4	16
CIP for SOX4 Architecture	20
SOX4 Use Cases	21
Chapter 2: Deployment and Configuration	25
General Resources	30
Notify, Investigate, Analyze, and Remediate	30
Notifications	30
Cases	31
Threat Response Manager via ArcSight CounterAct	31
CIP for SOX4 Device Coverage	31
Chapter 3: Solution Installation and Configuration	37
Deployment Planning	37
Verify Environment	37
Supported Platforms	38
Upgrade Planning	38
Install the SOX4 Solution	38
Installation Troubleshooting	40
Assign User Permissions	41
Configure the Sarbanes-Oxley 4 Solution	42
Configuration Planning	42
Model Assets (Assign Asset Categories)	43
Network Domains	44
ArcSight Site Asset Categories	45
Protected Address Space	46
Asset Criticality	46
Business Impact Analysis	46

How to Assign Asset Categories	47
One by One Using the Console UI	48
ArcSight Asset Import Connector	48
Sarbanes-Oxley Asset Import Template	49
Configure Active Lists	51
Configure Active Lists Using Console Active List Editor	53
Configure Active Lists by Importing a CSV File	54
Populating Active Lists from an Active Directory	55
Run the Active Directory User Group Puller Script	56
List Groups	57
Search	58
List Group Members	59
User-Role Active List	61
Configure My Filters	63
After Hours Filter	64
DBA Role	65
Intellectual Property Download Filter	66
Limit Regulation Filter	67
Maintenance Window Filter	68
Policy Definition Filter	69
Configuring the Policy Definition Filter	71
Configure Rules	72
Configure Cases	72
Configure Notification Destinations	74
Build FlexConnector(s) for Physical Access Devices	76
Configure Connector Event Mapping Files	77
Configure Sarbanes-Oxley Scenarios	78
Upgrade from SOX2 to SOX4	78
Compliance Insight Package Asset Categories	79
Compliance Insight Package Active Lists	81
Transfer SOX2 Customizations to SOX4	81
Mapping SOX2 Resources to SOX4	81
Asset Categories	81
Active Lists	84
Active Lists that Require Configuration	84
Upgrade and Configuration Instructions	88
Configure Oracle Connector to Access Monitoring	88
Oracle Preparation	89
Download the Audit SQL Scripts	89
Create a Unique Tablespace for the Audit Table	89
Configure Audit Options	91

Truncate Oracle Audit Logs	92
Create Truncate Package	92
Schedule Truncate Procedure	93
Back up and Uninstall the SOX4 Solution Package	93
Back Up the Solution Package	93
Uninstall the Solution Package	94
Verify Successful Uninstall	94
Chapter 4: ISO Sections for Sarbanes-Oxley	96
ISO 4: Risk Assessment and Treatment	96
Security Overview	96
High-Risk Event Analysis	97
Devices	97
Section 4 Resources	97
Section 4 Active Channels	97
Section 4 Dashboards	97
Section 4 Data Monitors	98
Section 4 Filters	99
Section 4 Rules	99
Section 4 Reports	99
Section 4 Queries	99
Section 4 Trends	99
ISO 5: Security Policy	100
Devices	100
Section 5 Resources	100
Section 5 Active Channels	100
Section 5 Dashboards	101
Section 5 Data Monitors	101
Section 5 Filters	101
Section 5 Rules	101
Section 5 Reports	101
Section 5 Queries	102
Section 5 Trends	102
ISO 6: Organization of Information Security	102
Case Reporting	102
Third-Party Activity	103
Devices	103
Configuration	103
Section 6 Resources	103
Section 6 Active Channels	104
Section 6 Dashboards	104

Section 6 Data Monitors	104
Section 6 Filters	104
Section 6 Rules	105
Section 6 Reports	106
Section 6 Queries	109
Section 6 Trends	111
ISO 7: Asset Management	111
Asset Inventory Reporting	111
Data Classification Reporting and Real Time Monitoring	111
Devices	112
Configuration	112
Section 7 Resources	112
Section 7 Active Channels	112
Section 7 Dashboards	113
Section 7 Data Monitors	113
Section 7 Filters	113
Section 7 Rules	113
Section 7 Reports	114
Section 7 Queries	115
Section 7 Trends	115
ISO 8: Human Resources	116
Observing New Hires	116
Internet Usage, Reporting and Monitoring	116
Former Employee Monitoring	116
Devices	117
Configuration	117
Section 8 Resources	117
Section 8 Active Lists	118
Section 8 Active Channels	118
Section 8 Dashboards	118
Section 8 Data Monitors	118
Section 8 Filters	119
Section 8 Rules	119
Section 8 Reports	119
Section 8 Queries	120
ISO 9: Physical and Environmental Security	120
Physical Building Access	120
Monitoring/Reporting Contractor's Physical Access	120
Former Employee Monitoring	121
Devices	121
Configuration	121

Section 9 Resources	121
Section 9 Active Channels	122
Section 9 Dashboards	122
Section 9 Data Monitors	122
Section 9 Filters	122
Section 9 Rules	123
Section 9 Reports	123
Section 9 Queries	123
ISO 10: Communications and Operations Management	124
User Attribution	124
Monitoring Maintenance Schedule	124
Monitoring/Reporting File Changes	125
Configuration Changes	125
Separation of Development, Test and Operational Facilities	125
Changes to Third-Party Services	125
Malicious Code Monitoring	125
System Monitoring	126
Exchange of Information and Electronic Commerce	126
Devices	126
Configuration	127
Section 10 Resources	128
Section 10 Active Lists	128
Section 10 Active Channels	128
Section 10 Dashboards	129
Section 10 Data Monitors	130
Section 10 Filters	133
Section 10 Rules	135
Section 10 Reports	136
Section 10 Queries	140
Section 10 Trends	144
Section 10 Session Lists	145
ISO 11: Access Control	145
Use Cases	145
Role-Based Access Monitoring	145
User Management	145
Authorization Changes	146
Password Policy Monitoring	146
Privileged Account Monitoring	146
Network Service Monitoring	146
Firewall Policy Monitoring	146
Network Routing Supervision	146

Network Policy Monitoring	146
Remote Access (VPN) Monitoring	147
Segregation of Networks	147
Devices	147
Configuration	147
Section 11 Resources	148
Section 11 Active Lists	150
Section 11 Session Lists	151
Section 11 Active Channels	151
Section 11 Dashboards	152
Section 11 Data Monitors	152
Section 11 Filters	155
Section 11 Rules	156
Section 11 Reports	159
Section 11 Queries	161
Section 11 Trends	163
ISO 12: Information System Acquisition Development and Maintenance	164
Use Cases	164
Attack Monitoring	164
Information Leak Monitoring	165
Systems with Persistent Vulnerabilities	165
Devices	165
Configuration Summary	166
Section 12 Resources	166
Section 11 Active Lists	166
Section 12 Active Channels	166
Section 12 Dashboards	167
Section 12 Data Monitors	167
Section 12 Filters	167
Section 12 Rules	168
Section 12 Reports	168
Section 12 Queries	169
Section 12 Trends	170
Section 12 Runtime Instructions	170
ISO 13: Information Security Incident Management	170
Use Cases	170
Escalated Threat Monitoring	170
Internal Reconnaissance	170
Devices	171
Section 13 Resources	171
Section 13 Active Channels	171

Section 13 Dashboards	171
Section 13 Data Monitors	172
Section 13 Filters	172
Section 13 Rules	172
Section 13 Reports	173
Section 13 Queries	174
Section 13 Trends	175
ISO 14: Business Continuity Management	175
Use Cases	175
Monitoring Highly Critical Machines	175
Availability Monitoring	175
Monitoring for Denial of Service Attacks	175
Devices	175
Section 14 Resources	176
Section 14 Active Channels	176
Section 14 Dashboards	176
Section 14 Data Monitors	176
Section 14 Filters	177
Section 14 Rules	177
Section 14 Reports	177
Section 14 Queries	178
ISO 15: Asset Management	178
Use Cases	178
Intellectual Property Rights Violations	178
Illegal Content Download	178
Peer-to-Peer Traffic	178
Information Leak Monitoring	179
Company Information	179
Personal Information	179
Misuse of Information Processing Facilities	179
Excessive Email Communications	179
Policy Breach Monitoring	179
Technical Compliance Checks	179
Monitoring Access to Monitoring System (ArcSight)	180
Devices	180
Configuration	180
Section 15 Resources	181
Section 15 Active Lists	181
Section 15 Active Channels	181
Section 15 Dashboards	182
Section 15 Data Monitors	182

Section 15 Filters	183
Section 15 Rules	183
Section 15 Reports	184
Section 15 Queries	185
Section 15 Trends	186
Chapter 5: Automated Response and Prevention	187
Automated Response and Prevention Architecture	187
Automated Response and Prevention Rules	187
Configure CounterAct Active Directory Resources	189
Download the CounterAct Active Directory Files	190
Configure and Copy Active Directory Files	190
Install and Configure the FlexCounterAct Connector	191
Configure the FlexCounterAct Connector as a Windows Service	191
Configure CounterAct Rules	192
Configure CounterAct Filters	194
Configure Threat Response Manager Resources	195
Install and Configure the CounterAct Connector	196
Configure CounterAct Rules	196
Configure CounterAct Filters	197
Send Documentation Feedback	199

Chapter 1: Compliance Insight Package for Sarbanes-Oxley Overview

With the passage of the Sarbanes-Oxley Act (SOX), all publicly traded companies must implement internal controls and reporting of their financial systems. Section 404 requires companies to report their internal control structures, and report about how effective those controls are at the end of each fiscal year.

The SOX Auditing Standard No. 2 published by the Public Company Accounting Oversight Board (PCAOB) further mandates that organizations and the parties who audit them assess

“control risk” in order to determine the effectiveness of your internal controls. Neither of these regulations, however, describes exactly how to demonstrate the effectiveness of your internal controls.

“Regulatory Compliance for IT Security” on page 7

“Compliance Insight Package for Sarbanes-Oxley 4.0” on page 8

“CIP for SOX4 Architecture” on page 14

“Notify, Investigate, Analyze, and Remediate” on page 21

“CIP for SOX4 Device Coverage” on page 22

Regulatory Compliance for IT Security

ArcSight’s approach to regulatory compliance in the Compliance Insight Package for Sarbanes-Oxley 4.0 (CIP for SOX4) is based on following clearly defined industry standards, in this case, ISO and NIST.

ISO Family of Standards

Compliance with the regulations that apply to your business can best be demonstrated by using a cohesive framework, such as the Code of practice for information security management, also known as ISO/IEC 17799. This standard was developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), and covers the controls and guidelines a company should consider implementing to follow due diligence and best practices in IT security. The standard covers a set of 11 main security categories:

- Risk Assessment and Treatment
- Security Policy
- Organizing Information Security
- Asset Management

- Human Resources Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Information Systems Acquisition
- Development and Maintenance Information Security Incident Management
- Business Continuity Management
- Compliance

The original version of ISO 17799 has been updated and revised and is known as ISO 17799:2005. From 2007, it is proposed that the ISO/IEC 17799 standard is renumbered to become ISO/IEC 27002. The 27000 family of ISO standards addresses information security concerns. There are currently four documents planned for the series, of which two have been published: ISO 27001 and ISO 27002 (formerly ISO 17799). ISO 27001 is the specification for an information security management system (ISMS), replacing the old BS 7799-2 standard. The basic objective of the standard is to help establish and maintain an effective information management system using a continual improvement approach. ISO 27001 is the formal standard against which organizations may seek independent certification of their Information Security Management Systems (meaning their frameworks to design, implement, manage, maintain and enforce information security processes and controls systematically and consistently throughout the organizations). Until ISO 27001 and 27002 are fully implemented later in 2007, the Sarbanes-Oxley solution will use the updated ISO 17799:2005 as its guideline.

The NIST Standards

The National Institute for Standards and Technology (NIST) develops and publishes a set of standards and guidelines for securing information systems. The Special Publication 800-53 covers the selection and employment of appropriate security controls for an information system. The document is very specific about the security controls that must be in place to comply with the standards, whereas the ISO 17799:2005 standard is more of a guideline.

Compliance Insight Package for Sarbanes-Oxley 4.0

The Compliance Insight Package for Sarbanes-Oxley version 4.0 (CIP for SOX4) provides an essential foundation for your Sarbanes-Oxley compliance program based on the ISO 17799:2005 standard. The solution enables you to monitor, prioritize, respond to, and report on network activity for systems that are subject to Sarbanes-Oxley compliance.

CIP for SOX4 provides a series of real-time checks specifically designed to evaluate risk, initiate immediate response, and provide comprehensive reporting of high and low-risk activity, to give you and your auditors assurance that the controls over the infrastructure that hosts your financial systems expose little or no risk.

CIP for SOX4 specifically addresses section 404 of the Sarbanes-Oxley Act, which applies to internal control structures. As shown in the illustration below, the solution monitors and secures the infrastructure upon which your financial systems operate. Securing your infrastructure mitigates the risk of compromise from an outside entity, and provides an essential foundation for your overall Sarbanes-Oxley reporting strategy.

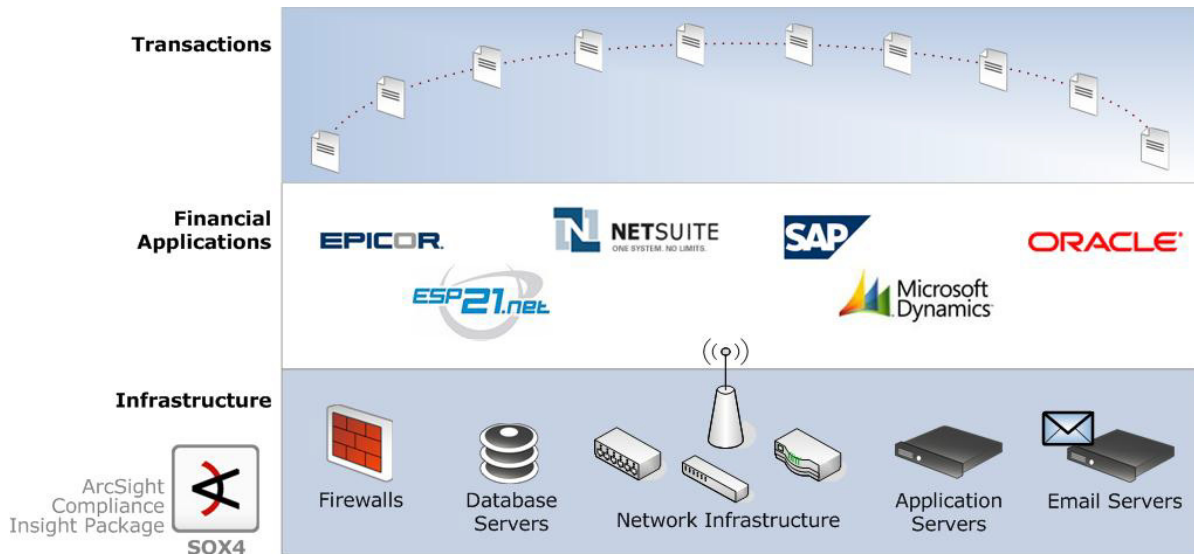


Figure 1-1 The SOX4 solution secures the infrastructure hosted on assets that are subject to Sarbanes-Oxley compliance.

This release emphasizes reporting and introduces trends, an ArcSight resource that gathers and aggregates data over long-range time periods. The trends included in the SOX4 solution provide long-term insight into activity on systems that are subject to SOX compliance, from tracking high-risk events and policy breaches to monitoring incident response and case closure rates.

This release also debuts identity management, which uses ESM v4.0's session correlation feature. Session correlation ties an IP address with a user name and role, so you can not only identify the assets involved in network traffic, but also the users behind the traffic, and their user role.

How CIP for SOX4 Works

The SOX4 solution operates specifically on SOX-related assets. The SOX4 solution uses ArcSight ESM features, such as event categorization, threat prioritization, trends, workflow, and case management, to easily identify and address activities and anomalies involving systems that are subject to Sarbanes-Oxley compliance.

The SOX4 solution is made up of a comprehensive and easily customizable set of ArcSight resources (rules, dashboards, data monitors, reports, and so on), which enable you to measure and report on your compliance with the Sarbanes-Oxley act using best practices outlined by the ISO 17799:2005 and NIST 800-53 standards. These resources satisfy the following major objectives: ■

- Real-time detection of compliance breaches, which enable you to actively identify and mitigate compliance violations before they significantly impact your business. ■
- Comprehensive reporting capabilities that support requirements of internal and external audit teams, as well as IT and executive management. ■
- The ability to demonstrate the effectiveness of controls over the infrastructure that hosts systems which are subject to Sarbanes-Oxley compliance to all levels of the organization as well as outside auditors.
- Flexibility to monitor, investigate, remediate, and report on Sarbanes-Oxley related activity and compliance status using customizable dashboards, data monitors, and reports.
- Satisfy SOX requirements for user management by associating the identity of individual users with the devices they use, and comparing their actions with their intended business role. By querying all events associated with a particular user, you can also validate that any access or authorization violation by that user did not compromise other IT or financial systems.

ISO 17799:2005 Use Cases

The SOX4 solution ensures compliance with Sarbanes-Oxley requirements by providing a comprehensive set of general security use cases based on sections 4 through 13 of the ISO 17799:2005 standard.

Each ISO section addressed by the SOX4 solution contains one or more use cases that, combined, create a comprehensive compliance strategy. These use cases directly and indirectly address Sarbanes-Oxley compliance requirements, and ensure a complete overall security monitoring, investigation, and status reporting strategy.

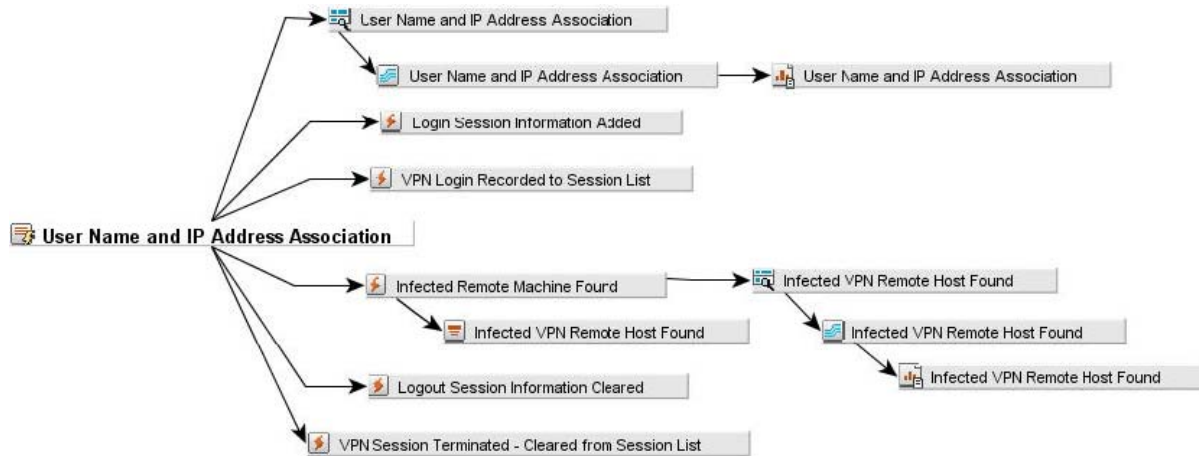
Identity Management Use Cases – New for SOX4

CIP for SOX4 adds two new identity management use cases to the IT governance structure, which satisfy sections 10 and 11 of the ISO 17799:2005 standard.

User Attribution

SOX4 includes a session list called User Name and IP Address Association that identifies IP addresses assigned during desktop and VPN logins with the user name to whom the IP address is assigned. This enables the solution to correlate events that involve traffic from those IP addresses with the username of the person who is assigned to that IP address.

A series of rules evaluate the event stream to detect when these sessions begin and end. The SOX4 solution then uses entries to this session list to detect infections that originate from remote machines and associate them with the user whose login introduced the infection. The solution also uses this list to allow access to assets by only qualified users.

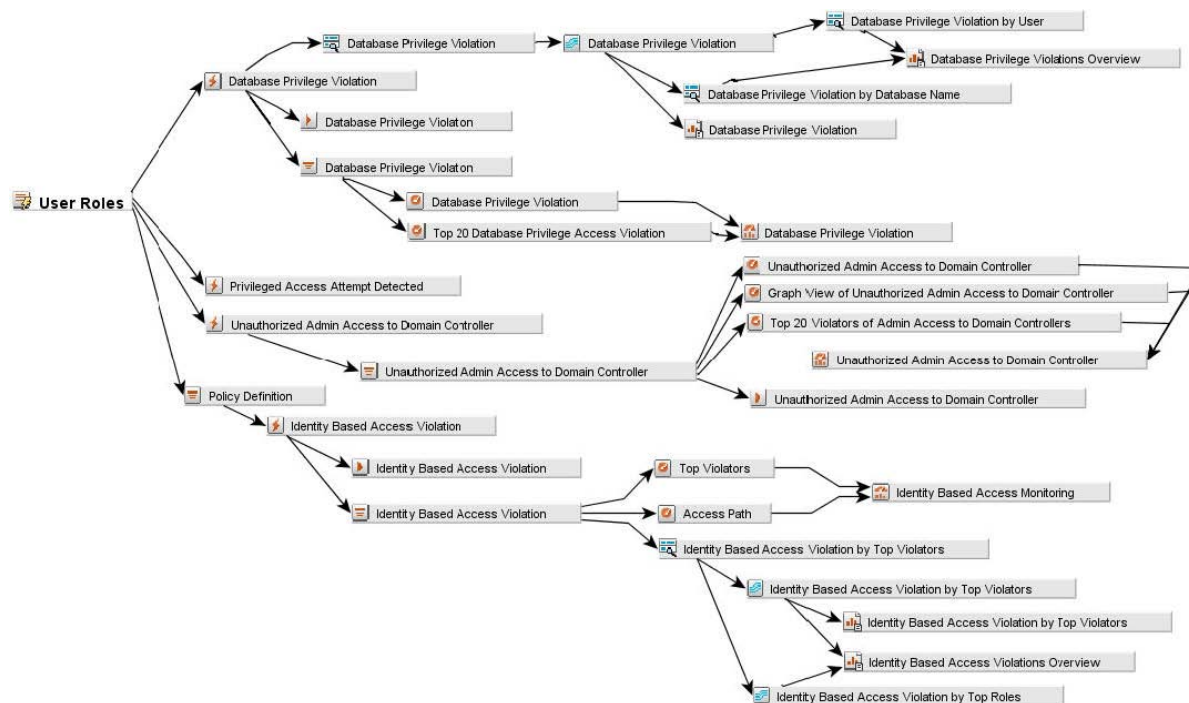


The solution also includes two long-term trends that use entries to this session list to track user/address associations and infected VPN log-ins over time. Reports then provide statistics about users and the IP addresses associated with them, and infections originating from remote hosts via VPN.

The user attribution content addresses part of the requirements of ISO section 10, Communications and Operations Management, and is described in “Section 10: Communications and Operations Management” on page 107.

Role-Based Access Monitoring

Section 11.1 of the ISO standard states that a policy should be in place to implement access controls based on business and security requirements. CIP for SOX4 provides a use case that uses an active list to store user names and their roles from manual entries, or exported directly from Active Directory. Rules then use entries to this list to detect users who attempt to gain access to a database, domain controller, or other privileged access account whose user roles do not grant them access privileges to these assets.



These rules and the policy definition filter provide a foundation for dashboards, active channels, and reports that monitor privileged user access attempts. Three trends track privileged access attempts over time, and populate identity-based access violation reports. For more about the role-based access monitoring use case, see “Section 11: Access Control” on page 128.

Executive Report– New for SOX4

CIP for SOX4 adds a new Executive Report showing an overall view of all activities in the solution as shown in the following figure.

Start Date/Time: 04-30-2007-16:25:40

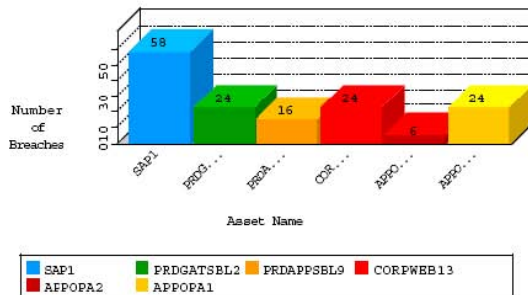
End Date/Time: 05-02-2007-16:25:40



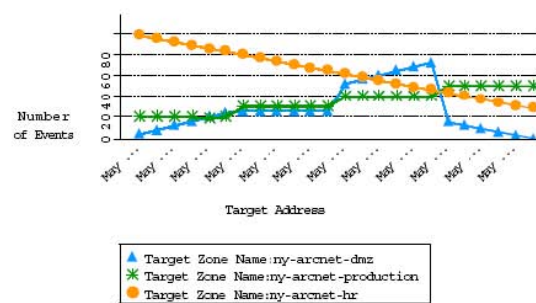
Executive View Report

Sarbanes-Oxley

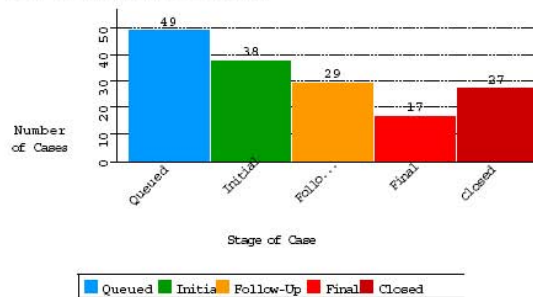
Policy Breaches



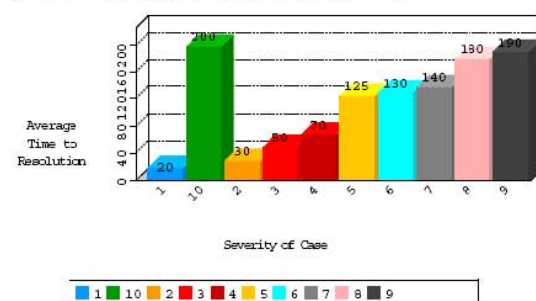
High Risk Events



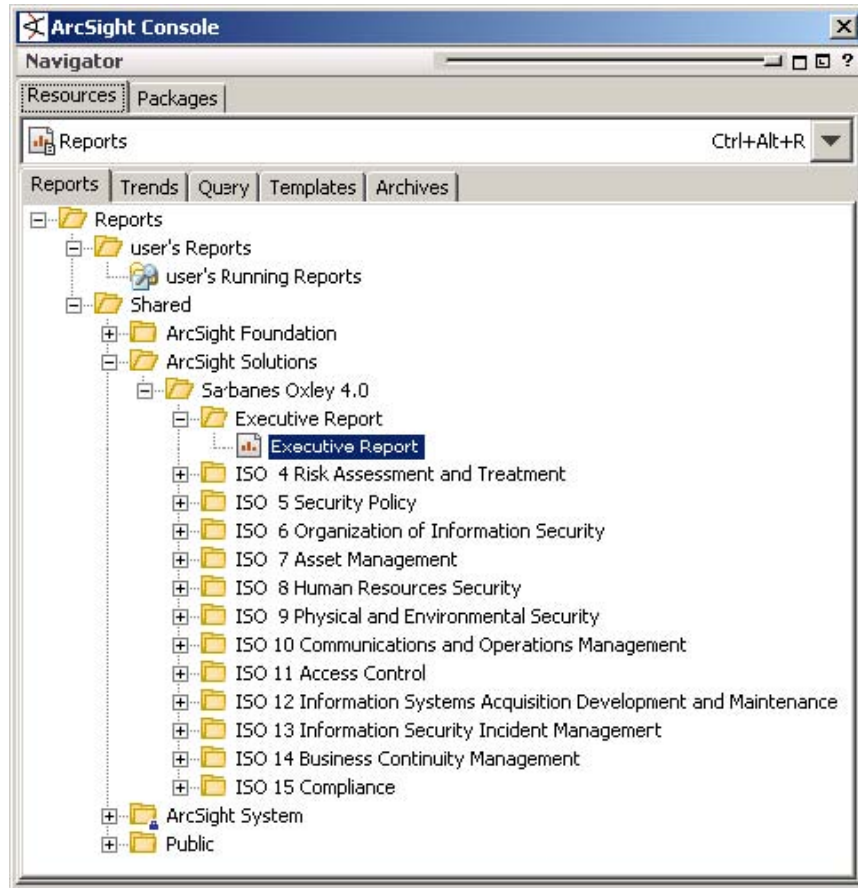
Cases in Various Stages



Cases Time to Resolution by Severity



The Executive Report is located in its own group as shown in the following figure.



The Executive Report is comprised of the resources listed in the following table.

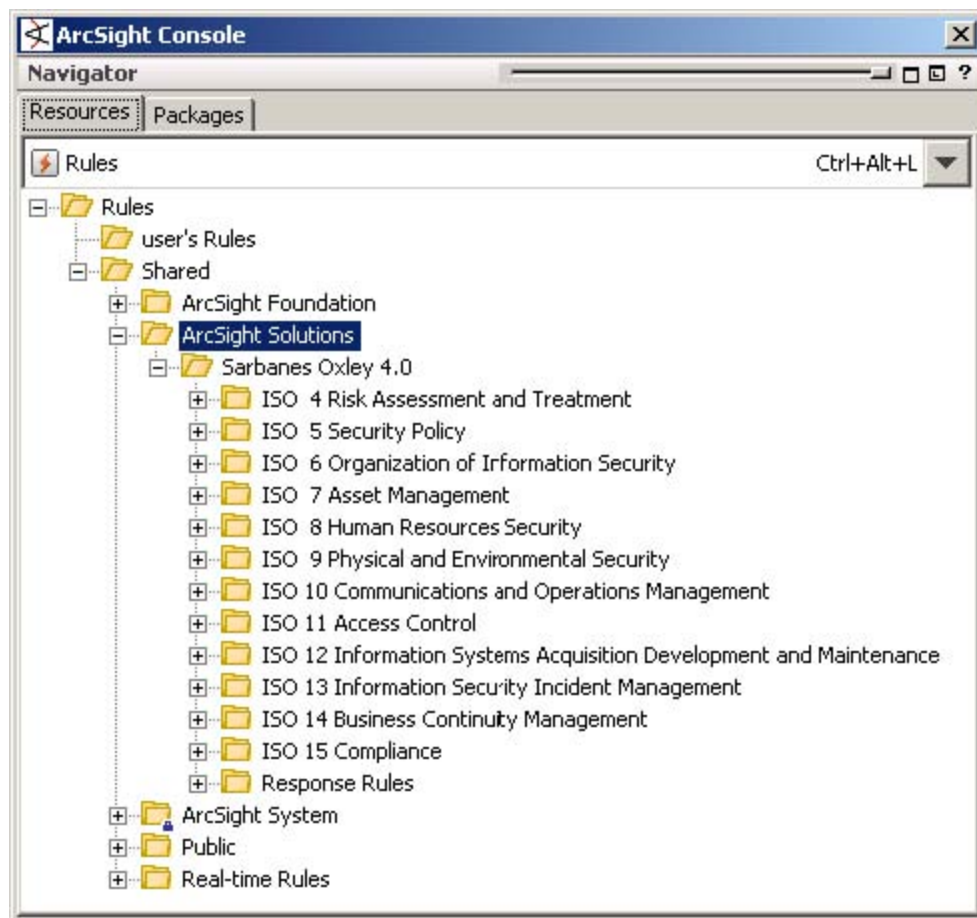
Resource Type	Name	Description	Location In the Navigator Panel
Report	Executive Report	Report showing an overall executive view of activities.	Go to Reports and navigate to ArcSight Solutions/Sarbanes Oxley 4.0/Executive Report/

Trend	Average Time to Resolution - By Case Severity	This trend accumulates data returned by the listed query to compute the average time to resolution of cases, sorted by case severity.	Go to Reports, select the Trends tab and navigate to ArcSight Solutions/Sarbanes Oxley 4.0/Executive Report/Executive Report
Trend	Case Stage Counts	This trend accumulates data returned by the listed query to track the stages of cases over time.	
Trend	High Risk Events per Zone - Executive View"	This trend uses the "High Risk Events per Zone - Executive View" query to show trend over time of the number of high-risk events targeting the different zones in the network.	
Trend	Machines Conducting Policy Breaches - Executive View	This trend accumulates data returned by the listed query to summarize machines conducting policy breaches over time.	

Query	Average Time to Resolution - By Case Severity	This query will show the Average Time to Resolution by Case Severity. It should be run once a week and reported to management.	Go to Reports, select the Query tab and navigate to ArcSight Solutions/Sarbanes Oxley 4.0/Executive Report/Executive Report
Query	Case Stage Counts	This query provides an overview of the cases in their current stages.	
Query	High Risk Events - Executive View Machines Conducting Policy Breaches - Exec View	This query searches for events with a Priority of 10.	
Query		This query is used to shows machines which were involved in policy breaches.	

CIP for SOX4 Architecture

CIP for SOX4 is organized according to the ISO 17799:2005 sections, as shown in the Reports tree below.



Each of the ISO sections operates independently of the other sections. Each of the ISO sections is described in its own chapter in this solution guide.

Although each section operates independently, there is a common set of filters and active lists that support more than one section. These common resources are explained in Chapter 2, Solution Installation and Configuration, on page 27. These configuration items are general parameters needed to tailor the content for your environment, such as privileged account names or the working hours in your organization.

SOX4 Use Cases

For implementation purposes, the ISO sections are organized into use cases. One or more use cases are addressed by content in the SOX4 package. Table 1-1 below shows the all the ISO sections and the use-cases implemented to address them in the SOX4 solution.

Table 1-1 ISO Sections and use-cases implemented in CIP for SOX4

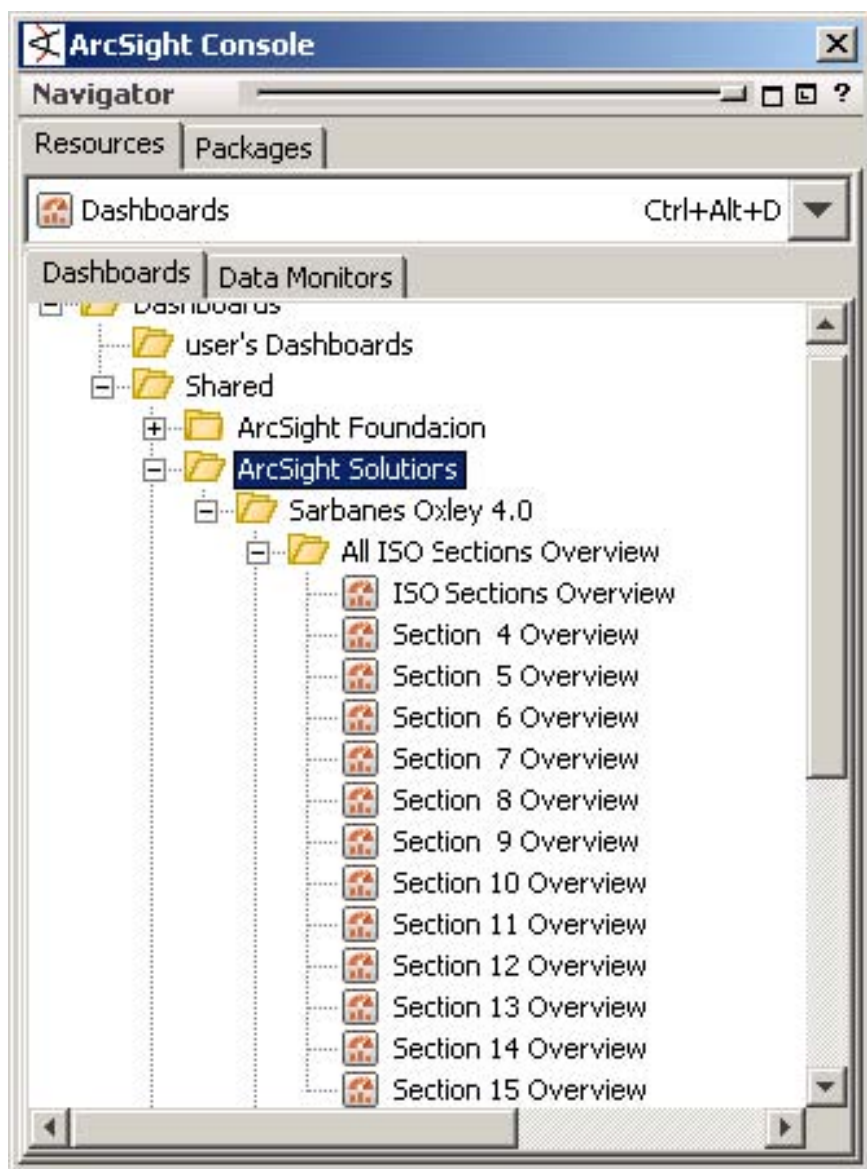
ISO Section	ISO Section Topic	Use Cases in CIP for SOX4
Sections 1-3	Introductory Sections	<ul style="list-style-type: none"> •Not applicable. These are introductory chapters in the ISO standard.
Section 4	Risk Assessment and Treatment	<ul style="list-style-type: none"> •Security overview •High-risk event analysis
Section 5	Security Policy	<ul style="list-style-type: none"> •Policy violations •Introduction of new services, as well as hosts
Section 6	Organization of Information Security	<ul style="list-style-type: none"> •Reporting around cases
Section 7	Asset Management	<ul style="list-style-type: none"> •Asset inventory reporting •Data classification reporting and real-time monitoring
Section 8	Human Resources Security	<ul style="list-style-type: none"> •Watching new hires •Internet usage reporting and monitoring •Former employee monitoring
Section 9	Physical and Environmental Security	<ul style="list-style-type: none"> •Physical building access •Monitoring/reporting contractor's physical access
Section 10	Communications and Operations Management	<ul style="list-style-type: none"> •Monitoring maintenance schedule •Monitoring/reporting file changes •Configuration changes •Separation of Development, Test and Operational Facilities •Changes to third-party services •Malicious code monitoring •IP address/user name attribution

Section 11	Access Control	<ul style="list-style-type: none"> •User management •Authorization changes •Password policy monitoring •Privileged account monitoring •Network service monitoring •Firewall policy monitoring •Network routing supervision •Network policy monitoring •Remote access (VPN) monitoring •Segregation of networks •Role-based access monitoring
Section 12	Information Systems Acquisition, Development and Maintenance	<ul style="list-style-type: none"> •Certificate management •Attack monitoring •Software installation •Information leak monitoring •Vulnerability management

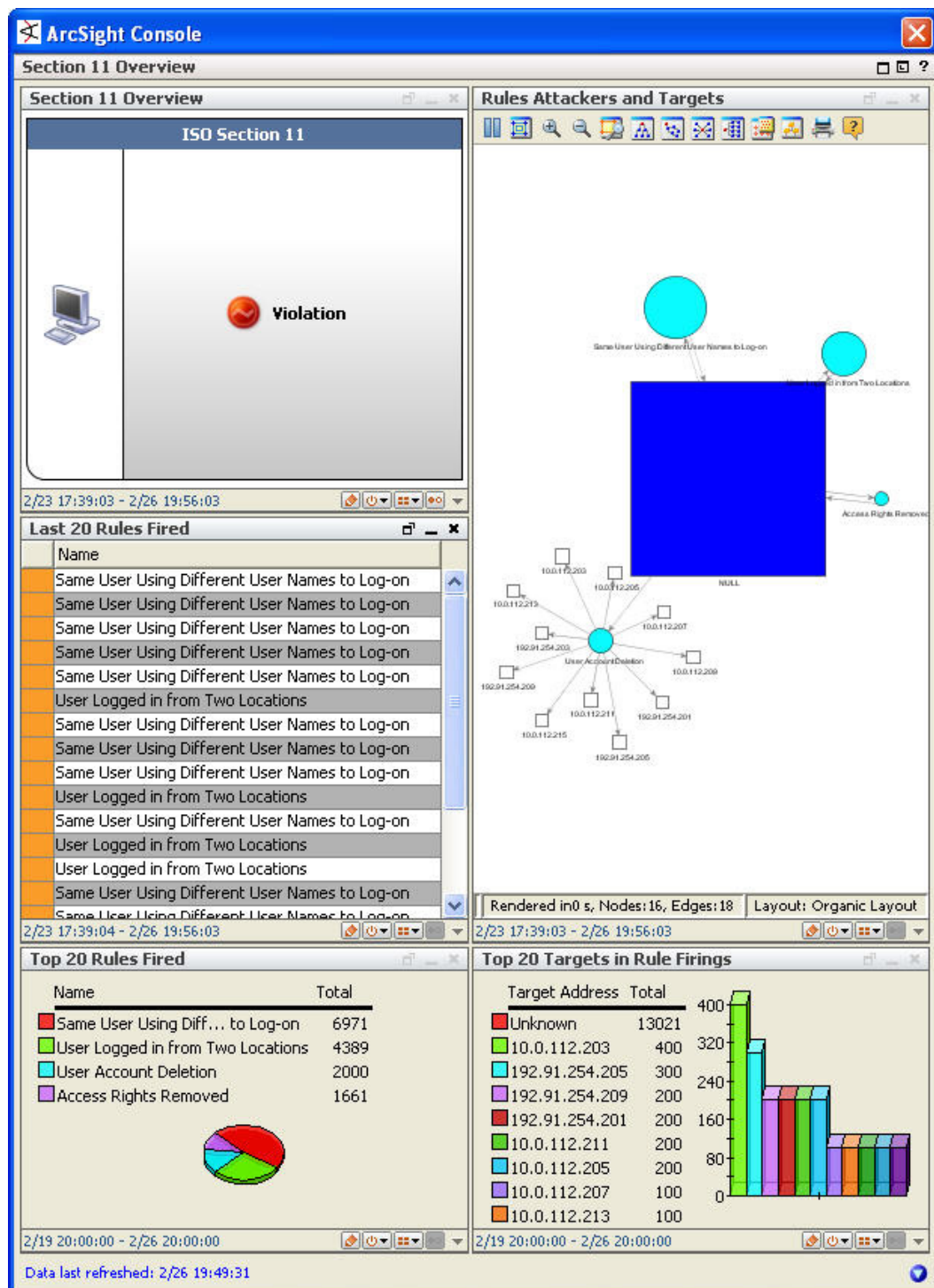
Section 13	Information Security Incident Management	<ul style="list-style-type: none"> •Escalated threat monitoring •Internal reconnaissance
Section 14	Business Continuity Management	<ul style="list-style-type: none"> •Availability monitoring •Monitoring highly critical machines •Monitoring for denial of service attacks
Section 15	Compliance	<ul style="list-style-type: none"> •Intellectual property rights violations •Illegal content download •Peer to peer traffic •Information leak monitoring •Company information •Personal information •Misuse of information processing facilities •Excessive email communications •Policy breach monitoring •Technical compliance checks •Monitoring access to monitoring system (ArcSight)

Chapter 2: Deployment and Configuration

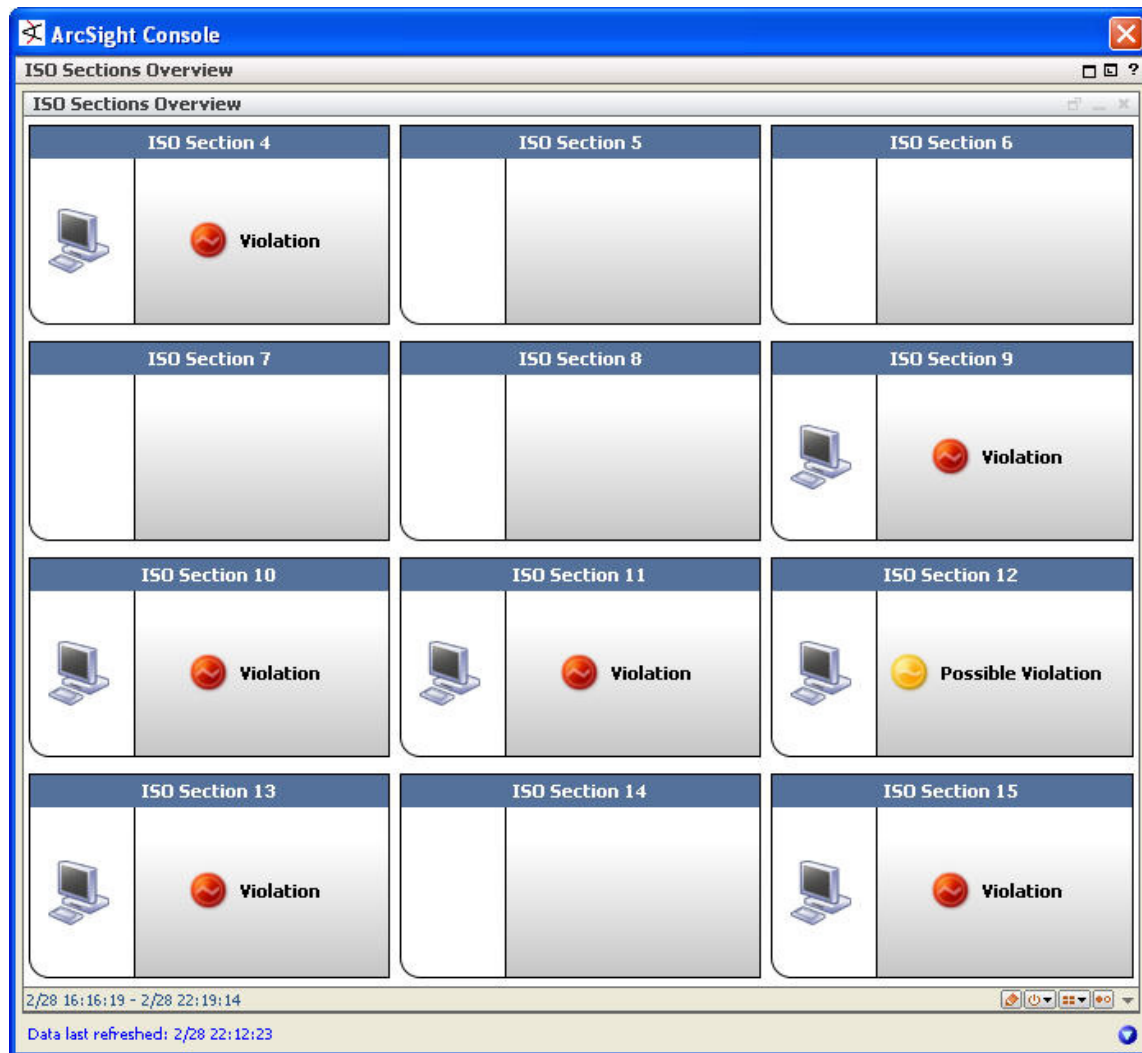
Along with active channels, filters, reports, data monitors, dashboards, and rules to address each of the use cases, every ISO section contains an overview dashboard that summarizes the compliance state determined by correlation rules triggered for that section.



Each dashboard presents a last-state data monitor, which shows a simple traffic-light graphic that indicates the compliance level of each section; an event graph to show the relationships of the non-compliant systems with other systems on the network; a list of the last 20 triggered rules; a pie chart that breaks down the percentage of each triggered rule; and a bar chart that shows the top 20 targets of the triggered rules. The example below shows the Section 11 overview dashboard.



The overview dashboards for each section report into the ISO Sections Overview dashboard, a centralized heads-up display that consists of a last-state data monitor for each of the ISO sections (4 through 15).



A data monitor is only populated when a possible violation or an actual violation occurs. A yellow or red data monitor can be turned to green manually when the situation is remedied by right-clicking the data monitor and selecting **Override Status...** The colors of the traffic lights indicate the following:

Color	State
Red	Compliance violation. This situation occurs when one or more rules are triggered by event activity that violates compliance for this ISO section.
Yellow	Possible Violation. This situation occurs when one or more marginal events occur that could indicate a policy problem, or is a borderline compliance violation.
Green	Compliant. Systems are considered compliant when any events related to this ISO section remain under the threshold of Yellow.

The following table defines the rules that can trigger a compliance violation (red) and possible violations (yellow) in the overview dashboards.

Severity	Rules	Violation Level
Very High	<ul style="list-style-type: none">• Privileged Account Changed• Information Security Incident• Shutdown of Highly Critical Machine• Severely Attacked System• Attack from Third-Party System• Successful Attack – Brute Force• Audit Log Cleared	Compliance Violation (Red)

High	<ul style="list-style-type: none"> • High to Low Classified Traffic Information Leak • Former Employee Account Activity • Activity from Badged-Out Employee • System Restarted at Unscheduled Time • Unscheduled Change in Status of Service • Application Brute Force Logins • Infected Remote Machine Found • Malicious Code Detected • Vulnerabilities Found – Business Information System • Database Privilege Violation • Unauthorized Admin Access to Domain Controller • Former Employee User Account Access Attempt • Inactive User Account Detected • Same User Using Different User Names to Log-on • User Logged in – Removed from Stale Accounts List • Default Password not Changed • Default Vendor Account Used • Privileged Access on a Remote Connection • Account Lockout • Generate Case for Attack Against remote Assets • Security Software Stopped or Paused • Attempted File Changes in Development Detected • Persistent Vulnerability Detected • Internal Recon Detected • Intellectual Property Rights Violation • Organizational Data Information Leak • Personal Information Leak • Email to Public Webmail Servers 	Compliance Violation (Red)
------	--	----------------------------

Medium	<ul style="list-style-type: none"> • New Host Detected • New Service Detected • After Hours Building Access by Contractors • Failed Building Access • Possible Information Interception • Outbound IM Traffic • Access Rights Removed Privileged Access Attempt Detected • User Account Deletion • Disallowed Port Access • Insecure Services Use Detected • Remote Access to Systems with Insecure Configuration • Multiple Invalid Data Input attempts Detected • Exploit of Vulnerability Detected • Peer to Peer Traffic 	Possible Violations (yellow)
--------	--	------------------------------

General Resources

While most of the content is organized by ISO sections, there is a set of filters and active lists that are used for more than one section. These general resources are explained in Chapter 2, Solution Installation and Configuration, on page 27.

Configure these items with data specific to your environment, such as the names of privileged accounts, or the working hours in your organization.

Notify, Investigate, Analyze, and Remediate

Once compliance-related activity is identified, the solution offers many ways to take action, investigate, and analyze.

Notifications

The first step in any escalation process is to notify the right people of a potential problem. The rules included in the SOX4 solution package are configured to activate your notification hierarchy in case of certain threats. You can configure this hierarchy to notify the right groups in the right situations.

For instructions about how to configure the notification hierarchy for your environment, see page “Configure Notification Destinations” on page 62.

Cases

Cases are ArcSight's built-in trouble-ticket system. When certain compliance-related conditions occur, the SOX4 solution opens a case and the appropriate people in your organization are notified so it can be investigated and properly remediated. This requires that notifications are configured, as described above.

Threat Response Manager via ArcSight CounterAct

The ArcSight Threat Response Manager (TRM) provides automated response to compliance-related activity by instantly quarantining nodes that are in violation at the exact moment of detection.

TRM requires the TRM CounterAct connector, which makes the TRM actions available in certain Sarbanes-Oxley rule actions.

The TRM remediation actions are not enabled by default. For a description of the rules that leverage TRM's capabilities and instructions about how to configure and use them, see Chapter 4, Automated Response and Prevention, on page 173.

CIP for SOX4 Device Coverage

CIP for SOX4 leverages event feeds from multiple sources. The following device coverage matrix shows the different ISO sections along with the device feeds and possible special configurations of the devices.

Table 1-2 This device coverage matrix shows the implemented ISO sections along with the device feeds and specific configurations for the devices to utilize the sections.

Use Case	Device Type	Special Device Configuration
Section 4 - Risk Assessment and Treatment		
<ul style="list-style-type: none"> • Security overview • High-risk event analysis 	<ul style="list-style-type: none"> • NIDS/NIPS • HIDS/HIPS 	None
Section 5 - Security Policy		
<ul style="list-style-type: none"> • Policy violations 	<ul style="list-style-type: none"> • NIDS/NIPS • HIDS/HIPS • ILP • Configuration Management 	Configure the policy for each of the devices.
<ul style="list-style-type: none"> • Introduction of new services and hosts 	<ul style="list-style-type: none"> • NBAD 	Ensure the right networks are monitored and the capabilities are turned on

Section 6 - Organization of Information Security		
• Reporting around cases	• N/A	See “Configure Cases ” on page 60 for a description of the Sarbanes-Oxley case management structure and how to configure it.
• Third-party monitoring	• NIDS/NIPS • Firewall • NBAD	None
Section 7 - Asset Management		
• Asset inventory reporting	• N/A	Set up and use ArcSight to manage your assets.
• Data classification reporting • Real-time monitoring	• Router • NIDS/NIPS • Firewall	Set up assets with classification levels. See “Model Assets (Assign Asset Categories)” on page 33.
Section 8 - Human Resources Security		
• Watching new hires • Former employee monitoring	• Application • Database • Proxy • IAM • OS • VPN	None
• Internet usage reporting and monitoring	• Proxy • Router • Firewall	None
Section 9 - Physical and Environmental Security		
• Physical building access by employees • Physical building access by contractors	• Physical Badge Access Systems	Many badge readers are set up to report in batch mode. The closer to real-time the feed can be configured, the better the correlation output will be.
Section 10 - Communications and Operations Management		
• Monitoring maintenance schedule	• OS • Application • Database	None

• Monitoring/reporting file changes	• OS • File Integrity Checker • HIDS/HIPS	Turn file auditing on for important files.
• Configuration changes • Changes to third-party services	• OS • Application • Database • Configuration Management • Any device logging configuration changes (most devices do)	Make sure configuration changes are logged
• Separation of Development, Test and Operational Facilities	• Router • Firewall • NIDS/NIPS	None
• Malicious code monitoring	• Anti Virus • NIDS/NIPS • HIDS/HIPS	None
• User attribution	• OS, VPN, IAM	None
Section 11 - Access Control		
• User Management • Authorization changes • Password policy monitoring	• OS • IAM • Application • Database	None
• Privileged account monitoring	• OS • IAM • VPN • Application • Database	None
• Network Service Monitoring	• Router • Firewall • NIDS/NIPS	None
• Firewall policy monitoring	• Firewall	None
• Network routing supervision	• Router • Switch	None
• Remote access (VPN) monitoring	• VPN	None
• Segregation of networks • Network policy monitoring	• Router • Firewall • NIDS/NIPS	None
• Identity based role monitoring	• Database, OS	Database auditing needs to be configured to allow log access. See <xref to database auditing setup> for details.
Section 12 - Information Systems Acquisition, Development and Maintenance		
• Certificate management	• NIDS/NIPS • OS • VPN • Application	None
• Attack monitoring	• NIDS / HIDS	None

• Software installation	• OS	Make sure the operating system is configured to detect installations of new applications
• Information leak monitoring	• ILP	Make sure the ILP device is configured to monitor for critical and confidential documents.
• Vulnerability management	• Vulnerability Scanner	None
Section 13 - Information Security Incident Management		
• Escalated threat monitoring	Any event configured to trigger a rule in the escalation filter.	None
• Internal reconnaissance	• NIDS/NIPS • NBAD	None
Section 14 - Business Continuity Management		
• Monitoring highly critical machines	• Router • Firewall • NIDS/NIPS • HIDS/HIPS • Database • Application • NBAD • OS	None
• Availability monitoring • Monitoring for DoS attacks	• NIDS/NIPS • NBAD	None
Section 15 - Compliance		
• Intellectual property rights violations	• NIDS/NIPS • ILP • Proxy	Configure sensors to detect intellectual property rights violations. This often involves defining new signatures or configurations.

• Illegal content download	• Proxy • NIDS/NIPS • ILP	Configure devices to report illegal content download. This often involves defining new rules or configurations.
• Peer to peer traffic	• NIDS/NIPS • ILP • NBAD	None
• Information leak monitoring • Company information • Personal information	• ILP	Make sure the ILP device is configured to monitor for critical and confidential documents.
• Misuse of information processing facilities	• Email • Router • Firewall	None
• Excessive email communications	• Email Server	Make sure your email server logs email communications that are relevant. [Possibly filtering internal-to internal communications to reduce event load.]
• Policy breach monitoring	• NIDS/NIPS • HIDS/HIPS • ILP • Configuration Management	Configure the policy for each of the devices.
• Technical compliance checks	• Vulnerability Scanner • Configuration Management	None
• Monitoring access to monitoring system (ArcSight)	• ArcSight	None
Legend:		

NI DS Network-based Intrusion Detection System	ILP	Information Leak Prevention
HI DS Host-based Intrusion Detection System	OS	Operating System
HI PS Host-based Intrusion Prevention System	NBAD IAM	Network-based Anomaly Detection Identity and Access Management

To gather events from physical access devices, such as badge readers, you must build a FlexConnector tailored to the type of physical access device you use. For instructions about how to build and configure a FlexConnector for a physical access device, see “Build FlexConnector(s) for Physical Access Devices” on page 63.

Chapter 3: Solution Installation and Configuration

The SOX4 solution is self-contained and does not rely on any other ArcSight solution. You can install the SOX4 solution alongside other solutions on the same Manager.

“Deployment Planning” on page 27

“Install the SOX4 Solution” on page 28

“Configure the Sarbanes-Oxley 4 Solution” on page 31

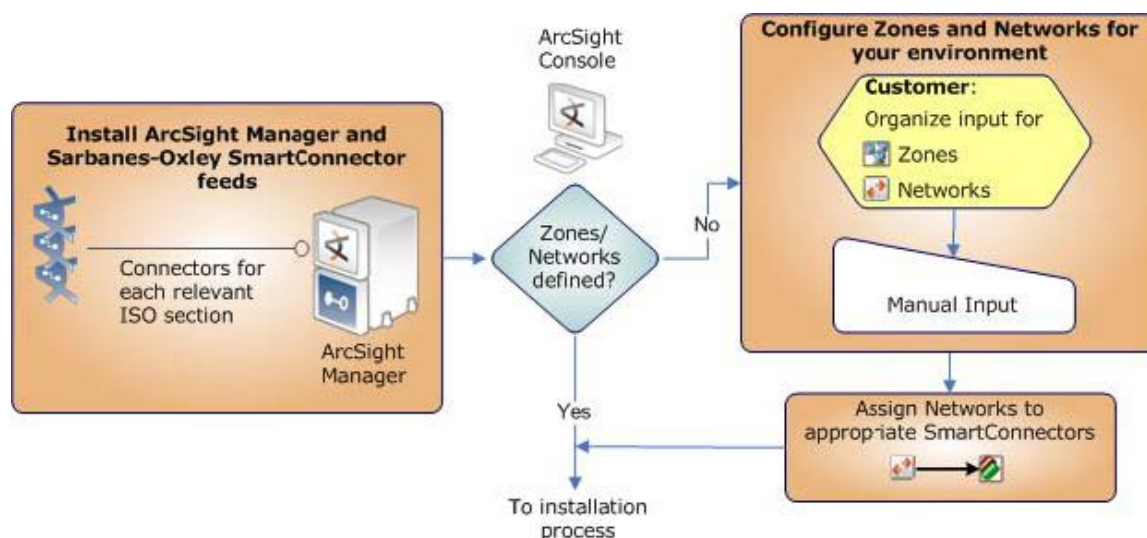
“Upgrade from SOX2 to SOX4” on page 65

“Configure Oracle Connector to Access Monitoring” on page 71

“Back up and Uninstall the SOX4 Solution Package” on page 76

Deployment Planning

Before installing or upgrading, prepare your environment and the data structures that will feed the SOX4 solution.



The process to prepare your environment for the SOX4 solution package involves SmartConnector installation and configuration with zones and networks.

Verify Environment

Before installing, review this installation and configuration preparation checklist.

1. Verify ArcSight ESM v4.0 installation. The SOX4 solution package runs on the following version of Enterprise Security Management (ESM):

v4.0

Verify that your system has the ArcSight Console connected to an ArcSight Manager with this ESM product version installed, and meets the prerequisite requirements for your operating system as detailed in the ESM v4.0 Installation and Configuration Guide.

2. Model network to include Sarbanes-Oxley devices. Verify that zones and networks are defined for your environment and that networks are assigned to the agents reporting Sarbanes-Oxley-relevant events into your ArcSight system. Learn more about ArcSight's network modeling process in ArcSight 101. Find instructions for how to configure zones and networks in the Console online Help.

Supported Platforms

The SOX4 solution operates on all supported ArcSight platforms, and is installed through the Console using the package import feature new with ESM v4.0.

Upgrade Planning

If you are upgrading from the Compliance Insight Package for Sarbanes-Oxley v2.0 (SOX2), see the upgrade overview and instructions on page 70.

Install the SOX4 Solution


The SOX4 solution is installed using an ArcSight package. The installation process is done:

- From the ArcSight Console
- Using the ArcSight Administrator login
- With the ArcSight Manager running

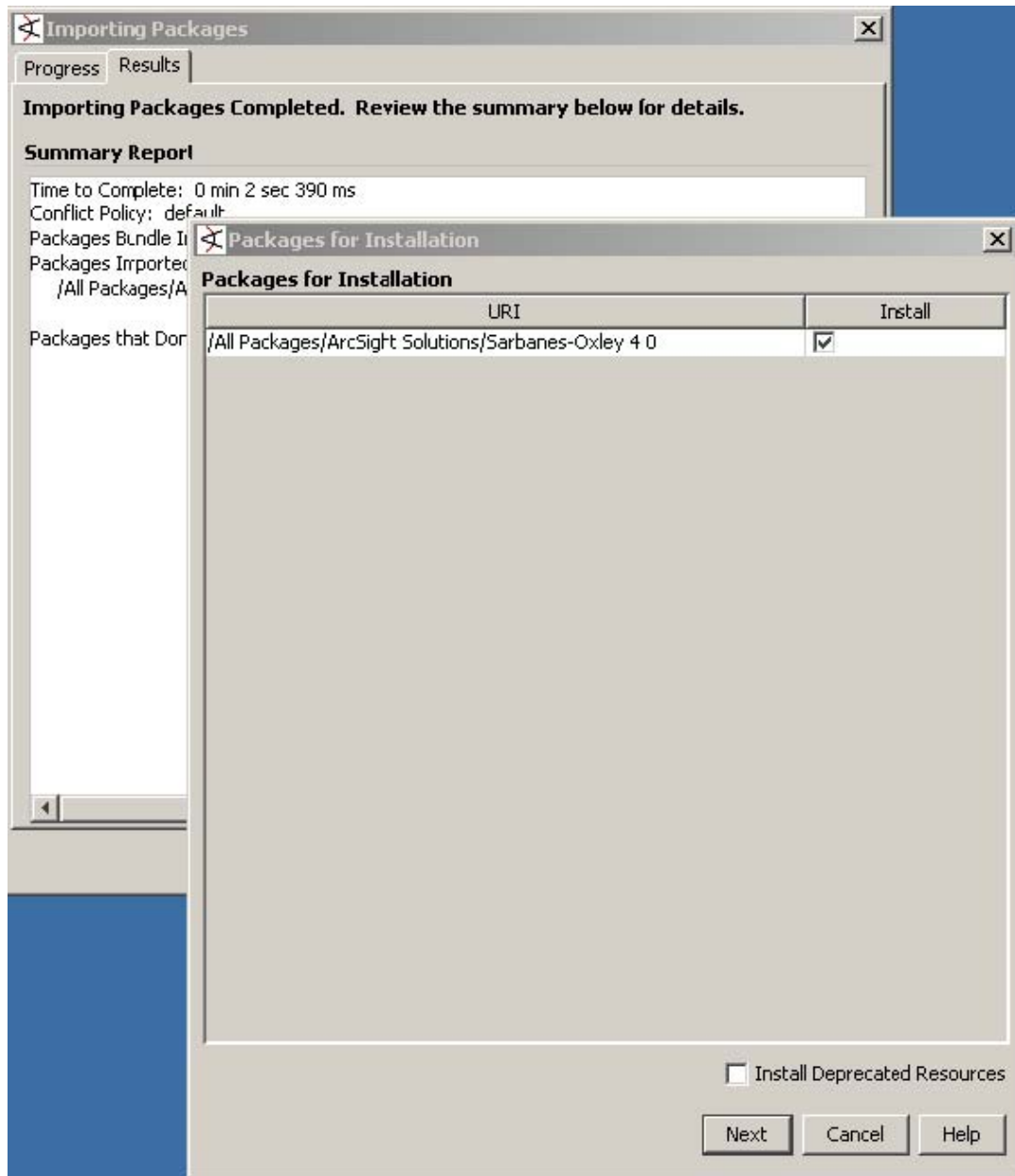
To install the SOX4 package:

1. Using the log-in credentials supplied to you by ArcSight, download the following SOX4 package bundle from the ArcSight support site (<https://support.arcsight.com/>) to the machine where you plan to launch the ArcSight Console: `ArcSight-ComplianceInsightPackage-SOX.4.0.x.arb`

Where x is the build number of the released SOX4 package, for example: 5224.

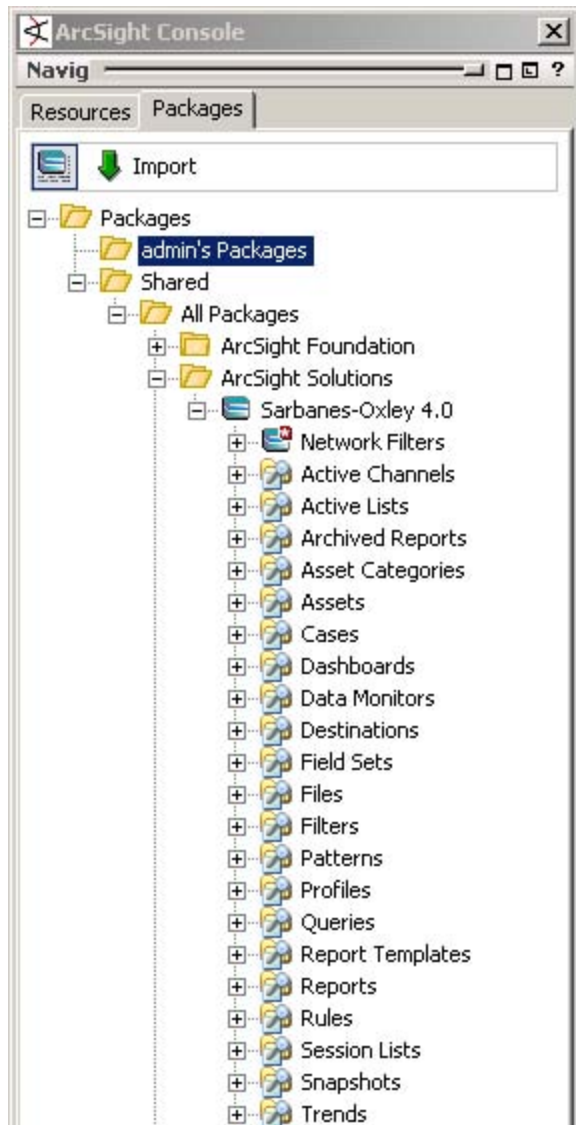
2. Log into the ArcSight Console as the ArcSight Administrator.
3. Click the Packages tab in the Navigator panel.
4. Click  Import

5. In the Open dialog box, browse and select the SOX4 package bundle file and select Open.
6. The progress of the import of the package bundle is displayed in the Progress tab of the Importing Packages dialog box.
7. When the import is complete, the Results tab of the Importing Packages dialog box is displayed as well as the Packages for Installation dialog box as shown in the following figure.



8. In the Packages for Installation dialog box, click Next.
9. The progress of the install is displayed in the Progress tab of the Installing Packages dialog box. When the install is complete, the Results tab of the Installing Packages dialog box displays the Summary Report.
10. In the Installing Packages dialog box, click OK. In the Importing Packages dialog box, click OK.

11. To verify that the installation was successful and the content is accessible in the Navigator panel, expand the ArcSight Solutions folder and the Sarbanes-Oxley 4.0 package. The SOX4 content displays as shown in the following figure.



Installation Troubleshooting

If the installation was not successful, contact ArcSight technical support:

Resource	Description
Support web site	http://support.arcsight.com/supportportal . Access to ArcSight incident reporting, knowledge base, software downloads, help, and new customer forum.

Customer forum	https://forum.arcsight.com . Offers a place for customers to share ArcSight tips and tricks.
----------------	---

Assign User Permissions

By default, users in the Default user group can view SOX4 content, and users in the ArcSight Administrators and Analyzer Administrators user groups will have read and write access to the SOX4 solution content. Depending on how you have set up user access controls within your organization, you may need to adjust those controls to make sure the new content is accessible to the right users in your organization.

This assumes that you have user groups set up and users assigned to them.

1. Log into the ArcSight Console as ArcSight Administrator.
2. In the Navigator panel, go to Active Channels and navigate to ArcSight Solutions/Sarbanes Oxley 4.0.
3. Right-click the Sarbanes Oxley 4.0 folder and select Edit Access Control to open the ACL editor in the Inspect/Edit panel.
4. In the ACL editor in the Inspect/Edit panel, select which user groups you want to have which permissions to the SOX4 active channels and click OK.
5. Repeat steps 2 through 4 for all resources that contain SOX4 content:
 - Active channels
 - Active lists
 - Cases
 - Dashboards
 - Data monitors
 - Field Sets
 - Filters
 - Queries
 - Reports
 - Rules
 - Session Lists
 - Trends

Configure the Sarbanes-Oxley 4 Solution

Several of the SOX4 solution resources should be configured with values specific to your environment. Some features also require some additional SmartConnectors or SmartConnector configuration. This section describes these configuration processes.

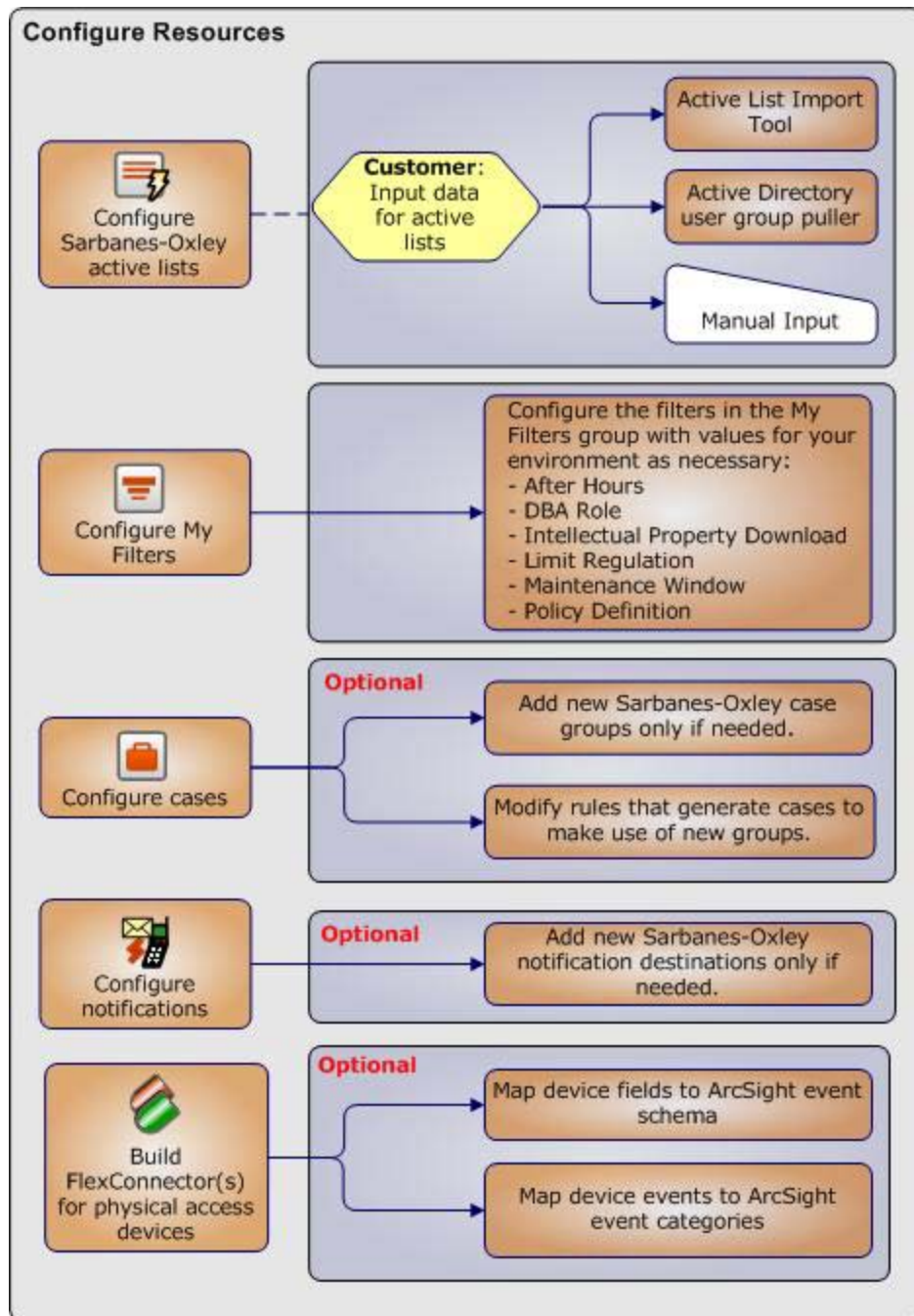
Configuration Planning

Depending on the features you want to implement and how your network is set up, some configuration is required and some is optional. The list below shows all the configuration tasks involved with the SOX4 solution, what scenario they are associated with, and where to find instructions for performing the configuration.

This chapter contains instructions required to enable content for the SOX4 solution.

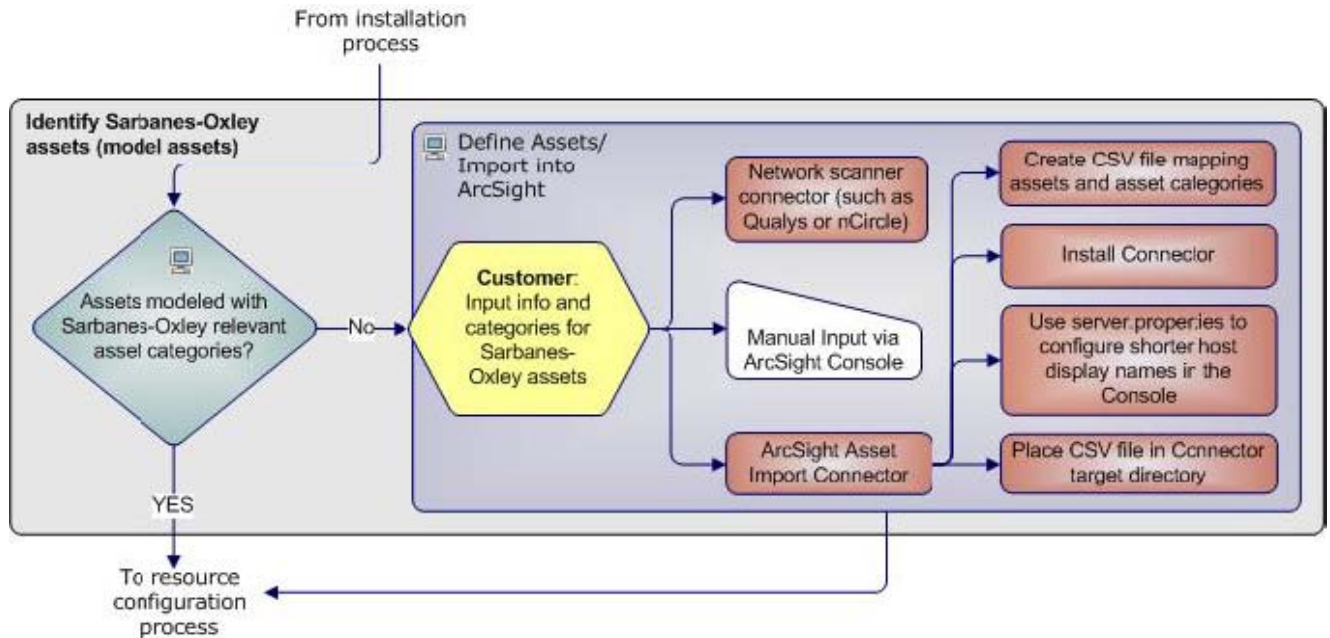
- Model Assets (Assign Asset Categories) on page 33
- Configure Active Lists on page 39
- Configure My Filters on page 49
- Configure Cases on page 60
- Configure Notification Destinations on page 62

If you want to enable the automated remediation capabilities of TRM to your SOX4 solution, refer to Chapter 4, Automated Response and Prevention, on page 173 for installation and configuration instructions. The configuration processes outlined in this portion apply to resources that feed multiple Sarbanes-Oxley scenarios.



Model Assets (Assign Asset Categories)

Asset modeling is essential to activate certain SOX4 solution content, such as those that evaluate highly critical and classified assets.

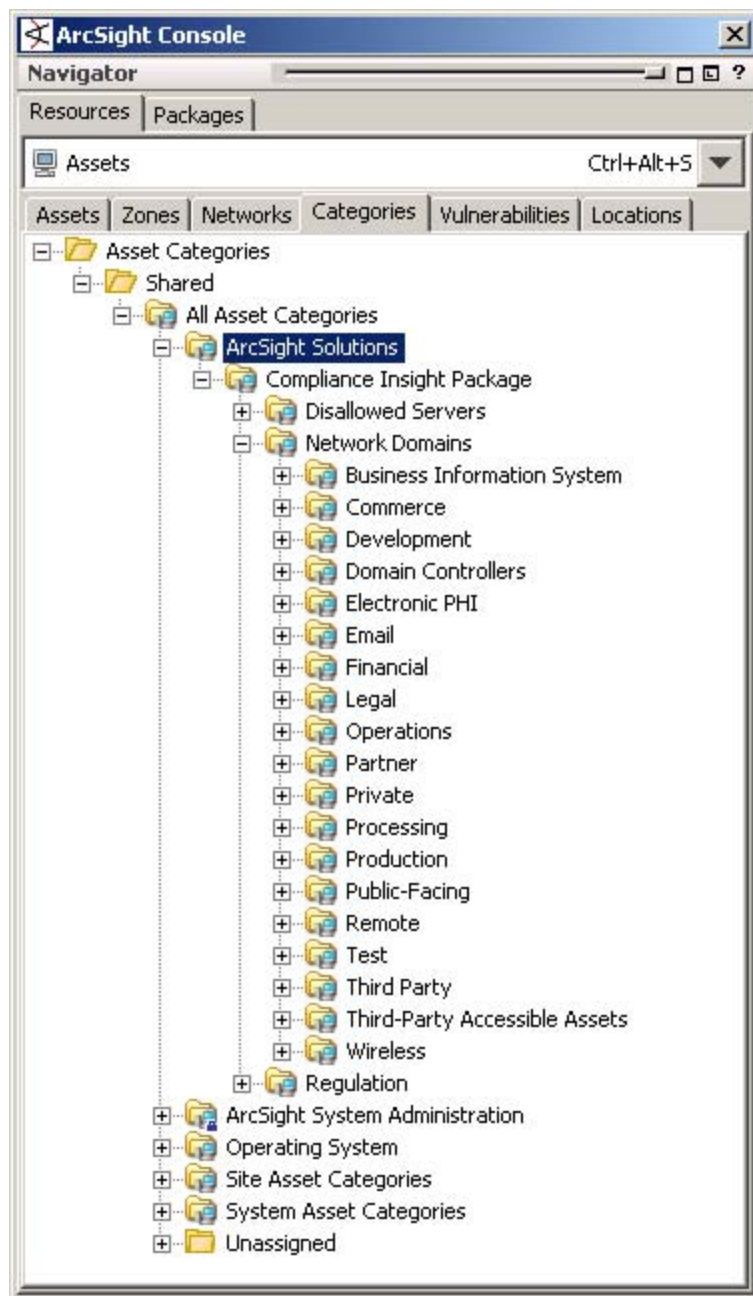


First identify network assets that are classified or considered highly critical, then map these assets to corresponding Sarbanes-Oxley asset categories.

Classifying assets in one or more of the Sarbanes-Oxley asset categories adds valuable business context to the events evaluated by the SOX4 solution. This section describes the Sarbanes-Oxley asset categories and explains how the solution uses them.

Network Domains

The most important systems in the network should be classified with the Compliance Insight Package Network Domain asset categories. The SOX4 solution offers the following asset categories to classify your assets.



This taxonomy is extensible, so you can add your own asset categories within these Sarbanes-Oxley groups. If you create your own groups, or modify the name of an existing group, you may have to modify some SOX4 content to make use of them.

Categorize your desktop assets using the Private category and your VPN zones using the Remote category.

ArcSight Site Asset Categories

The SOX4 solution also makes use of several ArcSight Site and System Asset Categories.

Protected Address Space

As part of ESM setup, you should categorize your assets in the Protected Address Space category. In the Navigator Panel, go to Assets, select the Categories tab and navigate to Site Asset Categories/Address Spaces/Protected. Much of the standard ESM content depends on assets being categorized as protected.

The SOX4 solution also uses this category to determine which machines are protected (or owned by the organization). This sets a baseline for determining what is considered inbound and outbound communication.

Asset Criticality

The SOX4 solution content also makes use of the Criticality category. In the Navigator Panel, go to Assets, select the Categories tab and navigate to System Asset Categories/Criticality. The criticality levels are factored into the event priority formula (threat level formula) calculation. They are also used in the SOX4 solution to determine which assets are critical to be monitored and protected.

Assigning asset criticality to your Sarbanes-Oxley assets is a critical part of deploying the SOX4 solution.

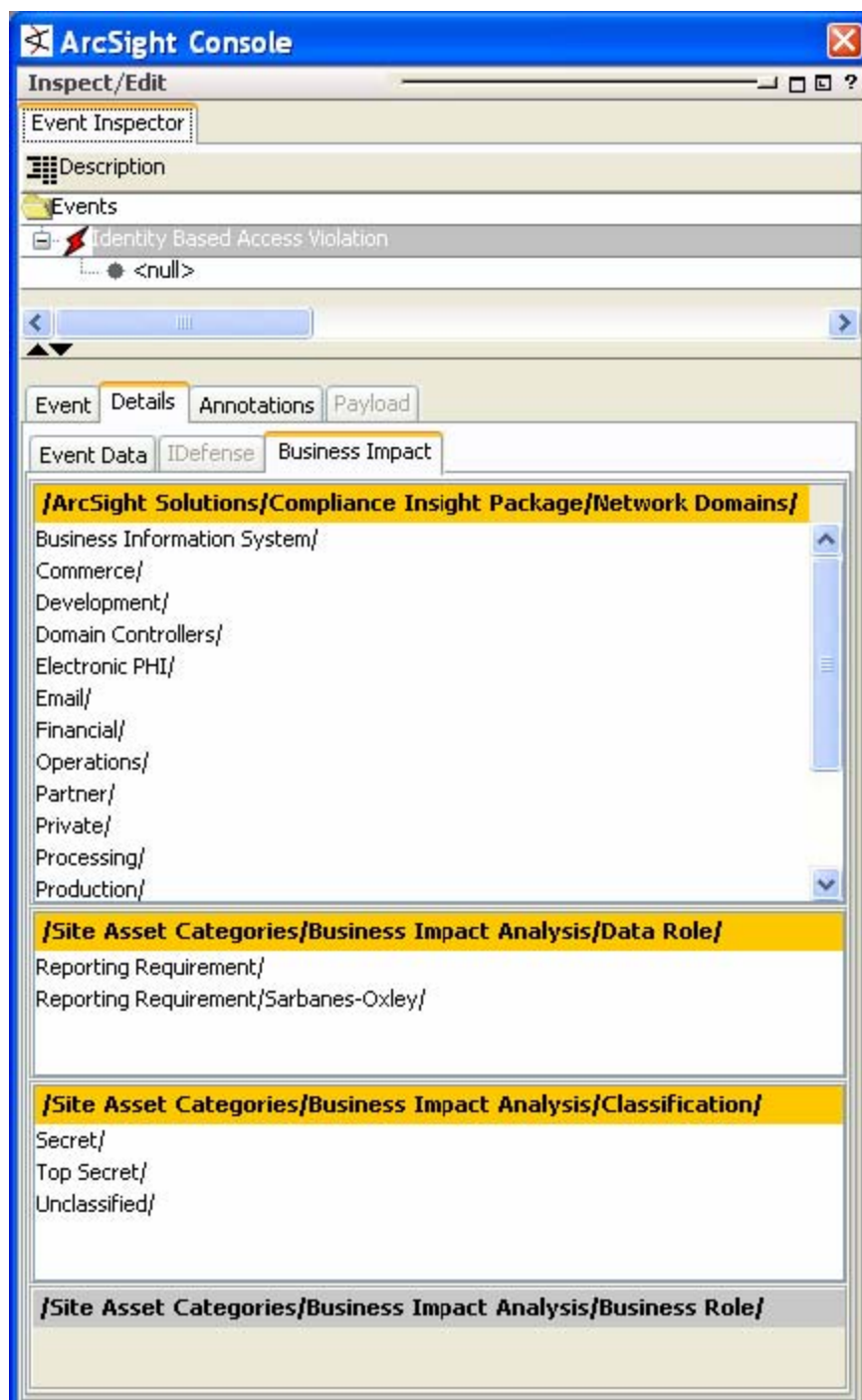
Business Impact Analysis

The Sarbanes-Oxley asset category group is also linked to the Business Impact Analysis group in the System content folder under Site Asset Categories (Site Asset Categories/Business Impact Analysis) so that targeted asset information will be displayed in the Business Impact tab of the Details tab in the Event Inspector. This provides more context around the target asset of an event.

By default, the Business Impact tab of the Details tab in the ESM Event Inspector is disabled. Any event entering the system, whether an original event from a device or a rule firing, that targets a machine classified in a Business Impact Analysis asset category, the event will have the Business Analysis tab enabled when that event is opened in the Event Inspector. This will show that the business impact analysis for the events that are categorized for Sarbanes-Oxley, as shown below.

ArcSight recommends reassigning the categories for assets that are categorized with the Business Impact Analysis/Business Role and Data Role asset categories to use the Network Domains categories. This will activate the content for these assets.






How to Assign Asset Categories

The Sarbanes-Oxley asset categories can be assigned using one of these two methods:

One by One Using the Console UI

Use this method if you have only a few assets to categorize as part of your Sarbanes-Oxley monitoring program. One asset can be categorized in more than one Sarbanes-Oxley asset category.

1. In the Navigator pane, go to Assets, select the Assets tab, and navigate to All Assets/Shared/ArcSight System Administration/Agents, where you will find the agents installed for your environment.
2. Right-click the asset you wish to categorize and select **Edit Asset**.
3. In the Inspect/Edit panel, click the **Categories** tab. Click the add icon () at the top of the screen to select new resources.
4. In the **Asset Categories Selector** pop-up window, navigate to the following asset categories and click OK.
The Sarbanes-Oxley category that applies to the asset, for example: All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Commerce
The criticality level that applies to the asset, for example: All Asset Categories/System Asset Categories/Criticality/High
5. Repeat steps 3 and 4 for every asset you wish to classify in one of the Sarbanes-Oxley asset categories.

Once you have assigned your assets to the Sarbanes-Oxley asset categories, you can also assign them to other asset categories, either within the solution package or the general ArcSight categories, or those you have created yourself.

ArcSight Asset Import Connector

If you have many assets that you want to track as part of your Sarbanes-Oxley monitoring program, you can configure them in a batch using the ArcSight Asset Import Connector. This connector can also create new assets as part of the batch function.

The ArcSight Asset Import Connector is available as part of ArcSight's connector download. For instructions about how to use this connector to configure your assets for the SOX4 solution, see the ArcSight Asset Import SmartConnector Configuration Guide. The steps below outline the process involved.

1. Create a comma-separated value (CSV) file in a spreadsheet that contains the following data for each asset you wish to categorize in one or more Sarbanes-Oxley asset category:

Header name	Data description
address	IP address of the asset

macAddress	Mac address of the asset with colons between the hexadecimals: 00:10:D6:AC:CA:35
hostName	Fully qualified host name of the asset
location	ArcSight asset location. This is an ArcSight URI, and may not be applicable in all environments.
category:N	The complete ArcSight URI of the asset category in which you wish to categorize the asset. Replace N with the name of the asset category. Add a category column for every asset category that applies to the asset.

The SOX4 solution provides a sample file as a File resource that you can use as a template. Instructions for downloading the sample file are provided in the section below.

A few lines of this template are shown on the next page. The template includes drop-down menus that contain the URIs of Sarbanes-Oxley asset categories you can use so you don't have to type them. The values for the drop-down menus are defined in the "MasterCategories" tab of the excel sheet.

The CSV file must contain these columns, although each row need not contain a value. You can add as many Category columns as you need to, but there must be at least one. Asset attributes and categories that appear in the CSV file but are not defined in the Manager will be added to the Asset model.

Make sure that the IP address or the hostname are populated. If neither of these are available, specify a macAddress.

2. Install the SmartConnector according to the instructions in the ArcSight Asset Import SmartConnector Configuration Guide.
3. Assign the SmartConnector to an ArcSight Network.
4. When you import the asset names as they appear to the network, they have long names that are hard to read in the Navigator panel. Formatting the asset naming structure in `server.properties` will display shorter host names in the Navigator panel that are easier to read.
5. Copy the CSV file into the target directory on the connector system. As soon as the CSV file is imported into the connector's target directory, the Manager consumes the file and populates the asset model with your asset data.

Sarbanes-Oxley Asset Import Template

The table below shows the first five rows of the Sarbanes-Oxley sample Asset Import table template, which you can use to populate your Sarbanes-Oxley asset lists and asset categories.

To download the template:

1. From the Resources tab in the Navigator pane, go to Files and navigate to `ArcSightSolutions/Sarbanes Oxley 4.0/Active Directory User Group Gen` folder.
2. Right-click the `AssetImportTemplate-SOX4.xls` file and select the Download option.

3. Browse for a directory location, for example the Desktop.
4. In the File name field, enter AssetImportTemplate-SOX4.xls and click Save.

A copy of the file is saved to the local file system.

address	mac Address	hostName	location	category: Network Domains	category: Criticality	category: Classification
10.0.0.1		servername1.customer.com	/All Assets/CustomerX/ Support	/All Asset Categories/ArcSight/Solutions/Compliance Insight Package/Network Domains/Commerce	/All Asset Categories/System Asset Categories/Criticality/High	/All Asset Categories/Site Asset Categories/Classification/Secret
10.0.0.2		servername2.customer.com	/All Assets/CustomerX/ ArcSight	/All Asset Categories/ArcSight/Solutions/Compliance Insight Package/Network Domains/Development	/All Asset Categories/System Asset Categories/Criticality/High	
10.0.0.3		servername3.customer.com	/All Assets/CustomerX/ E-mail	/All Asset Categories/ArcSight/Solutions/Compliance Insight Package/Network Domains/Email	/All Asset Categories/System Asset Categories/Criticality/Very High	/All Asset Categories/Site Asset Categories/Classification/Secret
10.0.0.4		servername4.customer.com	/All Assets/CustomerX/ CorporateNet	/All Asset Categories/ArcSight/Solutions/Compliance Insight Package/Network Domains/Business Information System	/All Asset Categories/System Asset Categories/Criticality/Very High	
10.0.0.5		servername5.customer.com	/All Assets/CustomerX/ PS	/All Asset Categories/ArcSight/Solutions/Compliance Insight Package/Network Domains/ElectronicPHI	/All Asset Categories/System Asset Categories/Criticality/High	/All Asset Categories/Site Asset Categories/Classification/Secret

Configure Active Lists

The SOX4 package contains numerous active lists that retain specific data that is cross-referenced dynamically during run-time by ArcSight resources that use conditions, such as filters, rules, and reports.

You can add entries to active lists, one-by-one, using the Active List editor in the ArcSight Console. For detailed instructions, see [Configure Active Lists Using Console Active List Editor](#).

You can also add entries in batch to active list from a comma separated value (CSV) file. For detailed instructions see [Configure Active Lists by Importing a CSV File](#).

The following table defines the active lists to configure to implement individual use cases.

Active Lists that Require Configuration

Active List	Description and Expected Data Entry
Administrative Accounts	List of all users with administrative privileges. Expected input per entry: User Name
Allowed Ports	Active list of all permissible destination ports, ie, all permissible services. Expected input per entry: Port number

Contractor Accounts	<p>List of all contractor user accounts. This list must be maintained on a regular basis.</p> <p>Expected input per entry: User Name</p>
Contractor Badges	<p>List of all contractor Badge IDs. This list must be maintained on a regular basis.</p> <p>Expected input per entry: Badge ID/ or User Name, depending on the badge reader configuration</p>
Default Vendor Accounts	<p>List of the default user account names for various vendors.</p>
Former Employees	<p>Lists all former employees. This list must be maintained on a regular basis.</p> <p>Expected input per entry: User Name</p>


Peer to Peer Ports	This active list is dynamically populated with port numbers of traffic classified as peer to peer traffic.
Privileged User Groups	<p>List of user groups with elevated, not necessarily administrative privileges.</p> <p>Expected input per entry: User Group Name</p>
Public Webmail	List of domain names of well-known public Webmail systems such as yahoo.com, hotmail.com, etc. This list is maintained indefinitely.
User Roles	This list contains the mappings of users to their roles. It can be used to monitor role-based access.

For specific descriptions and configuration tips for the active lists in each scenario, see the individual chapters that cover each ISO section.

Configure Active Lists Using Console Active List Editor

You can add entries to active lists, one-by-one, using the Active List editor of the ArcSight Console.

1. In the Navigator panel, go to Lists and navigate to ArcSight Solutions/Compliance Insight Package.

2. Right-click the active list you wish to populate and select **Show Entries**. The active list details are displayed in the Viewer panel.
3. For each entry you wish to add to the active list, repeat the following steps:
 - a. To add an entry to the list, click the add icon () in the active list header.
 - b. In the Active List Entry editor of the Inspect/Edit panel, enter values for each column in the list except for the dynamic columns listed in the following table and click **Add**.

Name	Value
Creation Time	This field is reserved for active lists that are populated dynamically by rule actions. Leave this field blank.
Last Seen Time	This field is reserved for active lists that are populated dynamically by rule actions. Leave this field blank.
Count	This field is reserved for active lists that are populated dynamically by rule actions. Leave this field unchanged.

Configure Active Lists by Importing a CSV File

Active lists can be populated in a single step, by importing entries from an existing CSV file. The number of columns in the active list must match the number of comma separated values in the CSV file. For example, if the active list has two columns of data, the imported CSV file must have two comma-separated fields.

1. In the Active Lists resource tree of the ArcSight Console, right-click an active list and choose **Import CSV File**.
A file browser opens.
2. Browse to find the CSV file you want to import, select it, and click **Open**. The Import Preview dialog displays the data from the CSV file to be imported into the active list.
3. To add the entries from the selected file into the active list, in the Import Preview dialog, click **OK**. The new entries from the file are appended to the existing entries in the active list.
4. To verify that your entries were imported as expected, right-click the active list you just populated with the CSV file and select **Show Entries**.

This displays the newly-added data from the CSV file in the Viewer panel as active list details.

Tip: By default, the active list displays 2000 entries at a time. To view entries outside the range shown, create an active list filter that specifies a different range (click **Filter** in the active list header).

Populating Active Lists from an Active Directory

Instead of manually transferring the list of valid user account and groups from an Active Directory, the SOX4 solution provides the Active Directory script (AD_user_group_gen.vbs) to assist in populating active lists. This script interrogates the data on an Active Directory using ADSI, creates a list of Active Directory user account names and groups, and generates a CSV file with the account information. This CSV file can then be used to populate active lists from the ArcSight Console as described in Configure Active Lists by Importing a CSV File on page 41.

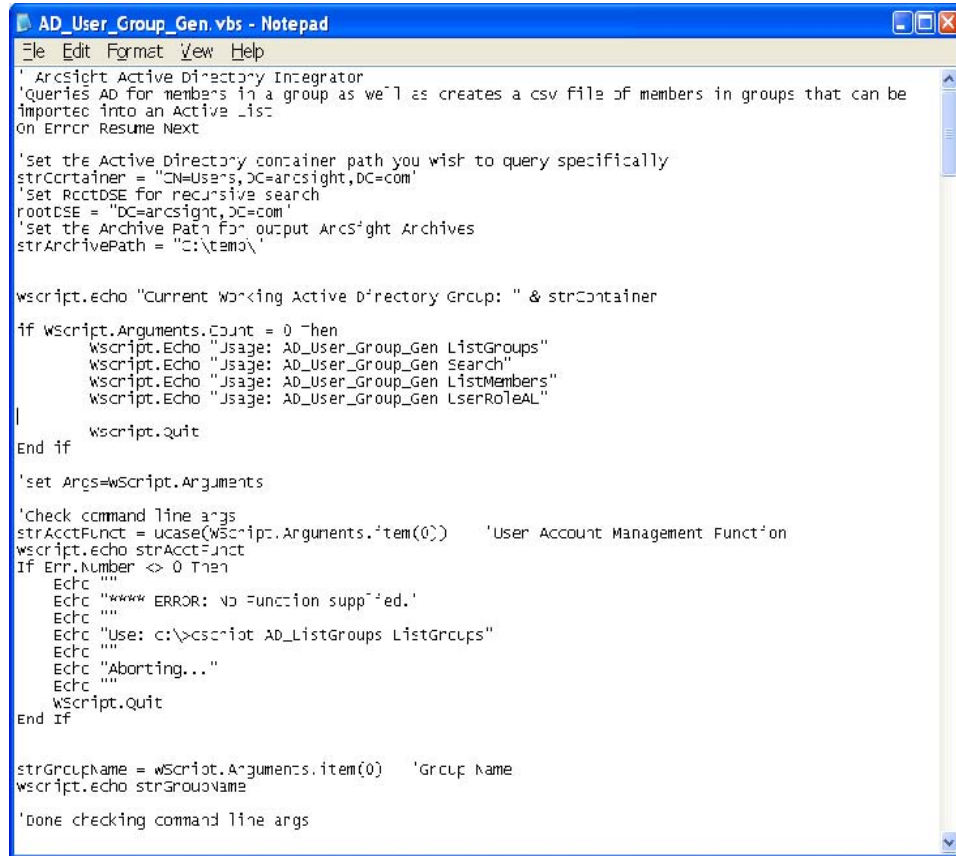
In addition, Active Directory script provides the ability to search an Active Directory for users, groups, and computers.

The user and group information stored in the CSV file can be used to populate specific Sarbanes-Oxley 4.0 active lists such as the At-Risk Users and the Privileged Users. You can also use the script to populate active lists that you create yourself and store in the /All Active Lists/ArcSight Solutions/Compliance Insight Package tree on the manager.

Tip: This utility can be run on any Windows 2000 SP4 server or greater as long as the user has sufficient privileges to view the Active Directory. The Active Directory script must be run on a Windows system, but the resulting CSV file can be imported into a Unix system.

1. From the **Resources** tab in the Navigator pane, go to Files and navigate to ArcSight Solutions/Sarbanes Oxley 4.0/Active Directory User Group Gen folder.
2. Right-click the AD_User_Group_Gen.vbs file and select the **Download** option.
3. Browse for a directory location.
4. In the **File name** field, enter AD_User_Group_Gen.vbs and click **Save**.
5. A copy of the file is saved to the local file system.
6. From a Windows command prompt, change to the directory location where AD_User_Group_Gen.vbs file is stored.
7. Make a back up of the Visual Basic script AD_User_Group_Gen.vbs.
8. In a text editor, open the original script AD_User_Group_Gen.vbs and configure the following values appropriately for your environment:
 - **Set the Active Directory container path:** Search for the following string: strContainer = "CN=Users,DC=arcsight,DC=com" as shown highlighted below. Modify this string with the Active Directory hierarchy that applies for your environment. OU=organizational unit; CN=common name; DC=domain component. For more about Active Directory object naming, see <http://www.comptechdoc.org/os/windows/win2k/win2kadname.html>.
 - **Set the rootDSE:** The rootDSE establishes the base of the directory service hierarchy and tells the tool where to start the recursive search through the Active Directory hierarchy of user groups.
 - **Set the ArcSight Archive output directory:** As an option, you can also specify a different output directory for the archive file other than the default temp directory. For security purposes, you may

wish to use a more secure directory however ensure that the specified directory exists on your system, otherwise the tool will not operate properly. Search for the string: `strArchivePath = "c:\temp\"` as shown in the following figure, and replace it with the full directory path of the desired output location.



```

AD_User_Group_Gen.vbs - Notepad
File Edit Format View Help
' Arcsight Active Directory Integrator
' Queries AD for members in a group as well as creates a csv file of members in groups that can be
' imported into an Active List
' On Error Resume Next

' Set the Active Directory container path you wish to query specifically
strContainer = "CN=Users,DC=arcsight,DC=com"
' Set RootDSE for recursive search
rootDSE = "DC=arcsight,DC=com"
' Set the Archive Path for output Arcsight Archives
strArchivePath = "c:\temp\"

wscript.echo "Current Working Active Directory Group: " & strContainer

if wscript.Arguments.Count = 0 then
    wscript.echo "Jsage: AD_User_Group_Gen ListGroups"
    wscript.echo "Jsage: AD_User_Group_Gen Search"
    wscript.echo "Jsage: AD_User_Group_Gen ListMembers"
    wscript.echo "Jsage: AD_User_Group_Gen UserRoleAL"
|
    wscript.quit
End if

' set Args=wscript.Arguments

' Check command line args
strAcctFunc = ucase(wscript.Arguments.item(0)) ' User Account Management Function
wscript.echo strAcctFunc
If Err.Number <> 0 Then
    Echo ""
    Echo "***** ERROR: no Function supplied."
    Echo ""
    Echo "Use: c:\>cscript AD_ListGroups ListGroups"
    Echo ""
    Echo "Aborting..."
    Echo ""
    wscript.quit
End If

strGroupName = wscript.Arguments.item(0) ' Group Name
wscript.echo strGroupName

' Done checking command line args

```

9. Save the script and exit the text editor.

Run the Active Directory User Group Puller Script

After configuring the Active Directory script by setting the appropriate values for the necessary variables, you can run the script. This script has four options as listed in the following table. To invoke the option, type the corresponding command at the command prompt as shown in the following table:

List Groups	Generates a list of user groups in the specified container. The list is displayed on the Console and saved into the temporary folder in a file called <code>_GroupList.csv</code> . <code>cscript AD_User_Group_Gen.vbs ListGroups</code>
Search	Searches for users, computers or user groups using key letters or words. The output is displayed on the screen only. <code>cscript AD_User_Group_Gen.vbs Search</code>
List Group Members	Generates a list of the members in the chosen groups and saves them in the temporary folder in a file named <code>_UserList.csv</code> <code>cscript AD_User_Group_Gen.vbs ListMembers</code> When this option is specified, the script displays a list of groups. From this list, select one or more groups as described below in detail.
User Role Active List	Generates a list of the members in the chosen groups and the groups in which they are members. The list is saved in the temporary directory in file named <code>_ActiveList.csv</code> <code>cscript AD_User_Group_Gen.vbs UserRoleAL</code> When this option is specified, the script displays a list of groups. From this list, select one or more groups as described below in detail.

Each script option is listed in more detail below.

List Groups

When running the `AD_User_Group_Gen.vbs` script, specify the **ListGroup** option to create a list of all the user groups in the Active Directory and save the list to a file.

1. Open a Windows command window.
2. Change to the directory location where `AD_User_Group_Gen.vbs` file is stored and type the following command: `cscript AD_User_Group_Gen.vbs ListGroups` The script generates a list of all the user groups in the Active Directory and saves the list to a file named `_GroupList.csv` in the directory specified by the Archive Path.
3. Use the generated `_GroupList.csv` file to populate an active list. For detailed instructions, see [Configure Active Lists by Importing a CSV File](#) on page 41. The `ListGroup` option can be used to populate the Privileged User Groups Active List.

Search

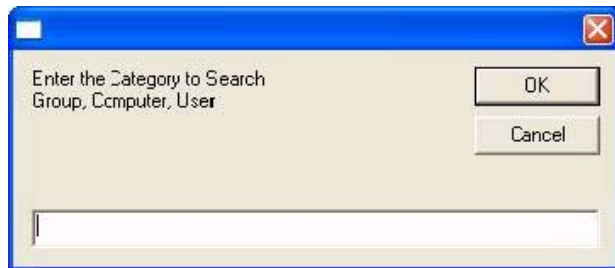
When running the `AD_User_Group_Gen.vbs` script, specify the Search option to search for an entity by name in the Active Directory. The following entities can be searched in the Active Directory: ■

- Users ■
- Computers ■
- User groups

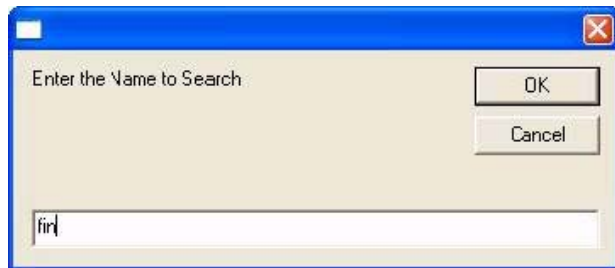
For example, if you know the group is sales related, you can type `finance` or `fin` to find all the finance group names. If you are looking for a specific user, search for the user name, not their user account (for example, search for `john`, not `jdoe`).

Note that all entries are case insensitive, for example typing `fin` is equivalent to typing `FIN`.

1. Open a Windows command window.
2. Change to the directory location where `AD_User_Group_Gen.vbs` file is stored and type the following command: `cscript AD_User_Group_Gen.vbs Search`
3. The script prompts for type of search. Enter **Group, Computer, or User** and click **OK**



4. The script prompts for the search string. In the example below, you are searching for finance group names. Enter the string you want to search for and click OK.



5. The script searches for matching entries and displays the result in the LDAP Entries Found dialog box. The dialog box displays the CN and DC hierarchy for the matching results.
6. You can use the generated list of users, computers, or groups to populate an active list, using one of the following methods:
 - Cut and paste from the LDAP Entries Found dialog box into the Active List editor of the ArcSight Console. For detailed instructions on using the Active List editor, see [Configure Active Lists Using](#)

Console Active List Editor.

- Create a comma separated (CSV) file using an editor and cut and paste from the LDAP Entries Found dialog box into a CSV file and then import the CSV file into an active list. For detailed instructions on importing a CSV file, see Configure Active Lists by Importing a CSV File.

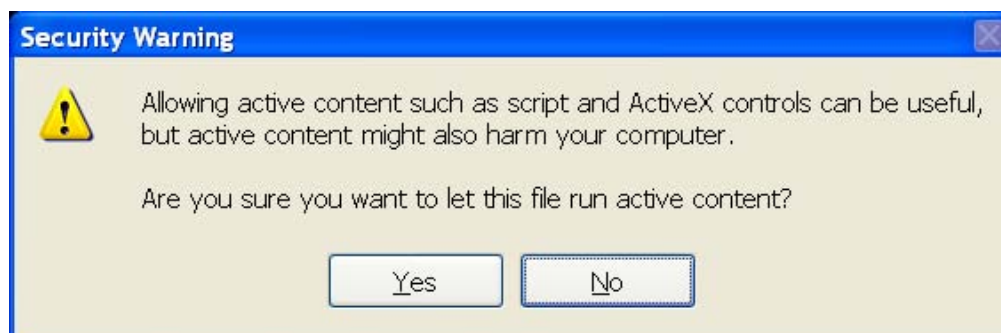
List Group Members

When running the `AD_User_Group_Gen.vbs` script, specify the **ListMembers** option to list the members of Active Directory groups. The generated user list is saved into a file named `_UserList.csv` in the directory specified by the Archive Path. You can then import the list into an Active List using the ArcSight Console.

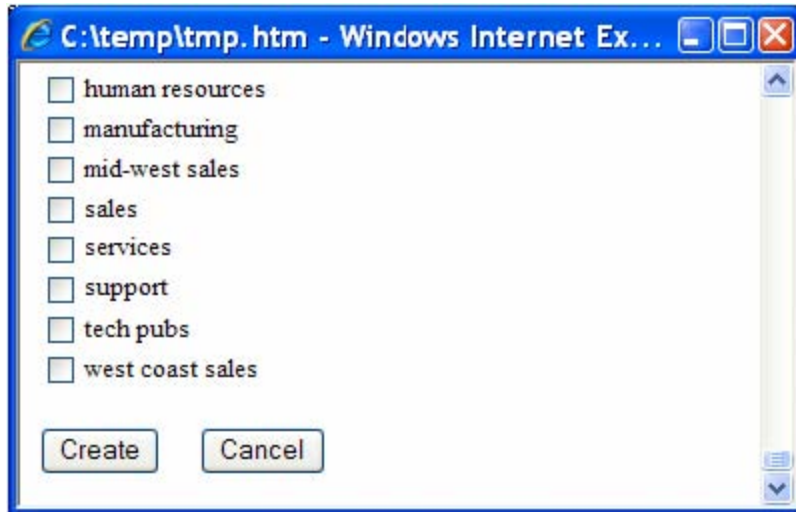
1. Open a Windows command window.
2. Change to the directory location where `AD_User_Group_Gen.vbs` file is stored and type the following command: `cscript AD_User_Group_Gen.vbs listmembers`
3. The script integrates the Active Directory and displays a Internet Explorer Browser window with all the groups in the container.
4. If your Browser is set to block scripts, click the **To help protect...** alert message at the top of the window and select the **Allow Blocked Content...** option as shown in the following figure.



5. To enable active content to run, in the Security Warning dialog box, click Yes as shown in the following figure.



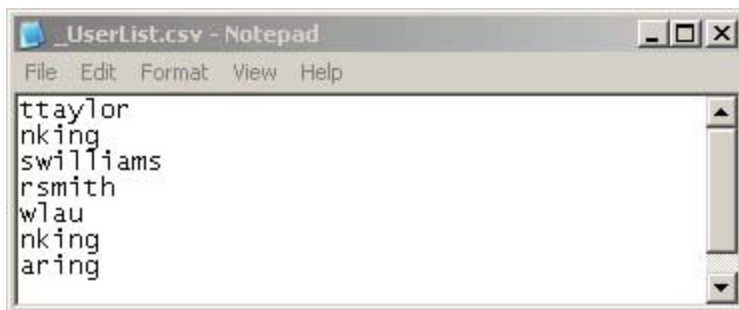
6. Select the groups whose members you would like to list and scroll down and click Create.



The script recursively searches for users who are members of the selected groups and places the list into the `_UserList.csv` file as a single-column list. All the members of a selected group are listed. The script lists a user of a non-selected group, if that non-selected group is a member of a selected group. For example, if aring is a member of the tech pubs group and the tech pubs group is a member of the corporate group, if the corporate group is selected but tech pubs group is not, the user aring is still listed.

If a user is member of multiple groups that are selected, the user is listed multiple times in the list. However, once the list is imported into an Active List, each user name is only listed once. For example, if both the services and support group are selected and the user nking is a member of both, nking is listed twice as shown in the following `_UserList.csv` file.

The generated user list is saved into a file named `_UserList.csv` in the directory specified by the Archive Path.



7. Use the generated `_UserList.csv` file to populate an active list. For detailed instructions, see [Configure Active Lists by Importing a CSV File](#) on page 41. The **ListMembers** option can be used to populate the following Active Lists:

- Administrative Accounts List
- Contractor Accounts

- Former Employees
- New Hire Accounts

User-Role Active List

When running the `AD_User_Group_Gen.vbs` script, specify the **UserRoleAL** option to list the user names of the selected groups. For each user name, all the groups that the user is a member of are listed. The generated list is saved into a file named `_ActiveList.csv` in the directory specified by the Archive Path.

The script searches recursively for users in the selected groups but only the top-level selected group is associated with the user. For example, if you selected the `corporate` group that has the `development` group as member and the user `wlau` is a member of `development` group, the output file lists `wlau` as a member of the `corporate` group as shown in the following example `_ActiveList.csv` file.

If a user is member of more than one selected group, that user name appears in the CSV file only once, comma-separated with all the selected groups the user is a member of. For example if `rsmith` is a member of the `finance` and `corporate` groups and both of these groups are selected, `rsmith` is listed only once, as shown in the following example `_ActiveList.csv` file.



The users listed in the beginning of preceding figure are all members of more than one group, while the users at the bottom of the figure are members only of only one group.

Each group must be separated with a pipe (|) delimiter. Separating group names using the pipe delimiter allows you to search uniquely for a group in the conditions of rules and filters. For example, you could specify the following condition in a filter:

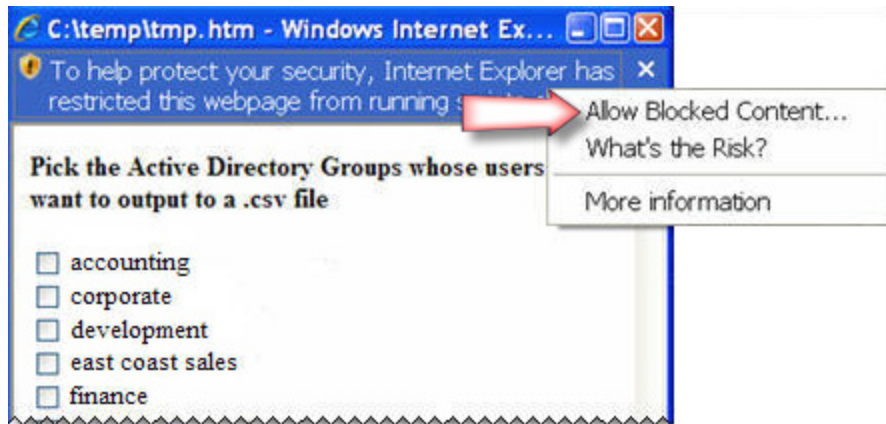
```
Role CONTAINS |finance|
```

This condition would match a group called `finance` but would not match a group called `finance managers`.

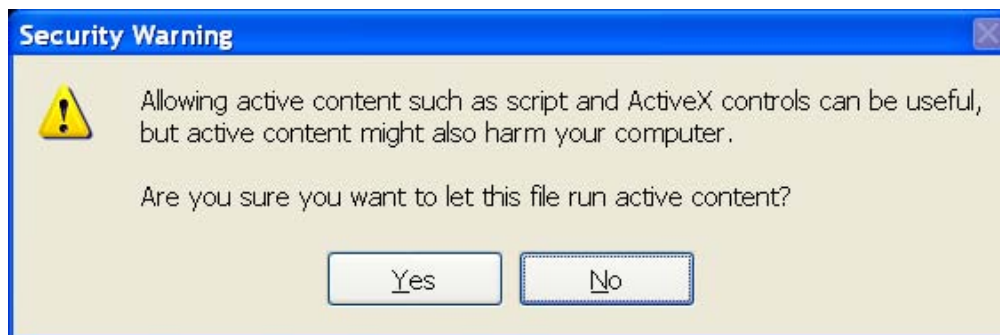
To generate the user-role CSV file:

1. Open a Windows command window.
2. Change to the directory location where `AD_User_Group_Gen.vbs` file is stored, and type the following command: `cscript AD_User_Group_Gen.vbs UserRoleAL`

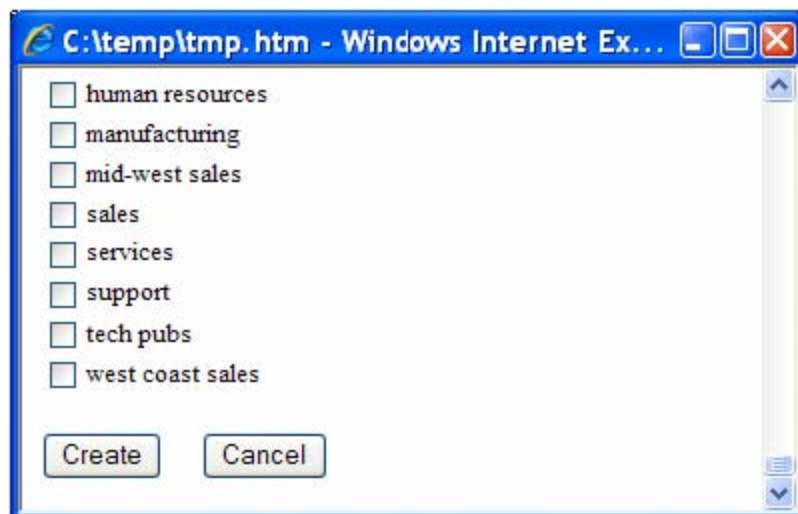
3. If your Browser is set to block scripts, click the **To help protect...** alert message at the top of the window and select the **Allow Blocked Content...** option as shown in the following figure.



4. To enable active content to run, in the **Security Warning** dialog box, click **Yes** as shown in the following figure.



5. Select the groups whose members you would like to list and scroll down and click **Create**.

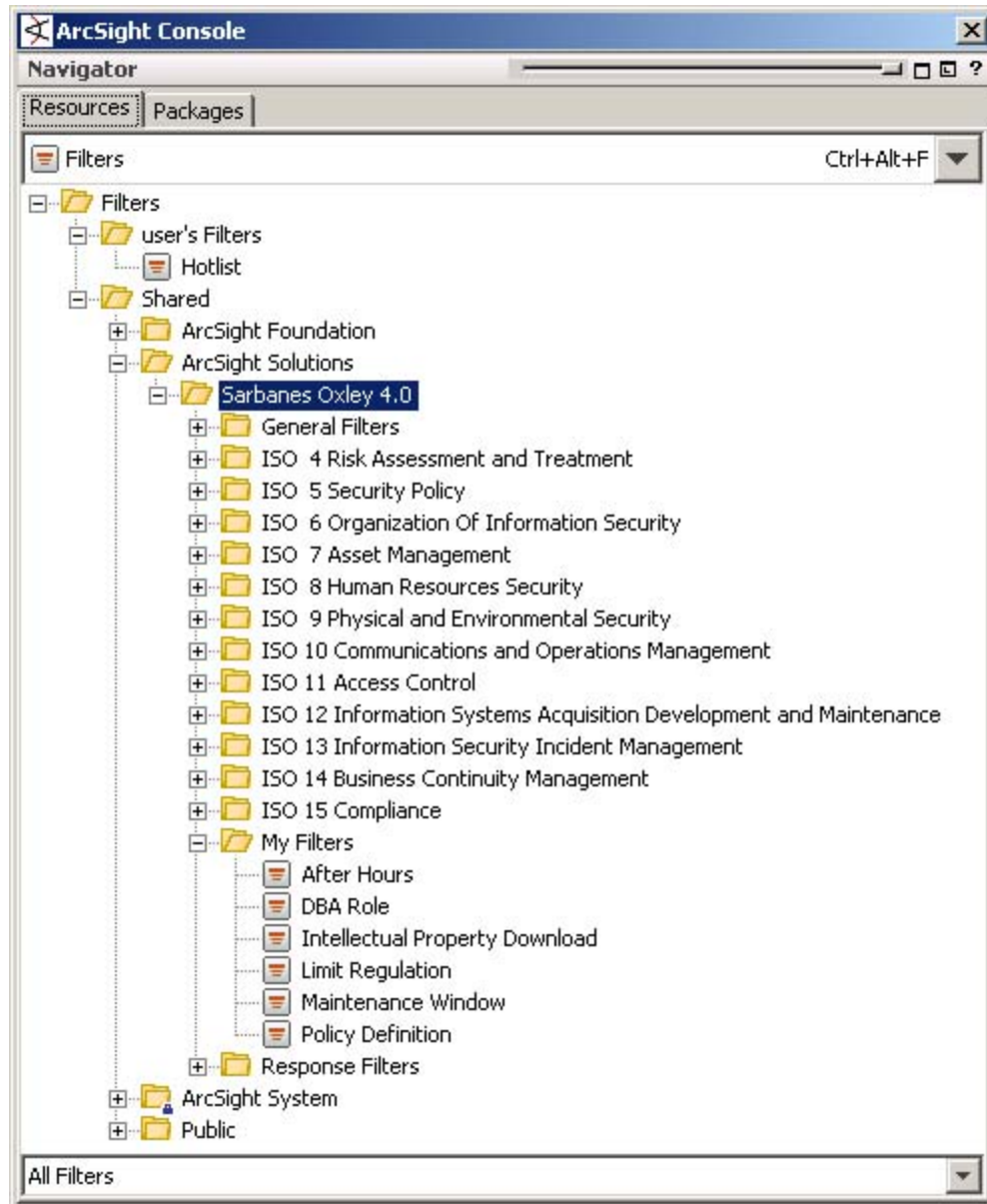


The generated list is saved into a file named `_ActiveList.csv` in the directory specified by the Archive Path.

6. Use the generated _ActiveList.csv file to populate an active list. For detailed instructions, see [Configure Active Lists by Importing a CSV File](#). The **UserRole** option can be used to populate the User Role Active List.

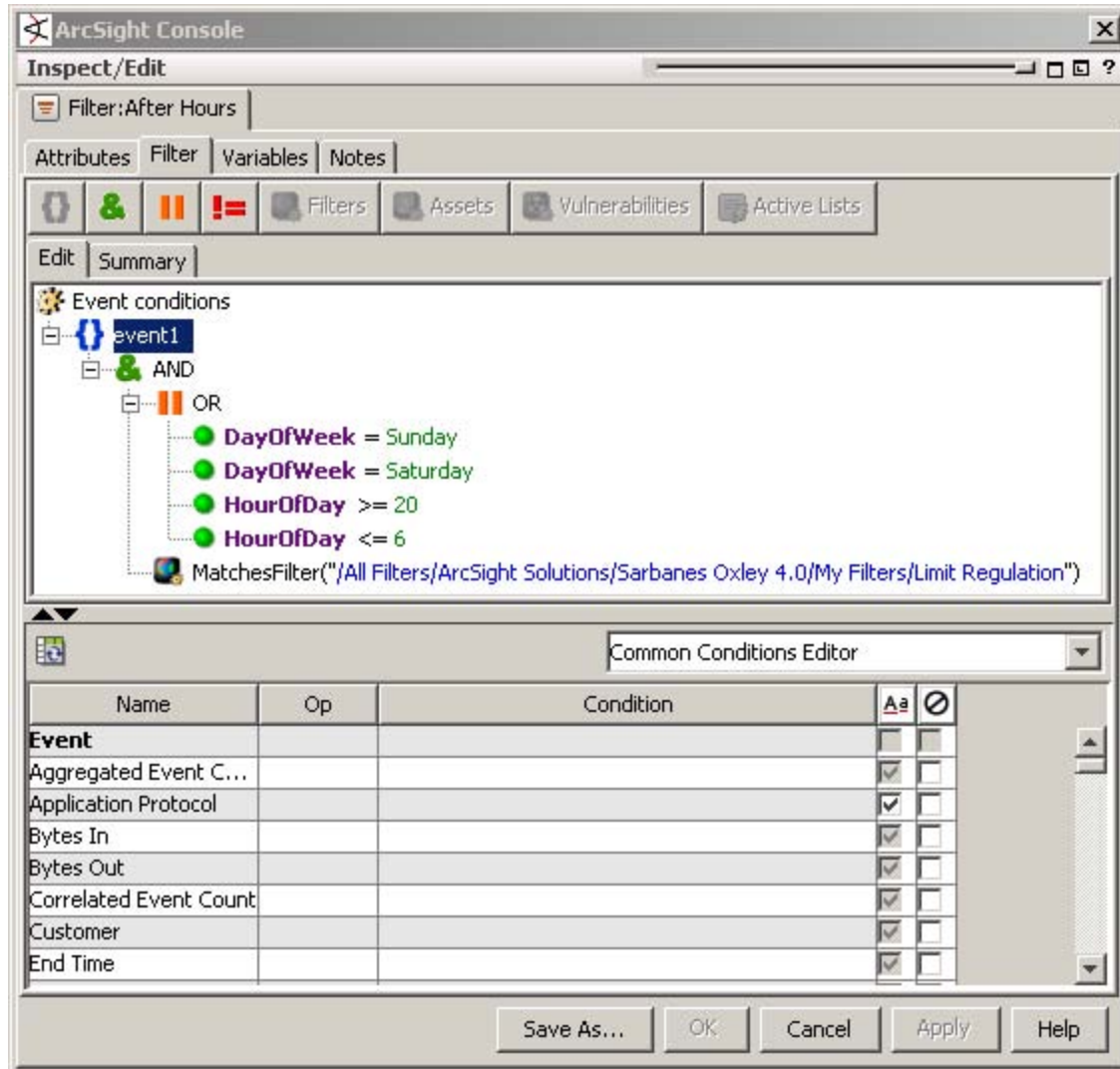
Configure My Filters

The My Filters group contains several filters that should be configured with values specific to your environment.



After Hours Filter

The After Hours filter defines the time period which is considered to be after business hours. The default after hours time period is set to 8:00 p.m. to 6:00 a.m. on weekdays, and all day Saturday and Sunday.



The filter uses two variables:

- DayOfWeek
- HourOfDay

You can change this filter to match what is considered to be after hours for your organization.

Tip: The DayOfWeek variable returns an integer value that is displayed on the ArcSight Console as a string value of the current day: Saturday, Sunday, Monday, Tuesday, Wednesday, Thursday,

or Friday. Since the DayOfWeek variable is an integer, you can specify a range of days such as (DayOfWeek >= Monday AND DayOfWeek <= Friday).

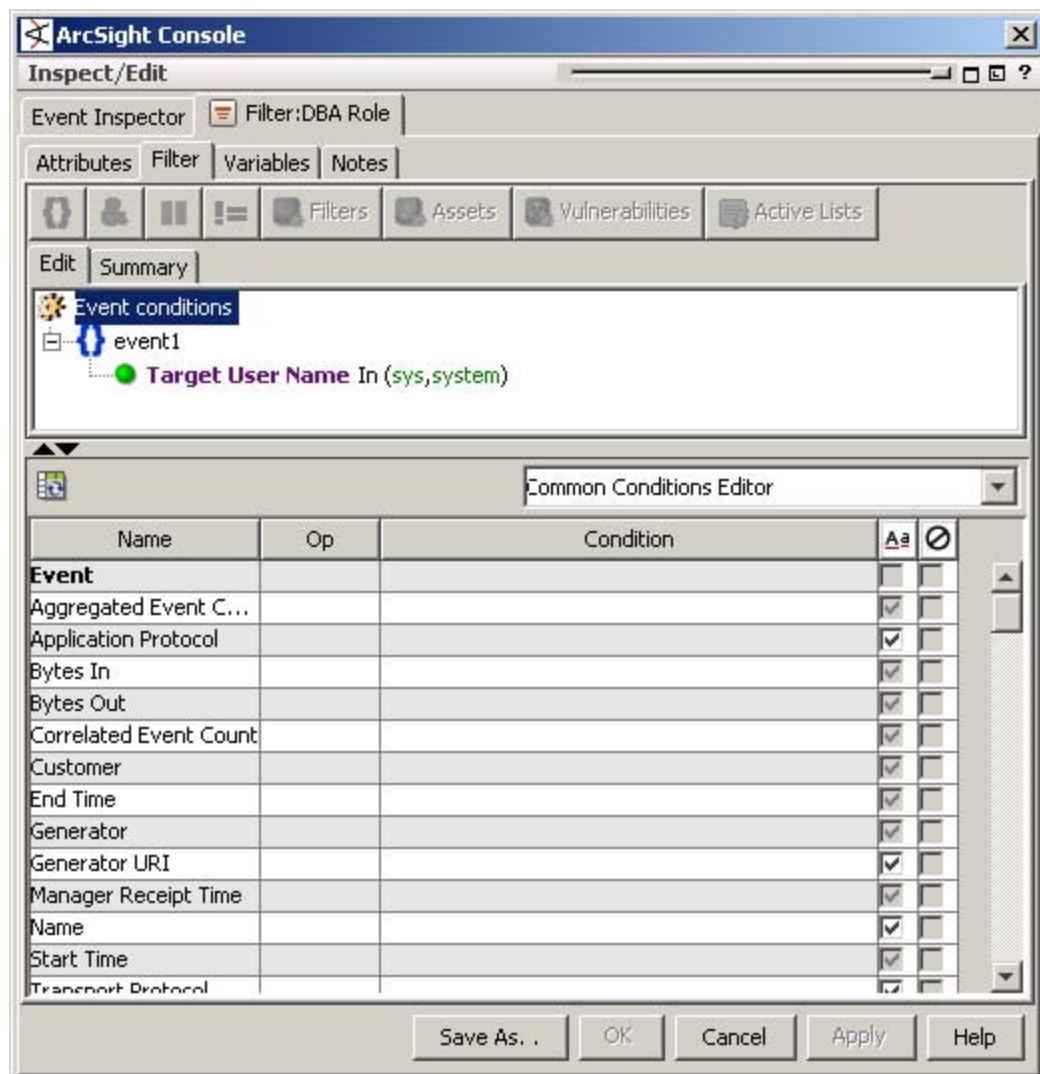
The HourOfDay variable returns a numerical value for the current hour in 24-hour format ranging from 12 AM = 0 to 11 PM = 23.

For example: After business hours from 6:00 PM to 8:00 AM on all weekdays, and all of Saturday and Sunday would be defined by the following filter expression:

(DayOfWeek = Saturday OR DayOfWeek = Sunday OR HourOfDay >= 18 OR HourOfDay <= 8)

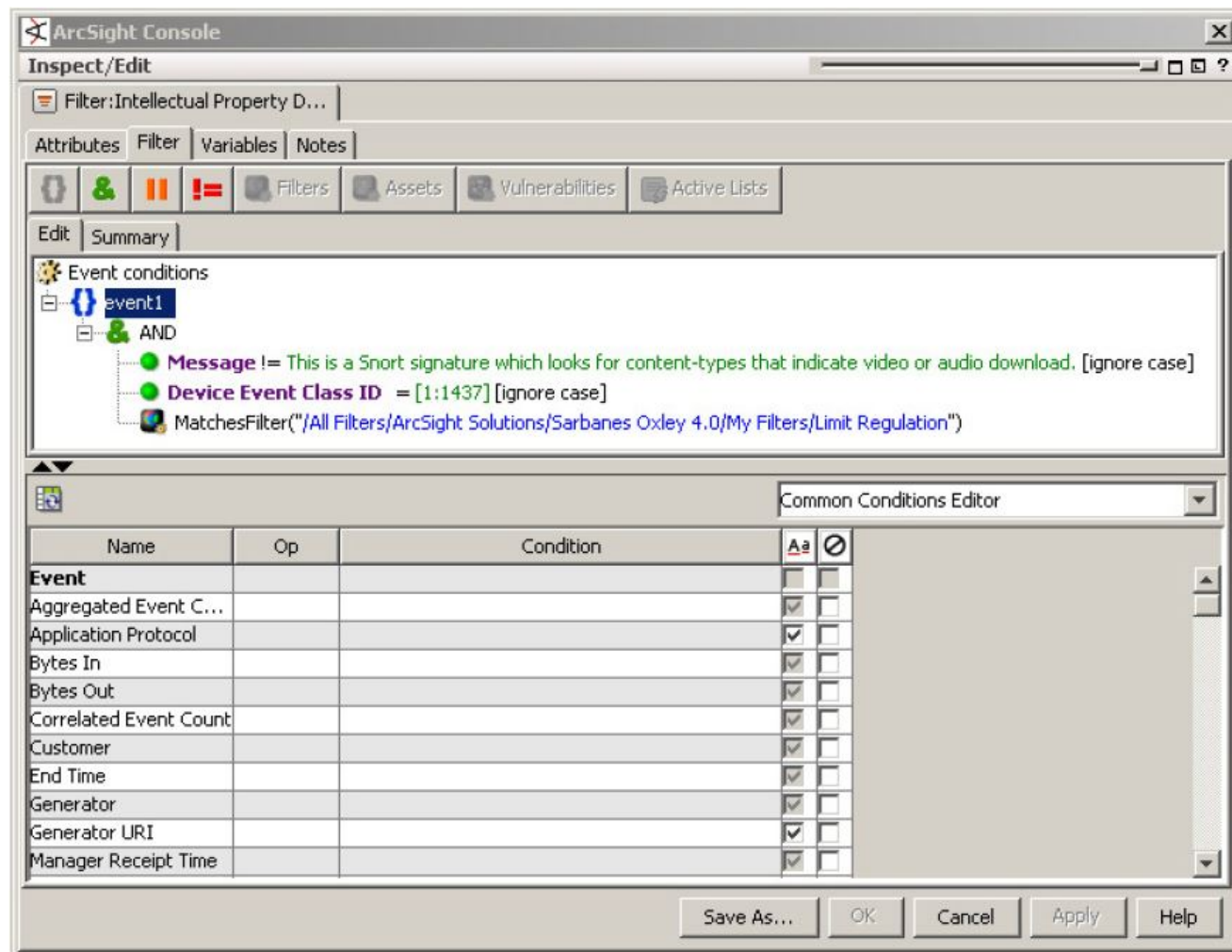
DBA Role

The DBA Role filter defines the privileged database administration (dba) user names. The user names specified in this filter are the default Oracle dba accounts called sys and system as shown in the following figure. Change or add new dba accounts to reflect your environment.



Intellectual Property Download Filter

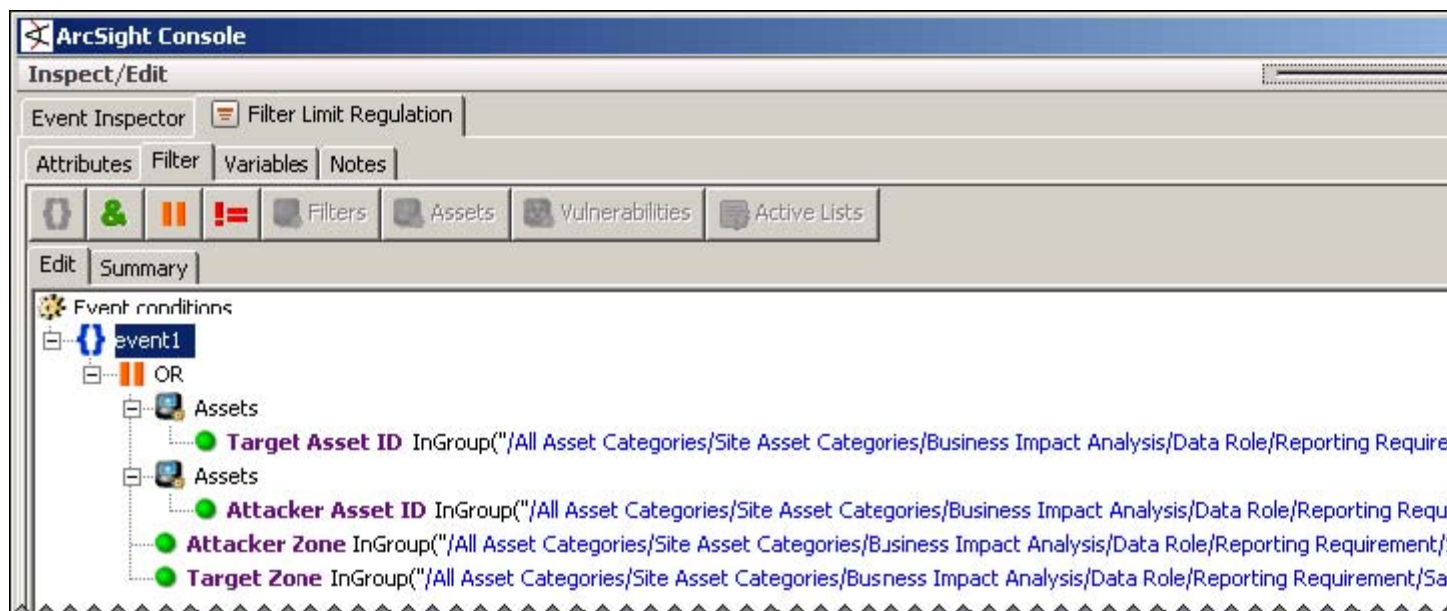
The [Intellectual Property Download](#) filter finds events that involve the download of possibly illegal intellectual property. By default, this filter is set to find a Snort signature that indicates video or audio download. Add the signatures for the content monitoring device(s) or NIDS you use that indicate intellectual property downloads, such as video streams, images, audio files, or possibly illegal intellectual property or copyrighted material.



Configuration Tip: Do not include conditions that select peer-to-peer protocols. That scenario is addressed in a separate filter.

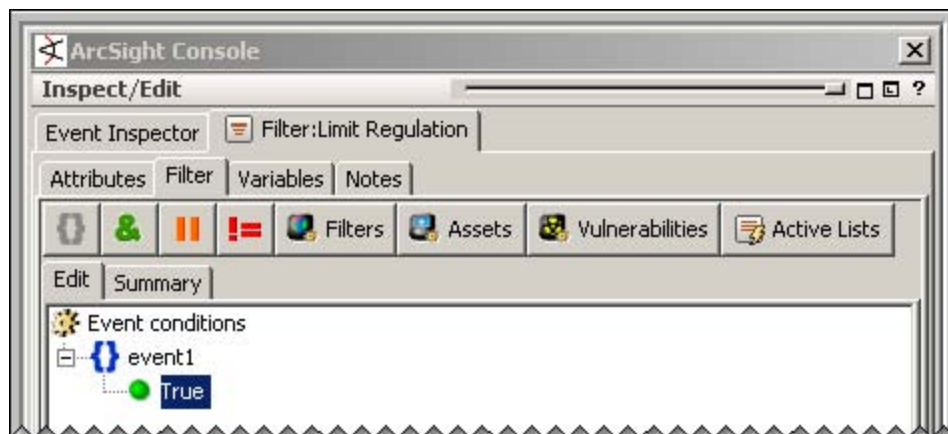
Limit Regulation Filter

By default, the Limit Regulation filter specifies that only events pertaining to Sarbanes- Oxley assets arriving at the Manager are evaluated by the SOX4 solution.



All SOX4 “decision-making” resources (filters, rules, active channels, reports, and data monitors) refer to this filter. For example, one of the AND conditions of the Default Vendor Account Used filter is a reference to MatchesFilter function with the Limit Regulation filter as the argument. This reference to the Limit Regulation filter by the Default Vendor Account Used filter means that only events pertaining to Sarbanes-Oxley assets are processed by the After Hours filter.

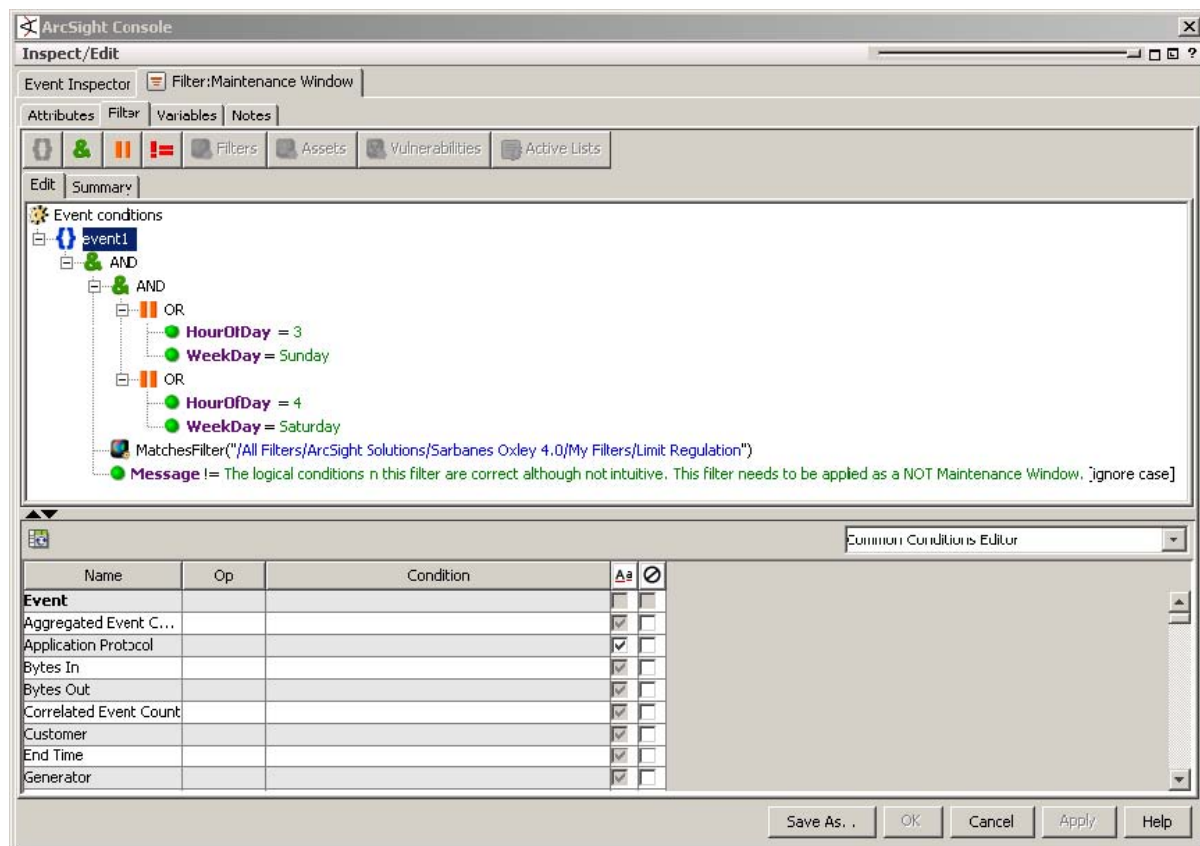
To configure this filter to direct all events to the SOX4 solution content for evaluation, modify the Limit Regulation filter, remove the existing conditions and create a default condition equal to True as shown in the following figure.



Maintenance Window Filter

This filter defines what is considered network maintenance time window(s). Various Sarbanes-Oxley resources look for events outside of the maintenance windows by first referencing this filter in their conditions, and then negating it.

The default maintenance windows are from 3:00 a.m. to 3:59 a.m. on Sundays, and 4:00 a.m. to 4:59 a.m. on Saturdays.



You can change this filter to adjust the default settings to match the maintenance window(s) for your environment.

The filter uses two variables:

- WeekDay
- HourOfDay

Configuration Tip: WeekDay returns a string value of the current day: Saturday, Sunday, Monday, Tuesday, Wednesday, Thursday, or Friday. HourOfDay returns a numerical value for the current hour in 24-hour format ranging from 12 AM = 0 to 11 PM = 23. **For example:** Maintenance windows of Tuesday morning, 1:00 AM to 3:00 AM, and Friday morning, 5:00 AM to

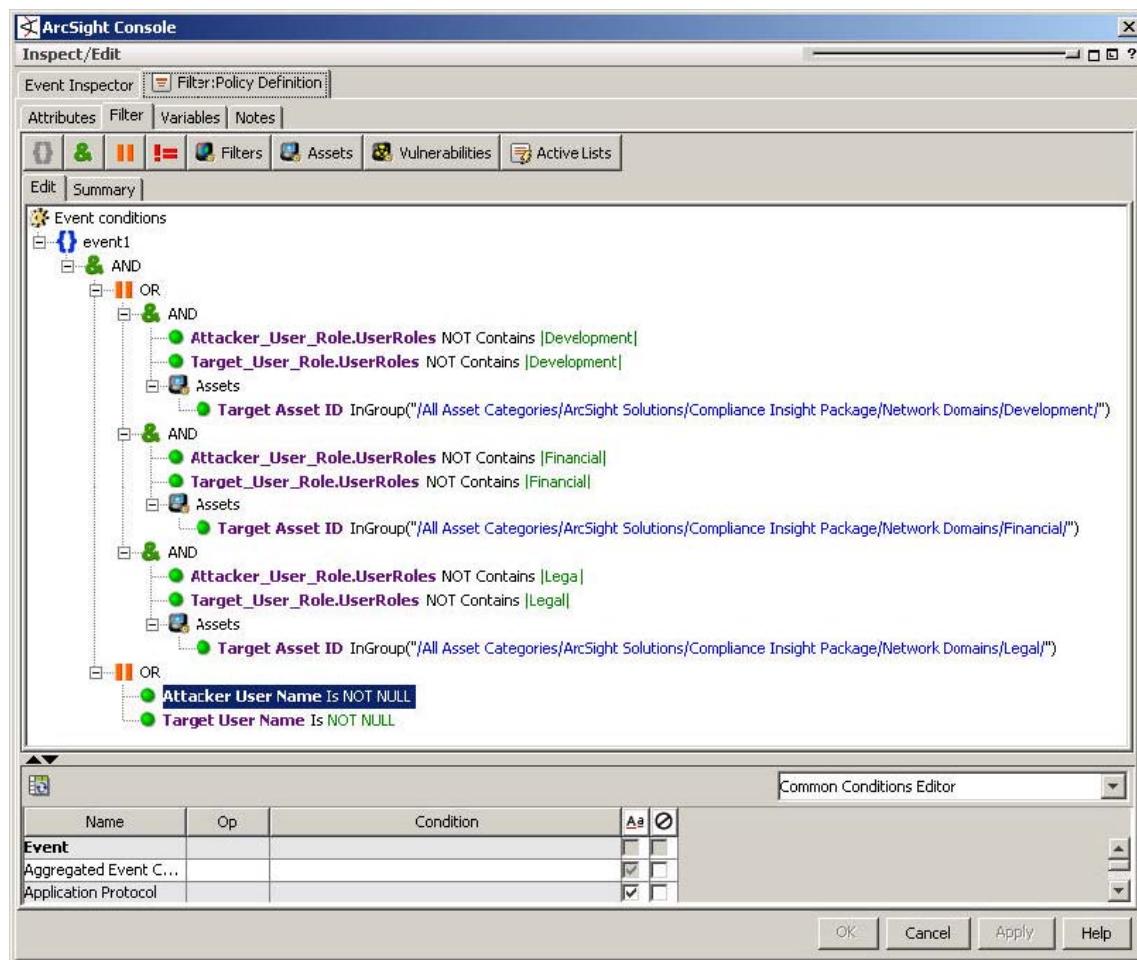
6:00 AM would be defined by the following filter expression:

(WeekDay = Tuesday OR HourOfDay >= 1 OR HourOfDay < 3) AND (WeekDay = Friday OR HourOfDay = 5)

If you build a resource that refers to this filter, use the NOT operator when referring to it to exclude events that occur in this time window.

Policy Definition Filter

This filter is used to define what users have permission to access what machines based on their respective roles and asset categories.



The filter consists of multiple sub-conditions that each verifies whether the given conditions are true. Multiple conditions are combined with an OR, so the filter will evaluate to true if any of the sub-conditions are true. A single condition is shown in the following figure:



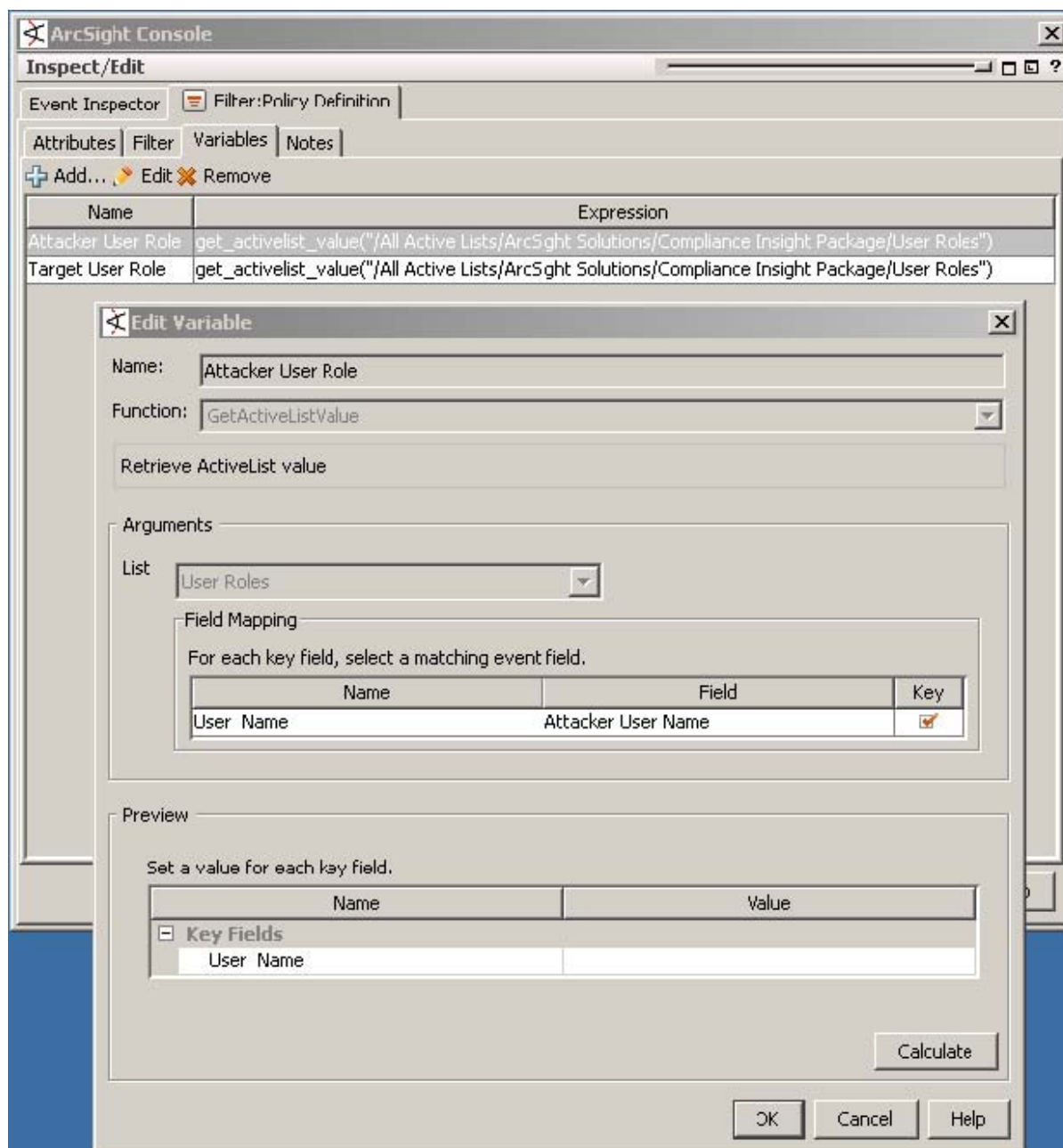
This condition evaluates to true if an event indicates someone accessing an asset categorized as a financial system and the user itself is not in the `Financial` user group, as expressed with the first two conditions.

The Identify Based Access Violation rule monitors this filter and fires for every instance where the role-based access is violated. For example, if the Target Asset ID is categorized as a `Financial` asset, the filter fires if neither the target User Name nor the attacker User Name from the event has the `Financial` role.

For example, a User Name `ttaylor` is granted access to the `Financial` and `Legal` roles in the User Role active list. An event is received where the Target Asset is categorized as a `Financial` asset, the filter checks that the User Roles associated with the Attacker User Name to make sure `Financial` is listed in the Active List. In addition, the filter checks the User Roles associated with the Target User Name to make sure `Financial` is listed in the Active List.

`Attacker_User_Role.UserRoles` and `Target_User_Role.UserRoles` are both variables that are populated by the `GetActiveListValue` function which takes as input the User Name, searches for the User Name in the User Roles active list and returns the list of all the User Roles for the UserName as shown in the following figure.

For this example, the Attacker User Name `ttaylor` is supplied to the `GetActiveListValue` function and the function checks the User Roles active list for the list of Roles associated with the Attacker User Name `ttaylor` and returns the values of `Financial` and `Legal` in the `Attacker User Role` variable. The filter tests the values returned by the Attacker User Role variable to see if `Financial` is not found in the list. In addition, the filter tests the values returned by the `Target User Role` variable to see if `Financial` is not found in the list.



Configuring the Policy Definition Filter

After modeling assets into the appropriate Network Domain, you may want to configure the default conditions in the Policy Definition filter. For example, if you categorized some assets into the Commerce category, you might want to add the following additional AND condition to the filter as shown by the following figure.



You may want to also add roles that can assess particular assets. For example if users assigned to the Administrator role need access to the Development servers, you may want to add the following conditions to the existing AND conditions as shown by the following figure.



Configure Rules

Configure the following ISO section 1.1.1 rules with the role name of the system administrator for your environment: ■

- Privileged Access Attempt Detected
- Unauthorized Admin Access to Domain Controller

By default, these rules specify the role name of sysadmin. Edit the rule and change sysadmin to the role name of the system administration for your environment. Do not remove the pipe (|) from the start or end of the string.

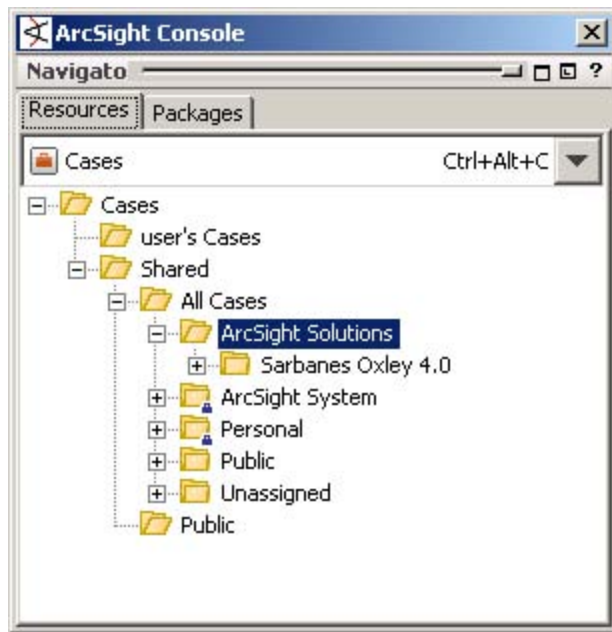
Configure the following ISO section 1.1.1 rule with the role name of the database administrator for your environment: ■

- Database Privilege Violation

By default, these rules specify the role name of dba. Edit the rule and change dba to the role name of the database administrator for your environment. Do not remove the pipe (|) from the start or end of the string.

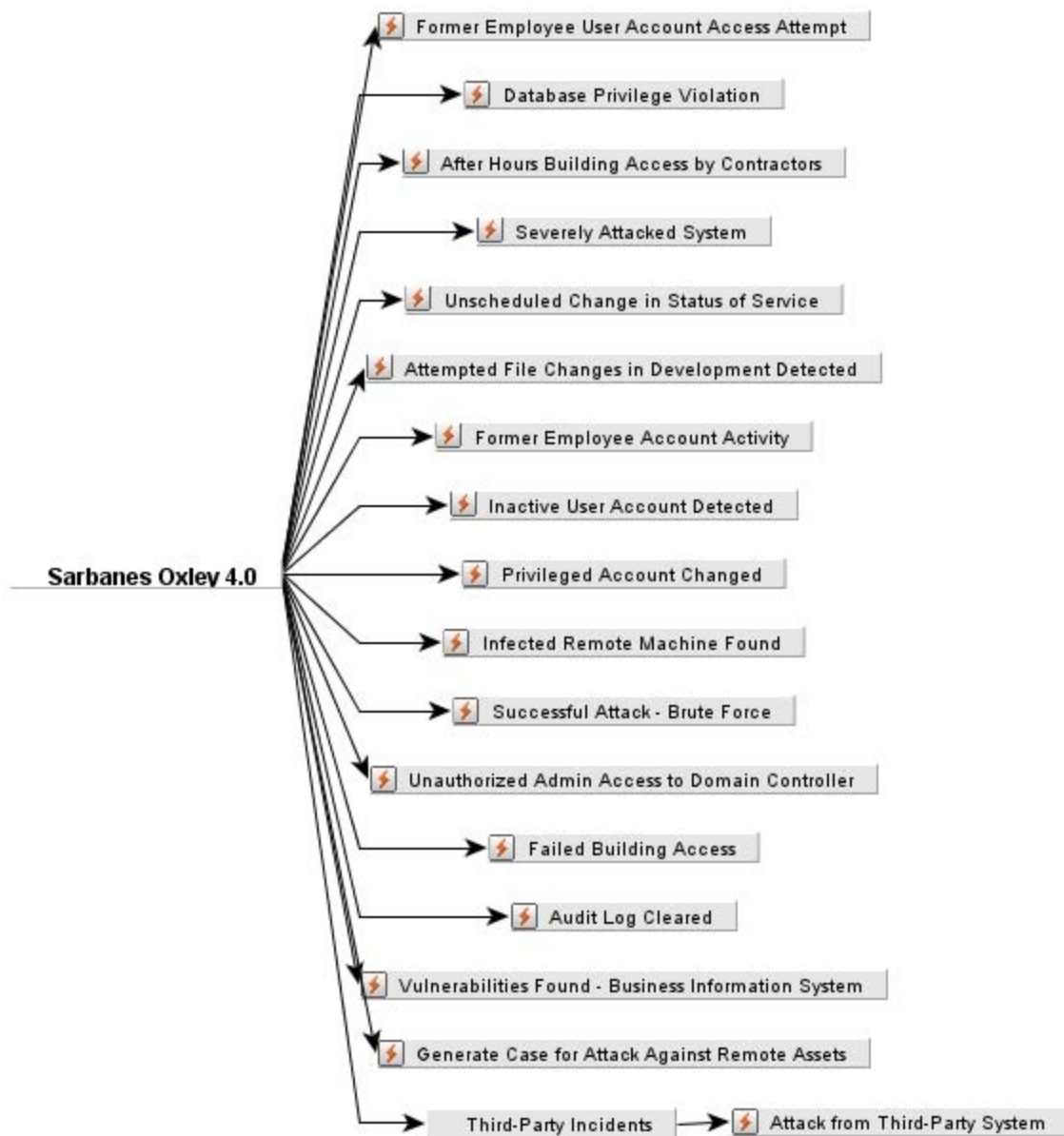
Configure Cases

Cases are ArcSight's trouble-ticket system that can be used as-is or in conjunction with a third-party trouble-ticket system. The SOX4 solution includes a special container for cases generated by Sarbanes-Oxley rules in the Compliance Insight Package group.



You can add more groups within the Compliance Insight Package group or your own group if you want to add more differentiations. If you do add more distinctions to the Compliance Insight Package group, modify the ArcSight rules that generate cases to make use of your new case groups.

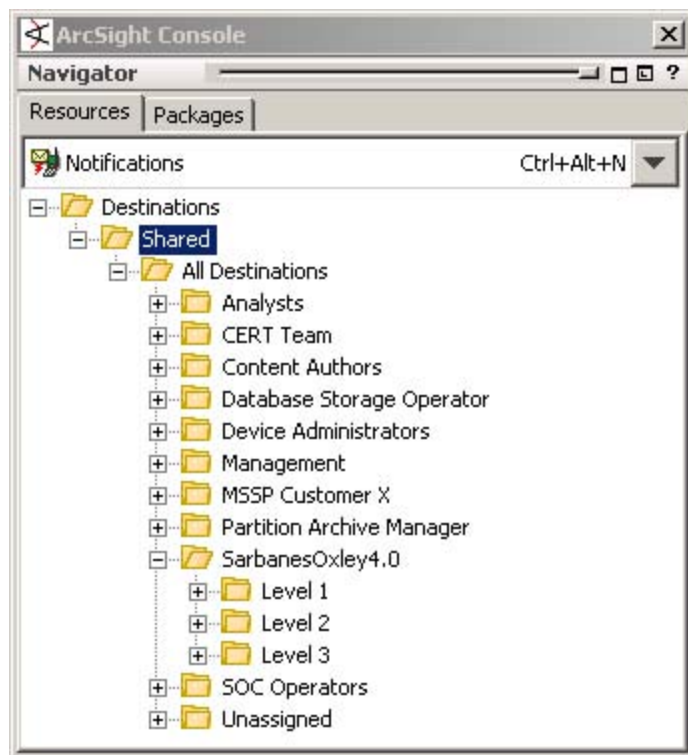
The rules in the following diagram all produce cases that are stored in the Sarbanes-Oxley group.



The Sarbanes-Oxley 4.0 cases group receives cases generated by the rules shown in the above resource graph.

Configure Notification Destinations

By default, the SOX4 solution rules make use of the following three levels of notification destinations:



Configure these levels with the users and/or user groups of those you wish to notify about Sarbanes-Oxley incidents. To configure the notification levels:

1. Right-click the notification level you wish to populate and select **New Destination**.
2. In the Notification editor, enter the following values and click **OK**:

Name	Value
Name	Enter a name for the notification destination. This will be used to identify the destination in the Navigator panel.
Start time	By default, the time values are set for 24 hours. If you wish to notify different people on different shifts, modify the start time with the start time of the shift.
End time	If you are specifying shifts, enter the end time of the shift.
Destination type	<p>Console. Select Console to notify the user with an alert in the ArcSight Console.</p> <p>E-mail. Select E-mail to notify the user or user group by e-mail. Enter the e-mail address of the user or user group on the next line.</p> <p>Pager. Select Pager to notify the user's pager. Enter the pager number, PIN, and pager provider, as applicable.</p> <p>Cell phone. Select Cell Phone to send a text message to a cell phone. Enter the e-mail address of the cell phone, for example, 2025551212@mycellphone.com.</p>
User/group	In the drop-down menu, navigate to the user or user group you wish to notify about Sarbanes-Oxley incidents at this level.

- Repeat step 2 for every group you wish to notify about those threats and for every method by which you want to notify them.

You can add your own notification destinations to this hierarchy.

Build FlexConnector(s) for Physical Access Devices

The SOX4 solution contains scenarios that make use of feeds from physical access systems, such as badge readers. This process is only required if you want to activate the SOX4 content that leverages feeds from physical access systems. If you do not complete this process, the content that leverages feeds from physical access systems will remain dormant.

To enable these scenarios, develop a FlexConnector according to the instructions in the *ArcSight FlexConnector Developer's Guide* with the following field mappings to map the key event data into the ArcSight event schema:

Field Mappings

ArcSight Field	Physical Access System Value
deviceEventClassId	Unique value for event type used for categorization
deviceReceiptTime	Access Time
destinationUserId	Users badge Id
deviceCustomString1	Location Accessed / Building

Use the following event categories for the following event types:

Event Categories

Event type	Object	Behavior	Technique	Device Group	Outcome	Significance
Successful building access	/Location	/Authentication/Verify		/Physical Access System	/Success	/Normal
Building access rejected	/Location	/Authentication/Verify		/Physical Access System	/Failure	/Information/Warning
Badge-out (someone is leaving a building) [not all badge reader systems support this]	/Location	/Access/Stop		/Physical Access System	/Success	/Normal

Event Categories, continued

Event type	Object	Behavior	Technique	Device Group	Outcome	Significance
Account created/deleted/modified - [Success assumed; in case of a failure, the Outcome needs to reflect that and the significance is /Informational/Error]	/Actor/User	/Authentication/ [Add Delete Modify]		/Physical Access System	/Success	/Informational
Giving someone access to another room/building - [Success assumed; in case of a failure, the Outcome needs to reflect that and the significance is /Informational/Error]	/Actor/User	/Authorization/Modify		/Physical Access System	/Success	/Informational
Granting access to a room/building for an entire group of users	/Actor/Group	/Authorization/Modify		/Physical Access System	/Success	/Informational

You can add more user context to the events generated by your badge reader by creating a connector event mappings file.

Configure Connector Event Mapping Files

Most devices generate event data that populate logs with basic operational information that is adequate for general device operation. In some cases, however, this basic data may not be adequate for the analysis and correlation required to identify possible regulation compliance violations.

It is possible to extend events from systems such as badge readers or VPNs with the user's Windows or Unix logon account name. This allows for correlation between VPN or physical access systems and operating system events.

In order to extend a device's event mappings, you can apply a simple map file generated in a text editor to the connector that translates the device's events to ESM.

1. On the Connector system, navigate to: <connector home>/user/agent/map/
2. In a text editor, create a map file similar to the example below. This example shows output from a badge reader system. The top line represents the column headings for the comma-separated values: badgereader is the device vendor, doors is the device product, 123xxx is the badge ID, and jdoe is the destination user name.



3. Save the file in the <connector home>/user/agent/map/ directory with the file name map.n.properties, where n is 0, 1, or the next sequential number in line.
- ArcSight connectors, whether built by ArcSight or FlexConnectors, contain the default map properties files map.0.properties and map.1.properties, which you can use to create your own custom mappings.
 - If 0 and 1 are already configured with other custom mappings, you can use the next available number. For example, if your connector already makes use of mapping files 0-10, name this file map.11.properties.

You can create mapping files like these for other devices whose user IDs may not match those of operating system logins, such as VPNs. Contact ArcSight Professional Services for tips about creating map files for other devices.

Configure Sarbanes-Oxley Scenarios

Additional configurations may be required or desired for individual resources for the Sarbanes-Oxley scenarios. Refer to individual chapters for details about the resources contained in them and how they are configured.

Note: The rules contained in the SOX4 solution are not enabled by default. To enable the rules you want to use, right-click the rule and select Enable Rule.

Upgrade from SOX2 to SOX4

The Compliance Insight Package for Sarbanes-Oxley 4.0 has been updated to utilize the ISO 17799:2005 framework. The solution significantly expanded to include more compliance-related use cases. It also includes enhanced monitoring and reporting features.

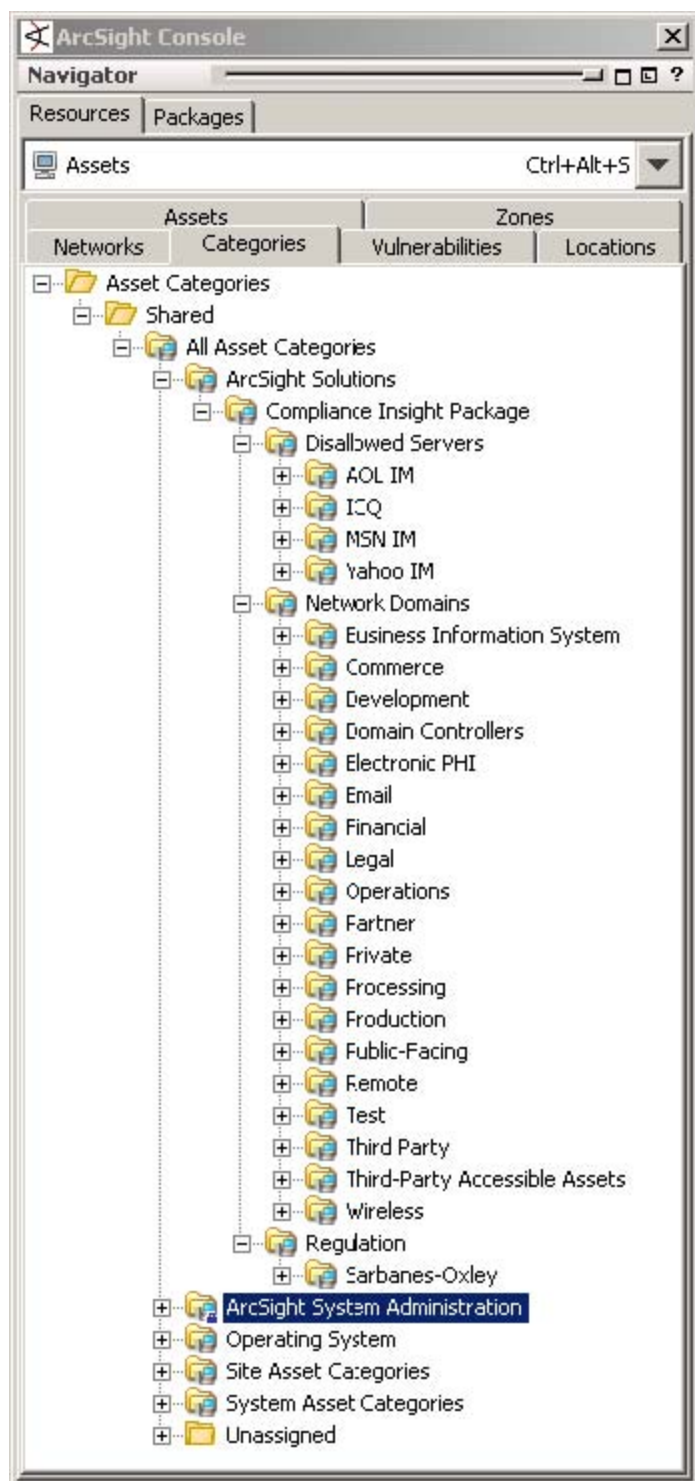
So as not to disrupt your existing Sarbanes-Oxley 2.0 (SOX2) installation and any customizations you have made to it, SOX4 installs into its own tree, so the two solutions can run side by side with your

already existing installation of SOX2. Typically running the two solutions together is not recommended because there are duplicate sets of rules running with the same conditions producing duplicate events.

The Sarbanes-Oxley 4.0 solution does not overwrite any existing SOX2 resources, either those supplied by ArcSight, or those you have created yourself.

Compliance Insight Package Asset Categories

All the Compliance Insight Packages share the Compliance Insight Package Asset Categories group. The following figure shows the expanded Compliance Insight Package Asset Categories group with the Sarbanes-Oxley 4.0 solution installed.



The new SOX4 asset categories will be installed to this existing structure. Because asset categories do not themselves contain any data, you do not have to worry about customizations being overwritten. Any asset categories you have added to the Compliance Insight Package tree will be preserved.

Compliance Insight Package Active Lists

The Compliance Insight Packages also share the Active Lists directory. The new SOX4 active lists install into a different location than the SOX2 active list but the SOX2 active lists are preserved. All active list entries you have made to the SOX2 active lists are preserved.

Transfer SOX2 Customizations to SOX4

Any modifications you have made to resources, such as filters and reports, will not be transferred to the SOX4 solution, but they will still be preserved and operational in the SOX2 material.

With both solutions installed in different groups, however, the SOX2 rules (such as methods to detect policy violations) will not be factored into the SOX4 overview dashboards, which show the overall compliance status.

As an option, you can also move the SOX2 dashboards and data monitors into the SOX4 structure, although no functionality is lost if you don't.

Once the content you want to preserve from v2.0 is transferred, you can manually delete the remaining SOX2 resources. It is also possible to do a "partial" uninstall of the SOX2, although manually deleting the version 2.0 resources is the recommended method.

Mapping SOX2 Resources to SOX4

There are two areas that have been preserved from SOX2: ■

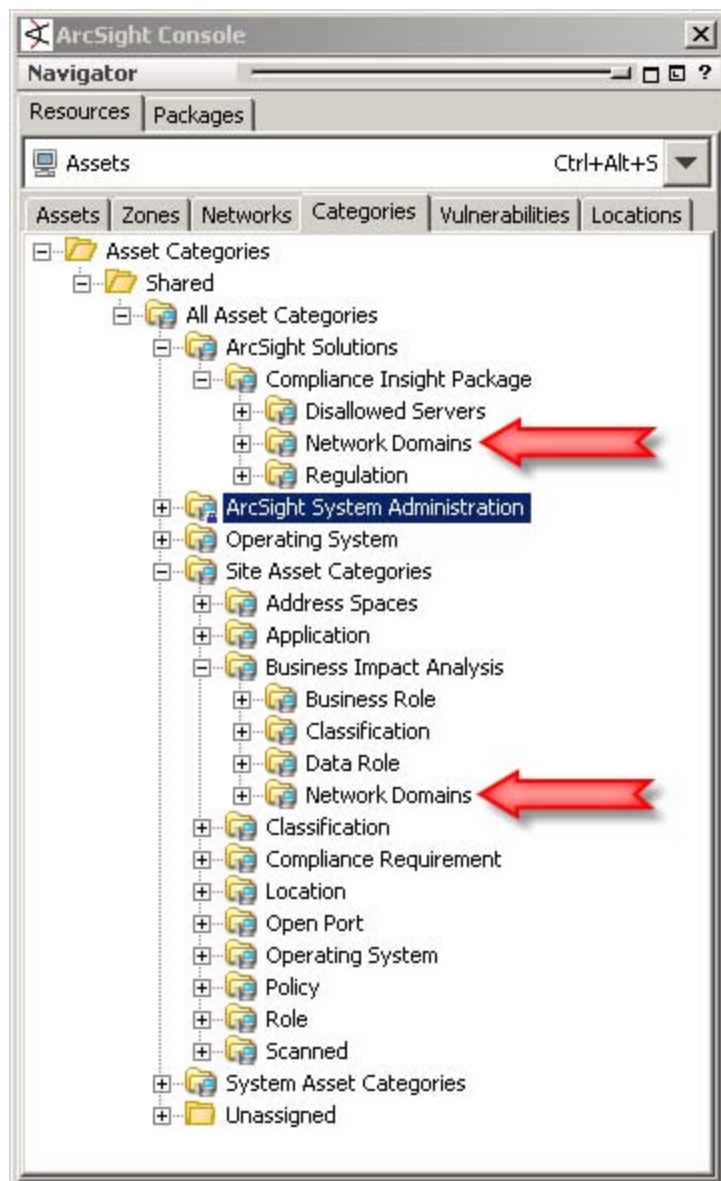
- Asset Categories ■
- Active Lists

Asset Categories

SOX4 contains seven new asset categories and some of the SOX2 asset categories were moved or deleted as summarized in the table below. If you have classified machines in one of the asset categories that has been deleted or moved, you will have to re-categorize those assets. For assets categorized in all the other SOX2 categories, no action is required; your assets will still be classified in those categories after the upgrade.

The main Sarbanes-Oxley asset category has not changed and assets that have already been categorized as Sarbanes-Oxley do not need to be re-categorized. For the complete list of asset categories that have not changed, see the following table.

The Networks Domains asset category is located in two locations and is linked. The following figure shows two locations of the Network Domains asset category.



Most of the SOX2 assets that have been categorized using the Network Domains asset categories do not need to be re-categorized. Since the two Network Domains assets categories are linked, if a SOX2 asset has been categorized, it is automatically categorized in the All Asset Categories/Compliance Insight Package/Network Domains asset category for SOX4.

Due to ESM 4.0 site asset categories resource changes, some SOX2 site asset categories are no longer used in SOX4. Some assets may need to be re-categorized.

The following new asset categories have been added to the Asset Categories/Shared/All Asset Categories/Compliance Insight Package asset category for SOX4: ■

- Disallowed Servers ■
- Disallowed Servers/AOL IM ■
- Disallowed Servers/ICQ

- Disallowed Servers/MSN IM ■
- Disallowed Servers/Yahoo IM ■
- Network Domains/Domain Controllers ■
- Network Domains/Legal

The table below shows how SOX2 asset categories map to the SOX4 asset categories and what action should be taken if you are upgrading from SOX2 to SOX4.

SOX2 Asset Category	SOX4 Asset Category	Action
After-Hours Sensitive	Not used in SOX4.	SOX2 assets categorized to this Asset category should be re-categorized.
Compliance Insight Package	Compliance Insight Package	None. SOX2 assets categorized to this asset category do not need be re-categorized.
Control Framework	Not used in SOX4.	SOX2 assets categorized to this Asset category should be re-categorized.
External	Not used in SOX4.	SOX2 assets categorized to this Asset category should be re-categorized.
ISO17799	Not used in SOX4.	SOX2 assets categorized to this Asset category should be re-categorized.
Network Visibility	Not used in SOX4.	SOX2 assets categorized to this Asset category should be re-categorized.
NIST 800-53	Not used in SOX4.	SOX2 assets categorized to this Asset category should be re-categorized.
Network Domains	Network Domains	None. SOX2 assets categorized to this asset category do not need be re-categorized. The Networks Domains asset category is located in two locations.
Regulation	Regulation	None. SOX2 assets categorized to this asset category do not need be re-categorized.
Sarbanes-Oxley	Sarbanes-Oxley	None. SOX2 assets categorized to this asset category do not need be re-categorized.

Commerce	Commerce	None. SOX2 assets categorized to this asset category do not need be re-categorized. The existing SOX2 asset category has been linked to the following new asset category location: Compliance Insight Package/Network Domains.
Development	Development	
Electronic PHI	Electronic PHI	
Email	Email	
Financial	Financial	
Partner	Partner	
Private	Private	
Processing	Processing	
Production	Production	
Public Facing	Public Facing	
Remote	Remote	
Third Parties	Third Parties	
Wireless	Wireless	

Active Lists

SOX4 uses one active list from the SOX2 release:

Administrative Accounts

This active list has been linked from the Site Active Lists group into the /All Active Lists/ArcSight Solutions/Compliance Insight Package group, so it can be more easily identified as part of the Compliance Insight Package infrastructure.

When loading the SOX4 solution, the existing active list will be linked to the new location and all the entries you have made prior will be retained.

Active Lists that Require Configuration

Active List	Description	Expected Input Per Entry
Active Directory Domains	This active list contains all the AD domains. This list is used on different scenarios like detecting when user account is deleted, enabled, disabled or special privileged assigned to a new log on, domains should be provided on lowercase.	Active Directory Domain (lowercase)

Administrative Accounts	<p>This active list should be populated with the usernames that have administrative privileges in your domain. Admins (those responsible for managing administrative users) populate this list manually whenever a new administrative user is added. Entries to this list are read by reports supplied in the content pack, but the list can also be added to or referenced in new content built around the provided infrastructure.</p> <p>This active list should be populated with the usernames that have administrative privileges in your domain. Entries in this list should be in all lower case. For example, the user Administrator should be added as "administrator".</p>	User name (lowercase)
Allowed Ports	<p>This active list contains all permissible destination ports (all permissible services). This active list should be populated according to your site policy.</p> <p>By default, all connection types and ports are allowed. To be considered a disallowed port, the connection type and port number must either be specified explicitly in the Disallowed Ports active list, or not specified in the Allowed Ports active list. If all ports are specified in the Allowed Ports active list (using the * character), the policy allows all ports (except those specified explicitly in the Disallowed Ports active list). Explicit (that is, not *) port entries in the Disallowed Ports active list always take precedence over entries in the Allowed Ports active list.</p>	Connection type and port number where Connection type could be: Inbound, outbound or internal
Badges to Accounts	<p>This list contains the computer account and employee type for every physical device badge.</p> <p>Populate this active list with the badge ID, primary computer account for the badge holder (in case it's a visitor use the visitor user name), and the employee type for users in your organization (in lowercase). Specifically, ensure that contractors and visitors are identified with the word "Contractor", "Visitor" (case insensitive) in the employee type field.</p>	<p>Badge ID, primary computer account for the badge holder (in case it's a visitor use the visitor user name), the employee type (lowercase).</p> <p>Specifically, ensure that Contractors and visitors are identified with the word "Contractor" "Visitor" (case insensitive) in the employee type field.</p>
Competitors	<p>This list stores competitor email domains on lower case, for example if the user email format of your competitor is jsmith@example.com then the email domain in this example is "example.com" (what goes after the @ in lowercase).</p>	Competitor email domains (lowercase)
Default Vendor Accounts	<p>This active list contains the default user account names for various vendors. This list should be configured at set-up time with existing vendor user account names, and updated as necessary on an ongoing basis.</p>	Default user account and vendor name (lowercase)

Disallowed Ports	<p>This active list contains all disallowed destination ports. This active list should be populated according to your site's policy.</p> <p>By default, all connection types and ports are allowed.</p> <p>To be considered a disallowed port, the connection type and port number must either be specified explicitly in the Disallowed Ports active list, or not specified in the Allowed Ports active list. If all ports are specified in the Allowed Ports active list (using the *character), the policy allows all ports (except those specified explicitly in the Disallowed Ports active list).</p> <p>Explicit (that is, not *) port entries in the Disallowed Ports active list always take precedence over entries in the Allowed Ports active list.</p>	<p>Connection type and port number where Connection type could be: inbound, outbound or internal</p>
DMZ Assets	<p>This List should contain DMZ assets on the organization like DNS, WEB, SMTP servers.</p> <p>It contains 2 fields: IPAddres and AssetType where the IPAddress is the IP Address of the asset and the AssetType is the type of the asset on lower case (by default supported 3 types dns,web,smtp) for example if your web server ip is x.y.z.w you should add it as:</p> <p>IPAddress=x.y.z.w ,AssetType=web</p>	<p>IP Address of authorized DNS,WEB, SMTP servers on your organization,</p> <p>Asset Type one of the following dns, web, smtp on lower case.</p>
Former Employees	<p>This active list contains user accounts of former employees. User accounts in this active list are retained indefinitely. All the entries in this list need to be in lowercase.</p>	<p>This list populated by the rule "Former Employee Account Detected," if this rule is disabled and not deployed this list should be maintained on regular basis and username should be provided on lowercase.</p>
Important Emails	<p>This list stores important emails of high-profile targets on the organization like C-level executives which could be targeted by spear phishing attacks.</p> <p>Entries in this list should be in all lower case.</p>	<p>Email and UserName (lowercase)</p>
Insecure Ports	<p>This active list includes ports related to unencrypted and thus insecure communication services.</p>	<p>Port Number</p>
Insecure Processes	<p>This active list includes the names of processes that provide unencrypted and thus insecure communications.</p>	<p>Process name (lowercase)</p>
Internet Ports	<p>This active list includes ports that are used for monitoring internet (Web traffic) communication. By default, it includes ports 80 and 443.</p>	<p>Port Number</p>

Meltdown and Spectre Signatures	This active list contains Meltdown and Spectre vulnerabilities signatures.	This list should be maintained on a regular basis.
Mobile Code Detection Signatures	This active list contains a list of mobile code detection signatures.	This list should be maintained on a regular basis.
Monitored Accounts	This active list is used to maintain user accounts to be monitored.	Username (lowercase)
Monitored FISMA Reports	<p>This active list is updated when a monitored FISMA report is accessed.</p> <p>Before enabling and deploying those rules, pay attention to the following:</p> <ol style="list-style-type: none"> 1. FISMA Report Accessed 2. FISMA Report not Accessed more than "x" days <p>Make sure to populate this active list with the reports that you want to monitor. For example if you want to monitor this report:</p> <p>/All Reports/Arcsight/Solution/FISMA/NIST 800-53/Access Control (AC)/AC- 7 - Unsuccessful Login Attempts/Unsuccessful User Logins</p> <p>Please add the following entries to the active list:</p> <p>Report : /All Reports/ArcSight Solutions/FISMA/NIST 800-53/Access Control (AC)/AC- 7 - Unsuccessful Login Attempts/Unsuccessful User Logins</p>	FISMA Report URI
Multi Factor Authentication Devices	This active list stores the multi- factor authentication devices. All the entries in this list must be in lowercase.	Device product, device vendor and device version (lowercase)
New Hire Accounts	This active list contains newly hired users and is automatically populated by the "New Hire Identification" rule. New users are retained for 7 days in the list.	User Name (lowercase). This list should be maintained on a regular basis.
Non Multi Factor Authentication Devices - Exception	This active list stores non multi- factor authentication devices which you want to exclude. All the entries in this list must be in lowercase.	Device product, device vendor and device version on Lower case
Test and Custom Accounts	This active list stores names of development, test, or custom application or user accounts. Populate this active list with additional custom accounts that should be disabled in a production environment. All the entries in this list must be in lowercase.	Account Name, in lowercase. This list should be maintained on a regular basis.

Unsecured Password Signatures	This active list contains unsecured password signatures.	This list should be maintained on a regular basis.
Users Authorized to Access High Impact Systems	This active list stores the usernames of the individuals who are authorized to access high impact systems. All the entries in this list must be in lowercase.	Username (lowercase)
VOIP Applications Detection Signatures	This active list contains a list of VOIP applications signatures.	This list should be maintained on a regular basis.

Upgrade and Configuration Instructions

SOX4 has no separate upgrade installer. To upgrade to SOX4, simply import the SOX4 package. To prepare for the import and configuration afterward, run through this preparation checklist.

Prepare for the installation

1. Back up existing SOX2 content
2. Import the SOX4 package. Follow instructions on page 28.
3. Configure the solution. Follow instructions on page 31.
4. If you have customized SOX2 resources, you may want to transfer the SOX2 customized resource configurations to SOX4:
 - Run a resource graph on the Sarbanes-Oxley 2.0 rules to see the filters that support it; make note of the 2.0 filters that support the 2.0 rules.
 - Transfer (move or copy) the Sarbanes-Oxley 2.0 rules into the Sarbanes Oxley 4.0 structure.
 - Transfer (move or copy) the Sarbanes-Oxley 2.0 filters that support the 2.0 rules into the Sarbanes Oxley 4.0 structure.
 - Once all that you wish to preserve from SOX2 is transferred to corresponding resources in SOX4, first back up, then delete the unused Sarbanes-Oxley 2.0 resources.

Configure Oracle Connector to Access Monitoring

The Identity Based Access Control use case controls the access to privileged database Oracle administration accounts. In order to implement this use case, the SOX4 solution needs to record when users are accessing Oracle accounts. In order to create this record, auditing for Oracle system activity needs to be enabled on the database. The solution provides scripts to perform these tasks.

Oracle Preparation

Before enabling these auditing levels, verify that the Oracle Database Audit SmartConnector is installed and configured according to the initial setup instructions in the Oracle Database Audit SmartConnector Configuration Guide. To enable these auditing processes, the SOX4 solution provides the following scripts as File resources.

Script	Description
oracleMoveAudit.sql	Create a unique tablespace for the audit table
oracleAuditing.sql	Configure the audit options
createTruncatePackage.sql	Create a truncate procedure in the database that truncates audit entries in the audit table. This procedure is scheduled by the scheduleTruncate.sql script to run at regular intervals.
scheduleTruncate.sql	Schedule the truncate procedure
oracleTruncateADM.sql	Immediately truncate the audit entries from the audit table

Note: It is strongly recommended that you execute the Oracle auditing scripts with the assistance of an Oracle DBA. These steps require sysdba permissions using sqlplus.

Download the Audit SQL Scripts

Repeat the following steps, to download all the audit SQL scripts listed in the preceding table:

1. From the Resources tab in the Navigator pane, go to Files and navigate to ArcSight Solutions/Sarbanes Oxley 4.0/oracle auditing folder.
2. Right-click on the sql script and select the Download option.
3. Browse for a directory location.
4. In the File name field, enter the name of the script and click Save.

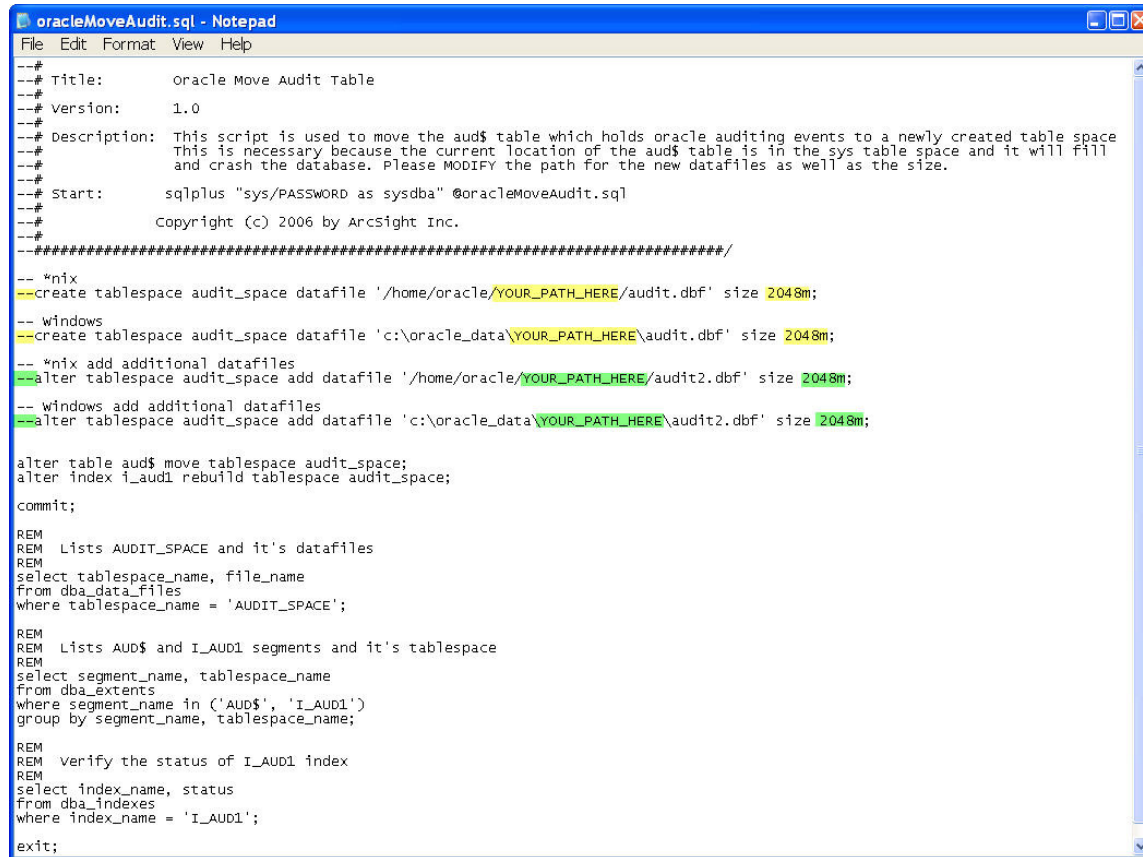
A copy of the file is saved to the local file system.

Create a Unique Tablespace for the Audit Table

The following process creates a separate tablespace just for auditing. Once, auditing is configured, audit events are logged whenever users access Oracle accounts. The SOX4 solution uses these audit tables to determine what users have attempted access to privileged database Oracle administration accounts. The Oracle audit table is stored in sys table space. Because Oracle generates a lot of audit messages, this fills up the audit table, which can cause the database to crash.

To avoid this problem, move the Oracle audit table into its own table space with its own data files separate from the core Oracle tables.

1. From a Windows command prompt, change to the directory location where sql scripts were downloaded.
2. Make a back up copy of the file oracleMoveAudit.sql.
3. In a text editor, open the original file oracleMoveAudit.sql and set the following values:



```

--#
--# Title:      oracle Move Audit Table
--#
--# Version:    1.0
--#
--# Description: This script is used to move the aud$ table which holds oracle auditing events to a newly created table space
--#              This is necessary because the current location of the aud$ table is in the sys table space and it will fill
--#              and crash the database. Please MODIFY the path for the new datafiles as well as the size.
--#
--# Start:      sqlplus "sys/PASSWORD as sysdba" @oracleMoveAudit.sql
--#
--#              Copyright (c) 2006 by ArcSight Inc.
--#
--#####/
-- *nix
--create tablespace audit_space datafile '/home/oracle/YOUR_PATH_HERE/audit.dbf' size 2048m;
-- windows
--create tablespace audit_space datafile 'c:\oracle_data\YOUR_PATH_HERE\audit.dbf' size 2048m;
-- *nix add additional datafiles
--alter tablespace audit_space add datafile '/home/oracle/YOUR_PATH_HERE/audit2.dbf' size 2048m;
-- windows add additional datafiles
--alter tablespace audit_space add datafile 'c:\oracle_data\YOUR_PATH_HERE\audit2.dbf' size 2048m;

alter table aud$ move tablespace audit_space;
alter index i_aud1 rebuild tablespace audit_space;
commit;

REM
REM Lists AUDIT_SPACE and it's datafiles
REM
select tablespace_name, file_name
from dba_data_files
where tablespace_name = 'AUDIT_SPACE';

REM
REM Lists AUD$ and I_AUD1 segments and it's tablespace
REM
select segment_name, tablespace_name
from dba_extents
where segment_name in ('AUD$', 'I_AUD1')
group by segment_name, tablespace_name;

REM
REM Verify the status of I_AUD1 index
REM
select index_name, status
from dba_indexes
where index_name = 'I_AUD1';

exit;

```

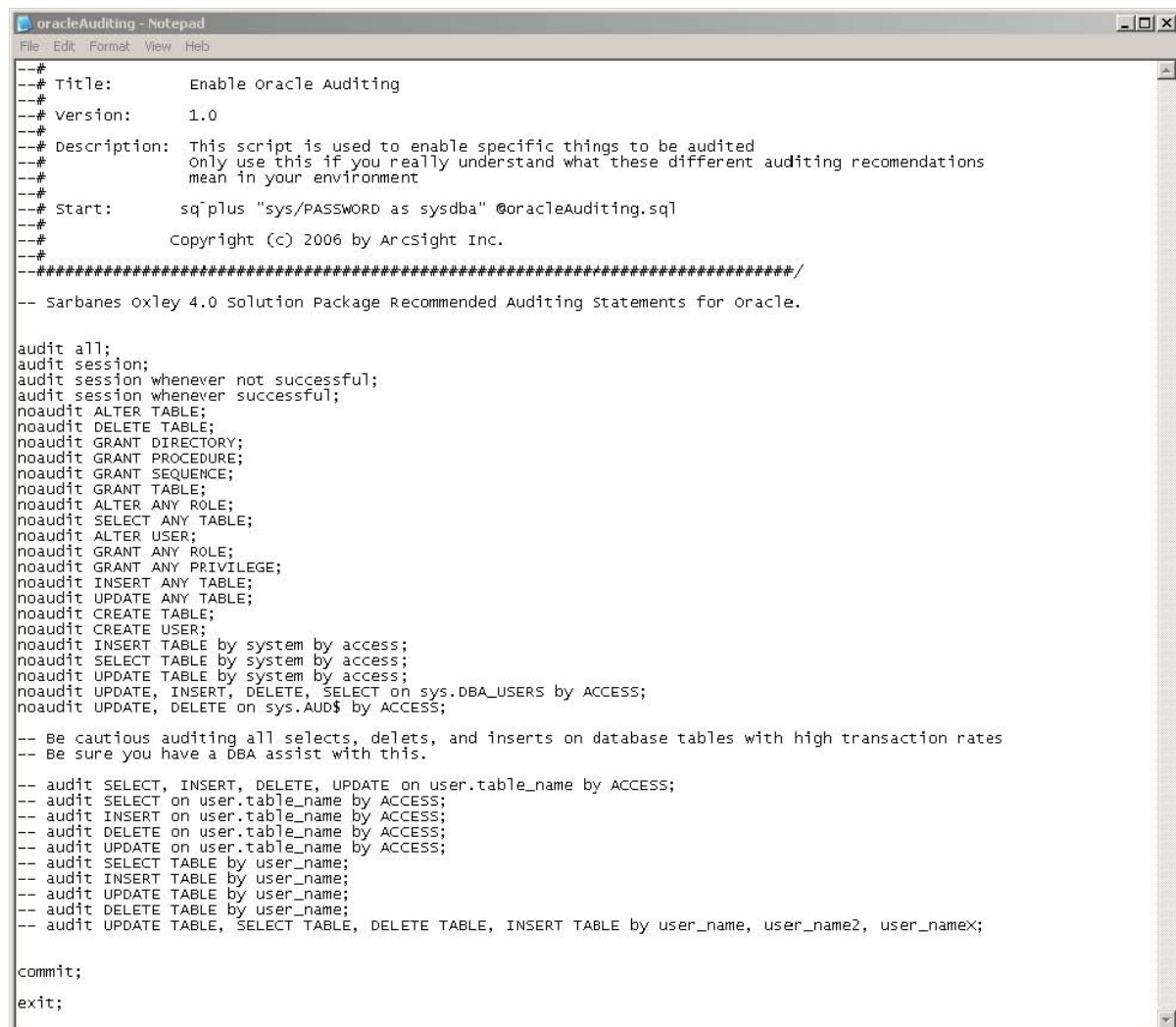
4. Configure the create tablespace line with the file path of where you want the Oracle audit.dbf file to be located:
5. Un-comment the “create tablespace” line that’s appropriate for your operating system by removing the two hyphens (--) as shown highlighted in yellow above.
6. Replace YOUR_PATH_HERE with the new path where you want your Oracle datafile to be located.
7. As an option, you can also change the default size of 2048m.
8. As an option, you can add additional data files if you want to extend the tablespace.
9. Un-comment the “alter tablespace” line that’s appropriate for your operating system by removing the two hyphens (--) as shown highlighted in green above.
10. Replace YOUR_PATH_HERE with the new path where you want your additional Oracle datafile to be located.
11. As an option, you can also change the default size of 2048m.
12. Save and close the file.

13. To run the script, at the command prompt, enter the following command: `sqlplus "sys/<your sys password> as sysdba" @oracleMoveAudit.sql`
14. The operation is successful when you see the table space name and audit space name displayed successfully.

Configure Audit Options

The next process tells Oracle the exact statements and actions to audit.

1. From a Windows command prompt, change to the directory location where sql scripts were downloaded.
2. Make a back up of the file `oracleAuditing.sql`
3. In a text editor, open the original `oracleAuditing.sql` and evaluate the default options and configure them so they are appropriate for your environment.



```

--#
--# Title:      Enable Oracle Auditing
--# Version:    1.0
--#
--# Description: This script is used to enable specific things to be audited
--#              Only use this if you really understand what these different auditing recommendations
--#              mean in your environment
--#
--# Start:      sqlplus "sys/PASSWORD as sysdba" @oracleAuditing.sql
--#
--#              Copyright (c) 2006 by Arcsight Inc.
--#
--#
--#####/
-- Sarbanes Oxley 4.0 Solution Package Recommended Auditing Statements for Oracle.

audit all;
audit session;
audit session whenever not successful;
audit session whenever successful;
noaudit ALTER TABLE;
noaudit DELETE TABLE;
noaudit GRANT DIRECTORY;
noaudit GRANT PROCEDURE;
noaudit GRANT SEQUENCE;
noaudit GRANT TABLE;
noaudit ALTER ANY ROLE;
noaudit SELECT ANY TABLE;
noaudit ALTER USER;
noaudit GRANT ANY ROLE;
noaudit GRANT ANY PRIVILEGE;
noaudit INSERT ANY TABLE;
noaudit UPDATE ANY TABLE;
noaudit CREATE TABLE;
noaudit CREATE USER;
noaudit INSERT TABLE by system by access;
noaudit SELECT TABLE by system by access;
noaudit UPDATE TABLE by system by access;
noaudit UPDATE, INSERT, DELETE, SELECT on sys.DBA_USERS by ACCESS;
noaudit UPDATE, DELETE on sys.AUD$ by ACCESS;

-- Be cautious auditing all selects, deletes, and inserts on database tables with high transaction rates
-- Be sure you have a DBA assist with this.

-- audit SELECT, INSERT, DELETE, UPDATE on user.table_name by ACCESS;
-- audit SELECT on user.table_name by ACCESS;
-- audit INSERT on user.table_name by ACCESS;
-- audit DELETE on user.table_name by ACCESS;
-- audit UPDATE on user.table_name by ACCESS;
-- audit SELECT TABLE by user_name;
-- audit INSERT TABLE by user_name;
-- audit UPDATE TABLE by user_name;
-- audit DELETE TABLE by user_name;
-- audit UPDATE TABLE, SELECT TABLE, DELETE TABLE, INSERT TABLE by user_name, user_name2, user_name3;

commit;
exit;

```

4. Configure the recommended auditing statements. By default, all the recommended auditing statements for the SOX4 solution are enabled. To disable any that you do not want to audit,

comment them out by adding two hyphens to the beginning of the line, as shown above.

Caution: DO NOT audit things that are accessed regularly by automated accounts. These automated actions will flood the audit logs.

5. Save and close the file.
6. To verify that the settings you made are correct, test them on a non-production system. For example, log in as one of the users you want to audit, do the action you want to audit, and see if the action appears in the audit log.
7. Run the script at command prompt by typing: `Sqlplus "sys/<your password here> as sysdba" @oracleAuditing.sql`
8. The operation is successful when you see the message: `Audit succeeded.`

Truncate Oracle Audit Logs

After auditing is enabled for some time, the security administrator may want to delete records from the database audit trail, both to free audit trail space and to facilitate audit trail management.

To accomplish this optional housekeeping feature, the SOX4 solution package contains the following scripts:

- `oracleTruncateADM.sql` – Invoking this script immediately truncates the audit entries from the audit table
- `createTruncatePackage.sql` – Invoking this script creates a truncate procedure in the database that truncates audit entries in the audit table. This procedure is scheduled by the `scheduleTurncate.sql` script to run at regular intervals.
- `scheduleTruncate.sql` – Invoking this script schedules the truncate procedure created in the `createTruncatePackage.sql` script to run at regular intervals.

Caution: This step deletes items from the audit table. Although ArcSight maintains a record of all events for the configured retention period, if you must maintain records of every transaction for auditors, you should probably not do this step.

Note: Only the user SYS, a user who has the DELETE ANY TABLE privilege, or a user to whom SYS has granted DELETE privilege on SYS.AUD\$ can delete records from the database audit trail.

Create Truncate Package

This script creates a truncate procedure, which tells the database the truncate the aud\$ table.

1. From a Windows command prompt, change to the directory location where sql scripts were downloaded.

2. At the command prompt, type: `sqlplus "sys/<your password here> as sysdba"`
`@createTruncatePackage.sql` For example, if your sysdba password is mypassword, type
`Sqlplus "sys/mypassword as sysdba" @createTruncatePackage.sql`
3. The operation is successful when you see the message: Procedure created.

Schedule Truncate Procedure

This script schedules the truncate procedure that we created in the previous step. By default, the procedure is scheduled to run at 2:00 a.m. local system time.

1. At command prompt, type `Sqlplus "sys/<your password here> as sysdba"`
`@scheduleTruncate.sql` Once the schedule script has been run, the db should be checked to ensure that the `job_queue_processes` parameter is set correctly to run scheduled jobs.
2. At a command prompt, type: `sqlplus "sys as sysdba"`
3. Next, run: `show parameter job`
4. The output will look like this. The number at the end indicates the job queue process setting.

NAME	TYPE	VALUE
-----	-----	-----
<code>job_queue_processes</code>	<code>integer</code>	<code>0</code>

5. If the job queue process setting is 0, it means that it has no queue processes, and no jobs will run. If this is the case, then run the following (this should be done by an Oracle DBA): `alter system set job_queue_processes=2; create pfile from spfile;` This sets the job queue processes to 2.

Back up and Uninstall the SOX4 Solution Package

This section provides instructions for back up and uninstall of the SOX4 solution package. This section is not part of the initial configuration and is provided if you want to uninstall the SOX4 solution package at a later date.

Back Up the Solution Package


If you have made changes to the resources, you may want to back up the solution content before an uninstall of the SOX4 solution package. You can back up the solution content to a package bundle file that ends in the `.arb` extension as described below.

The back up process should be done:

- From the ArcSight Console
- Using the ArcSight Administrator login

- With the ArcSight Manager running

To back up the SOX4 solution package:

1. Log into the ArcSight Console as ArcSight Administrator.
2. In the Packages tab of the Navigator panel, navigate to ArcSight Solutions/Sarbanes-Oxley 4.0.
3. Right-click on the Sarbanes-Oxley package bundle () and select **Export Package to Bundle**.
4. The **Package Bundle Export** dialog box displays.
5. In the **Package Bundle Export** dialog box, you can optionally browse for a directory location and change the default file name and click **Next**.
6. The **Progress** tab of the **Export Packages** dialog box displays the progress of the export. When the export is finished, click **OK**.
7. The SOX4 solution package is saved into the package bundle file that ends with the .arb extension. You can restore the contents of this package at a later time by importing this package bundle file.


Uninstall the Solution Package

Uninstall and delete the SOX4 solution package bundle using the Packages tab of the Navigator pane as described in the process below.

The uninstall process should be done:

- From the ArcSight Console
- Using the ArcSight Administrator login
- With the ArcSight Manager running

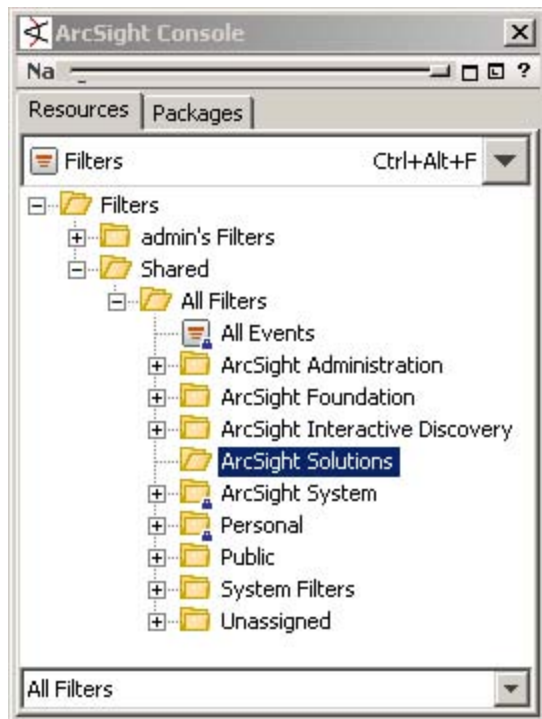
To uninstall and delete the SOX4 package:

1. Log into the ArcSight Console as ArcSight Administrator.
2. Click on the Packages tab in the Navigator panel.
3. In the Packages tab of the Navigator panel, navigate to ArcSight Solutions/Sarbanes-Oxley 4.0.
4. Right-click on the Sarbanes-Oxley package bundle () and select Uninstall Package.
5. In the Uninstall Package dialog box, click OK.
6. The progress of the uninstall displays in the Progress tab of the Uninstalling Packages dialog box. When the uninstall is finished, click OK.
7. Right-click on the Sarbanes-Oxley 4.0 package bundle and select Delete Package.

Verify Successful Uninstall

To verify that uninstall was successful:

1. Open an ArcSight Console that is attached to the Manager from which you uninstalled the Compliance Insight Package.
2. In the Navigator panel, select the **Resources** tab, go to Filters, and click the ArcSight Solutions folder. If you have no other ArcSight solutions installed, the ArcSight Solutions folder should be present, but empty.



Chapter 4: ISO Sections for Sarbanes-Oxley

The following topics are covered here:

- ["ISO 4: Risk Assessment and Treatment" below](#)
- ["ISO 5: Security Policy" on page 100](#)
- ["ISO 6: Organization of Information Security" on page 102](#)
- ["ISO 7: Asset Management" on page 111](#)
- ["ISO 8: Human Resources" on page 116](#)
- ["ISO 9: Physical and Environmental Security" on page 120](#)
- ["ISO 10: Communications and Operations Management" on page 124](#)
- ["ISO 11: Access Control" on page 145](#)
- ["ISO 12: Information System Acquisition Development and Maintenance" on page 164](#)
- ["ISO 13: Information Security Incident Management" on page 170](#)
- ["ISO 14: Business Continuity Management" on page 175](#)
- ["ISO 15: Asset Management" on page 178](#)

ISO 4: Risk Assessment and Treatment

Section 4 of ISO addresses the ability to understand and assess the risk to the information system assets. ArcSight's approach entails prioritizing risk and providing information about the higher threats and risks.

Use Cases

To address section 4 requirements, the SOX4 (SOX4) solution provides the following use cases.

Security Overview

An important process in any risk assessment is to continuously identify risk sources. The resources in this chapter provide an overview of the major events identified by the solution pack and the system in general.

Filters, rules, dashboards and reports provide monitoring of the high risk events in the system as well as control of the solution pack's heartbeat and performance, thus ensuring that the evaluation process is continuous.

High-Risk Event Analysis

Some resources are specifically designed to identify the critical events on a system. These events, such as hosts that have been compromised or high priority events, are displayed in dashboards and reports.

Devices

The following devices supply the events that apply to ISO section 4.

Section 4 Use Case	Device	Device Configuration Required
Security overview	NIDS/NIPS	None
High-risk event analysis	HIDS/HIPS	None

Section 4 Resources

This section lists all the resources that address the information systems acquisition development and maintenance requirements of ISO section 4.

Section 4 Active Channels

Active Channel	Description
High-risk	This active channel shows high priority events which translate into high risk.

Section 4 Dashboards

Dashboard	Description
Most Fired Rule by Section	This dashboard shows a bar chart for every ISO section in the solution that indicates the top triggered rule for each section.
Overall ISO Rule Firings	This dashboard shows a summary bar chart that provides statistics about the number of rules fired for each ISO section.
Risk - Geo View	Dashboard to show all risks posed by the way of reconnaissance and attack activity.
Risk Overview	Dashboard to show all attack related, rule-firing related activity along with a view of attacks to assets.

Section 4 Data Monitors

Data Monitor	Description
Attacks - GeoView	This dashboard shows a bar chart for every ISO section in the solution that indicates the top triggered rule for each section.
Attacks per Asset Category	This dashboard shows a summary bar chart that provides statistics about the number of rules fired for each ISO section.
Compromised Hosts	Dashboard to show all risks posed by the way of reconnaissance and attack activity.
Overall ISO Rule Firings	Dashboard to show all attack related, rule-firing related activity along with a view of attacks to assets.
Priority Distribution	This data monitor shows the distribution of priorities across all events.
Reconnaissance - GeoView	This data monitor shows all reconnaissance events on a world map.
Rule Firings	This event graphs shows all the rule firings along with the machines involved in them.
ISO 4 - Most fired rule	This Data Monitor shows the rule that fired most in ISO chapter 4 in the last hour.
ISO 5 - Most fired rule	This Data Monitor shows the rule that fired most in ISO chapter 5 in the last hour.
ISO 6 - Most fired rule	This Data Monitor shows the rule that fired most in ISO chapter 6 in the last hour.
ISO 7 - Most fired rule	This Data Monitor shows the rule that fired most in ISO chapter 7 in the last hour.
ISO 8 - Most fired rule	This Data Monitor shows the rule that fired most in ISO chapter 8 in the last hour.
ISO 9 - Most fired rule	This Data Monitor shows the rule that fired most in ISO chapter 9 in the last hour.
ISO 10 - Most fired rule	This Data Monitor shows the rule that fired most in ISO chapter 10 in the last hour.
ISO 11 - Most fired rule	This Data Monitor shows the rule that fired most in ISO chapter 11 in the last hour.
ISO 12 - Most fired rule	This Data Monitor shows the rule that fired most in ISO chapter 12 in the last hour.
ISO 13 - Most fired rule	This Data Monitor shows the rule that fired most in ISO chapter 13 in the last hour.
ISO 14 - Most fired rule	This Data Monitor shows the rule that fired most in ISO chapter 14 in the last hour.
ISO 15 - Most fired rule	This Data Monitor shows the rule that fired most in ISO chapter 15 in the last hour.

Section 4 Filters

Filter	Description
Attacks	This filter looks for all attack events.
Attacks - Public Addresses	Filter to select attack events involving public addresses.
Compromises	This filter looks for generic compromises.
Reconnaissance - Public Addresses	This filter looks for reconnaissance events from nonprivate addresses to filter out the NULL coordinates.
Rule Firings	This filter looks for all the rule firings of the SOX4 solution.

Section 4 Rules

Rule	Description	Config?
Severely Attacked System	This rule looks for an accumulation in attacks targeting a single machine.	Optional: Tune the threshold.

Section 4 Reports

Report	Description
High Risk Events	This report shows high risk events.

Section 4 Queries

Section	Query	Description
4	High Risk Events	This query shows high risk events.

Section 4 Trends

Trend	Description
High Risk Events	A trend collection to gather high risk events on a daily basis.
High Risk Events - Executive Report	This report shows high risk events to be used by the executive report with reduced number of event fields.

ISO 5: Security Policy

Section 5 of ISO addresses controls used to enforce security policies. Areas of interest include reviewing and monitoring policy violations and vulnerabilities exposed on assets. The reports and dashboards in this section can be used to build out your security policy by getting an insight into the organization's current operations and verifying the security policy or identifying gaps where the policies need to be extended.

Use Cases

To address section 5 requirements, the SOX4 solution provides the following use cases.

- Policy violations
- Introduction of new services, as well as hosts

Devices

The following devices supply the events that apply to ISO section 5.

Section 5 Use Case	Device	Device Configuration Required
Policy Violations	NIDS/NIPS HIDS/HIPS ILP Configuration Management	Configure each device to comply with your company's policies.
Introduction of new services and hosts	NBAD	Ensure the right networks are monitored and the capabilities are turned on.

Section 5 Resources

This section lists all the resources that address the information systems acquisition development and maintenance requirements of ISO section 5.

Section 5 Active Channels

Active Channel	Description
New Hosts and Services	This active channel shows events related to new services and new hosts found on the network.

Policy Breaches	This active channel looks for policy violations in the past.
-----------------	--

Section 5 Dashboards

Dashboard	Description
New Hosts and Services	Dashboard to show new hosts and services as they are detected
Policy Breaches	Dashboard to show top 10 policy violators.

Section 5 Data Monitors

Section	Data Monitor	Description
5.1.2	New Hosts	This data monitor shows new hosts that were detected on the network.
5.1.2	New Services	This data monitor shows new services that were detected on the network.
5.1.2	Top 10 Policy Violations	This data monitor shows the top 10 policy breach events.
5.1.2	Top 10 Policy Violators	This data monitor shows the top 10 policy violators.

Section 5 Filters

Section	Filter	Description
5.1.2	New Host Detected	Filter to select events where a new host was detected by an IDS.
5.1.2	New Service Detected	Filter to select events where a new service was detected by an IDS.
5.1.2	Vulnerabilities	This filter looks for events which have a vulnerability field populated.

Section 5 Rules

Section	Rule	Description
5.1.2	New Host Detected	This rule triggers when new hosts are found on the network.
5.1.2	New Service Detected	This rule fires when new services are found on machines.

Section 5 Reports

Section	Report	Description
5.1.2	Machines Conducting Policy Breaches	This report shows machines which were involved in policy breaches.

5.1.2	New Hosts	This report shows new hosts which were detected on the network.
5.1.2	New Services	This report shows the new services discovered on the network.
5.1.2	Top 20 Policy Breach Events	This report shows the top 20 policy breach events.

Section 5 Queries

Section	Query	Description
5.1.2	New Hosts	This query shows new hosts which were detected on the network.
5.1.2	New Services	This query shows the new services discovered on the network.
5.1.2	Top 20 Policy Breach Events	This query shows the top 20 policy breach events.
5.1.2	Machines Conducting Policy Breaches	This query shows machines which were involved in policy breaches.

Section 5 Trends

Section	Trend	Description
5.1.2	Machines Conducting Policy Breaches	Trend to capture and report on events where machines were involved in policy breaches.

ISO 6: Organization of Information Security

ISO Section 6 is concerned with managing information security within an organization. The SOX4 solution helps to communicate specific data about the organization's security posture to guide the implementation of security programs and policies.

This section is also concerned with third party contracts and security. To support the verification of third-party security controls, this section implements reporting and monitoring of third-party devices.

Use Cases

To address section 6 requirements, the SOX4 solution provides the following use cases.

Case Reporting

A management framework should be established to initiate and control the implementation of information security within the organization; Information security activities should be coordinated by representatives from different parts of the organization with relevant roles and job functions in order to ensure that security activities are executed in compliance with the information security policy.

The SOX4 solution addresses these requirements by implementing case reporting. Reports are built around security activities tracked in cases within ArcSight ESM.

Third-Party Activity

The security of the organization's information and information processing facilities that are accessed or communicated to by external parties must be maintained.

The SOX4 solution addresses this requirement with the use of dashboards and reports that show third party activity. These resources rely on categorization of third party assets into the /All Asset Categories/Site Asset Categories/Address Spaces/Protected/External/Third Party asset category.

Devices

The case management part of this section does not require any specific device feeds. Every rule can be configured to generate a case, which means that every device has a potential to report into this use-case.

Use Case	Devices	Device Configuration Required
Reporting around cases	N/A	See "Configure Cases " for a description of the Sarbanes-Oxley case management structure and how to configure it.
Third-party monitoring	NIDS/NIPS Firewall NBAD	None

Configuration

To activate the content that addresses this section, classify assets of third-party providers in the Third Party asset category (All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/ThirdParty).

Section 6 Resources

This section lists all the resources that address the information systems acquisition development and maintenance requirements of ISO section 6.

Section 6 Active Channels

Active Channel	Description
Attacks or Suspicious Activity - Third Party Systems	This active channel shows attacks or suspicious activity coming from third party systems.

Section 6 Dashboards

Section	Dashboard	Description
6.2.1	Third-Party Activity	Dashboard to show tabulated views of last 10 attacks and suspicious activity to, and from, third-party network segments.
6.2.1	Third-Party Activity - Event Graphs	Dashboard to show a graph view of attacks and suspicious activity to, and from. Thirdparty network segments.

Section 6 Data Monitors

Section	Data Monitor	Description
6.2.1	Attacks and Suspicious Activity from Third-Party Assets (Target Port)	This data monitor provides a breakdown of events from assets categorized in the Third- Party Network Domain broken down by target port.
6.2.1	Attacks and Suspicious Activity Targeting Third- Party Assets (Target Port)	This data monitor provides a breakdown of events that target assets categorized in the Third-Party Network Domain broken down by target port.
6.2.1	Last 10 Attacks and Suspicious Activity from Third-Party Assets	This data monitor provides a list of the last 10 events from assets categorized in the Third-Party Network Domain.
6.2.1	Last 10 Attacks and Suspicious Activity Targeting Third-Party Assets	This data monitor provides a list of the last 10 events that target assets categorized in the Third-Party Network Domain.

Section 6 Filters

Section	Filter	Description
6.2.1	Attacks and Suspicious Activity From Third-Party Assets	This filter identifies events of interest generated by assets categorized in the Third-Party Network Domain.
6.2.1	Attacks and Suspicious Activity Targeting Third- Party Assets	This filter identifies events of interest that target assets categorized in the Third-Party Network Domain.

Section 6 Rules

Section	Rule	Description
6.2.1	Attack from Third-Party System	This rule looks for attacks from third-party systems.

Section 6 Reports

Section	Report	Description
6.1.1	Executive Summary - Case Metrics	
6.1.2	Average Time to Resolution - By Case Severity	This report will show the Average Time to Resolution by Case Severity. It should be run once a week and reported to management.
6.1.2	Average Time to Resolution - By Day	This report will show the Average Time to Resolution by Day, for all cases closed on the day it is run. This report should be run once a week and reported to management.
6.1.2	Average Time to Resolution - By User	This report will show how long it is taking individuals to close their cases. This report should be run once a week and reported to management.
6.1.2	Case Chart	This report provides a graphic overview of current cases.
6.1.2	Case Stage Counts	This report provides an overview of the cases in their current stages.
6.1.2	Case Status by Owner	This report provides a breakdown by owner of all cases.
6.1.2	Max Time to Resolution - By User	This report will show the maximum time it takes users to close their cases. This report should be run once a week and reported to management.
6.1.2	Open Cases	This report shows all currently open cases.
6.1.3	Asset Identification Report	This report shows all assets and their respective network domain.
6.2.1	Administrative Logins and Logouts Targeting Third- Party Assets	This report provides a listing of administrative logins and logouts targeting assets categorized as Third-Party.
6.2.1	Administrative Logins and Logouts from Third-Party Assets	This report provides a listing of administrative logins and logouts coming from assets categorized as Third-Party.
6.2.1	Assets Available to Third Parties by Domain	This report shows the assets that are available to third parties as defined by the assets available to 3rd parties asset category. This report is organized by network domain.
6.2.1	Assets Available to Third- Parties by Criticality	This report shows the assets that are available to third parties as defined by the assets available to 3rd parties asset category. This report is organized by asset criticality.
6.2.1	Policy Violations from Third-Party Assets	This report provides a listing of events categorized by ArcSight as policy violations coming from assets categorized as Third- Party.

6.2.1	Third-Party - Sourced Attacks	This report provides a listing of hostile and suspicious events coming from Third-Party categorized Assets.
6.2.1	Third-Party - Targeting Attacks	This report provides a listing of hostile and suspicious events coming targeting Third-Party categorized Assets.
6.2.1	Third-Party Access	This report will show all access attempts to assets by third parties.
6.2.1	Third-Party Incidents - Closed Cases	This report shows all cases involving third party systems that have been closed.
6.2.1	Third-Party Incidents - Open Cases	This report shows all cases involving third party systems that are still open.
6.2.1	Unsuccessful Administrative Logins from Third-Party Assets	This report provides a listing of unsuccessful administrative login attempts coming from assets categorized as Third-Party.
6.2.1	Unsuccessful Administrative Logins to Third-Party Assets	This report provides a listing of unsuccessful administrative login attempts which target assets categorized as Third-Party.
6.2.1	Unsuccessful User Logins from Third-Party Assets	This report provides a listing of unsuccessful user login attempts coming from assets categorized as Third-Party.
6.2.1	Unsuccessful User Logins to Third-Party Assets	This report provides a listing of unsuccessful user login attempts which target assets categorized as Third-Party.
6.2.1	User Logins and Logouts from Third-Party Assets	This report provides a listing of user logins and logouts coming from assets categorized as Third-Party.
6.2.1	User Logins and Logouts to Third-Party Assets	This report provides a listing of administrative logins and logouts which target assets categorized as Third-Party.
6.2.2	Compromised Assets Available to Third Parties	This report shows all assets that may have been compromised that are available to third parties.
6.2.2	File Creations on Third- Party Accessible Systems	This report shows all file creations on assets accessible to 3rd parties.
6.2.2	File Deletions on Third- Party Accessible Systems	This report shows all file deletions on assets accessible to 3rd parties.
6.2.2	File Modifications on Third-Party Accessible Systems	This report shows all file modifications on assets accessible to 3rd parties.
6.2.2	File Related Activity on Third-Party Accessible Systems	This report shows all file activity on assets accessible to 3rd parties.
6.2.2	Services Accessed by Third-Parties	This report shows the ports/services that are being accessed by 3rd parties and the firewall that is passing the traffic.

6.2.2	Services on Assets Available to Third Parties	This report shows the open ports/services on vulnerable assets that are available to 3rd parties.		
6.2.2	Vulnerable Assets Available to Third Parties by Criticality	This report shows the vulnerabilities, sorted by criticality, on systems that are accessible to 3rd parties.		
6.2.2	Vulnerable Assets Available to Third Parties by Domain	This report shows the vulnerabilities, sorted by domain, on systems that are accessible to 3rd parties.		

Section 6 Queries

Section	Report	Description
6.1.2	Average Time to Resolution - By Day	This query will show the Average Time to Resolution by Day, for all cases closed on the day it is run. This query should be run once a
6.1.2	Average Time to Resolution - By User	This query will show how long it is taking individuals to close their cases. This query should be run once a week and Queried to management.
6.1.2	Max Time to Resolution - By User	This query will show the maximum time it takes users to close their cases. This query should be run once a week and Queried to management.
6.1.2	Open Cases	This query shows all currently open cases.
6.1.2	Average Time to Resolution - By Case Severity	This query will show the Average Time to Resolution by Case Severity. It should be run once a week and Queried to management.
6.1.2	Case Stage Counts	This query provides an overview of the cases in their current stages.
6.1.2	Case Stage Counts	This query provides an overview of the cases in their current stages.
6.1.3	Asset Identification Query	This query shows all assets and their respective network domain.
6.2.1	Unsuccessful Administrative Logins from Third- Party Assets	This query provides a listing of unsuccessful administrative login attempts coming from assets categorized as Third-Party.
6.2.1	Administrative Logins and Logouts Targeting Third-Party Assets	This query provides a listing of administrative logins and logouts targeting assets categorized as Third-Party.
6.2.1	Assets Available to Third Parties by Domain	This query shows the assets that are available to third parties as defined by the assets available to 3rd parties asset category. This query is organized by network domain.
6.2.1	Assets Available to Third-Parties by Criticality	This query shows the assets that are available to third parties as defined by the assets available to 3rd parties asset category. This query is organized by asset criticality.
6.2.1	Third-Party - Targeting Attacks	This query provides a listing of hostile and suspicious events coming targeting Third-Party categorized Assets.
6.2.1	Third-Party Access	This query will show all access attempts to assets by third parties.

6.2.1	Third-Party Incidents - Closed Cases	This query shows all cases involving third party systems that have been closed.
6.2.1	Third-Party Incidents - Open Cases	This query shows all cases involving third party systems that are still open.
6.2.1	Unsuccessful Administrative Logins to Third- Party Assets	This query provides a listing of unsuccessful administrative login attempts which target assets categorized as Third-Party.
6.2.1	Unsuccessful User Logins from Third- Party Assets	This query provides a listing of unsuccessful user login attempts coming from assets categorized as Third-Party.
6.2.1	Unsuccessful User Logins to Third- Party Assets	This query provides a listing of unsuccessful user login attempts which target assets categorized as Third-Party.
6.2.1	User Logins and Logouts from Third- Party Assets	This query provides a listing of user logins and logouts coming from assets categorized as Third-Party.
6.2.1	User Logins and Logouts to Third- Party Assets	This query provides a listing of administrative logins and logouts which target assets categorized as Third-Party.
6.2.1	Administrative Logins and Logouts from Third-Party Assets	This query provides a listing of administrative logins and logouts coming from assets categorized as Third-Party.
6.2.1	Policy Violations from Third-Party Assets	This query provides a listing of events categorized by ArcSight as policy violations coming from assets categorized as Third-Party.
6.2.1	Third-Party - Sourced Attacks	This query provides a listing of hostile and suspicious events coming from Third-Party categorized Assets.
6.2.2	File Creations on Third-Party Accessible Systems	This query shows all file creations on assets accessible to 3rd parties.
6.2.2	File Deletions on Third-Party Accessible Systems	This query shows all file deletions on assets accessible to 3rd parties.
6.2.2	File Modifications on Third-Party Accessible Systems	This query shows all file modifications on assets accessible to 3rd parties.
6.2.2	File Related Activity on Third-Party Accessible Systems	This query shows all file activity on assets accessible to 3rd parties.
6.2.2	Services Accessed by Third-Parties	This query shows the ports/services that are being accessed by 3rd parties and the firewall that is passing the traffic.
6.2.2	Services on Assets Available to Third Parties	This query shows the open ports/services on vulnerable assets that are available to 3rd parties.
6.2.2	Compromised Assets Available to Third Parties	This query shows all assets that may have been compromised that are available to third parties.
6.2.2	Vulnerable Assets Available to Third Parties by Criticality	This query shows the vulnerabilities, sorted by criticality, on systems that are accessible to 3rd parties.
6.2.2	Vulnerable Assets Available to Third Parties by Domain	This query shows the vulnerabilities, sorted by domain, on systems that are accessible to 3rd parties.

Section 6 Trends

Section	Trends	Description
6.2.1	Administrative Logins and Logouts from Third-Party Assets	Trend to capture and report on administrative logins and logouts from third-party assets type events.
6.2.1	Policy Violations from Third-Party Assets	Trend to capture and report on policy violations from third-party assets type events.
6.2.1	Third-Party - Sourced Attacks	Trend to capture and report on attacks originating from end points in the third- party network segments.
6.2.1	Unsuccessful Administrative Logins from Third-Party Assets	Trend to capture and report on events of the type 'unsuccessful administrative logins from third-party assets'
6.2.2	Compromised Assets Available to Third Parties	Trend to capture events and report on all assets that may have been compromised that are available to third parties.
6.2.2	Vulnerable Assets Available to Third Parties by Criticality	Trend to capture and report on events where vulnerable assets are accessible to third-parties, sorted by criticality.
6.2.2	Vulnerable Assets Available to Third Parties by Domain	Trend to capture and report vulnerable assets that are available to third-parties, sorted by domain.

ISO 7: Asset Management

ISO section 7 is concerned with a sound asset management policy and infrastructure to support it. This includes the protection of assets and assignment of ownership. This section also addresses details about information protection and classification.

Use Cases

To address section 7 requirements, the SOX4 solution provides the following use cases.

Asset Inventory Reporting

Controls must be in place to implement asset inventories and ownership. The SOX4 solution provides a series of Asset Management reports that address asset creation, modification, and deletion. These reports also indicate asset criticality to assist in the organization's asset management policy.

Data Classification Reporting and Real Time Monitoring

Data and assets must be classified in order to ensure that information receives the appropriate level of protection. The SOX4 solution uses reports on classification of assets by network domain, and uses rules and filters to monitor communications between classified machines.

Devices

The following devices supply the events that apply to ISO section 7.

Use Case	Devices	Device Configuration Required
Asset inventory reporting	N/A	See “Configure Cases ” for a description of the Sarbanes- Oxley case management structure and how to configure it.
Data classification reporting and Real-time monitoring	Router NIDS/NIPS Firewall	Set up assets with classification levels. See “Model Assets (Assign Asset Categories)”.

Configuration

In addition to the asset modeling and configurations to the common resources described in “Configure the Sarbanes-Oxley 4 Solution”, the following resources should be configured as necessary to comply with your policies.

Resource Type	Resource Name	What to configure
Cases	N/A	Configure the Cases repository as necessary to reflect your security policies.
Asset Category	Classification categories	Assets bearing classified data should be configured with the /All Asset Categories/Site Asset Categories/Classification categories.

Section 7 Resources

This section lists all the resources that address the information systems acquisition development and maintenance requirements of ISO section 7.

Section 7 Active Channels

Active Channel	Description
Asset Creation Deletion and Modifications	This active channel shows events related to asset creations, asset deletions, and asset modifications. The channel can be used to keep track of the asset inventory.
Traffic to and from Classified Machines	This active channel shows all the network traffic going to or coming from machines which are categorized with the Site Asset Categories/Classification category.

Section 7 Dashboards

Section	Dashboard	Description
7.1	Asset Activity	Dashboard to show creation, deletion, and modification of assets.
7.2	Classification Level Traffic	Dashboard to show flow of traffic between various levels of higher and lower classification in both directions.

Section 7 Data Monitors

Section	Data Monitor	Description
7.1	Last 10 Asset Creations	This data monitor provides a list of the last 10 assets created.
7.1	Last 10 Asset Deletions	This data monitor provides a list of the last
7.1	Last 20 Asset Modifications	This data monitor provides a list of the last 20 asset modifications done to assets.
7.2	Classification Level Traffic High to Low	This data monitor shows a graph of network traffic which went from a higher-classified asset to a lower-classified one.
7.2	Classification Level Traffic Low to High	This data monitor shows a graph of network traffic which went from a lower-classified asset to a higher-classified one.

Section 7 Filters

Section	Filter	Description
7.2	Asset Creation	Select events indicating the creation of a
7.2	Asset Deletion	Select events indicating the deletion of an asset.
7.2	Asset Modification	Select events indicating the modification of an asset.
7.3	Traffic from Higher to Lower Classification Level	This filter shows events going from an asset in a higher classification level to an asset in a lower classification level.
7.3	Traffic from Lower to Higher Classification Level	This filter shows events going from an asset in a lower classification level to an asset in a higher classification level.

Section 7 Rules

Section	Rule	Description
7	High to Low Classified Traffic Information Leak	This rule looks for information leak events which originated from a high-security classified system.

Section 7 Reports

Section	Report	Description	Config?
7.1	Asset Creation by Location	This report provides a listing of newly created assets. This report may (and should) be focused based on the Network Domain of interest.	Y: Select focus group
7.1	Asset Deletion by Location	This report provides a listing of deleted assets. This report may (and should) be focused based on the Network Domain of interest.	Y: Select focus group
7.1	Asset Modification by Location	This report provides a listing of modified assets. This report may (and should) be focused based on the Network Domain of interest.	Y: Select focus group
7.1	Assets by Network Domain (Creation Time) - Template	This report provides the listing of all the assets for the various Network Domains. This report may (and should) be focused based on the Network Domain of interest. Sorted by Creation time.	Y: Select focus group
7.1	Assets by Network Domain - Template	This report provides the listing of all the assets for the various Network Domains. This report may (and should) be focused based on the Network Domain of interest.	Y: Select focus group
7.1	Criticality of Assets	This report will show the asset criticality sorted by their criticality and network domain.	N
7.1	Assets in the Development Network Domain [Focused Report]	This report provides the listing of all the assets for the Development Network Domain.	N
7.1	Assets in the Development Network Domain (Creation-Time Sorted) [Focused Report]	This report provides the listing of all the assets for the Development Network Domain, sorted by creation time.	N
7.1	Assets in the Public-Facing Network Domain [Focused Report]	This report provides the listing of all the assets for the Public-Facing Network Domain.	N
7.1	Assets in the Public-Facing Network Domain (Creation-Time Sorted) [Focused Report]	This report provides the listing of all the assets for the Public-Facing Network Domain, sorted by creation time.	N

7.2	Classification of Assets	This report will show the asset classifications sorted by network domain.	N
7.2	High to Low Classified Asset Communication	This report shows all the assets which are classified in a higher classification level which are communicating with a lower-classified asset.	N
7.2	Low to High Classified Asset Communication	This report shows all the assets which are classified in a lower classification level which are communicating with a higher-classified asset.	N

Section 7 Queries

Section	Query	Description
7.1	Asset Creation by Location	This query provides a listing of newly created assets. This query may (and should) be focused based on the Network Domain of interest.
7.1	Asset Deletion by Location	This query provides a listing of deleted assets. This query may (and should) be focused based on the Network Domain of interest.
7.1	Asset Modification by Location	This query provides a listing of modified assets. This query may (and should) be focused based on the Network Domain of interest.
7.1	Assets by Network Domain (Creation Time) - Template	This query provides the listing of all the assets for the various Network Domains. This query may (and should) be focused based on the Network Domain of interest. Sorted by Creation time.
7.1	Assets by Network Domain - Template	This query provides the listing of all the assets for the various Network Domains. This query may (and should) be focused based on the Network Domain of interest.
7.1	Criticality of Assets	This query will show the asset criticality sorted by their criticality and network domain.
7.2	Classification of Assets	This query will show the asset classifications sorted by network domain.
7.2	Low to High Classified Asset Communication	This query shows all the assets which are classified in a lower classification level which are communicating with a higher-classified asset.
7.2	High to Low Classified Asset Communication	This query shows all the assets which are classified in a higher classification level which are communicating with a lower-classified asset.

Section 7 Trends

Section	Trends	Description
7.2	High to Low Classified Asset Communication	Trend to capture and report on events where communications occurred from a higher-to-lower classification.

ISO 8: Human Resources

The human factor is considered by many to be the least predictable element in the defense of the IT environment and digital assets. Staff that is insufficiently trained in secure operation of the IT environment or unaware of the organization's security undertaking and risks can undermine the entire security program.

This chapter addresses the human factor as it pertains to information security. It suggests controls that should be in place prior to employment, during employment, and upon termination, in order to reduce the risk of theft, fraud, unnecessary exposure to vulnerability, or misuse of facilities.

This section also relates to user awareness and the process of exiting or changing employment in an orderly manner. It covers current and potential employees, third party users and contractors.

Use Cases

To address section 8 requirements, the SOX4 solution provides the following use cases.

Observing New Hires

New employees can potentially impose a greater threat than veteran and trusted employees. Competitors or foreign agents may attempt to gain access to information by inserting impostors that would have any kind of network access. In contrast, new employees are susceptible to making unintentional mistakes that could have severe consequences.

The SOX4 solution identifies activities performed by new employees that can be considered suspicious and report them.

Internet Usage, Reporting and Monitoring

The SOX4 solution monitors Internet usage per user and per machine. This can be an indicator for people doing excessive Web browsing. It also identifies the most visited Web pages access by users. Monitoring these statistics for anomalies can help identify potential problems in an early stage.

Former Employee Monitoring

One of the most common attacks is using accounts of employees who have already left the company. It is essential to delete old accounts from the system and the use of these accounts must be investigated.

The SOX4 solution uses an active list which has to be populated with former employee user account names to flag all of their behavior.

Devices

The following devices supply the events that apply to ISO section 8.

Use Case	Devices	Device Configuration Required
Watching new hires	• Application • Database	None
Former employee monitoring	• Proxy • IAM	
Internet usage reporting and monitoring	• OS • VPN • Proxy • Router • Firewall	

Configuration

In addition to the asset modeling and configurations to the common resources described in “Configure the Sarbanes-Oxley 4 Solution”, the following resources should be configured as indicated.

Resource Type	Resource Name	What to configure
Active List	New Hire Accounts	This active list is populated automatically with new hire account information by the rule New Hire Identification, but it can also be populated manually. The standard timeout for this active list is 7 days. After that period of time, a new hire is dropped from the active list and not monitored anymore.
Active List	Former Employees	Configure this active list with the names of employees who have left the organization. Entries to this active list do not time out. Former employees’ user accounts stay on the list until they are removed manually.
Filter	Machine Internet Bases Activity	In this section, Internet activity is defined as communication to external addresses on ports 22, 80, 443 and 21. Modify this filter as necessary to modify this definition of Internet activity.
Filter	User Internet Based Activity	In this section, Internet activity is defined as communication to external addresses on ports 22, 80, 443 and 21. Modify this filter as necessary to modify this definition of Internet activity.

Section 8 Resources

This section lists all the resources that address the information systems acquisition development and maintenance requirements of ISO section 8.

Section 8 Active Lists

Active List	Description
New Hire Accounts	This list contains newly hired users and is automatically populated by the rule "New Hire Identification". New users are retained for 7 days in the list.
Former Employees	This Active List contains user accounts of former employees. User accounts in this Active List are retained indefinitely.

Section 8 Active Channels

Active Channel	Description
Internet Activity (Machine based)	This Active Channel shows Machine-based Internet Activity. Internet activity is defined as all communication from external addresses on ports 80, 443, 20, 21. To modify this definition, see Filter /All Filters/ArcSight Solutions/Compliance Insight Package/ISO 8 Human Resources Security/8.2 During Employment/8.2.3 Disciplinary Process/Machine Internet-based Activity
Internet Activity (User based)	This Active Channel shows User-based Internet Activity. Internet activity is defined as all communication from external addresses on ports 80, 443, 20, 21. To modify this definition, see Filter /All Filters/ArcSight Solutions/Compliance Insight Package/ISO 8 Human Resources Security/8.2 During Employment/8.2.3 Disciplinary Process/User Internet-based Activity

Section 8 Dashboards

Dashboard	Description
ISO 8 Human Resources Security	This Dashboard displays IT activities by former employees, suspicious activities by new hires, Internet activity per machine and Internet activity per user.

Section 8 Data Monitors

Data Monitor	Description
Suspicious Activity by	New hires suspicious activity count. Suspicious activity is counted for 7 days (as long as the user is defined new, s "New Hire Accounts" Active List) .
Internet Activity Per Machine	This Data Monitor shows Internet activity per reporting device per machine over a week's period.
Internet Activity Per User	This Data Monitor shows Internet activity per reporting device per user over a week's period.
Activity by Former Employees	This Dashboard displays the number of times a former employee's account appeared on the network in the last 24 hours.

Section 8 Filters

Filter	Description
Attacks	This filter looks for all attack events.
Attacks - Public Addresses	Filter to select attack events involving public addresses.
Compromises	This filter looks for generic compromises.
Reconnaissance - Public Addresses	This filter looks for reconnaissance events from nonprivate addresses to filter out the NULL coordinates.
Rule Firings	This filter looks for all the rule firings of the SOX4 solution.

Section 8 Rules

Rule	Description
New Hire Identification	This rule looks for newly created or renamed user accounts. It writes the new user names to the "New Hire Accounts" active list.
Former Employee Account Activity	This rule is looking for any activity of users that have been placed on the "Former Employees" Active List. This Rule will create a case for each unique user name that is attempted in the ArcSight Solutions/"Compliance Insight Package" folder in the case tree.

Section 8 Reports

Report	Description
Summary of Suspicious Activity by New Hires	This report displays the number of suspicious events per new hires.
Suspicious Activity by New Hires	This report displays all the identified suspicious activity performed by new users.
Internet Activity per Device per Machine	This report shows machine based Internet activity per reporting device. It shows the number of different Internet sessions requested by the machine and the number of different Internet addresses accessed by the machine.
Internet Activity per Device per User	This report shows user based Internet activity per reporting device. It shows the number of different Internet sessions requested by the user and the number of different Internet addresses visited by the user.
Activity by Former Employees	This report shows any activity performed by users who are known to be terminated.

Section 8 Queries

Query	Description
Summary of Suspicious Activity by New Hires	This query displays the number of suspicious events per new hires.
Suspicious Activity by New Hires	This query displays all the identified suspicious activity performed by new users.
Internet Activity per Device per Machine	This query shows machine based Internet activity per Querying device. It shows the number of different Internet sessions requested by the machine and the number of different Internet addresses accessed by the machine.
Internet Activity per Device per User	This query shows user based Internet activity per Querying device. It shows the number of different Internet sessions requested by the user and the number of different Internet addresses visited by the user.
Activity by Former Employees	This query shows any activity performed by users who are known to be terminated.

ISO 9: Physical and Environmental Security

The Physical and Environmental Security section covers physical access, loss prevention, damage, theft, compromise of assets and interference to the organization's premises and information.

Use Cases

To address section 9 requirements, the SOX4 solution provides the following use cases.

Physical Building Access

Tracking physical access to facilities is an important additional feed of information to track about users. The solution can detect access to computing infrastructure from people who are not badged into the building. It also provides reporting and monitoring around general physical access activity.

The SOX4 solution identifies activities performed by new employees that can be considered suspicious and report them.

Monitoring/Reporting Contractor's Physical Access

Contractors have limited access only to the areas of the facility in which they perform their jobs. Unauthorized access by contractors to other areas should be monitored and investigated, as necessary. The solution flags contractor access to buildings during offhours.

Former Employee Monitoring

One of the most common attacks is using accounts of employees who have already left the company. It is essential to delete old accounts from the system and the use of these accounts must be investigated.

The SOX4 solution uses an active list which has to be populated with former employee user account names to flag all of their behavior.

Devices

The following devices supply the events that apply to ISO section 8.

Use Case	Devices	Device Configuration Required
Physical building access by employees	Physical Badge Access System	Many badge readers are set up to report in batch mode. The closer to real-time the feed can be configured, the better the correlation output will be.
Physical building access by contractors		

Configuration

In addition to the asset modeling and configurations to the common resources described in “Configure the Sarbanes-Oxley 4 Solution”, the following resources should be configured as necessary to comply with your policies.

Resource Type	Resource Name	What to configure
Filter	After Hours	The time component of the “After Hour Building Access – Success” is defined in the filter /All Filters/ArcSight Solutions/Compliance Insight Package/My Filters/After Hours. Configure this filter as necessary to match what your organization considers after hours.

Section 9 Resources

This section lists all the resources that address the information systems acquisition development and maintenance requirements of ISO section 9.

Section 9 Active Channels

Active Channel	Description
Physical Security	This Active Channel shows all physical access related activities.

Section 9 Dashboards

Section	Dashboard	Description
9.1.2	Building Access - Event Graph	This dashboard shows a bar chart for every ISO section in the solution that indicates the top triggered rule for each section.
9.1.2	Last 20 Building Access Events	Dashboard showing the last 20 people accessing a building.
9.1.2	Top Users Accessing Buildings	Dashboard showing the top users who accessed buildings.

Section 9 Data Monitors

Data Monitor	Description
Last 20 Rules Fired	Data monitor to display a graphic distribution of the last 20 correlation rules fired from this section.
Rules Attackers and Targets	Event graph to show attacker-target pair relationship for the various rule firings from this section.
Section9 Overview	A high level data monitor to indicate that a rule in this section has fired.
Top 20 Rules Fired	Data monitor to display a graphic distribution of the 20 most frequently firing correlation rules of this section.
Top 20 Targets in Rule Firings	Data monitor to show which targets are most frequently involved in rule firings for that section. This may reveal a trend about certain targets.

Section 9 Filters

Filter	Description
After Hours Building Access - Success	This filter selects all events indicating successful occurrences of physical access after hours. The actual time slot is defined in the referenced filter.
All Physical Events	This filter selects all events sent to ArcSight by physical security systems.
Contractor Access After Hours	This filter looks for the real-time detection of contractors accessing buildings after hours.

Section 9 Rules

Rule	Description
Activity from Badged-Out Employee	This rule detects network activity on an internal network segment even though the employee is not physically present in the building.
After Hours Building Access by Contractors	This rule detects building access events after business hours.
Badged-In Employees	This rule detects successful building access and adds the users to the badged in active list.
Badged-Out Employees	This rule detects when someone leaves a building and removes the user from the badged in active list.
Failed Building Access	This rule detects failed physical building access.

Section 9 Reports

Report	Description
High Risk Events	Relates to physical access of a building after business hours, regardless of whether the access was granted, or not. Actual time values are defined in the filter referenced in the 'Conditions' pane.
Failed Building Access Events	This query shows failed attempts to enter a building at any time.
Successful Building Access Events	This report shows successful building access events at all times.

Section 9 Queries

Query	Description
After Hours Building Accesses	Relates to physical access of a building after business hours, regardless of whether the access was granted, or not. Actual time values are defined in the filter referenced in the 'Conditions' pane.
Failed Building Access Events	This query shows failed attempts to enter a building at any time.
Successful Building Access Events	This query shows successful building access events at all times.

ISO 10: Communications and Operations Management

A large amount of the computer related tasks performed in an organization involve communications and operations. This chapter addresses operational procedures, third parties service delivery, system planning, capacity management, malicious code, network controls, exchange of information and electronic commerce services.

Use Cases

To address section 10 requirements, the SOX4 solution provides the following use cases.

User Attribution

SOX4 includes a session list called User Name and IP Address Association that identifies IP addresses assigned during desktop and VPN logins with the user name to whom the IP address is assigned. This enables the solution to correlate events that involve traffic from those IP addresses with the username of the person who is assigned to that IP address.

A series of rules evaluate the event stream to detect when these sessions begin and end. The SOX4 solution then uses entries to this session list to detect infections that originate from remote machines and associate them with the user whose login introduced the infection. The solution also uses this list to allow access to assets by only qualified users.

The solution also includes two long-term trends that use entries to this session list to track user/address associations and infected VPN log-ins over time. Reports then provide statistics about users and the IP addresses associated with them, and infections originating from remote hosts via VPN.

Content in other sections uses this session list to attribute IP addresses back to user names. For example, Section 11 - Role-Based Access Monitoring uses this list.

Monitoring Maintenance Schedule

Unscheduled changes to maintenance tasks should be analyzed carefully, since they can indicate an intrusion to the system. They may also affect operational tasks in an undesired way.

The SOX4 solution includes filters, rules, and data monitors that provide insights on changes to services and hosts that occurred outside of the scheduled maintenance window. The maintenance window is defined by the user in the Maintenance Window filter. For configuration instructions, see “Maintenance Window Filter”.

Monitoring/Reporting File Changes

Modification of sensitive files should be monitored for proper use and authorizations. These files are the "crown jewels" of the organization and contain its most sensitive information.

The SOX4 solution provides a report on all file changes detected based on reports from the File Integrity Checker. The default time window is the last 24 hours, which can be changed by the user.

Configuration Changes

Information processing systems and applications should be subject to strict change management procedures.

Reports and data monitors provide insight on any configuration changes to OS, applications, firewalls and network equipment. These are presented both per modification and per asset. These reports show the changes for the last 24 hours, which can be modified by the user.

Separation of Development, Test and Operational Facilities

Development, test, and operational facilities should be separated to reduce the risks of unauthorized access or changes to the operational system. Filters identify all traffic between development, operational and test environment, and Active Channels display these events. Reports were designed to display all hostile or suspicious traffic, as well as cross-talk between the operations, test and development segments.

Changes to Third-Party Services

It is important to implement an appropriate level of information security in regard to the integration of third party devices in the environment. Active channels show all traffic originating from or targeting third party assets. Filters identify and reports and data monitors show all suspicious activities targeting and originating in third party devices as well as any changed made to third party applications.

Third party assets are categorized by the user in the third party network domain.

Malicious Code Monitoring

Malicious code is continuously being developed and deployed faster and more deviously every day.

An active channel displays malicious code activity such as DoS, and backdoors. A filter identifies events where malicious code activity is detected. Reports show all the attacks targeting email systems, any failed ant-virus updates on systems, incidents where malicious code was detected, Trojan horse activity, and a summary of viruses detected on systems sorted by virus and by hosts.

A data-monitor renders an event graph showing malicious code activity between Attacker- Target pairs. A rule monitors for malicious code detected on any of the Network Domain host systems. Qualifying hosts are then added to the "malicious code addresses list" active list.

System Monitoring

This use case aims at detecting both day-to-day operations that occur on systems such as user logins and other tasks that may raise more suspicion, such as deletion of the audit logs.

Reports present information on account creations and deletions, password changes, authorization changes, account lockouts, after-hour system access and after hour logins to sensitive systems, database access and failed database access, logins that are identified as brute force, all user and administrative logins and log-outs, clearing of audit logs, fault logging and clock synchronization issues.

Data Monitors show updated information regarding many of these events such as unsuccessful administrative logins and authorization modifications. The filters that detect these events are using the Administrative Accounts List Active List to track the administrative accounts. Rules focus on brute force logins and clearing of audit logs, Active Channels display all authentication events.

Exchange of Information and Electronic Commerce

The risk of compromising security on public-facing systems that are used for exchange of information and electronic commerce is high because they are exposed to every internet user. If these systems support business processes, their compromise could mean loss of money as well as reputation. Thus, it is essential to closely monitor all exchange of information with public systems.

Reports show events that represent possible interception of data, originating and targeting devices that are categorized by the user as "public facing" or "production," and log-ins to public-facing systems, outbound IM events, and vulnerable business systems.

Data Monitors display information interception events, attackers and suspicious information that involve public facing assets as well as top IM out-bound sources, vulnerable business systems and information regarding scanner events. Rules are triggered when an IM application is targeted (the list of IM applications can and should be updated by the user). Active channels display attacks and suspicious activities regarding public facing assets and exchange of information.

Devices

The following devices supply the events that apply to ISO section 10.

Use Case	Device	Device Configuration Required
User Attribution	•OS •VPN	None
Monitoring maintenance schedule	•OS •Application •Database	None
Monitoring/reporting file changes	•OS •File Integrity Checker •HIDS/HIPS	Turn file auditing on for important files.
Configuration changes and Changes to third-party services	•OS •Application •Database •Configuration Management •Any device logging configuration changes (most devices do)	Make sure configuration changes are logged
Separation of Development, Test and Operational Facilities	•Router •Firewall •NIDS/NIPS	None
Malicious code monitoring	•Anti Virus •NIDS/NIPS •HIDS/HIPS	None

Configuration

In addition to the asset modeling and configurations to the common resources described in “Configure the Sarbanes-Oxley 4 Solution”, the following resources should be configured as necessary to comply with your policies.

Resource Type	Resource Name	What to configure
Filter	Maintenance Window	Define the maintenance window in the filter Unscheduled Change in Status of Service and in the filter /All Filters/ArcSight Solutions/Compliance Insight Package/My Filters/Maintenance Window.
Assets	Test, Operations, and Development	The assets “Test”, “Operations” and “Development” in the group “Network Domains” should be populated according to the environment the asset is located in.
Active List	Administrative Accounts List	The filters Successful Administrative Login, Successful Administrative Logouts and Unsuccessful Administrative Logins depend on entries from the Active List Administrative Accounts List. For instructions about how “Configure Active Lists ” on page 39.

Asset Category	Network Domains/Third Parties	Several filters depend on third-party assets, such as services offered by vendors or partners, being categorized in the Network Domain asset category Third Parties. “Model Assets (Assign Asset Categories)” on page 33.
Assets	AOL IM ICQ MSN IM Yahoo IM	The use cases that deal with tracking and reporting on instant messaging activity require that: • You create assets in the ArcSight asset model for instant messaging servers. The assets representing instant messaging servers be categorized in the asset categories appropriate for their service in All Asset Categories/ArcSight Solutions/Compliance Insight Package/Disallowed Servers/...AOL, ICQ, MSN IM, Yahoo IM..
Asset Category	Public-Facing	The filters Attacks and Suspicious Activity From Public-Facing Assets and Attacks and Suspicious Activity Targeting Public-Facing Assets depend on public-facing assets being categorized in the Asset Category /All Asset Categories/ArcSight Solutions/Compliance Insight Package/Network Domains/Public-Facing. For instructions about how to assign asset categories, see “Model Assets (Assign Asset Categories)” on page 33.

Section 10 Resources

This section lists all the resources that address the information systems acquisition development and maintenance requirements of ISO section 10.

Section 10 Active Lists

Active List	Description
Administrative Accounts	This Active List should be populated with the usernames that have administrative privileges in your domain. Admins (those responsible for managing administrative users) populate this list manually whenever a new administrative user is added.
Malicious Code Addresses	List of all hosts with malicious code detected on them.

Section 10 Active Channels

Active Channel	Description
Attacks and Suspicious Activity Targeting Public-Facing Assets	This active channel shows all events where the target is an asset from Public-Facing Assets category.
Attacks and Suspicious Activity Targeting Third-Party Assets	This active channel shows all events where the target is an asset from Third-Parties assets category.

Attacks and Suspicious Activity from Public-Facing Assets	This active channel shows all events where the source is an asset from Public-Facing assets category.
Attacks and Suspicious Activity from Third-Party Assets	This active channel shows all events where the source is an asset from Third-Parties assets category.
Authentication Events	Channel to show when any log-on occurs in real-time over a 2 hour continuously sliding window.
Development to Test or Operations Traffic	Display traffic from Development segment to Test or Operations segments in real-time over a 2 hour continuously sliding window.
Exchange of Information	Active channel to show exchange of information activity in real-time over a 2 hour continuously sliding window.
Infected VPN Remote Host Found	Active channel to show all rule firing events when the rule 'Infected VPN Remote Host Found' fires.
Malicious Code Activity	Channel to show malicious code activity such as DoS, backdoors, etc.
Operations to Test or Development Traffic	Display traffic from Operations segment to Test or Development segments in real-time over a 2 hour continuously sliding window.
Test to Development or Operations Traffic	Display traffic from Test segment to Development or Operations segments in real-time over a 2 hour continuously sliding window.

Section 10 Dashboards

Section	Description	Dashboard
10.1.2	Unscheduled Change of Service	Dashboard showing machines which showed an unscheduled change of a service.
10.10.1	Accounts Activity	Dashboard showing account activities per machine and activity, such as accounts created, modified, and deleted
10.10.1	Authorization Changes	Dashboard showing authorization changes i.e. changes to access right or privileges of users.
10.10.1	Device and OS Configuration Modifications	Dashboard showing device and operating system configuration changes.
10.10.2	Unsuccessful User Logins	Dashboard showing unsuccessful login attempts.
10.10.2	User Logins and Logouts	Dashboard showing logins and logouts.
10.10.4	Administrative Logins and Logouts	Dashboard showing administrative logins and logouts.
10.10.4	Unsuccessful Administrative Logins	Dashboard showing failed administrative logins.
10.2.2	Last 10 Events Activity to and from Third-Party Assets	Dashboards showing activity from third-party devices.
10.2.2	Target Port Based Activity for Third-Party Assets	Dashboard showing activity from third-party devices based on activity per port.

10.4.1	Malicious Code Activity	Dashboard showing malicious code activity and infected vpn hosts.
10.6.1	Network Controls	Dashboard showing devices which are sending events and firewall rule configuration.
10.8.1	Information Interception	Dashboard showing information interception attacks.
10.8.4	Outbound IM Traffic	Dashboard showing instant messenger traffic leaving the corporate network.
10.8.5	Scanner Event Views	Dashboard showing events from vulnerability scanners.
10.8.5	Vulnerable Business Information Systems	Dashboard showing vulnerable business machines.
10.9.3	Last 10 Events Activity to and from Public-Facing Assets	Dashboard showing activity surrounding public-facing assets such as Web servers.
10.9.3	Target Port Based Activity for Public-Facing Assets	Dashboard showing activity surrounding public facing assets broken down per port.

Section 10 Data Monitors

Data Monitor	Description
Unscheduled Change of Service	Data monitor to show events where a change of service was affected on a host outside of the scheduled maintenance window.
Last 10 Device and OS Configuration Modifications	This data monitor tracks the most recent configuration modifications to assets categorized in Network Domains
Last 10 Information System Accounts Created	This data monitor provides a list of the last 10 account creations in your assets categorized in Network Domains.
Last 10 Information System Accounts Deleted	This data monitor provides a list of the last 10 account deletions in your assets categorized in Network Domains.
Last 20 Information System Accounts Modified	This data monitor provides a list of the last 10 account modifications in your assets categorized in Network Domains.
Last 25 Authorization Changes	This data monitor provides an overview of the authorization changes across assets categorized in Network Domains.
Top 10 Asset Network Domains with Account Creation	This data monitor provides a list of the Network Domain asset categories in which the most accounts have been created so that you can identify those Network Domains that are most often modified in this fashion.
Top 10 Asset Network Domains with Account Deletion	This data monitor provides a list of the Network Domain asset categories in which the most accounts have been deleted so that you can identify those Network Domains that are most often modified in this fashion.
Top 10 Asset Network Domains with Account Modification	This data monitor provides a list of the Network Domain asset categories in which the most accounts have been modified so that you can identify those Network Domains that are most often modified in this fashion.

Top 10 Devices with Configuration Modifications	This data monitor provides a list of the assets categorized in Network Domains that have their configurations changed frequently.
Top Authorization Changes By User - Last 24 Hours	This data monitor provides the top users making authorization changes across assets categorized in Network Domains in the last 24 hours.
Top Authorization Changes By User - Last Hour	This data monitor provides the top users making authorization changes across assets categorized in Network Domains in the last hour.
Last 10 Successful User Logins	This data monitor provides a list of the last 10 successful logins across your assets categorized in Network Domains.
Last 10 Successful User Logouts	This data monitor provides a list of the last 10 successful user logouts across your assets categorized in Network Domains.
Last 20 Unsuccessful User Logins	This data monitor provides a list of the last 20 unsuccessful logins across your assets categorized in Network Domains.
Top 10 Hosts with Unsuccessful User Logins	This data monitor provides a list of the users who most commonly have login failures.
Top 10 Network Domains with Unsuccessful User Logins	This data monitor provides an ordered list of the Network Domains that most commonly have user login failures.
Top 10 Users with Unsuccessful Logins	This data monitor provides a list of the users who most commonly have failed logins.
Last 10 Successful Administrative Logins	This data monitor provides a list of the last 10 successful administrative logins across your assets categorized in Network Domains.
Last 10 Successful Administrative Logouts	This data monitor provides a list of the last 10 administrative logouts across your assets categorized in Network Domains.
Last 20 Unsuccessful Administrative Logins	This data monitor provides a list of the last 20 unsuccessful administrative logins across your assets categorized in Network Domains.
Top 10 Administrative Users with Unsuccessful Logins	This data monitor provides a list of the administrative users who most commonly have login failures.
Top 10 Hosts with Unsuccessful Administrative Logins	This data monitor provides a list of the hosts that most commonly have unsuccessful administrative logins.
Top 10 Network Domains with Unsuccessful Administrative Logins	This data monitor provides an ordered list of the Network Domains that most commonly have administrative login failures.
Attacks and Suspicious Activity Targeting Third-Party Assets	Data monitor to show all activity destined towards Third-Party assets, sorted by target ports.
Attacks and Suspicious Activity From Third-Party Assets	Data monitor to show all activity originating from Third-Party assets, sorted by target ports.

Last 10 Attacks and Suspicious Activity Targeting Third-Party Assets	This data monitor displays the last 10 events where the traffic is destined for a third-party asset.
Last 10 Attacks and Suspicious Activity from Third-Party Assets	This data monitor displays the last 10 events where the traffic originated from a third-party asset.
Infected VPN Remote Host Found	Data monitor to show a traffic light style indicator when a virus infected host is found coming in over a VPN session. The user name associated with the VPN session is displayed in the tile.
Malicious Code Activity	Data monitor to render an event graph showing malicious code activity between Attacker-Target pairs.
Firewall Open Ports	This data monitor is used to determine which ports a particular firewall is allowing traffic on.
Logging Devices	Data monitor to show all devices other than ArcSight that are sending their logs.
Last 10 Information Interception Events	This data monitor shows the last 10 Information Interception Events
Top Information Interception Attackers	This is a pie chart of the attackers triggering information interception events
Outbound IM Traffic	Event graph data monitor to show the IM traffic.
Top IM Outbound Sources	This data monitor shows the top IM users.
Last 10 Vulnerable Business System Events	Shows the last 10 scanner events finding vulnerabilities on business information systems
Last 20 Scanner Events	Data monitor to display in real-time the last 20 scanner-generated events related to assets categorized in.
Last Vulnerable Business System Assets	Shows the last vulnerable business system assets by agent severity.
Top Machines by Scanner Event Count	Data monitor to show in real-time the top 20 machines with vulnerabilities as shown by scanner events.
Top Vulnerable Business Information Systems	Top vulnerable business information systems
Attacks and Suspicious Activity Targeting Public-Facing Assets	Data monitor to show all activity destined towards public-facing assets, sorted by target ports.

Attacks and Suspicious Activity From Public-Facing Assets	This data monitor displays all activity originating from public-facing assets, and is sorted according to the target ports.
Last 10 Attacks and Suspicious Activity Targeting Public-Facing Assets	This data monitor displays the last 10 events where the traffic is destined for a public-facing asset.
Last 10 Attacks and Suspicious Activity from Public-Facing Assets	This data monitor displays the last 10 events where the traffic originated from a public-facing asset.

Section 10 Filters

Section	Filter	Description
10.1.2	Unscheduled Change in Status of Service	Filter to select events any time a service on a host is changed when it is outside of a scheduled maintenance window. The maintenance window is defined by the referenced filter.
10.1.4	Development to Test or Operations	Filtering in traffic where the Attacker Asset belong to Development, and the target asset belongs to either Test or Operations.
10.1.4	Operations to Test or Development	Filtering in traffic where the Attacker Asset belong to Operations, and the target asset belongs to either Test or Development.
10.1.4	Test to Development or Operations	Filter in traffic originating from a Test asset and going to a target asset that is either a development or operations asset.
10.1	Device and Operating System Configuration Modifications	This filter identifies configuration modifications occurring on assets categorized in Network Domains.
10.1	Password Changes	This filter identifies password changes events that occur on assets categorized in one of your Network Domains.
10.10.1	Account Creation	This filter identifies account creation events that occur on assets categorized in one of your Network Domains.
10.10.1	Account Deletion	This filter identifies account deletion events that occur on assets categorized in one of your Network Domains.
10.10.1	Account Modification	This filter identifies account modification events that occur on assets categorized in one of your Network Domains.
10.10.1	Authorization Changes	This filter looks for changes of access privileges.
10.10.2	Account Lockouts	This filter will show Account Lockouts.
10.10.2	Successful Brute Force Logins	This filter identifies events generated by the Probable Successful Brute Force rule that involve assets categorized in one of your Network Domains.
10.10.2	Successful User Login	This filter identifies events that indicate successful user logins to assets categorized in one of your Network Domains.

10.10.2	Successful User Logout	This Filter identifies events that indicate successful user logouts from Assets in one of your Network Domains.
10.10.2	Successful and Unsuccessful User Logins	This filter identifies failed and successful login events that involve assets categorized in Network Domains.
10.10.2	Unsuccessful User Login	This filter identifies events that indicate unsuccessful user login attempts to an asset categorized in one of your Network Domains.
10.10.2	User Login and Logout	This filter identifies login and logout events that relate to assets categorized in one of your Network Domains
10.10.4	Successful Administrative Login	This filter identifies events that indicate successful administrative logins to assets categorized in one of your Network Domains.
10.10.4	Successful Administrative Logout	This filter identifies events that indicate successful administrative logouts from assets categorized in one of your Network Domains.
10.10.4	Unsuccessful Administrative Login	This filter identifies events that indicate unsuccessful administrative login attempts to an asset categorized in one of your Network Domains.
10.10.2	Attacks and Suspicious Activity From Third-Party Assets	This filter identifies events that are generated by assets categorized in the Third-Party Network Domain.
10.10.2	Attacks and Suspicious Activity Targeting Third-Party Assets	This filter identifies events that are destined for assets categorized in the Third-Party Network Domain.
10.4.1	Host Found Infected with Virus	Filter to select events where a host is found infected by a virus.
10.4.1	Infected VPN Remote Host	Filter to select events when the 'Infected Remote Machine Found' rule fires.
10.4.1	Malicious Code Activity	Filter to select events where malicious code activity is detected.
10.4.1	VPN Login Detected	Filter to select events where a user was successfully authenticated by VPN.
10.4.1	VPN Session Terminated	Filter to select events where a user successfully logs out of VPN.
10.8.1	Information Interception Events	This filter shows possible information interception events such as spoofing attempts or man in the middle attacks
10.8.4	Outbound IM Traffic	Filter to select all outbound instant messaging traffic.
10.8.5	Vulnerabilities on Business Information Systems	This filter shows all scanner events that indicate a vulnerability on a business information system
10.9.3	Attacks and Suspicious Activity From Public-Facing Assets	This filter identifies events that are generated by assets categorized in the Public-Facing Network Domain.
10.9.3	Attacks and Suspicious Activity Targeting Public-Facing Assets	This filter identifies events that target assets categorized in the Public-Facing Network Domain.

Section 10 Rules

Section	Rule	Description
10.1.1	System Restarted at Unscheduled Time	This rule monitors hosts that were restarted. This flags for graceful shutdowns and startups as well as unexpected shutdowns and other events that indicate a system restart. Windows Collector Agents must monitor for Security and System logs. Note: Windows Only 6006 - Event Log Stopped 6009 - Startup Message 6005 - Event Log Started 6008 - Unexpected. The catch all condition is that an OS was started or stopped.
10.1.2	Unscheduled Change in Status of Service	This rule will fire any time a service on a host is changed when it is outside of a scheduled maintenance window. The maintenance window is defined by the referenced filter. A case is opened for each host on which this anomaly is detected.
10.10.2	Application Brute Force Logins	This rule identifies brute force login attempts against applications installed on assets categorized in network domains.
10.10.2	Login Session Information Added	This rule is used to update the session list to keep track of user-to-IP address associations whenever a login to a desktop is detected
10.10.2	Logout Session Information Cleared	This rule is used to terminate the session list entry when a log-out event is detected
10.10.2	Successful Attack Brute Force	This rule detects brute force attacks.
10.10.3	Audit Log Cleared	This rule monitors for clearing of the audit log on Windows systems.
10.4.1	Infected Remote Machine Found	This rule detects when a remote machine, i.e. a host authenticated by a VPN device, is found infected by a virus.
10.4.1	Malicious Code Detected	This rule monitors for malicious code detected on any of the Network Domain host systems. Qualifying hosts are then added to the referenced active list.

10.8.1	Possible Information Interception	This rule is looking for attacks where information could be redirected and collected by an unintended party.
10.8.4	Outbound IM Traffic	This rule will fire any time the system detects outbound IM traffic using the well known instant messaging application. The well known applications blacklist can be modified in the Conditions tab.
10.8.5	Vulnerabilities Found - Business Information System	The purpose of this rule is to look for vulnerabilities being found on an asset that is categorized as a business information system.

Section 10 Reports

Section	Report	Description
10.1.1	System Restarted at Unscheduled Time	Report to show unscheduled restarts of hosts in the last 24 hours. This report is based on a rule firing in the corresponding section.
10.1.2	Application Configuration Modifications	This report will show any configuration modifications of any application on a system. Default time window: Last 24 hours.
10.1.2	File Integrity Changes Detected	Report all file changes detected based on reports from the File Integrity Checker. Default time window: Last 24 hours.
10.1.2	Firewall Configuration Modifications	This report will show any configuration modifications of any firewall. Default time window: Last 24 hours.
10.1.2	Network Device Configuration Modifications	This report will show any configuration modifications of any network equipment. Default time window: Last 24 hours.
10.1.2	OS Configuration Modifications	This report will show any configuration modifications of any operating system. Default time window: Last 24 hours.
10.1.2	Syslog Restart Events	This report shows all restarts of syslog on systems.
10.1.2	Unscheduled Change in Service	Track starting or stopping of services outside of scheduled maintenance windows in the last 24 hours. NOTE: Alter the parameters in the referenced filter in order to redefine the time- slot of the maintenance window.
10.1.4	Attacks from Development Targeting Production	This report provides a listing of hostile or suspicious traffic from development machines targeting production facilities.

10.1.4	Attacks from Production Targeting Development	This report provides a listing of hostile or suspicious traffic from production facilities targeting development machines.
10.1.4	Development to Test or Operations Cross-Talk	Reports all cross-talk in the last 24 hours from assets in Development category to assets in either Test or Operations categories.
10.1.4	Operations to Test or Development Cross-Talk	Reports all cross-talk in the last 24 hours from assets in Operations category to assets in either Test or Development categories.
10.1.4	Test to Development or Operations Cross-Talk	Reports all cross-talk in the last 24 hours from assets in Test category to assets in either Development or Operations categories.
10.10.1	Account Creation - Template	This report provides a listing of newly created Information System Accounts. This report may (and should) be focused based on the Network Domain of interest.
10.10.1	Account Deletion - Template	This report provides a listing of deleted Information System Accounts. This report may (and should) be focused based on the Network Domain of interest.
10.10.1	Authorization Changes - Template	This report provides a listing of modified Information System Accounts. This report may (and should) be focused based on the Network Domain of interest.
10.10.1	Changes to Development Machines	This report lists changes made to development systems categorized as a Regulated systems.
10.10.1	Device and OS Configuration Changes	This report provides a listing (sorted by Asset) of configuration modifications to Assets in your Network Domains.
10.10.1	Operating System Changes	This report lists changes made to operating systems of Governed systems.
10.10.1	Operating System Configuration Modifications	This report will show all OS configuration changes made to Regulated systems.
10.10.1	Password Changes	This report provides a list of password changes on Network Domain categorized assets. The results are sorted by asset. This report can (and should) be focused based on the Network Domain of interest.
10.10.2	Account Lockouts by System	This report will show all the account lockouts on Governed Assets organized by system.
10.10.2	Account Lockouts by User	This report will show all the account lockouts on Governed Assets organized by user.
10.10.2	After Hours Systems Access by System	This report shows all the systems that were accessed sorted by user after normal business hours.
10.10.2	After Hours Systems Access by User	This report shows all the systems that were accessed sorted by user after normal business hours.

10.10.2	After-Hours Logins to Sensitive Systems	This report provides a listing of after-hours login attempts which target systems categorized as sensitive by Asset. This report may be focused based on the Network Domain of interest.
10.10.2	Database Access - All	This report shows all authentication events on databases.
10.10.2	Failed Database Access	This report shows all failed attempts to access databases.
10.10.2	File Modifications on Assets	This report will show all file modifications on systems in the last 24 hours as reported by a file integrity application.
10.10.2	Non-Secured Access of Assets from External System	This report shows the authentications from non-protected sources to systems.
10.10.2	Number of Successful User Logins	This report provides a listing of users with successful logins by Asset. The users are sorted by the number of attempts in a decreasing order. This report may (and should) be focused based on the Network Domain of interest.
10.10.2	Number of Unsuccessful User Logins	This report provides a listing of users with unsuccessful login attempts. The users are sorted by the number of attempts in a decreasing order. This report may (and should) be focused based on the Network Domain of interest.
10.10.2	Successful Brute Force Logins	This report provides a listing of events categorized by ArcSight as probable successful brute force login attempts. This report may (and should) be focused based on the Network Domain of interest.
10.10.2	Top 10 Unsuccessful User Logins	This report provides a chart showing the top 10 users with unsuccessful login attempts. This report may (and should) be focused based on the Network Domain of interest.
10.10.2	Unsuccessful User Logins	This report provides a listing of unsuccessful user login attempts. This report may (and should) be focused based on the Network Domain of interest.
10.10.2	User Logins and Logouts	This report provides a listing of unsuccessful user login attempts. This report may (and should) be focused based on the Network Domain of interest.
10.10.2	User Name and IP Address Association	Report of user names-to-IP address associations recorded on a daily basis from the contents of the 'User Name and IP Address Association' session list. This report may be run and the output stored as a hard copy for historical purposes.
10.10.2	VPN Access Report	This report provides an overview of access via VPN into your Network Domains.
10.10.2	VPN Access Report by Target Asset	This report provides a listing of VPN access events which target the various Network Domains. This report may (and should) be focused based on the Network Domain of interest.
10.10.3	Audit Log Cleared	Report to show all events where an audit log was cleared from a host.
10.10.4	Administrative Logins and Logouts	This report provides a listing of administrative logins and logouts by Asset. This report may (and should) be focused based on the Network Domain of interest.
10.10.4	Administrator Actions - All	This report lists all actions taken by an administrative user.

10.10.4	Number of Successful Administrative Logins	This report provides a listing of administrative users with successful logins by Asset. The administrative users are sorted by the number of attempts in a decreasing order. This report may (and should) be focused based on the Network Domain of interest.
10.10.4	Number of Unsuccessful Administrative Logins	This report provides a listing of administrative users with unsuccessful login attempts. The administrative users are sorted by the number of attempts in a decreasing order. This report may (and should) be focused based on the Network Domain of interest.
10.10.4	Top 10 Unsuccessful Administrative Logins	This report provides a chart showing the top 10 administrative users with unsuccessful login attempts. This report may (and should) be focused based on the Network Domain of interest.
10.10.4	Unsuccessful Administrative Logins by Asset	This report provides a listing of unsuccessful administrative login attempts. This report may (and should) be focused based on the Network Domain of interest.
10.10.5	Fault Logs	Fault Logging report.
10.10.6	Agents Reporting Inaccurate Times	This report will display all agent detect time error events.
10.2.2	Attacks and Suspicious Activity Targeting Third-Party Assets	Report to show all attacks and suspicious activity where the target was an asset in the Third-Parties asset category. Default time window: Last 24 hours.
10.2.2	Attacks and Suspicious Activity from Third-Party Assets	Report to show all attacks and suspicious activity where the source was an asset in the Third-Parties asset category. Default time window: Last 24 hours.
10.2.3	Changes to Third-Party	Report to show changes made to applications on third-party resources.
10.3.1	Resource Exhaustion Detected	Report on resources reaching their upper end of utilization (for capacity management and planning purposes).
10.4.1	Attacks Targeting Email Systems	Report showing all the attacks targeting email systems.
10.4.1	Failed Anti-Virus Updates	This report will show all the failed AV updates on systems.
10.4.1	Infected VPN Remote Host Found	Report to show the number of virus infections detected over a VPN based user session.
10.4.1	Malicious Code Detected	Report of incidents where malicious code was detected based on the referenced filter's criteria.
10.4.1	Trojan Code Activity	This report shows all trojan activity.
10.4.1	Virus Summary	This report will show a summary of viruses detected on systems sorted by virus.

10.4.1	Virus Summary by Hosts	This report will show a summary of viruses detected on systems sorted by host.
10.6.1	Device Logging Review	This report shows the different products that are logging to ArcSight ESM.
10.6.1	Firewall Open Port Review	This report should be used to review the traffic that is being passed by the firewalls around the organization.
10.8.1	Information Interception	this report shows events that represent a possible interception of data
10.8.4	Outbound IM Traffic	This report shows outbound IM traffic.
10.8.5	Vulnerable Business Information Systems	This report shows the business information systems that have vulnerabilities.
10.9.3	Attacks and Suspicious Activity Targeting Public-Facing Assets	This report shows all the attacks and suspicious attacks where the target asset belonged to the Public-Facing asset category.
10.9.3	Attacks and Suspicious Activity from Public-Facing Assets	This report shows all the attacks and suspicious attacks where the source asset belonged to the Public-Facing asset category.
10.9.3	Events Targeting Public-Facing and Production Assets	This report provides a listing of hostile or suspicious traffic which targets the assets categorized as public-facing or production.
10.9.3	External Logins to Public Facing Systems	This report provides a listing of user authentications on external facing systems from external sources.

Section 10 Queries

Section	Query	Description
10.1.2	Application Configurations	This report will show any configuration modifications of any application on a system. Default time window: Last 24 hours.
10.1.2	File Integrity Changes Detected	Report all file changes detected based on reports from the File Integrity Checker. Default time window: Last 24 hours.
10.1.2	Network Device Configuration Modifications	This report will show any configuration modifications of any network equipment. Default time window: Last 24 hours.
10.1.2	OS Configuration Modifications	This report will show any configuration modifications of any operating system. Default time window: Last 24 hours.
10.1.2	Syslog Restart Events	This report shows all restarts of syslog on systems.

10.1.4	Attacks from Development Targeting Production	This report provides a listing of hostile or suspicious traffic from development machines targeting production facilities.
10.1.4	Development to Test or Operations Cross-Talk	Reports all cross-talk in the last 24 hours from assets in Development category to assets in either Test or Operations categories.
10.1.4	Operations to Test or Development Cross-Talk	Reports all cross-talk in the last 24 hours from assets in Operations category to assets in either Test or Development categories.
10.1.4	Test to Development or Operations Cross-Talk	Reports all cross-talk in the last 24 hours from assets in Test category to assets in either Development or Operations categories.
10.10.1	Account Creation - Template	This report provides a listing of newly created Information System Accounts. This report may (and should) be focused based on the Network Domain of interest.
10.10.1	Account Deletion - Template	This report provides a listing of deleted Information System Accounts. This report may (and should) be focused based on the Network Domain of interest.\n
10.10.1	Authorization Changes - Template	This report provides a listing of modified Information System Accounts. This report may (and should) be focused based on the Network Domain of interest.
10.10.1	Changes to Development Machines	This report lists changes made to development systems categorized as a Regulated systems.
10.10.1	Device and OS Configuration Changes	This report provides a listing (sorted by Asset) of configuration modifications to Assets in your Network Domains.
10.10.1	Operating System Changes	This report lists changes made to operating systems of Governed systems.
10.10.1	Operating System Configuration Modifications	This report will show all OS configuration changes made to Regulated systems.
10.10.1	Password Changes	This report provides a list of password changes on Network Domain categorized assets. The results are sorted by asset. This report can (and should) be focused based on the Network Domain of interest.
10.10.2	Account Lockouts by System	This report will show all the account lockouts on Governed Assets organized by system.
10.10.2	Account Lockouts by User	This report will show all the account lockouts on Governed Assets organized by user.
10.10.2	After Hours Systems Access by System	This report shows all the systems that were accessed sorted by user after normal business hours.
10.10.2	After Hours Systems Access by User	This report shows all the systems that were accessed sorted by user after normal business hours.

10.10.2	After-Hours Logins to Sensitive Systems	This report provides a listing of after-hours login attempts which target systems categorized as sensitive by Asset. This report may be focused based on the Network Domain of interest.
10.10.2	Database Access - All	This report shows all authentication events on databases.
10.10.2	Failed Database Access	This report shows all failed attempts to access databases.
10.10.2	File Modifications on Assets	This report will show all file modifications on systems in the last 24 hours as reported by a file integrity application.
10.10.2	Non-Secured Access of Assets from External System	This report shows the authentications from non-protected sources to systems.
10.10.2	Number of Successful User Logins	This report provides a listing of users with successful logins by Asset. The users are sorted by the number of attempts in a decreasing order. This report may (and should) be focused based on the Network Domain of interest.
10.10.2	Number of Unsuccessful User Logins	This report provides a listing of users with unsuccessful login attempts. The users are sorted by the number of attempts in a decreasing order. This report may (and should) be focused based on the Network Domain of interest.
10.10.2	Successful Brute Force Logins	This report provides a listing of events categorized by ArcSight as probable successful brute force login attempts. This report may (and should) be focused based on the Network Domain of interest.
10.10.2	Top 10 Unsuccessful User Logins	This report provides a chart showing the top 10 users with unsuccessful login attempts. This report may (and should) be focused based on the Network Domain of interest.
10.10.2	Unsuccessful User	This report provides a listing of unsuccessful user login attempts. This report may (and should) be focused based on the Network Domain of interest.
10.10.2	User Logins and Logouts	This report provides a listing of user logins and logouts by Asset. This report may (and should) be focused based on the Network Domain of interest.
10.10.2	VPN Access Report	This report provides an overview of access via VPN into your Network Domains.\n
10.10.2	VPN Access Report by Target Asset	This report provides a listing of VPN access events which target the various Network Domains. This report may (and should) be focused based on the Network Domain of interest.
10.10.3	Audit Log Cleared	Report to show all events where an audit log was cleared from a host.
10.10.4	Administrative Logins and Logouts	This report provides a listing of administrative logins and logouts by Asset. This report may (and should) be focused based on the Network Domain of interest.
10.10.4	Administrator Actions - All	This report lists all actions taken by an administrative user.
10.10.4	Number of Successful Administrative Logins	This report provides a listing of administrative users with successful logins by Asset. The administrative users are sorted by the number of attempts in a decreasing order. This report may (and should) be focused based on the Network Domain of interest.

10.10.4	Number of Unsuccessful Administrative Logins	This report provides a listing of administrative users with unsuccessful login attempts. The administrative users are sorted by the number of attempts in a decreasing order. This report may (and should) be focused based on the Network Domain of interest.
10.10.4	Top 10 Unsuccessful Administrative Logins	This report provides a chart showing the top 10 administrative users with unsuccessful login attempts. This report may (and should) be focused based on the Network Domain of interest.
10.10.4	Unsuccessful Administrative Logins by Asset	This report provides a listing of unsuccessful administrative login attempts. This report may (and should) be focused based on the Network Domain of interest.
10.10.5	Fault Logs	Fault Logging report.
10.10.6	Agents Reporting Inaccurate Times	This report will display all agent detect time error events.
10.2.2	Attacks and Suspicious Activity Targeting Third-Party Asset	Report to show all attacks and suspicious activity where the target was an asset in the Third-Parties asset category. Default time window: Last 24 hours.
10.2.3	Changes to Third-Party	Report to show changes made to applications on third party resources.
10.3.1	Resource Exhaustion Detected	Report on resources reaching their upper end of utilization (for capacity management and planning purposes).
10.4.1	Malicious Code Detected	Report of incidents where malicious code was detected based on the referenced filter's criteria.
10.4.1	Trojan Code Activity	This report shows all trojan activity.
10.4.1	Virus Summary	This report will show a summary of viruses detected on systems sorted by virus.
10.4.1	Virus Summary by Hosts	This report will show a summary of viruses detected on systems sorted by host.
10.6	Device Logging Review	This report shows the different products that are logging to ArcSight ESM.
10.6.1	Firewall Open Port Review	This report should be used to review the traffic that is being passed by the firewalls around the organization.
10.8.1	Information Interception	This report shows events that represent a possible interception of data
10.8.4	Outbound IM Traffic	This report shows outbound IM traffic.
10.8.5	Vulnerable Business Information Systems	This report shows the business information systems that have vulnerabilities.

10.9.3	Attacks and Suspicious Activity Targeting Public-Facing Assets	This report shows all the attacks and suspicious attacks where the target asset belonged to the Public-Facing asset category.
10.9.3	Attacks and Suspicious Activity from Public-Facing Assets	This report shows all the attacks and suspicious attacks where the source asset belonged to the Public-Facing asset category.
10.9.3	Events Targeting Public-Facing and Production Assets	This report provides a listing of hostile or suspicious traffic which targets the assets categorized as public-facing or production.

Section 10 Trends

Section	Trends	Description
10.1.1	System Restarted at Unscheduled Time	Trend to capture and report events where a system was restarted outside of the standard maintenance window as defined by the referenced filter.
10.1.2	Firewall Configuration Modifications	Trend to capture and report on all firewall modification changes recorded.
10.1.2	Unscheduled Change in Status of Service	Trend to capture and report on events where a change in status of a service occurred outside of the maintenance window.
10.1.4	Attacks from Production Targeting Development	Trend to capture and report on suspicious or hostile traffic from production facilities to development segments.
10.10.2	User Name and IP Address Association	Trend to query user names-to-IP address associations by recording the contents of the 'User Name and IP Address Association' session list.
10.2.2	Attacks and Suspicious Activity from Third-Party Assets	Trend to capture and report on all attacks and suspicious activity where the source was an asset in the Third-Parties asset category.
10.9.3	Attacks Targeting Email Systems	Trend to capture and report on all the attacks targeting email systems.
10.4.1	Failed Anti-Virus Updates	Trend to capture and report on all the failed AV updates on systems.
10.4.1	Infected VPN Remote Host Found	Trend to capture and report on all cases of virus incidents over a VPN connection.
10.9.3	External Logins to Public Facing Systems	Trend to capture and report on a listing of user authentications on external facing systems from external sources.

Section 10 Session Lists

Session List	Description
User Name and IP Address Association	A session list to associate user logins to ip addresses. This list is fed by OS and VPN logins and can be referenced in order to correlate IP address to user name information. This Session List is available from the following location: All Session Lists/ArcSight Solutions/Compliance Insight Package/

ISO 11: Access Control

Section 11 of ISO addresses controls used around access to systems. Areas of interest entail all aspects of logical access including user names, passwords, traversal of various types of network traffic between different functional segments of the network.

Use Cases

To address section 11 requirements, the SOX4 solution provides the following use cases.

Role-Based Access Monitoring

Section 11.1 of the ISO standard states that a policy should be in place to implement access controls based on business and security requirements. CIP for SOX4 provides a use case that uses an active list to store user names and their roles from manual entries, or exported directly from Active Directory. Rules then use entries to this list to detect users who attempt to gain access to a database, domain controller, or other privileged access account whose user roles do not grant them access privileges to these assets.

These rules and the policy definition filter provide a foundation for dashboards, active channels, and reports that monitor privileged user access attempts. Three trends track privileged access attempts over time, and populate identity-based access violation reports.

User Management

Formal procedures should be in place to control the allocation of access rights to information and services. Special attention should be given to the need to control the allocation of privileged access rights that allow users to override system controls. The SOX4 solution addresses these issues by implementing filters, data monitors, rules, active lists, and reports to monitor cases where default vendor accounts, default vendor accounts, and former employee accounts are used. Changes to privileged accounts are also monitored.

Authorization Changes

Authorization changes should be monitored in order to ensure that changes are approved. Changes implemented without approval could indicate an attack on the system. The SOX4 solution provides reports that show changes to access rights to effectively monitor appropriate authorization changes.

Password Policy Monitoring

Passwords are a common means of verifying a user's identity, and organizations should have policies in place to ensure effective and secure password management. The Sarbanes-Oxley section 11 reports show when default passwords are not changed and default vendor accounts are used.

Privileged Account Monitoring

It is necessary to regularly review users' access rights to maintain effective control over access to data and information services. Changes to privileged accounts should be logged for periodic review. The solution provides dashboards, data monitors, rules, rules and filters that enable monitoring and logging of privileged account activity.

Network Service Monitoring

Users and assets should only be provided with access to the services that they have been specifically authorized to use. Use of network services is monitored in many ways by the solution, including reporting on disallowed port usage and the use of insecure services.

Firewall Policy Monitoring

Traffic blocked at the firewall level is tracked to and from classified assets in order to promote effective network access control.

Network Routing Supervision

Changes to network routing should be monitored in order to maintain the security and availability of information systems. A report is enabled which show all router configuration modifications.

Network Policy Monitoring

Insecure and unauthorized use of network services should be restricted. This control is especially important for connections to sensitive or critical networks. Active channels, reports, data monitors, and

filters are provided to monitor suspicious transmissions, insecure services, and transmissions between zones.

Remote Access (VPN) Monitoring

Significant risks to corporate information systems arise due to the use of remote access and wireless for mobile computing. The solution provides active lists, filters, and reports to signal potential problems or attacks against VPN and wireless systems.

Segregation of Networks

A common methodology for controlling security in large networks is to divide them into separate logical domains (zone) bases on function or criticality. The SOX4 solution provides reports which indicate traffic between zones and access to particular machines such as development machines, etc.

Devices

The following devices supply the events that apply to ISO section 11.

Use Case	Device	Device Configuration Required
•Identity Based Access Control	•OS •Database •Application	None
•User Management •Authorization changes •Password policy monitoring	•OS •IAM •Application •Database	None
•Privileged account monitoring	•OS •IAM •VPN •Application •Database	None
•Network Service Monitoring	•Router •Firewall •NIDS/NIPS	None
•Firewall policy monitoring	•Firewall	None
•Network routing supervision	•Router •Switch	None
•Remote access (VPN) monitoring	•VPN	None
•Segregation of networks •Network policy monitoring	•Router •Firewall •NIDS/NIPS	None

Configuration

In addition to the asset modeling and configurations to the common resources described in “Configure the Sarbanes-Oxley 4 Solution”, the following resources should be configured as necessary to comply with your policies.

Section 11 Resources

This section lists all the resources that address the information systems acquisition development and maintenance requirements of ISO section 4.

Resource Type	Resource Name	What to Configure
Filter	Security Service Stopped or Paused	Optionally you can add more security services to the filter to not only capture the services already configured in this filter.
Filter	Security Service Stopped or Paused	Optionally you can add more security services to the filter to not only capture the services already configured in this filter.
Filter	Former Employees	Nothing to be configured here. The configuration is done via the Active List.
Filter	Default Vendor Account Used	Nothing to be configured here. The configuration is done via the Active List.
Filter	Default Password not Changed	This filter is not meant to be used for configuration.
Filter	Insecure Services	This filter should be configured with services that are considered insecure, such as telnet or FTP where traffic is transmitted in plain text.
Active List	Privileged User Group	This active list should be configured with all the privileged user groups in the organization.
Active List	Former Employees	A list of former employees needs to be entered here. Make sure you update this on a regular basis, as soon as an employee leaves the company.

Active List	User Roles	Configure this active list with the User Roles. Each entry in the Active List has a User Name value and User Roles value. A User Name value contains a single value while the User Roles value can contain one or more user roles separated by the pipe () delimiter as shown by the following example entry: ttaylor, Sales Financial In addition, the last role listed must have a trailing pipe () delimiter. User Role values should align with the Network Domains asset categories of Sarbanes-Oxley systems. For example, users who roles require access to systems categorized as Financial must have role Financial in the active list. You may need to add additional asset categories to Network Domains. This active list can also be used for defining the database administration roles for users. For more information about populating this active list from an Active Directory, see “User-Role Active List”.
Filter	Successful User Login	Not used for configuration purposes
Active List	Users with Default Passwords	Not used for configuration purposes
Active List	Default Vendor Accounts	Configure this active list with all the default vendor accounts that are known to be used in your environment.
Active List	Allowed Ports	Active list of all permissible destination ports, such as all permissible services. This active list should be populated by the end-user according to site policy.
Active List	Privileged Users Group	Not used for configuration purposes.
Active List	System with Insecure Configurations Active List	Configure this filter with the hours that reflect after hours for your organization.
Filter	After Hours	Configure this filter with the hours that reflect after hours for your organization.
Filter	Policy Definition	Configure this filter with the user roles targeting categorized assets. It will evaluate to true when the asset category of the target does not match any of the user's roles as defined in the User Roles active list. A precondition is that the attacker user name or target user name event fields must be populated, which can be disabled if a tighter policy is desired. For more information, see “Policy Definition Filter”
Filter	DBA Role	Configure this filter to reflect the privileged database administration (dba) for your environment. For more information, see “DBA Role” on page 52.

Rule	Database Privilege Violation	Configure this rule to reflect your privileged database administration account.
Rule	Privileged Access Attempt Detected	Configure this rule to reflect your privileged system administration account.
Rule	Unauthorized Admin Access to Domain Controller	Configure this rule to reflect your privileged system administration account.

Section 11 Active Lists

Active List	Description
Administrative Accounts	This Active List should be populated with the usernames that have administrative privileges in your domain. Admins (those responsible for managing administrative users) populate this list manually whenever a new administrative user is added. Entries to this list are read by reports supplied in the Compliance Insight Packages, but the list can also be added to or referenced in new content built around the provided infrastructure.
Allowed Ports	Active list of all permissible destination ports, ie, all permissible services. This active list should be populated by the end-user according to site policy.
Default Vendor Accounts	This is a static Active List that contains the default user account names for various vendors. This list should be configured at set-up time with existing vendor user account names, and updated as necessary on an ongoing basis.
Former Employees	This Active List contains user accounts of former employees. User accounts in this Active List are retained indefinitely.
Privileged User Groups	This active list is used to define user groups with elevated privileges.
Stale Accounts	Active list to maintain user names that have not shown any log-on activity in the last 6 months. Using 183 days to account for leap years.
Systems with Insecure Configurations	Active list of all hosts with open ports which connote the presence of an inherently insecure network service, ie, telnet, FTP, etc. This list should be populated by the end-user according to site policy.
Users with Default Passwords	Holding area for account IDs that are up to 2 days old. The list is populated as an action to a new user ID being created.
User Roles	This Active List contains the mappings of users to their roles. It can be used to monitor role-based access.

Section 11 Session Lists

Session List	Description
User Name and IP Address Association	A session list to associate user logins to ip addresses. This list is fed by OS and VPN logins and can be referenced in order to correlate IP address to user name information. This Session List is available from the following location: All Session Lists/ArcSight Solutions/Compliance Insight Package/

Section 11 Active Channels

Active Channel	Description
Access Right Removed	Channel to show a 'live' feed of events reflecting a removal of a user's access privileges. Manager Receipt Time is used as the time-stamp of choice to retain the real-time nature of the channel.
Account Lockouts	Channel to show events where a rule fired to lock out a user ID.
Database Privilege Violation	Active channel to show a live feed of events where a violation of database privileges was detected.
Direct Root or Administrator Access	Active channel to show events where there was a direct log-on as root or administrator.
Identity Based Access Violation	Active channel to show real time feed of events where a role based access violation is detected by the system.
Insecure Services Activity	Channel to show a live feed of events where the traffic was using an inherently insecure service. Such services are detailed in the referenced filter.
Log-On with Default Vendor Account	Channel to show a 'live' feed of events reflecting access by using vendor provided default credentials. This is based on the related rule firing. Manager Receipt Time is used as the time-stamp of choice to retain the real-time nature of the channel.
Login Attempts	Active channel to show a real-time feed of events where a login attempt was made.
Privileged Account Changed	Channel to show a 'live' feed of events reflecting alteration of privileges. This is based on the related rule firing. Manager Receipt Time is used as the time-stamp of choice to retain the real-time nature of the channel.
Security Services Stopped or Paused	Channel to show events where a security service (as named in the filter tab) is stopped on a system.
Unauthorized Admin Access to Domain Controller	This channel shows events where a user without the sysadmin role attempted to access a domain controller.

Section 11 Dashboards

Section	Dashboard	Description
11.1.1	Database Privilege Violation	Dashboard showing views of database privilege violations in which the user is not specified to have dba rights.
11.1.1	Identity Based Access Monitoring	Dashboard showing violations in which the user does not have the defined role to access an asset.
11.1.1	Unauthorized Admin Access to Domain Controller	Dashbboard showing events where users not designated as administrators attempt to use the administrator accounts on domain controllers.
11.2	User Access and Password Management	Dashboard showing all user access related and password/account name management related activities.
11.4.1	Insecure Services	Dashboard showing activity involving inherently insecure services.
11.4.2	Potentially Problematic Remote Access	Dashboard showing privileged access on remote connections, or remote access to systems with insecure configuration.
11.4.5	Segregation in Networks	Dashboard showing activity where traffic is traversing boundaries of different functional network segments.
11.5.1	Account Lockouts	Dashboard showing activity where a user account has been locked out.
11.5.2	General Login Attempts	Dashboard showing user login activity.
11.5.2	Unsuccessful Login Attempts	Dashboard showing last 20 failed user and administrative logins.
11.7.1	Suspicious Events Targeting Wireless Assets	Dashboard showing suspicious events targeting wireless assets.
11.7.1	Suspicious Events from Wireless Assets	Dashboard showing suspicious events from wireless assets.
11.7.2	Security Services	Dashboard showing all security services and their status related events.

Section 11 Data Monitors

Section	Data Monitor	Description	Config?
11.1.1	Access Path	Shows a graphical view of Identity Based Access Violations with a mapping of User Name to Target IP Address and Target Asset Category.This will allow analysts to quickly view which users are accessing systems to which they do not have the assigned roles required for access.	User Role Active List
11.1.1	Database Privilege Violation	Data monitor to show the access privilege violations on databases with mention of the violator, the privileged user ID used, the instance of the database and the host name where this instance was running.	N

11.1.1	Graph View of Unauthorized Admin Access to Domain Controller	Data monitor to show graphical view of unauthorized administrative access to a domain controller. The graph shows the violator's user name, the IP address of the domain controller, and the user name given to the administrator.	N
11.1.1	Top 20 Database Instances with Access Privilege Violation	Data monitor to show the top 20 instances of the databases that had access privilege violations.	N
11.1.1	Top 20 Database Privilege Access Violation	Data monitor to show top 20 users who were flagged for database access privilege violation.	N
11.1.1	Top 20 Violators of Admin Access to Domain Controllers	Data monitor to show top 20 violators of administrative access to domain controllers, grouped by the user names.	N
11.1.1	Top Violators	Data monitor top user name and role violations.	N
11.1.1	Unauthorized Admin Access to Domain Controller	Data monitor to show last 10 unauthorized attempts by users to log in to domain controllers as an administrator.	.
11.2.1	Former Employees Access Attempts	Data monitor to show access attempts with a User ID that was already placed in the Notice-Given active list. i.e. employees who have been served a termination of services notice.	Filter Former Employees
11.2.3	Default Vendor Account Used	Display log-on events where user has attempted to log-on to a system with vendor supplied default User IDs.	Filter Default Vendor Account Used
11.2.3	Vendor Default Log- On Credentials Used	Data monitor to display log-on attempts with default credentials supplied by a product vendor.	Default Password not Changed
11.2.4	Privileged Account	Display events where authorization/access changes have been made to a privileged user's account.	N
11.4.1	Top Suspicious Transmissions	Data monitor to show top 10 communications using inherently insecure services. Such services are listed in the referenced filter.	Filter Insecure Services
11.4.1	Top Suspicious Transmissions Between Zones	Data monitor to show top 10 communications, sorted by attacker and target zones, using inherently insecure services. Such services are listed in the referenced filter.	Filter Insecure Services

11.4.1	Weak Services Communication by Address	Data monitor to show a graph view of insecure traffic from a particular attacker address to a target address.	Filter Insecure Services
11.4.1	Weak Services Communication by Zone	Data monitor to show a graph view of insecure traffic from a particular attacker zone to a target zone.	Filter Insecure Services
11.4.2	Privileged Access on a Remote Connection	Data Monitor to display an event graph anytime a connection is reported by a VPN device, where the user name belongs to a privileged account.	Active List Privileged User Group
11.4.2	Remote Access to Systems with Insecure Configuration	Data Monitor to display an event graph of access attempts via a VPN gateway to system known for running an insecure service. Such services are listed in the referenced Active List.	N
11.4.5	Traffic Between Zones- Protocol	Shows Target Ports and Target Zones names for all traffic that was permitted passage by a firewall.	N
11.5.1	Account Lockouts	Data monitor to display events when an account has been locked out; triggered by a related rule firing.	N
11.5.2	Last 20 Login Attempts	Data monitor to show in real-time the last 20 login attempts detected by the system.	N
11.5.2	Last 20 Unsuccessful Administrative Logins	Data monitor to show in real-time when an administrative level user id is used in an unsuccessful login event. Last 20 such events are displayed.	N
11.5.2	Last 20 Unsuccessful User Logins	Data monitor to show the last 20 unsuccessful login attempts in real- time.	N
11.5.2	Top User Login Activity	Data monitor to show the top 20 users attempting to login to a system.	N
11.7.1	Last 10 Suspicious Events from Wireless Assets	This data monitor shows, in real- time, the last 10 suspicious events originating from wireless assets.	N
11.7.1	Last 10 Suspicious Events Targeting Wireless Assets	This data monitor shows, in real- time, the last 10 suspicious events targeting wireless assets.	N
11.7.1	Suspicious Events from Wireless Assets (Target Ports)	Data monitor to show, in real-time, the top 10 ports targeted by suspicious traffic originating on wireless assets.	N

11.7.1	Suspicious Events Targeting Wireless Assets (Target Port)	Data monitor to show, in real-time, the top 10 ports targeted by suspicious traffic destined to wireless assets.	N
11.7.2	Last 20 Security Service Stopped or Paused Events	This data monitor shows the last 20 security service stopped paused or disabled events.	Filter Security Service Stopped or Paused
11.7.2	Security Service Stopped or Paused	This shows the last state of systems that have had security services stopped or paused.	Filter Security Service Stopped or Paused

Section 11 Filters

Section	Filters	Description
11.1.1	Access Removed	Filter to select events where any access right to a host is removed.
11.1.1	Database Privilege Violation	Filter to select events where the named rule fires.
11.1.1	Identity Based Access Violation	Filter to select events when the named rule fires.
11.1.1	Unauthorized Admin Access to Domain Controller	Filter to select events where a rule called 'Unauthorized Admin Access to Domain Controller' has fired.
11.2.1	Former Employees	Checking in the referenced active list to see whether an employee has been terminated.
11.2.2	Default Password not Changed	Selects events where users did not change their default password within the prescribed duration from the creation of the account. The time period is determined by the TTL in the referenced Active List.
11.2.3	Default Vendor Account Used	Filter in events where system access with vendor supplied accounts is attempted.
11.2.4	Privileged Account Changed	Filter to select events where a privileged account, as defined by the referenced Active List, is changed, or removed.
11.2.4	Stale Account Log-on	Filter to select events showing a log-on attempt by a user name whose account has been inactive for the last 6 months.
11.4.1	Insecure Services	Filter to select events based on inherently insecure services.
11.4.2	Privileged Access on a Remote Connection	Filter to select events where a connection is reported by a VPN device, and the user name belongs to a privileged account.

11.4.2	Remote Access to Systems with Insecure Configuration	Filter to select events showing access attempts via a VPN gateway to system known for running an insecure service. Such services are listed in the referenced Active List.
11.4	Suspicious External to Internal Traffic	Filter to select events where suspicious traffic originates from an external network segment and the target is in an internal network segment.
11.4	Suspicious Internal to External Traffic	Filter to select events where suspicious traffic originates from an internal network segment and the target is in an external network segment.
11.5.1	Account Lockout - Correlation	This filter shows the correlated events indicating an account has been locked out.
11.5.3	Direct Root or Administrator Access	Shows all attempts to logon to a system as root or administrator.
11.7.1	Events Targeting Wireless Assets	This filter identifies events of interest that target assets categorized in the Wireless Network Domain.
11.7.1	Events from Wireless Assets	This filter identifies events of interest generated by assets categorized in the Wireless Network Domain.
11.7.2	Security Service Stopped or Paused	Filter to select events where any of the named security services are stopped on any system. Refer to the Filter tab for the list of such services.

Section 11 Rules

Section	Rule	Description	Config?
11.1.1	Access Rights Removed	Rule to catch the event where: 1). Either a user is removed from a host, or 2). User's authentication privileges are modified.	N
11.1.1	Database Privilege Violation	Rule triggered by events where a privileged access to a database was detected where the user was not authorized to do so.	Privileged Database Administration Account for your environment
11.1.1	Identity Based Access	This rule will fire when the asset category of the target does not match any of the user's roles as defined in the User Roles active list.	Policy Definition filter
11.1.1	Privileged Access Attempt Detected	Rule to fire whenever an attempt to log in as the administrator is detected by a user who does not have an administrative role assigned.	Configure this rule to reflect your privileged system administration account.
11.1.1	Unauthorized Admin Access to Domain Controller	This rule will detect any non- sysadmin role user attempting to log into a domain controller, over the network, with sysadmin privileges. Instead of using user names to make decisions, users' roles are used to determine whether or not the access in question is permitted.	Configure this rule to reflect your privileged system administration account.

11.2.1	Former Employee User Account Access Attempt	This rule detects any authentication event, whether failed or successful, where the username has been placed on the "Former Employees" Active List. This rule creates a case in the ArcSight Solutions folder in the case tree for each unique user name that is attempted.	Active List: Former Employees
11.2.1	Inactive User Account Detected	This rule will fire every time an entry ages out of the stale user accounts active list.	N
11.2.1	Same User Using Different User Names to Log-on	Rule to look for people connecting with two different user names.	N
11.2.1	User Account Deletion	This rule detects user account deletions from systems. When triggered, the rule adds as well as deletes users from the appropriate active lists.	N
11.2.1	User Logged in - Removed from Stale Accounts List	This rule is used to only remove an active user name from the stale accounts active list.	N
11.2.1	User Logged in From Two Locations	Someone is using the same user name to log in from two different zones. This might indicate user name sharing among people.	Optional: Successful User Login filter.
11.2.1	User Logged Out - Added to Stale Accounts List	This rule is used to only populate the stale accounts active list.	N
11.2.3	Default Password not Changed	Rule fires when an entry expires out of the referenced Active List, signifying that the new (default) password was not changed within the prescribed time. Time limit is defined by the TTL in the Active List.	Optional: Users with Default Passwords Active List
11.2.3	Default Vendor Account Used	This rule looks for users attempting to access system using default user accounts. Default user accounts are defined in the corresponding filter.	Optional: Default Vendor Accounts Active List
11.2.3	New User Account Created	This rule will fire any time a new account is created. The related user name will be put in an active list to track users with default, i.e. unchanged passwords.	N
11.2.3	User Password Change Detected	Rule to detect when a user's password is changed. This rule will then take the user name off the list where it was kept to track whether or not the default password was changed.	N
11.2.4	Privileged Account Changed	This rule fires whenever an access/authorization change is made to a privileged user's account. A case is created for each such incident.	N

11.4.1	Disallowed Port Access	This rule is triggered when traffic to a target port that is not on the "Allowed Ports" Active List occurs.	Optional: Allowed Ports Active List
11.4.1	Insecure Services Use Detected	This rule detects when insecure protocols, such as Telnet or RSH, are used. When triggered, it adds an entry to the "Systems with Insecure Configurations" Active List.	N
11.4.2	Privileged Access on a Remote Connection	NIST AC 17 This rule will fire anytime any connection is reported by a VPN device, where the user name belongs to a privileged account.	Optional: Privileged Users Group Active List
11.4.2	Remote Access to Systems with Insecure Configuration	NIST AC 17 Rule to detect access attempts via a VPN gateway to system known for running an insecure service. Such services are listed in the referenced Active List.	Optional: System with Insecure Configurations Active List
11.4.2	VPN Login Recorded to Session List	This rule will create a session list entry with the user name and IP address allocated, when a user is successfully authenticated by a VPN concentrator. The sole purpose of this rule is to populate the session list.	N
11.4.2	VPN Session Terminated - Cleared from Session List	This rule will clear a session list entry with the user name and IP address allocated, when a user logs out of a VPN concentrator. The sole purpose of this rule is to clear the session list.	N
11.4.6	Disallowed Port Access	This rule is triggered when traffic to a target port that is not on the "Allowed Ports" Active List occurs.	Active List: Allowed Ports
11.5.1	Account Lockout	This Rule detects account lockouts. This activity is suspicious.	N
11.5.6	After-Hours Login to Sensitive Systems	This rule identifies after-hours login attempts on systems that have been categorized as highly- critical. Such hours are defined in the referenced filter.	Y: After Hours filter
11.7.1	Generate Case for Attack Against Remote Assets	This rule generates cases for attacks against remote assets.	N
11.7.2	Security Software Stopped or Paused	This rule is triggered when a Windows security software service has been disabled.	N

Section 11 Reports

Section	Report	Description
11.1.1	Account Activity by User Name	Report to show all activity of a particular user. The user name is a required parameter for this report.
11.1.1	Database Privilege Violation	Report to show all database privileged access violations in a tabular form. The violator's name, privileged user ID, database instance are the primary fields of the table displayed.
11.1.1	Database Privilege Violations Overview	Report to show an overview of database access privilege violations. There are two charts in this report showing information as follows: 1). Names, and the associated count, of the violators attempting to access a database with a privilege that they are not authorized to use, and 2). Names of the databases, ie. instance names, that saw such violations along with the associated count.
11.1.1	Identity Based Access Violation by Top Violators	This report shows the most frequent violators of the Identity Based Access Violation Rule.
11.1.1	Identity Based Access Violations Overview	An overview report to show the following pieces of identity based access violations: 1). The roles that were violated with an associated count, and 2). The users that committed violations with an associated count.
11.1.1	Removal of Access Rights	Report removal of access rights from a host resource. Removal could mean that either the user was removed from the system, or the privileges related to that ID were modified.
11.2.1	Former Employee Account Access Attempt	Report to list all log-in activity from a former employee. The aforesaid employees' list is maintained as the referenced active list.
11.2.1	Inactive User Account Detected	Report to show all user names that were aged out of the stale accounts active list.
11.2.1	Same User Using Different User Names	Report to show attempts by the same user to log-on using different user ids.
11.2.1	User Account Deletion	Report to list removal of user accounts from a system.
11.2.1	User Logged in from Two Locations	Report to show log-in attempts with the same user name from two different locations.

11.2.3	Default Password Not Changed - Policy Violation	Reports on user IDs that did not change their default password within the prescribed duration from the creation of the account. The time period is determined by the TTL in the referenced Active List.
11.2.3	Default Vendor Account Used - Policy Violation	Report to show if a vendor supplied user account is still being used by user to log- on.
11.2.4	Privileged Account Changed	Report to list the number of times a privileged user's access privileges were altered. This report depends on the referenced rule's firing.
11.4.1	Blocked Firewall Traffic from Assets - Template	This report provides a listing (sorted by target Asset) of the blocked outbound firewall traffic originating from Assets in your Network Domains. This report may (and should) be focused based on the Network Domain of interest.
11.4.1	Blocked Firewall Traffic to Assets - Template	This report provides a listing (sorted by target Asset) of the blocked inbound firewall traffic directed at Assets in your Network Domains. This report may (and should) be focused based on the Network Domain of interest.
11.4.5	Disallowed Ports	This report shows traffic that should not be seen per the allowed ports active list.
11.4.1	Insecure Transmissions	Report to list all traffic deemed as inherently insecure. All such traffic is listed in the referenced filter.
11.4.1	Network Routing Changes	This report will show all router configuration modifications.
11.4.1	Policy Violations - Template	This report provides a listing of events categorized by ArcSight as policy violations which target the various Network Domains by Asset. This report may (and should) be focused based on the Network Domain of interest.
11.4.1	Services by Asset - Template	This report will show all successful access attempts.
11.4.1	Traffic from Dark Address Space	This report will show all traffic from a dark address range targeting systems. This should be considered very suspicious.

11.4.1	Traffic from External to Internal Protected Domain	This report provides a listing of all traffic coming from assets categorized as external which target assets categorized as internal.
11.4.1	Traffic from Internal to External Protected Domain	This report provides a listing of all traffic events coming from assets categorized as internal which target assets categorized as external.
11.4.1	Traffic to Dark Address Space	This report will show all traffic directed to a dark address range. This should be considered very suspicious.
11.4.2	Privileged Access on a Remote Connection	Report to show all connections reported by a VPN device, where the user name belongs to a privileged account.
11.4.2	Remote Access to Systems with Insecure Configuration	Report to show all access attempts via a VPN gateway to system known for running an insecure service.
11.4.5	Access to Development Machines	This report shows all access attempts to systems considered to be Development systems.
11.4.5	Traffic Between Zones - Protocol	This report is to review the different protocols passing between zones.

Section 11 Queries

Section	Query	Description
11.1.1	Account Activity by User Name	Query to show all activity of a particular user. The user name is a required parameter for This query.
11.1.1	Database Privilege Violation by Database Name	Query based on trend to capture and Query on events where an privilege violation was sensed on access to a database. The information is sorted by the databases' names.Trend referenced: Database Privilege Violation.
11.1.1	Database Privilege Violation by User	Query based on trend to capture and Query on events where an privilege violation was sensed on access to a database. The information is sorted by users' names.Trend referenced: Database Privilege Violation.

11.1.1	Removal of Access Rights	Query removal of access rights from a host resource. Removal could mean that either the user was removed from the system, or the privileges related to that ID were modified.
11.1.1	Database Privilege Violation	Query to collect all events pertaining to the Database Privilege Violation use-case.
11.1.1	Identity Based Access Violation by Top Violators	Query to capture top identity based role violating users by their names.
11.2.1	Inactive User Account Detected	Query to show all user names that were aged out of the stale accounts active list.
11.2.1	Same User Using Different User Names	Query to show attempts by the same user to log-on using different user ids.
11.2.1	User Account Deletion	Query to list removal of user accounts from a system.
11.2.1	User Logged in from Two Locations	Query to show log-in attempts with the same user name from two different locations.
11.2.1	Former Employee Account Access Attempt	Query to list all log-in activity from a former employee. The aforesaid employees' list is maintained as the referenced active list.
11.2.3	Default Password Not Changed - Policy Violation	Querys on user IDs that did not change their default password within the prescribed duration from the creation of the account. The time period is determined by the TTL in the referenced Active List.
11.2.3	Default Vendor Account Used - Policy Violation	Query to show if a vendor supplied user account is still being used by user to log-on.
11.2.4	Privileged Account Changed	Query to list the number of times a privileged user's access privileges were altered. This query depends on the referenced rule's firing.
11.4.1	Blocked Firewall Traffic from Assets - Template	This query provides a listing (sorted by target Asset) of the blocked outbound firewall traffic originating from Assets in your Network Domains. This query may (and should) be focused based on the Network Domain of interest.
11.4.1	Blocked Firewall Traffic to Assets - Template	This query provides a listing (sorted by target Asset) of the blocked inbound firewall traffic directed at Assets in your Network Domains. This query may (and should) be focused based on the Network Domain of interest.
11.4.1	Insecure Transmissions	Query to list all traffic deemed as inherently insecure. All such traffic is listed in the referenced filter.
11.4.1	Network Routing Changes	This query will show all router configuration modifications.
11.4.1	Policy Violations - Template	This query provides a listing of events categorized by ArcSight as policy violations which target the various Network Domains by Asset. This query may (and should) be focused based on the Network Domain of interest.

11.4.1	Services by Asset - Template	This query will show all successful access attempts.
11.4.1	Traffic from Dark Address Space	This query will show all traffic from a dark address range targeting systems. This should be considered very suspicious.
11.4.1	Traffic from External to Internal Protected Domain	This query provides a listing of all traffic coming from assets categorized as external which target assets categorized as internal.
11.4.1	Traffic from Internal to External Protected Domain	This query provides a listing of all traffic events coming from assets categorized as internal which target assets categorized as external.
11.4.1	Traffic to Dark Address Space	This query will show all traffic directed to a dark address range. This should be considered very suspicious.
11.4.2	VPN Access Query	This query provides an overview of access via VPN into your Network Domains.
11.4.2	VPN Access Query by Target Asset	This query provides a listing of VPN access events which target the various Network Domains. This query may (and should) be focused based on the Network Domain of interest.
11.4.2	Privileged Access on a Remote Connection	Query to show all connections Queried by a VPN device, where the user name belongs to a privileged account.
11.4.2	Remote Access to Systems with Insecure Configuration	Query to show all access attempts via a VPN gateway to system known for running an insecure service.
11.4.5	Disallowed Ports	This query shows traffic that should not be seen per the allowed ports active list.
11.4.5	Access to Development Machines	This query shows all access attempts to systems considered to be Development systems.
11.4.5	Traffic Between Zones - Protocol	This query is to review the different protocols passing between zones.
11.5.3	Systems Accessed as Root or Administrator	This query shows all systems that users have tried to access directly as root or administrator.
11.7.1	Top Wireless Events - Suspicious Activity	This query provides an overview of hostile activity targeting your Wireless Network Domain, broken down by Asset.

Section 11 Trends

Section	Trend	Description
11.1.1	Database Privilege Violation	Trend to capture and report on all events pertaining to the Database Privilege Violation use-case.

11.1.1	Identity Based Access Violation by Top Roles	Report to show all the identity based access violations observed. The output is sorted by the roles, which are analogous to domains, to show which roles saw how many violations.
11.1.1	Identity Based Access Violation by Top Violators	This trend tracks the most frequent violators of the Identity Based Access Violation Rule.
11.2.1	Former Employee Account Access Attempt	Trend to capture and report on all log-in activity from a former employee. The aforesaid employees' list is maintained as the referenced active list.\n
11.2.4	Privileged Account Changed	Trend to capture and report on the number of times a privileged user's access privileges were altered. This report depends on the referenced rule's firing.

ISO 12: Information System Acquisition Development and Maintenance

Section 12 of ISO addresses controls used around acquisition, development and maintenance of information systems. Areas of interest addressed include aspects of safe functioning of the systems such as verifying the validity of input data, safeguards against malicious data input.

Use Cases

To address section 12 requirements, the SOX4 solution provides the following use cases.

Certificate Management

Cryptographic controls should be in place to protect the confidentiality, integrity, and availability of information. The SOX4 solution provides filters, reports, and active channels on use of expired or invalid certificates, which can indicate problems or compromises of cryptographic controls.

Attack Monitoring

Validation checks should be incorporated to detect corruption of information through deliberate acts or processing errors. SOX4 addresses this by implementing filters for vulnerability exploits including buffer overflows and overruns, which can cause processing errors in information systems.

Software Installation

Procedures should be in place to control the installation of software on operational systems. If operating systems are configured to detect installations of new applications, SOX4 filters, rules, and reports can indicate this activity.

Information Leak Monitoring

Opportunities for information leakage should be prevented. The risk for information leakage can be mitigated by regular monitoring of personnel and system activities. An active channel is provided to monitor all information leak events in real time.

Systems with Persistent Vulnerabilities

If a machine gets scanned and it exposes HIGH or VERY HIGH severity vulnerabilities, it is considered a policy violation. To indicate this policy violation, the scanned machine will be added to the Systems with Vulnerabilities active list.

This active list has a default time-to-live of 30 days (you can configure this timeout to match your corporate policy). If a machine stays on this list for 30 days, it will expire from the list and triggers the Persistent Vulnerability Detected rule, which indicates this machine has vulnerabilities that were never fixed.

The Systems with Persistent Vulnerabilities report shows a summary of these events.

From a workflow perspective, if a system with a HIGH or VERY HIGH severity vulnerability gets fixed, it should either be manually removed from the Systems with Vulnerabilities active list, or the system should be rescanned before the entry times-out on the active list. If you rely on a scan, a system of rules and active lists determine if the vulnerability has been adequately remedied.

Devices

The following devices supply the events that apply to ISO section 12.

Use Case	Device	Device Configuration Required
Certificate management	• NIDS/NIPS • OS • VPN • Applications	None
Attack monitoring	• NIDS / HIDS	None
Software installation	• OS	Make sure the operating system is configured to detect installations of new applications
Information leak monitoring	• Information Leak Prevention systems	Make sure the ILP device is configured to monitor for critical and confidential documents.
Vulnerability management	• Vulnerability Scanner	None

Configuration Summary

In addition to the asset modeling and configurations to the common resources described in “Configure the Sarbanes-Oxley 4 Solution” on page 31, the following resources should be configured as necessary to comply with your policies.

Resource Type	Resource Name	What to configure
Active List	Systems with Vulnerabilities	This active list has a default time-to-live for entries of 30 days. Modify this entry time-out to match your corporate policy of how long it should take to patch a vulnerability on a machine.
Rule	Exploit of Vulnerability Detected	This rule triggers the action to set event field actions on time window expiration. Depending on how many events trigger this rule, you can adjust the action threshold as needed.

Section 12 Resources

This section lists all the resources that address the information systems acquisition development and maintenance requirements of ISO section 12.

Section 11 Active Lists

Active List	Description	Config?
Systems with Vulnerabilities	Active list to age out the vulnerability timer, so that a rule can fire if a system is still found vulnerable after the prescribed amount of time to remediate.	Optional. Adjust default 30-day timeto- live to match your organization's policies.

Section 12 Active Channels

Active Channel	Description
All Information Leak Events	Channel to show real-time feed of events where the technique reflects information leakage.
Buffer Overflows and Overruns	Channel to show real-time feed of events where buffer overflow type event is detected.
Invalid Data Input	Channel to show a real-time feed of events where an invalid data input is detected.
Invalid or Expired Certificate Presented	Channel to show a real-time feed of events where an attempt to access a resource that presented an invalid/expired certificate was detected.
Vulnerable Assets	Channel to show real-time feed of events that indicate the existence of vulnerabilities in the Development, Test or Operations segments.

Section 12 Dashboards

Section	Dashboard	Description
12.6.1	Vulnerabilities Overview	Dashboard to give overviews of vulnerabilities found, along with vulnerable systems.

Section 12 Data Monitors

Section	Data Monitor	Description
12.6.1	Top 10 Vulnerabilities on Systems	This Data Monitor shows the top 10 vulnerabilities on systems by vulnerability name.
12.6.1	Top Systems with Vulnerabilities	This moving average Data Monitor shows the top 10 systems with vulnerabilities over the last 7 days.

Section 12 Filters

Section	Filter	Description
12.2.1	Invalid Data Input	This filter selects events where invalid data input is detected.
12.2.2	Exploit of Vulnerability	Filter to select events where an attempt at exploiting a vulnerability in an application is detected.
12.3.2	Invalid or Expired Certificate Presented	Filter to select events where an attempt at a resource that presented an invalid/expired certificate was detected.
12.4.1	Traffic to Operations	Filter to select all traffic destined for the operations segment(s) of the network.
12.4.2	Traffic to Test from Others	Filter to select all traffic destined for the test segment(s) of the network, which did not originate from a test segment.
12.4.3	Traffic from Development to Non Development	Filter to select all traffic originating from a development segment of the network that is not destined for a development segment.
12.4.3	Traffic from Others to Development	Filter to select all traffic destined for the development segment(s) of the network that did not originate from within a development segment.
12.5.3	Changes to Operating Systems	Filter to select events where an attempt to modify any component of an operating system is detected.
12.5.4	All Information Leak Events	Filter to select events where the technique reflects information leakage.
12.6.1	Systems with Persistent Vulnerabilities	Filter to select events where an entry has expired its TTL in System with Persistent Vulnerabilities active list.
12.6.1	Vulnerable Assets	Filter to select events that indicate the existence of vulnerabilities in the Development, Test or Operations segments.

Section 12 Rules

Section	Rule	Description	Config?
12.2.1	Multiple Invalid Data Input Attempts Detected	Rule will fire in case multiple attempts at entering invalid data to application(s) on the same host are detected.	No
12.2.2	Exploit of Vulnerability Detected	Rule will fire in case multiple attempts at exploiting a vulnerability in application(s) on the same host are detected.	Optional: Tune the threshold.
12.4.3	Attempted File Changes in Development Detected	Rule will fire in case it detects attempts to change a file(s) on a host in the development segment from a source that is not in the development segment.	No
12.6.1	System with Vulnerabilities	The sole purpose of this rule is to populate the active list, referenced in actions, when a system is found to have vulnerabilities.	No
12.6.1	Persistent Vulnerability Detected	This rule will fire every time an entry expires out of the Systems with Persistent Vulnerabilities active list. The assumption is that the vulnerability on the system was not yet patched.	No

Section 12 Reports

Section	Report	Description
12.2.1	Invalid Data Input	Report all incidents of invalid data input to any application.
12.2.2	Exploit of Vulnerability	Report all incidents of attempts to exploit vulnerabilities in an application.
12.3.2	Invalid Certificate Presented	Report on all incidents of invalid or expired certificates seen.
12.4.1	Software Changes in Operations	Report all changes to any software installed in the operations segment.
12.4.3	File Changes in Development	Report all changes made to any files on a development system from a non- development segment.

12.5.3	Changes to Operating Systems	Report to detect any changes made to an operating system.
12.5.4	All Information Leaks	Report to show all activity that was flagged as information leakage.
12.6.1	Systems with Persistent Vulnerabilities	Report to show all the expiration of entries from the Systems with Persistent Vulnerabilities active list, implying that a vulnerability was left unattended on a system for more than the prescribed duration.

Section 12 Queries

Section	Query	Description
12.2.1	Invalid Data Input	Query all incidents of invalid data input to any application.
12.2.2	Exploit of Vulnerability	Query all incidents of attempts to exploit vulnerabilities in an application.
12.3.2	Invalid Certificate Presented	Query on all incidents of invalid or expired certificates seen.
12.4.1	Software Changes in Operations	Query all changes to any software installed in the operations segment.
12.4.3	File Changes in Development	Query all changes made to any files on a development system from a non-development segment.
12.5.3	Changes to Operating Systems	Query to detect any changes made to an operating system.
12.5.4	All Information Leaks	Query to show all activity that was flagged as information leakage.
12.6.1	Systems with Persistent Vulnerabilities	Query to show all the expiration of entries from the Systems with Vulnerabilities active list, implying that a vulnerability was left unattended on a system for more than the prescribed duration.
12.6.1	Top 10 Vulnerable Assets - Public Facing	This query provides a listing of the 10 most vulnerable Assets in your Public Facing Network Domains.
12.6.1	Vulnerabilities - Top 10	This query shows the top 10 vulnerabilities exposed on the systems.
12.6.1	Vulnerabilities - Top 10 Assets	This query shows the top 10 systems with vulnerabilities exposed.

Section 12 Trends

Section	Trend	Description
12.2.2	Exploit of Vulnerability	Trend to capture and report on all incidents of attempts to exploit vulnerabilities in an application.
12.5.4	All Information Leaks	Trend to capture and report on all activity that was flagged as information leakage.

Section 12 Runtime Instructions

Some resources require some manual interaction during run-time operations.

Remove Entries from Systems with Vulnerabilities Active List When a HIGH or VERY HIGH vulnerability is remedied on a system and you do not want to rely on a vulnerability scanner to remove the entry from the active list, you should manually remove the entry from the active list when the system is fixed.

ISO 13: Information Security Incident Management

Section 13 of ISO addresses controls used around managing information related to information security incidents, and their handling. Areas of interest entail all aspects of incident handling and reporting such as types of attacks, the sources and targets of the attacks. This area also addresses monitoring reconnaissance and malicious code related activity.

Use Cases

To address section 13 requirements, the SOX4 solution provides the following use cases.

Escalated Threat Monitoring

Section 13 deals with proper handling of escalated events. The SOX4 solution provides escalated event monitoring by filtering events according to user-configurable rules. The filter populates an active channel that can be monitored by analysts.

Internal Reconnaissance

Section 13 also requires that efforts must be made to prevent employees from attempting to prove suspected security weaknesses. Testing weaknesses can cause damage and should be interpreted as misuse of information systems. the SOX4 solution provides event filtering based on internal reconnaissance events to populate active channels, data monitors, and reports.

Devices

The following devices supply the events that apply to ISO section 13.

Use Case	Device	Device Configuration Required
Escalated threat monitoring	Any event that is configured to trigger a rule in the escalation filter.	None
Internal reconnaissance	NIDS/NIPS NBAD	None

Section 13 Resources

This section lists all the resources that address the information systems acquisition development and maintenance requirements of ISO section 13.

Section 13 Active Channels

Active Channel	Description
Confidentiality and Integrity Breaches	This active channel looks for integrity and confidentiality breaches.
DoS Attacks	This channel shows DoS attacks.
Escalated Information Security Events	Active channel to show all events where an escalated level of threat in information security is detected.
Information System Failures	This active channel looks for information system failures.
Internal Reconnaissance	This active channel shows reconnaissance events originating internal to the corporation.
Malicious Code Activity	This channel shows malicious code activity.
Misuse of Information Systems	This active channel looks for misuses of information systems.

Section 13 Dashboards

Section	Dashboard	Description
13.11	Escalated Information Security Events	Dashboard to show escalated threat activity to the targets and services.
13.12	Internal Reconnaissance	Dashboard to show internal reconnaissance related activities.

Section 13 Data Monitors

Section	Data Monitor	Description
13.1.1	Escalated Threat Targets	This data monitor shows the types of assets involved in escalated threat activity.
13.1.1	Top 10 Targeted Machines	This data monitor shows the top 10 machines involved in escalated threat scenarios.
13.1.1	Top 10 Targeted Services	This data monitor shows the top 10 services involved in escalated threat scenarios.
13.1.2	Internal Reconnaissance	This event graph shows all the internal reconnaissance activity.
13.1.2	Top Internal Reconnaissance Sources	This data monitor shows the top internal reconnaissance sources identified by the rule in this section.

Section 13 Filters

Section	Filter	Description
13.1.1	Escalation Filter	This filter is used to drive the escalation active channel and dashboard. The events included in this filter will be shown in that active channel and the corresponding dashboard.
13.1.2	Internal Recon	This filter looks for reconnaissance events that originated internal to the organization. This could be a policy violation of someone trying to scan the network.
13.1.2	Internal Recon Correlation Events	This filter picks up the rule firings indicating internal reconnaissance activity.
13.2.1	Confidentiality and Integrity Breaches	This filter looks for confidentiality and integrity breaches.
13.2.1	Information System Failures	This filter looks for information system failures.
13.2.1	Misuse of Information Systems	This filter looks for misuses of information systems. Also referred to as policy breaches.

Section 13 Rules

Section	Rule	Description
13.1.2	Internal Recon Detected	This rule looks for internal reconnaissance activity.
13.2.1	Information Security Incident	This rule fires for various kinds of information security incidents, e.g., Attacks, Malicious Code activities, Denial of Service, etc.

Section 13 Reports

Section	Report	Description
13.1.1	Covert Channel Activity	This report shows all covert channel activity.
13.1.1	Escalated Threat Activity	This report shows the details of escalated threat activities.
13.1.1	Escalated Threat Activity Top Sources	This report shows the top sources involved in escalated threat activity.
13.1.1	Escalated Threat Activity Top Targets	This report shows the top targets involved in escalated threat activity.
13.1.1	Events Targeting Internal Assets	This report provides a listing of hostile or suspicious traffic which targets the assets categorized as internal.
13.1.2	Internal Reconnaissance Top Events	This report shows the top events executed for internal reconnaissance.
13.1.2	Internal Reconnaissance Top Sources	This report shows the top sources conducting internal reconnaissance.
13.1.2	Internal Reconnaissance Top Targets	This report shows the top targets accessed by internal reconnaissance activity.
13.2.1	Confidentiality and Integrity Breach Sources	This report shows sources involved in integrity and confidentiality breaches.
13.2.1	Denial of Service Sources	This report shows all the sources involved in denial of service activity.
13.2.1	Information System Failure Hosts	This report shows the information system which generated error log entries.
13.2.1	Least Frequent 10 Attack Sources	This report provides a listing of the 10 least frequent sources of attacks against Assets in your Public Facing Network Domain.
13.2.1	Least Frequent 10 Attacked Targets	This report provides a listing of the 10 least frequently attacked Assets in your Public Facing Network Domain.
13.2.1	Least Frequent 10 Events	This report provides a listing of the 10 least frequent events targeting Assets in your Public Facing Network Domain.
13.2.1	Malicious Code Sources	This report shows the sources of malicious code activity.
13.2.1	Misuse of Information Systems Sources	This report shows the sources involved in misuse of information systems.
13.2.1	Most Frequent 10 Attackers Chart	This report provides a chart showing the top 10 most frequent sources of attacks against Assets in your Public Facing Network Domain.
13.2.1	Most Frequent 10 Targets Chart	This report provides a chart of the top 10 most frequently attacked Assets in your Public Facing Network Domain.
13.2.1	Top 10 Events Chart	This report provides a chart of the top 10 most frequent events targeting Assets in your Public Facing Network Domain.

Section 13 Queries

Section	Query	Description
13.1.1	Covert Channel Activity	This query shows all covert channel activity.
13.1.1	Escalated Threat	This query shows the details of escalated threat activities.
13.1.1	Escalated Threat Activity Top Sources	This query shows the top sources involved in escalated threat activity.
13.1.1	Escalated Threat Activity Top Targets	This query shows the top targets involved in escalated threat activity.
13.1.1	Events Targeting Internal Assets	This query provides a listing of hostile or suspicious traffic which targets the assets categorized as internal.
13.1.2	Internal Reconnaissance Top Sources	This query shows the top sources conducting internal reconnaissance.
13.1.2	Internal Reconnaissance Top Targets	This query shows the top targets accessed by internal reconnaissance activity.
13.1.2	Internal Reconnaissance Top Events	This query shows the top events executed for internal reconnaissance.
13.2.1	Confidentiality and Integrity Breach Sources	This query shows sources involved in integrity and confidentiality breaches.
13.2.1	Denial of Service Sources	This query shows all the sources involved in denial of service activity.
13.2.1	Information System Failure Hosts	This query shows the information system which generated error log entries.
13.2.1	Least Frequent 10 Attack Sources	This query provides a listing of the 10 least frequent sources of attacks against Assets in your Public Facing Network Domain.
13.2.1	Least Frequent 10 Attacked Targets	This query provides a listing of the 10 least frequently attacked Assets in your Public Facing Network Domain.
13.2.1	Least Frequent 10 Events	This query provides a listing of the 10 least frequent events targeting Assets in your Public Facing Network Domain.
13.2.1	Malicious Code Sources	This query shows the sources of malicious code activity.
13.2.1	Misuse of Information Systems Sources	This query shows the sources involved in misuse of information systems.
13.2.1	Most Frequent 10 Attackers Chart	This query provides a chart showing the top 10 most frequent sources of attacks against Assets in your Public Facing Network Domain.
13.2.1	Most Frequent 10 Targets Chart	This query provides a chart of the top 10 most frequently attacked Assets in your Public Facing Network Domain.
13.2.1	Top 10 Events Chart	This query provides a chart of the top 10 most frequent events targeting Assets in your Public Facing Network Domain.

Section 13 Trends

Section	Trend	Description
13.1.1	Events Targeting Internal Assets	Trend to capture and report on a listing of hostile or suspicious traffic which targets the assets categorized as internal.
13.1.2	Internal Reconnaissance Top Events	Trend to capture and report on the top events executed for internal reconnaissance.

ISO 14: Business Continuity Management

Section 14 of ISO addresses controls used in business continuity management. Areas of interest include availability of critical assets and attacks that can impact the availability of those assets.

Use Cases

To address section 14 requirements, the SOX4 solution provides the following use cases.

Monitoring Highly Critical Machines

Availability of highly critical machines is generally of utmost importance to an organization. This use case monitors machines with an asset categorization criticality set to very high for traffic, configuration changes, shutdowns, and other activity.

Availability Monitoring

Information systems availability is critical for the ongoing operations of an organization. Many resources in the solution are designed to monitor and report on events and conditions which can affect system availability.

Monitoring for Denial of Service Attacks

Denial of service attacks can cause outages to computers and networks that can cripple corporate operations. This solution filters events with category technique = DOS and feeds reports and active channels with DoS activity.

Devices

The following devices supply the events that apply to ISO section 14.

Use Case	Device	Device Configuration Required
Monitoring highly critical machines	Router • Firewall • NIDS/NIPS • HIDS/HIPS • Database • Application • NBAD • OS	None
Availability monitoring Monitoring for denial of service attacks	NIDS/NIPS • NBAD	None

Section 14 Resources

This section lists all the resources that address the information systems acquisition development and maintenance requirements of ISO Section 14.

Section 14 Active Channels

Active Channel	Description
Activity of Highly Critical Machines	This active channel shows traffic to and from highly critical machines. This can be used for the business continuity management process to monitor activity of highly critical machines.
Availability Impacts	This active channel shows events which could have an impact on the availability of information systems, such as DoS attacks.

Section 14 Dashboards

Section	Dashboard	Description
14.1	Highly Critical Asset Activity	Dashboard to show activity related to systems whose availability has a high impact as they are very critical systems.

Section 14 Data Monitors

Section	Data Monitor	Description
14.1.1	Traffic Involving Highly Critical Assets	This event graph shows traffic involving highly critical assets.

14.1.1	Up Down Status of Highly Critical Assets	This last state data monitor shows the state of highly critical assets, whether they are up or down.
14.1.2	Top Attacking Machines Targeting Highly Critical Assets	This data monitor shows attacking machines which are focusing on attacking the availability of highly critical assets.
14.1.2	Top Impacted Highly Critical Assets	This data monitor shows the top highly critical assets which were impacted from an availability standpoint.

Section 14 Filters

Section	Filter	Description
14.1	System Shutdown	This filter looks for system shut downs.
14.1.1	Traffic Involving Highly Critical Assets	This filter looks for traffic involving highly critical assets.
14.1.1	Up Down Status For Highly Critical Assets	This filter looks for shutdowns and startups of highly critical machines.
14.1.2	Attacked Highly Critical Assets	This filter looks for availability attacks on highly critical assets.
14.1.2	Availability Attacks	This filter shows generic availability attacks.
14.1.2	Availability Impact on Highly Critical Assets	This filter shows highly critical assets which were impacted from an availability standpoint.
14.1.2	DoS Attacks	This filter looks for denial of service attacks.

Section 14 Rules

Section	Rule	Description
14.1	Shutdown of Highly Critical Machine	This rule looks for shutdown events from highly critical machines.

Section 14 Reports

Section	Report	Description
14.1.1	Critical Assets	This report lists all the critical assets. It can be used to gather the key assets to implement the business continuity process.
14.1.2	Availability Attacked Assets	This report shows assets which were targeted with an availability attack.
14.1.2	DoS Attacks	This report shows denial of service attacks.

Section 14 Queries

Section	Query	Description
14.1.1	Critical Assets	This query lists all the critical assets. It can be used to gather the key assets to implement the business continuity process.
14.1.2	Availability Attacked Assets	This query shows assets which were targeted with an availability attack.
14.1.2	DoS Attacks	This query shows denial of service attacks.

ISO 15: Asset Management

Section 15 of ISO addresses controls used around enforcing a security policy. Areas of interest entail reviewing and monitoring the discovery of policy violations, existence of vulnerabilities to assist in addressing the issues.

Use Cases

ISO section 15 states: “Appropriate procedures should be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.” To address section 15 requirements, the SOX4 solution provides the following use cases.

Intellectual Property Rights Violations

Filters, rules, dashboards, and reports are in place to monitor and report on peer to peer file sharing activity that could result in illegal download and misuse of intellectual property.

Illegal Content Download

Active lists, data monitors, and filters are in place to track peer-to-peer port activity in order to find potential intellectual property rights violations.

Peer-to-Peer Traffic

Many intellectual property rights violations occur as the result of peer-to-peer file sharing networks. An active list is dynamically and manually populated with port numbers of traffic classified as peer-to-peer traffic so that this traffic can be monitored appropriately.

Information Leak Monitoring

Opportunities for information leakage should be prevented. To limit the risk of information leakage, regular monitoring of personnel and system activities must be performed. The solution uses filters for personal and organizational records to feed the appropriate data monitors and dashboards.

Company Information

The SOX4 solution uses filters for personal and organizational records to feed the appropriate data monitors and dashboards.

Personal Information

The SOX4 solution uses filters for personal and organizational records to feed the appropriate data monitors and dashboards.

Misuse of Information Processing Facilities

Users should be deterred from using information processing facilities for unauthorized purposes. Intrusion detection, content inspection, and other monitoring tools may help detect misuse of technology. The SOX4 solution provides resources to detect misuse, such as excessive email, and internal use of public mail systems.

Excessive Email Communications

Excessive email communications can indicate spam or excessive personal use of email for personal reasons. The SOX4 solution provides several reports to indicate top mail users by amount and data, and so on.

Policy Breach Monitoring

Policy breaches can be detected through a variety of input sources. In section 15, the Misuse of Information Processing Facilities report shows policy breaches.

Technical Compliance Checks

Information Processing Facilities must adhere to policy and configuration standards. The solution uses filters to flag events from vulnerability scanners and configuration management systems when new vulnerabilities or misconfigurations are found. Reports identify technical compliance issues.

Monitoring Access to Monitoring System (ArcSight)

It is important to audit access to monitoring system. The SOX4 solution uses an ArcSight Login Events filter to catch these events and feed the Information System Audit Tool Logins report and active channel.

Devices

The following devices supply the events that apply to ISO section 15.

Section 15 Use Case	Device	Device Configuration Required
Intellectual property rights violations	•NIDS/NIPS •ILP •Proxy	None
Illegal content download	•Proxy •NIDS/NIPS •ILP	None
Peer to peer traffic	•NIDS/NIPS •ILP •NBAD	None
Information leak monitoring Company information Personal information	• ILP	Make sure the ILP device is configured to monitor for critical and confidential documents.
Misuse of information processing facilities	•Email •Router •Firewall	None
Excessive email communications	• Email Server	Make sure your email server logs email communications that are relevant. [Possibly filtering internal-to internal communications to reduce event load.]
Policy breach monitoring	• NIDS/NIPS • HIDS/HIPS • ILP • Configuration Management	Configure the policy for each of the devices
Technical compliance checks	• Vulnerability Scanner • Configuration Management	None
Monitoring access to monitoring system (ArcSight)	• ArcSight	None

Configuration

In addition to the asset modeling and configurations to the common resources described in “Configure the Sarbanes-Oxley 4 Solution”, the following resources should be configured as necessary to comply with your policies.

Resource Type	Resource Name	What to configure
Filter	Intellectual Property Download	The filter references should be configured to contain all the events pertaining to this use-case. The filter is located in the My Filters group.
Active List	Peer to Peer Ports	This is a dynamic active list, which is populated by section 15 peer-to-peer rules during run-time. You can also manually add known peer-to-peer ports to this list.
Active List	Public Web Mail Servers	This active list should be populated with public Web mail servers. Examples which are already configured are gmail, yahoo, hotmail, etc.

Section 15 Resources

This section lists all the resources that address the information systems acquisition development and maintenance requirements of ISO Section 15.

Section 15 Active Lists

Active List	Description	Config?
Peer to Peer Ports	This active list is dynamically populated with port numbers of traffic classified as peer to peer traffic.	Optional. This is a dynamic active list, which is populated by section 15 peer-to-peer rules during run-time. You can also manually add known peer-to-peer ports to this list.
Public Webmail	This list contains all the DNS domains for public webmail servers. For example hotmail.com. This list is used to detect when big emails are sent to those domains, being a possible information leak.	This active list should be populated with public Web mail servers. Examples which are already configured are gmail, yahoo, hotmail, etc.

Section 15 Active Channels

Active Channel	Description
Information System Audit Tool Logins	This Active Channel shows all the logins to the Information System Audit Tool - ArcSight.
Intellectual Property Rights Violations	This active channel looks for intellectual property rights violations. To do so, it shows all the rule-firings that are indicating intellectual property rights violations.
Personal and Organizational Records Information Leak	This channel looks for leaks of personal information.
Technical Compliance Check Failures	This active channel looks for events which indicate that a technical compliance check failed, meaning that an either misconfigured or vulnerable system was found.

Section 15 Dashboards

Dashboard	Description
Email to Public Web Mail Servers	Dashboard to show activity related to e-mail traffic to public web mail services.
Information Leaks	Dashboard to show activity related to leakage of personal and organizational information.
Intellectual Property Rights Violations	Dashboard to show activity related to intellectual property movement and peer-to-peer traffic.
Technical Compliance Checking	Dashboard to show events pertaining to failure of technical compliance for security.

Section 15 Data Monitors

Section	Data Monitor	Description
15.1.2	Peer to Peer Bandwidth Consumption	This data monitor shows per port used in peer to peer traffic, what the total bandwidth consumption was.
15.1.2	Peer to Peer Ports	This last state data monitor shows all the ports involved in peer to peer traffic.
15.1.2	Top 10 Intellectual Property Rights Violations	This data monitor shows the top 10 violations concerning intellectual property by looking for the rule-firing in this use- case.
15.1.2	Top 10 Intellectual Property Rights Violators	This data monitor shows the top 10 violators downloading intellectual property by looking for the rule-firing in this use-case.
15.1.3	Organizational Records Leak	This graph shows events which pertain to information leaks of organizational records.
15.1.4	Personal Information Leak	This graph shows the communications pertaining to personal information leaks.
15.1.5	Public Web Mail Traffic	This event graph shows traffic that is targeting public Web mail servers.
15.1.5	Sender of Email to Public Web Mail Servers	Last state data monitor to raise a flag when a user sends e-mail to a recipient in a public web mail service.
15.2.2	Last 20 Failed Technical Compliance Checks	This data monitor shows the last 10 events indicating failed technical compliance checks.
15.2.2	Last 20 Machines Failing Technical Compliance Checks	This data monitor reports the last 10 machines that were reported to have failed technical compliance check.
15.2.2	Top 10 Failed Technical Compliance Checks	This data monitor shows the top ten events indicating failed technical compliance checks.
15.2.2	Top 10 Machines Failing Technical Compliance Checks	This data monitor shows the top 10 machines with failed compliance checks.

Section 15 Filters

Section	Filter	Description
15.1.2	Intellectual Property Rights Violations	This filter looks for violations of intellectual property rights by looking at the rule for this use-case.
15.1.2	Peer to Peer Traffic	This filter looks for peer to peer traffic.
15.1.3	Organizational Records Information Leak	This filter looks for information leaks with regard to company information.
15.1.4	Personal Information Leak	This filter looks for any personal information being transferred or referenced by an event.
15.1.5	Email to Public Web Mail Servers	This filter looks for emails going to public Web mail servers such as yahoo or gmail.
15.1.5	Email Traffic	This filter looks for generic email traffic.
15.1.5	Misuse of Information Processing Facilities	This filter looks for events which indicate clear misuse of information processing facilities.
15.2.2	Failed Technical Compliance Check	This filter looks for events which indicate a compliance check failure.
15.2.3	ArcSight Login Events	This filter shows all the login events to the information system audit tool, ArcSight.

Section 15 Rules

Section	Rule	Description	Config?
15.1.2	Intellectual Property Rights Violation	This rule looks for intellectual property rights violations. The filter references should be configured to contain all the events pertaining to this use-case. The filter is located in the My Filters group.	Intellectual Property Download Filter
15.1.2	Peer to Peer Traffic	This rule checks for peer to peer traffic in order to find Intellectual property rights violations.	Peer-to- peer active list.

15.13	Organizational Data Information Leak	This rule is looking for any organizational information being sent out of the corporate network.	N
15.14	Personal Information Leak	This rule is looking for any personal information being sent out of the corporate network.	N
15.15	Email to Public Webmail Servers	This rule looks for email messages being sent to public Web mail accounts such as Yahoo.	Public Web Mail Servers filter

Section 15 Reports

Section	Report	Description	Config?
15.12	Intellectual Property Rights Violations	This report shows the different intellectual property rights violations.	N
15.12	Intellectual Property Rights Violators	This report shows all the assets which violated intellectual property rights.	N
15.12	Peer to Peer Ports Used	This report shows all the ports that were involved in peer-to-peer traffic.	Y: Peer-to-peer active list.
15.12	Peer to Peer Sources	This report shows all the machines using peer-to-peer applications.	Y: Peer-to-peer active list.
15.13	Organizational Records Information Leaks	This report shows the communications which were classified as information leaks of organizational records.	N
15.14	Personal Information Leaks	This report shows events which indicate a personal information leak.	N
15.15	Misuse of Information Processing Facilities	This report shows machines which misuse information processing facilities for activity which constitutes a policy breach.	N
15.15	Top Email Receivers (Amount)	This report shows the top email recipients based on the number of emails received.	N

15.15	Top Email Receivers (Size)	This report shows the top email recipients based on the size of emails received.	N
15.15	Top Email Senders (Amount)	This report shows the top email senders based on the number of emails sent.	N
15.15	Top Email Senders (Size)	This report shows the top email senders based on the size of emails sent.	N
15.15	Top Largest Emails	This report shows the top 100 largest emails including the sender and recipients.	N
15.15	Top Public Web Mail Senders	This report shows the top 100 senders of emails which went to a public Web mail server.	N
15.2.2	Assets that Failed Technical Compliance Check	This report finds assets which failed the technical compliance check.	N
15.2.3	Information System Audit Tool Logins	This report shows logins, both successes and failed, to ArcSight - the information system audit tool. This report will also show instances where the archive tool was executed, not just console logins.	N

Section 15 Queries

Section	Query	Description
15.1.2	Intellectual Property Rights Violations	This query shows the different intellectual property rights violations.
15.1.2	Intellectual Property Rights Violators	This query shows all the assets which violated intellectual property rights.
15.1.2	Peer to Peer Ports Used	This query shows all the ports that were involved in peer-to-peer traffic.
15.1.2	Peer to Peer Sources	This query shows all the machines using peer- to-peer applications.
15.1.3	Organizational Records Information Leaks	This query shows the communications which were classified as information leaks of organizational records.
15.1.4	Personal Information Leaks	This query shows events which indicate a personal information leak.
15.1.5	Misuse of Information Processing Facilities	This query shows machines which misuse information processing facilities for activity which constitutes a policy breach.
15.1.5	Top Email Receivers (Amount)	This query shows the top email recipients based on the number of emails received.
15.1.5	Top Email Receivers (Size)	This query shows the top email recipients based on the size of emails received.

15.1.5	Top Email Senders (Amount)	This query shows the top email senders based on the number of emails sent.
15.1.5	Top Email Senders (Size)	This query shows the top email senders based on the size of emails sent.
15.1.5	Top Largest Emails	This query shows the top 100 largest emails including the sender and recipients.
15.1.5	Top Public Web Mail Senders	This query shows the top 100 senders of emails which went to a public Web mail server.
15.2.2	Assets that Failed Technical Compliance Check	This query finds assets which failed the technical compliance check.
15.3.2	Information System Audit Tool Logins	This query shows logins, both successes and failed, to ArcSight - the information system audit tool. This query will also show instances where the archive tool was executed, not just console logins.

Section 15 Trends

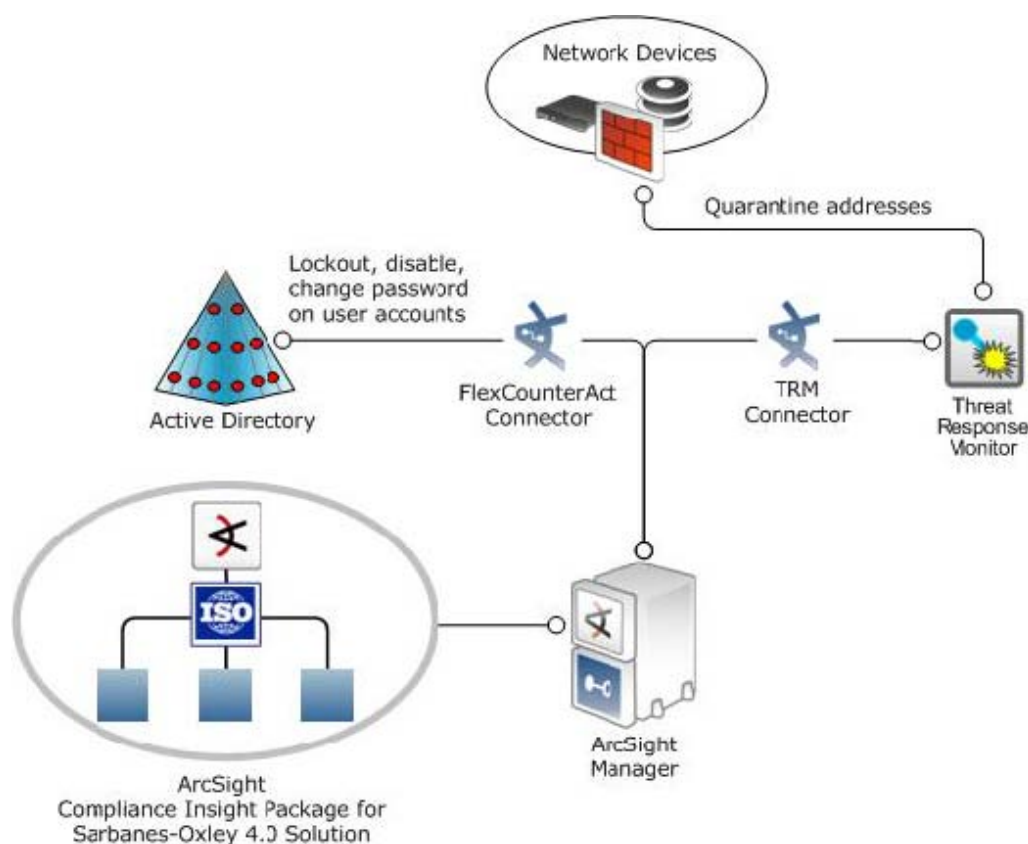
Section	Trend	Description
15.1.3	Organizational Records Information Leaks	Trend to capture and report on the communications which were classified as information leaks of organizational records

Chapter 5: Automated Response and Prevention

This chapter describes how to set up and use Active Directory, ArcSight Threat Response Manager (TRM), and their corresponding ArcSight CounterAct-enabled connectors to provide automated response and remediation to compliance violations. These features are optional.

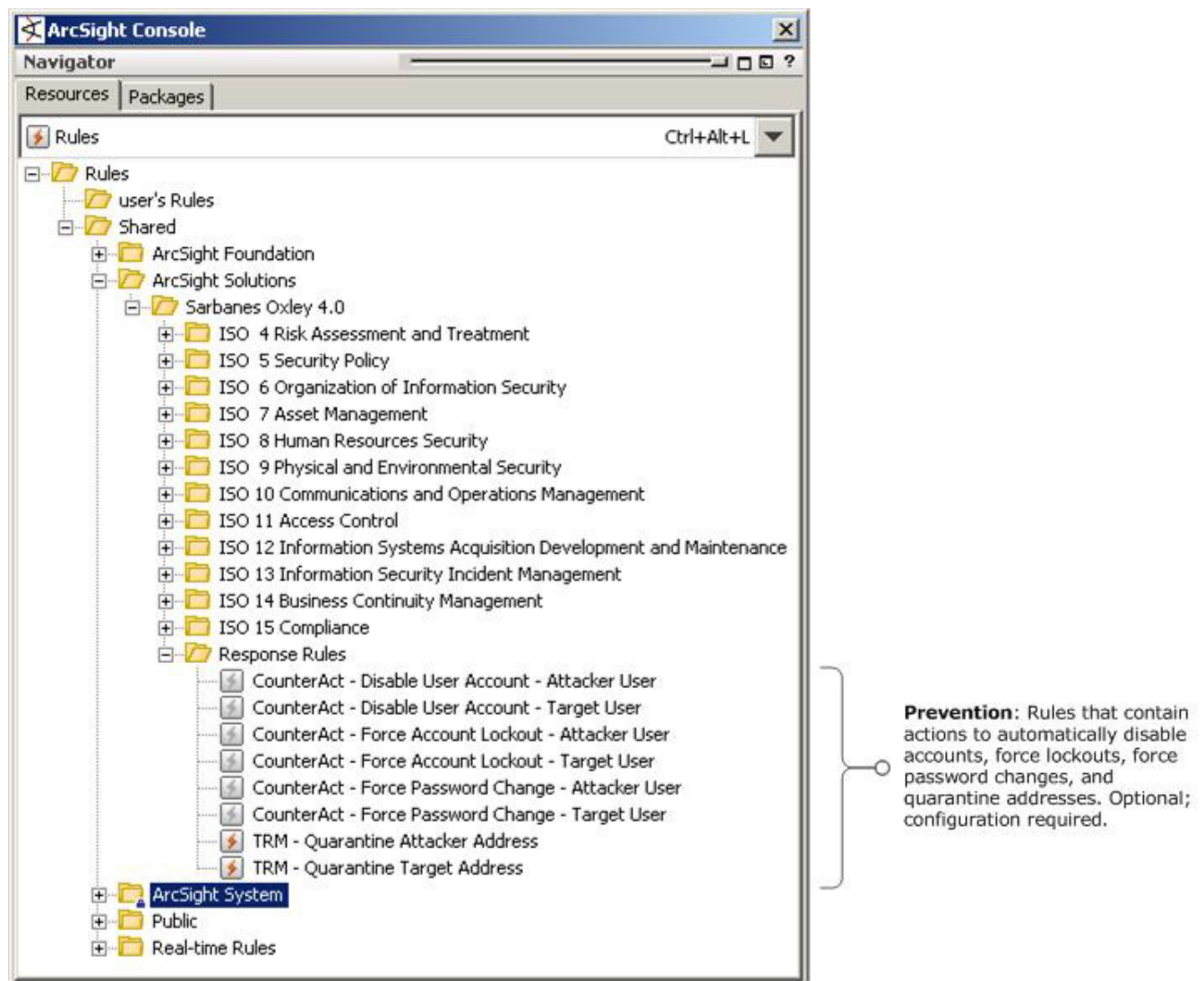
Automated Response and Prevention Architecture

The SOX4 solution includes a series of rules that leverage ArcSight CounterAct connectors to send commands to Active Directory and network devices in order to automatically disable accounts, force lockouts and password changes, and quarantine addresses.



Automated Response and Prevention Rules

The prevention layer controls consist of the following rules:



The table below describes these rules in more detail. Because the automated response and prevention feature is optional, all the rules require configuration, and must be explicitly enabled.

Rule	Description	Config?
CounterAct - Disable User Account - Attacker User	This rule is designed to disable a user account. Please refer to the documentation on how this should be configured.	Yes
CounterAct - Disable User Account - Target User	This rule is designed to disable a user account. Please refer to the documentation on how this should be configured.	Yes
CounterAct - Force Account Lockout - Attacker User	This rule is designed to force an account lockout on a user account. Please refer to the documentation on how this should be configured.	Yes
CounterAct - Force Account Lockout - Target User	This rule is designed to force an account lockout on a user account. Please refer to the documentation on how this should be configured.	Yes
CounterAct - Force Password Change - Attacker User	This rule is designed to force a password change on a user account. Please refer to the documentation on how this should be configured.	Yes

CounterAct - Force Password Change - Target User	This rule is designed to force a password change on a user account. Please refer to the documentation on how this should be configured.	Yes
TRM - Quarantine Attacker Address	This rule is designed to quarantine an attacker address using ArcSight's Threat Response Manager.	Yes
TRM - Quarantine Target Address	This rule is designed to quarantine a target address using ArcSight's Threat Response Manager.	Yes

There are eight CounterAct rules you can use, four actions with two variations each, one for attacker and one for target. Six rules are for the FlexCounterAct agent that manages actions to user accounts on Active Directory; the other two are for the TRMCounterAct agent that quarantines addresses.

The rules and actions are all independent, and you will likely want to configure and enable them on a case-by-case basis once you've had an opportunity to observe the Compliance violation events coming through your system. For example, if the Section 10.10.2 rule Successful Attack – Brute Force is triggered, the offender in this event is the attacker, and you may want to disable this user account, or even quarantine the attacker address.

In this case, you would configure the rule/filter pair for the action you want to take: CounterAct – Disable User Account – Attacker User to disable the user account, or TRM – Quarantine Attacker Address if you want to quarantine the address.

Configure CounterAct Active Directory Resources

The CounterAct resources work with Active Directory to initiate automated response and prevention on user accounts.

Tip: The SOX4 CounterAct content for Active Directory is limited to Microsoft Windows Active Directory. The script must run from a Windows 2000 system SP4 or greater that includes the Windows Scripting capabilities. The current version of the script requires that the script be executed with the administrative privileges from a system that is currently part of the Active Directory being controlled.

The configuration process involves the following processes:

- Download Sarbanes-Oxley Active Directory script `ArcSightCounterACT_AD.vbs` and the `flexcounteract.counteract.properties` file
- Configure the Sarbanes-Oxley Active Directory script `ArcSightCounterACT_AD.vbs`. Copy the configured script and the `flexcounteract.counteract.properties` file to the intended FlexCounterAct connector machine.
- Install and configure the FlexCounterAct connector; configure it to run as a Windows Service
- Configure CounterAct Rules

- Configure CounterAct Rule Filters
- Enable CounterAct Rule

The following sections describe these processes in more detail.

Download the CounterAct Active Directory Files

The CounterAct Active Directory files listed in the following table can be downloaded from the SOX4 package.

File	Description
ArcSightCounterACT_AD.vbs	This script provides three different actions: - Forces a password change for a particular user - Forces a user account lockout - Disables a user account
Flexcounteract.counteract.properties	Provides the properties required by the FlexCounterAct connector during connector installation and configuration.

Repeat the following steps, to download all files the listed in the preceding table:

1. From the **Resources** tab in the Navigator pane, go to Files, and navigate to ArcSight Solutions/Sarbanes Oxley 4.0/counteract folder.
2. Right-click on the file and select the **Download** option.
3. Browse for a directory location.
4. In the File name field, enter the name of the file and click **Save**.

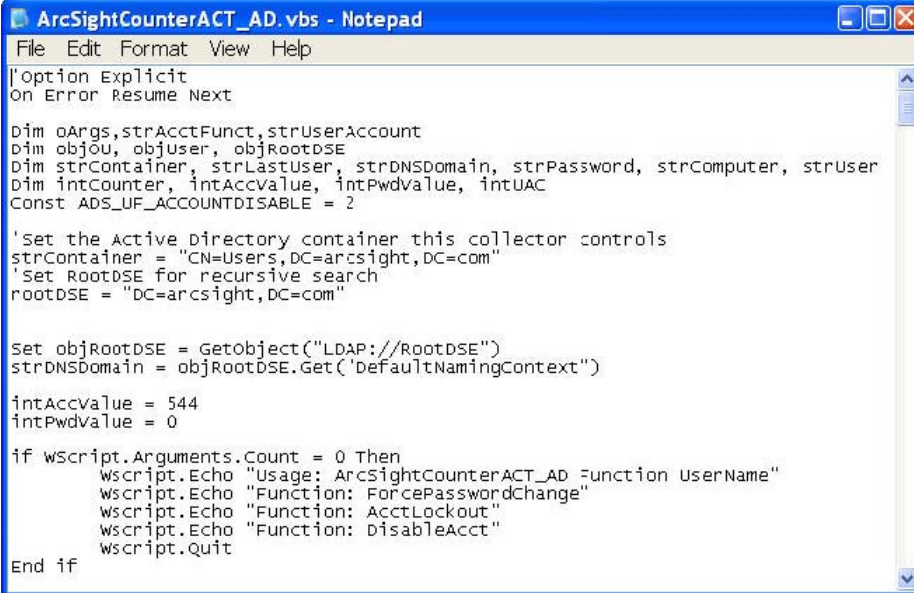
A copy of the file is saved to the local file system.

Configure and Copy Active Directory Files

This process configures the CounterAct Active Directory script ArcSightCounterACT_AD.vbs and copies the configured script and the flexcounteract.counteract.properties file to the intended FlexCounterAct connector machine.

1. Open a Windows command window.
2. Change to the directory location where ArcSightCounterACT_AD.vbs file is stored.
3. Make a back up of the Visual Basic script ArcSightCounterACT_AD.vbs.
4. In a text editor, open the original script ArcSightCounterACT_AD.vbs and configure it with the following values for your environment:
 - Set the Active Directory container path: Search for the following string: strContainer = "CN=Users,DC=arcsight,DC=com" as shown below. Modify this string with the Active Directory hierarchy that applies for your environment. OU=organizational unit; CN=common name; DC=domain component. For more information about Active Directory object naming, see <http://www.comptechdoc.org/os/windows/win2k/win2kadname.html>.

- Set the rootDSE: The rootDSE establishes the base of the directory service hierarchy and tells the tool where to start the recursive search through the Active Directory hierarchy of user groups.



```

ArcSightCounterACT_AD.vbs - Notepad
File Edit Format View Help
'Option Explicit
On Error Resume Next

Dim oArgs, strAcctFunc, strUserAccount
Dim objOU, objUser, objRootDSE
Dim strContainer, strLastUser, strDNSDomain, strPassword, strComputer, strUser
Dim intCounter, intAccValue, intPwdValue, intUAC
Const ADS_UF_ACCOUNTDISABLE = 2

'Set the Active Directory container this collector controls
strContainer = "CN=Users,DC=arcsight,DC=com"
'Set RootDSE for recursive search
rootDSE = "DC=arcsight,DC=com"

Set objRootDSE = GetObject("LDAP://RootDSE")
strDNSDomain = objRootDSE.Get('DefaultNamingContext')

intAccValue = 544
intPwdValue = 0

if wscript.Arguments.Count = 0 Then
    wscript.Echo "Usage: ArcSightCounterACT_AD Function UserName"
    wscript.Echo "Function: ForcePasswordChange"
    wscript.Echo "Function: AcctLockout"
    wscript.Echo "Function: DisableAcct"
    wscript.Quit
End if
  
```

5. Save the script and exit the editor.
6. Copy the downloaded CounterAct files to any directory on the system on which you will install the FlexCounterAct connector. These files will be required during the connector installation and configuration process.

Install and Configure the FlexCounterAct Connector

Once the Sarbanes-Oxley Active Directory scripts are copied to the system on which you will install the FlexCounterAct connector, you can install the connector according to the instructions in the FlexCounterAct Connector Configuration Guide.

Tip: If you are running ArcSight v4.0, obtain the license for the FlexCounterAct connector and install it according to the instructions in the FlexCounterAct Connector Configuration guide

When prompted for the properties file, browse to the location where you copied the file `flexcounteract.counteract.properties`. This properties file contains the settings required to launch the `ArcSightCounterACT_AD.vbs` script from the CounterAct Connector.

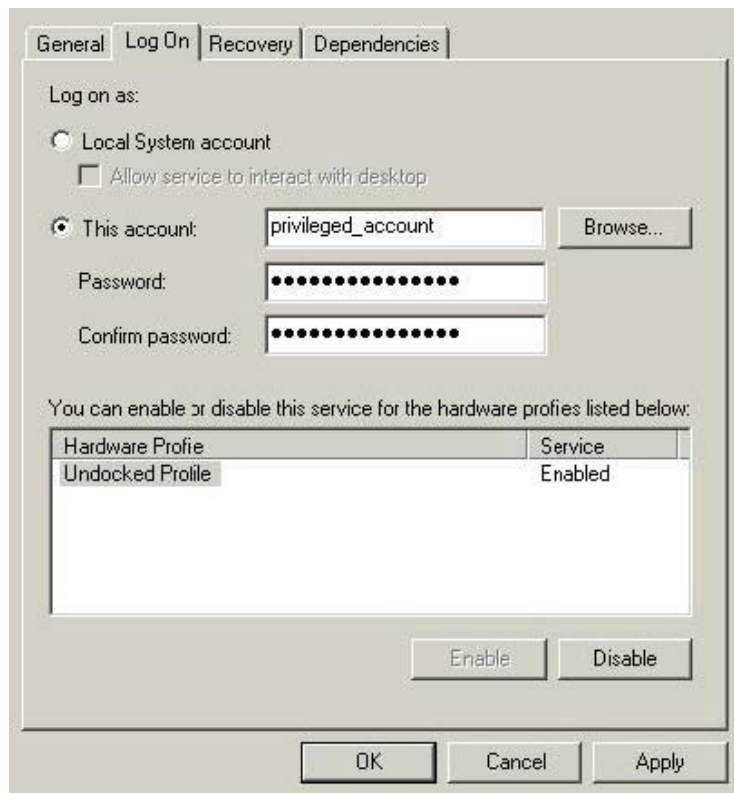
Configure the FlexCounterAct Connector as a Windows Service

For the `ArcSightCounterACT_AD.vbs` script to be executed automatically, the FlexCounterAct connector must be a part of the Active Directory domain it's controlling and run with a Windows Service account with the appropriate privileges to make changes (Read/Write) to that Active Directory.

1 On the FlexCounterAct connector Windows machine, go to **Control Panel | Administrative Tools | Services**.

2 Right-click the ArcSight FlexCounterAct service and select **Properties**.

3 In the FlexCounterAct Properties window, select the **Log On** tab. In the Log on as section, select This account and browse for the account name that has sufficient permissions to execute scripts on Active Directory. Enter the password for this account and click OK.



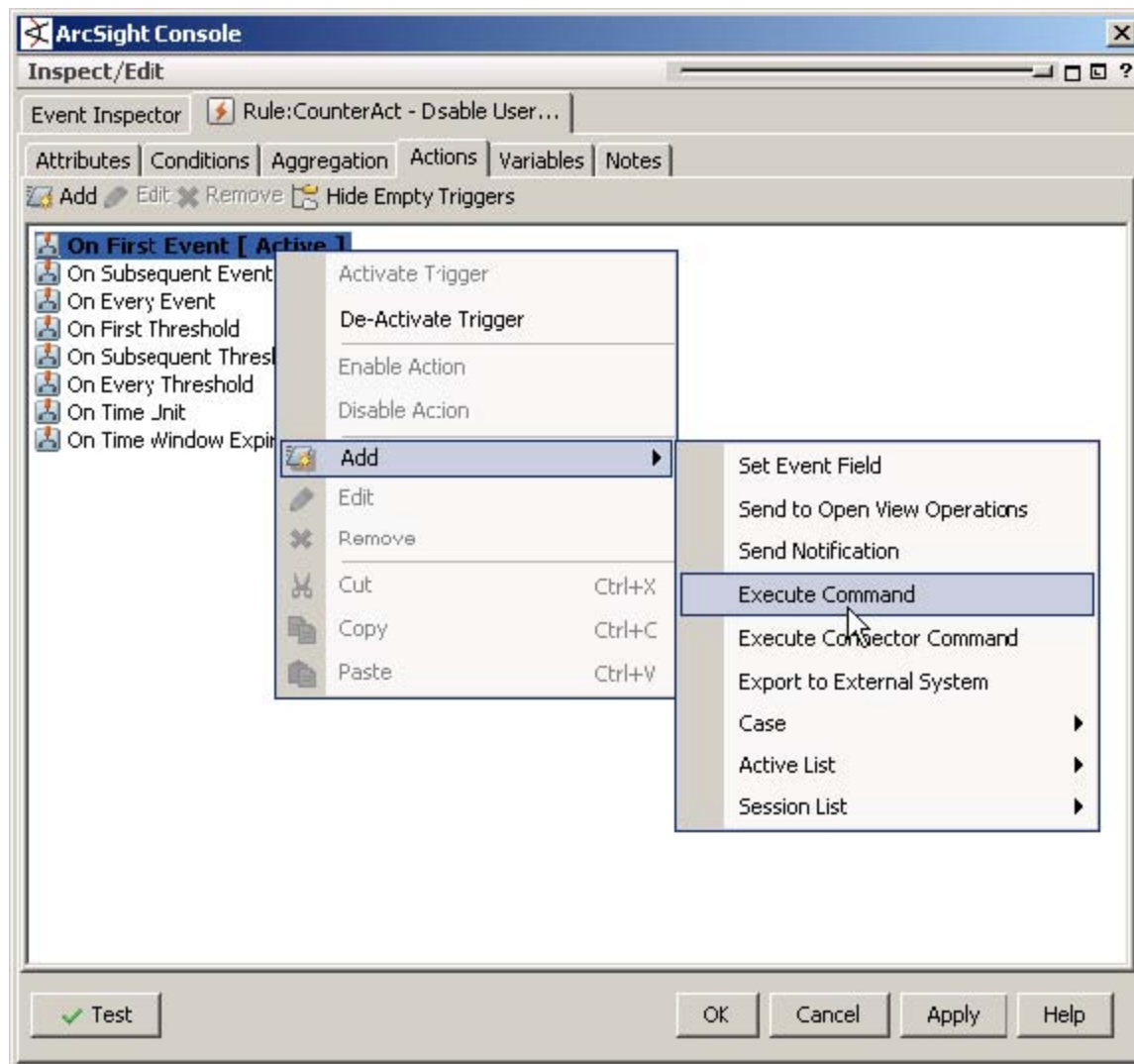
Configure CounterAct Rules

Any CounterAct rules you wish to use require that their conditions and trigger thresholds be configured.

The example below uses the rule CounterAct – Disable User Account – Target User.

1. On the Console in the Navigator panel, go to Rules and navigate to ArcSight Solutions/Sarbanes Oxley 4.0/Response Rules.
2. Open the CounterAct rule in the Rule editor in the Inspect/Edit panel (double-click the rule or right-click and select Edit Rule)
3. In the rule editor in the Inspect/Edit panel, select the Action tab.
4. Remove the default action (Execute command): Select, then right-click Execute Command and select Remove.

- Right-click the trigger **On First Event (Active)** and select **Add | Execute Connector Command**. This launches the Add “Execute Connector Command” Action dialog box.



- In the **Add “Execute Connector Command” Action** dialog box, enter the following values and click **OK**:
- In the **Connector** field, navigate to the ArcSight CounterAct connector you installed in the previous process.
- In the **Command** field, navigate to the action you want the connector to execute. Choose the action that matches the name of the rule you are editing, in this case `DisableUserAccount`.
- When you choose the command, you will get the name | value fields in the bottom pane. For the Target rule, enter the script execute command that matches, in this case `$targetUserName`. If editing the Attacker rule, enter `$attackerUserName`.



10. Enable the rule: In the Navigator panel, right-click the rule and select Enable.
11. Repeat steps 2 through 7 for all the CounterAct rules you want to activate.

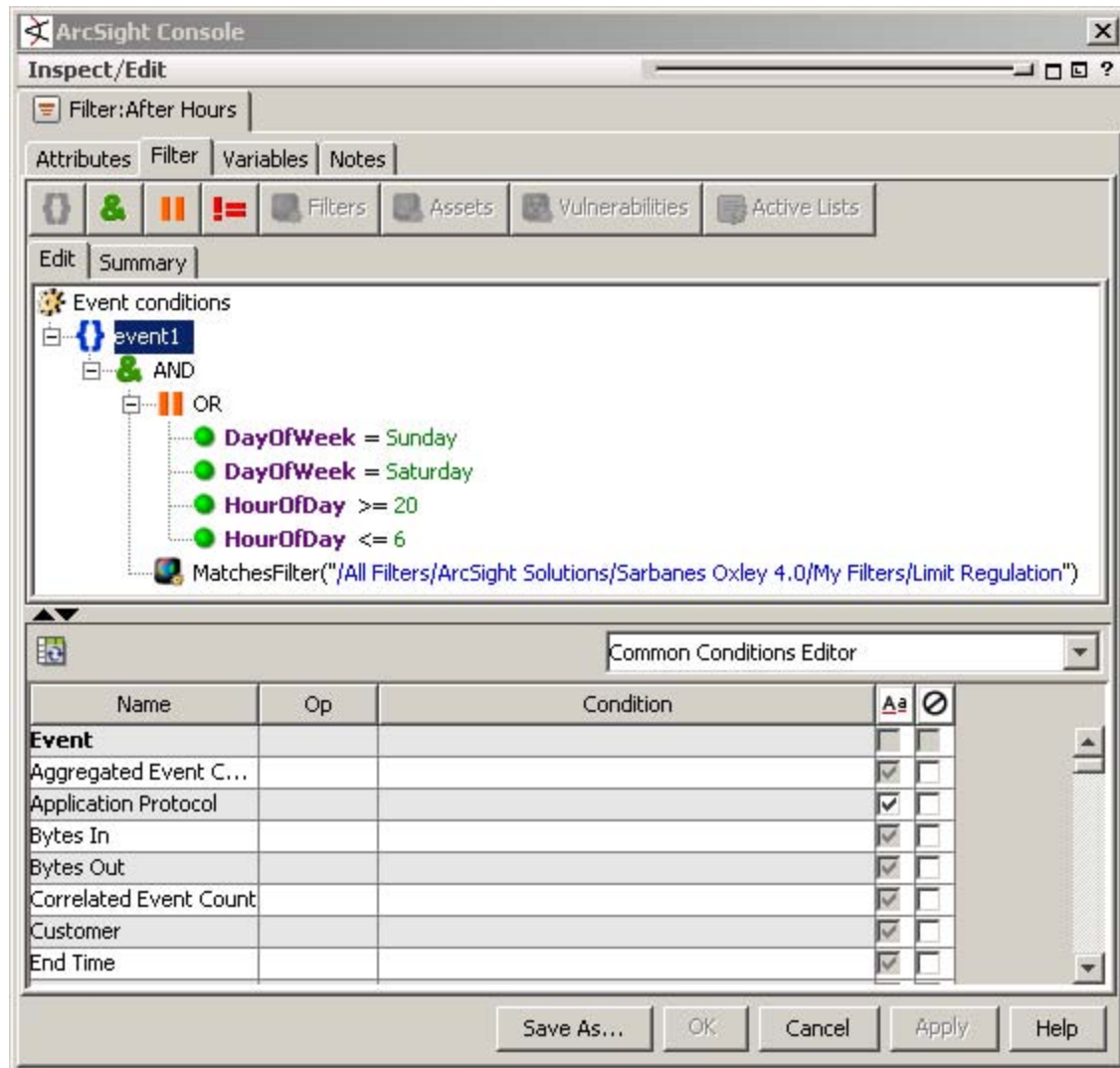
Configure CounterAct Filters

Once the rule actions are configured, configure the Response filters with the names of the rules that you want to trigger the CounterAct action.

For example, you might want to lock out a user that just successfully gained access to a high-value database by brute force (as detected by the Section 10.10.2 rule Successful Attack – Brute Force).

The example below shows how you would configure the CounterAct – Disable User Account – Attacker User filter with the rule name of the early warning rule.

- a. On the Console in the Navigator panel, go to Filters and navigate to ArcSight Solutions/Sarbanes Oxley 4.0/Response Filters
- b. Open the filter in the Filters editor in the Inspect/Edit panel (double-click the filter or right-click and select **Edit Filter**).
- c. In the Filter Editor in the Inspect/Edit panel, select the **Filter** tab.
- d. Select the line with the default value Name = rule_name_1_here. In the event fields below, find the Event | Name field and change the value to the name of the rule you want to trigger the lock-out action, in this case, the Section 10.10.2 rule Successful Attack – Brute Force. Verify that the name is entered exactly as it appears in the rule editor. You can copy and paste using the Edit menu copy/paste tools. Values are not case sensitive.



- e. As an option, you can enter more rule names in the OR statement lines (OR Name = rule_name_2_here and OR Name = rule_name_3_here). It is OK to leave these default values in place. You can also add more lines as needed.
- f. Repeat steps 2 through 5 for every CounterAct filter you need to configure.

Configure Threat Response Manager Resources

The ArcSight Threat Response Manager (TRM) is an ArcSight offering that provides automated response to attacks by instantly quarantining nodes at the exact moment of detection.

TRM requires the TRM CounterAct connector, which makes the TRM actions available in certain Sarbanes-Oxley rule actions. By default, these features are not enabled. This section describes how to configure these resources.

The TRM configuration process involves the following processes: ■

- Install and configure the TRMCounterAct connector
- Configure TRMCounterAct Rules
- Configure TRMCounterAct Rule Filters
- Enable TRMCounterAct Rule

The following sections describe these processes in more detail.

Install and Configure the CounterAct Connector

Install the connector according to the instructions in the FlexCounterAct Connector Configuration Guide. During Counteract configuration, the installer asks for the address of the TRM appliance and requests an TRM username and password.

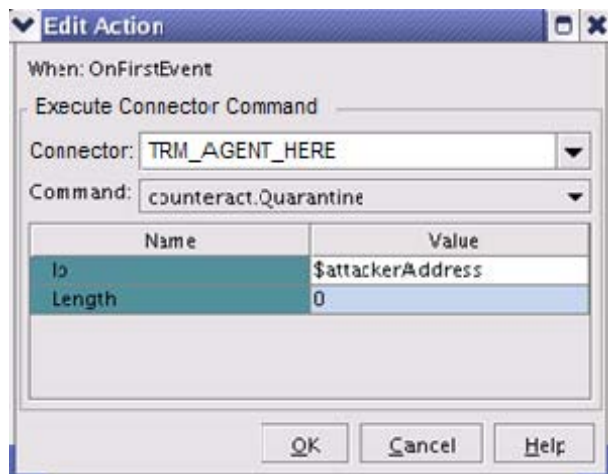
Configure CounterAct Rules

The SOX4 solution includes the following two CounterAct rules to trigger quarantine actions in response to the Compliance violations conditions you want to configure:

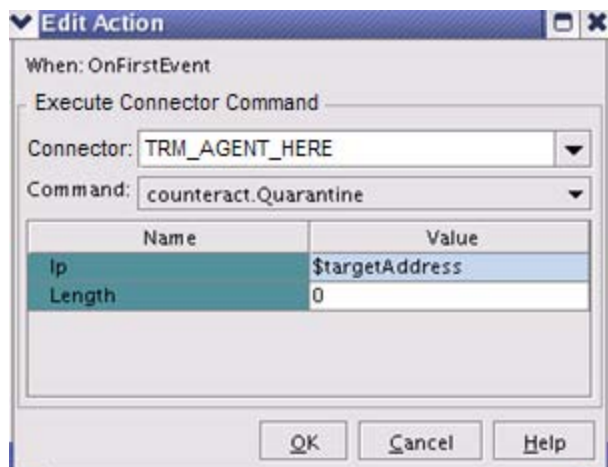
- TRM– Quarantine Attacker Address
- TRM – Quarantine Target Address

Configure these rules with the CounterAct Connector.

1. On the Console in the Navigator panel, go to Rules and navigate to ArcSight Solutions/Sarbanes Oxley 4.0/Response Rules
2. Open the Quarantine Attacker Address rule in the Rule editor in the Inspect/Edit panel (double-click the rule or right-click and select Edit Rule)
3. In the rule editor in the Inspect/Edit panel, select the Action tab.
4. Right-click the trigger On First Event (Active) and select Add | Execute Connector Command. This launches the Add “Execute Connector Command” Action dialog box.
5. In the Edit Action dialog box, enter the following values and click OK.
6. In the Agent field, navigate to the ArcSight CounterAct connector you installed in the previous process.



7. In the Command field, navigate to the action you want the connector to execute. Choose the action that matches the name of the rule you are editing, in this case counteract.Quarantine.
8. When you choose the command, you will get the name | value fields in the bottom pane. For the Attacker rule, enter the script execute command that matches, in this case **\$attackerAddress**. If editing the Target rule, enter **\$targetAddress**. Click OK.



9. Enable the rule: in the Navigator panel, right-click the rule and select Enable.
10. Repeat steps 2 through 6 for the TRM Quarantine Target Address rule.

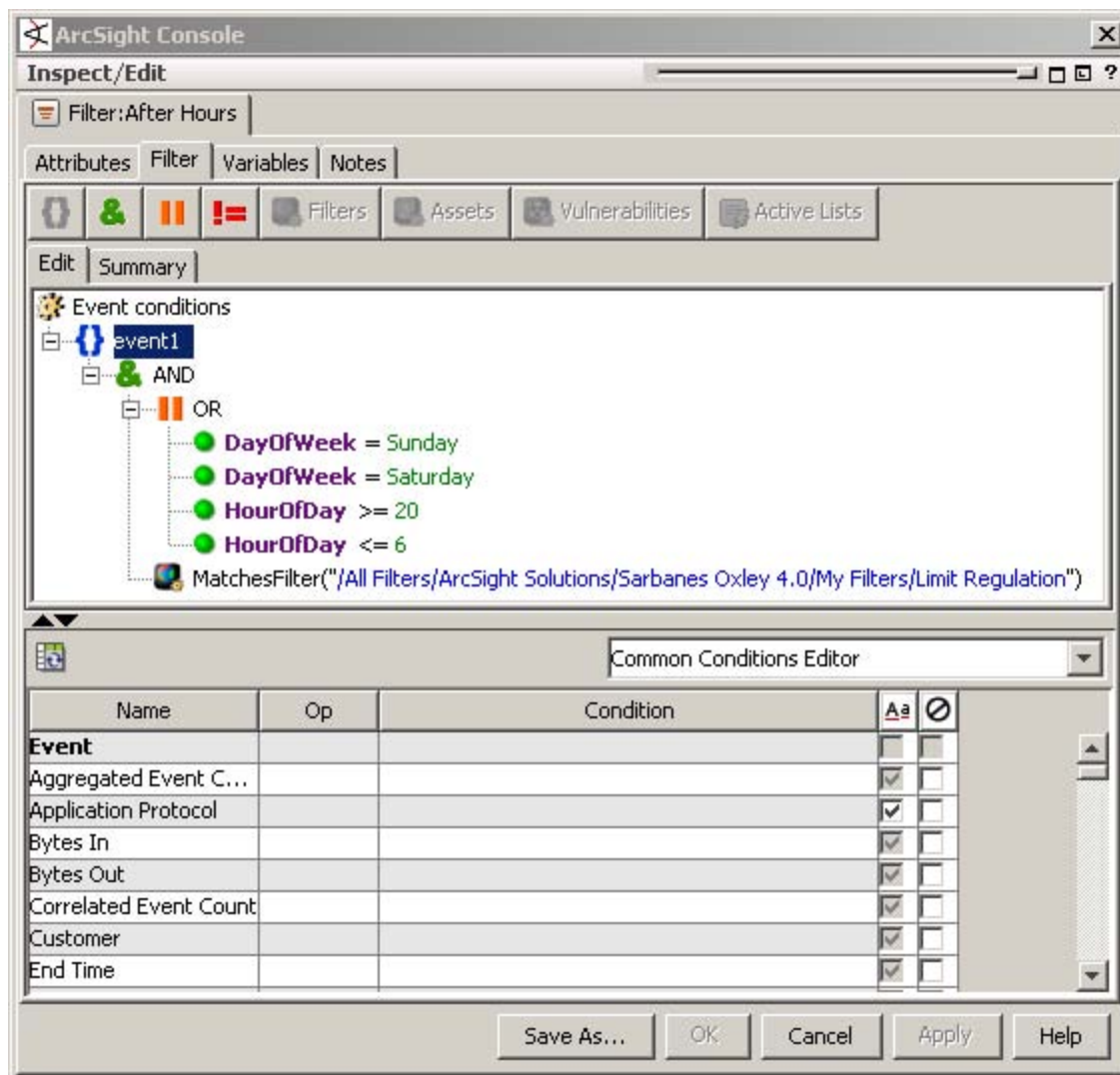
Configure CounterAct Filters

Once the CounterAct rule actions are configured, configure the CounterAct filters with the names of the rules that you want to trigger the CounterAct action.

For example, you might want to quarantine an address that just successfully gained access to a high-value database by brute force (as detected by the Section 10.10.2 rule Successful Attack – Brute Force).

The example below shows how you would configure the CounterAct – Disable User Account – Attacker filter with the rule name of the early warning rule.

1. On the Console in the Navigator panel, go to Filters and navigate to ArcSight Solutions/Sarbanes Oxley 4.0/Response Filters.
2. Open the CounterAct filter in the Filters editor in the Inspect/Edit panel (double-click the filter or right-click and select Edit Filter)
3. In the Filter Editor in the Inspect/Edit panel, select the Filter tab.
4. Select the line with the default value Name = rule_name_1_here. In the event fields below, find the Event | Name field and change the value to the name of the rule you want to trigger the quarantine action, in this case, the Section 10.10.2 rule Successful Attack – Brute Force. Verify that the name is entered exactly as it appears in the rule editor. You can copy and paste using the Edit menu copy/paste tools. Values are not case sensitive.



5. As an option, you can enter more rule names in the OR statement lines (OR Name = rule_name_2_here and OR Name = rule_name_3_here). It is OK to leave these default values in place. You can also add more lines as needed.
6. Repeat steps 2 through 5 for the other CounterAct filter.

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 computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Solutions Guide (ESM CIP for SOX 4.02)

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 arc-doc@hpe.com.

We appreciate your feedback!