# ArcSight Enterprise Security Manager (ESM) 7.6.6
# Security Target

| | |
|---|---|
| *Date:* | December 11, 2025 |
| *Version:* | 1.29 |
| *Prepared By:* | *OpenText* |
| *Prepared For:* | *OpenText*<br>*275 Frank Tompa Drive*<br>*Waterloo ON N2L 0A1*<br>*Canada* |


## Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), ArcSight Enterprise Security Manager (ESM) 7.6.6. This ST defines list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

# Table of Contents

# List of Tables



# List of Figures

# 1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), Security Target organization, document conventions, and terminology. It also includes an overview of the evaluated product.

## 1.1 ST Reference

| | |
|---|---|
| **ST Title** | ArcSight Enterprise Security Manager (ESM) 7.6.6 Security Target |
| **ST Revision** | 1.29 |
| **ST Publication Date** | December 11, 2025 |
| **Author** | Dawn Adams |

## 1.2 TOE Reference

| | |
|---|---|
| **TOE Reference** | ArcSight Enterprise Security Manager (ESM) 7.6.6.18296.0 (ESM 7.6.4 with patch 7.6.6)<br><br>The TOE is also referred to as ArcSight ESM 7.6.6 or simply ArcSight ESM. For the purposes of this document, each is equivalent to ArcSight Enterprise Security Manager (ESM) 7.6.6. |

## 1.3 Document Organization

This Security Target follows the following format:

| SECTION | TITLE | DESCRIPTION |
|---|---|---|
| 1 | Introduction | Provides an overview of the TOE and defines the hardware and software that make up the TOE as well as the physical and logical boundaries of the TOE |
| 2 | Conformance Claims | Lists evaluation conformance to Common Criteria versions, Protection Profiles, or Packages where applicable |
| 3 | Security Problem Definition | Specifies the threats, assumptions and organizational security policies that affect the TOE |
| 4 | Security Objectives | Defines the security objectives for the TOE/operational environment and provides a rationale to demonstrate that the security objectives satisfy the threats |
| 5 | Extended Components Definition | Describes extended components of the evaluation (if any) |
| 6 | Security Requirements | Contains the functional and assurance requirements for this TOE |
| 7 | TOE Summary Specification | Identifies the IT security functions provided by the TOE and identifies the assurance measures targeted to meet the assurance requirements. |

**Table 1 - ST Organization and Section Descriptions**

## 1.4 Document Conventions

The notation, formatting, and conventions used in this Security Target are consistent with those used in Version 3.1 of the Common Criteria. Selected presentation choices are discussed here to aid the Security Target reader. The Common Criteria allows several operations to be performed on functional requirements: The allowable operations defined in Part 2 of the Common Criteria are *refinement, selection, assignment* and *iteration*.

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment operation is indicated by showing the value in square brackets, i.e. [assignment_value(s)].
- The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by bold text. Any text removed is indicated with a strikethrough format (Example: ~~TSF~~).
- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by *italicized* text.
- Iterated functional and assurance requirements are given unique identifiers by appending to the base requirement identifier from the Common Criteria an iteration number inside parenthesis, for example, FMT_MTD.1.1 (1) and FMT_MTD.1.1 (2) refer to separate instances of the FMT_MTD.1 security functional requirement component.

When not embedded in a Security Functional Requirement, italicized text is used for both official document titles and text meant to be emphasized more than plain text.

## 1.5 Document Terminology

The following table describes the acronyms used in this document:

| TERM | DEFINITION |
|---|---|
| CC | Common Criteria version 3.1 |
| EAL | Evaluation Assurance Level |
| EOE | Events Originating External to the TOE |
| ISO | International Standards Organization. When referring to a CD or DVD it means ISO-9660 |
| NTP | Network Time Protocol |
| OSP | Organizational Security Policy |
| OVF | Open Virtualization Format |
| SFP | Security Function Policy |
| SFR | Security Functional Requirement |
| ST | Security Target |
| TOE | Target of Evaluation |
| TSF | TOE Security Function |

**Table 2 - Acronyms Used in Security Target**

## 1.6 TOE Overview

The TOE is ArcSight Enterprise Security Management (ESM) 7.6.6. ArcSight ESM is a Security Information and Event Management (SIEM) solution that combines event correlation and security analytics to identify and prioritize threats in real time and remediate incidents early. It is able to concentrate, normalize, analyze, and report the results of its analysis of security event data

generated by various Intrusion Detection System (IDS) sensors and scanners in the operational environment. ArcSight ESM allows users to monitor events in real-time, correlate events for in-depth investigation and analysis, and resolve events with automated escalation procedures and actions.

The TOE is operating in FIPS mode.

ArcSight ESM is an enterprise network tool. It requires ArcSight SmartConnectors[1] to gather events from the network and normalize them into a standard scheme for correlation.

The TOE consists of the following components:

- Manager
- CORR-Engine (Correlation Optimized Retention and Retrieval Engine)
- ArcSight Console
- ArcSight Command Center (ACC)

The basic configuration is depicted in the figure[2] below:

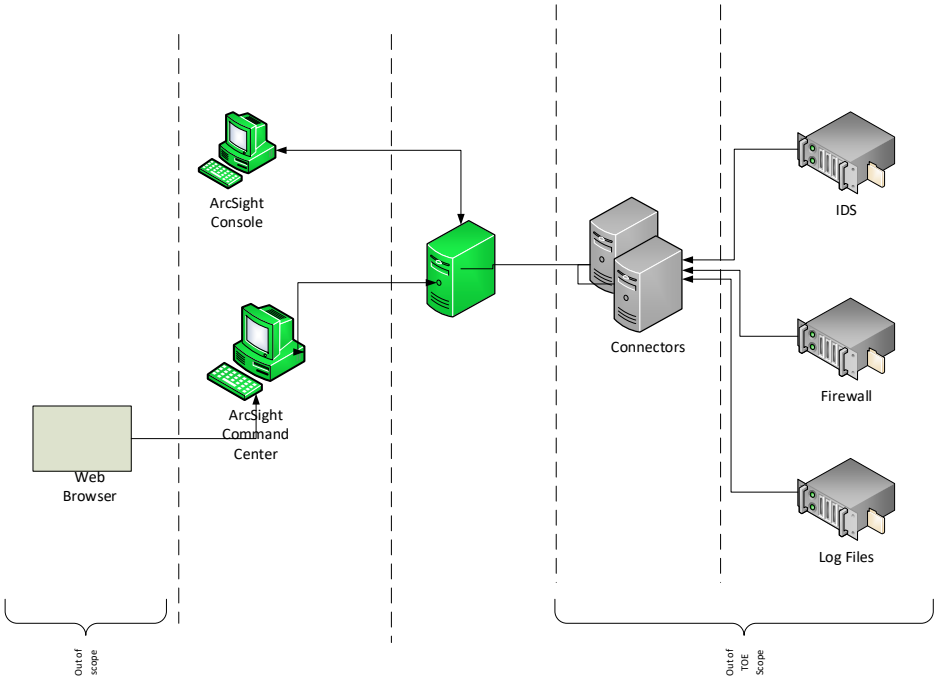



**Figure 1 –ArcSight ESM 7.6.6 Evaluated Configuration**

The TOE uses HTTPS/TLS v1.2 to protect communications between:

TOE and the connector(s)
Command center and User console and ArcSight ESM
web browser(s) and Command Center
Bouncy Castle v1.0.2.3 FIPS libraries provide TLS. The Bouncy Castle CMVP certificate is #3514.

[1] ArcSight Smart Connectors are outside of the TOE.
[2] Components that are not part of the TOE are to the right of the dotted line and in grey. These components are included in this diagram for completeness of documentation.

ArcSight ESM works by:

1. Gathering logs, events, and security information from the configured event sources in the IT environment.
2. Normalizing the collected logs, events, and security information into a common format.

This architecture enables ArcSight to:

1. Provide event searches across the entire ArcSight ESM infrastructure. i.e. on ArcSight ESM servers distributed across the globe.
2. Perform statistical analysis to establish baselines. These can then be used to compare the events that are currently occurring to determine if there are masked or not obvious problems.
3. Correlate sets of similar, or comparable, events in a given period to determine a pattern.
4. Organization of events into incidents for efficient response management and tracking.
5. Report based on real time and historical events.

### 1.6.1 Manager (a.k.a Persistor)

Manager performs management, correlation event enrichment, filtering, and processing for all security events collected in the system. The Manager is the center of ArcSight ESM and links the various components listed below ( i.e. Console, Command Center, Correlation Engines, and SmartConnectors).

### 1.6.2 ArcSight Console

The Console serves two functions. The first is to enable the configuration of security management functions including resource definition, monitoring and analysis of events, and responses. The second is to allow for the review and output from the product. Outputs include alerts (indicating anomalies) and reports indicating status and events. Access to Administrator or User functions are allowed based on user roles.

### 1.6.3 ArcSight Command Center

The Command Center is a web-based GUI that enables management of the system including event monitoring, running of reports, and managing storage. It is also used for license and user management.

### 1.6.4 Connectors

The connectors receive information from the various data sources and route them to ArcSight ESM.

### 1.6.5 Correlation Engine

The Correlation engine (aka CORR-Engine) is the mechanism that stores events and security management configuration information. This information includes users, groups, permissions, rules, zones, assets, templates, display layout, and other preferences.

### 1.6.6 Hardware and Software Supplied by the IT Environment

The TOE consists of a set of software applications. The hardware, operating systems and all third-party support software on the systems on which the TOE executes are excluded from the TOE boundary.

The TOE requires the following minimum hardware and software configuration:

| TYPE | VERSION/MODEL NUMBER |
|---|---|
| Operating System | Red Hat Enterprise Linux Server (RHEL) 8.10 64-bit |
| Processors | 16 cores total |
| Memory | 64 GB |
| Storage | 1.5 TB |

**Table 3– IT Environment**

**Other Supported operating systems for ArcSight ESM software:**

| Operating System |
|---|
| SUSE Linux Enterprise Server (SLES) 15 Service Pack 3, with or without FIPS enabled |
| Rocky Linux 8.10 |

All the supported Linux distributions require ESM patch 25.02 which can be obtained from https://sld.microfocus.com/mysoftware/download/downloadCenter

**Supported operating systems for the ArcSight Console**

| Operating System |
|---|
| SUSE Linux Enterprise Desktop 15 Service Pack 3 |
| Rocky Linux 8.10 |
| Red Hat Enterprise Linux Server (RHEL) 8.10 64-bit |
| Windows Server 2019 |
| Windows 10 Enterprise (including patches) |

**Supported browsers for ArcSight Command Center**

The latest version of Chrome, Firefox Extended Support Release, or Microsoft Edge (chromium-based only)

**Other Software supplied by the environment:**

OS time stamp

Connectors:

For the connectors you need one of:

Forwarding Connector - ArcSight-8.4.0.8962.0-SuperConnector64-Linux64.bin
Actor MIC for Linux - ArcSight-8.4.0.8954.0-ADActorModelConnector-Linux64.bin
Actor MIC for Windows - ArcSight-8.4.0.8954.0-ADActorModelConnector-Win64.exe
Asset MIC for Linux - ArcSight-8.4.0.8956.0-AssetModelImportConnector-Linux64.bin
Asset MIC for Windows - ArcSight-8.4.0.8956.0-AssetModelImportConnector-Win64.exe

Firewall The TOE can be configured to collect events from local systems or firewall, whatever the end user wishes to collect events from. These events will be input data into the ArcSight ESM TOE.

ArcSight ESM collects output from data sources like network nodes, intrusion detection and prevention systems, vulnerability assessment tools, firewalls, anti-virus and anti-spam tools, encryption tools, application audit logs, and physical security logs.

## 1.7 TOE Description

### 1.7.1 Physical Boundary

ArcSight ESM is a software product. It contains the following components:

- ArcSight Console v7.6.6
- ArcSight Command Center v7.6.6
- Manager v7.6.6
- Correlation Engine v7.6.6

The ArcSight Command Center, Manager, and Correlation Engine is contained in the ArcSightESMSuite-7.6.4.2572.0.tar with addition of Patch 7.6.6. (Patch-7.6.6.18296-ESM.zip)

The ArcSight Console is contained in ArcSight-7.6.6.0.18303.0-Console-Win.exe for the Windows environment or ArcSight-7.6.6.0.18303.0-Console-Linux.bin for the Linux environment.

### 1.7.2 Logical Boundary

This section outlines the boundaries of the security functionality of the TOE; the logical boundary of the TOE includes the security functionality described in the following table:

| TSF | DESCRIPTION |
|---|---|
| Security Audit | The TOE generates reports on the event analysis activities. Additionally, the TOE supports the provision of log data from each system component, such as user login/logout and incident/ticket management actions. It also records security events such as failed login attempts, etc. Audit trails can be stored for later review and analysis. |
| User Data Protection | The TOE provides a mechanism to segment access control and enable security attributes for access controls. |
| Identification and Authentication | The TOE enforces individual I&A in conjunction with group/role based I&A mechanisms. Operators must successfully authenticate using a unique identifier and password prior to performing any actions on the TOE. |
| Security Management | The TOE provides administrators with the capabilities to configure, monitor and manage the TOE. Security Management principles relate to management of access control policies as well as management of events and incidents. Administrators configure the TOE with the Console via Web-based connection. |
| TOE Access | The TOE provides a mechanism to automatically lock access and require re-authentication prior to re-enabling access. |
| Protection of the TSF | The TOE provides protected communications between the parts of the TOE. The TOE supports TLS v 1.2 as configured by the Administrator. The data is protected from modification and disclosure. |

| TSF | DESCRIPTION |
|---|---|
| Trusted Path / Channels | The TOE provides trusted channels between itself and external components (connectors) from disclosure and modification via HTTPS/TLS. The Trusted path is established (via HTTPS/TLS) for initial authentication and subsequent actions. The use of HTTPS/TLS protects communications from disclosure or modification. |
| Incident Management | The TOE provides Incident Management functions provide the capability to analyze security event data and incident workflow and alert. Audit data is collected by the TOE from the various devices that send event data, and the TOE analyzes this information against a set of correlation rules and filters. |

**Table 4 – Logical Boundary Descriptions**

### 1.7.3 Excluded TOE Capabilities:

The following features and capabilities of the TOE described in the guidance documentation are not included within the scope of the evaluation:

- Peer relationships between Persistor Nodes
- Pattern Discovery
- ArcSight Express Appliance
- Integrations with RepSM, ArcSight Event Broker, and ArcSight Investigate
- High Availability (HA) deployments
- The ability of the TOE to send Security Events as SNMP traps
- Support for external LDAP or RADIUS servers for user authentication
- Service Layer API
- Non-FIPS mode
- Suite B mode

SMTP, DNS and NTP are excluded from the evaluation.

### 1.7.4 TOE Product Documentation

In addition to the documentation generated for the certification, the TOE includes the following product and guidance documentation generated by OpenText. Documents are in both html and pdf format. These can be found on the document download site: ArcSight Enterprise Security Manager (ESM) 7.6 - Documentation | Micro Focus once the customer is given an account.

**NOTE: Software 7.6.4 is a scheduled release and has complete documentation. 7.6.6 is a patch and does not have documentation except release notes.**

- Release Notes for ArcSight ESM 7.6.6
- Technical Requirements for ESM 7.6
- Micro Focus Administrators Guide for ESM 7.6
- Micro Focus Security ArcSight ESM Software Version: 7.6.4 Installation Guide
- Micro Focus Security ArcSight ESM Software Version: 7.6.4Upgrade Guide
- Micro Focus Security ArcSight Forwarding Connector Software Version: 7.6.4 Configuration Guide Published: March 23, 2023

- Micro Focus Security ArcSight ESM Software Version: 7.6.4 ESM Best Practices Trends Published
- Micro Focus Security ArcSight ESM Software Version: 7.6.4 ArcSight Administration and ArcSight System Standard Content Guide
- ESM 101 Software version 7.6
- Micro Focus Security ArcSight Console User's Guide 7.6.4

The ArcSight ESM Operational User Guidance and Preparative Procedures Supplement (AGD-IGS), version 0.14, December 11, 2025, is supplied for those customers that need guidance on how to set the TOE in the evaluated configuration. This is maintained in a Micro Focus Teams repository.

### 1.7.5 TOE Delivery Mechanism:

The TOE software is provided to customers via secure download from the download portal https://sld.microfocus.com/mysoftware/download/downloadCenter

7.6.4 software is provided as a .tar file, ArcSightESMSuite-7.6.4.2572.0.tar. This requires the addition of Patch 7.6.6. (Patch-7.6.6.18296-ESM.zip)

Note: The cryptographic modules OpenSSL and Bouncy Castle are in the ESM tar file.

In addition to the tarfile, connector and console installation software must be downloaded.

For the console you need one of:

ArcSight-7.6.6.0.18303.0-Console-Win.exe
ArcSight-7.6.6.0.18303.0-Console-Linux.bin

Once downloaded, and extracted, the setup files can be executed to perform the installation.

# 2 Conformance Claims

## 2.1 CC Conformance Claim

The TOE is conformant to Common Criteria Version 3.1 CC Revision 5, April 2017 Part 2 extended and Part 3 conformant.

## 2.2 PP Claim

The TOE does not claim conformance to any registered Protection Profile.

## 2.3 Package Claim

The TOE claims conformance to the EAL3+ assurance package defined in Part 3 of the Common Criteria Version 3.1 Revision 5 (April 2017). The TOE does not claim conformance to any other functional package. The TOE EAL3 assurance package is augmented with ALC_FLR.3.

## 2.4 Conformance Rationale

No conformance rationale is necessary for this evaluation since this Security Target does not claim conformance to a Protection Profile.

# 3 Security Problem Definition

In order to clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:

- Any known or assumed threats to the assets against which specific protection within the TOE or its environment is required
- Any organizational security policy statements or rules with which the TOE must comply
- Any assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used.

This chapter identifies assumptions as A.*assumption*, threats as T.*threat* and policies as P.*policy*.

## 3.1 Threats

The following are threats identified for the TOE and the IT System the TOE monitors. The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all threats is unsophisticated.

The TOE addresses the following threats:

| THREAT | DESCRIPTION |
|---|---|
| T.NO_AUTH | An unauthorized user may gain access to the TOE and alter the TOE configuration. |
| T.INTEGRITY_COMP | An unauthorized user attempts to modify or destroy audit or IDS data by removing events. |
| T.NO_PRIV | An authorized user of the TOE exceeds his/her assigned security privileges resulting in unauthorized modification of the TOE configuration and/or user account data. |

**Table 5 - Threats Addressed by the TOE**

## 3.2 Organizational Security Policies

The TOE meets the following organizational security policies:

| ASSUMPTION | DESCRIPTION |
|---|---|
| P.EVENTS | All events from network-attached devices shall be monitored and reported. This enables the detection of potential events that may represent a security issue or other issues that may require additional analysis and mitigation. |
| P.CONFIG | The TOE is configured to receive all events from network-attached devices. |
| P.INCIDENTS | Security events that are correlated and classified as incidents result in alerts being sent to authorized personnel in order to have the incidents resolved more quickly. |

**Table 6 – Organizational Security Policies**

## 3.3 Assumptions

This section describes the security aspects of the environment in which the TOE is intended to be used. The TOE is assured to provide effective security measures in a co-operative non-hostile environment only if it is installed, managed, and used correctly. The following specific conditions are assumed to exist in an environment where the TOE is employed.

| ASSUMPTION | DESCRIPTION |
|---|---|
| A.LOCATE | The processing platforms (including operating system and HW) on which the TOE resides are trusted and are assumed to be located within a facility that provides controlled access. |
| A.MANAGE | Administrators of the TOE are assumed to be appropriately trained and competent to undertake the installation, configuration and management of the TOE in a secure and trusted manner. |
| A.NOEVIL | Administrators of the TOE and users on the local area network are not careless, willfully negligent, malicious, or hostile. |
| A.PROTECT | The TOE is protected from unauthorized physical and logical access. Communications are protected using TLS1.2 (includes Connector to Server and Console to Server). |
| A.TIMESOURCE | The environment provides a reliable, trusted timestamp to the TOE. |
| A.TRUSTED_IT | The connectors are considered to be a trusted IT product. |
| A.FILES | The operating system filesystem protects files written to the filesystem. |

**Table 7– Assumptions**

# 4 Security Objectives

## 4.1 Security Objectives for the TOE

The following are the TOE security objectives:

| OBJECTIVE | DESCRIPTION |
|---|---|
| O.AUDIT | The TOE shall be able to generate audit records of security-relevant events. |
| O.AUDIT_REVIEW | The TOE shall provide a means for authorized users to review the audit records generated by the TOE. |
| O.CAPTURE_EVENT | The TOE shall collect data in the form of events from security and non-security products with accurate timestamps and apply analytical processes to derive conclusions about events. The collected data is critical to the analysis and tracking of events in the environment which might indicate security issues. |
| O.CONFIGURE | The TOE is properly configured to allow event capturing. |
| O.MANAGE_INCIDENT | The TOE shall provide a mechanism to manage events and incidents. The TOE also manages the classification and correlation of the events. This mechanism enables the TOE to provide responses that authorized users may execute to analyze and expedite potential security events and issues, thus enabling TOE users to respond more quickly to events. |
| O.PROT_COMMS | TOE communications are protected from disclosure or modification. |
| O.SEC_ACCESS | The TOE shall ensure that only those authorized users and applications are granted access to security functions and associated data. This prevents unauthorized users from performing actions that may disable the TOE and result in undetected security events and issues. |

**Table 8 – TOE Security Objectives**

## 4.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are addressed below:

| OBJECTIVE | DESCRIPTION |
|---|---|
| OE.TIME | The TOE operating environment shall provide an accurate timestamp. |
| OE.ENV_PROTECT | The TOE operating environment shall provide mechanisms to isolate the TOE Security Functions (TSF) and assure that TSF components cannot be tampered with or bypassed. |
| OE.PERSONNEL | Authorized administrators are non-hostile and follow all administrator guidance. They must ensure that the TOE is installed, managed, and operated in a manner that maintains the TOE security.<br>Authorized administrators are also required to manage and administer the TOE in a secure manner. Authorized administrators must be competent and security aware personnel. |
| OE.PHYSEC | The facility surrounding the processing platform in which the TOE resides must provide a controlled means of access into the facility. |
| OE.TRUSTED | The TOE has communications with Connectors, a trusted IT product. |

**Table 9– Operational Environment Security Objectives**

## 4.3 Security Objectives Rationale

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions, threats, and Organizational Security Policies.

| OBJECTIVES / ASSUMPTIONS/ THREATS/ POLICIES | O.AUDIT | O.AUDIT_REVIEW | O.CAPTURE_EVENT | O.CONFIGURE | O.MANAGE_INCIDENT | O.PROT_COMMS | O.SEC_ACCESS | OE.TIME | OE.ENV_PROTECT | OE.PERSONNEL | OE.PHYSEC | OE.TRUSTED |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A.LOCATE | | | | | | | | | | | ✓ | |
| A.MANAGE | | | | | | | | | | ✓ | | |
| A.NOEVIL | | | | | | | | | | ✓ | | |
| A.PROTECT | | | | | | | | | ✓ | | ✓ | |
| A.TIMESOURCE | | | | | | | | ✓ | | | | |
| A.TRUSTED_IT | | | | | | | | | | | | ✓ |
| A.FILES | | | | | | | | | ✓ | | | |
| T.NO_AUTH | ✓ | | | | | ✓ | ✓ | | | | | |
| T.INTEGRITY_COMP | ✓ | ✓ | | | | | ✓ | | | | | |
| T.NO_PRIV | ✓ | | | | | | ✓ | | | | | |
| P.EVENTS | | | ✓ | | | | | | | | | |
| P.CONFIG | | | ✓ | ✓ | | | | | | | | |
| P.INCIDENTS | | | | | ✓ | | | | | | | |

**Table 10 - Mapping of Assumptions, Threats, and OSPs to Security Objectives**

### 4.3.1 Security Objectives Mapping Rationale

| ASSUMPTION/ THREAT/ POLICY | RATIONALE |
|---|---|
| A.LOCATE | This assumption is addressed by<br>• OE.PHYSEC which ensures that the facility surrounding the processing platform in which the TOE resides provides a controlled means of access into the facility |
| A.MANAGE | This assumption is addressed by<br>• OE.PERSONNEL, which ensures that the TOE is managed and administered in a secure manner by a competent and security aware personnel in accordance with the administrator documentation. This objective also ensures that those responsible for the TOE install, manage, and operate the TOE in a secure manner |
| A.NOEVIL | This assumption is addressed by<br>• OE.PERSONNEL, which ensures that the TOE is managed and administered in a secure manner by non-hostile or non-malicious personnel. |

| ASSUMPTION/ THREAT/ POLICY | RATIONALE |
|---|---|
| A.PROTECT | This assumption is addressed by<br>• OE.ENV_PROTECT ensures the environment provides the protected domains the TOE executes in so the TOE functionality cannot be bypassed or tampered with.<br>• OE.PHYSEC which ensures that the facility surrounding the processing platform in which the TOE resides provides a controlled means of access into the facility |
| A.TIMESOURCE | This assumption is addressed by<br>• OE.TIME, which ensures the provision of a reliable and accurate time stamp. |
| A.TRUSTED_IT | This assumption is addressed by<br>• OE.TRUSTED which recognizes Connectors as trusted IT products. |
| A.FILES | This assumption is addressed by<br>• OE.ENV_PROTECT which protects files written to the OS filesystem. |
| T.NO_AUTH | This threat is countered by the following:<br>• O.AUDIT which ensures that the TOE shall be able to generate audit records of security-relevant events<br>• O.PROT_COMMS which provides communications protections for the TOE.<br>• O.SEC_ACCESS, which ensures that the TOE allows access to the security functions, configuration, and associated data only by authorized users and applications. |
| T.INTEGRITY_COMP | This threat is countered by:<br>• O.AUDIT which ensures that the TOE shall be able to generate audit records of security-relevant events.<br>• O.AUDIT_REVIEW which ensures that the TOE shall provide a means for authorized users to review the audit records generated by the TOE.<br>• O.SEC_ACCESS which ensures that only authorized users and applications are granted access to security functions and associated data. |
| T.NO_PRIV | This threat is countered by<br>• O.AUDIT which ensures that the TOE shall be able to generate audit records of security-relevant events<br>• O.SEC_ACCESS, which ensures that the TOE allows access to the security functions, configuration, and associated data only by authorized users and applications. |
| P.EVENTS | This organizational security policy is enforced by<br>• O.CAPTURE_EVENT, which ensures that the TOE collects security events from security products and non-security products deployed within a network and applies analytical processes to derive conclusions about the events and inform authorized personnel that the event requires resolution. |
| P.CONFIG | This organizational security policy is addressed by<br>• O.CAPTURE_EVENT which ensures the TOE can collect data from events in the environment.<br>• O.CONFIGURE which ensures the TOE is properly configured to properly capture events. |

| ASSUMPTION/ THREAT/ POLICY | RATIONALE |
|---|---|
| P.INCIDENTS | This organizational security policy is enforced by<br>• O.MANAGE_INCIDENT, which ensures that the TOE will provide the capability to provide workflow functionality to manage the resolution of incidents. |

**Table 11 - Mapping of Threats, Policies, and Assumptions to Objectives**

# 5 Extended Components Definition

A class of Security Information and Event Management (SIEM) requirements was created to specifically address the data collected, analyzed, and managed by a SIEM solution. The purpose of this class is to address the unique nature of SIEM solutions and provide requirements about collecting events and managing incidents. These requirements have no dependencies since the stated requirements embody all the necessary security functions.

## 5.1 Definition of Extended Components

### 5.1.1 Class SIEM: Incident Management

Incident Management functions provide the capability to analyze security event data and incident workflow.

#### 5.1.1.1 Event Analysis SIEM_ANL_EXT

**Family Behavior**

This family defines the requirements for security event analysis functionality.

**Component Leveling**


SIEM_ANL_EXT Event Analysis provides the analysis of security event data.

**Management: SIEM_ANL_EXT.1**

The following actions could be considered for the management functions in FMT:

a) Configuration of the analysis to be performed

**Audit: SIEM_ANL_EXT.1**

There are no auditable events foreseen.

**SIEM_ANL_EXT.1 Event Analysis**

Hierarchical to: No other components
Dependencies: No dependencies

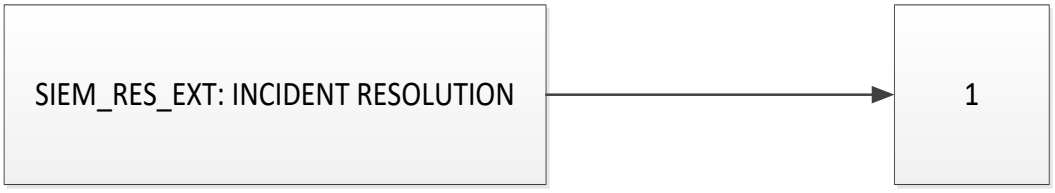
SIEM_ANL_EXT.1.1 The TSF shall perform [assignment: list of analysis functions] analysis function(s) on data collected from security and non-security products within a network.

#### 5.1.1.2 Incident Resolution SIEM_RES_EXT

**Family Behavior**

This family defines the requirements for security incident functionality.

**Component Leveling**




SIEM_RES_EXT provides the incident resolution workflow functionality.

**Management: SIEM_RES_EXT.1**

There are no management activities foreseen.

**Audit: SIEM_RES_EXT.1**

There are no auditable events foreseen.

**Incident Resolution: SIEM_RES_EXT.1**

Hierarchical to: No other components
Dependencies: No dependencies

SIEM_RES_EXT.1.1 The TSF shall provide a method to track the workflow of the resolution of an incident.

### 5.1.2 Class FTA: TOE Access

TOE Access functions provide facilities and controls for access to the TOE.

#### 5.1.2.1 Session locking and termination FTA_SSL_EXT

**Component Levelling**


FTA_SSL_EXT TSF-initiated session locking includes system-initiated locking of an interactive session after an administrator configured of user inactivity time interval has expired, but does not include clearing or overwriting the display.

**Management: FTA_SSL_EXT.1**

The following actions could be considered for the management functions in FMT:

a) specification of the time of user inactivity after which termination of the interactive session occurs for an individual user;

**Audit: FTA_SSL_EXT.1**

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Locking of an interactive session by the session locking mechanism.

b) Minimal: Successful unlocking of an interactive session.

c) Basic: Any attempts at unlocking an interactive session.

**FTA_SSL_EXT.1**

Hierarchical to: No other components
Dependencies: FIA_UAU.1 Timing of authentication

| | |
|---|---|
| FTA_SSL_EXT.1.1 | The TSF shall lock an interactive session after [assignment: a user inactivity time interval] by disabling any users actions other than unlocking the session. |
| FTA_SSL_EXT.1.2 | The TSF shall require the following events to occur prior to unlocking the session [assignment: events to occur]. |

# 6 Security Requirements

The security requirements that are levied on the TOE and the IT environment are specified in this section of the ST.

## 6.1 Security Functional Requirements

The functional security requirements for this Security Target consist of the following components from Part 2 of the CC, which are summarized in the following table:

| CLASS HEADING | CLASS_FAMILY | DESCRIPTION |
|---|---|---|
| Security Audit | FAU_GEN.1 | Audit Data Generation |
| | FAU_SAR.1 | Audit Review |
| | FAU_SAR.2 | Restricted Audit Review |
| | FAU_SAR.3 | Selectable Audit Review |
| | FAU_STG.1 | Protected Audit Storage |
| User Data Protection | FDP_ACC.1 | Subset Access Control |
| | FDP_ACF.1 | Security Attribute Based Access Control |
| | FTP_ITT.1 | Basic internal TSF data transfer protection |
| Identification and Authentication | FIA_AFL.1 | Authentication failure handling |
| | FIA_ATD.1 | User Attribute Definition |
| | FIA_SOS.1 | Verification of Secrets |
| | FIA_UAU.1 | Timing of Authentication |
| | FIA_UAU.5 | Multiple authentication mechanisms |
| | FIA_UID.1 | Timing of Identification |
| Security Management | FMT_MOF.1 | Management of Security Function Behaviour |
| | FMT_MSA.1 | Management of Security Attributes |
| | FMT_MSA.3 | Static Attribute Initialization |
| | FMT_MTD.1 | Management of TSF Data |
| | FMT_SMF.1 | Specification of Management Functions |
| | FMT_SMR.1 | Security Roles |
| TOE Access | FTA_SSL_EXT.1 | TSF-initiated session locking |
| | FTA_SSL.4 | User-initiated termination |
| | FTP_TRP.1 | Trusted Path |
| Incident Management | SIEM_ANL_EXT.1 | Event Analysis |
| | SIEM_RES_EXT.1 | Incident Resolution |

**Table 12 - TOE Security Functional Requirements**

### 6.1.1 Security Audit (FAU)

#### 6.1.1.1 FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;
b) All auditable events for the [*not specified*] level of audit; and
c) [User login/logout of the TOE;
d) Login failures;

e) Events from security products and non-security products]

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [no other audit relevant information].

#### 6.1.1.2 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide [the Administrator, and designated operators] with the capability to read [all audit data generated within the TOE, all data received / processed] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

#### 6.1.1.3 FAU_SAR.2 Restricted Audit Review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

#### 6.1.1.4 FAU_SAR.3 Selectable Audit Review

FAU_SAR.3.1 The TSF shall provide the ability to apply [sorting] of audit data based on [date and time, subject identity, type of event, success or failure of related event].

#### 6.1.1.5 FAU_STG.1 Protected Audit Storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to [***prevent***] unauthorized modifications to the stored audit records in the audit trail.

### 6.1.2 User Data Protection (FDP)

#### 6.1.2.1 FDP_ACC.1 Subset Access Control

FDP_ACC.1.1 The TSF shall enforce the [Administrative Access Control SFP] on [

Subjects: Administrator, Administrator Analyzer, Operator, Analyzer

Objects: System reports, component audit logs, configuration, timeouts, passwords, event queries, user accounts

Operations: create, modify, and delete users, query events, modify configuration data, create session termination timeouts, determine password complexity, change password, change defaults, modify the SFP, view dashboard, run reports, manage reports and searches, manage security incidents, and manage correlation rules]

]

#### 6.1.2.2 FDP_ACF.1 Security Attribute Based Access Control

FDP_ACF.1.1 The TSF shall enforce the [Administrative Access Control SFP] to objects based on the following: [
Subjects: Administrator, Administrator Analyzer, Operator, Analyzer
Objects: System reports, component audit logs, configuration, timeouts, passwords, event queries, user accounts
Attributes: password complexity, timeout duration, event log data usernames, account permissions, SFP defaults
]

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects as shown in the table below

| Functions | Administrator | Administrator Analyzer | Operator | Analyst |
|---|---|---|---|---|
| Configure TOE (includes PW complexity and timeout interval) | X | | | |
| Create/delete user accounts | X | | | |
| Modify user accounts | X | | | |
| Query Events | X | X | X | X |
| Change Defaults | X | | | |
| Modify the Administrative access control SFP | X | | | |
| Change own password | X | X | X | X |
| Run reports | X | X | X | X |
| Manage reports and searches | X | X | X | X |
| Manage security incidents | X | | X | |
| Manage correlation rules | X | X | | |
| View dashboard | X | X | X | X |

].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [no additional rules].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [no additional rules].

### 6.1.3 Security Management (FMT)

#### 6.1.3.1 FMT_MOF.1 Management of Security Function Behavior

FMT_MOF.1.1 The TSF shall restrict the ability to [*modify the behavior of*] the functions [of IDS analysis and reaction] to [Administrator, Analyzer Administrator].

#### 6.1.3.2 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [Administrative Access Control SFP] to restrict the ability to [*change_default values, query, modify, delete*] the security attributes [User identity or Roles] to [Administrator].

#### 6.1.3.3 FMT_MSA.3 Static Attribute Initialization

FMT_MSA.3.1 The TSF shall enforce the [Administrative Access Control SFP] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [Administrator] to specify alternative initial values to override the default values when an object or information is created.

#### 6.1.3.4 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to [*perform the functions listed in Table 14*] the [data described in the Table 14] to [Administrator]:

| ROLE DATA | CHANGE_DEFAULT | QUERY | MODIFY | DELETE |
|---|---|---|---|---|
| User Role | ✓ | ✓ | ✓ | ✓ |
| User Account Attributes | | ✓ | ✓ | |

**Table 13 - Management of TSF data**

#### 6.1.3.5 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [

a) Create accounts
b) Modify accounts
c) Define User Roles
d) Change Default, Query, Modify the attributes associated with the Administrative Access Control SFP
e) Modify the behavior of the Administrative Access Control SFP
f) Manage security incidents
g) Manage correlation rules
h) Manage Reports and Searches
i) Change the user inactivity timeout interval].

*Application Note: Security incidents are groups of events that represent an actionable security incident, plus associated state and meta-information. Incidents are created manually or through Correlation rules.*

#### 6.1.3.6 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [Administrator, Analyzer Administrator, Operator and Analyst roles].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

### 6.1.4 Identification and Authentication (FIA)

#### 6.1.4.1 FIA_AFL.1 Authentication Failure Handling

FIA_AFL .1.1 The TSF shall detect when [*an administrator configurable positive integer within [*1 to 10*]*] unsuccessful authentication attempts occur related to [user login]

FIA_AFL .1.2 When the defined number of unsuccessful authentication attempts has been [*met*], the TSF shall [disable the user account, either for an administrator configurable period of time, or until re-enabled by an administrator].

#### 6.1.4.2 FIA_ATD.1 – User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [User Identity, Authentication Data, Authorizations Group membership, eMail address].

#### 6.1.4.3 FIA_SOS.1 Verification of Secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [the following constraints for all user accounts: minimum length 6 characters, maximum 20 characters consisting of alphanumeric characters].

#### 6.1.4.4 FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow [java servlets status and authenticate process initiation] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

#### 6.1.4.5 FIA_UAU.5 Multiple Authentication Mechanisms

FIA_UAU.5.1 The TSF shall provide [passwords, digital certificates] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [following:
- Users can be configured for the following authentication modes: Password-based , Password-based and certificate-based , Password-based or certificate-based , Certificate-based
- Users configured for "password-based or certificate-based" select the authentication mechanism during login
- Users configured for "password-based and certificate-based" must satisfy the

authentication requirements of both mechanisms in order to be successfully authenticated**].**

#### 6.1.4.6 FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow [java servlets status and authenticate] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

### 6.1.5 TOE Access (FTA)

#### 6.1.5.1 FTA_SSL-EXT.1 TSF-initiated session locking

FTA_SSL_EXT.1.1 The TSF shall lock an interactive session [after an administrator-configured user inactivity time interval has expired] by disabling any user actions other than unlocking the session.

FTA_SSL_EXT.1.2 The TSF shall require the following events to occur prior to unlocking the session: [the user must re-authenticate to the TOE].

**Application Note**: This SFR applies only to the Command Center and not the Console.

#### 6.1.5.2 FTA_SSL.4 User-initiated termination

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's own interactive session.

### 6.1.6 Protection of the TSF (FPT)

*Application Node: As defined in TLS v1.2, Diffie-Hellman is used to exchange keys for TLS.*

#### 6.1.6.1 FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1.1 The TSF shall protect TSF data from [*disclosure, modification]* when it is transmitted between separate parts of the TOE.

### 6.1.7 Trusted path/channels (FTP)

*Application Node: As defined in TLS v1.2, Diffie-Hellman is used to exchange keys for TLS.*

#### 6.1.7.1 FTP_ITC.1

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [*TSF, another trusted IT product]* to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [transfer of event data to the TOE].

#### 6.1.7.2 FTP_TRP.1 Trusted path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [*remote*] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **[***disclosure, [modification]*]**.**

FTP_TRP.1.2 The TSF shall permit [*remote users*] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [*initial user authentication*, *[all remote administrative actions]*].

### 6.1.8 Incident Management (SIEM)

#### 6.1.8.1 SIEM_ANL_EXT.1 Event Analysis

SIEM_ANL_EXT.1.1 The TSF shall perform [filtering and correlation] analysis function(s) on data collected from security and non-security products within a network.

#### 6.1.8.2 SIEM_RES_EXT.1 Incident Resolution

SIEM_RES_EXT.1.1 The TSF shall provide a method to track the workflow of the resolution of an incident.

## 6.2 Security Assurance Requirements

The Security Assurance Requirements for this evaluation are listed in Section 6.3.4 – Security Assurance Requirements.

## 6.3 Security Requirements Rationale

### 6.3.1 Security Functional Requirements

The following table provides the correspondence mapping between security objectives for the TOE and the requirements that satisfy them.

| OBJECTIVE / SFR | O.AUDIT | O.AUDIT_REVIEW | O.CAPTURE_EVENT | O.MANAGE_INCIDENT | O.SEC_ACCESS | O.PROT_COMMS |
|---|---|---|---|---|---|---|
| FAU_GEN.1 | ✓ | | ✓ | ✓ | | |

| SFR \ OBJECTIVE | O.AUDIT | O.AUDIT_REVIEW | O.CAPTURE_EVENT | O.MANAGE_INCIDENT | O.SEC_ACCESS | O.PROT_COMMS |
|---|---|---|---|---|---|---|
| FAU_SAR.1 | | ✓ | ✓ | ✓ | | |
| FAU_SAR.2 | | ✓ | | | | |
| FAU_SAR.3 | | ✓ | | | | |
| FAU_STG.1 | ✓ | | ✓ | | | |
| FDP_ACC.1 | | | | | ✓ | |
| FDP_ACF.1 | | | | | ✓ | |
| FIA_AFL.1 | | | | | ✓ | |
| FIA_ATD.1 | | | | | ✓ | |
| FIA_SOS.1 | | | | | ✓ | |
| FIA_UAU.1 | | | | | ✓ | |
| FIA_UAU.5 | | | | | ✓ | |
| FIA_UID.1 | | | | | ✓ | |
| FMT_MOF.1 | | | | | ✓ | |
| FMT_MSA.1 | | | | | ✓ | |
| FMT_MSA.3 | | | | | ✓ | |
| FMT_MTD.1 | | | | | ✓ | |
| FMT_SMF.1 | | | | | ✓ | |
| FMT_SMR.1 | | | | | ✓ | |
| FTA_SSL_EXT.1 | | | | | ✓ | |
| FTA_SSL.4 | | | | | ✓ | |
| FTP_TRP.1 | | | | | | ✓ |
| FTP_ITC.1 | | | | | | ✓ |
| FPT_ITT.1 | | | | | | ✓ |
| SIEM_ANL_EXT.1 | | | ✓ | | | |
| SIEM_RES_EXT.1 | | | | ✓ | | |

**Table 14 - Mapping of TOE Security Functional Requirements and Objectives**

### 6.3.2 Dependency Rationale

This ST satisfies all the security functional requirement dependencies of the Common Criteria. The table below lists each SFR to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

| SFR CLAIM | DEPENDENCIES | DEPENDENCY MET | RATIONALE |
|---|---|---|---|
| FAU_GEN.1 | FPT_STM.1 | YES | Satisfied by the Operational Environment (OE.TIME) |
| FAU_SAR.1 | FAU_GEN.1 | YES | |
| FAU_SAR.2 | FAU_SAR.1 | YES | |
| FAU_SAR.3 | FAU_SAR.1 | YES | |
| FAU_STG.1 | FAU_GEN.1 | YES | |
| FDP_ACC.1 | FDP_ACF.1 | YES | |
| FDP_ACF.1 | FDP_ACC.1<br>FMT_MSA.3 | YES | |
| FIA_AFL.1 | FIA_UAU.1 | YES | |
| FIA_ATD.1 | N/A | N/A | |
| FIA_SOS.1 | N/A | N/A | |
| FIA_UAU.1 | FIA_UID.1 | YES | |
| FIA_UAU.5 | N/A | N/A | |
| FIA_UID.1 | N/A | N/A | |
| FMT_MOF.1 | FMT_SMR.1,<br>FMT_SMF.1 | YES | |
| FMT_MTD.1 | FMT_SMR.1,<br>FMT_SMF.1 | YES | |
| FMT_MSA.1 | FDP_ACC.1<br>FMT_SMF.1<br>FMT_SMR.1 | YES | |
| FMT_MSA.3 | FMT_MSA.1<br>FMT_SMR.1 | YES | |
| FMT_MTD.1 | FMT_SMF.1<br>FMT_SMR.1 | YES | |
| FMT_SMF.1 | N/A | N/A | |
| FMT_SMR.1 | FIA_UID.1 | YES | |
| FPT_STM.1 | N/A | N/A | Satisfied by the Operational Environment (OE.TIME) |
| FTA_SSL_EXT.1 | FIA_UAU.1 | Yes | |
| FTA_SSL.4 | N/A | N/A | |
| FTP_ITC.1 | N/A | N/A | |
| FPT_ITT.1 | N/A | N/A | |
| FTP_TRP.1 | N/A | N/A | |
| SIEM_ANL_EXT.1 | N/A | N/A | |
| SIEM_RES_EXT.1 | N/A | N/A | |

**Table 15 - Mapping of SFRs to Dependencies**

### 6.3.3 Sufficiency of Security Requirements

The following table presents a mapping of the rationale of TOE Security Requirements to Objectives.

| Objective | RATIONALE |
|---|---|
| O.AUDIT | The TOE shall be able to generate audit records of security-relevant events.<br>• FAU_GEN.1 defines the auditing capability for administrative access control and requires that authorized users will have the capability to read and interpret data stored in the audit logs<br>• FAU_STG.1 requires the TOE protect the audit records from unauthorized deletion and modifications. |
| O.AUDIT_REVIEW | The TOE shall provide a means for authorized users to review the audit records generated by the TOE.<br>• FAU_SAR.1— specifies which roles can read data from stored audit records.<br>• FAU_SAR.2—specifies that the ability to read data from stored audit records is restricted to only the specified roles.<br>• FAU_SAR.3—FAU_SAR.1 by specifying capabilities for sorting audit records based on date / time the event is recorded, type of audit event, the subject of the audit event, and outcome of the event |
| O.CAPTURE_EVENT | The objective to ensure that the TOE will collect events from security products and non-security products deployed within a network and applies analytical processes to derive conclusions about the events is met by the following security requirements:<br>• FAU_GEN.1 and FAU_SAR.1 define the auditing capability for events and administrative access control and requires that authorized users will have the capability to read and interpret data stored in the audit logs<br>• FAU_STG.1 ensures that the TOE protects the audit records from unauthorized deletion and modifications.<br>• SIEM_ANL_EXT.1 ensures that the TOE performs analysis on all security events received from network devices |
| O.MANAGE_INCIDENT | The objective to ensure that the TOE provides a workflow to manage incidents is met by the following security requirements:<br>• FAU_GEN.1 and FAU_SAR.1 define the auditing capability for incidents and administrative access control and requires that authorized users will have the capability to read and interpret data stored in the audit logs<br>• SIEM_RES_EXT.1 ensures that the TOE provides the capability to manage status and track action items in the resolution of incidents |
| O.PROT_COMMS | TOE communications are protected from disclosure or modification. This is met by the following security requirements:<br>• FPT_ITT.1, FTP_ITC.1 and FTP_TRP which specify that communications are protected from disclosure and modifications. |

| Objective | RATIONALE |
|---|---|
| O.SEC_ACCESS | This objective ensures that the TOE allows access to the security functions, configuration, and associated data only by authorized users and applications.<br>• FDP_ACC.1 requires that all user actions resulting in the access to TOE security functions and configuration data are controlled<br>• FDP_ACF.1 supports FDP_ACC.1 by ensuring that access to TOE security functions, configuration data, audit logs, and account attributes is based on the user roles and their allowable actions<br>• FIA_AFL.1 controls the response to failed access attempts.<br>• FIA_ATD.1 specifies security attributes for users of the TOE<br>• FIA_SOS.1 controls consistency and requirements for passwords<br>• FIA_UAU.1 allows the user to view the java servlets status and initiate the authentication service before the user is authenticated. The TOE enforces authentication of all users prior to accessing any other TSF functionality.<br>• FIA_UAU.5 enables the TOE to use multiple authentication mechanisms.<br>• FIA_UID.1 enables the TOE to identify a user prior to performing any other actions.<br>• FMT_MOF.1 the TOE restricts the ability to modify the behavior to administrators and analyzer administrators.<br>• FMT_MSA.1 specifies that only privileged administrators can manage security attributes.<br>• FMT_MSA.3 ensures that all default values of security attributes are restrictive in nature as to enforce the access control policy for the TOE. The Administrator can specify alternative initial values that will override default values.<br>• FMT_MTD.1 restricts the ability to perform the functions listed in Table 15 on TSF data to the Administrator.<br>• FMT_SMF.1 and FMT_SMR.1 support the security functions relevant to the TOE and ensure the definition of an authorized administrator role.<br>• FTA_SSL_EXT.1 requires the TSF lock after a period of inactivity.<br>• FTA_SSL.4 requires the user be able to initiate a session termination. |

**Table 16 - Rationale for TOE SFRs to Objectives**

### 6.3.4 Security Assurance Requirements

The assurance security requirements for this Security Target are taken from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 3 (EAL3) augmented with ALC_FLR.3. The assurance components are summarized in the following table:

| CLASS HEADING | CLASS_FAMILY | DESCRIPTION |
|---|---|---|
| ADV: Development | ADV_ARC.1 | Security Architecture Description |
| | ADV_FSP.3 | Functional Specification with Complete Summary |
| | ADV_TDS.2 | Architectural Design |
| | AGD_OPE.1 | Operational User Guidance |

| CLASS HEADING | CLASS_FAMILY | DESCRIPTION |
|---|---|---|
| AGD: Guidance Documents | AGD_PRE.1 | Preparative Procedures |
| ALC: Lifecycle Support | ALC_CMC.3 | Authorization Controls |
| | ALC_CMS.3 | Implementation representation CM coverage |
| | ALC_DEL.1 | Delivery Procedures |
| | ALC_DVS.1 | Identification of Security Measures |
| | ALC_LCD.1 | Developer defined life-cycle model |
| | ALC_FLR.3 | Systematic flaw remediation |
| ATE: Tests | ATE_COV.2 | Analysis of Coverage |
| | ATE_DPT.1 | Testing: Basic Design |
| | ATE_FUN.1 | Functional Testing |
| | ATE_IND.2 | Independent Testing - Sample |
| AVA: Vulnerability Assessment | AVA_VAN.2 | Vulnerability Analysis |

**Table 17 - Security Assurance Requirements at EAL3+**

### 6.3.5 Security Assurance Requirements Rationale

The ST specifies Evaluation Assurance Level 3+. EAL3+ was chosen because it is based upon good commercial development practices with thorough functional testing. EAL3+ provides the developers and users a moderate level of independently assured security in conventional commercial TOEs. The threat of malicious attacks is not greater than low, the security environment provides physical protection, and the TOE itself offers a very limited interface, offering essentially no opportunity for an attacker to subvert the security policies without physical access.

### 6.3.6 Security Assurance Requirements Evidence

This section identifies the measures applied to satisfy CC assurance requirements.

| SECURITY ASSURANCE REQUIREMENT | EVIDENCE TITLE |
|---|---|
| ADV_ARC.1 Security Architecture Description | ArcSight 7.6.6 Security Architecture (ADV_ARC) |
| ADV_FSP.3 Functional Specification with Complete Summary | ArcSight 7.6.6 Functional Specification |
| ADV_TDS.2 Architectural Design | ArcSight 7.6.6 Architectural Design |
| AGD_OPE.1 Operational User Guidance | ArcSight Administration Guide March 2023<br>ArcSight User Guide March 2023<br>ArcSight Installation and Configuration Guide March 2023<br>ArcSight 7.6.6<br>Operational User Guidance and Preparative Procedures Supplement |
| AGD_PRE.1 Preparative Procedures | ArcSight 7.6.6 Operational User Guidance and Preparative Procedures Supplement |
| ALC_CMC.3 Authorization Controls | ArcSight ESM 7.6.6 Configuration Management Processes and Procedures (ALC_CM) |

| SECURITY ASSURANCE REQUIREMENT | EVIDENCE TITLE |
|---|---|
| ALC_CMS.3 Implementation representation CM coverage | ArcSight ESM 7.6.6 Configuration Management Processes and Procedures (ALC_CM) |
| ALC_DEL.1 Delivery Procedures | ArcSight ESM 7.6.6 Secure Delivery Processes and Procedures: (ALC_DEL) |
| ALC_DVS.1 Identification of Security Measures | ArcSight ESM 7.6.6 Development Security Measures (ALC_DVS) |
| ALC_LCD.1 Developer defined life-cycle model | ArcSight ESM 7.6.6 Life Cycle Development Process (ALC_LCD) |
| ALC_FLR.3: Flaw Remediation Procedures | ArcSight ESM 7.6.6 Systematic Flaw Remediation (ALC_FLR) |
| ATE_COV.2 Analysis of Coverage | ArcSight ESM 7.6.6 Test Plan and Coverage Analysis |
| ATE_DPT.1 Testing: Basic Design | ArcSight ESM 7.6.6 Test Plan and Coverage Analysis |
| ATE_FUN.1 Functional Testing | ArcSight ESM 7.6.6 Test Plan and Coverage Analysis |

**Table 18 - Security Assurance Rationale and Measures**

# 7 TOE Summary Specification

This section presents the Security Functions implemented by the TOE.

## 7.1 TOE Security Functions

The security functions performed by the TOE are as follows:

- Security Audit
- Identification and Authentication
- Incident Management
- Security Management
- TOE Access
- Protection of the TSF
- Trusted Path / Channels
- User Data Protection

## 7.2 Security Audit

**System Events**: System events are a means to report on the status and status change of the TOE. While the TOE accepts events from outside, it can generate three classes of events:

- Internal Events: These are informational and describe a single state or change of state in the system. They report when a user logs in or fails to authenticate, when a process is started, or a correlation rule is activated.
- Performance Events: These are generated on a periodic basis and describe average resources used by different parts of the system.
- Audit Events: These are generated internally. Each time an audited method is called, or an audited data object is modified, audit framework generates audit events. There are two types of Audit Events. One which monitors user actions for example, user login/out, add/delete user and another which monitors system actions/health, for example, process start/stop. Audit Events can be logged into log files, saved into database, and sent out as Audit Event at the same time. (Internal Events are only sent out as events.).

System Events record the date and time of the event, type of event, event subject identity and outcome of the event.

The TOE generates the following audit data:

- Start-up and shutdown of the audit functions (instantiated by start-up of the TOE)
- User login/logout
- Login failures

**Audit Handing:** The TOE provides the Administrator with the capability to read all audit data generated within the TOE via the Console. The GUI provides a suitable means for an Administrator to interpret the information from the audit log.

The TOE prevents the audit log from unauthorized deletion and modification entries in the log files.

The TOE provides users with the capability to filter security event data queries and searches. Filter expressions are simple math expressions and simple evaluations. Filters work on selection sets by matching events against the specified criteria. Filters are applied to data collected by the TOE. The

Correlation Engine provides the capability for users to correlate security events. Correlation automates analysis of event data to find patterns of interest. The TOE enables users to define correlations between events through the definition of rules that define these patterns of interest.

The A.TIMESOURCE is added to the assumptions on operational environment, and OE.TIME is added to the operational environment security objectives. The time and date are provided by the operational environment. The TOE ensures that the audit trail data is stamped when recorded with a dependable date and time received from the OE (operating system). In this manner, accurate time and date is maintained on the TOE.

The Security Audit function is designed to satisfy the following security functional requirements:

- FAU_GEN.1
- FAU_SAR.1
- FAU_SAR.2
- FAU_SAR.3
- FAU_STG.1

## 7.3 Identification and Authentication

The Console provides user interfaces that administrators may use to manage TOE functions. The Console provides web-based access to TOE functions through supported web browsers.

The TOE enforces individual identification and authentication and provides a centralized authentication mechanism. The TOE handles issues with authentication failure. The TOE enables multiple authentication mechanisms as well as the ability to specify rules for password acceptance. The TOE also provides multiple authentication mechanisms to log into the Command Center which also allows resource access based on user type.

Operators with management access must successfully authenticate themselves using a unique identifier and authenticator prior to performing any actions on the TOE. The TOE maintains authorization information that determines which TOE functions an authenticated administrator or user (of a given role) may perform.

The TOE maintains the following list of security attributes belonging to individual users:

- User Identity (i.e., username)
- Password
- Roles

The Identification and Authentication function is designed to satisfy the following security functional requirements:

- FIA_AFL.1
- FIA_ATD.1
- FIA_SOS.1
- FIA_UAU.1
- FIA_UAU.5
- FIA_UID.1

## 7.4 Incident Management

The TOE provides the capability for analysis as well as automating and tracking incident response processes. The TOE tracks security problems from identification through resolution by allowing the creation of "workflows". Workflows are designed to provide a simple, flexible solution for automating and tracking an enterprise's incident response processes. Workflow refers to the way in which people in the organization are informed about incidents, how incidents are escalated to other users, and how incident responses are tracked.

The administrator creates a notification rule. Once that rule containing notification action is triggered, the ArcSight ESM notification engine notifies all active destinations in the first escalation level within the notification group. The notification engine then waits for a certain time period for a user to acknowledge having received the notification. If no acknowledgment is received within the specified time interval, the same notification is escalated to the next level within the group. This process repeats until there are no more escalation levels or the notification is acknowledged by the appropriate recipients. The notification structure contains notification groups, escalation levels, and destinations.

**Events Originating External to the TOE (EOE)**: These external events are collected, either via a push or pull, from the various event sources. Event sources may include and are not limited to, network nodes, intrusion detection and prevention systems, vulnerability assessment tools, firewalls, anti-virus and anti-spam tools, encryption tools, application audit logs, and physical security logs.

These events are consumed by the TOE and are normalized into a common schema and classification taxonomy. This data is then correlated and used to detect abnormal behavior and anomalies within your infrastructure. These may also include alerts that indicate interesting events such as those dealing with security or threshold violations.

EOE includes timestamps, origin, event information, completion status of the event, and other data as specified in the report.

When ArcSight ESM receives the formatted data from the connectors, a correlation is made of the events.

Correlation is a process that discovers the relationships between events, infers the significance of those relationships, prioritizes them, then provides a framework for taking actions.

The ArcSight Manager is a Java-based server that drives analysis, workflow, and services. It also correlates output from a wide variety of security systems. The Manager writes events to the CORR-Engine as they stream into the system. It simultaneously processes them through the correlation engine, which evaluates each event with network model and vulnerability information to develop real-time threat summaries.

ArcSight ESM comes with default configurations and standard foundation use cases consisting of filters, rules, reports, data monitors, dashboards, and network models that make ArcSight ESM ready to use upon installation. You can also design the entire process that the Manager drives, from detection, to correlation, to escalation.

The Incident Management function is designed to satisfy the following security functional requirements:

- SIEM_RES_EXT.1
- SIEM_ANL_EXT.1

## 7.5 Security Management

Security Management is provided by enforcement of roles. Each role consists of a series of privileges. Roles can have privileges added to or removed from them. These roles are then assigned to individuals. Note a user may only have one role at a time.
The TOE restricts the ability to change the functions of analysis to administrators and analyzer administrators.
Only Administrators have the capability to change default values, query, modify, or delete users or roles.
The TOE provides restrictive default values for security attributes by requiring the Administrator to explicitly allow access to Users. Only the Administrator may be able to change defaults.
Only the Administrator can control user privileges and user accounts attributes.

The TOE provides the following management functions. The associated SFRs are noted in the table below.

| SFR |
|---|
| FMT_MOF.1 |
| FMT_MSA.1 |
| FMT_MSA.3 |
| FMT_MTD.1 |
| FMT_SMF.1 |
| FMT_SMR.1 |

The TOE provides multiple user roles including Administrator, Analyzer Administrator, Operator and Analyst roles. The following table has a description of each role.

| Role | Responsibilities |
|---|---|
| Administrator | Administrators are responsible for overseeing the installation of the system and maintaining overall system health. Administrators install and configure the Manager, Console and SmartConnectors, and integrate ArcSight ESM with devices from multiple vendors.<br><br>Install and configure ArcSight ESM<br>Add and maintain ArcSight ESM users and permissions<br>Sets security policies<br>View ArcSight Status Monitors (ASMs)<br>Monitor Manager administration e-mails<br>Maintain the health of the Manager and data store<br>Use the Packages and archive utilities to backup and support Manager deployments<br>Monitor the health of SmartConnectors and the devices that report to them<br>Design and maintain workflow infrastructure |
| Analyzer Administrator | Analyzer Administrators are responsible for developing use cases that address enterprise needs and goals. This role oversees the content that shapes the nature and direction of how investigation, historical |

| | |
|---|---|
| | analysis, and remediation are conducted in the security operations center.<br><br>Identify and design use cases that address specific enterprise needs<br>Evaluate existing standard content and use cases and adapt them to meet enterprise goals<br>Develop and test new correlation content and use cases using filters, rules, data monitors, active lists, and session lists<br>Develop and test new monitoring tools using active channels, dashboards, reports, and trends<br>Develop and post knowledge base articles; develop Threat Detector profiles |
| Operator | Security operations center operators are responsible for daily event monitoring and investigating incidents to a triage level. Operators observe real-time events and replay events using replay tools. They interpret events and respond to events with preset, automated actions. They also run reports.<br><br>Watch active channels and dashboards<br>Create annotations and create cases<br>Forward events and cases to analysts for further investigation |
| Analyst | Security analysts are responsible for specialized investigation and remediation when triggered into action by notifications from security center operators. Analysts may also be operators, or they can be specialists who respond to particular situations.<br><br>Investigate incidents using channels, event graphs, annotations, cases, and reports<br>Recommend and implement responses |

**Table 19 – Role description**

| **Functions** | **Administrator** | | **Administrator Analyzer** | **Operator** | **Analyst** |
|---|---|---|---|---|---|
| Configure TOE (includes PW complexity and timeout interval) | X | | | | |
| Create user accounts | X | | | | |
| Modify user accounts | X | | | | |
| Change Defaults | X | | | | |
| Modify the Administrative access control SFP | X | | | | |

| | | | | | |
|---|---|---|---|---|---|
| Change own password | X | | X | X | X |
| Query | X | | X | X | X |
| Run reports | X | | X | X | X |
| Manage reports and searches | X | | X | X | X |
| Manage security incidents | X | | | X | |
| Manage correlation rules | X | | X | | |

**Table 20 – Roles and access to functions**

## 7.6 TOE Access

The TOE provides a mechanism to automatically lock access and require re-authentication prior to re-enabling access. Note: this only applies to the Command Center, not to the Console.

The user has the ability to terminate their own session without waiting for a session timeout.

This function is designed to satisfy the following security functional requirements.

- FTA_SSL_EXT.1
- FTA_SSL.4

## 7.7 Protection of the TSF

The TOE protects transfers between parts of the TOE using TLS v1.2. Data is protected from modification or disclosure. For Java code, it's either the JCE/JSSE libraries (when ArcSight ESM is in non-FIPS mode), or Bouncy Castle v1.0.2.3 FIPS libraries when in FIPS mode. The Bouncy Castle CMVP certificate is #3514.

This satisfies FPT_ITT.1.

## 7.8 Trusted Path

The TOE supports TLS v 1.2 as configured by the Administrator. Browsers coming into the TOE must use TLS1.2 to establish a connection.

The TOE uses a cryptographic module that provides support for the HTTPS/TLS communications used between TOE components and between the TOE and external web servers.
For Java code, it's either the JCE/JSSE libraries (when ArcSight ESM is in non-FIPS mode), or Bouncy Castle v1.0.2.3 FIPS libraries when in FIPS mode. The Bouncy Castle CMVP certificate is #3514.

Connections between the Connectors and the TOE are protected by TLS v1.2.

The Trusted Path/Channels function is designed to satisfy the following security functional requirements:

- FTP_TRP.1 from the Web browser (external) to the TOE.
- FTP_ITC.1 from Connectors to the TOE

TLS Cipher suites:
The following cipher suites are supported:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_ SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_ SHA384

## 7.9 User Data Protection

The TOE provides a mechanism for User Data Protection via subset access controls and security attribute-based access controls.

The User Data Protection mechanisms are designed to satisfy the following security functional requirements:

- FDP_ACC.1
- FDP_ACF.1