Micro Focus Security ArcSight ESM Threat Detector

Software Version: 2.10

Solutions Guide

Document Release Date: June, 2018
Software Release Date: June, 2018

Legal Notices

Copyright Notice

Trademark Notices

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/ct-p/productdocs

Contents

Chapter 1: Overview

This chapter discusses the following topics:

What Threat Detector Can Do for You

Threat Detector, powered by ArcSight Pattern Discovery, helps you detect subtle, specialized, or long-term patterns in the flow of events. The Threat Detector product license enables the Pattern Discovery feature.

A Pattern Discovery profile defines the event fields to include in a pattern search; the scope and properties of the pattern; and the time period to search. Threat Detector provides the following profiles:

- **Browsing Pattern Detector** - This profile detects multiple computers connecting to the same sequence of external web servers. A short sequence of web servers usually indicates normal browsing, for example, users following links on web sites. However, any unexpected sequence of web servers should be investigated, as it might indicate activity such as:
  - Malware or spyware spreading through your organization and trying to connect to a command and control center.
  - Many users involved in a shared,non-work activity, such as a sports event webcast or online gaming.
- **Distributed Attacks Detector** - This profile detects patterns of attacks that originate from multiple sources and target a single host. These patterns indicate a distributed attack, which might be sophisticated and specifically targeting your organization. By analyzing a detected pattern, you can group together attacks that would otherwise be considered discrete, and ensure a more comprehensive and accurate response.
- **Early Stage Attack Detector** - This profile detects patterns of attacks that originate from a single source and target multiple destinations over time. Such a pattern often indicates a reconnaissance mission—either the early stage of a targeted attack, or an attempt to find vulnerabilities for a zero day exploit. The detected pattern can provide an early warning of upcoming attacks and valuable information to help mitigate those attacks.
- **AV Activity Profiler** - This profile detects patterns in the way antivirus (AV) software handles detected malware. The detected pattern groups together the events

generated by the AV software as it detects and mitigates a threat on a host. These patterns establish a baseline for normal AV activity and can be used to determine abnormal activity, which might indicate either an AV system malfunction or a malware outbreak.

- **Penetration Attempts** - Detects patterns that indicate a penetration attempt, such as a web application scanner looking for application vulnerabilities.

For information about using the Threat Detector profiles, see "Getting Started" on page 34.

For detailed information about Pattern Discovery, see Chapter 3, "Pattern Discovery" on page 10.

Supported Devices

The following devices typically generate events that apply to the Threat Detector profiles:

- Intrusion Prevention Systems (IPSs) and other solutions that include IPS functionality, such as firewalls and Unified Threat Management (UTM).
- Anti-virus software and other malware detection systems.

Chapter 2: Installing and Configuring Threat Detector

This chapter discusses the following topics:

Verifying Your Environment

Before you install Threat Detector, make sure that you are running a supported version of ArcSight ESM software version; or ArcSight ESM on ArcSight Express and ESM Express appliances. The *Threat Detector 2.10 Release Notes* indicate the supported ESM versions.

Installing the Threat Detector Content

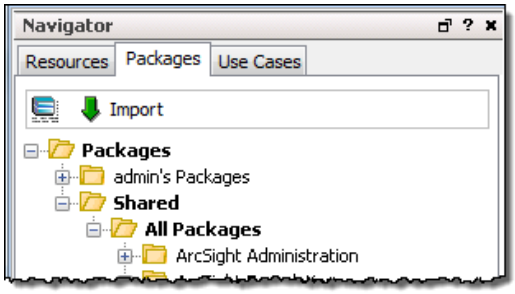
The Threat Detector product license enables the Pattern Discovery feature. The Threat Detector content is a self-contained solution that does not rely on any other ArcSight solution. You can install the Threat Detector content package alongside other solutions on the same ArcSight Manager. Before installing a new solution, Micro Focus recommends that you back up any existing solutions installed on the ArcSight Manager. For detailed instructions, see "Uninstalling Threat Detector" on page 40.

To install the Threat Detector content package:

1. Download the following Threat Detector content package bundle to the machine where you plan to run the ArcSight Console:

   `ArcSight-SolutionPackage-ThreatDetector.2.10.<nnnn>.0.arb`

   where `<nnnn>` is the 4 character build number specified in the *Threat Detector 2.10 Release Notes*.
2. Log into the ArcSight Console with an account that has administrative privileges.
3. In the Navigator panel, click the **Packages** tab.



4. Click **Import** ( ).
5. In the Open dialog, browse and select the package bundle file, and then select **Open**.
6. In the Packages for Installation dialog, leave the Threat Detector 2.10 checkbox selected and click **Next**.

   The Installing Packages dialog opens. The Progress tab shows how the installation is progressing. When the import is complete, the Results tab of the Importing Packages dialog is displayed together with the Packages for Installation dialog.
7. In the Installing Packages dialog, click **OK**.
8. In the Importing Packages dialog, click **OK**.
9. On the Packages tab of the Navigator panel, expand the Threat Detector 2.10 group to verify that the installation is successful and that the content is accessible in the Navigator panel.

Assigning User Permissions

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

The following process assumes that you have user groups set up and users assigned to those groups. In the following procedure, assign user permissions to all the following resource types:

- Dashboards
- Data monitors
- Filters
- Pattern Discovery (Profiles, Patterns and Snapshots)
- Queries
- Query Viewers

- Trends
- Use Cases

To assign user permissions:

1. Log into the ArcSight Console with an account that has administrative privileges.
2. For all the resource types listed above, change the user permissions:
   a. In the Navigator panel, go to the resource type and navigate to `ArcSight Solutions/Threat Detector 2.10`.
   b. Right-click the **Threat Detector 2.10** group and select **Edit Access Control** to open the ACL editor in the Inspect/Edit panel.
   c. In the ACL editor of the Inspect/Edit panel, select the user groups for which you want to grant permissions to the Threat Detector resources and click **OK**.

Configuring the Threat Detector Profiles

If you find that a profile detects too many false positives, edit the profile and increase the `Minimum Pattern Length` and `Minimum Pattern Occurrences` values. These values determine the number of events that constitute the pattern and the number of hosts for which the pattern is common.

Chapter 3: Pattern Discovery

ArcSight Pattern Discovery enables you to discover previously unknown patterns, which might pose a threat, and view them for analysis.

This chapter contains the following sections:

Pattern Discovery Overview

When finding threats by matching events against rules, you have to know the threat characteristics and create a rule that matches them. Pattern Discovery enables you to search for threat patterns with known characteristics as well, but you can also find unknown patterns, where the only characteristic you specify is that the transactions are related and repeat.

The purpose of Pattern Discovery is to:

- Effectively search streams of potentially millions of events for patterns, which are simply repeating sequences of related events.
- Establish a baseline of patterns that represent normal event traffic and filter them out.
- Analyze what remains for threats.

In this way you can discover and investigate patterns that might represent new threats or threats whose characteristics are not known to you.

ArcSight Pattern Discovery is a separate feature, installed with ESM, but is enabled by a separate product license. Contact your ArcSight representative to obtain a license key.

Pattern Discovery Lifecycle

The creation and use of Pattern Discovery consists of three phases:

- Create a profile (see "Creating or Editing a Profile" below)
- Generate snapshots (see "Taking a Snapshot" on page 19)
- Investigate patterns (see "Investigating Patterns" on page 24)

Use these options to analyze and respond to the patterns you discover in snapshots.

Option	Usage
Create Rule	Use the Rules Editor to create a rule from a detected pattern of events or a selected event-level in the pattern hierarchy.
Show Related Events	Open a new channel filtered with a `matchesPattern` operator that uses the whole pattern, or event-levels, as its argument.
Show Event Graph	Graph the complete pattern or a selected event-level in the pattern hierarchy, to analyze using the ArcSight Console's visualization tools.
Inspect Pattern	The Pattern Inspector shows details, and you can click the **Actions** button to apply the options described in this table.
Investigate	You can create an active channel, or add a filter to the editor, using (or not using) the name of the selected event item in the pattern.
Tools	Choose one of the network tools ArcSight provides to explore the origin of the selected event item.
Annotate Pattern	You can mark the pattern with a workflow collaboration **Stage** and **Assign** it to a user for filtering by Stages and Users resources.

Creating or Editing a Profile

A profile is a set of filters that define what fields to include in your pattern search, and the scope and properties of a pattern. It also specifies the time period to search. Profiles can be general or specific. Typically you would use several different profiles to define the parameters of snapshots, which collect all the events in the specified time frame and evaluates them according to the filters set in the profile.

Pattern Discovery profiles are in the `\All Profiles\ArcSight System` folder.

Use the following procedure to 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 on the Profile Editor **Attributes** tab, you can modify most of the values.

You cannot rename or delete profiles in the ArcSight System Profiles group. You can edit them, but Micro Focus recommends that you edit a copy you have pasted into another profiles folder. To use one of these profiles as is, see "Taking a Snapshot" on page 19.

Caution: You can delete or modify a profile if it has patterns and snapshots derived from it. However if you delete it, the patterns and snapshots that are derived from it no longer work and are not removed. If you modify it, they may not work as expected. Delete such patterns and snapshots when deleting their profile.

To copy and paste a profile to another folder, select the profile to copy. Go to **Edit | Copy (Paste)** or use Ctrl + C (V).

Editing Profile Attributes

Use the following procedure to edit a profile:

1. In the Navigator panel, go to Pattern Discovery and click the **Profiles** tab.
2. Expand the Profiles resource tree and navigate to the profile you want to modify.
3. In the Inspect/Edit panel on the **Attributes** tab, you can change most values and click **Apply**. Some values, such as version ID, are set by ArcSight and are not editable.

   Pattern Discovery Profile Attributes

Property	
Summary	A profile summary appears below the Attributes tab. The underlined items are 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 default value is **2** events.
Minimum Pattern Occurrences	Type or use the up/down arrows to select the minimum number of times for an event-association of the specified length to reoccur in order to qualify as a pattern. The default value is **2** occurrences.

Pattern Discovery Profile Attributes, continued

Property	
Start Time	Select a time stamp expression for the snapshot start time. Expressions are described below. • **$Now** The current time in the format hh:mm:ss. • **$Now - 1h** The current time minus 60 minutes. • **$Now - 1d** The current time minus 24 hours. • **$Now - 1w** The current time minus 7 days. • **$Today** The start of the current day (12:00:00). • **$Today - 1d** The start of the current day at midnight (12:00:00) minus 24 hours. In other words, the start of yesterday. • **$CurrentWeek** The start of the current week (Sunday 12:00:00). • **$CurrentMonth** The start of the current month (the 1st 12:00:00). The format of start time is $Now-<time>. The time is in increments of hours, days, weeks, or months.
End Time	Use the **$Now** drop-down menu to select a timestamp expression for the snapshot end time. The formats are the same as for Start Time, above.
Events:	
Event Fields Source Target	You can select one or more of these (event field, source, and target) for the pattern portion snapshot to display. Click in the data entry area and then click drop-down menu to see the field's chooser. In the Available Fields area, click the tab from which you want to choose. you can select one or more: • Field Sets. For more information, see the *ArcSight Console User's Guide*. • Local variables you created for this profile (see "Creating Local Variables" on page 17). • Fields and global variables that are relevant to a Pattern Discovery profile. In the Selected Fields section: • Use the up and down arrows to specify the order in which they appear. • Use the green alias icon to create an alias version. • Use the red X icon to remove one from the list. • You cannot specify date/time fields. • If you are going to add fields to a list, those fields must appear in this section (except the End Time field, which does not have to be here).
Restrict by Filter	Click the All Events drop-down menu to choose a filter from the Filters resource tree. The filter restricts the pool of events from which the snapshot is constructed.
Advanced: The check boxes in this section instruct the snapshot to capture elements pertaining to time, which can lend vital insight to a pattern.	

Pattern Discovery Profile Attributes, continued

Property	
Record Time Order	This includes 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 percent of the time, B-A-C 35 percent, and A-C-B 25 percent. Because event sequences can reveal intent, you can detect and act upon certain kinds of activity even sooner.
Split on Inactivity	This detects potentially meaningful decreases in activity between duplicate source/target pairs. It creates 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 means 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 time frame 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 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.
Version ID	If this profile came in a package or if you have exported it to a package, this is the package’s version ID.
Description	A text description of the profile.

Pattern Discovery Profile Attributes, continued

Property	
Assign:	
Owner	The user with responsibility for the profile.
Notification Groups	The user groups to notify concerning changes to a profile.

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

Specifying Actions

The **Actions** tab enables you to select a trigger, then specify the action to take when that trigger occurs.

To specify an action:

1. 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. Specify when to take the action (the trigger). Select one of the following trigger options:

Trigger Option	Description
On Pattern Discovered	This specifies that the action 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** and select one of the following options:

Pattern Discovery Actions

Action Option	Description
Annotate Pattern	In the dialog box, enter the following values and click **OK**: • Select a Stage from the drop-down menu. • Assign a user from the drop-down menu.
Set Event Field	In the dialog box, enter the following values and click **OK**: • Select a Field Set from the drop-down menu. • In the event fields grid, set values for the event fields you are interested in.

Pattern Discovery Actions, continued

Action Option	Description
Send Notification	Specify a notification group in the Notification Group dropdown menu. • Click **Ack Required** if those notified should acknowledge that they received notification. • Write the message to send in the Message field.
Execute Command	In the dialog box, enter the following values and click **OK**: • Select an operating system platform from the dropdown menu. • Enter the command string. Use correct syntax; the system does not validate command strings. • Enter required parameters. For example, the archive tool needs the manager name, admin name, and password. Specifying them lets the system execute the command without user intervention. • In the Action Type drop-down menu, select one of the following: **Automatically run on manager:** Initiates the command with no user intervention. **Run on Manager with Console confirmation**: Displays a confirmation dialog box in the ArcSight Console for the designated user before the command is initiated. **Run on connector(s):** Sends the command to the connectors that report the events.
Execute Connector Command	Specify a command to be executed at the SmartConnector reporting the events, such as pause or stop/start event flow. Enter the following values and click **OK**: • In the Connector drop-down menu, select the SmartConnector to execute the command. When you select an connector, the command field is populated with the commands available for that connector. • In the Command field, select the command for the connector to execute. The command may containrequired parameters.

Pattern Discovery Actions, continued

Action Option	Description
Export to External System	You can export the pattern to an external tracking system if you configured it to operate with ArcSight 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**. • You cannot add fields to an Active List f they are not present in the Events section of the Profile. • You cannot add any date/time-based fields to an Active List since data/time fields cannot be included in the Events section of the profile.
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**. • You cannot add fields to an Session List if they are not present in the Events section of the Profile. • You cannot add any date/time-based fields to an Session List (except EndTime) since data/time fields cannot be included in the Events section of the profile. The End time displayed in the Add to Session List action is the time the entries are added to the session list.

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

Creating Local Variables

Click the **Local Variables** tab to manage local variables for this profile. These are available to select from the drop-down menu on the **Attributes** tab for Event Fields, Source, and Target attributes associated with the pattern.

From this tab you can:

- Add a new variable, which enables you to
  - Name the variable.
  - Specify a function (expression).

  - Specify the arguments. Available arguments depend on the function.
- Edit an existing variable.
- Remove a selected variable.
- Make a variable global, which means it is available to resources outside this profile. If you make a local variable global, it moves it from the **Local Variables** tab to the **Fields and Global Variables** tab in the chooser for Event Fields, Sources and Targets, on the **Attributes** tab.

For more information on using local and global variables, see the *ArcSight Console User's Guide*.

Pattern Discovery supports the following variable return data types:

Byte Double Enumeration Integer	• Long • Resource ID • String • Address

Therefore, function variables that return an unsupported data type are not supported. For example, the following functions or function categories are not supported:

- Non-SQL-mode variables.
- Variables that return a list, such as `ActorByAccountID.AccountID` and variables that operate on multi-mapped active lists or overlapping session lists.
- Variables that return a boolean value, such as the Category Model function `hasRelationship`.

Adding Notes

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**.

   Caution: You can delete or modify a profile if it has patterns and snapshots derived from it. However if you delete it, the patterns and snapshots that are derived from it no longer work and are not removed. If you modify it, they may not work

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

Deleting 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**.

   Caution: You can delete or modify a profile if it has patterns and snapshots derived from it. However if you delete it, the patterns and snapshots that are derived from it no longer work and are not removed. If you modify it, they may not work as expected. Delete such patterns and snapshots when deleting their profile.

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

Taking a Snapshot

A snapshot is a record of qualifying events that occurred over a specified period of time and evaluated according to the snapshot profile. When the Pattern Discovery algorithm runs on the specified data set, it displays the result as a graphic, which you can use for investigation and analysis.

You can generate snapshots manually, or run them on a schedule.You are likely to generate snapshots 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** on the Snapshots tab.

You can also discover patterns directly from active channels. Right-click a channel in the Navigator panel and choose **Discover Patterns**.

To take snapshots:

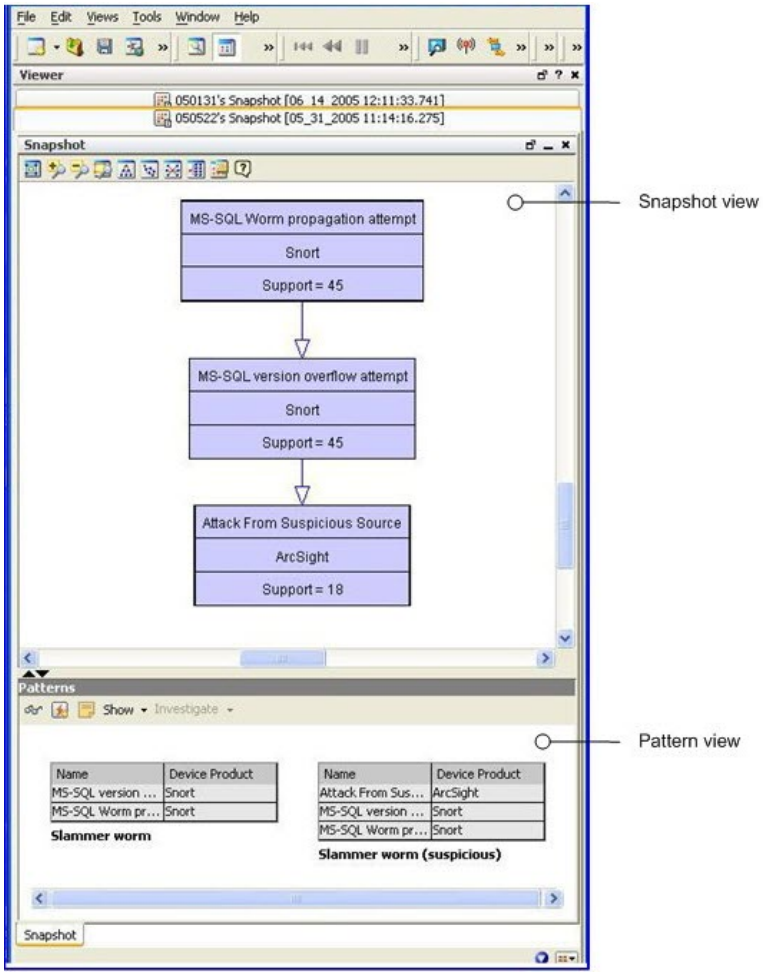
1. In the Navigator panel, go to Pattern Discovery and click the **Profiles** tab.
2. Right-click a profile in the resource tree and select **Take Snapshot**.
3. In the Viewer panel, the system processes the snapshot request and shows each process as the Pattern Discovery engine runs:

4. When the process finishes, the system displays the snapshot in the Viewer panel. See "Exploring a Snapshot" below to continue.

Tip: If the pattern is empty, no events passed the profile's filter restrictions during the specified period. Adjust these profile specifications and generate the snapshot again.

Exploring a Snapshot

Following is an example of a snapshot. The views are linked; click a node in the snapshot view to see its details in the patterns view.



The upper part of the Viewer panel presents the snapshot view, which shows a hierarchy of related event nodes.

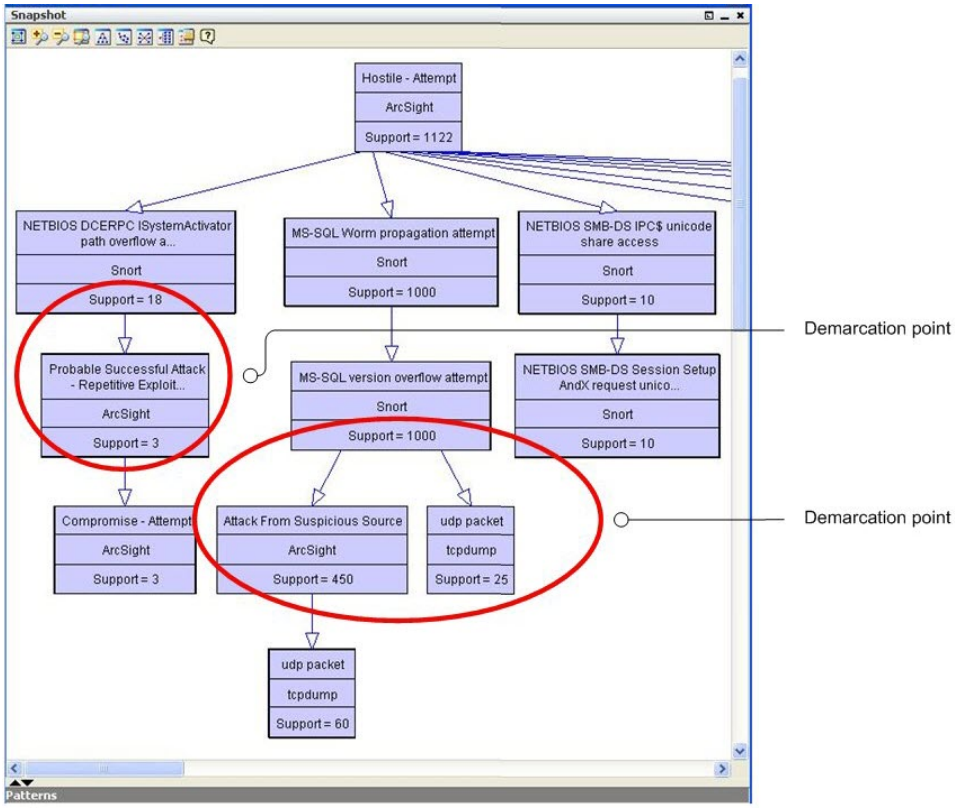
The lower part of the Viewer panel is the patterns view, which shows blocks of events from the hierarchy that are most closely related. Each block of events represents one specific path through the pattern hierarchy.

The example shows two patterns and a demarcation point (between support = 45 and support= 18). The top two events are the SQL worm. The last event is generated by the system. 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. Determining that will help you to tighten your network security.

The “support” value for each node is the number of times that event occurred with its related events. The higher the number, the higher the item appears in the hierarchy.

For example, in the following image, 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 attack stages, and sometimes variations of the same type of attack on different network systems. 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 tcpdump. This can indicate how different systems process the same type of SQL worm attack. Demarcation points are circled, as shown:



Arranging Elements in Graph View

Use 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.

Tools for Rearranging Graphic Elements

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	Arranges nodes based on minimum edge length, which tends to cluster items with a common relation. Clusters with items in common also tend to group together.
	Circular Layout	Hub-and-spoke arrangements with each node 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.
	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.

Scheduling a Snapshot

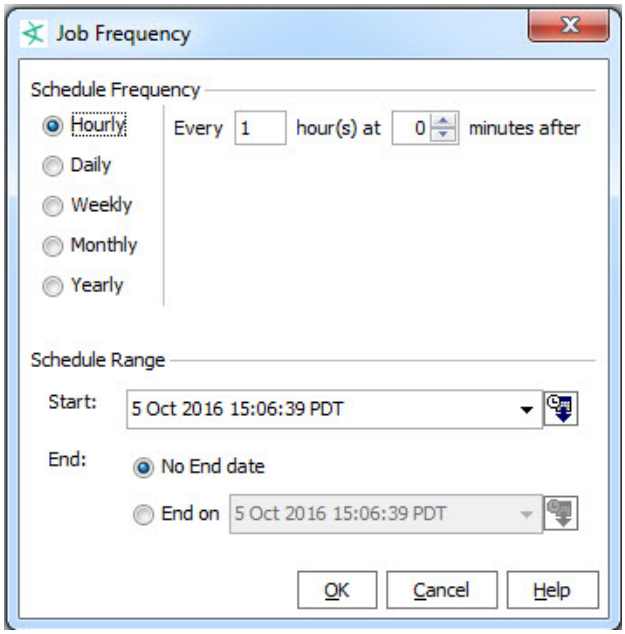
You can schedule a snapshot to be taken at intervals. The schedule frequency can be part of your daily analysis and operations. For example, as a best practice, you can run Pattern Discovery once a day to capture event patterns that happened over the last 24 hours. You can specify a longer period to find patterns with a longer term. To fully automate daily Pattern Discovery, add actions to a schedule, such as sending notifications, opening cases, 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**.

Note: Profiles in the System Profiles group are locked; you cannot add to or modify the schedules for profiles in the System Profiles folder.

To use one of the System Profiles as a template, copy it to another folder.

3. On the Jobs tab, click **Add**.
4. In the Summary field at the bottom, select **Click here** to set up schedule frequency. This activates the Job Frequency dialog.



5. Click **OK** when you have set the frequency and time range.
6. Repeat the process to add more schedules for the same snapshot.
7. When you have added all the schedules for this snapshot, click **OK** at the bottom of the Jobs tab.
8. 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 in "Specifying Actions" on page 15.

Re-opening 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. Right-click the snapshot and select **Show Snapshot**.

When the snapshot's graphic has formed in the Viewer panel, you can click the icons at the top of the view to change its layout as described in the *ArcSight Console User's Guide*.

Deleting 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.

Investigating 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.

Investigating Patterns in Snapshot View

Pattern Discovery gives you access to investigative tools from a series of buttons. These same 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. 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:

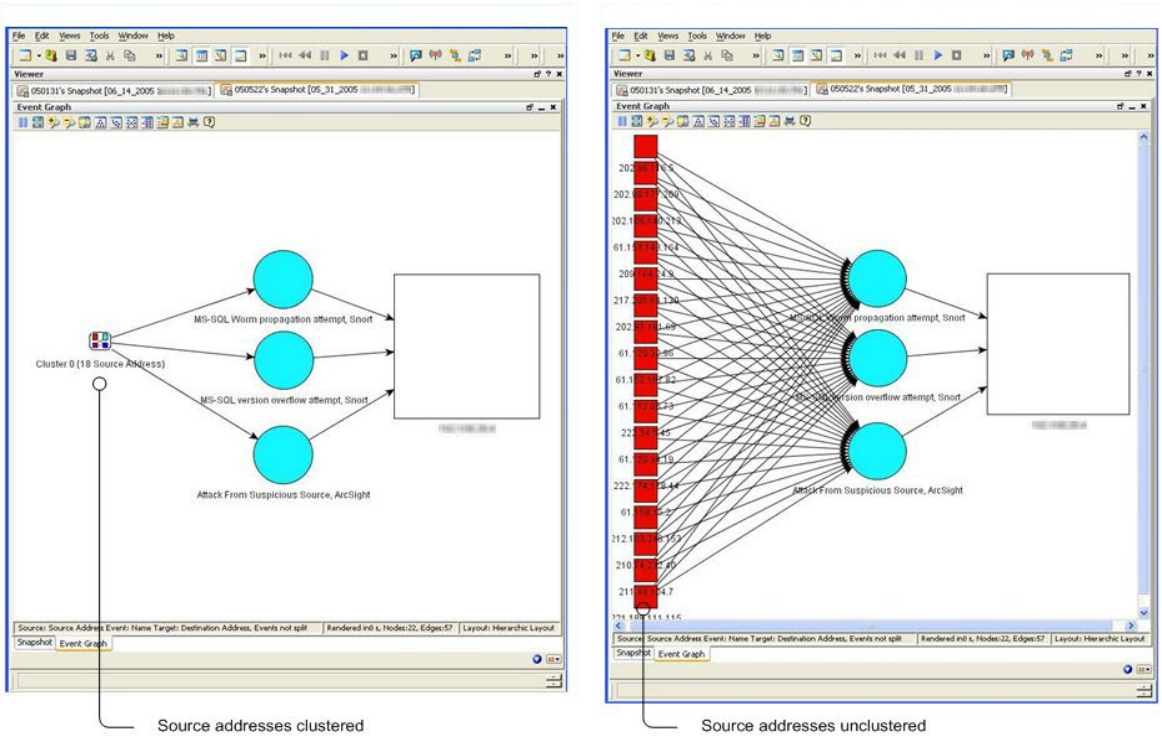
Right-Click Options for Pattern Investigation

Right-Click Option	Description
Show related events	Opens a new active channel in the Snapshots tab, filtered with a matchesPattern operator. This channel uses the 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 (for older ESM versions) Analyze in Channel (for ESM 6.11 or later)	Creates a channel in a grid view that contains the associated events sorted according to Attacker Address, Name, and Target Address.

Right-Click Options for Pattern Investigation, continued

Right-Click Option	Description
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 such as WWW or FTP 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. • **Results** - provides the results of running a network tool using the attributes of the selected pattern block For more information about network tools, see the online Help.
Create Rule...	Launches a Rules Editor in the Inspect/Edit panel. The rule you create here is 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 the topic "Creating Rules from Patterns" on page 29.
Show Event Graph	Displays the pattern as an event graph, which shows pattern components and their relationships in graphic form. For more information about ESM Threat Detector 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 re-display 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 in shows our sample pattern displayed as an event graph. To save space, the event graph 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 on the right, uncluster the node by right-clicking the node and selecting **Uncluster** selected nodes.



Toggle between multiple views in the Snapshot window using tabs. Unclustering 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, it 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 and select Close.

To rearrange open tabs in snapshot view:

1. Use the down arrow ( ) to tile the open tabs horizontally, vertically, or to fit.
2. To select different views on an event graph, use the button. For details about viewing event graphs, see the online Help.

Investigating Patterns in the Pattern View

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 selections 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 described in "Investigating Patterns in Snapshot View" on page 24.

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

Toolbar Buttons in Patterns View

Button	Right-Click Option	Description
	Inspect Pattern	Opens the Pattern Inspector in the Inspect/Edit panel. For more information, see "Investigating Patterns" on page 24.
	Create rule from Pattern	Launches a Rules Editor in the Inspect/Edit panel. The rule you create here is stored in the Rules resource tree under the personal rules of the creating user. For instructions about how to construct a rule, see the topic "Creating Rules from Patterns" on page 29.
	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 "Annotating Patterns" on page 31.
	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 Threat Detector event graphs, see the topic "Graphing Attacks" in the *ArcSight Console User's Guide*.
	Related Events	Click this to open a grid view of the events contained in the Pattern Discovery snapshot.
	Create Channel	Creates a channel based on the selected pattern block.
	Add Condition to Editor	Enables you to edit the condition statements associated with this pattern block.

Viewing Patterns with Filter

You can view patterns assigned to a particular user or stage using Annotations.

1. In the Navigator panel in Pattern Discovery, click the **Patterns** tab.
2. Navigate to the pattern.
3. Right-click a pattern and select **View Patterns with Filter**.
4. To filter for patterns assigned to a user, use the Select a User drop-down menu.
5. To filter for patterns assigned to a workflow stage, use the Select a Stage drop-down menu.
6. You can use one or both parameters for your search.

Inspecting 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:

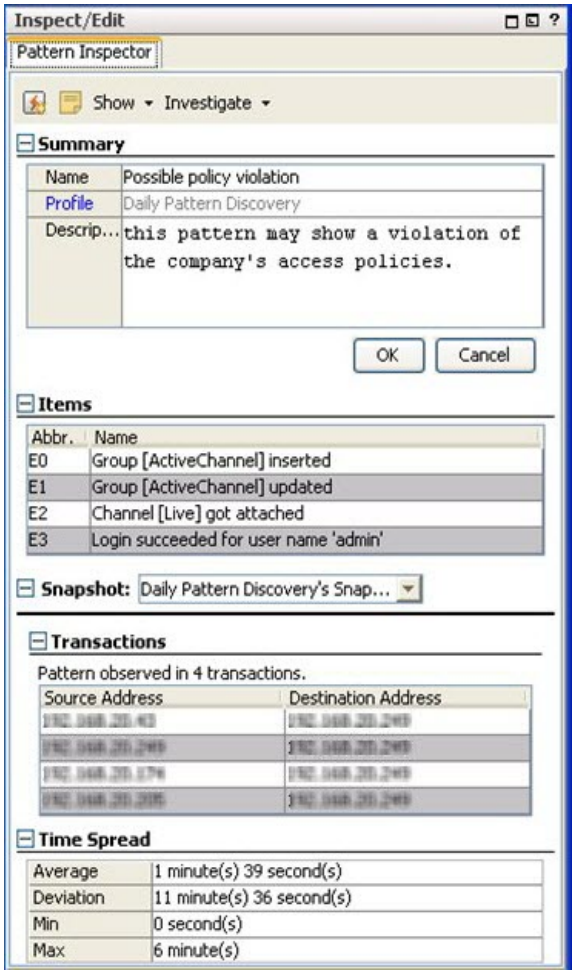
1. In the Navigator panel, go to **Pattern Discovery** and click the **Patterns** tab.
2. Right-click a pattern in the resource tree and choose **Inspect Pattern**.

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:

Pattern Details

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

The following 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.



Creating Rules from Patterns

You can create rules based on discovered patterns. 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 can create a rule to notify users or quarantine a server whenever the system detects traffic that matches this pattern. For additional information on creating and managing rules, see "Managing Rule Actions" topic in the *ArcSight Console User's Guide*.

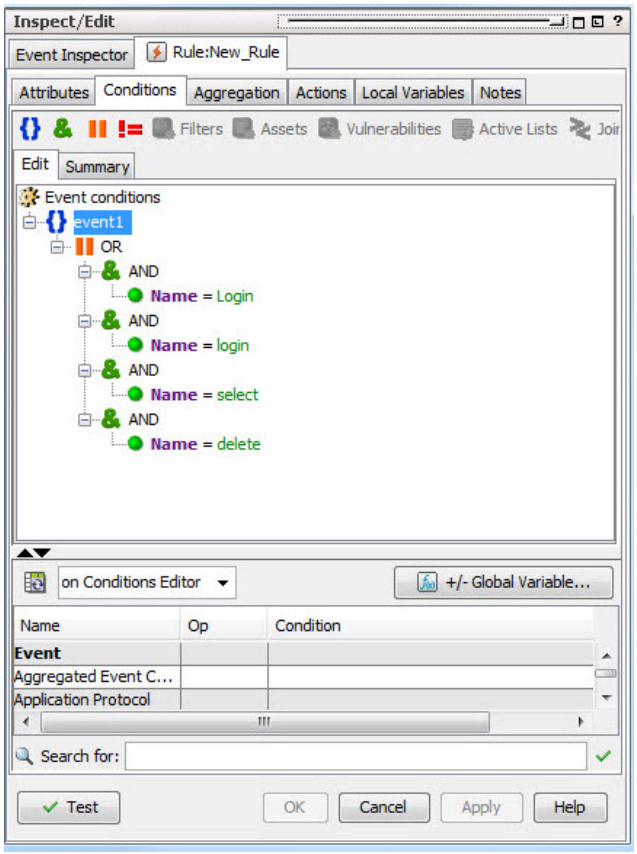
You can create rules from patterns in the Snapshot view in the Viewer panel, or in the Pattern Inspector in the Inspect/Edit panel.

- 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.

The Rules Editor opens in the Inspect/Edit panel showing the Attributes tab. Once the Rules Editor is open, do the following:

1. 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 on the Conditions tab, the pattern's elements already appear in the common conditions editor. Modify the logic to express additional conditions for the rule to evaluate. For information, see the "Rules Authoring" chapter in the *ArcSight Console User's Guide*.



Note: The OR conditions are intentional. OR is a more memory-efficient way to process rules than AND 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 time frame for the rule.

4. At the Actions tab, set the actions for the rule to trigger when the thresholds are met.
   a. Click **Hide Empty Triggers** in the top row. This reduces the list of available thresholds to 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. See the ArcSight Console User's Guide.
5. At the Variables tab, enter variables. Variables break down compound data fields into smaller parts so they can 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 be reassembled in a more human-readable order, or sorted by 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:
   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 column header.

Annotating Patterns

Annotation is a light-weight method to escalate a pattern to other users through your workflow system for analysis or investigation. You can use annotations instead of cases 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 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 and double-click it.

3. In the Inspect/Edit pane on the Pattern Inspector tab button menu, click the **Annotate Pattern** button.
4. In the Resource Annotation editor, enter the following values and click **OK**.

Field	Value
Stage	Select a stage from the drop-down menu. The default is Queued.
Assign to	Select a user from the drop-down menu.
Comments	Enter any comments to communicate to other ArcSight users.

Deleting Patterns

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 patterns in the resource tree and choose **Delete Pattern**.
4. Click **Yes** to confirm.

Usage Guidelines

Establishing a Baseline of Normal Patterns

Use broader profiles and more frequent snapshots to capture an example of all the patterns that occur as part of normal business practices. identifying normal patterns takes time and investigation, and requires that you be familiar with traffic in your enterprise.

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

Using 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 at intervals.
- **Investigation and analysis.** Once assigned to an analyst, the analyst can use the full array of ArcSight'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 ArcSight 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.

Performance Considerations

Pattern Discovery jobs can be resource intensive. Under high EPS, for example, greater than 15K, Pattern Discovery jobs can cause a degradation in performance, and may fail to return a matching result set. Micro Focus recommends that you reduce the scope or frequency of Pattern Discovery jobs when running a system with high EPS.

Adjusting Pattern Discovery Memory

By default, Pattern Discovery limits its memory usage to about 4 GB of memory. However, if the search for patterns involves too many transactions and events, the task can run out of memory and abort. If the Pattern Discovery task aborts, a message to that effect appears in the ArcSight Console. Run the Pattern Discovery task again after increasing the Pattern Discovery memory usage limit.You can control the memory usage limit indirectly by changing the maximum number of transactions and events that can be held in memory.

For information, see "Adjusting Pattern Discovery Memory" topic in the Configuration chapter of the *ESM Administrator's Guide*.

Chapter 4: Using Threat Detector Content

This chapter discusses the following topics:

Getting Started

Use the Threat Detector profiles to generate snapshots of events and investigate patterns of suspicious activity in your network. You can access the profiles from the Threat Detector use case, or directly from the Navigator panel, as described in the following procedures. If you are new to Threat Detector, try the use case first, as it provides a dashboard of the events that pertain to Threat Detector.

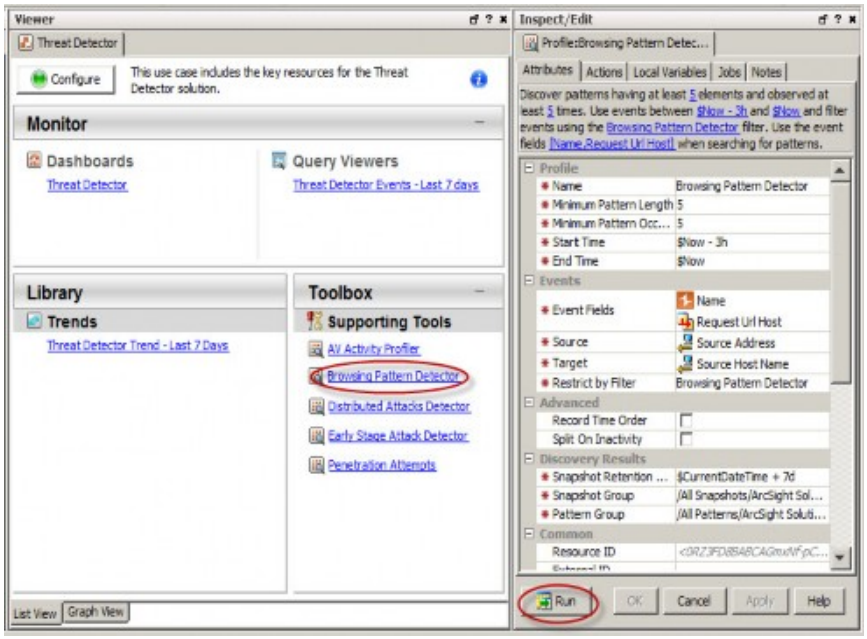
To use the Threat Detector use case:

1. In the Navigator panel, select the **Use Cases** tab.
2. Navigate to the Threat Detector use case at:

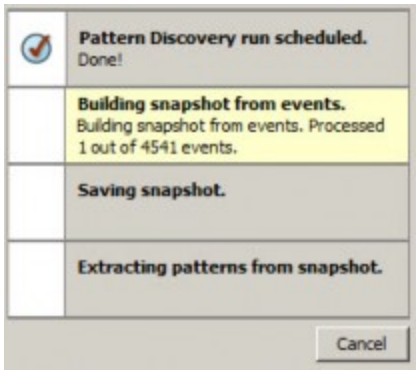
   `All Use Cases/ArcSight Solutions/Threat Detector 2.10/Threat Detector`
3. Right-click the use case and select **Open Use Case**.

   The resources that make up the use case are displayed.
4. Click the **Threat Detector** dashboard listed under Dashboards to display the events for the last seven days which satisfy the conditions of the Pattern Discovery profiles.

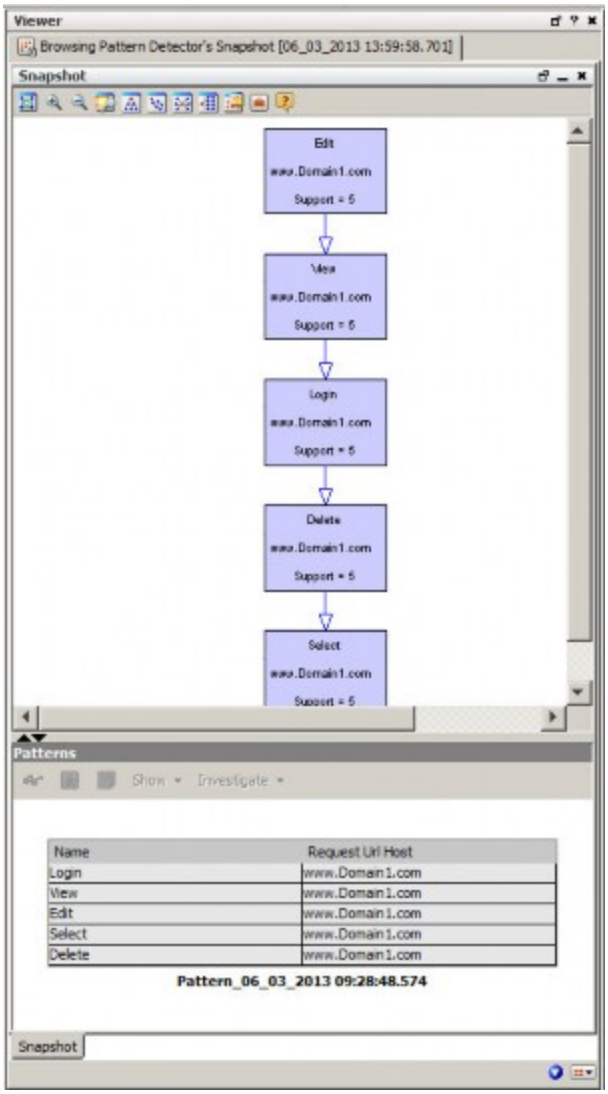
   For an explanation of the profiles, see "Overview" on page 5.
5. Return to the use case and click one of the Pattern Discovery profiles listed under **Supporting Tools** to open the profile in the Inspect/Edit panel.
6. Review the profile settings, and then click **Run** at the bottom of the Inspect/Edit panel to take a snapshot of events.



In the Viewer panel, the system processes the snapshot request and shows each process as the Pattern Discovery engine runs:



Following is a sample snapshot:



For detailed instructions on how to investigate patterns, schedule snapshots, and more, see "Pattern Discovery" on page 10.

To access the profiles from the Navigator:

1. Open the ArcSight Console, select **Pattern Discovery** in the Navigator panel, and navigate to `/All Profiles/ArcSight Solutions/Threat Detector 2.10`.
2. Right-click a profile, and select **Take Snapshot**.

Resources That Support the Threat Detector Use Case

The following table lists all the resources explicitly assigned to the Threat Detector use case and any dependent resources.

Monitor Resources

Resource	Description	Type	URI
Threat Detector	This dashboard includes a data monitor that displays the last 30 events and a query viewer that displays events from the last seven days that pertain to Threat Detector.	Dashboard	ArcSight Solutions/Threat Detector 2.10/
Threat Detector Events - Last 7 days	This query viewer displays events from the last seven days that pertain to Threat Detector.	Query Viewer	ArcSight Solutions/Threat Detector 2.10/

Library Resources

Resource	Description	Type	URI
Threat Detector Last 30 Events	This data monitor displays last 30 events that pertain to Threat Detector.	Data Monitor	ArcSight Solutions/Threat Detector 2.10/
Browsing Pattern Detector	This filter detects events with a port of 80 or 443 and a request URL.	Filter	ArcSight Solutions/Threat Detector 2.10/
IDS Found	This filter detects events that are categorized as found by an intrusion detection system (IDS).	Filter	ArcSight Solutions/Threat Detector 2.10/
Threat Detector Events	This filter detects all events that pertain to Threat Detector.	Filter	ArcSight Solutions/Threat Detector 2.10/
Malware Activity	This filter detects events categorized as malware.	Filter	ArcSight Solutions/Threat Detector 2.10/

Library Resources, continued

Resource	Description	Type	URI
AV Activity Profiler	This profile detects patterns in the way antivirus (AV) software handles detected malware. The detected pattern groups together the events generated by the AV software as it detects and mitigates a threat on a host. These patterns establish a baseline for normal AV activity and can be used to determine abnormal activity, which might indicate either an AV system malfunction or a malware outbreak.	Profile	`ArcSight Solutions/Threat Detector 2.10/`
Penetration Attempts	This profile detects patterns that indicate a penetration attempt, such as a web application scanner looking for application vulnerabilities.	Profile	`ArcSight Solutions/Threat Detector 2.10/`
Browsing Pattern Detector	This profile detects multiple computers connecting to the same sequence of external web servers. A short sequence of web servers usually indicates normal browsing, for example, users following links on web sites. However, any unexpected sequence of web servers should be investigated, as it might indicate activity such as: • Malware or spyware spreading through your organization and trying to connect to a command and control center. • Many users involved in a shared, non-work activity, such as a sports event webcast or online gaming.	Profile	`ArcSight Solutions/Threat Detector 2.10/`
Early Stage Attack Detector	This profile detects patterns of attacks that originate from a single source and target multiple destinations over time. Such a pattern often indicates a reconnaissance mission–either the early stage of a targeted attack, or an attempt to find vulnerabilities for a zero day exploit. The detected pattern can provide an early warning of upcoming attacks and valuable information to help mitigate those attacks.	Profile	`ArcSight Solutions/Threat Detector 2.10/`
Distributed Attacks Detector	This profile detects patterns of attacks that originate from multiple sources and target a single host. These patterns indicate a distributed attack, which might be sophisticated and specifically targeting your organization. By analyzing a detected pattern, you can group together attacks that would otherwise be considered discrete, and ensure a more comprehensive and accurate response.	Profile	`ArcSight Solutions/Threat Detector 2.10/`

Library Resources, continued

Resource	Description	Type	URI
Threat Detector Events - Last 7 Days	This trend-based query retrieves all of the events for the last seven days that pertain to Threat Detector.	Profile	`ArcSight Solutions/Threat Detector 2.10/`
Threat Detector Events	This query retrieves events detected by the Threat Detector filters.	Query	`ArcSight Solutions/Threat Detector 2.10/`
Threat Detector Trend - Last 7 Days	This trend stores the events from the last seven days that pertain to Threat Detector.	Trend	`ArcSight Solutions/Threat Detector 2.10/`

Appendix A: Uninstalling Threat Detector

This appendix provides instructions on how to backup and uninstall Threat Detector.

Backing Up Threat Detector

Micro Focus recommends that you keep a backup of the current state before making content changes or installing and uninstalling solution packages.

You can back up the solution content to a package bundle file that ends in the .arb extension as described in the process below.

To back up a solution package:

1. Log into the ArcSight Console with an account that has administrative privileges.
2. In the **Packages** tab of the Navigator panel, navigate to `All Packages/ArcSight Solutions`.
3. Right-click the Threat Detector 2.10 package () and select **Export Package to Bundle**.

   The Package Bundle Export dialog displays.
4. In the Package Bundle Export dialog, browse for a directory location, specify a filename and click **Next.**
5. When the export is complete, click **OK**.

The resources are 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.

Uninstalling the Package

Before uninstalling the Threat Detector content package, back up all the packages for all the solutions currently installed. For example, if the Threat Detector content and the CIP for SOX solution are both installed on the same ArcSight system, export the package for each solution before uninstalling either solution. Back up the CIP for SOX package into a package bundle (`.arb`) file and then back up the Threat Detector content package into a different package bundle (`.arb`) file before uninstalling either solution.

To uninstall the content package:

1. Log into the ArcSight Console with an account that has administrative privileges.
2. Delete any snapshots that were generated by Threat Detector:
   a. In the Navigator panel Resources tab, select **Pattern Discovery** from the drop-down menu.
   b. Click the **Snapshots** tab, navigate to `All Snapshots/Arcsight Solutions/Threat Detector 2.10`, and expand the group.
   c. Press the Ctrl key and click each snapshot, until all the snapshots are highlighted.
   d. Right-click the snapshots, select **Delete Snapshot**, and agree to the delete confirmation prompt.
3. Delete any patterns that were generated by Threat Detector:
   a. In the Navigator panel Resources tab, click the **Patterns** tab, navigate to `All Patterns/Arcsight Solutions/Threat Detector 2.10`, and expand the group.
   b. Press the Ctrl key and click each pattern group, until all the groups are highlighted.
   c. Right-click the groups, select **Delete Group**, and agree to the delete confirmation prompts.
4. In the Navigator panel, click the **Packages** tab.
5. Navigate to ArcSight Solutions, right-click the Threat Detector 2.10 package ( ), and select **Uninstall Package**.
6. In the Uninstall Packages dialog, click **OK**. The progress of the uninstall displays in the Progress tab of the Uninstalling Packages dialog.

   If a message displays indicating that there is a conflict, select an option in the **Resolution Options** area and click **OK**.
7. When the uninstall is finished, review the summary and click **OK**.

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 Threat Detector 2.10)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to Documentation-Feedback@microfocus.com.

We appreciate your feedback!