# Table of Contents

1. Revision History 3
2. Joint-Solution Overview 4
3. Use Cases 5
4. Outbound Integration 6
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>08/23/2017</td>
<td>First edition of this Configuration Guide.</td>
</tr>
<tr>
<td>08/29/2017</td>
<td>Elastic Stack versions 5.6 and 6.0 Certified by HPE Enterprise Security</td>
</tr>
</tbody>
</table>
Logstash ArcSight Module Integration Guide

This guide provides information for configuring Elastic’s Logstash ArcSight module integration for ArcSight ESM. The Elastic Stack versions 5.6 and 6.0 are supported.

Joint-Solution Overview

The Elastic Stack is a market leading real-time search and analytics platform for a wide range of use cases including security analytics. Logstash is the central data streaming engine in the stack, which features an ArcSight module that taps into the ArcSight Data Platform data stream via the EventBroker, processes the incoming CEF data on the fly, and includes various Kibana dashboards to begin exploring your security data immediately.

With this integration, ArcSight and Elastic can together provide a strong joint solution that combines the best of both worlds for analyzing security data.
Use Cases
This section describes important use cases supported by this integration.

- Network and firewall analytics
- Endpoint analytics
- Microsoft DNS analytics

These Kibana visualizations enable you to quickly understand the top devices, endpoints, attackers, and targets. This insight, along with the ability to instantly drill down on a particular host, port, device, or time range, offers a holistic view across the entire environment to identify specific segments that may require immediate attention or action. You can easily discover answers to questions like:

- Who are my attackers and what are they targeting?
- Which of my devices or endpoints are the busiest and what services were rendered?
- How many unique attackers, techniques, signatures, or targets were triggered at any given point in time?
- What are the top sources, destinations, protocols, and behaviors that are causing the elevated count of failures?
Outbound Integration

This Logstash Module for ArcSight integration will tap into the ADP data stream, either consuming off the EventBroker or receiving CEF events from the SmartConnectors. The events will be processed into Elasticsearch and visualized in Kibana. Kibana will also have dashboards that enable customers to explore network/firewall, endpoint, and Microsoft DNS datasets.

Instructions are below on how to get started. Existing ADP customers can tap into their existing EventBroker environments directly.

Getting Started Requirements
- The Elastic Stack (Logstash, Elasticsearch, Kibana) is running locally with default ports exposed, namely Elasticsearch as “localhost:9200” and Kibana as “localhost:5601”.
- By default, the ArcSight Module consumes from the EB “eb-cef” topic. For additional EB settings, see ArcSight Module Configuration Options. Consuming from a secured EB port is not currently available.

Instructions

1. Download and unpack Elasticsearch, Kibana, and Logstash.

2. In the Elasticsearch install directory, install X-Pack and start Elasticsearch:

```bash
bin/elasticsearch-plugin install x-pack
bin/elasticsearch
```

3. In the Kibana install directory, install X-Pack and start Kibana:

```bash
bin/kibana-plugin install x-pack
bin/kibana
```

4. Install X-Pack on Logstash, which includes the ArcSight Module. Then update the Logstash Kafka input plugin to an EB compatible version. In the Logstash install directory:

```bash
bin/logstash-plugin install x-pack
bin/logstash-plugin install --version 6.2.7 logstash-input-kafka
```

5. Start the ArcSight Module by running the following command in the Logstash install directory:

```bash
bin/logstash --modules arcsight --setup
-M "arcsight.var.input.eventbroker.bootstrap_servers={eb_host}:{eb_port}"  
-M "arcsight.var.elasticsearch.username=elastic"
-M "arcsight.var.elasticsearch.password=changeme"
-M "arcsight.var.kibana.username=elastic"
-M "arcsight.var.kibana.password=changeme"
```

The `--modules arcsight` option spins up an ArcSight CEF-aware Logstash pipeline for ingestion. The `--setup` option creates an “arcsight-*” index pattern in Elasticsearch and imports Kibana dashboards and visualizations. On subsequent module runs or when scaling out the Logstash deployment, the `--setup` option
should be omitted to avoid overwriting the existing Kibana dashboards.

6. Explore your data with Kibana:
   a. Open browser @ http://localhost:5601 (username: “elastic”; password: “changeme”)
   b. Open the “[ArcSight] Network Overview Dashboard”
   c. See Exploring Your Security Data for additional details on data exploration.

Prerequisites

<table>
<thead>
<tr>
<th>Product Name</th>
<th>Version Information</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>ArcSight Event Broker</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ArcSight Smart Connectors</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:

Elastic

Email - arcsight@elastic.co

Instructions – Please use this email alias when ArcSight or a joint customer/prospect requires assistance on this integration.
Additional ArcSight Documentation

For more information about our partner joint-solutions, visit the HPE ArcSight Marketplace:

For more information about HPE Security ArcSight ESM: