SN65: ArcSight ESM Tools and Integration with ArcSight Logger and ArcSight TRM

Ken Mermoud
Dhaval Shah
Software Development Manager
September 2010
Agenda

- Tools Integration Background
- Integration Command Feature
- Authoring Integration Commands
- Case Studies
  - Logger Integration Commands
  - TRM Integration Commands
Tools Integration Background
What is Tools Integration?

- Integrate ESM with other applications
- Integrate to show external views
- Integrate to launch external actions/third-party tools
- Make use of context and existing tools
  - NOC-SOCs have collection of homegrown or external tools
- Build NOC-SOC synergy
- Both automation and user driven
Some Use Cases for Tools Integration

- Logger search
- Invoke TRM actions
- Launch third-party web interfaces
- Launch scripts
- Web search
- View submitted tickets
- Asset / vulnerability information
- IDM information
Integration Command Feature
Integration Commands

- Integration Command
  - A lightweight way to link information
  - Think hyperlinks in a web page
  - ESM Resource
    - Can be shared (archive/package)
    - Access Control
    - Configurable

- Command execution mechanisms
  - URI (HTTP)
  - Local script/executable (“tool”)
  - Connector

- Result rendering
  - Internal web browser/external web browser
  - Script/executable output
  - Connector structured result
**Integration Commands: The Trio of Resources**

**Integration Target:**
Contains information about server, connectors, etc, where command can be executed.

**Integration Configuration:**
Binds commands and targets together, also contain information about renderer and context.

**Integration Command:**
Describes integration type, and parameterized command.
Example Group of Integration Commands

Command

Configuration

Target
Authoring Integration Commands
Integration Command: Types (1)

- **URL command**
  - Launch browser to an URL
  - Set to use embedded browser or external browser
  - Can use velocity template
  - E.g. Web Search
    `http://www.google.com/search?q=+$selectedItem+${deviceVendor}+${deviceProduct}`

- **Script command**
  - Specify path, working directory, parameters, etc. of existing executable
  - Run on the Console machine
  - E.g. Ping, Traceroute, Whois, etc.
Integration Command: Types (2)

- Connector command (new in ESM v5.0)
  - Runs a command on a Connector
  - Integration with any Connector command, but Connector must be connected and running to execute properly
  - Reuses the same output renderer from regular Connector command
  - E.g. Lancope Connector’s Get Flows
Integration Target

- Specify information like IP address, port number, etc. for your servers
  - Logger Servers
  - TRM Servers
  - Search Providers
  - IT/Security Portals
  - Asset/Vulnerability Info
  - Ticketing Web Servers
Integration Configuration

- Represents a family of commands
- Ties them to targets
- Provides context on where to enable in UI
Case Study
Logger Integration Commands
Logger Integration Commands

Overview

- Run a Logger search from within the ESM Console
- Use Case Example
  - Find attacker in an Active Channel in ESM Console
  - Run a search for all the events from that attacker on Logger
- Introduced in ESM 4.5 SP1 Patch2
- Compatible with Logger 4.0+
Logger Integration Commands

1st Type: Logger Search

- Allows the user to select an event in an active channel and run a search based on one of the fields that will be presented in a list:
  - Event Name
  - Destination
  - Source
  - Destination and Source
  - User
  - Device Vendor and Product

- If there is more than one Logger Appliance accessible from ESM, the user can select which Logger he wants to run the search on.

- Pop-up dialogs to select the field and the Logger Appliance.
Logger Integration Commands

2nd Type: Logger Quick Search

- Allows the user to do a “quick-search” by selecting one field in an active channel and the search will be based on the field and the value that has been selected
- Quick search without pop-up dialog
- Will take the selected item for the field, and the default Logger Appliance that has been configured
Logger Quick Search (Destination Address)

https://192.168.36.5/app/redirect?user=admin&pass=password&url=/logger/search_ausm.ftl?ausm_query=destinationAddress=1.1.1.1&from=15 JUL 2009 10:00:00 PST&to=15 JUL 2009 12:00:00 PST

Steps:
- Authenticate with admin/password on 192.168.36.5
- Redirect to the Logger search page (/logger/search_ausm.ftl)
- Run query "destinationAddress=1.1.1.1" for the specified time range

https://192.168.36.5/app/redirect?user=admin&pass=password&url=/logger/search_ausm.ftl?ausm_query=destinationAddress=1.1.1.1&from=15 JUL 2009 10:00:00 PST&to=15 JUL 2009 12:00:00 PST
### ESM Integration Command:

```plaintext
https://${LoggerHost}/app/redirect?user=${LoggerUser}&pass=${LoggerPassword}&url=/logger/search_ausm.ftl?ausm_query=destinationAddress=${destinationAddress}&from=${Now-2h}&to=${Now}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>${LoggerHost}</code></td>
<td>Logger Hostname</td>
</tr>
<tr>
<td><code>${LoggerUser}</code></td>
<td>Logger User</td>
</tr>
<tr>
<td><code>${LoggerPassword}</code></td>
<td>Logger Password</td>
</tr>
<tr>
<td><code>destinationAddress=${destinationAddress}</code></td>
<td>Query Parameters: here we want to pass the destination address</td>
</tr>
<tr>
<td><code>${Now-2h}</code></td>
<td>Start Time of the Query</td>
</tr>
<tr>
<td><code>${Now}</code></td>
<td>End Time of the Query</td>
</tr>
</tbody>
</table>
Logger Integration Commands

Demos

Logger Search

Logger Quick Search
Case Study
TRM Integration Commands
Investigating a Rogue Host

- You have a rogue host problem!
- You are alerted on the ESM about the IP of the rogue host
- What do you do now?
  - Where is it? Where is the target?
  - What are the options to contain it?
  - And how are the commands executed?
Invoking a TRM Command
Invoking a TRM Command
Attacker Target Map

Maps

Target: 10.0.0.5

Attacker: 10.0.0.2
Target: 10.0.0.5
Target port: 9000
Priority: 7 (High)
Detailed Results of Investigation—ArcSight TRM

- See detailed results about investigated node
- See Layer 3 connections
- See Layer 2 access into the network

Understand Impact
ArcSight TRM: Smarter Response Decisions

Provide any IP Address
ArcSight TRM provides detailed node, layer 2/3 information

Simulation determines best method to handle quarantine

Authorization
Quarantine method

ArcSight TRM takes action and tracks the change
Reliable Quarantine—ArcSight TRM

Active quarantine: executed and logged
Rogue Host Example—Summary

- You now know where the rogue host is!
- And you know what you can do about it
- And have the ability to do it
- From the same ESM Console

Empowers the security analyst and provides the information and tools to take informed actions
Investigating an Unauthorized User Activity

- You have an unauthorized user activity
- You are alerted on the ESM and you know the username
- What do you do now?
  - Who is it?
  - And how can you surgically disable that user?
Invoking a TRM Command
Disabling Enterprise Account

Search Enterprise Accounts


Select Source Destination:

Select Source Destination To Search:
- Solutions AD Server

Next Step

Search on an Attribute

Pick a Directory Service. E.g. MS AD Forest
## Disabling Enterprise Account

**Disable Enterprise Accounts**

1. **Select Source Destination**: "Directory Service" 
2. **Select User**: "ArcSight" 
3. **Select Account**: "1" 
4. **Disable**

<table>
<thead>
<tr>
<th>User Information</th>
<th>First Name</th>
<th>Last Name</th>
<th>Full Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>ArcSight</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Add Quarantine Information

- **Expiration Time Length**: 0
- **Trouble Ticket**: 21341943
- **Category**: Virus or Worm

### Quarantine Information

- **Quarantine ID**: 5
- **Type**: Disable Enterprise Account
- **Status**: Active
- **Expiration**: None

### Task Information

- **Job ID**: 1
- **Type**: Disable Enterprise Account
- **Submitted**: 09/02/2010 16:24:16
- **Finished**: 09/02/2010 16:24:16

### Comments

- **Disabling User**
Unauthorized User Activity—Summary

- You now know the user!
- And you know what you can do about it
- And have the ability to do it
- From the same ESM Console

Empowers the security analyst and provides the information and tools to take informed actions
Your Feedback Builds a Better Conference!

- Text to 32075 (USA & Canada) or 447786204951 (Non-USA)
- Type **ARCS <space> 65** and the letter to each response

<table>
<thead>
<tr>
<th>Rate the speaker</th>
<th>Excellent</th>
<th>Good</th>
<th>Fair</th>
<th>Poor</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>b</td>
<td>c</td>
<td>d</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Rate the content</th>
<th>e</th>
<th>f</th>
<th>g</th>
<th>h</th>
</tr>
</thead>
</table>

Please provide comments: (*) enter any comments/feedback

Download session replays after the conference:

[https://protect724.arcsight.com/community/protect10](https://protect724.arcsight.com/community/protect10)