Common Event Format Integration Guide

Attivo Networks
BOTSink
Date: Friday, June 02, 2017
# Table of Contents

Attivo BOTSink Integration Guide .................................................................................................................. 4

Joint Solution Overview ...................................................................................................................................... 4

Use Cases .......................................................................................................................................................... 4

CEF Integration .................................................................................................................................................. 5

A. Configuration of Attivo BOTSink to output CEF events ............................................................................. 5

B. Events ........................................................................................................................................................ 6

C. Device Event Mapping to ArcSight Data Fields ......................................................................................... 7

ArcSight Content for Attivo BOTSink .............................................................................................................. 7

Prerequisites .................................................................................................................................................. 7

Support .......................................................................................................................................................... 8

Additional ArcSight Documentation ............................................................................................................... 8
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>03/17/2017</td>
<td>First edition of this Configuration Guide.</td>
</tr>
<tr>
<td>06/02/2017</td>
<td>Version 4.0 Certified by HP Enterprise Security</td>
</tr>
</tbody>
</table>
Attivo BOTSink Integration Guide

This guide provides information for configuring Attivo BOTSink for syslog event collection. This integration is supported on Linux platforms. Device versions starting at 4.0 are supported.

Joint-Solution Overview

Attivo Networks is an award-winning provider of deception for in-network threat detection, attack forensic analysis, and continuous threat response. Attivo BOTSink complements and augments existing security infrastructure. Attivo BOTSink in conjunction with HPE ArcSight provides centralized view and correlation of threat data.

Inbound integration with HPE ArcSight will enable Attivo BOTSink to send its threat data as CEF events to HPE ArcSight.

Use Cases

This section describes important use cases supported by this integration.

- Centralized view and correlation of threat data
- Real-Time substantiated alerts from actual attacker engagements
- Prioritization of critical threats and incidents over billions of logged data
CEF Integration

A. Configuration of Attivo BOTSink to output CEF events

Before configuring Attivo BOTSink, configure a TCP / UDP Receiver with CEF as Source Type at HPE ArcSight Logger or install and configure a Syslog Daemon SmartConnector for integrations with ArcSight ESM. You can then configure the Attivo BOTSink Manager to forward events and system faults as syslog messages to ArcSight.

In the **Syslog Configuration** page, you configure the ArcSight Logger Receiver details as the Syslog Server to which you want the events to be forwarded. You can also configure the details to include and the format to be used for syslog messages. Select the format of Syslog message as CEF.

The high-level steps to forward events and fault messages to HPE ArcSight (syslog server) is as follows:

1. Select a default Syslog Profile *Attivo_Default_TCP_CEF* or *Attivo_Default_UDP_CEF* if it matches your requirement. Otherwise, create a syslog profile in which you define the format for the syslog message and the information to be forwarded. To create a Syslog profile
   a. Specify the severity of the events to be forwarded
   b. Optionally, map the Attivo BOTSink severity to Syslog severity
   c. Select CEF as Message Format
   d. Enable forwarding of BOTSink fault messages and select the format for the same as CEF

2. Create a syslog server record in which you define the IP address of the HPE ArcSight Logger or SmartConnector, the protocol to be used, the syslog profile to be used, and the syslog server port number. The details have to match the TCP / UDP Receiver configured at HPE ArcSight Logger.
B. Events

For a complete list of events that can be generated and sent to ArcSight, please contact Attivo support.

The screenshot below shows several sample events sent from Attivo BOTSink to ArcSight Logger.

```
<9>CEF:0|Attivo|BotSink|4.0.0.439|100202|Telnet connection ended|10|cat=Access dvc= src=192.168.1.66 dhost=Ubuntu131 msg=Telnet connection ended ( 17/6/1@20:36:03: EXIT: telnet status=1 pid=11644)

<9>CEF:0|Attivo|BotSink|4.0.0.439|100201|Telnet connection started|10|cat=Access dvc= src=192.168.1.66 dhost=Ubuntu131 msg=Telnet connection started ( 17/6/1@20:36:02: START: telnet pid=11644 from=192.168.1.66)

<9>CEF:0|Attivo|BotSink|4.0.0.439|100403|SMB authentication failure|10|cat=Access dvc= src=192.168.1.66 dhost=Ubuntu131 msg=SMB authentication failure ( user: guest; Jun 1 20:36:27 Ubuntu131 smbd[11723]: check_ntlm_password: Authentication for user [guest] -> [guest] FAILED with error NT_STATUS_NO_SUCH_USER ) dpt=445 spt=61232

<9>CEF:0|Attivo|BotSink|4.0.0.439|100404|SMB authentication failure|10|cat=Access dvc= src=192.168.1.66 dhost=Ubuntu131 msg=SMB authentication failure ( user: guest; check_ntlm_password: Authentication for user [guest] -> [guest] FAILED with error NT_STATUS_NO_SUCH_USER ) dpt=445 spt=61232

<9>CEF:0|Attivo|BotSink|4.0.0.439|31108|HTTP Connection Request|10|cat=Access dvc= src=192.168.1.66 dhost=Ubuntu131 msg=HTTP Connection Request ( 192.168.1.66 - [01/Jun/2017:20:36:16 +0000] "GET /robots.txt HTTP/1.1" 404 1544 "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
```

C. Device Event Mapping to ArcSight Data Fields

Information contained within vendor-specific event definitions is sent to the ArcSight Logger by mapping to CEF Extension field keys.

The following table lists the mappings from vendor-specific event definitions to ArcSight CEF Extension field keys.

<table>
<thead>
<tr>
<th>Vendor-Specific Event Definition</th>
<th>ArcSight CEF Extension Field Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP</td>
<td>src</td>
</tr>
<tr>
<td>Source Port</td>
<td>spt</td>
</tr>
<tr>
<td>Destination Host</td>
<td>dhost</td>
</tr>
<tr>
<td>Destination Port</td>
<td>dpt</td>
</tr>
<tr>
<td>Event Description</td>
<td>msg</td>
</tr>
<tr>
<td>Event Category</td>
<td>cat</td>
</tr>
<tr>
<td>Device IP</td>
<td>dvc</td>
</tr>
<tr>
<td>Event Timestamp</td>
<td>rt</td>
</tr>
</tbody>
</table>

ArcSight Content for Attivo BOTSink

No ArcSight content has been developed to support this integration at this time

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>6.0</td>
<td>Linux</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

Phone -1-510-353-3763

Email - support@attivonetworks.com

Instructions – Customers can contact Attivo Support team to report any issues with Attivo-ArcSight integration

Additional ArcSight Documentation

For more information about the joint-solution, visit the HPE ArcSight Marketplace: https://marketplace.saas.hpe.com/arcsight/category/partner-integrations