Common Event Format Integration Guide

Acalvio Technologies
ShadowPlex
Date: Thursday, August 10, 2017
## Table of Contents

1. Revision History .................................................................................................................. 3

2. Joint-Solution Overview .................................................................................................... 4

3. Use Cases .......................................................................................................................... 4
   - High-Fidelity Intrusion Detection .................................................................................... 4
   - Assist in Breach Investigation ....................................................................................... 4

4. ShadowPlex CEF Integration ............................................................................................. 5
   - Configuration of ShadowPlex to output CEF events ..................................................... 5
   - Events ............................................................................................................................. 5
   - Device Event Mapping to ArcSight Data Fields ............................................................ 7

5. Prerequisites ...................................................................................................................... 8

6. Support .............................................................................................................................. 8

7. Additional ArcSight Documentation .................................................................................. 9
ArcSight Integration Guide

This document is provided for informational purposes only, and the information herein is subject to change without notice. Please report any errors herein to HPE. HPE does not provide any warranties covering this information and specifically disclaims any liability in connection with this document.

Certified Integration:

The integration complies with the requirements of the HPE Technology Alliance Partner program. For inbound integrations, the HPE ArcSight CEF connector will be able to process the events correctly and the events will be available for use within HPE’s 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 HPE ArcSight to a third party platform. The integration has been tested and demonstrated to HPE by the third party.

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>07/17/2017</td>
<td>First edition of this Configuration Guide.</td>
</tr>
<tr>
<td>08/10/2017</td>
<td>Version 2017.07 Certified by HPE Enterprise Security</td>
</tr>
</tbody>
</table>
Acalvio Integration Guide

This guide provides information for configuring Acalvio ShadowPlex for syslog event collection. This integration is supported on Windows and Linux platforms. Acalvio ShadowPlex versions starting at [2017.07] are supported.

Joint-Solution Overview

Acalvio ShadowPlex, is a comprehensive, distributed deception platform which provides early, accurate and cost-effective detection of breaches and insider threats. ShadowPlex is built on Acalvio’s patented Deception 2.0 technology that delivers scale, automation and authenticity with low IT impact.

ShadowPlex consists of sensors (virtual or physical) that are installed in the enterprise network and a Deception Center that is either on-premises or hosted on a public or private cloud. The sensors build software tunnels to the deception center and project decoys in the enterprise network and deploy breadcrumbs. Any access to a decoy raises a deception alert. The deception center analyzes the alert, adds various attributes to the alert and creates a deception event. The deception center provides a REST API interface to access the deception events in CEF.

The ArcSight CEF Connector connects to the ShadowPlex deception center and pulls the deception events periodically and pushes the events to the ArcSight ESM. The deception events can be accessed from the ArcSight dashboard.
Use Cases
This section describes important use cases supported by this integration.

- High-Fidelity Intrusion Detection
- Assist in Breach Investigation

High-Fidelity Intrusion Detection
Decoy hosts and services are not part of normal business processes. Any access to such decoys is a breach or an insider threat, with high probability. The security operations team can use these high-fidelity deception events as starting points for investigations.

Assist in Breach Investigation
ShadowPlex provides a number of attributes along with each deception event. The attributes include the time stamp of the access, source IP address and port of the access, the IP address and port of the decoy host, the decoy service accessed and credentials used. These attributes help the security operations team in profiling the attack.

CEF Integration

A. Configuration of ShadowPlex to output CEF events
Arcsight CEF Connector needs to be configured to pull deception events from ADC REST API.

Prerequisite: Contact Acalvio to get the cert.pem file.

1. Start Arcsight Connector configuration wizard
2. Select to install Arcsight CEF REST connector
3. Import the provided cert.pem file into Arcsight Connector keystore.
4. Select “Basic” authentication
5. Configure connector to pull events from
   https://<ADC IP>:8443/getTrippedEvents?limit=100&offset=0&cef=true
6. For “User Name” and “Password” fields, enter credentials used to access ADC WebUI
B. Events

Acalvio Event ID is listed below-

1. Low-tripped event

Following are the sub types of low tripped event-

- rdp
- vnc
- http
- mysql
- ssh
- telnet
- ftp
- ms-sql-s
- postgresql
- netbios-ssn
- loc-srv
1 Device Event Mapping to ArcSight Data Fields

Information contained within vendor-specific event definitions is sent to the ArcSight SmartConnector, then mapped to an ArcSight data field.

The following table lists the mappings from ArcSight data fields to the supported vendor-specific event definitions.

**ArcSight CEF REST Connector Field Mappings**

<table>
<thead>
<tr>
<th>Vendor-Specific Event Definition</th>
<th>ArcSight Event Data Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>eventType</td>
<td>cn1</td>
</tr>
<tr>
<td>Id</td>
<td>externalId</td>
</tr>
<tr>
<td>protocolType</td>
<td>cs4</td>
</tr>
<tr>
<td>Eventid</td>
<td>cat</td>
</tr>
<tr>
<td>service</td>
<td>app</td>
</tr>
<tr>
<td>cefDateTimeStr</td>
<td>start</td>
</tr>
<tr>
<td>cefDateTimeStr</td>
<td>rt</td>
</tr>
<tr>
<td>Src_ipv4</td>
<td>src</td>
</tr>
<tr>
<td>HI_ipv4</td>
<td>dst</td>
</tr>
<tr>
<td>destPort</td>
<td>dpt</td>
</tr>
<tr>
<td>mac</td>
<td>dmac</td>
</tr>
<tr>
<td>flipType</td>
<td>cs1</td>
</tr>
<tr>
<td>subnet</td>
<td>cs2</td>
</tr>
<tr>
<td>subnetName</td>
<td>cs3</td>
</tr>
</tbody>
</table>
Prerequisites

<table>
<thead>
<tr>
<th>Product Name</th>
<th>Version Information</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>HPE Security ArcSight</td>
<td></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:

Customer Support - Charles Vong

Phone - 408-891-8890

Email - charles@acalvio.com

Instructions

1. Please install all the Acalvio components and ArcSight CEF REST Connector first.

2. Contact Acalvio to get the cert.pem file specific to your installation.

3. Follow the above setup instructions to configure the ArcSight Connector to pull events from Acalvio ShadowPlex.

4. If there no decoys created yet, then create at least one decoy in one subnet using ShadowPlex UI.

5. Generate a deception trip event by accessing one of the services of the decoy.

6. If the trip event does not show up in ArcSight ESM console, please contact the support person listed above.
Additional ArcSight Documentation

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

For more information about HPE Security ArcSight ESM: