Hewlett Packard
Enterprise

Protect 2016

Please give me your feedback

Session ID: B10047 **Speaker:** Patrick Cain and Gregory Hedge

—Use the mobile app to complete a session survey

1. Access “My schedule”
2. Click on the session detail page
3. Scroll down to “Rate & review”
   - If the session is not on your schedule, just find it via the app’s “Session Schedule” menu, click on this session, and scroll down to “Rate & Review”
   - If you don’t have it, download the event app today. Go to your phone’s app store and search for “HPE Protect 2016”

—To access the session survey online, go to the Agenda Builder in the event session catalog and click on your session

Thank you for providing your feedback, which helps us enhance content for future events.

Gregory Hedge
Castle Ventures Corporation
ghedge@castleventures.com

Patrick Cain
Boston College
patrick.cain@bc.edu

Taking Action with ESM

Methods ArcSight ESM Can Take Action

- Action Connectors
- Scripting
- Integration Commands

Why?

Automate

- Instantaneous response
- 24x7
- Not enough humans
- Better than humans

Integrate

- Single pane of glass
- Tools work better when they work together

What Are Action Connectors?

- Provide bi-directional communication between event source and ESM.
- Gives ESM the capability to send commands back to an event source.
- Commands can request more information or have the event source perform an action like block an endpoint.
- These commands can be manual or automated. Some use Integration Commands and Rules, some just Integration Commands.
- Do not confuse Action Connectors with Forwarding Connectors.

Action Connectors

Certified Action Connectors Examples

- ForeScout CounterACT
- Digital Guardian
- Niara Security Intelligence
- Blue Coat Security Analytics
- Ixia Anue Net Tool Optimizer

More Action Connectors

Action Connector Development Guide

- Make your own

Scripting

A Rule can execute a script.

- Bro IDS
- Palo Alto
- Trend Micro TippingPoint
- Aruba ClearPass

Integration Commands

Integration commands are defined within the ESM or Express Console and enable the user to initiate external commands.

- Can be launched from within different content such as Active Channels, Active Lists and Query Viewers.
- Associate parameters with commands to leverage data gathered by ESM in the context in which the commands are called.
- Can be populated with values such as user name and password required for running the external command.
- Prompt for additional information to be used in the command parameters.

Examples of Integration Commands

Typical activities to build and run commands in the ArcSight Console.

- Launch a browser to a web site or solution web interface.
- Launch scripts.
- Run external searches.
- Ticketing system integration.
- Get payload information.
- Get vulnerability scan information.

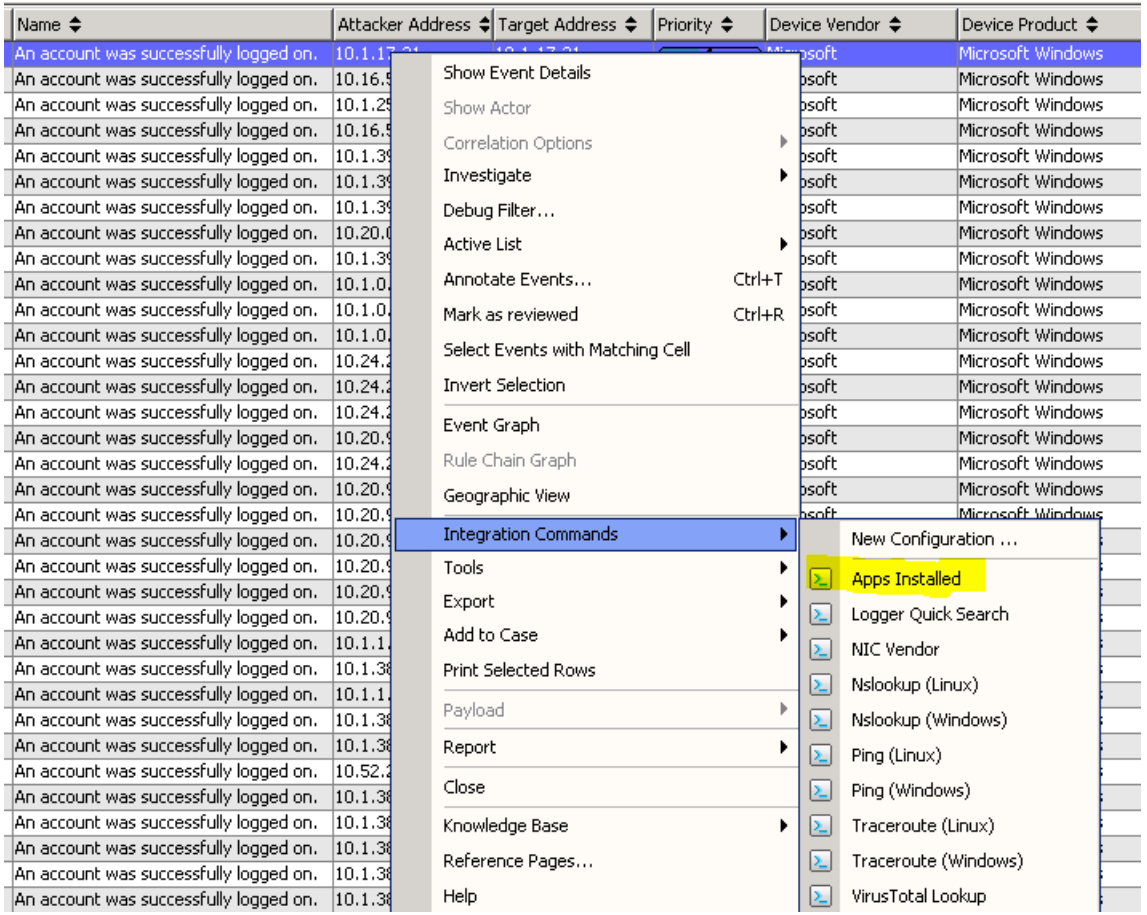
ArcSight – ForeScout Use Cases

Examples of Automated Response Use Cases directed by ArcSight.

- Quarantine an infected endpoint
- Quarantine or alert on a non-compliant endpoint
- Retrieve endpoint information
- Scanning on demand

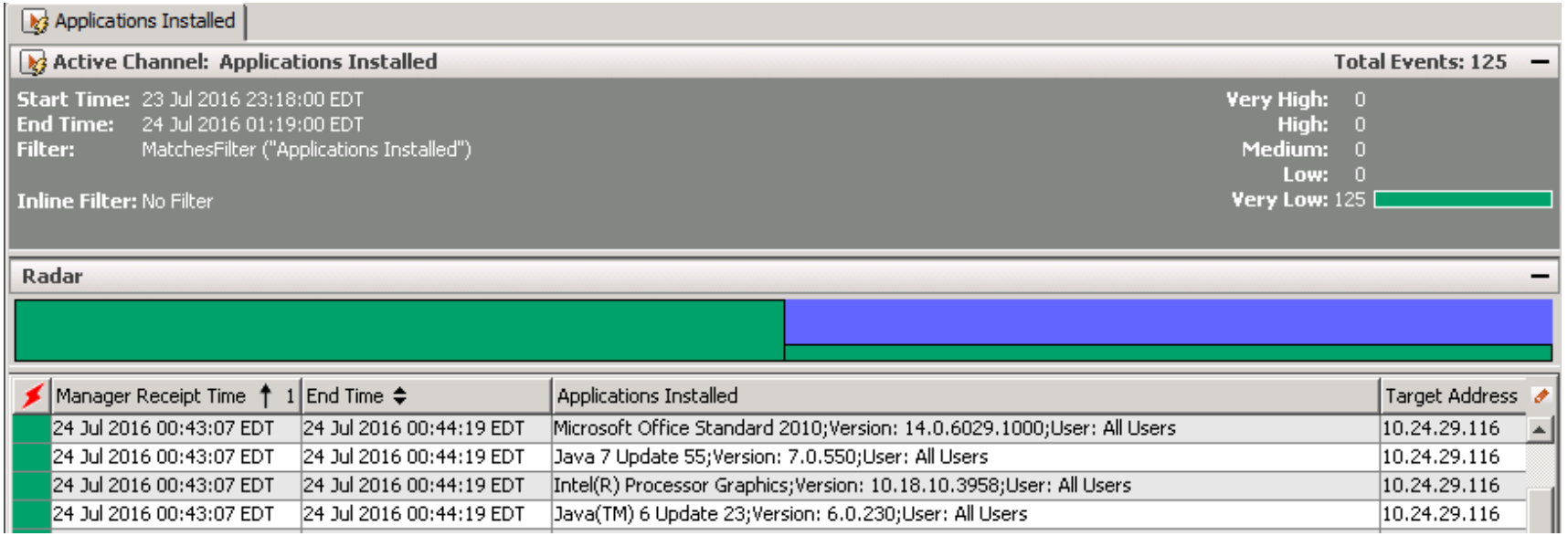
ForeScout Example

Applications Installed (Integration Command)



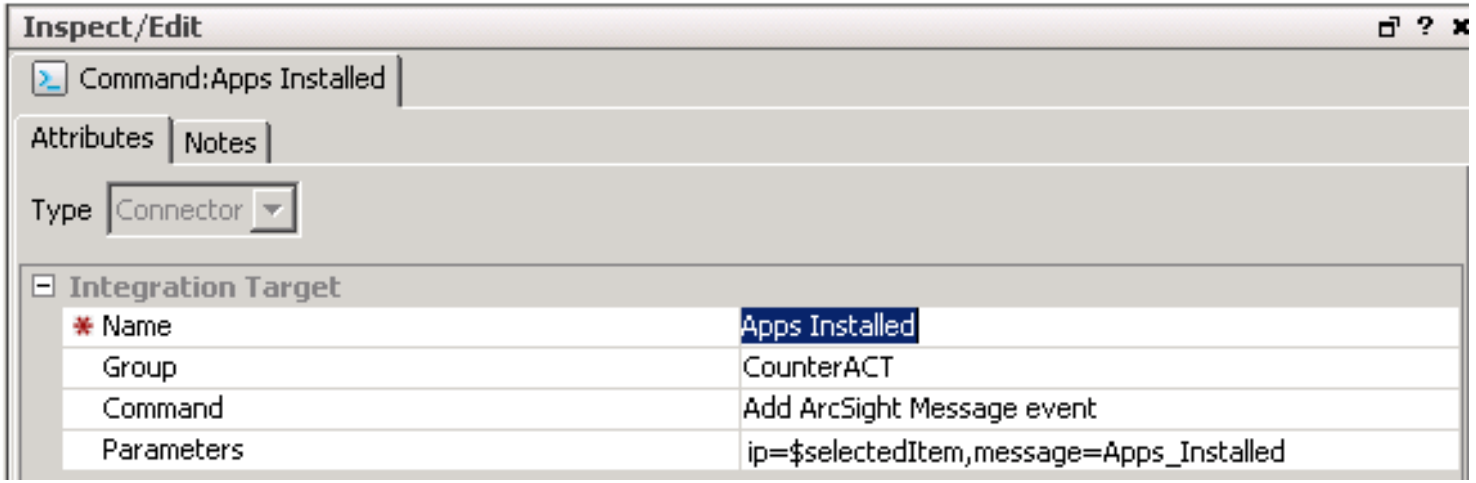
ForeScout Example

Applications Installed (Integration Command)



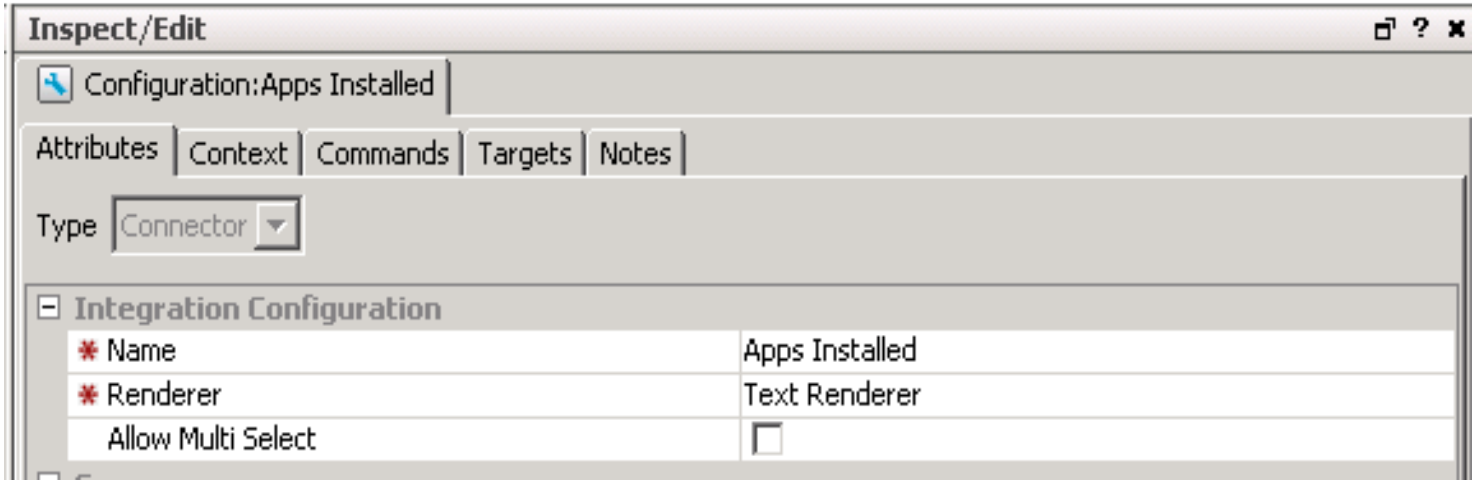
ForeScout Example

Applications Installed (Integration Command)



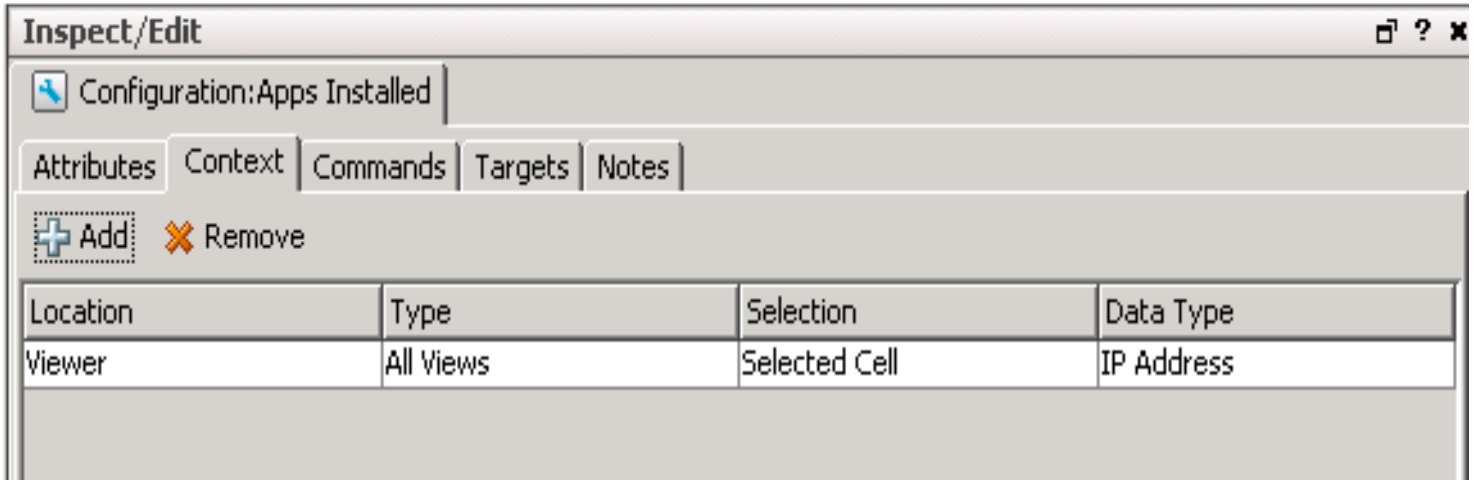
ForeScout Example

Applications Installed (Integration Command)



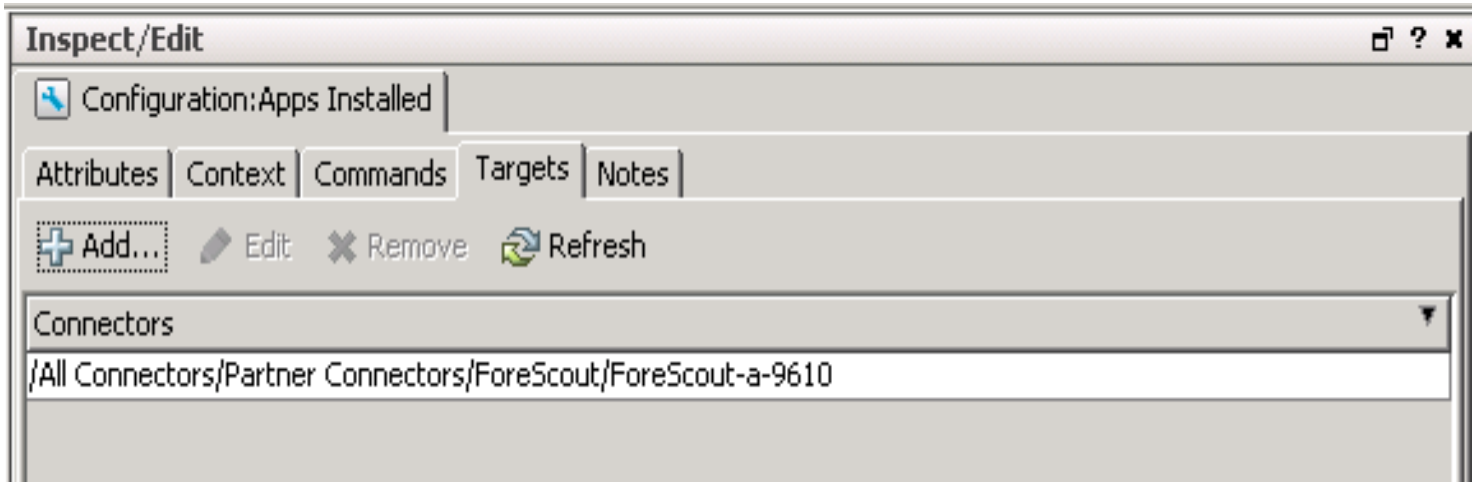
ForeScout Example

Applications Installed (Integration Command)



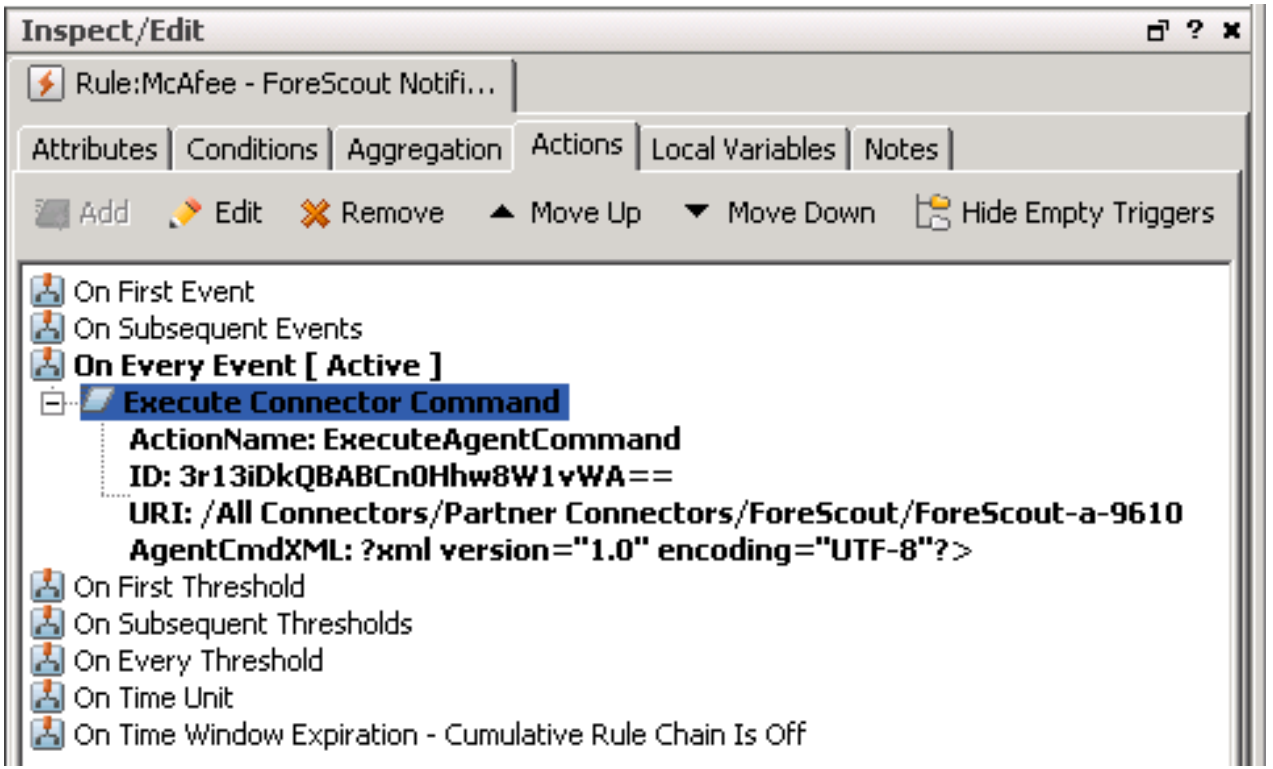
ForeScout Example

Applications Installed (Integration Command)



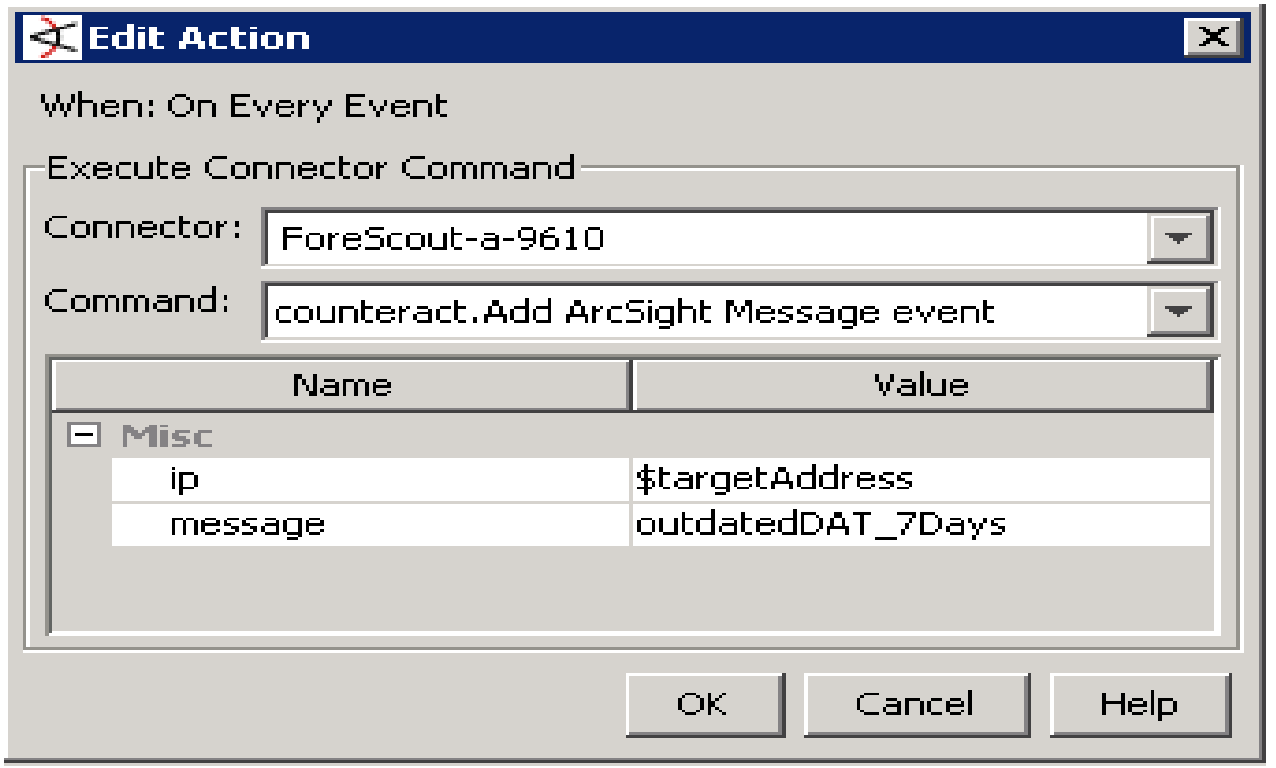
ForeScout Example

Out of Date DAT File



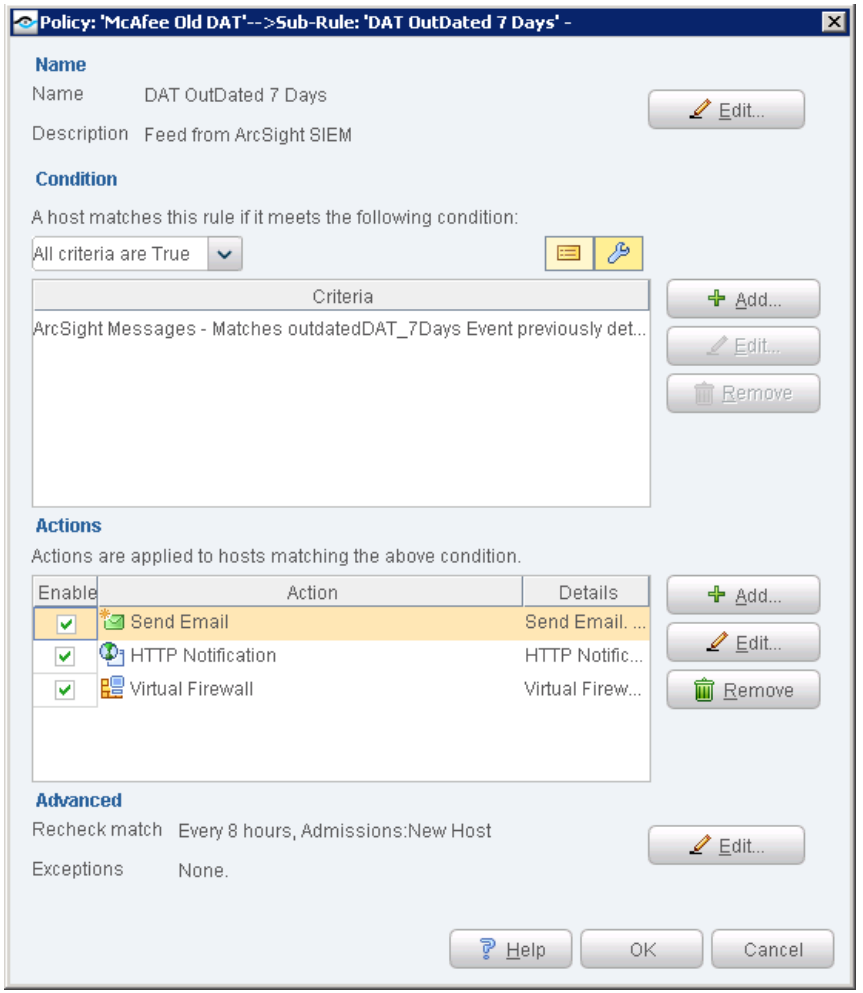
ForeScout Example

Out of Date DAT File



ForeScout Example

Out of Date DAT File



ArcSight – Other Devices Use Cases

- Mostly Defensive Activities
  - Deter people from scanning our networks
  - Persuade directory trolls to go elsewhere
- Some more Offensive
  - Alert Users about compromised devices
  - Remove compromised devices from network

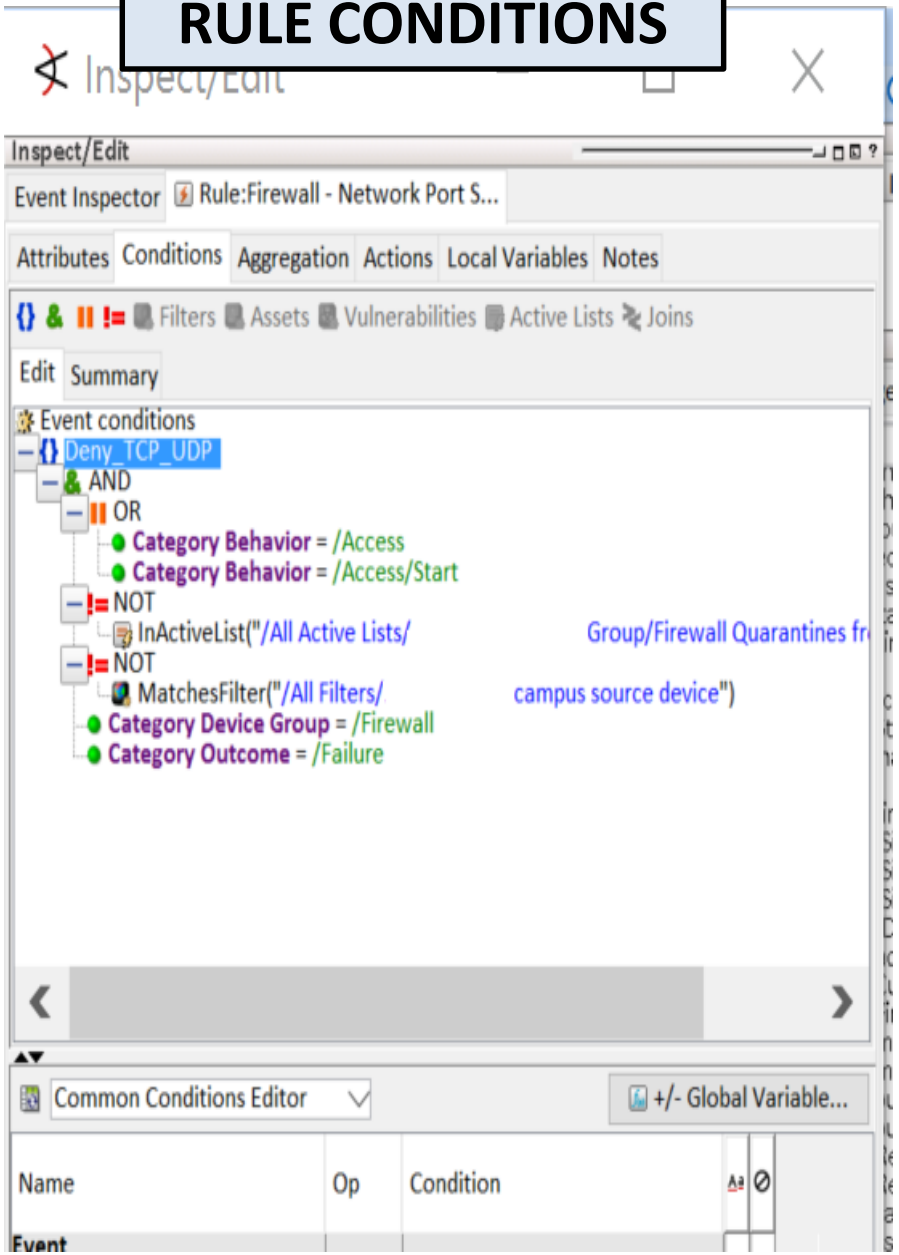
Political Considerations

- What happens when the Actions make an error?
  - The President's computer is removed
  - The primary website gets blocked
- Human override is built into the processes
  - Many IP addresses excluded from the automatics
- The 24/7 NOC has a web page to undo actions
  - They can undo, unquarantine, re-enable, etc
- Reports can be run for metrics to look for oddity

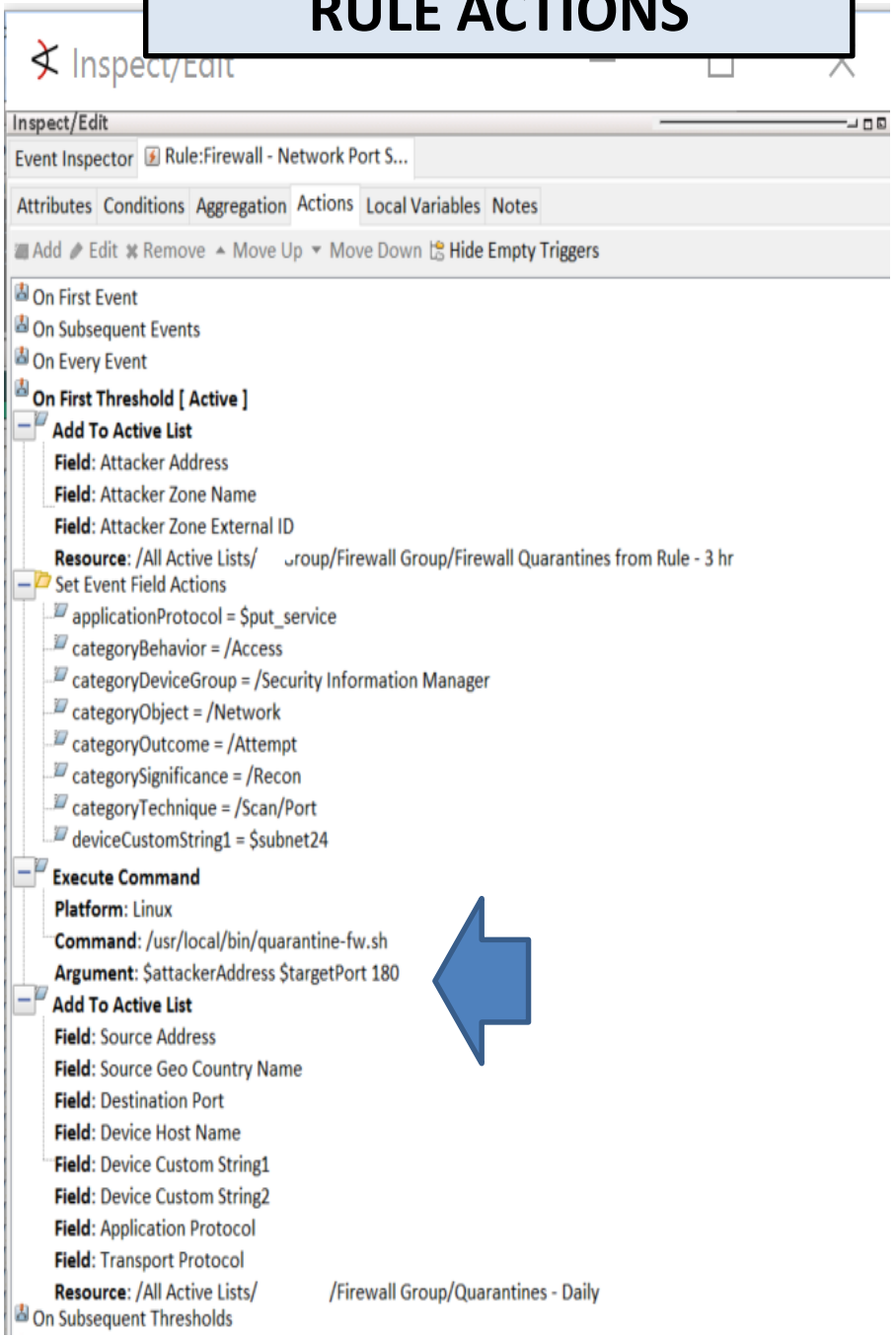
Use Case: Overly Friendly Scanners

- Our networks get port and host scanned a *lot*
- The earlier we can toss that traffic the better
  - There is a border firewall and some TippingPoint IPSes in the way
- There was a perl script that watched firewall logs and responded with a “quarantine” command to the TPs
  - It worked great until the guy who wrote it left and that system was retired
  - Generating reports was a pain (i.e., mysql, more perl, etc)
- Hey! The firewall logs are going to the ESM, too
  - Maybe we should do this as an ArcSight ESM Rule

RULE CONDITIONS



RULE ACTIONS



Extended Use Case: Other “scanners”

- Other Rules conditions now also do:
  - Directory Trolls, multiple failed SSH logins, WordPress brute forces
- As I talk to you, we are quarantining IP addresses.
  - Varies from 1100 to 8500 per day
- Easily add new conditions periodically
  - E.g., repeated odd WordPress things
  - It’s quite easy to add new conditions
    - MUCH easier than changing the original perl script ;)
- Both reporting and alerting are quite easy
- These could be Action Connectors, too.

Use Case: Alert the Masses

- I get (too many) ESM Reports every morning
- …and find out too late if an account got compromised
  - 8am report says “root” got owned 17 hours ago.
- Crafted a Rule to look for failed SSH logins followed by a successful one for the same user
  - The 24/7 NOC uses Zabbix as a monitoring tool
  - The Rule action sends a (blinking) Zabbix alert
  - The NOC operator then triages with the user

RULE CONDITIONS

Attributes Conditions

Filters

Edit Summary

Event conditions

- Matching Event (Matching within 10m)
  - AND
    - event1.**Target User Name** = event2.**Target User Name**
    - event1.**End Time** <= event2.**End Time**
    - event1.**Device Host Name** = event2.**Device Host Name**
- {} event1
  - AND
    - **Name** = multiple ssh failures to one host
    - MatchesFilter("/All Filters/ off-campus destination device")
- {} event2
  - AND
    - **Name** = session opened
    - **Category Outcome** = /Success
    - **Device Process Name** = sshd

RULE ACTIONS

Event Inspector | Rule:ssh login afta failures v...

Attributes | Conditions | Aggregation | Actions | Local Variables | Notes

Add | Edit | Remove | Move Up | Move Down | Hide Empty Triggers

On First Event [Active]

Send Notification

AckRequired: No

NotificationMessage: good ssh after failures v2. User: $targetUserName, source: $targetAddress, $targetHostName ; destination: $deviceHostName - $deviceAddress

Resource: /All Destinations/Pat/

Execute Command

Platform: Linux

Command: /usr/local/zabbix/bin/zabbix_sender

Argument: -c /usr/local/zabbix/etc/zabbix_agent.conf -k sshlogins -o "User: $targetUserName, from IP: $targetAddress, $targetHostName successfully logged in after failures on: $deviceHostName - $deviceAddress" -z hawkeye

On Subsequent Events

On Every Event

On First Threshold

On Subsequent Thresholds

Use Case: Too Many Infections, too Little Time

- Make a system to score IDS, IPS, and AV alerts
  - There is a Query Viewer that runs every 15 minutes to identify the top offenders
  - There is also a Rule that runs looking for them.
- For spyware and C&C alerts, the Rule action can send a ticket to the user
    - There is an email interface to Service Center
    - The Rule has lots of “exception” conditions
- There is a Rule action to send a ”blacklist” command to the Aruba controllers, removing the offender from the network
  - This is currently not being used (see Political Considerations)

Other Ideas

Things to try at home

- WMI Commands (see Protect 2014 - “Automation in Incident Response”)
- Ticketing system integration
- SNMP Traps
- ESM and Logger APIs
- Forwarding Connectors

Q&A

Please give me your feedback

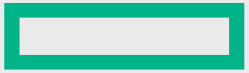
Session ID: B10047 **Speaker:** Patrick Cain and Gregory Hedge

—Use the mobile app to complete a session survey

1. Access “My schedule”
2. Click on the session detail page
3. Scroll down to “Rate & review”
   - If the session is not on your schedule, just find it via the app’s “Session Schedule” menu, click on this session, and scroll down to “Rate & Review”
   - If you don’t have it, download the event app today. Go to your phone’s app store and search for “HPE Protect 2016”

—To access the session survey online, go to the Agenda Builder in the event session catalog and click on your session

Thank you for providing your feedback, which helps us enhance content for future events.



Hewlett Packard
Enterprise

Thank you