Table of Contents

ArcSight Action Connector Integration Guide ................................................. 1

Table of Contents ......................................................................................... 2
Revision History .............................................................................................. 3
Ixia Action Connector Integration Guide ......................................................... 4
Joint-Solution Overview .................................................................................. 4
Configuration ................................................................................................... 5
Action Integration ............................................................................................. 6
Integration Command Configuration ............................................................... 6
A. Installing a Content Package in ArcSight ESM .............................................. 6
B. Using an integration command ................................................................... 7
Flex CounterACT Configuration ...................................................................... 9
A. Installing a Flex CounterACT Action Connector ......................................... 10
B. Executing Flex CounterACT commands ..................................................... 10
ArcSight Content for Ixia NTO ....................................................................... 13
Prerequisites .................................................................................................. 13
Support .......................................................................................................... 13
Additional ArcSight Documentation ................................................................. 14
Certified Integration:

The integration complies with the requirements of the Micro Focus Technology Alliance Partner program. For inbound integrations, the Micro Focus ArcSight CEF connector will be able to process the events correctly and the events will be available for use within Micro Focus ArcSight product. In addition, the event content has been deemed to be in accordance with standard SmartConnector requirements. For action and outbound integrations, the integration establishes outbound communications from Micro Focus ArcSight to a third party platform. The integration has been tested and demonstrated to Micro Focus by the third party.

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/12/2012</td>
<td>First edition of this Configuration Guide. (TcL API)</td>
</tr>
<tr>
<td>11/30/2012</td>
<td>Version 3.3 certified by HP Enterprise Security</td>
</tr>
<tr>
<td>2/11/2014</td>
<td>Second edition of this Configuration Guide (Web API)</td>
</tr>
<tr>
<td>2/12/2014</td>
<td>Version 3.9 certified by HP Enterprise Security</td>
</tr>
<tr>
<td>6/15/2017</td>
<td>Version 4.6 certified by HP Enterprise Security</td>
</tr>
<tr>
<td>9/21/2017</td>
<td>Rebranding HPE/Microfocus &amp; Ixia/Keysight</td>
</tr>
</tbody>
</table>
Ixia Action Connector Integration Guide

This guide provides information for configuring the Ixia Net Tool Optimizer (NTO) response actions for ArcSight ESM. This integration is supported on ESM versions 6.0.0.1333 and later. Ixia NTO version(s) 3.9 or newer is supported. (recently re-certified for version 4.6)

Joint-Solution Overview

The Ixia Net Tool Optimizer™ (NTO™) works in concert with ArcSight’s Security Information and Event Management (SIEM) system and your security tools (forensic recorders, IPS/IDS, DLP and malware analyzers) to protect your network. The Ixia NTO passively directs out-of-band network traffic from multiple access points (SPANs or TAPs) in the network to security tools for analysis. Traffic is aggregated from all needed access points in the network to provide comprehensive visibility. The Ixia NTO’s Automated Response Technology complements the ArcSight Enterprise Security Manager (ESM) product’s ability to detect, analyze and respond to security threats. When the ArcSight ESM detects an anomaly, the Ixia NTO can automatically, or via a right mouse click from ESM, send the right traffic to a forensic recorder or other security probe. Incident remediation can begin the instant an anomaly occurs with the benefit of having all the required packet information. The joint solution speeds root cause analysis, eliminates time consuming manual steps and simplifies compliance.
Configuration

No special configuration of the Ixia NTO is required to support this integration. In ArcSight, scripts are configured to access the NTO, the scripts will need to be populated with valid NTO IP address, administrator user name & password, and relevant port names on the NTO. Sample scripts are available as indicated below.

Pre-Requisites
- Ixia NTO running version 3.9 or newer which includes the WebAPI
- Scripting interpreter on the ArcSight console which supports making RESTful Web API queries (common examples are Perl, PHP, and Python)
  - The sample .pl scripts referenced below are tested with Strawberry Perl v5.18 for windows although other versions of PERL should work fine. (note: Perl comes installed by default on most Linux and Mac systems, for Windows you may need to install the interpreter)
  - Perl JSON, Data::Dumper, and strict modules loaded (this came included by default with Strawberry Perl)
- CURL interpreter is available and placed in same directory as your scripts listed below (we tested with CURL 7.32 for windows, but CURL for other OS ok too). Note: CURL can be placed elsewhere if you edit PATH in the .bat script below

The Following files are needed:
  - filterByIp.bat
  - createIpFilter.pl
  - deleteIpFilter.pl
- Edit .BAT and .PL scripts as appropriate for your environment (i.e. NTO Address, User, PW, Network & Tool Interfaces). See remarks within the files themselves for further details.
- Place the .BAT and .PL files in appropriate directories for your environment. You will need to edit the integration commands and the properties file to specify the correct location of these files if you do not use the default location. The default configuration uses C:\Arcsight as the directory.
Action Integration

Integration Command Configuration

The Action connector used in this integration makes use of the Flex CounterACT SDK developed by ArcSight to provide the ability to automatically reconfigure Ixia NTO based on triggers from ArcSight. The trigger can be a right-click of an event in ArcSight using integration commands, or from rules defined in ArcSight using the Flex CounterACT Connector. Once triggered the NTO is reconfigured to send the desired network traffic to the desired monitoring tool.

The following section outlines how to install the package and its contents.

A. Installing a Content Package in ArcSight ESM

1 Log into the ArcSight ESM Console with an account that has sufficient privileges to install a package.
2 Click the Packages tab in the Navigator panel.
3 Click Import ( ).
4 In the Open dialog, browse and select the package bundle file and select Open.

The progress of the import of the package bundle is displayed in the Progress tab of the Importing Packages dialog.

5 When the import is complete, the Results tab of the Importing Packages dialog is displayed as well as the Packages for Installation dialog.
6 Leave the checkbox selected, and in the Packages for Installation dialog click Next.

The progress of the install is displayed in the Progress tab of the Installing Packages dialog. When the install is complete, the Results tab of the Installing Packages dialog displays the Summary Report.

7 In the Installing Packages dialog, click OK.
8 In the Importing Packages dialog, click OK.

You should see the package now installed:

9 To verify that the installation was successful navigate to the Resources tab of the Navigator panel and select Integration Commands from the drop down menu. Navigate to the ArcSight Partner Sample Content folder and open the Ixia Group.
Included Content

The following Integration Commands are included in this package:
- Ixia Capture by IP
- Ixia Packet Capture History

B. Using an integration command

Preparation

- Login to the Ixia NTO GUI of the NTO unit you are testing with
  
  o Note: during pre-setup the Integration files where loaded, the scripts should have been edited to use the NTO IP Address and an NTO user ID / password to be used by the integration. For the GUI you must login with a different user id / password.

- Sample NTO configuration show below, note the Packet Analyzer is awaiting Integration signal from Arcsight (no packets being passed to Tool)
1. From ArcSight, Right click on an event in an active channel or other configured viewer and select **Integration Commands → Ixia Capture by IP**

Returning to Ixia NTO, you will note the Attacker's traffic being redirected to the Packet Analyzer for a period of time specified in the .BAT script.

2. (Optionally) Right Click on an event from a configured Dashboard and select **Integration Commands → Ixia Capture by IP**
To view a history of previously packet filtering - Right click on an event in an active channel or other configured viewer and select **Integration Commands → Ixia Packet Capture History**.

### Flex CounterACT Configuration

The Action connector used in this integration makes use of the Flex CounterACT SDK developed by ArcSight to provide the ability to automatically reconfigure NTO based on triggers from ArcSight. The trigger can be a right-click of an event in ArcSight using integration commands, or from rules defined in ArcSight using the Flex CounterACT Connector. Once triggered the NTO is reconfigured to send the desired network traffic to the desired monitoring tool.

The following section outlines how to install the connector and its functionality.
A. Installing a Flex CounterACT Action Connector

1. Follow the normal installation wizard to install the ArcSight SmartConnectors.

2. Follow the configuration steps in the wizard. Select the Flex CounterACT connector from the list of available connectors. After selecting the connector you will need to enter the name of the Configuration File (the extension will be added automatically). Complete the wizard.

Configuration

The following configuration file is used in this integration. This file contains the commands that you will be able to execute.

```
ixiasendtopacketrecorder.counteract.properties
```

1. Copy this file to the `<ArcSight_Home>\current\user\agent\flexagent` directory.

2. Start the connector.

B. Executing Flex CounterACT commands

From a Rule:

1. In the Navigator panel of the ArcSight console, create or edit a rule. Add an action to the rules and select Execute Connector Command.
2. Select your action connector and the command you wish to have executed from the list of commands. Provide fields if necessary for any parameters for your command.

![Edit Action Window]

3. For example (above), if the parameter is an IP Address, you could enter "\$attackerAddress" for the parameter. Whenever this rule fires and the action is triggered, it will execute the command using the attacker address of the event that triggered the rule. Click OK.
4. Once applicable events have triggered the rule, the rule will fire and be indicated by the Lightning Bolt icon.

5. As soon as you see a Rule Trigger, move back to the NTO screen and note the corresponding NTO Filters being called – Triggered Events are sent to a Packet Recorder for more analysis.
ArcSight Content for Ixia NTO

The following resources are included in the Ixia_Net_Tool_Optimizer_1_2.arb package:

Integration Commands:
- Ixia Capture by IP
- Ixia Packet Capture History

Integration Configurations:
- Ixia Capture by IP
- Ixia Packet Capture History

Prerequisites

<table>
<thead>
<tr>
<th>Product Name</th>
<th>Version Information</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Micro Focus Security ArcSight</td>
<td>6.0.0.1333.0 or higher</td>
<td></td>
</tr>
<tr>
<td>IXIA NTO</td>
<td>3.9 or higher</td>
<td></td>
</tr>
</tbody>
</table>

Support

Integration support information when an issue is outside of the ArcSight team’s scope
In some cases the ArcSight customer service team is unable to help with issues that lie within the configuration itself in which case, the certified vendor should be contacted for assistance:

Greg Copeland - Ixia

Phone – 713-561-3966

Email – gcopeland@ixiacom.com

Instructions – contact is available during CST business hours, Monday to Friday
Additional ArcSight Documentation

For more information about the joint-solution, visit the Micro Focus ArcSight Marketplace:

https://marketplace.microfocus.com/arcsight/content/ixia-nettool-optimizer

For more information about Micro Focus ArcSight ESM:

https://marketplace.microfocus.com/arcsight/content/enterprise-security-manager-esm