ArcSight Pattern Discovery™

For ArcSight™ ESM Version 4.0

March 14, 2007

ArcSight Pattern Discovery™

For ArcSight™ ESM Version 4.0

March 14, 2007

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

Revision History

Date	Product Version	Description
10/24/05	ESM 3.5	Final document for v. 3.5 release.
1/25/07	ESM 4.0	Draft revision for v. 4.0
3/9/07	ESM 4.0	Draft revision for v. 4.0
3/14/07	ESM 4.0	Final document for v. 4.0 release.

Contents

ArcSight Pattern Discovery 1

Patterns 2

Anatomy of a Pattern 2

Pattern Components 2

Component Relationships 2

Component Groups (Transactions) 3

How Pattern Discovery Works 3

Pattern Discovery Lifecycle 5

Establish a Baseline of Normal Event Patterns 6

Use Pattern Discovery in Routine Operations 6

Installing Pattern Discovery 7

How to Use Pattern Discovery 9

1 Create a Profile 9

Modify a Profile in System Profiles 10

Create a New Profile 11

Specify Actions 14

Add Notes 17

Edit a Profile 17

Delete a Profile 17

2 Take a Snapshot 18

Explore Snapshots 19

Arrange Elements in Graphic View 21

Investigate Patterns in Snapshots 22

Investigate Patterns from the Snapshots View 22

Investigate Patterns from the Patterns View 25

Schedule a Snapshot 25

Re-open a Snapshot 26

Delete a Snapshot 27

3 Investigate Patterns 27

View Patterns 27

View Patterns with Filter 27

Inspect Patterns 28

Create Rules from Patterns 30

Enable Rule and Activate It in Real-time Rules Folder 35

Annotate Patterns 36

Delete a Pattern 37

Index 38

ArcSight Pattern Discovery

Patterns are relationships between events that may indicate emerging threats and attacks. But finding them can be difficult, because they hide among millions of raw events from hundreds of devices over varied time intervals. Being able to identify patterns quickly is imperative to effectively managing your network security and avoiding a significant compromise.

ArcSight Pattern Discovery™ can automatically detect subtle, specialized, or long-term patterns that might otherwise go undiscovered in the flow of events. You can use Pattern Discovery to:

- **Discover day-zero attacks**: Because Pattern Discovery does not rely on encoded domain knowledge (such as predefined rules or filters), it can discover patterns that otherwise go unseen, or are unique to your environment.
- **Detect low-and-slow attacks**: Pattern Discovery can process up to a million events in just a few seconds (excluding read-time from the disk). This makes Pattern Discovery effective to capture even low-and-slow attack patterns.
- **Profile common patterns on your network**: New patterns discovered from current network traffic are like signatures for a particular subset of network traffic. By matching against a database of historical patterns, you can detect attacks in progress.

  The patterns discovered in an event flow that either originate from or target a particular asset can be used to categorize those assets. For example, a pattern originating from machines that have a back door (unauthorized program that initiates a connection to the attacker) installed can all be visualized as a cluster. If you see the same pattern originating from a new asset, it is a strong indication that the new asset also has a back door installed.
- **Automatically create rules**: The patterns discovered can be transformed into a complete rule set with a single mouse click. These rules are derived from data patterns unique to your environment, whereas predefined rules must be generic enough to work in many customer environments.

Pattern Discovery is a vital tool for preventive maintenance and early detection in your ongoing security management operations. Using periodic, scheduled analysis, you can always be scanning for new patterns over varying time intervals to stay ahead of new exploit behavior.

Patterns

A pattern is a collection of events with specific component parts that interrelate in some way in a given time frame. These events are uniquely identified by their event data signature (such as source and target IP addresses, ports, host names, and so on). You can also look for patterns that involve a specific data point you are interested in. For example, if you wish to find patterns that involve a particular type of sensor, you can set that device type as one of the parameters.

Many event patterns are normal or benign. The purpose of ArcSight Pattern Discovery is to effectively mine large streams of event data for unique patterns that you can use to inform your network security decisions, whether it's remediating an attack or establishing a baseline of normal event traffic.

Elements that define a pattern include:

- **High Frequency of occurrence**: As a pattern becomes longer and longer, the probability that it occurs just by chance in a stream becomes lower and lower. A higher frequency of occurrence can be used for making inferences.

- **Recurrence**: Recurrence means a whole pattern with the same characteristics that occurs more than once. High frequency of occurrence implies recurrence, but recurrence does not necessarily imply high frequency. Some low and slow attacks belong to this category and are harder to detect.

Anatomy of a Pattern

The Pattern Discovery algorithm first converts an event into its individual parts, called *components*, and then applies a relationship definition to identify groups of components that are related by common properties, such as source, destination, attacker, target, time stamp, name, and so on. These groups of related components are called *transactions*. Each pattern discovered lists the components involved and the transactions where the common components were observed. This data is output as a pattern resource.

Pattern Components

Patterns are composed of an event field, or a small set of event fields, such as event name, custom string1 and an ArcSight category. These pieces of event data are referred to as *components*.

Component Relationships

To qualify as a pattern, event components must occur together. Together can mean:

- **Together in a session**: All the components occur in the same session. In an event stream, this information is not provided, it must be derived.

- **Together in a sub-stream**: The event stream can be divided into sub-streams using a “group by” operation on a subset of event fields. This step can also take time of occurrence into account.

- **Together in time**: All the components occur together in a small time window.

Component Groups (Transactions)

Event components with some kind of relationship are grouped together as *transactions*, which then become potential candidates for patterns. The Pattern Discovery algorithm processes all the transactions it finds and produces patterns, depending on whether they satisfy one or more conditions that make them discernable as patterns.

Event components are subdivided into transactions in two major ways: time-based division, and event field-based division. These two methods are orthogonal and can be combined.

Time-Based Division

Time-based division is based on timing constraints, and is very similar to the constraints used in defining rules. For example, the system creates a transaction at every division of an event stream. The event stream can be divided depending on the rate of occurrence of events and changes in those rates. This works well for dividing event streams that display events in bursts of activity.

Event Field-Based Division

Event field-based division is very similar to doing a “group by” operation on event fields. Every related group of events is a sub-stream of the original stream of events. For example:

- **Based on source and target address and port**: Suppose there are three distinct source addresses in the event stream. After doing a “group by,” three sub-streams are generated, each one originating from and corresponding to a unique source address.

- **Based on source and target address**: In this case, all the events that have the same source and target address belong to the same sub-stream.

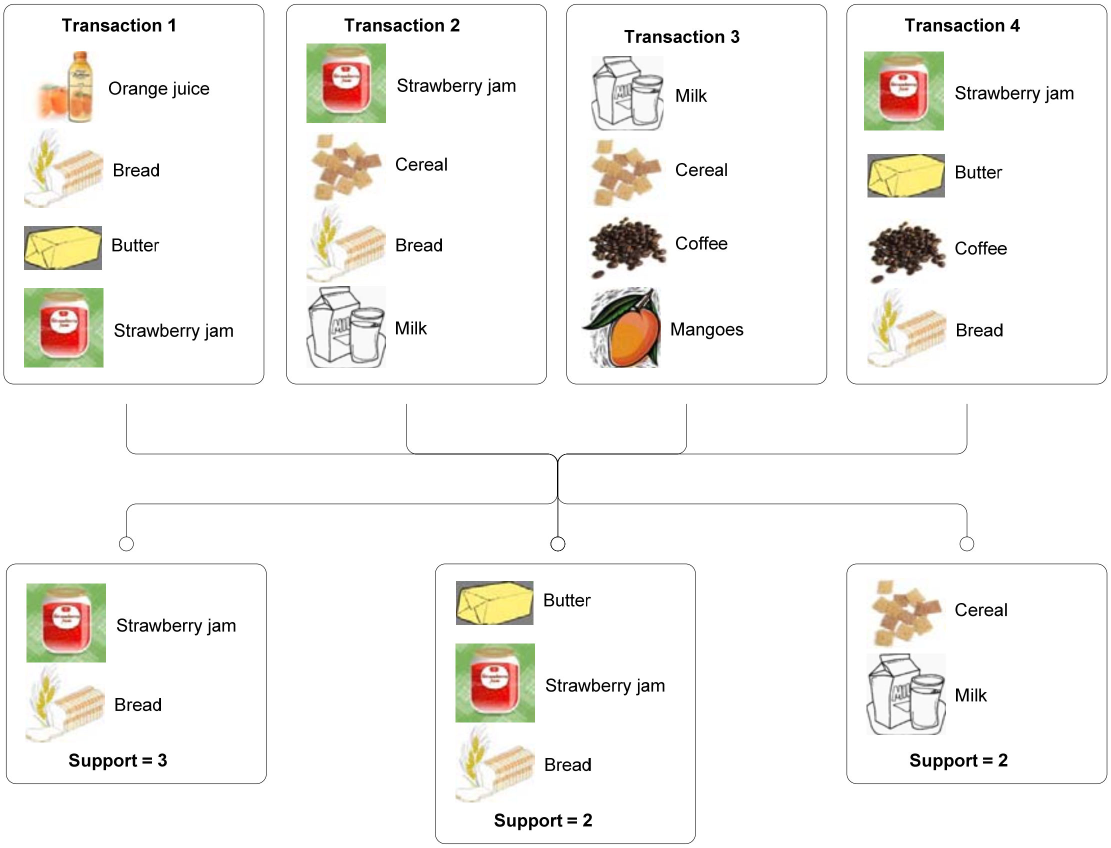
How Pattern Discovery Works

Once the event stream is divided into transactions, Pattern Discovery then characterizes the events that occur in each transaction using a subset of the event fields, such as the event name or the event category. Events that occur together in multiple transactions are identified and grouped together.

These events are further sub-grouped by support level. The *support* value for each event is the number of times that event occurred in conjunction with its related events. A higher support number means that a particular pattern has occurred more frequently than others.

For example, consider several simple grocery transactions, as pictured below. In this case, one transaction is a multi-item grocery order. Several patterns emerge: every time bread was purchased, strawberry jam was also purchased. Bread, butter, and jam were also purchased together, as were milk and cereal, and jam and coffee. Once these patterns are discovered, an analyst can draw certain conclusions, for example, that these shoppers all intend to make toast, or have cereal for breakfast.

Bread and strawberry jam also appear in two of the patterns, and thus, are a sub-pattern.



The common elements of several simple grocery transactions reveal several patterns. The number of times the pattern elements occur together is called the support value.

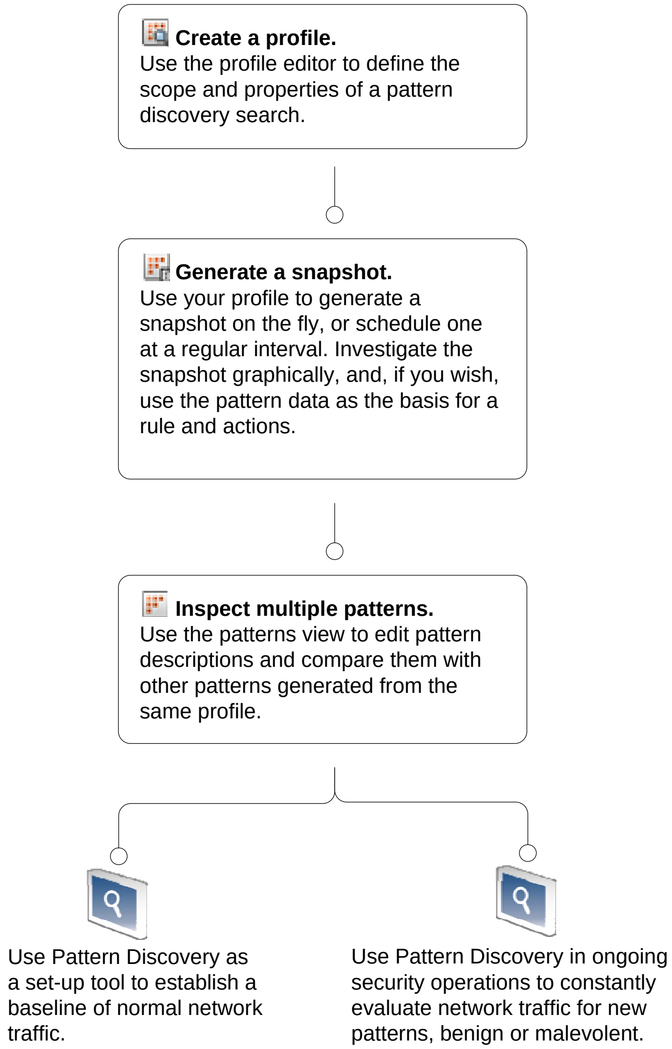
Once a pattern is discovered, you can take several actions. If certain patterns are considered normal traffic, you can mask these patterns out so the system recognizes them and does not evaluate them again.

Another pattern may be something you want to keep an eye out for, so you can build a rule based on the characteristics of this pattern. When the pattern occurs, the rule can trigger an action, such as notifying a group of users, initiating a command script, or adding a pattern to an active list for further observation.

Pattern Discovery Lifecycle

The lifecycle of how Pattern Discovery fits into your security operations consists of two phases:

- Establish a baseline of event patterns that are considered normal.
- Use Pattern Discovery in routine operations to identify, investigate, and analyze new patterns to enable zero-day response to new threats.



Create a profile. Use the profile editor to define the scope and properties of a pattern discovery search.

Generate a snapshot. Use your profile to generate a snapshot on the fly, or schedule one at a regular interval. Investigate the snapshot graphically, and, if you wish, use the pattern data as the basis for a rule and actions.

Inspect multiple patterns. Use the patterns view to edit pattern descriptions and compare them with other patterns generated from the same profile.

Use Pattern Discovery as a set-up tool to establish a baseline of normal network traffic.

Use Pattern Discovery in ongoing security operations to constantly evaluate network traffic for new patterns, benign or malevolent.

Pattern Discovery is a three-phase process that can be applied to set-up activities and ongoing security operations to establish a normal baseline of traffic and find new threats.

Establish a Baseline of Normal Event Patterns

To accomplish phase one, you would use broader profiles and more frequent snapshots in order to capture an example of all the patterns that occur as part of normal business practices.

Next, identify the patterns that are normal or benign. To identify all normal patterns may take some time and investigation, and requires that you have in-depth knowledge and familiarity with the traffic in your enterprise.

Once you have identified the normal patterns, the best method for moving them out of the analysis workflow is to use annotation. You can also use filters, but it is more reliable to move patterns by annotating them to a stage, such as **Closed**, because this assures that the pattern has actually been inspected and classified. For instructions about how to use event annotation to manage Pattern Discovery workflow, see *Annotate Patterns* on page 36.

Use Pattern Discovery in Routine Operations

Once normal patterns are identified and annotated so they are removed from the routine traffic flow, you can focus on the new patterns that are not yet classified. Routine operations consist of the following tasks:

- **Workflow**. As Pattern Discovery turns up new or unclassified patterns, a designated user needs to review them and start them through the workflow using the ESM annotations feature. You can also schedule Pattern Discovery to run automatically at regular time intervals.

- **Investigation and analysis**. Once assigned to an analyst, the analyst can use the full array of ESM's investigation and analysis tools, including snapshot and pattern graphics, event graphs, filters, and rules, to determine the level of threat represented by the pattern.

  During this investigation, it may be useful to drill down to the native device information to help identify the significance of a pattern. For example, if an event in a pattern was generated by Snort, you can retrieve the Snort rule number and look for its detailed explanation to obtain important event details.

- **Take action**. When a threat level is determined, the analyst can take a number of actions, such as use the ESM rule builder to take a prescribed action on this pattern and others that match it that may occur in the future; assign it to another user for follow-up; or close the pattern if it is deemed benign.

Installing Pattern Discovery

ArcSight Pattern Discovery is a separate feature of ArcSight Enterprise Security Management (ESM™), and is enabled by a separate product license. To obtain this new license, contact your ArcSight representative. You will subsequently receive a welcome email that includes the URL to the Support page and instructions on obtaining your login and password information.

The downloaded license is in the form of files packaged within a .zip file. To use this .zip file to update your ArcSight license, please follow the steps below:

1. On the system where ArcSight Manager is installed, copy the package (.zip file) to the ARCSIGHT_HOME directory (the directory that contains the ArcSight installation).

2. Run the following command: arcsight deploylicense

The resulting wizard replaces the currently installed license with the new Pattern Discovery enabled one. ArcSight Manager automatically detects the new license.

How to Use Pattern Discovery

The goal of Pattern Discovery is to learn which patterns are benign, so you can apply ESM's correlation, analysis, and remediation capabilities to those that are not.

Pattern Discovery is as easy as 1-2-3:

1. **Create a profile**. A profile specifies the filters and timeframe you wish to examine for patterns.

2. **Take a snapshot**. A snapshot collects all the events in a specified timeframe, automatically discovers any patterns, and displays the result in a graphical view. This graphical view is saved in the **Snapshots** tab.

3. **Analyze patterns**. When a snapshot is taken, the pattern it discovers is saved at the Patterns tab. Use this view to investigate pattern details.

1 Create a Profile

A profile is a set of constraints and filters that define the scope and properties of a Pattern Discovery search. It determines what slice of events you wish to examine for patterns, and what defines a pattern.

When you create a profile, it generates a resource in ESM that reconstructs transactions and characterizes events based on a time range you specify and any filters you wish to apply to limit the event stream.

Once you create a profile, you can use it to take a snapshot, which collects all the events in the specified timeframe and evaluates them according to the parameters you set in the profile.

Pattern Discovery ships with two profiles already created in the **All Profiles | ArcSight System** folder:

- **Daily Pattern Discovery**. Evaluates the past 24 hours worth of events for patterns starting from the moment you take the snapshot. This profile is not scheduled and can be run on demand.

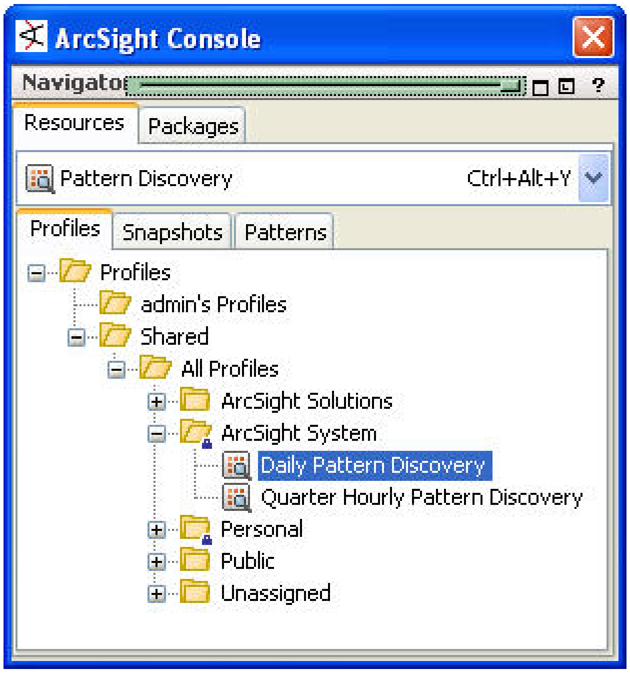
- **Quarter hourly Pattern Discovery**. Evaluates the past 15 minutes worth of events for patterns starting from the moment you take the snapshot. This profile is not scheduled and can be run on demand.

You can use these profiles, or you can create your own in a user-modifiable folder in the Profiles tree, such as the Personal or Public folder.

The ArcSight System Profiles group is locked, which means that the Daily and Quarter Hourly Pattern Discovery profiles cannot be renamed or deleted. You can, however, modify them with new conditions or time parameters.

For best results, it is recommended that you modify a copy of these profiles in a user-modifiable folder.

For instructions about how to use one of these profiles as is, go to the next section, *Take a Snapshot* on page 18.



Pattern Discovery tree in the Navigator panel.

Modify a Profile in System Profiles

If you wish to modify a profile in the System Profiles folder, first copy and paste it into a Profiles folder that is not the System Profiles folder.

4 In the Navigator panel, select the profile you wish to copy. Go to **Edit | Copy**. You can also use the key command **Ctrl + C**.

5 Click the folder in which you wish to paste the profile, then go to **Edit | Paste**. You can also use the key command **Ctrl + V**.

6 Double click the copied profile and edit its attributes in the **Inspect/Edit** panel.

A profile cannot be deleted or modified if it has patterns and snapshots derived from it. This is to safeguard the relationships among snapshots that share the same profile. If you wish to modify or delete a profile, first delete any snapshots or patterns associated with it.

Create a New Profile

1. In the Navigator panel, go to Pattern Discovery and click the **Profiles** tab.

2. Expand the Profiles resource tree. Right-click a group in the resource tree and select **New Profile**.

3. In the Inspect/Edit panel at the Profile Editor **Attributes** tab, enter the following values and click **Apply**.

Property	**Usage**
Summary	A profile summary appears just below the Attributes tab. The underlined items represent the values entered in the fields below.
Profile	
Name	Enter a descriptive name for your profile
Minimum Pattern Length	Type or use the up/down arrows to select the minimum number of unique associated events necessary to qualify the events as a pattern. The minimum default value is **1**.
Minimum Pattern Occurrences	Type or use the up/down arrows to select the minimum number of times that an event-association of the specified length must reoccur in order to qualify as a pattern. The minimum default value is **2**.
Start Time	Use the drop-down menu to select a timestamp expression for the snapshot start time. Expressions are described in the table below.

Function	**Description**
$Now	The current time in the format hh:mm:ss.
$Now – 1h	The current time minus 60 minutes 00 seconds.
$Now – 1d	The current time minus 24 hours 00 minutes 00 seconds.
$Now – 1w	The current time minus 7 days 00 hours 00 minute 00 seconds.
$Today	The start of the current day (12:00:00).
$Today – 1d	The start of the current day (12:00:00) minus 24 hours 00 minutes and 00 seconds.
$CurrentWeek	The start of the current week (Sunday 12:00:00).

Property	Usage
	$CurrentMonth The start of the current month (1st 12:00:00). The format of start time is $Now-<time>. The time specified here must be in increments of hours, days, weeks, or months.
End Time	Use the $Now drop-down menu to select a timestamp expression for the snapshot end time. See *Start Time* in the table on the previous page for a description of the available formats.
Events	
Event Fields	You can select which event fields you want the snapshot to display. Click the Name drop-down menu to expose the Event field's chooser. In the Available Fields area, click a check box to select an event field. You can select more than one. In the Fields to Show section, use the up and down arrows to specify the order in which you want to see the event fields displayed. To remove an event field from the list, select the event field and click ✖.
Source	You can select which source fields you want the pattern portion of the snapshot to display. Click the Source Address drop-down menu to expose the Source field's chooser. In the Available Fields area, click a check box to select a source field. You can select more than one. In the Fields to Show section, use the up and down arrows to specify the order in which you want to see the source fields displayed. To remove a source field from the list, select the event field and click ✖.
Target	You can select which target fields you want the pattern portion of the snapshot to display. Click the Destination Address drop-down menu to expose the Target field's chooser. In the Available Fields area, click a check box to select a target field. You can select more than one. In the Fields to Show section, use the up and down arrows to specify the order in which you want to see the target fields displayed. To remove an event field from the list, select the event field and click ✖.
Restrict by Filter	Click the All Events drop-down menu to choose a filter from the Filters resource tree. This applies an existing filter to restrict the pool of events from which the snapshot will be constructed.
Advanced	The checkboxes in this section instruct the snapshot to capture elements pertaining to time, which can lend vital insight to a pattern.

Property	Usage
Record Time Order	Select this check box to include the time sequence of the events contained in patterns. For example, for a three-event pattern, it could record that A-B-C occurred 40%, B-A-C 35%, and A-C-B 25%. Because event sequences can reveal intent, you can possibly detect and act upon certain kinds of activity even sooner.
Split on Inactivity	Split on inactivity is an advanced time feature that detects potentially meaningful decreases in activity between duplicate source/target pairs. Select this check box to create a break if there is a pause or significant drop in the number of times a particular pattern occurs. This treats occurrences of the pattern on either side of the break as separate instances. On analysis, a split on occurrences of the same source/target pairs will notify the analyst that there was a slow-down or break in occurrences. This enables you to discover patterns that happen repeatedly for one source/target pair.
Discovery Results	
Snapshot Retention Time	Click the drop-down menu to select how long you want the system to save a snapshot and its series of events. Snapshots retain all the needed components of the events and make them available during analysis. For example, when you drill down in an event and select “Show related events”, the events saved within the timeframe set here will be searched for matches. The default retention time is 7 days.
Snapshot Group	Choose a group in the Snapshot resource tree in which to store the resulting snapshots. By default, the system adds the snapshot to the same folder you right clicked to add the profile.
Pattern Group	Choose a group in the Patterns resource tree in which to store the resulting patterns. By default, the system adds the pattern to the same folder you right clicked to add the profile.
Common	
External ID	An identification string suitable for, and which can be referenced by, systems outside ArcSight. Common applications of External IDs include appropriate naming for Case and Asset resources that are tracked in common with defect reporting or vulnerability-management systems. Your ArcSight administrator can advise you on the correct values for this field, if applicable.
Alias	An identification string suitable for referencing resources within ArcSight. A given alias will appear in place of the resource's name everywhere it may be seen. Your ArcSight administrator can advise you on the correct values for this field, if applicable.

Property	Usage
Description	A text description of the profile.
Assign	
Owner	The ESM user with responsibility for the profile
Notification Groups	The ESM user group(s) to notify concerning changes to a profile.

4 Click **OK** to apply the changes and close the editor.

Specify Actions

1 To specify an action, open the profile in the profile editor (double click the profile in the Navigator panel).

2 In the Inspect/Edit panel, click the **Actions** tab.

3 Before you add an action, you first must specify when you want the action to be taken (the trigger). Select one of the following trigger options:

Occurrence option	Description
On Pattern Discovered	This specifies that the action will be taken the first time a new pattern appears. Choose this option for assigning new patterns to an analyst to investigate.
On Pattern Re-discovered	This specifies that the action will be taken if a new pattern is repeated. Choose this option for ongoing operations.

4 Click Add (Add) and select one of the following options:

Action option	Description
Annotate Pattern	In the dialog box, enter the following values and click **OK**: ♦ In Annotate Pattern, select a Stage from the drop-down menu. ♦ Assign a user by selecting a user name from the drop-down menu.
Set Event Field	In the dialog box, enter the following values and click **OK**: ♦ In Set EventField, select a Field Set from the drop-down menu. ♦ In the event fields grid, set values for the event fields you are interested in.
Send Notification	In the dialog box, enter the following values and click **OK**: ♦ In Send Notification, specify a notification group in the Notification Group drop-down menu. ♦ Click **Ack Required** if you want those notified to acknowledge that they received notification. ♦ Write the message you wish to send in the Message field.
Execute Command	In the dialog box, enter the following values and click **OK**: ♦ In Execute Command, Select an operating system platform from the Platform drop-down menu. ♦ In the Command field, enter the command string you wish to execute. Syntax must be correct; the system does not test the accuracy of your command string. ♦ In the Parameters field, enter any parameters required for the command. For example, the archive tool requires the Manager name, admin name and password. This provides the system all the parameters necessary to execute the command without user intervention. ♦ In the Action Type drop-down menu, select one of the following: ♦ **Automatically Run on Manager**: This initiates the command automatically with no user intervention. ♦ **Run on Manager with Console Confirmation**: This initiates a confirmation dialog box in the console for the designated user before the command is initiated. ♦ **Run on Connector(s)**: This sends the command to the connector(s) that report the events.

Action option	Description
Execute Connector Command	You can specify a command to be executed at the SmartConnector reporting the events, such as pause, stop or start event flow, or terminate or restart connector process. In the dialog box, enter the following values and click OK: ♦ In the Connector drop-down menu, select the SmartConnector you wish to execute the command. When you select an connector, the command field will be populated with the commands available for that connector. ♦ In the Command field, select the command you wish the connector to execute. The command may contain parameters that you must populate with appropriate values.
Export to External System	You can export the pattern to an external tracking system, such as BMC Remedy, if you have it configured to operate with ESM. Click **OK**.
Active List	You can add (or remove) a pattern to an active list, where its event details are available to other correlation tools for reference. ♦ To add a pattern to an active list, select **Add to Active List**. In the dialog box, select an active list from the drop-down menu and click **OK**. ♦ To remove a pattern from an active list, select **Remove from Active List**. In the dialog box, select an active list from the drop-down menu and click **OK**.
Session List	You can add a pattern to a session list, or terminate a session list based on a pattern, where its event details are available to other correlation tools for reference. ♦ To add a pattern to a session list, select **Add to Session List**. In the dialog box, select a session list from the drop-down menu and click **OK**. ♦ To terminate a session list, select **Terminate Session List**. In the dialog box, select a session list from the drop-down menu and click **OK**.

5 The action summary will be displayed in the Actions tab. To remove lines that are not used, click Hide Empty Triggers (Hide Empty Triggers).

Add Notes

You can keep track of changes made to a profile using the Notes feature. To add a note:

1. In the Profile Editor, click the **Notes** tab.
2. In the Notes field, enter a note and click **Save**. The entry is logged in the Table/List tabs.
3. You can view notes as a table or as a list by toggling between the Table and List tabs. You can re-order the table view by clicking the header of the column by which you wish to sort.

Edit a Profile

1. In the Navigator panel, go to Pattern Discovery and click the **Profiles** tab.
2. Right-click a profile in the resource tree and choose **Edit Profile**.
3. In the Profile Editor, click the **Attributes** tab and change the information necessary to modify the profile, according to the profile properties described below.

> The event fields and advanced operations in a profile that has patterns and snapshots derived from it cannot be modified. This is to safeguard the relationships among snapshots that share the same profile. If you wish to modify these properties in the profile, you must first delete any snapshots or patterns associated with it.

4. Click Apply to put your changes into effect and leave the editor open, or OK to apply the changes and close the editor.

Delete a Profile

1. In the Navigator panel, go to Pattern Discovery and click the **Profiles** tab.
2. Right-click a profile in the resource tree and choose **Delete Profile**.

> A profile cannot be deleted if it has patterns and snapshots derived from it. This is to safeguard the relationships among snapshots that share the same profile. If you wish to delete a profile, first delete any snapshots or patterns associated with it.

3. Click **Delete** in the confirmation dialog box.

2 Take a Snapshot

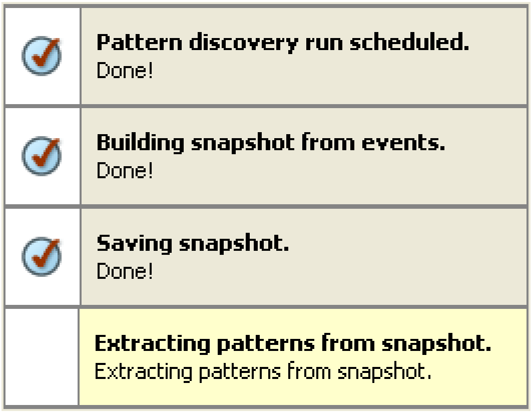
A snapshot is a record of qualifying events collected in a timeframe and evaluated according to the parameters you set in the profile. When the Pattern Discovery algorithm runs on the data set specified, it groups events into transactions and divides them into patterns sorted by how often they occur together (support). The result is displayed as a graphic, which you can use to drill down to investigate and analyze.

You can generate snapshots manually, or you can run them automatically on a set schedule as part of your daily security operations. You are more likely to generate snapshots from a particular profile more frequently during the early stage of implementation, when you are establishing a baseline of normal patterns. Each snapshot is stored in the Navigator panel in Pattern Discovery at the **Snapshots** tab.

1 In the Navigator panel, go to Pattern Discovery and click the **Profiles** tab.

2 Right-click a profile in the resource tree and select **Take Snapshot**.

3 In the Viewer panel, the system processes the snapshot request:



Pattern discovery run scheduled.
Done!

Building snapshot from events.
Done!

Saving snapshot.
Done!

Extracting patterns from snapshot.
Extracting patterns from snapshot.

The snapshot checklist indicates the process the Pattern Discovery engine is running.

4 When the process finishes, the system will display the snapshot's graphic in the Viewer panel.

5 If the pattern is empty, there may not have been any events that passed the filter restrictions selected in the profile, or the time period specified does not contain any events that pass the filter restrictions. Adjust these settings in the profile and generate the snapshot again.

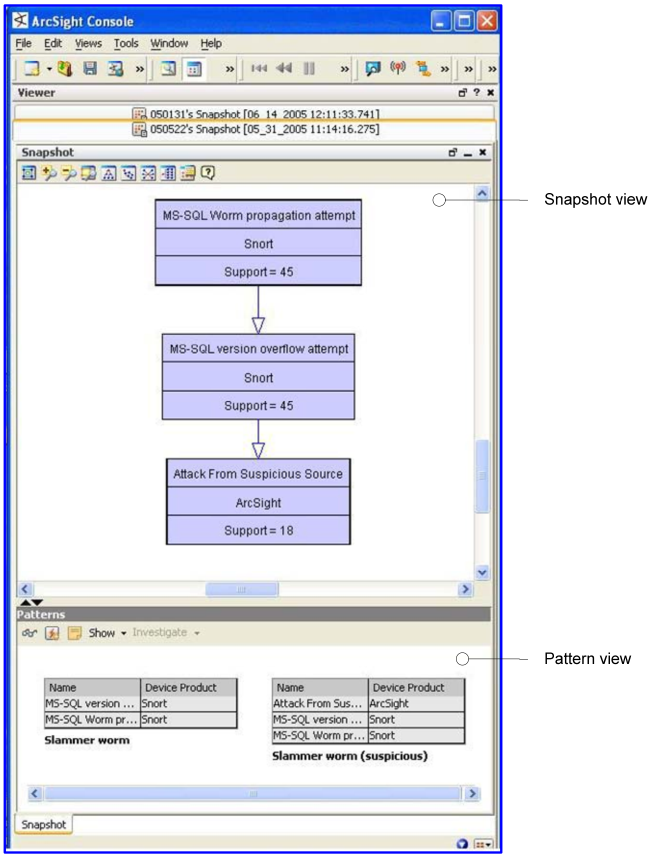
Explore Snapshots

Once the snapshot is generated, there are several ways you can explore and manipulate a snapshot to better understand its significance.

The Viewer panel presents snapshots as a two-pane window. The upper pane shows a hierarchy of related event nodes displayed in a graphic. This is called the *snapshot view*.

The lower pane shows blocks of events from the hierarchy that are most closely related. Each block of events represents one specific path through the pattern hierarchy. This is called the *patterns view.*

The example on the following page shows two patterns and a demarcation point. The top two events are the SQL worm. The last event is generated by ESM. Pattern Discovery classified 18 of 45 sources as suspicious. There are 27 sources that ran the slammer worm in the network, but they were not added to the suspicious list. This discovery enables you to investigate why all 27 systems were not caught by the other surveillance mechanisms in place on your network. What are the factors that make those that got by sneakier than the others? This enables you to tighten the drag net around your network.


ArcSight Console
File
Edit
Views
Tools
Window
Help
Viewer
050131's Snapshot [06_14_2005 12:11:33.741]
050522's Snapshot [05_31_2005 11:14:16.275]
Snapshot
MS-SQL Worm propagation attempt
Snort
Support = 45
MS-SQL version overflow attempt
Snort
Support = 45
Attack From Suspicious Source
ArcSight
Support = 18
Patterns
Show
Investigate
Snapshot
Snapshot view
Pattern view

Name	Device Product
MS-SQL version ...	Snort
MS-SQL Worm pr...	Snort

Slammer worm

Name	Device Product
Attack From Sus...	ArcSight
MS-SQL version ...	Snort
MS-SQL Worm pr...	Snort

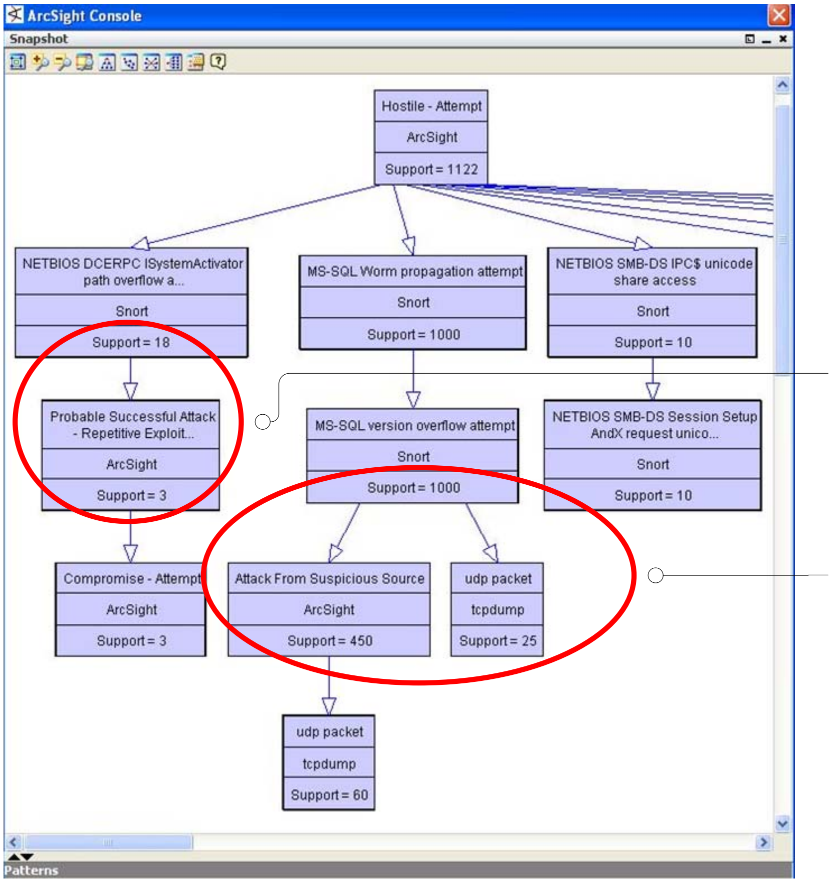
Slammer worm (suspicious)

The Pattern Discovery snapshot and patterns view in the Viewer panel. The snapshot view and the patterns view are linked; click on a node in the snapshot view to see details of that node in the patterns view.

The "support" value for each node is the number of times that event occurred in conjunction with its related events. The higher the number of times the event occurred, the higher the item will appear in the hierarchy.

For example, in the graphic below, there are two points at which there are sharp differences in support from one item to the next. This shift in support level is called a demarcation point, and indicates a sub-pattern in a longer sequence.

The demarcation points indicate multiple stages of an attack, and sometimes variations of the same type of attack on different types of systems within the network. For example, the SQL worm propagation attempt makes up 1000 of the 1122 hostile attempts. The demarcation point in the center of the graphic shows that there are two variations: attack from suspicious source, and UDP packet tcp dump. This can indicate how different systems process the same type of SQL worm attack.



Demarcation point

Demarcation point

Zoom-in on the snapshot graphic view using the zoom (🔍) button.

Arrange Elements in Graphic View

There are a number of ways you can view and rearrange elements in the graphic view. The buttons across the top allow you to zoom in, zoom out, and arrange the elements in different formations to give you better visibility of the overall pattern, whose shape can vary.

Snapshot Control Buttons

Button	Control	Description
	Fit Content	Sizes the graphic to the available display space.
	Zoom In / Zoom Out	Increases or decreases the size of the displayed graphic.
	Zoom Selected	Zooms in on a selected portion of a graphic.
	Hierarchic Layout	Presents nodes in a vertically descending cascade, similar to a family tree. Hierarchic layouts are appropriate when viewing relationships with a common root.
	Organic Layout	Displays nodes in an arrangement based on minimum edge length, which tends to cluster items with a common relation. Likewise, clusters with items in common will also tend to group together.
	Circular Layout	Positions items in hub-and-spoke arrangements with each one radiating edges to, or receiving edges from, the items with which it interacts. Circular layouts are most useful when multiple roots are present or there are a number of source-target relationships to clarify. If an organic layout is difficult to read because the edges are too dense, try a circular layout instead.
	Orthogonal Layout	Arranges items on the basis of logical connections, using electrical schematic-style right-angle layouts. These layouts are useful for clearly tracing connections and identifying node clusters.
	Overview	Opens a reduced rendering of the entire graph. You can drag the highlighted section in the reduction to move the displayed area in the main view.

Drag Items in Graphic View

In addition to rearranging the entire layout using the control buttons, you can rearrange an individual item by dragging and dropping it in the Viewer panel. In a graphic with many elements, this allows you to view individual items that may be overlapped.

Investigate Patterns in Snapshots

Pattern Discovery gives you immediate access to a host of investigative tools from a series of buttons. These same investigative tools are available from the right-click menu. The snapshot view and the patterns view offer most of the same investigative tools with a few specific differences.

Investigate Patterns from the Snapshots View

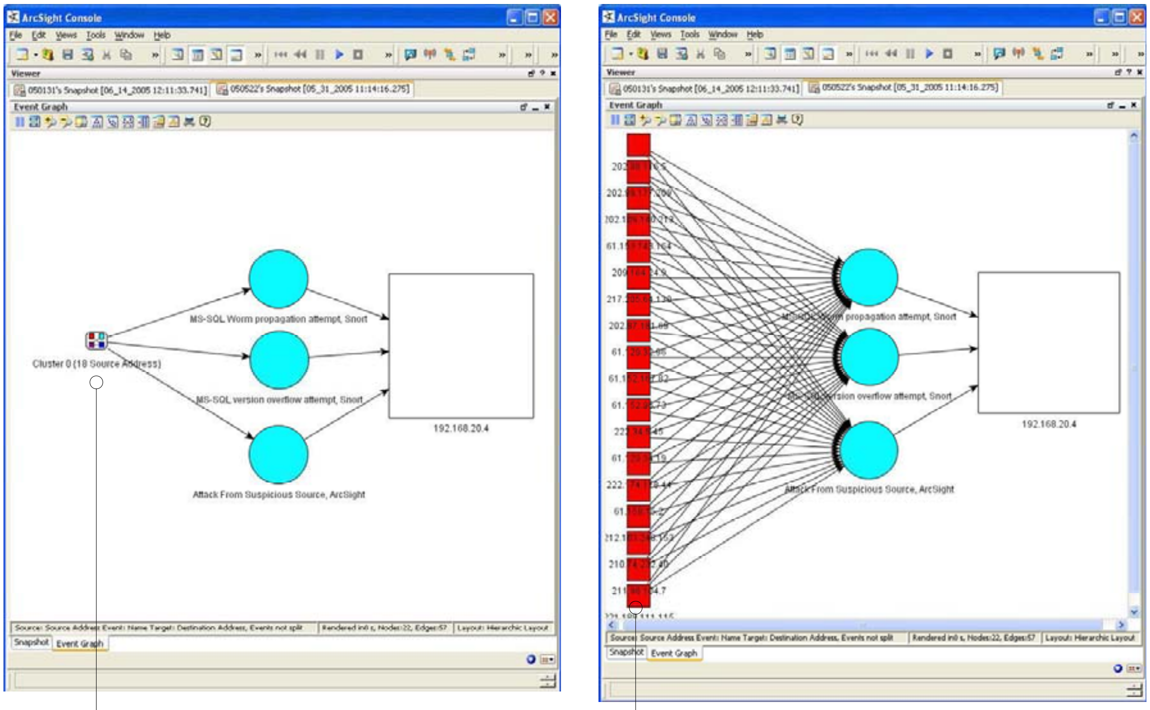
Right-click on any item in the graphical Snapshots view to open a new window within the snapshot view that contains details about the related events:

Right-Click Option	Description
Show related events	Click this view to open a new active channel within the **Snapshots** tab, filtered with a `matchesPattern` operator. This channel uses the contents of the complete pattern, or selected event-level in the pattern hierarchy, as its argument. To toggle back to the graphic view, click the Snapshot tab at the bottom of the snapshot Viewer panel.
Investigate	Click this to create a channel in a grid view that contains the associated events sorted according to the following criteria: ▪ Attacker Address ▪ Name ▪ Target Address
Tools	Click this drop down menu to use one of the following investigative network tools. **Configure…** includes the following options, and can be accessed directly through the larger Tools menu: ▪ **Nslookup**. Resolves an IP address to a host name (domain name) and vice versa. ▪ **Ping**. Determines whether a particular IP address is online and/or it tests and debugs a network by sending a packet and waiting for a response. ▪ **PortInfo**. Lists standard usage, e.g., WWW, FTP, etc. for a specified port number. ▪ **Traceroute**. Shows the path from the ArcSight Console to the IP address selected in the grid view, reporting the IP addresses of all routers in between. ▪ **WebSearch**. Search the Web through Google to find links to the keywords present in currently selected active channel grid view cells. ▪ **Whois**. Looks up who is behind a given domain name; information might include addresses and telephone numbers.

Right-Click Option	Description
	• **Results…** provides the results of running a network tool using the attributes of the selected pattern block For more information about ESM's network tools, see the online Help.
Create Rule…	Launches a Rules Editor in the Inspect/Edit panel. The rule you create here will be stored in the Rules resource tree under the personal rules of the user who created it. For instructions about how to construct a rule, see *Create Rules from Patterns* on page 30.
Show Event Graph	Displays the pattern as an event graph, which renders the pattern components and their relationships in a graphic form. For more information about ESM event graphs, see the online Help.
Show	Allows you to reset the graphic view with the following options: ▪ **Show all nodes**. Displays the entire snapshot graphic. This is helpful if you have drilled down and wish to redisplay the original snapshot. ▪ **Show all nodes containing selected items**. Displays only the event hierarchy that contains the selected item. ▪ **Hide all nodes containing selected items**. Displays all the event hierarchies that do not contain the selected item.

The example on the following page shows our sample pattern displayed as an event graph. By default to save space, the event graph clusters, (consolidates) items that have many members. In this case, the sample on the left shows the source address nodes consolidated into a single cluster with a single line representing the connections to each of the event name nodes.

To see the details and number of these connections, as shown in the example below on the right, you can uncluster the node by right-clicking the node and selecting **Uncluster selected nodes**.


ArcSight Console
File Edit Views Tools Window Help
Viewer
050131's Snapshot [06_14_2005 12:11:33.741]
050522's Snapshot [05_31_2005 11:14:16.275]
Event Graph
MS-SQL Worm propagation attempt, Snort
MS-SQL version overflow attempt, Snort
Attack From Suspicious Source, ArcSight
Cluster 0 (18 Source Address)
192.168.20.4
Snapshot
Event Graph

Source addresses clustered

Source addresses unclustered

Toggle between multiple views in the Snapshot window using tabs. Uncluserting the source address nodes allows you to see the details of those nodes.

When you use the right-click menu to open a new view, the view displays in a new tab within the snapshot pane. Use the tabs at the bottom of the pane to toggle between the views.

To close tabs in the snapshot view:

- Right-click the tab at the bottom of the snapshot view and select **Close**.

To rearrange open tabs in snapshot view:

- Use the down arrow (▼) to tile the open tabs horizontally, vertically, or as they fit best in the window.

- To select different views on an event graph, use the ▦▾ button. For details about viewing event graphs, see the online Help.

Investigate Patterns from the Patterns View

In the Patterns view, you can click the **Actions** button or right-click a pattern, where you can:

Button	Right-Click Option	Description
👓	Inspect Pattern	Click this option to open the Pattern Inspector in the Inspect/Edit panel. For more about how to inspect patterns, see *Investigate Patterns* on page 26.
⚡	Create rule from Pattern	Launches a Rules Editor in the Inspect/Edit panel. The rule you create here will be stored in the Rules resource tree under the personal rules of the user who created it. For instructions about how to construct a rule, see *Create Rules for Patterns* on page 30.
📝	Annotate Pattern	Click this to open the Annotations dialog box. This allows you to escalate a pattern to another user for further investigation. For more information about how to annotate a pattern, see *Annotate Patterns* page 36.
Show ▾	Event Graph	Displays the events as an event graph, which shows interactions between two or more devices. For more information about how to use ESM event graphs, see the online Help.
Show ▾	Related Events	Click this to open a grid view of the events contained in the Pattern Discovery snapshot.
Investigate ▾	Create Channel	Creates a channel based on the selected pattern block.
Investigate ▾	Add Condition to Editor	Displays the condition statement(s) associated with this pattern block. Conditions Editor (CCE). You can use this as a basis for building a new filter.

Schedule a Snapshot

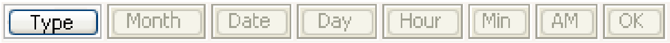
You can schedule a snapshot to be taken automatically at regular intervals. The frequency and timing you choose for snapshot schedules can be an important part of your daily analysis and operations. For example, as part of daily best practices, you can run Pattern Discovery once a day to capture event patterns that happen over a 24-hour period. You can extend the length of time to find patterns in longer term trends. To fully automate daily Pattern Discovery, you can add actions to a schedule, such as notifications, opening a case, or adding systems to an active list, if certain conditions are met.

1. In the Navigator panel, go to Pattern Discovery and click the **Profiles** tab.
2. Right-click a profile in the resource tree and select **Schedule Snapshots**.

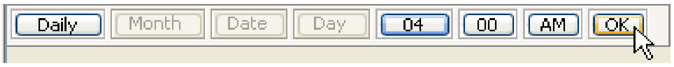
Because the profiles in the System Profiles group are locked, you cannot add a schedule to the profiles in the System Profiles folder.

If you wish to use one of the System Profiles as a template, first copy, then paste the profile into a user-writeable folder.

3 In the Scheduled Task Editor, click Add... or the space labeled **Click here for a new schedule**. This activates the schedule buttons.



4 Click **Type** and select the interval for the schedule from the list. This will activate the appropriate schedule buttons. Click the activated buttons to specify the exact time you wish the snapshot to be taken and click **OK** at the far right of the schedule button row, as shown below.



Select values from the appropriate schedule buttons and click OK.

5 Repeat step 4 to add more schedules for the same snapshot.

6 When you have added all the schedules you wish to add for this snapshot, click **OK** at the bottom of the Scheduled Task editor.

7 To add an action to be taken every time the profile is run, specify an action in the Actions tab of the profile editor, as described on page 14.

Re-open a Snapshot

If you have closed a snapshot in the Viewer panel, you can re-open it.

1 In the Navigator panel, go to Pattern Discovery and click the **Snapshots** tab.

2 Navigate to the snapshot graph you wish to view. Right-click the snapshot and select **Show Snapshot**.

Delete a Snapshot

1 In the Navigator panel, go to Pattern Discovery and click the **Snapshots** tab.

2 Right-click a snapshot in the resource tree and choose **Delete Snapshot**.

3 Click **Yes** to confirm the deletion.

3 Investigate Patterns

When you take a snapshot, the Pattern view shown in the snapshot is also saved in the **Patterns** tab of the Pattern Discovery resource tree. You can use the Patterns tab to access more event investigation tools.

View Patterns

You can re-open just the patterns view part of the snapshot in the Viewer panel.

1 In the Navigator panel, go to Pattern Discovery and click the **Patterns** tab.

2 Select one or more patterns in the resource tree, right-click the selection(s) and choose **View Pattern**. This opens the Pattern pane in the Viewer panel.

3 You can take the same actions on the Pattern view as outlined on page 25.

View Patterns with Filter

You can view patterns that have been assigned to a particular user or that are assigned to a particular stage using Annotations.

1 In the Navigator panel in Pattern Discovery, click the **Patterns** tab. Navigate to the pattern you wish to search on. Right click that pattern and select **View Patterns with Filter**.

2 To filter for patterns assigned to a particular user, use the Select a User drop-down menu to select a user. Click **OK**.

3 To filter for patterns assigned to a particular stage in a workflow, use the Select a Stage drop-down menu to select a stage. Click **OK**.

4 You can use one or both parameters for your search.

Inspect Patterns

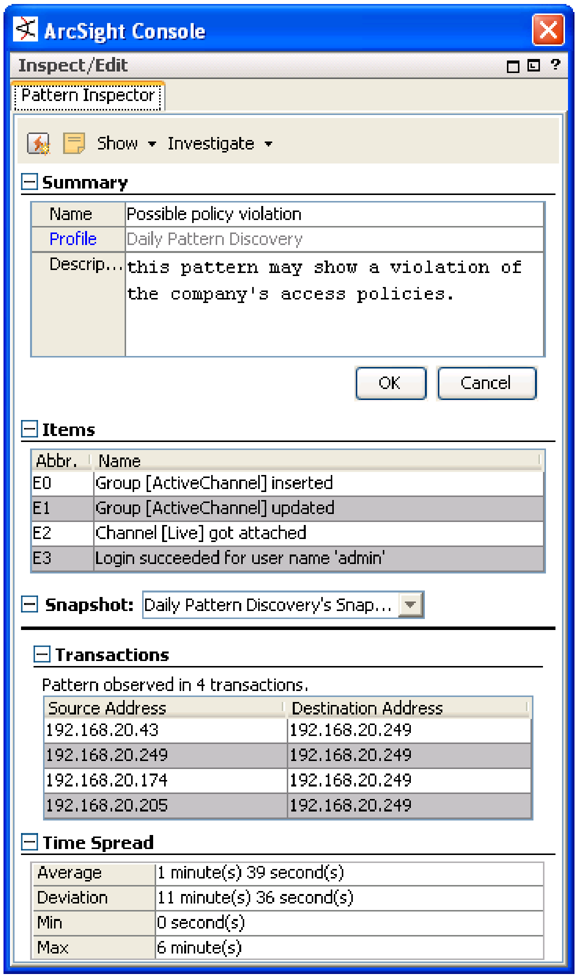
The Pattern Inspector provides you one more level of investigative control. If you decide that a pattern requires more investigation, you can use the Pattern Inspector to edit its details to be more descriptive for other users.

For example, you can rename the pattern from the default date and time of the snapshot to something more specific, such as “Potential worm attack.” Then you can add a description of the pattern so that another user can verify your findings.

To launch the Pattern Inspector:

1. In the Navigator panel, go to Pattern Discovery and click the **Patterns** tab.
2. Right-click a pattern in the resource tree and choose **Inspect Pattern…**.
3. Details of the pattern are displayed in the Inspect/Edit panel. Use the following sections as described below to tailor the pattern for further investigation:

Section	Description
Summary	Use this section to modify the name of the pattern from the default date-and-time name to a more descriptive name. You can also add a description of the pattern to aid other analysts. The Profile field is not editable.
Items	Use the **Investigate** drop-down button or right-click an item name to display the associated event details in a channel in the Viewer panel.
Snapshot	Use this drop-down menu to open patterns generated from the same profile definition so you can compare them.
Transactions	This table shows the source and destination data defined in the profile (address, port, host name, and so on) for the events involved in the pattern.
Time Spread	This table is only present if you selected Record Time Order in the profile. This table shows the details about the time spans involved between pattern occurrences. ▪ **Average**: the average time between events in this pattern ▪ **Deviation**: the difference in time spread between multiple occurrences of this pattern ▪ **Min**: the minimum time between events in this pattern ▪ **Max**: the maximum time between events in this pattern



Summary

Name	Possible policy violation
Profile	Daily Pattern Discovery
Descrip...	this pattern may show a violation of the company's access policies.

Items

Abbr.	Name
E0	Group [ActiveChannel] inserted
E1	Group [ActiveChannel] updated
E2	Channel [Live] got attached
E3	Login succeeded for user name 'admin'

Snapshot: Daily Pattern Discovery's Snap...

Transactions

Pattern observed in 4 transactions.

Source Address	Destination Address
192.168.20.43	192.168.20.249
192.168.20.249	192.168.20.249
192.168.20.174	192.168.20.249
192.168.20.205	192.168.20.249

Time Spread

Average	1 minute(s) 39 second(s)
Deviation	11 minute(s) 36 second(s)
Min	0 second(s)
Max	6 minute(s)

The Pattern Inspector shows item details and source/target transactions. You can rename a pattern to something more specific than the default date and time, and you can include a description.

Create Rules from Patterns

You can create rules based on the patterns that Pattern Discovery finds. Going back to our example, if Pattern Discovery finds a pattern between an MS-SQL worm propagation attempt reported by Snort, an MS SQL version overflow attempt, and an attack from a suspicious source, this indicates dangerous worm activity, and you may wish to create a rule that notifies users or quarantines a server whenever the system detects traffic that matches this pattern.

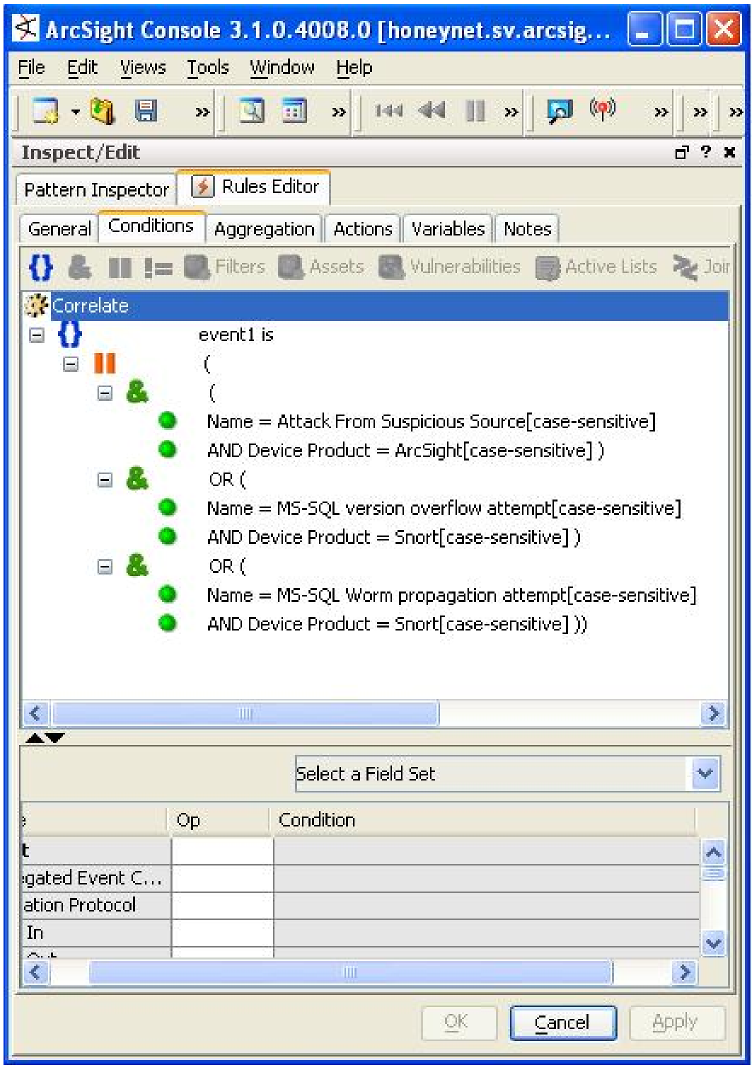
You can create rules from patterns within the Snapshot view in the Viewer panel, or within the Pattern Inspector in the Inspect/Edit panel.

- **To access the Rules Editor from the Snapshot view**: Right click on any item in the hierarchy graphic and select **Create Rule...**
- **To access the Rules Editor from the Snapshot Patterns view**: Right click on any item in the pattern block and select **Create Rule...**. You can also click the create rule button () in the button menu.
- **To access the Rules Editor from the Pattern Inspector**: In the button menu, click the create rule button ().

Once the Rules Editor is opened, do the following:

1. The Rules Editor will open in the Inspect/Edit panel showing the Attributes tab. Enter a name for the rule. You can also assign an external ID, alias, description, Version ID, owner, notification groups for the filter, and mark a resource as deprecated. Click **Apply**.

2. In the Rules Editor at the **Conditions** tab, you will see that the pattern's elements are already expressed in the common conditions editor. Modify the logic to express additional conditions you wish the rule to evaluate.



```
Correlate
    event1 is
      (
        (
          Name = Attack From Suspicious Source[case-sensitive]
          AND Device Product = ArcSight[case-sensitive] )
        OR (
          Name = MS-SQL version overflow attempt[case-sensitive]
          AND Device Product = Snort[case-sensitive] )
        OR (
          Name = MS-SQL Worm propagation attempt[case-sensitive]
          AND Device Product = Snort[case-sensitive] ))
```

Rules Editor Conditions tab automatically loads the pattern items.

The OR conditions are intentional and should be left in place. The Rules engine uses OR as a more memory-efficient way to process rules than AND. This is because it also applies a threshold value (the number of items involved) and distinct item names to track the components of the rule, rather than a blanket (join) approach.

3 At the **Aggregation** tab, set the number of matches and timeframe conditions you wish to set for the rule.

4 At the **Actions** tab, set the actions you wish the rule to carry out. These actions are triggered when the rule thresholds are met.

  a Click **Hide Empty Triggers** in the top row. This reduces the list of available thresholds to only those that are active (applicable to the conditions set in the rule).

  b Select a threshold from the list and click **Add**. Choose an action from the list that appears.

Action	Description
Set event field	In the dialog box, enter the following values and click **OK**: ♦ In Set Event Field, choose a field set from the drop-down menu. ♦ In the event fields grid, set values for the event fields you are interested in.
Send to open view operation	Communicates the triggered rule's associated events to a specialized ArcSight SmartConnector that resides with the Manager, which in turn forwards the information to an H-P Open View Operations installation for management purposes. This applies only in those environments where Open View has specifically been integrated with ArcSight. Request the ArcSight Tech Note concerning H-P Open View Ops for more information.
Send notification	In the dialog box, enter the following values and click **OK**: ♦ Specify a notification group in the Event Group drop-down menu. ♦ Click **Ack Required** if you want those notified to acknowledge that they received notification. ♦ Write the message you wish to send in the Message field.

Action	Description
Execute command	In the dialog box, enter the following values and click **OK**: ♦ Select an operating system platform from the drop-down menu. ♦ In the Command field, enter the command string you wish to execute. Syntax must be correct; the system does not test the accuracy of your command string. ♦ In the Parameters field, enter any parameters required for the command. For example, the archive tool requires the Manager name, admin name and password. This provides the system all the parameters necessary to execute the command without user intervention. ♦ In the Action Type drop-down menu, select one of the following: ♦ **Automatically run on manager**: This initiates the command automatically with no user intervention. ♦ **Run on Manager with Console confirmation**: This initiates a confirmation dialog box in the console for the designated user before the command is initiated. ♦ **Run on connector(s)**: This sends the command to the connector(s) that report the events.
Execute connector command	You can specify a command to be executed at the SmartConnector reporting the events, such as pause, stop or start event flow, or terminate or restart connector process. In the dialog box, enter the following values and click OK: ♦ In the Connector drop-down menu, select the SmartConnector you wish to execute the command. When you select an connector, the command field will be populated with the commands available for that connector. ♦ In the Command field, select the command you wish the connector to execute. The command may contain parameters that you must populate with appropriate values.
Export to external system	You can export the pattern to an external tracking system, such as BMC Remedy, if you have it configured to operate with ESM. In the dialog box, click **OK**.

Action	Description
Case	**Create new case**: You can add a pattern to a new or existing case. To add a pattern to a new case, enter the following values in the dialog box and click **OK**: ♦ In the case name field, enter a name for the case. Spaces and special characters are OK. ♦ In the description field, enter a description for the case. ♦ In the case group drop-down menu, select an existing case group in which to store this case profile. ♦ In the Consequence Severity drop-down menu, select a value that reflects the criticality of this pattern. This value appears in the Priority rating in the active channel if the conditions are met and the rule is triggered. ♦ 0-None ♦ 1-Insignificant ♦ 2-marginal ♦ 3-critical ♦ 4-catastrophic **Add to existing case**: To add a pattern to an existing case, enter the following values in the dialog box: ♦ In the Case drop-down menu, browse to an existing case and click **OK**.
Active List	You can add (or remove) a pattern to an active list, where the pattern details are available to other correlation tools for reference. ♦ To add a pattern to an active list, select **Add to Active List**. In the dialog box, select an active list from the drop-down menu and click **OK**. ♦ To remove a pattern from an active list, select **Remove from Active List**. In the dialog box, select an active list from the drop-down menu and click **OK**.

Action	Description
Session List	You can add a pattern to a session list, or terminate a session list based on a pattern, where its event details are available to other correlation tools for reference. ♦ To add a pattern to a session list, select **Add to Session List**. In the dialog box, select a session list from the drop-down menu and click **OK**. ♦ To terminate a session list, select **Terminate Session List**. In the dialog box, select a session list from the drop-down menu and click **OK**.

5 At the **Variables** tab, enter variables. Variables break down compound data fields into smaller parts so they can then be sorted and acted upon. For example, you can break the 7-part timestamp field or a multi-value URI into component parts, which can then be re-assembled in a more human-readable order, or sorted by individual component. For more about dependent variables, see the online Help and search for *Dependent Variables*.

6 You can keep track of changes made to a profile using the Notes feature. To add a note:

a In the Inspect/Edit panel, click the **Notes** tab.

b In the Notes field, enter a note and click **Save**. The entry is logged in the Table/List tabs.

c You can view notes as a table or as a list by toggling between the Table and List tabs. You can re-order the table view by clicking the header of the column by which you wish to sort.

Enable Rule and Activate It in Real-time Rules Folder

Before your rule can be used, it must be enabled and made active by being placed in the Real-Time Rules folder.

1 Verify that the rule is enabled. In the Navigator panel, right-click the rule and verify that **Enable Rule** is deactivated.

2 In the Navigator panel, expand the Real-time Rules folder until you see the subfolder in which you wish to link the rule. You can also link the rule to the top level of the Real-time Rules folder.

3 Select the rule and drag it from the host folder into the Real-time Rules folder or subfolder. In the Drag & Drop Options dialog box, select **Link**. This creates a linked copy of the rule so that if the rule is modified in one location, the change is reflected in the other.

Annotate Patterns

Annotation is a light-weight way to escalate a pattern to other users through your workflow system for analysis or investigation. You can use annotations instead of cases if you wish to escalate only one pattern. Use cases to escalate multiple patterns, or if you use a third-party incident management system.

You can annotate patterns from the snapshot and Pattern views in the Viewer panel, or within the Pattern Inspector in the Inspect/Edit panel.

To access the Annotation Editor from the Snapshot Patterns view:

1 In the Navigator panel, go to Pattern Discovery and click the **Snapshots** tab.

2 Double-click the snapshot you wish to see to display it in the Viewer panel.

3 Expand the pane so you can see the Patterns view at the bottom.

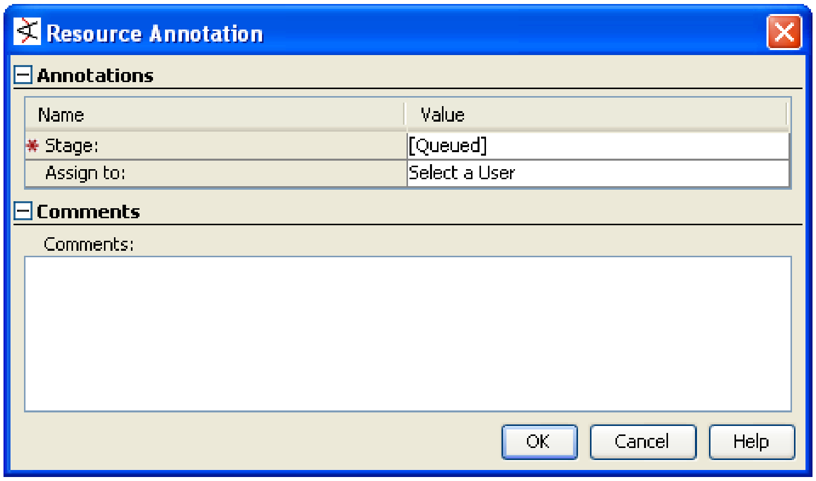
4 Right click any item in the pattern block and select **Annotate Pattern...**. You can also click the Annotate Pattern button (🗒) in the button menu.

To access the Annotation Editor from the Pattern Inspector:

1 In the Navigator panel, go to Pattern Discovery and click the **Patterns** tab.

2 Navigate to the pattern you wish to see and double-click it.

3 In the Inspect/Edit pane at the Pattern Inspector tab button menu, click the Annotate Pattern button (🗒).



Annotations

Name	Value
* Stage:	[Queued]
Assign to:	Select a User

Comments

Comments:

Workflow annotation for a pattern.

Once the Annotation Editor is open, enter the following values and click **OK**.

Field	Value
Stage	Select a stage from the drop-down menu. Queued is the default value.
Assign to	Select a user from the drop-down menu.
Comments:	Enter any comments you wish to communicate to other ESM users.

Delete a Pattern

1. In the Navigator panel, go to Pattern Discovery and click the **Patterns** tab.

2. Select one or more patterns.

3. Right-click the selected pattern (s) in the resource tree and choose **Delete Pattern**.

4. Click **Yes** to confirm the deletion.

Index

A

Actions tab, 14, 16, 26, 31

Aggregation tab, 31

annotate pattern, 15

Annotation Editor, 37

Attributes tab, 11, 17

C

components, 2, 23

- definition, 2
- groups, 2, 3, 35
- relationships, 2, 35

Conditions tab, 30, 31

N

notes

- adding, 17

Notes tab, 17, 35

P

Pattern Discovery

- algorithms, 2, 3, 18
- annotation, 6
- definition, 1, 2, 3, 9
- installation, 7
- lifecycle, 5, 6
- profiles, 9, 10

Pattern Inspector, 29

patterns

- active list, 16, 34
- annotate, 36
- cases, 34
- definition, 1, 2, 9, 13, 25, 28
- elements, 2
- export, 16, 33
- frequency, 2, 4
- investigation, 22, 27
- new, 1, 2, 4, 6, 14
- normal, 6
- recurrence, 2
- rules, 23, 30
- session list, 16, 35
- stages, 6

Patterns tab, 9, 27, 28, 36, 37

profile

- cases, 34
- definition, 9, 13, 14
- editor, 14
- modification, 10, 11, 17
- notes, 17
- notification groups, 14

Profiles tab, 11, 17, 18, 25

S

snapshots

- control buttons, 21
- definition, 9
- deleting, 27
- exploring, 19
- graphic view, 20, 22, 23, 24
- group, 13
- patterns, 12, 28, 30, 36
- scheduling, 25
- taking, 18

Snapshots tab, 9, 18, 22, 26, 27, 36

T

tabs

- Actions, 14, 16, 26, 31
- Aggregation, 31
- Notes, 17, 35
- Patterns, 9, 27, 28, 36, 37
- Profiles, 11, 17, 18, 25
- Snapshots, 9, 18, 22, 26, 27, 36

V

Variables tab, 35