­­

Integration Guide

Micro Focus Common Event Format Integration Guide

Polyverse Corporation

ZeroTect

Date: November 14, 2020

Logo

Description automatically generated





# Contents

[Contents 2](#_Toc56321226)

[Revision History 3](#_Toc56321227)

[Polyverse Integration Guide 4](#_Toc56321228)

[This guide provides information for configuring the Polyverse Zerotect integration for ArcSight ESM. This integration is supported on ESM versions [6.0.0.1333] and later. Polyverse Zerotect version(s) 0.4.x is supported. 4](#_Toc56321229)

[Joint Solution Overview 4](#_Toc56321230)

[Use Cases 4](#_Toc56321231)

[CEF Integration 4](#_Toc56321232)

[1. Configuration of [partner product] to output CEF events 4](#_Toc56321233)

[2. Events 6](#_Toc56321234)

[3. Device Event Mapping to ArcSight Data Fields 6](#_Toc56321235)

[ArcSight Content for [partner product] 6](#_Toc56321236)

[Prerequisites 6](#_Toc56321237)

[Support 7](#_Toc56321238)

[Additional ArcSight Documentation 7](#_Toc56321239)

**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 Micro Focus. Micro Focus 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 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

|  |  |
| --- | --- |
| Date | Description |
| 11/15/2020 | First edition of this Configuration Guide. |

# 

# Polyverse Integration Guide

# This guide provides information for configuring the Polyverse Zerotect integration for ArcSight ESM. This integration is supported on ESM versions [6.0.0.1333] and later. Polyverse Zerotect version(s) 0.4.x is supported.

# Joint Solution Overview

[Add an overview of the product and integration here; for example: “The [vendor and product name] is the market leading Incident Response Platform… [Vendor’s] solution, in conjunction with Micro Focus ArcSight, provides users…”] Please ensure this section only contains information for the product that is being integrated with ArcSight and not all partner products. This section should focus on the problem Micro Focus and partner solve together and the benefits the integration provides to the customer.

Zerotect is an open-source agent that, when integrated with Micro Focus ArcSight, detects attempted zero-day attacks with no prior knowledge of the vulnerability or attack.

# Use Cases

This section describes important use cases supported by this integration.

* Ex: Insider threat prevention

[expand on use cases above if appropriate]

Use case 1 explanation (copy exact text listed above as use case in this heading, delete current text)

Explanation

Use case 2 explanation (copy exact text listed above as use case in this heading, delete current text)

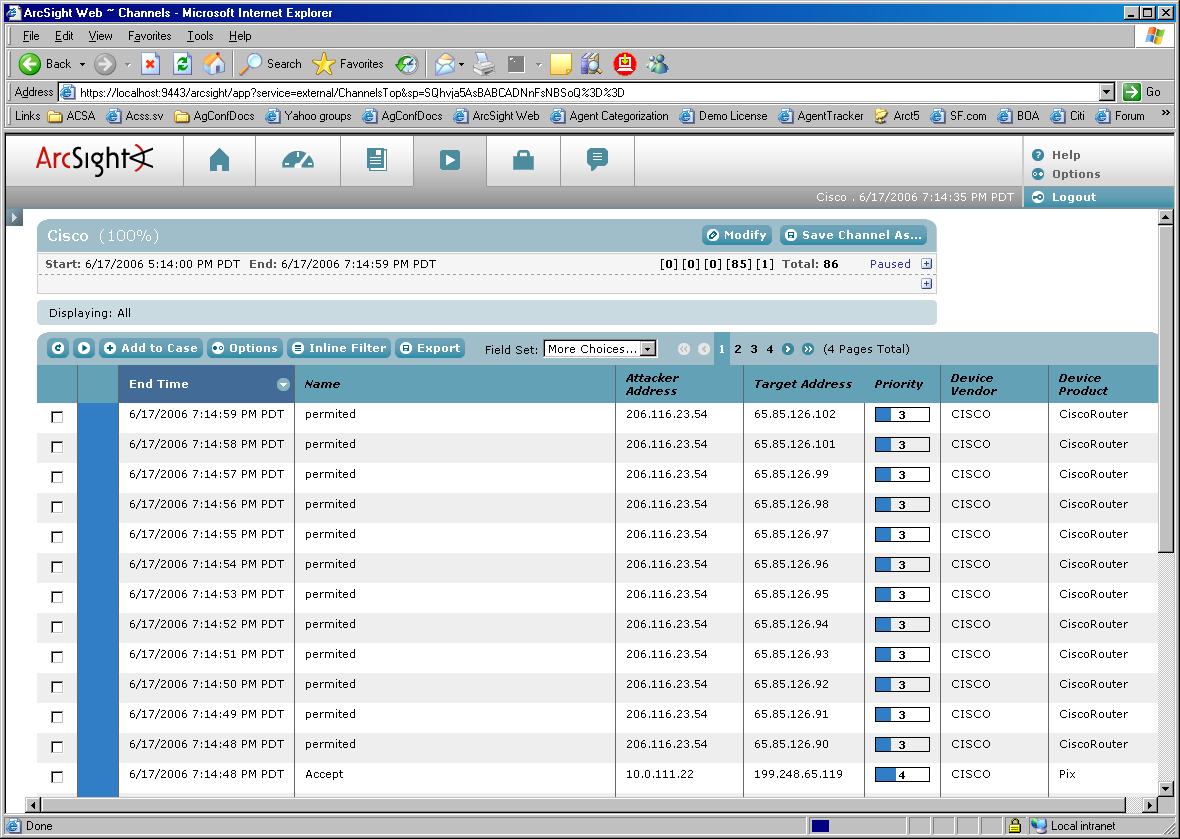
Explanation

# CEF Integration

# Configuration of [partner product] to output CEF events

[Please describe how your products need to be configured in order to send out CEF-formatted syslog output and include screenshots if applicable]

[Please include in the document a screenshot similar to the one below in which you have sent events from your solution to the ArcSight hosted server. It is beneficial to send as many different events as possible] Please center images.



# Events

[Please provide us with a list of all your events and event IDs. This can be provided in a separate document.]

# 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.

[Name of Connector] Connector Field Mappings

|  |  |
| --- | --- |
| Vendor-Specific Event Definition | ArcSight Event Data Field |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# ArcSight Content for [partner product]

**NOTE: If ArcSight content (Rules, Reports, Dashboards, etc) has been developed to support the integration, describe that here.**

**\* Delete this box\***

# Prerequisites

|  |  |  |
| --- | --- | --- |
| Product Name | Version Information | Operating System |
| Micro Focus ArcSight |  |  |

# 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:

**[NAME] Customer Support**

**Phone -[x-xxx-xxx-xxxx]**

**Email -[x@x.com]**

**Instructions –** [place instructions here on how the joint-customer should engage with the above options when calling about support of an integration with the ArcSight SIEM product.]

# Additional ArcSight Documentation

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

<https://marketplace.microfocus.com/arcsight/category/partner-integrations>

For more information about Micro Focus Security ArcSight ESM:

<https://software.microfocus.com/en-us/software/siem-security-information-event-management>