Hewlett Packard Enterprise
ArcSight ESM
Security Target

Version 1.3
13 June 2017

Prepared for:

Hewlett Packard
Enterprise

1160 Enterprise Way
Sunnyvale CA, 94089

Prepared By:

Accredited Testing and Evaluation Labs
6841 Benjamin Franklin Drive
Columbia, MD 21046

TABLE OF CONTENTS

LIST OF TABLES

1. Introduction

This section introduces the Target of Evaluation (TOE) and provides the Security Target (ST) and TOE identification, ST and TOE conformance claims, ST conventions, glossary and list of abbreviations.

The TOE is ArcSight Enterprise Security Management (ESM) 6.11.0 from Hewlett Packard Enterprise. 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 ST contains the following additional sections:

- TOE Description (Section 2)—provides an overview of the TOE and describes the physical and logical boundaries of the TOE
- Security Problem Definition (Section 3)—describes the threats and assumptions that define the security problem to be addressed by the TOE and its environment
- Security Objectives (Section 4)—describes the security objectives for the TOE and its operational environment necessary to counter the threats and satisfy the assumptions that define the security problem
- IT Security Requirements (Section 5)—specifies the security functional requirements (SFRs) and security assurance requirements (SARs) to be met by the TOE
- TOE Summary Specification (Section 6)—describes the security functions of the TOE and how they satisfy the SFRs
- Rationale (Section 7)—provides mappings and rationale for the security problem definition, security objectives, security requirements, and security functions to justify their completeness, consistency, and suitability.

1.1 Security Target, TOE and CC Identification

ST Title – Hewlett Packard Enterprise ArcSight ESM Security Target

ST Version – Version 1.3

ST Date – 13 June 2017

TOE Identification – ArcSight ESM 6.11.0

TOE Developer – Hewlett Packard Enterprise

Evaluation Sponsor – Hewlett Packard Enterprise

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012

1.2 Conformance Claims

This ST and the TOE it describes are conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, Version 3.1 Revision 4, September 2012.
    - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1 Revision 4, September 2012.
    - Part 3 Conformant

This ST and the TOE it describes are conformant to the following package:

- EAL2.

1.3 Conventions

The following conventions are used in this document:

- Security Functional Requirements—Part 1 of the CC defines the approved set of operations that may be applied to functional requirements: iteration; assignment; selection; and refinement.
    - Iteration—allows a component to be used more than once with varying operations. In this ST, iteration is identified with a number in parentheses following the base component identifier. For example, iterations of FCS_COP.1 are identified in a manner similar to FCS_COP.1(1) (for the component) and FCS_COP.1.1(1) (for the elements).
    - Assignment—allows the specification of an identified parameter. Assignments are indicated using bold text and are enclosed by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
    - Selection—allows the specification of one or more elements from a list. Selections are indicated using bold italics and are enclosed by brackets (e.g., [***selection***]).
    - Refinement—allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Other sections of the ST—other sections of the ST use bolding to highlight text of special interest, such as captions.

1.4 Glossary

This ST uses a number of terms that have a specific meaning within the context of the ST and the TOE. This glossary provides a list of those terms and how they are to be understood within this ST.

active list	A configurable data store that can hold information derived from events and other sources. Active lists can monitor activity based on any rule-driven combination of event attributes or set of custom fields.
analyzer	The function of an IDS that applies analytical processes to IDS data collected by sensors or scanners in order to derive conclusions about potential or actual intrusions. This is the functionality provided by ArcSight ESM.
assets	The computers, network infrastructure devices, etc. installed throughout the enterprise that ArcSight ESM monitors for vulnerability or attack. See also "IT system".
case	An ESM resource used to track, investigate, and resolve suspicious events in a workflow-type environment. When suspicious events occur, cases are created and assigned to users, who then investigate and resolve them based on enterprise policies and practices.
condition	A logical expression used to qualify events or other groupings of elements.
correlation	A process that identifies relationships between events, infers the significance of those relationships, prioritizes them, and provides a framework for taking action.
event	A record of security-sensitive activity occurring on a device in an IT system.
IDS	Intrusion Detection System—a combination of sensors, scanners, and analyzers that monitors an IT system for activity that may inappropriately affect the IT system or its resources, and that can react appropriately if such activity is detected.
IDS data	Refers both to raw data (i.e., events) forwarded to the TOE by scanners and sensors in its operational environment, and to the results of analysis applied by the TOE to that data.

IT system	A combination of computers, network infrastructure devices, cables, etc.
query	A resource that defines the parameters of the data to report on derived from a data source. Queries are used in reports either directly or as the basis for trends reporting.
rule	A programmed procedure that attempts to correlate events and generates new events that report on correlation when it occurs.
rule action	An automatic procedure that occurs when all rule conditions and threshold settings have been met.
scanner	A function of an IDS involving collection of static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT system.
sensor	A function of an IDS involving collection of real-time events that may be indicative of vulnerabilities in or misuse of IT system resources.
session list	Similar to active lists, session lists can monitor activity based on any rule-driven combination of event attributes or set of custom fields. They differ in some of their fields, in how they partition data, and how they handle time-based queries.
SIEM	Security Information and Event Management—combines security information management (SIM) and security event management (SEM) to provide real-time analysis of security alerts generated by network hardware and applications.
SmartConnectors	Collectors of security event information generated by multi-vendor security devices throughout the enterprise. SmartConnectors normalize and correlate this data into events, expressed as ArcSight Messages, which are forwarded to the TOE for further processing. SmartConnectors enable the TOE to receive events from sensors and scanners in its operational environment.
threshold	There are two types of thresholds: rule thresholds and event thresholds. A rule threshold is the point at which a rule is triggered and a correlation event generated. An event threshold is the number of times the event must occur before triggering the rule threshold.
trend	A resource that defines how and over what time period data will be aggregated and evaluated for trends. A trend executes a specified query on a defined schedule and time duration.

1.5 Abbreviations and Acronyms

The following abbreviations and acronyms are used throughout this ST:

ACC	ArcSight Command Center
API	Application Programming Interface
CC	Common Criteria
CSV	Comma-separated values
EAL	Evaluation Assurance Level
EPS	Events per second
ESM	Enterprise Security Management
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
IDS	Intrusion Detection System
IMAP	Internet Message Access Protocol—an Internet standard protocol used by e-mail clients to retrieve e-mail messages from a mail server over a TCP/IP connection

IT	Information Technology
LDAP	Lightweight Directory Access Protocol
POP3	Post Office Protocol version 3—an application-layer Internet standard protocol used by local e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection.
RADIUS	Remote Authentication Dial-In User Service—a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA or Triple A) management for users who connect and use a network service.
RAID	Redundant Array of Independent Disks—a data storage virtualization technology that combines multiple physical disk drive components into a single logical unit for the purposes of data redundancy, performance improvement, or both.
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SIEM	Security Information and Event Management
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOA	Service-Oriented Architecture
ST	Security Target
TCP/IP	Transmission Control Protocol/Internet Protocol—communications protocols used on the Internet and similar computer networks.
TOE	Target of Evaluation
TLS	Transport Layer Security
TSF	TOE Security Function

2. TOE Description

2.1 Overview

The TOE, ArcSight ESM Version 6.11.0, is a Security Information and Event Management (SIEM) product that normalizes and aggregates data from devices across the enterprise network, provides tools for analysis and investigation, and offers options for automatic and workflow-managed remediation. As such, ArcSight ESM provides a means to centrally manage all network events and activities in the enterprise. ArcSight ESM provides authorized users with capabilities to monitor events, correlate events for in-depth investigation and analysis, and resolve events with automated escalation procedures and actions.

ArcSight ESM is deployed in the enterprise network. It uses entities called ArcSight SmartConnectors to gather event data from the network. SmartConnectors translate event data from devices into a normalized schema that becomes the starting point for correlation. SmartConnectors are outside the TOE boundary.

2.2 Architecture

The TOE consists of the following components:

- ArcSight Manager
- CORR-Engine (Correlation Optimized Retention and Retrieval Engine)
- ArcSight Console
- ArcSight Command Center (ACC)
- ESM Service Layer APIs.

The ArcSight Manager, CORR-Engine, and ArcSight Command Center web server are installed on the same server. The ArcSight Manager processes and stores event data in the CORR-Engine. Users monitor events using ArcSight Console (a workstation-based application) or the ArcSight Command Center (a web-based interface), which can run reports, develop resources, and perform investigation and system administration. In addition, ESM Service Layer APIs expose ESM functionality as web services, enabling users to integrate ESM functionality into their own applications. The ArcSight components can communicate with each other using IPv4 or IPv6 in dual (IPv4/IPv6) and IPv6-only modes.

The primary means for authorized users to interact with the TOE is via the ArcSight Console or the ArcSight Command Center. In addition, the TOE provides various command scripts and utility programs, generically termed "ArcSight Commands" or "shell commands" (because they are executed from a command prompt or command shell on the underlying operating system). The shell commands are described in the guidance documentation and are categorized as follows:

- Allowed for use in the evaluated configuration
- Allowed only for installation/initial configuration
- Not allowed in the evaluated configuration.

The shell commands and their disposition are identified in the Common Criteria Evaluated Configuration Guide, while each command's method of use is fully described in the ESM Administrator's Guide.

The ArcSight Manager and ArcSight Console components also rely on properties files that are stored in the file system of the underlying operating system supporting that component. Each properties file is a text file containing pairs of keys and values. The keys determine which setting is configured and the value determines the configuration value. The TOE maintains two versions of each properties file—the default properties file (e.g., `server.default.properties`) and the equivalent user properties file (e.g., `server.properties`). The default properties files are provided with the TOE. The user properties files are created during initial configuration of the TOE using the appropriate setup wizard (the ArcSight Manager and ArcSight Console each has its own setup wizard that is automatically launched as part of the installation and configuration process). Settings in the user properties file override settings in the default properties file. The component first reads in the values in the default properties file,

and then reads in the user properties file and updates any settings that have different values. Each component performs bounds and sanity checks on the configuration values before applying them to its configuration.

The TOE can be configured in either of two modes: non-FIPS mode (the default mode); and FIPS 140-2 compliant mode. The configured mode determines the cryptographic protocols and the underlying cryptographic provider the TOE uses to implement secure communications. In non-FIPS mode, the TOE supports secure communications using TLS v1.0 (the default), TLS v1.1, or TLS v1.2. In this mode, the TOE uses SunJCE and Bouncy Castle as the cryptographic providers—SunJCE is used for TLS and most other cryptographic needs, while Bouncy Castle is used for certificate generation in the TOE's setup wizard. The TOE uses X.509 Version 3 certificates. The default key size for the public key in the certificate is 2048 bits.

In FIPS 140-2 mode, the TOE uses the Bouncy Castle Java cryptographic module, version BouncyCastle-fips v1.0. Communications are protected using TLS v1.0, TLS v1.1 or TLS v1.2. While it is recommended that the TOE operate in FIPS 140-2 mode, this is not required for the evaluated configuration.

The following figure illustrates how the TOE components can be deployed in a network.

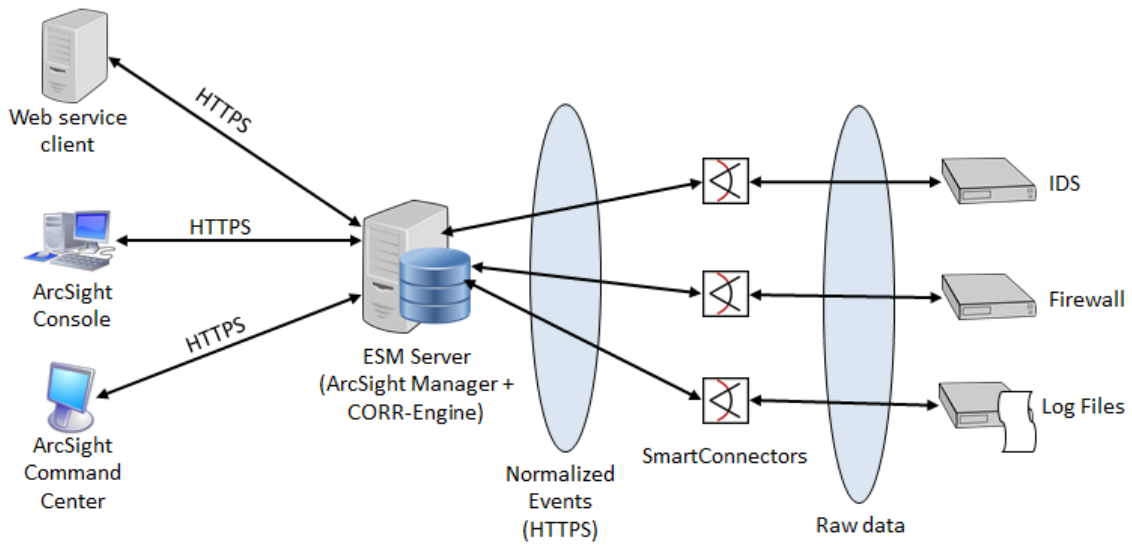

Figure 1: Example TOE Deployment

2.2.1 ArcSight Manager

ArcSight Manager is a high performance engine that manages, correlates, filters, and processes all occurrences of security events collected from the IT System. The ArcSight Manager sits at the center of ESM and acts as a link between the ArcSight Console, ACC, CORR-Engine, and ArcSight SmartConnectors. The ArcSight Manager relies on the underlying operating system to provide a file system to store configuration files and error logs. The ArcSight Manager requires the underlying operating system to also protect the file system. The underlying operating system and its file system are considered part of the operational environment of ArcSight Manager.

An ArcSight Manager can establish a peer relationship with one or more other Managers to enable distributed searches and Content Management. ArcSight Managers can send content to, or receive content from, other Managers when they are in a peer relationship. When two Managers peer with each other, one initiates the relationship. The initiator sends credentials to authenticate itself to the target system. If the authentication succeeds, a peer relationship is established between the two Managers.

The ArcSight Manager can be configured for High Availability (HA), using the ESM HA Module. This provides for a backup ESM machine with automatic failover capability should the primary ESM machine experience any communication or operational problems. The HA Module is installed on the primary of two adjacent machines connected by an Ethernet crossover cable. The HA Module replicates the installation and all data by mirroring the hard disk partition to the secondary machine.

For the ArcSight Manager to send notification messages via e-mail, the outgoing mail server (part of the environment) must be accessible from the ArcSight Manager. ArcSight Manager uses Simple Mail Transfer Protocol (SMTP) to send e-mail.

2.2.2 CORR-Engine

The CORR-Engine is the logical access mechanism, particular schema, and table spaces that stores all captured events, and saves all security management configuration information, such as system users, groups, permissions, defined rules, zones, assets, report templates, displays, and preferences. The CORR-Engine stores data in data files on the file system available to the operating system where ArcSight Manager is also installed. The ArcSight Manager is the only component that communicates directly with the CORR-Engine.

2.2.3 ArcSight Console

The ArcSight Console is a workstation-based interface to ArcSight Manager that provides real-time monitoring, in-depth investigative capabilities, and automated responses and resolutions to events. The ArcSight Console provides authorized users with a graphical user interface (GUI) to perform security management functions, including management of TOE resources, management of the TOE's analysis and reaction functions, viewing audit data and analysis results, and user management.

The ArcSight Console connects to a single ArcSight Manager at a time via the network. The ArcSight Console requires the underlying operating system to provide protection for the TOE. The underlying operating system is considered part of the environment.

2.2.4 ArcSight Command Center

The ArcSight Command Center is a web-based user interface that provides a streamlined interface for: managing storage, and event data; monitoring events and running reports; and configuring storage, updating licenses, managing component authentication, and setting up storage notifications. With content management, an authorized user can establish peer relationships with other ESM installations, and search and synchronize ESM content across peers.

2.2.5 Service Layer APIs

The Service Layer APIs use a service-oriented architecture (SOA) that supports multiple web service clients written in different languages. They provide developers the ability to:

- Run an ESM report and feed it back to a third-party system
- Create and update cases
- Manage resource groups.

2.3 Physical Boundaries

2.3.1 Physical TOE Components

ArcSight ESM is a software product provided in the following form:

- `ArcSightESMSuite-6.11.0.2149.0.tar` file, the software distribution and installation file for the ArcSight Manager, CORR-Engine, ArcSight Command Center and Service Layer API components
- `ArcSight-6.11.0.2339.0-Console-Win.Exe`, a self-extracting archive file and installer for the ArcSight Console on Windows
- `ArcSight-6.11.0.2339.0-Console-Linux.bin`, a self-extracting archive file and installer for the ArcSight Console on Linux.

2.3.2 Operational Environment Components

The ArcSight ESM suite (`ArcSightESMSuite-6.11.0.2149.0.tar`) can be installed on 64-bit Red Hat Enterprise Linux (RHEL) 6.8 or 7.3 and CentOS 6.8 or 7.3. The following browsers are supported for accessing the ArcSight Command Center:

- Internet Explorer 11 on Windows
- Safari 10.x on Mac OS X
- Firefox 45.7 ESR on Linux, Windows and Mac OS X
- Chrome (latest version) on Windows.

The ArcSight Console for Windows (`ArcSight-6.11.0.2339.0-Console-Win.Exe`) is supported on the following platforms in the evaluated configuration: Windows Server 2012 R2, 64-bit; Windows 7, 8.1, and 10, 64-bit.

The ArcSight Console for Linux (`ArcSight-6.11.0.2339.0-Console-Linux.bin`) is supported on the following platform in the evaluated configuration: RHEL Workstation/CentOS 6.8, 64-bit; RHEL Workstation/ CentOS 7.3, 64-bit.

The following table outlines the recommended hardware requirements for ESM.

	Minimum	**Mid-Range**	**High Performance**
Processors	8 cores (16 preferred)	32 cores	40 cores
Memory	48 GB RAM (64 preferred)	192 GB RAM	512 GB RAM
Hard Disk	Six 600 GB disks (1.5 TB) (RAID 10) 15,000 RPM	20 1TB disks (10 TB) (RAID 10) 10,000 RPM	12 TB (RAID 10) Solid state

Table 1: Recommended Hardware Requirements

Note: The "Minimum" values apply to systems running base system content at low Events per Second (EPS) (typical in lab environments). It should not be used for systems running a high number of customer-created resources, or for systems that need to handle high event rates. Use the "Mid-Range" or "High Performance" specifications for production environments that handle a sizable EPS load with additional content and user activity.

In addition to the hardware and software platforms identified above, the TOE requires the following in its operational environment:

- SmartConnectors—collect raw IDS data generated by multi-vendor security devices throughout the IT system being monitored. SmartConnectors normalize and correlate this data into events that are forwarded to the TOE for further processing. SmartConnectors enable the TOE to receive events from sensors and scanners in its operational environment.
- SMTP Server—supports e-mail notifications. POP3 and IMAP can be used to check for e-mail acknowledgments. SMTP servers can be configured to use Transport Layer Security (TLS).

2.3.3 Excluded Components

The following ESM components are outside the evaluated configuration since they are not considered part of the core product and/or require a separate license to activate. Licensing, installing, or enabling these components, which have not been subject to evaluation and are not part of the evaluated configuration of the TOE, will render the TOE out of its evaluated configuration.

- Pattern Discovery
- ArcSight Express appliance
- ESM Express appliance

2.4 Logical Boundaries

This section summarizes the security functions provided by the TOE.

2.4.1 Security Audit

The ArcSight Manager is able to generate audit records of security-relevant events, which it stores in CORR-Engine. The stored audit records are protected by CORR-Engine from unauthorized modification and deletion. The TOE provides Administrators and Analyst Administrators with capabilities to review the generated audit records, including capabilities for sorting audit records based on such characteristics as date and time the event is recorded, the type of audit event, the subject associated with the audit event, and the outcome of the event.

2.4.2 Identification & Authentication

The TOE maintains accounts of the authorized users of the system. The user account includes the following attributes associated with the user: user identity; authentication data; authorizations (groups or roles); and e-mail address information. This information is stored in CORR-Engine. The TOE supports both passwords and certificates for authentication and users can be configured for password-only, certificate-only, password or certificate, and password and certificate. The TOE enforces restrictions on password structure, including minimum length and minimum number of different character types (i.e., alphabetic, numeric, special).

By default, the TOE allows a maximum three consecutive failed login attempts, after which the user account is locked for 10 minutes. The TOE requires users to provide unique identification and authentication data before any access to the TOE via the ArcSight Console or the ArcSight Command Center is granted. Users have the ability to terminate their own interactive sessions by logging out of the ArcSight Console or ArcSight Command Center. Users that have been identified and authenticated by the underlying operating system are able to execute a limited set of shell commands for ArcSight Manager and ArcSight Console, although some of these commands also require entry of a user identity and matching password.

2.4.3 Security Management

The TOE provides the following default security management roles: Administrator; Analyzer Administrator; Operator; and Analyst. The TOE enforces restrictions on which management capabilities are available to each role. Administrators and Analyzer Administrators are able to modify the behavior of the IDS analysis and reaction function. Only the Administrator role is able to manage user accounts and to modify passwords of other users. The TOE's security management functions are accessible via the ArcSight Console and ArcSight Command Center.

2.4.4 Protection of the TSF

The TOE uses HTTPS to protect TSF data communicated between the ArcSight Console and the ArcSight Manager components of the TOE.

2.4.5 Trusted Path/Channels

The TOE provides a trusted channel between itself and the following external IT entities that protects transmitted information from disclosure and modification:

- Web service clients—connect to the TOE via the TOE's Service Layer APIs. All such connections are made over HTTPS.
- SmartConnectors—SmartConnectors establish HTTPS connections with the TOE to forward events to the TOE.

The TOE provides a trusted path for TOE administrators to communicate with the TOE. The trusted path is implemented using HTTPS for access to the ArcSight Command Center.

Administrators initiate the trusted path by establishing an HTTPS connection (using a supported web browser). The trusted path is used for initial authentication and all subsequent administrative actions. The use of HTTPS ensures all communication over the trusted path is protected from disclosure and modification.

2.4.6 Intrusion Detection System

The TOE collects information from network sources and subjects it to statistical and signature-based analysis, depending on configured rules. Rules trigger responses either on first match or after a given threshold has been passed. Notification destinations (e.g., authorized users) can be configured to be notified of a triggered rule at the GUI (ArcSight Console or ArcSight Command Center) or via e-mail. The authorized users can view all event information from the IDS data. To prevent IDS data loss, a warning is sent to a configured e-mail destination should CORR-Engine begin to run out of storage space for IDS data. The default setting for generating this notification is 90% of capacity. If no action is taken to address the warning, an error is sent if IDS storage exceeds the configured error threshold (95% by default).

2.5 Capabilities Provided by the Operational Environment

The TOE relies on the operational environment for the following components and capabilities:

- The underlying operating system of each TOE component is relied on to protect the component and its configuration from unauthorized access.
- The underlying operating system of each TOE component is relied on to provide a reliable date and time stamp for use by the TOE.
- The SmartConnectors in the operational environment are relied on to collect raw IDS data from sensors and scanners and to forward it to the TOE for analysis.

2.6 Capabilities Excluded from the Scope of Evaluation

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 ArcSight Managers
- 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.

2.7 TOE Documentation

This section identifies the guidance documentation included in the TOE. The documentation comprises:

- HPE Security ArcSight ESM—ESM Installation Guide, Software Version 6.11.0, April 14, 2017
- HP ArcSight ESM—Administrator's Guide, Software Version 6.11.0, March 21, 2017
- HP ArcSight ESM—ESM 101, Software Version 6.11.0, April 4, 2107
- HP ArcSight ESM—ArcSight Console User's Guide, Software Version 6.11.0, March 30, 2017
- HP ArcSight ESM Command Center—User's Guide, Software Version 6.11.0, March 29, 2017
- Common Criteria Evaluated Configuration Guide – ArcSight ESM 6.11.0, Version 1.0, June 9, 2017
- HP ArcSight ESM: Service Layer (Web Services) Developer's Guide, Software Version 6.11.0, December 5, 2016
- HPE Security ArcSight ESM - API Reference Vol. 1: Core-Client Services (1.2), Software Version: 6.11.0 March 1, 2017
- HPE Security ArcSight ESM-API Reference Vol. 2: Manager-Client Services (1.1), Software Version 6.11.0, March 1, 2017
- HPE ArcSight ESM Support Matrix, March 22, 2017

- HPE Security ArcSight ESM – Upgrade Guide, April 14, 2017

3. Security Problem Definition

This section defines the security problem to be addressed by the TOE, in terms of threats to be countered by the TOE or its operational environment, and assumptions about the intended operational environment of the TOE.

3.1 Assumptions

This section contains assumptions regarding the operational environment and the intended usage of the TOE.

A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.PLATFORM	The underlying operating system of each TOE component will protect the component and its configuration from unauthorized access.
A.PROTECT	The TOE software critical to security policy enforcement will be protected from unauthorized physical modification.

3.2 Threats

This section identifies and describes the threats to be countered by the TOE and its operational environment.

T.BRUTE_FORCE	An unauthorized user may gain access to the TOE through repeated password-guessing attempts.
T.INTEGRITY_COMPROMISE	An unauthorized user may attempt to modify or destroy audit or IDS data, thus removing evidence of unauthorized or malicious activity.
T.NETWORK_COMPROMISE	TSF data communicated between components of the TOE, or between the TOE and external entities, is disclosed or modified.
T.NO_ACCOUNTABILITY	Authorized users of the TOE perform adverse actions on the TOE, or attempt to perform unauthorized actions, which go undetected.
T.UNAUTHORIZED_ACCESS	An unauthorized user may gain access to the TOE security functions and data.
T.UNAUTHORIZED_ACTIVITY	Authorized users perform unauthorized actions on the TOE.
T.UNDETECTED_THREATS	Events generated by entities in the IT system indicative of misuse or unauthorized or malicious activity go undetected.

4. Security Objectives

This section identifies the security objectives for the TOE and its operational environment. The security objectives identify the responsibilities of the TOE and its environment in addressing the security problem defined in Section 3.

4.1 Security Objectives for the TOE

The following are the TOE security objectives:

O.ANALYZER	The TOE shall analyze collected IDS data in order to identify misuse and unauthorized or malicious activity and shall be able to record the results of its analysis.
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.I_AND_A	The TOE shall provide a means for users to be identified and authenticated before gaining access to TOE services.
O.PASSWORD_CONTROLS	The TOE shall provide a mechanism to reduce the likelihood that users choose weak passwords.
O.PROTECTED _COMMS	The TOE shall protect communications between distributed parts of the TOE, and between the TOE and external entities, from disclosure and modification.
O.RESPONSE	The TOE shall respond to misuse and unauthorized or malicious activity it identifies based on its configuration.
O.REVIEW	The TOE shall provide capabilities for effective review of stored IDS data.
O.SECURITY_MANAGEMENT	The TOE shall restrict the ability to perform security management functions on the TOE to authorized administrators having appropriate privileges.
O.STORAGE	The TOE shall protect stored audit records and IDS data from unauthorized modification or deletion.
O.THROTTLE	The TOE shall limit the rate at which consecutive unsuccessful authentication attempts can be performed.

4.2 Security Objectives for the Operational Environment

The following are the security objectives for the operational environment of the TOE.

OE.PERSONNEL	Those responsible for the TOE must ensure that personnel working as authorized administrators have been carefully selected and trained for proper operation of the TOE.
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
OE.PLATFORM	The underlying operating system of each TOE component will protect the component and its configuration from unauthorized access.
OE.SENSORS	The operational environment of the TOE has the capability to collect IDS data from the IT system the TOE is monitoring and to provide that IDS data to the TOE in a form suitable for the TOE to analyze.
OE.TIME	The underlying operating system of the TOE provides a reliable time source for use by the TOE.

5. IT Security Requirements

5.1 Extended Components Definition

5.1.1 Intrusion Detection System (IDS)

This ST defines a new functional class for use within this ST: Intrusion Detection System (IDS). This family of IDS requirements was created to specifically address the data collected and analyzed by an IDS. The audit family of the CC (FAU) was used as a model for creating these requirements. The purpose of this family of requirements is to address the unique nature of IDS data and specify requirements for collecting, analyzing and reviewing IDS data.

5.1.1.1 IDS Data Collection (IDS_SDC)

This family defines requirements for being able to collect IDS data from targeted IT resources. It specifies requirements for both a Sensor capability and a Scanner capability.

Management: IDS_SDC.1

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

a) maintenance of the parameters that control IDS data collection.

Audit: IDS_SDC.1

There are no auditable events foreseen.

IDS_SDC.1 – IDS data collection

Hierarchical to: No other components.

Dependencies: None

IDS_SDC.1.1 The TSF shall be able to collect the following information from targeted IT System resource(s):

a) **[selection: Start-up and shutdown, identification and authentication events, data accesses, service requests, network traffic, security configuration changes, data introduction, detected malicious code, access control configuration, service configuration, authentication configuration, accountability policy configuration, detected known vulnerabilities]**; and

b) **[assignment: *other specifically defined events*]**.

Application Note: *The ST will define the IDS capabilities of the TOE. This requirement indicates that the TOE must support at least a Sensor capability or a Scanner capability, by requiring the TOE be able to collect information pertaining to at least one of the selections in bullet a above. A Sensor would generally collect information pertaining to the following events in bullet a: start-up and shutdown, identification and authentication events, data accesses, service requests, network traffic, security configuration changes, and data introduction. The Scanner would generally collect static configuration information which include the following events in bullet a: detected malicious code, access control configuration, service configuration, authentication configuration, accountability policy configuration, and detected known vulnerabilities. Malicious code includes viruses, worms, simple Trojan horses, etc. Access control configuration includes access control lists, search for writeable files and directories, etc. Service configuration includes identification of network services and/or associated network ports, host services, versions of services, protocols acknowledged by services, etc. Authentication configuration includes cracking passwords, configuration settings (e.g., minimum password length, duration between allowed and required password changes), acceptable authentication means (e.g., NTLM, kerberos), defined guest accounts, account authorisations, etc. Accountability policy configuration includes size of audit trails, whether audit is enabled, what to do when the audit trail fills, etc. Known vulnerabilities is fairly open ended, but may include installed patches, checks for common or default configuration errors, etc.*

IDS_SDC.1.2 At a minimum, the TSF shall collect and record the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) The additional information specified in the *Details* column of the following table.

Event	Details
Start-up and shutdown	None
Identification and authentication events	User identity, location, source address, destination address
Data accesses	Object identifier, requested access, source address, destination address
Service requests	Specific service, source address, destination address
Network traffic	Protocol, source address, destination address
Security configuration changes	Source address, destination address
Data introduction	Object identifier, location of object, source address, destination address
Detected malicious code	Location, identification of code
Access control configuration	Location, access settings
Service configuration	Service identification (name or port), interface, protocols
Authentication configuration	Account names for cracked passwords, account policy parameters
Accountability policy configuration	Accountability policy configuration parameters
Detected known vulnerabilities	Identification of the known vulnerability

Application Note: *In the case where a Sensor is collecting host-based events, for the identification and authentication event, the source address could be a subject IDS on a local machine and the destination is defined by default. For the data access and data introduction events, the source address could be filename and the destination address may be target location for the file.*

5.1.1.2 IDS Analyzer (IDS_ANL)

This family defines requirements for being able to analyze collected IDS data.

Management: IDS_ANL.1

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

a) maintenance of the parameters that control IDS data analysis.

Audit: IDS_ANL.1

There are no auditable events foreseen.

IDS_ANL.1 – Analyzer analysis

Hierarchical to: No other components.

Dependencies: IDS_SDC.1, FPT_STM.1

IDS_ANL.1.1 The TSF shall perform the following analysis function(s) on all IDS data received:

a) **[selection: statistical, signature, integrity]**; and

b) **[assignment: *other analytical functions*]**.

Application Note: *Statistical analysis involves identifying deviations from normal patterns of behavior. For example, it may involve mean frequencies and measures of variability to identify abnormal usage. Signature analysis involves the use of patterns corresponding to known attacks or misuses of a System. For example, patterns of System settings and user activity can be compared against a database of known attacks. Integrity analysis involves comparing System settings or user activity at some point in time with those of another point in time to detect differences.*

IDS_ANL.1.2 The TSF shall record within each analytical result at least the following information:

a) Date and time of the result, type of result, identification of data source; and

b) **[assignment: *other security relevant information about the result*]**.

Application Note: *The analytical conclusions drawn by the analyser should both describe the conclusion and identify the information used to reach the conclusion.*

5.1.1.3 Intrusion Reaction (IDS_RCT)

This family defines requirements for being able to react to the results of IDS data analysis.

Management: IDS_RCT.1

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

b) maintenance of the parameters that control IDS reaction.

Audit: IDS_RCT.1

There are no auditable events foreseen.

IDS_RCT.1 – Analyzer reaction

Hierarchical to: No other components.

Dependencies: IDS_ANL.1

IDS_RCT.1.1 The TSF shall send an alarm to **[assignment: *alarm destination*]** and take **[assignment: *appropriate actions*]** when an intrusion is detected.

Application Note: *There must be an alarm, though the ST should refine the nature of the alarm and define its target (e.g., administrator console, audit log). The Analyzer function may optionally perform other actions when intrusions are detected; these actions should be defined in the ST. An intrusion in this requirement applies to any conclusions reached by the Analyzer function related to past, present, and future intrusions or intrusion potential.*

5.1.1.4 IDS Data Review (IDS_RDR)

This family defines requirements for reviewing IDS data and restricting access to IDS data.

Management: IDS_RDR.1

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

c) maintenance of the group of users with read access rights to the IDS data.

Audit: IDS_RDR.1

There are no auditable events foreseen.

IDS_RDR.1 – Restricted data review

Hierarchical to: No other components.

Dependencies: IDS_SDC.1, IDS_ANL.1

IDS_RDR.1.1 The TSF shall provide **[assignment: *authorized users*]** with the capability to read **[assignment: *list of IDS data*]** from the IDS data.

IDS_RDR.1.2 The TSF shall provide the IDS data in a manner suitable for the user to interpret the information.

IDS_RDR.1.3 The TSF shall prohibit all users read access to the IDS data, except those users that have been granted explicit read access.

Application Note: *This requirement applies to authorized users of the TOE. The requirement is left open for the writers of the ST to define which authorized users may access what IDS data.*

5.1.1.5 IDS Data Storage (IDS_STG)

This family defines requirements for securely storing IDS data.

Management: IDS_STG.1, IDS_STG.2

There are no management actions foreseen.

Audit: IDS_STG.1, IDS_STG.2

There are no auditable events foreseen.

IDS_STG.1 – Guarantee of IDS data availability

Hierarchical to: No other components.

Dependencies: IDS_SDC.1, IDS_ANL.1

IDS_STG.1.1 The TSF shall protect the stored IDS data from unauthorized deletion.

IDS_STG.1.2 The TSF shall protect the stored IDS data from modification.

Application Note: *Authorized deletion of data is not considered a modification of IDS data in this context. This requirement applies to the actual content of the IDS data, which should be protected from any modifications.*

IDS_ STG.1.3 The TSF shall ensure that **[assignment: *metric for saving IDS data*]** IDS data will be maintained when the following conditions occur: **[selection: IDS data storage exhaustion, failure, attack]**.

Application Note: *The ST needs to define the amount of IDS data that could be lost under the identified scenarios.*

IDS_STG.2 – Action in case of possible IDS data loss

Hierarchical to: No other components.

Dependencies: IDS_STG.1

IDS_STG.2.1 The TSF shall **[assignment: *actions to be taken in case of possible IDS storage failure*]** if the IDS storage exceeds **[assignment: *pre-defined limit*]**.

Application Note: *The ST must define a pre-defined limit of IDS storage capacity and the actions the TOE takes when that limit is reached.*

5.2 TOE Security Functional Requirements

This section specifies the security functional requirements (SFRs) for the TOE. SFRs were drawn from Part 2 of the Common Criteria v3.1 Revision 4, and from the extended components defined in Section 5.1 above.

Requirement Class	Requirement Component
FAU: 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 trail storage
FIA: 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

Requirement Class	Requirement Component
FMT: Security Management	FMT_MOF.1: Management of security function behaviour
	FMT_MTD.1(*): Management of TSF data
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security roles
FPT: Protection of the TSF	FPT_ITT.1: Basic internal TSF data transfer protection
FTA: TOE Access	FTA_SSL.4: User-initiated termination
FTP: Trusted Path/Channels	FTP_ITC.1: Inter-TSF trusted channel
	FTP_TRP.1: Trusted path
IDS: Intrusion Detection System	IDS_ANL.1: Analyzer analysis
	IDS_RCT.1: Analyzer reaction
	IDS_RDR.1: Restricted data review
	IDS_STG.1: Guarantee of IDS data availability
	IDS_STG.2(*): Action in case of possible IDS data loss

Table 2: TOE Security Functional Components

5.2.1 Security Audit (FAU)

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) [**the following auditable events:**

- **Reading of information from the audit records**
- **Unsuccessful attempts to read information from the audit records**
- **All use of the authentication mechanism**
- **All use of the user identification mechanism**
- **The reaching of the threshold for unsuccessful authentication attempts and the actions taken by the TOE, including restoration to the normal state (i.e., re-enabling the user account).**
- **All modifications in the behavior of the functions of the TSF**
- **All modifications to the values of TSF data**
- **Use of the management functions**
- **Modifications to the group of users that are part of a role**
- **Termination of an interactive session by the user**].

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, 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, [**none**].

FAU_SAR.1 – Audit review

FAU_SAR.1.1 The TSF shall provide [**Administrator, Analyzer Administrator**] with the capability to read [**all audit information**] 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.

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.

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**].

FAU_STG.1 – Protected audit trail storage

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

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

5.2.2 Identification and Authentication (FIA)

FIA_AFL.1 – Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when [***an administrator configurable positive integer within [1..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, depending on configuration**].

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**
- **E-mail address**].

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**
- **Number of alphabetic characters**
- **Number of numeric characters**
- **Number of special characters**].

FIA_UAU.1 – Timing of authentication

FIA_UAU.1.1 The TSF shall allow [**actions where the operational environment has authenticated the user**] 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.

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 rules:**

- **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**].

FIA_UID.1 – Timing of identification

FIA_UID.1.1 The TSF shall allow [**actions where the operational environment has identified the user**] 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.

Application Note: The TOE provides command scripts and utility programs that can be used to support management of the TOE and that are executed from a command prompt or command shell on the underlying operating system. Except where otherwise excluded from the evaluated configuration, these commands can be executed by a user that has access to the underlying operating system, has been successfully identified and authenticated by the underlying operating system, and has appropriate permissions to the operating system file system locations from which the commands are executed.

5.2.3 Security Management (FMT)

FMT_MOF.1 – Management of security function behaviour

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**].

FMT_MTD.1(1) – Management of TSF data (user accounts)

FMT_MTD.1.1(1) The TSF shall restrict the ability to [***modify, delete, [create]***] the [**user accounts**] to [**Administrator**].

FMT_MTD.1(2) – Management of TSF data (password of another user)

FMT_MTD.1.1(2) The TSF shall restrict the ability to [***modify***] the [**password of another user**] to [**Administrator**].

FMT_SMF.1 – Specification of Management Functions

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

- **Manage IDS analysis and reaction**
- **Manage user accounts**
- **Modify user passwords**].

FMT_SMR.1 – Security roles

FMT_SMR.1.1 The TSF shall maintain the roles: [

- **Administrator**
- **Analyzer Administrator**
- **Operator**
- **Analyst**].

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

5.2.4 Protection of the TSF (FPT)

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.

5.2.5 TOE Access (FTA)

FTA_SSL.4 – User-initiated termination

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

5.2.6 Trusted Path/Channels (FTP)

FTP_ITC.1 – Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication path 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 [***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 [**no functions**].

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***, ***[undetected 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]***].

5.2.7 Intrusion Detection System (IDS)

IDS_ANL.1 – Analyzer analysis

IDS_ANL.1.1 The TSF shall perform the following analysis function(s) on all IDS data received:

a) [***statistical, signature***]; and

b) [**no other analytical functions**].

IDS_ANL.1.2 The TSF shall record within each analytical result at least the following information:

a) Date and time of the result, type of result, identification of data source; and

b) [**no other security relevant information about the result**].

IDS_RCT.1 – Analyzer reaction

IDS_RCT.1.1 The TSF shall send an alarm to [**ESM Manager and to any monitoring ArcSight Console session or e-mail address**] and take [**action specified by the rule that was triggered by the event**] when an intrusion is detected.

IDS_RDR.1 – Restricted data review

IDS_RDR.1.1 The TSF shall provide [**Administrator, Analyzer Administrator, Operator, Analyst**] with the capability to read [**all event information**] from the IDS data.

IDS_RDR.1.2 The TSF shall provide the IDS data in a manner suitable for the user to interpret the information.

IDS_RDR.1.3 The TSF shall prohibit all users read access to the IDS data, except those users that have been granted explicit read-access.

IDS_STG.1 – Guarantee of IDS data availability

IDS_STG.1.1 The TSF shall protect the stored IDS data from unauthorized deletion.

IDS_STG.1.2 The TSF shall protect the stored IDS data from modification.

IDS_STG.1.3 The TSF shall ensure that [**the most recent, limited by available event storage**] IDS data will be maintained when the following conditions occur: [***IDS data storage exhaustion***].

IDS_STG.2(1) – Action in case of possible IDS data loss (warning threshold)

IDS_STG.2.1(1) The TSF shall **[send a warning to a configured e-mail address]** if the IDS storage exceeds **[the configured warning threshold (default 90%)]**.

IDS_STG.2(2) – Action in case of possible IDS data loss (error threshold)

IDS_STG.2.1(2) The TSF shall **[send an error to a configured e-mail address]** if the IDS storage exceeds **[the configured error threshold (default 95%)]**.

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL 2 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

Requirement Class	Requirement Component
ADV: Development	ADV_ARC.1: Security architecture description
	ADV_FSP.2: Security-enforcing functional specification
	ADV_TDS.1: Basic design
AGD: Guidance documents	AGD_OPE.1: Operational user guidance
	AGD_PRE.1: Preparative procedures
ALC: Life-cycle support	ALC_CMC.2: Use of a CM system
	ALC_CMS.2: Parts of the TOE CM coverage
	ALC_DEL.1: Delivery procedures
ASE: Security Target evaluation	ASE_CCL.1: Conformance claims
	ASE_ECD.1: Extended components definition
	ASE_INT.1: ST introduction
	ASE_OBJ.2: Security objectives
	ASE_REQ.2: Derived security requirements
	ASE_SPD.1: Security problem definition
	ASE_TSS.1: TOE summary specification
ATE: Tests	ATE_COV.1: Evidence of coverage
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing – sample
AVA: Vulnerability assessment	AVA_VAN.2: Vulnerability analysis

Table 3: TOE Security Assurance Components

5.3.1 Development (ADV)

ADV_ARC.1 – Security architecture description

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

ADV_ARC.1.1C	The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.
ADV_ARC.1.2C	The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.
ADV_ARC.1.3C	The security architecture description shall describe how the TSF initialisation process is secure.
ADV_ARC.1.4C	The security architecture description shall demonstrate that the TSF protects itself from tampering.
ADV_ARC.1.5C	The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.
ADV_ARC.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.2 – Security-enforcing functional specification

ADV_FSP.2.1D	The developer shall provide a functional specification.
ADV_FSP.2.2D	The developer shall provide a tracing from the functional specification to the SFRs.
ADV_FSP.2.1C	The functional specification shall completely represent the TSF.
ADV_FSP.2.2C	The functional specification shall describe the purpose and method of use for all TSFI.
ADV_FSP.2.3C	The functional specification shall identify and describe all parameters associated with each TSFI.
ADV_FSP.2.4C	For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.
ADV_FSP.2.5C	For each SFR-enforcing TSFI, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions.
ADV_FSP.2.6C	The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.
ADV_FSP.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_FSP.2.2E	The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

ADV_TDS.1 – Basic design

ADV_TDS.1.1D	The developer shall provide the design of the TOE.
ADV_TDS.1.2D	The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.
ADV_TDS.1.1C	The design shall describe the structure of the TOE in terms of subsystems.
ADV_TDS.1.2C	The design shall identify all subsystems of the TSF.
ADV_TDS.1.3C	The design shall describe the behavior of each SFR-supporting or SFR non-interfering TSF subsystem in sufficient detail to determine that it is not SFR-enforcing.
ADV_TDS.1.4C	The design shall summarise the SFR-enforcing behavior of the SFR-enforcing subsystems.
ADV_TDS.1.5C	The design shall provide a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.
ADV_TDS.1.6C	The mapping shall demonstrate that all TSFIs trace to the behavior described in the TOE design that they invoke.
ADV_TDS.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_TDS.1.2E	The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

5.3.2 Guidance Documents (AGD)

AGD_OPE.1 – Operational user guidance

AGD_OPE.1.1D	The developer shall provide operational user guidance.
AGD_OPE.1.1C	The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.
AGD_OPE.1.2C	The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.
AGD_OPE.1.3C	The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.
AGD_OPE.1.4C	The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
AGD_OPE.1.5C	The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.
AGD_OPE.1.6C	The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.
AGD_OPE.1.7C	The operational user guidance shall be clear and reasonable.
AGD_OPE.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1 – Preparative procedures

AGD_PRE.1.1D	The developer shall provide the TOE including its preparative procedures.
AGD_PRE.1.1C	The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.
AGD_PRE.1.2C	The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.
AGD_PRE.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AGD_PRE.1.2E	The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.3.3 Life-cycle Support (ALC)

ALC_CMC.2 – Use of a CM system

ALC_CMC.2.1D	The developer shall provide the TOE and a reference for the TOE.
ALC_CMC.2.2D	The developer shall provide the CM documentation.
ALC_CMC.2.3D	The developer shall use a CM system.
ALC_CMC.2.1C	The TOE shall be labelled with its unique reference.
ALC_CMC.2.2C	The CM documentation shall describe the method used to uniquely identify the configuration items.
ALC_CMC.2.3C	The CM system shall uniquely identify all configuration items.
ALC_CMC.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_CMS.2 – Parts of the TOE CM coverage	
ALC_CMS.2.1D	The developer shall provide a configuration list for the TOE.
ALC_CMS.2.1C	The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE.
ALC_CMS.2.2C	The configuration list shall uniquely identify the configuration items.
ALC_CMS.2.3C	For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.
ALC_CMS.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DEL.1 – Delivery procedures	
ALC_DEL.1.1D	The developer shall document and provide procedures for delivery of the TOE or parts of it to the consumer.
ALC_DEL.1.2D	The developer shall use the delivery procedures.
ALC_DEL.1.1C	The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.
ALC_DEL.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4 Security Target Evaluation (ASE)

ASE_CCL.1 – Conformance claims	
ASE_CCL.1.1D	The developer shall provide a conformance claim.
ASE_CCL.1.2D	The developer shall provide a conformance claim rationale.
ASE_CCL.1.1C	The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.
ASE_CCL.1.2C	The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.
ASE_CCL.1.3C	The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.
ASE_CCL.1.4C	The CC conformance claim shall be consistent with the extended components definition.
ASE_CCL.1.5C	The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.
ASE_CCL.1.6C	The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.
ASE_CCL.1.7C	The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.
ASE_CCL.1.8C	The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.
ASE_CCL.1.9C	The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.
ASE_CCL.1.10C	The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.
ASE_CCL.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_ECD.1 – Extended components definition

ASE_ECD.1.1D	The developer shall provide a statement of security requirements.
ASE_ECD.1.2D	The developer shall provide an extended components definition.
ASE_ECD.1.1C	The statement of security requirements shall identify all extended security requirements.
ASE_ECD.1.2C	The extended components definition shall define an extended component for each extended security requirement.
ASE_ECD.1.3C	The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.
ASE_ECD.1.4C	The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.
ASE_ECD.1.5C	The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.
ASE_ECD.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ASE_ECD.1.2E	The evaluator shall confirm that no extended component can be clearly expressed using existing components.

ASE_INT.1 – ST introduction

ASE_INT.1.1D	The developer shall provide an ST introduction.
ASE_INT.1.1C	The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.
ASE_INT.1.2C	The ST reference shall uniquely identify the ST.
ASE_INT.1.3C	The TOE reference shall identify the TOE.
ASE_INT.1.4C	The TOE overview shall summarise the usage and major security features of the TOE.
ASE_INT.1.5C	The TOE overview shall identify the TOE type.
ASE_INT.1.6C	The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.
ASE_INT.1.7C	The TOE description shall describe the physical scope of the TOE.
ASE_INT.1.8C	The TOE description shall describe the logical scope of the TOE.
ASE_INT.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ASE_INT.1.2E	The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

ASE_OBJ.2 – Security objectives

ASE_OBJ.2.1D	The developer shall provide a statement of security objectives.
ASE_OBJ.2.2D	The developer shall provide a security objectives rationale.
ASE_OBJ.2.1C	The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.
ASE_OBJ.2.2C	The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.
ASE_OBJ.2.3C	The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.
ASE_OBJ.2.4C	The security objectives rationale shall demonstrate that the security objectives counter all threats.
ASE_OBJ.2.5C	The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.
ASE_OBJ.2.6C	The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

ASE_OBJ.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_REQ.2 – Derived security requirements

ASE_REQ.2.1D	The developer shall provide a statement of security requirements.
ASE_REQ.2.2D	The developer shall provide a security requirements rationale.
ASE_REQ.2.1C	The statement of security requirements shall describe the SFRs and the SARs.
ASE_REQ.2.2C	All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.
ASE_REQ.2.3C	The statement of security requirements shall identify all operations on the security requirements.
ASE_REQ.2.4C	All operations shall be performed correctly.
ASE_REQ.2.5C	Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.
ASE_REQ.2.6C	The security requirements rationale shall trace each SFR back to the security objectives for the TOE.
ASE_REQ.2.7C	The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.
ASE_REQ.2.8C	The security requirements rationale shall explain why the SARs were chosen.
ASE_REQ.2.9C	The statement of security requirements shall be internally consistent.
ASE_REQ.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_SPD.1 – Security problem definition

ASE_SPD.1.1D	The developer shall provide a security problem definition.
ASE_SPD.1.1C	The security problem definition shall describe the threats.
ASE_SPD.1.2C	All threats shall be described in terms of a threat agent, an asset, and an adverse action.
ASE_SPD.1.3C	The security problem definition shall describe the OSPs.
ASE_SPD.1.4C	The security problem definition shall describe the assumptions about the operational environment of the TOE.
ASE_SPD.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.1 – TOE summary specification

ASE_TSS.1.1D	The developer shall provide a TOE summary specification.
ASE_TSS.1.1C	The TOE summary specification shall describe how the TOE meets each SFR.
ASE_TSS.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ASE_TSS.1.2E	The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.

5.3.5 Tests (ATE)

ATE_COV.1 – Evidence of coverage

ATE_COV.1.1D	The developer shall provide evidence of the test coverage.
ATE_COV.1.1C	The evidence of the test coverage shall show the correspondence between the tests in the test documentation and the TSFIs in the functional specification.
ATE_COV.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_FUN.1 – Functional testing	
ATE_FUN.1.1D	The developer shall test the TSF and document the results.
ATE_FUN.1.2D	The developer shall provide test documentation.
ATE_FUN.1.1C	The test documentation shall consist of test plans, expected test results and actual test results.
ATE_FUN.1.2C	The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.3C	The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.4C	The actual test results shall be consistent with the expected test results.
ATE_FUN.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2 – Independent testing – sample	
ATE_IND.2.1D	The developer shall provide the TOE for testing.
ATE_IND.2.1C	The TOE shall be suitable for testing.
ATE_IND.2.2C	The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.
ATE_IND.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.2.2E	The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.
ATE_IND.2.3E	The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.3.6 Vulnerability Assessment (AVA)

AVA_VAN.2 – Vulnerability analysis	
AVA_VAN.2.1D	The developer shall provide the TOE for testing.
AVA_VAN.2.1C	The TOE shall be suitable for testing.
AVA_VAN.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_VAN.2.2E	The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.
AVA_VAN.2.3E	The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE.
AVA_VAN.2.4E	The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

6. TOE Summary Specification

This section describes the following security functions implemented by the TOE to satisfy the SFRs claimed in Section 5.2:

- Security audit
- Identification and authentication
- Security management
- Protection of the TSF
- Trusted path/channels
- Intrusion Detection System.

6.1 Security Audit

The TOE processes and records the following general types of event:

- External events—generated by devices in the IT System monitored by the TOE and forwarded to the TOE for analysis. External events provide the source of the TOE's IDS data; they are discussed separately in Section 6.5.
- Internal events—these are divided into **audit events** and **status monitor events**. Status monitor events provide information on the status and performance of the TOE; they are not discussed further. Audit events provide information on TOE activity, including security-related activity.

The ArcSight Manager generates audit events and stores them in CORR-Engine.

The TOE can generate audit records for the following auditable events:

- The start-up and shutdown of audit functions (the audit function automatically starts at system start-up and can only be shutdown at system shutdown. In both instances, a record of the event is recorded.)
- Reading of information from the audit records
- Unsuccessful attempts to read information from the audit records
- All use of the authentication mechanism
- All use of the user identification mechanism
- The reaching of the threshold for unsuccessful authentication attempts and the actions taken by the TOE, including restoration to the normal state (i.e., re-enabling the user account).
- All modifications in the behavior of the functions of the TSF
- All modifications to the values of TSF data
- Use of the management functions
- Modifications to the group of users that are part of a role
- Termination of an interactive session by the user.

Users in the Administrator and Analyzer Administrator roles can view the audit events using either the ArcSight Console or the ArcSight Command Center. Access to the audit events is restricted to the Administrator and Analyzer Administrator roles.

The audit events include the date and time of the event, the type of event, the subject identity, and the outcome of the event, such as whether it was a success or failure. The TOE relies on and obtains a reliable date/timestamp from the operational environment. The audit events are presented in a readable format—as such, Administrators and Analyzer Administrators can read and interpret the content of the information. In addition, Administrators and Analyzer

Administrators can sort the audit events based on the following event attributes: date and time of the event; subject identity; type of event; and success or failure of the related event.

As noted above, audit records are a specific type of event and they are handled, in terms of storage, in exactly the same way as IDS data events. Details of event storage are described in Section 6.6.4.

The Security Audit security function satisfies the following security functional requirements:

- FAU_GEN.1—audit records are generated for security relevant events and include the date and time of the event, type of event, subject identity, and outcome of the event.
- FAU_SAR.1—the TOE provides authorized users with the capability to read all audit information from the audit records. The audit records are displayed in a manner suitable for the authorized user to interpret the information.
- FAU_SAR.2—the TOE prohibits all users read access to the audit records, except those users that have been granted explicit read-access.
- FAU_SAR.3—the TOE provides capabilities to filter the audit data based on event type or date range.
- FAU_STG.1—the TOE protects stored audit records from unauthorized modification and deletion.

6.2 Identification and Authentication

The ArcSight Manager maintains accounts of the authorized users of the TOE. The user account includes the following attributes associated with the user: user identity; authentication data; authorizations; and e-mail address information.

In order to access the functions provided by the TOE via either the ArcSight Console or the ArcSight Command Center, the user must first be identified and authenticated. The TOE supports the following user authentication methods:

- Password-based authentication— as part of the login process, the user submits a password that must match the password associated with the user account
- Password-based and certificate-based authentication—as part of the login process, the user submits a password that must match the password associated with the user account and the client additionally sends the digital certificate matching the user identity
- Password-based or certificate-based authentication—the user is presented the choice of authenticating with either the appropriate password or a digital certificate matching the user identity
- Certificate-based authentication—the user is authenticated by a digital certificate matching the user identity.

The TOE enforces the following restrictions on passwords:

- The minimum password length is 6 characters
- The maximum password length is 20 characters
- A password cannot be the same as the name of its User resource, cannot contain whitespace characters (spaces, tabs, etc.), and can have a maximum of three consecutive repeated characters
- Passwords expire after 60 days, requiring the user to change the password
- Accounts that have been inactive for 90 days are deactivated, preventing access.

To protect the passwords, the ArcSight Manager stores only SHA-256 hashes of the passwords in the CORR-Engine database. When a password is submitted for authentication during login, the TOE hashes the submitted password and compares the resultant value with the hash value stored with the applicable user account in CORR-Engine. If either the login name or the password is incorrect, the login request fails and no administrator functions are made available. As result of a successful login, the interactive session is established and the administrator functions appropriate to the user's assigned roles are made available. By default, the TOE allows a maximum three consecutive failed login attempts, after which the user account is locked for 10 minutes. Alternatively, the TOE can be configured to lock the

user account until it is re-enabled by a user in the Administrator role. The configuration of the authentication failure mechanism is controlled by settings in the `server.properties` file.

The ArcSight Console and ArcSight Command Center provide the primary means for authorized users to interact with the TOE. In addition, the TOE provides various command scripts and utility programs, generically termed "ArcSight Commands" or "shell commands" (because they are executed from a command prompt or command shell on the underlying operating system). The shell commands are described in the guidance documentation and are categorized as follows:

- Allowed for use in the evaluated configuration
- Allowed only for installation/initial configuration
- Not allowed in the evaluated configuration.

The shell commands are executed from the `\bin` directory within the installation directory of the TOE in the underlying operating system's file system. In order to run a shell command, the user first has to be identified and authenticated by the TOE operational environment (i.e., the underlying operating system of the machine on which the TOE component is installed). The following shell commands additionally require the user to provide a user identity and password for a TOE user account: `console`; `managerinventory`; and `package`. These commands (and all other shell commands) are fully described in the Administrator's Guide. For these commands, the ArcSight Manager identifies and authenticates the user, in the same way as a user accessing the TOE via the ArcSight Console or ArcSight Command Center.

A further means of interacting with the TOE is provided by the Service Layer APIs. In order to make use of the services provided by the Service Layer APIs, the client must first login to the TOE via the **LoginService**. The client submits a user identity and associated authentication data as part of the login request. If the TOE successfully authenticates the user identity, it returns a session token to the client that the client includes with every subsequent service request during the session. The session ends when the client logs out or the TOE invalidates the session (e.g., due to session inactivity).

The Identification and Authentication function satisfies the following security functional requirements:

- FIA_AFL.1—the TOE is able to detect when an administrator-configurable positive integer of unsuccessful authentication attempts occur related to user authentication. When the defined number of unsuccessful authentication attempts has been met, the TOE locks the user account either for a specified time period or until it is re-enabled by an Administrator, as configured by an authorized administrator.
- FIA_ATD.1—the TOE maintains the following security attributes associated with each user: user identity; authentication data; authorization group (role); and e-mail address.
- FIA_SOS.1—the TOE enforces a password policy that ensures all secrets (i.e., passwords) associated with user accounts meet policy requirements.
- FIA_UAU.1—the TOE allows certain specific actions related to invocation of shell commands to be performed on behalf of the user, where the operational environment has authenticated the user, without authentication by the TOE. The TOE requires each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
- FIA_UAU.5—the TOE supports the use of passwords and digital certificates for user authentication.
- FIA_UID.1—the TOE allows certain specific actions related to invocation of shell commands to be performed on behalf of the user, where the operational environment has identified the user, without identification by the TOE. The TOE requires each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
- FTA_SSL.4—the TOE allows users to terminate their own interactive sessions.

6.3 Security Management

6.3.1 Security Management Roles

When an Administrator creates a user account, the account is created within a user group. The user is granted the authorizations associated with its containing user group(s) (a user can belong to more than one group). Each user group has an Access Control List (ACL) associated with it that specifies the read and write access that users within the group have to all the resources managed by the TOE. This is the TOE's mechanism for implementing security management roles.

The TOE provides the following built-in security management roles:

- Administrator—uses the ArcSight Console to view the overall health of an enterprise and perform administrative tasks such as managing, configuring, and integrating ESM with multi-vendor devices. Users in the Administrator role have full authorization to perform all functions in the TOE, including modifying the behavior of the TOE's analysis and reaction functions, managing the audit function and creating other users.
- Analyzer Administrator—the Analyzer Administrator role (also identified as Author in the guidance documentation) uses the ArcSight Console to manage resources such as rules, filters, and data monitors, to enforce enterprise security policies and procedures. Users in the Analyzer Administrator role have authorization to modify the behavior of the TOE's analysis and reaction functions and to query and modify most TSF data. However, the Analyzer Administrator role is not able to create or modify user accounts.
- Operator—uses the ArcSight Console to assist in observing, interpreting, and responding to events. Operators can observe real-time and replay events using Views, interpret events with Event Inspector and Replay Controls, and respond to events with preset, automated actions, Replay Control Tools, Reports, and Knowledge Base articles. Users in the Operator role have authorization to view Analyzer events, reports, query viewers, and configuration information, but do not have authorizations to modify the behavior of the TOE's analysis and reaction functions, to create or modify user accounts or to modify the filters that control which auditable events are actually audited.
- Analyst—uses the ArcSight Console to investigate events that have been forwarded to them by security operations center staff and other users, and can create custom resources, such as filters, rules, and data monitors to respond to security threats. With regard to management of TOE security functions and TSF data, users in the Analyst role have the same authorization levels as Operators.

6.3.2 Security Management Functions

The ArcSight Console and ArcSight Control Center implement the GUIs that provide the Administrators, Analyzer Administrators, Operators and Analysts with the interfaces to perform security management tasks. The tasks include the ability to manage user accounts, modify user passwords, and manage the IDS analysis and reaction functions.

The TOE requires user authentication before any administrative actions, security-related or otherwise, can be performed (other than entry of identification and authentication data) on the ArcSight Console or ArcSight Control Center. As a result, only users belonging to one of the security management roles (Administrator, Analyzer Administrator, Operator or Analyst) can access any function on the TOE via the ArcSight Console or ArcSight Control Center. The Administrator and Analyzer Administrator roles have the capabilities to modify the behavior of the TOE's analysis and reaction functions, by virtue of having read and write access to the various TOE resources that control how the TOE analyzes and reacts to security events.

Users with the Administrator or Analyzer Administrator role have the ability to query and modify the configuration of the TOE as it relates to the generation of IDS data. The Administrator is the only role that can create and modify user accounts. Users in all roles have the ability to modify their own passwords, but only users in the Administrator role can modify the password of another user.

The Security Management function satisfies the following security functional requirements:

- FMT_MOF.1—the TOE restricts the ability to manage the functions of IDS data analysis and reaction to the Administrator and Analyzer Administrator roles.

- FMT_MTD.1(*)—the TOE restricts the ability to manage user accounts and to modify another user's password to the Administrator role.
- FMT_SMF.1—the TOE provides the capabilities necessary to manage the security of the TOE.
- FMT_SMR.1—the TOE maintains the Administrator, Analyzer Administrator, Operator and Analyst security management roles and is able to associate users with these roles.

6.4 Protection of the TSF

The TOE comprises the ArcSight Manager, CORR-Engine, ArcSight Console, ArcSight Command Center and Service Layer APIs. Of these, the Manager, CORR-Engine, Command Center and Service Layer APIs are collocated on the same server. The ArcSight Console is installed on a separate workstation and communicates with the ArcSight Manager via a network connection. The ArcSight Console and ArcSight Manager communicate with each other using HTTPS (HTTP over TLS), which ensures the data transmitted between them is protected from disclosure (through the use of symmetric encryption) and modification (through the use of a cryptographic hash).

The Protection of the TSF function satisfies the following security functional requirements:

- FPT_ITT.1—the TOE uses HTTPS to protect TSF data communicated between the ArcSight Console and ArcSight Manager.

6.5 Trusted Path/Channels

6.5.1 Trusted Channel

The TOE supports communications via trusted channels with other trusted IT products for the following functions:

- Access to TOE web services via the Service Layer APIs
- Collection of normalized events from SmartConnectors.

Web service clients can initiate communication via the trusted channel to perform the following functions supported by the Service Layer APIs:

- Run an ESM report and feed it back to a third-party system
- Create and update cases
- Manage resource groups.

SmartConnectors can initiate communication via the trusted channel to forward events to the TOE for further processing.

Trusted channels are implemented using HTTPS. The TOE supports TLS v1.0, TLS v1.1 and TLS v1.2 in non-FIPS mode and FIPS 140-2 Mode. The TOE supports the following TLS ciphersuites, as defined in RFC 2246, RFC 4346 and RFC 5246:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_ CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

6.5.2 Trusted Path

The TOE provides a trusted path for administrators of the TOE to communicate with the TOE. The trusted path is implemented using HTTPS (i.e., TLS over HTTP) for access to the ArcSight Command Center. Administrators

initiate the trusted path by establishing an HTTPS connection using a supported web browser. The TOE's implementation of TLS is described in the previous section (Trusted Channel).

The trusted path is used for initial authentication and all subsequent administrative actions. The use of HTTPS ensures all communication over the trusted path is protected from disclosure and modification.

The Trusted Path/Channels function satisfies the following security functional requirements:

- FTP_ITC.1—the TOE supports establishment of trusted channels for communicating with trusted IT entities using HTTPS.
- FTP_TRP.1—the TOE provides a trusted path for administrators to communicate with the TOE, using HTTPS to access the ArcSight Command Center.

6.6 Intrusion Detection System

6.6.1 Analysis

The ArcSight Manager uses a collection of tools that allow authorized users to track, respond, and resolve security threats and attacks. The Correlation Engine prioritizes events based on the threat they pose to the protected network, identifies statistical anomalies in the content or volume of events, and uses rules to both correlate events using signatures and trigger automated response actions. The Correlation Engine in ArcSight Manager correlates events across vendor, device, and time. By correlating different events, the Correlation Engine detects successful attacks, their criticality, and threat level.

The Correlation Engine is a sub-component of the ArcSight Manager implemented using threat evaluation formulae, statistical data monitors, and rules. The threat evaluation formulae are used to compute a numeric priority for each event. Statistical data monitors generate meta-events when fluctuations are observed in the volume or content of the event stream. Rules may either be a simple filter or may perform a complex join across several events in real-time. Rules then aggregate the occurrences of the matching events. Rules trigger responses either on first match or after a given threshold has been passed. A rule threshold is defined as either a set number of matches or a given amount of time. If the threshold is passed, the Correlation Engine generates a derived event and performs the other actions associated with the rule.

There are predefined threat level formulae, statistical data monitors, and rules to detect intrusions and perform actions. Some built in rules and data monitors are designed to monitor the operation and integrity of the ArcSight Manager and ArcSight SmartConnectors. Other rules and data monitors detect and respond to attacks and suspicious activity, specific types of attacks on various sensor types, network components, or assets, and attack results or success of attack.

6.6.2 Reaction

Rule actions are automatic procedures that occur when all rule conditions and threshold settings have been met. A rule is a programmed procedure that can analyze network events and generate additional correlation events, as determined by security policy. When creating rules, the Analyzer Administrators[1] define the rule events and conditions, thresholds, and rule actions. Conditions define which events trigger the rule, thresholds set when a correlation event is generated, and actions state which responses are taken when a correlation event is generated. A rule requires at least one event and one condition. The Analyzer Administrator can also assign more than one rule action to any rule. For example, the notification rule actions are used to inform ArcSight users that an incident has occurred. The notification may be delivered to the user on the ArcSight Console or by e-mail. Rule actions can also be set to send information about the event to a case or active list.

- Cases are entries in an event-tracking system used to track, investigate, and resolve suspicious events in a workflow-type environment. When suspicious events occur, cases are created and assigned to users, who then investigate and resolve them based on enterprise policies and practices.
- Active list can be used to create a configurable data store that can hold information derived from events or other sources. Active lists can monitor activity based on any rule-driven combination of event attributes or

[1] Note that Administrators also have the capability to create rules.

set of custom fields. For example, active lists are very useful for tracking suspicious or hostile IP addresses as well as targets of attacks that may be compromised. The main uses of active lists are to:

- Maintain information, such as in the system content provided "Hostile List" or "Trusted List", which maintain information on hostile and trusted IP addresses (and corresponding zones)
- Check for the existence of particular information in lists using the InActiveList condition. For example, when a system is compromised (such as in a security breach), it can be added to the compromise list using rule actions. The information in the active list can then be used to collect all the events that occur on the asset while it is compromised. This can be used for tracking and further investigation on other systems that have come into contact with the compromised system.

The following list summarizes the rule actions supported by the TOE. Further details of these rule actions are provided in the guidance documentation:

- Set Event Field—Fills in a data field value for correlation events generated by the rule
- Send to OpenView Operations—requires HP OpenView to be integrated with ESM, so serves no purpose in the evaluated configuration
- Send Notification—Sends e-mail messages to specified TOE users when rules are triggered
- Execute Command—execute a command line function when the rule is triggered. The action specifies the command line function to be executed and any variables the function requires. Additionally, the action specifies where and how the command line function is to be executed. The following options are available:
  - Automatically on the Manager host, in which case the command is executed without further intervention
  - On the Manager host only after execution confirmation is received from an authorized user at a Console
  - On applicable SmartConnectors
- Execute Connector Command—Execute a SmartConnector command that is applicable to the device it monitors
- Export to External System—Sends the rule and the triggering events to an external system that is integrated with ESM (serves no purpose in the evaluated configuration)
- Create New Case—Creates a new case when the rule is triggered
- Add to Existing Case—Adds the associated events to an already-defined case
- Add to Active List—Adds the events to an existing Active List
- Remove from Active List—Remove the associated events from an existing Active List
- Add to Session List—Add the associated events to an existing Session List
- Terminate Session List—Add the associated events to the selected Session List and end the Session List
- Add Asset Category to Asset—Associates an asset category to the specified asset
- Remove Asset Category from Asset—Removes the associated category to the specified asset.

6.6.3 IDS Data Review

The TOE provides various capabilities for users in the Administrator, Analyzer Administrator, Operator and Analyst roles to view IDS data (i.e., events) via either the ArcSight Console or the ArcSight Command Center.

The ArcSight Console provides the following tools for monitoring events:

- Active channels—provide a streaming view of events coming into the TOE that can be viewed numerous ways using numerous types of filters and field sets

- Dashboards—provide graphical displays of data gathered from data monitors and query viewers. Dashboards can display data in a number of graphical formats, including pie and bar charts, tables, and custom layouts
- Data monitors—collect summary information on top events, most recent event activity, partial rule occurrences, hourly event counts, or event averages
- Query viewers—a type of resource for defining and running SQL queries on other resources, including trends, assets, cases, connectors, and events. Each query viewer contains an SQL query along with other logic for establishing and comparing baseline results, analyzing historical data to find patterns in network activity, and performing drill-down investigation on a particular aspect of the results
- Active lists—can monitor activity based on any rule-driven combination of event attributes or set of custom fields.

The ArcSight Command Center provides the following tools for monitoring events:

- Active channels—operate similarly to active channels viewed via the ArcSight Console, described above
- Dashboards—ArcSight Command Center provides two means of viewing system information: the Dashboard page and Dashboard Navigator page. Information appears in these two pages in the form of dashlets. From the Dashboard page, users can add any available dashlets, while from the Dashboard Navigator page users can view dashboards comprised of data monitor and query viewer dashlets. Unlike the Dashboard page, dashboards in the Dashboard Navigator page cannot be modified since they originate in the ArcSight Console. The dashlets can be saved as CSV files.

All data is presented in such a manner that it can be read and the contents of the data can be interpreted; thus the reader can understand the content of the information presented.

6.6.4 Event Storage

Incoming events are stored in the CORR-Engine database for search and correlation analysis. The CORR-Engine uses storage groups for managing the storage of events. Two storage groups (Default Storage Group and Internal Storage Group) are predefined in the TOE and users can create up to four additional storage groups.

The CORR-Engine's event storage operates on two types of retention—time-based and space-based. They operate in cycles, with time-based retention as the default and space-based retention as a protection from loss of incoming data if space is beginning to run out.

- Time-based retention—a job runs daily to remove aging events (older than retention period).
- Space-based retention—when the main storage is about to run out of space, space based retention will be triggered. It removes the oldest events to free up enough space to meet the space requirement. When space is available again, time based retention resumes.

As events flow into ESM, they receive a time stamp at Manager Receipt Time (MRT). All events time stamped for a particular day (12:00:00 a.m. to 11:59:59 p.m.) are grouped together. Either manually or at a set time (12:00:00 by default), the previous day's events can be copied into an archive.

By default, all events are sent to the Default Storage Group, where they are retained for thirty days, after which they are deleted. These default settings can be managed using capabilities of the ArcSight Command Center, enabling events from different connectors to be sent to different storage groups and the retention period of each storage group to be configured. Additionally, the daily events from each storage group can be archived as needed, so that all necessary events can be retained as long as needed. The TOE supports one archive per day per storage group.

Events that are online in the CORR-Engine are available for search and correlation analysis. Unless an archive is created for them, events exist online in the CORR-Engine database only. Events remain online in the CORR-Engine database until their retention period expires. Once events have passed their retention period and are removed from the CORR-Engine database, one of two things will happen:

- If they have been archived, they will no longer be searchable, but will still be backed up in off-line storage. These archives can be made searchable again, if necessary.
- If they have not been archived, they are permanently deleted.

To prevent IDS data loss, two warnings are sent to a configured notification destination (e.g., Administrator) in the event the CORR-Engine database begins to run out of storage space. The first notification comes in the form of a warning and is sent at 90% of capacity by default. The second notification comes in the form of an error and is sent at 95% of capacity by default.

If CORR-Engine storage fills up, the ArcSight Manager stops accepting new events from all ArcSight SmartConnectors. Those ArcSight SmartConnectors will use local operating system disk-based cache to preserve those events until the ArcSight Manager starts accepting events once again. If that local cache also fills, then SmartConnectors will discard the oldest blocks of event data from that local cache in order to continue receiving and storing new events. Once space has been freed on the CORR-Engine storage, the ArcSight Manager is re-enabled so that the cached and live events may flow up from the ArcSight SmartConnectors.

The Intrusion Detection System function satisfies the following security functional requirements:

- IDS_ANL.1—the TOE performs statistical and signature analysis on IDS data (events) collected by sensors and scanners in its operational environment and records the results of its analysis.
- IDS_RCT.1—the TOE can send an alarm to a configured destination and take additional specified actions when an intrusion is detected.
- IDS_RDR.1—the TOE provides authorized users with the capability to read all IDS information from the IDS data. The IDS data are displayed in a manner suitable for the authorized user to interpret the information.
- IDS_STG.1—the TOE protects stored IDS data from modification and unauthorized deletion.
- IDS_STG.2(*)—the TOE will send warning and error messages to configured e-mail addresses when the storage space consumed by IDS data exceeds the configured warning and error thresholds respectively.

7. Rationale

This section provides the rationale for completeness and consistency of the Security Target. The rationale addresses the following areas:

- Security Objectives
- Security Functional Requirements
- Security Assurance Requirements
- Requirement Dependencies
- TOE Summary Specification.

7.1 Security Objectives Rationale

This section shows that all secure usage assumptions and threats are completely covered by security objectives for the TOE or operational environment. In addition, each objective counters or addresses at least one assumption or threat.

	T.BRUTE_FORCE	T.INTEGRITY_COMPROMISE	T.NETWORK_COMPROMISE	T.NO_ACCOUNTABILITY	T. UNAUTHORIZED_ACCESS	T.UNAUTHORIZED_ACTIVITY	T.UNDETECTED_THREATS	A. MANAGE	A. PLATFORM	A.PROTECT
O.ANALYZER							X			
O.AUDIT				X						
O.AUDIT_REVIEW				X						
O.I_AND_A					X					
O.PASSWORD_CONTROLS	X									
O.PROTECTED_COMMS			X							
O.RESPONSE							X			
O.REVIEW							X			
O.SECURITY_MANAGEMENT						X				
O.STORAGE		X								
O.THROTTLE	X									
OE.PERSONNEL								X		
OE.PHYSICAL										X
OE.PLATFORM					X				X	
OE.SENSORS							X			
OE.TIME				X			X			

Table 4: Security Problem Definition to Security Objective Correspondence

T.BRUTE_FORCE

An unauthorized user may gain access to the TOE through repeated password-guessing attempts.

This threat is countered by the following security objectives:

- O.PASSWORD_CONTROLS—addresses this threat by providing a mechanism, configurable by an administrator, which encourages users to choose difficult-to-guess passwords.
- O.THROTTLE—addresses this threat by providing a mechanism, configurable by an administrator, to lock a user account after a specified number of consecutive failed authentication attempts has been met.

T.INTEGRITY_COMPROMISE

An unauthorized person may attempt to modify or destroy audit or IDS data, thus removing evidence of unauthorized or malicious activity.

This threat is countered by the following security objective:

- O.STORAGE—addresses this threat by ensuring the TOE is able to protect stored audit records and IDS data from unauthorized modification and deletion.

T.NETWORK_COMPROMISE

TSF data communicated between components of the TOE, or between the TOE and external entities, is disclosed or modified.

This threat is countered by the following security objective:

- O.PROTECTED_COMMS—addresses this threat by ensuring all communications between the TOE and external entities are protected from disclosure and undetected modification.

T.NO_ACCOUNTABILITY

Authorized users of the TOE perform adverse actions on the TOE, or attempt to perform unauthorized actions, which go undetected.

This threat is countered by the following security objectives:

- O.AUDIT—addresses this threat by ensuring the TOE is able to generate audit records of security relevant events.
- O.AUDIT_REVIEW—supports O.AUDIT in addressing the threat by ensuring the TOE provides capabilities for effective review of stored audit records.
- OE.TIME—supports O.AUDIT by ensuring the operational environment is able to provide the TOE with a reliable time source that can be used to generate time stamps for inclusion within generated audit records.

T.UNAUTHORIZED_ACCESS

An unauthorized user may gain access to the TOE security functions and data.

This threat is countered by the following security objectives:

- O.I_AND_A—addresses this threat by ensuring all users of the TOE are identified and authenticated prior to gaining further access to the TOE and its services.
- OE.PLATFORM—supports O.I_AND_A by ensuring the operating system underlying each TOE component protects the component and its configuration from unauthorized access.

T.UNAUTHORIZED_ACTIVITY

Authorized users perform unauthorized actions on the TOE.

This threat is countered by the following security objective:

- O.SECURITY_MANAGEMENT—addresses this threat by providing a mechanism that requires authorized users to have appropriate privileges in order to perform actions on the TOE.

T.UNDETECTED_THREATS

Events generated by entities in the IT system indicative of misuse or unauthorized or malicious activity go undetected.

This threat is countered by the following security objectives:

- O.ANALYZER—addresses this threat by ensuring the TOE is able to analyze collected IDS data in order to identify misuse and unauthorized or malicious activity in the IT system being monitored, and be able to record the results of its analysis.
- O.RESPONSE—supports O.ANALYZER in addressing this threat by ensuring the TOE is able to respond to identified misuse and unauthorized or malicious activity.
- O.REVIEW—supports O.ANALYZER in addressing this threat by ensuring the TOE provides capabilities for reviewing the results of its analysis of collected IDS data.
- OE.SENSORS—supports O.ANALYZER in addressing this threat by ensuring the operational environment provides capabilities to collect IDS data from the IT system is monitoring and to provide that IDS data to the TOE in a form suitable for the TOE to analyze.

A.MANAGE

There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

This assumption is satisfied by the following security objective:

- OE.PERSONNEL—this objective satisfies the assumption by ensuring those assigned as authorized administrators are properly trained in operating the TOE.

A.PLATFORM

The underlying operating system of each TOE component will protect the component and its configuration from unauthorized access.

This assumption is satisfied by the following security objective:

- OE.PLATFORM—this objective satisfies the assumption by ensuring the operating system underlying each TOE component protects the component and its configuration from unauthorized access.

A.PROTECT

The TOE hardware and software critical to the security policy enforcement will be located within controlled access facilities which will prevent unauthorized physical access.

This assumption is satisfied by the following security objective:

- OE.PHYSICAL—this objective satisfies the assumption by ensuring the TOE is protected from physical attack.

7.2 Security Functional Requirements Rationale

All security functional requirements identified in this Security Target are fully addressed in this section and each is mapped to the objective it is intended to satisfy. Table 5 summarizes the correspondence of functional requirements to TOE security objectives.

	O.ANALYZER	O.AUDIT	O.AUDIT_REVIEW	O.I_AND_A	O.PASSWORD_CONTROLS	O.PROTECTED_COMMS	O.RESPONSE	O.REVIEW	O.SECURITY_MANAGEMENT	O.STORAGE	O.THROTTLE
FAU_GEN.1		X									
FAU_SAR.1			X								
FAU_SAR.2			X								
FAU_SAR.3			X								
FAU_STG.1										X	
FIA_AFL.1											X
FIA_ATD.1				X							
FIA_SOS.1					X						
FIA_UAU.1				X							
FIA_UAU.5				X							
FIA_UID.1				X							
FMT_MOF.1									X		
FMT_MTD.1(*)									X		
FMT_SMF.1									X		
FMT_SMR.1									X		
FPT_ITT.1						X					
FTA_SSL.4				X							
FTP_ITC.1						X					
FTP_TRP.1						X					
IDS_ANL.1	X										
IDS_RCT.1							X				
IDS_RDR.1								X			
IDS_STG.1										X	
IDS_STG.2(*)										X	

Table 5: Objectives to Requirement Correspondence

O.ANALYZER

The TOE shall analyze collected IDS data in order to identify misuse and unauthorized or malicious activity and shall be able to record the results of its analysis.

The following security functional requirement contributes to satisfying this security objective:

- IDS_ANL.1—the ST includes IDS_ANL.1 to specify the capability to perform statistical and signature-based analysis functions on IDS data it receives from its operational environment and to record the results of its analysis.

O.AUDIT

The TOE shall be able to generate audit records of security-relevant events.

The following security functional requirement contributes to satisfying this security objective:

- FAU_GEN.1—the ST includes FAU_GEN.1 to specify the capability to generate audit records of security-relevant events, and to specify the specific events to be audited and the content of generated audit records of those events.

O.AUDIT_REVIEW

The TOE shall provide a means for authorized users to review the audit records generated by the TOE.

The following security functional requirements contribute to satisfying this security objective:

- FAU_SAR.1—the ST includes FAU_SAR.1 to specify which roles are to be able to read data from stored audit records.
- FAU_SAR.2—the ST supports FAU_SAR.1 by including FAU_SAR.2 to specify that the ability to read data from stored audit records is restricted to only the roles specified in FAU_SAR.1.
- FAU_SAR.3—the ST supports FAU_SAR.1 by including FAU_SAR.3 to specify capabilities for sorting audit records based on date and time the audit event is recorded, the type of audit event, the subject associated with the audit event, and the outcome of the event, which assists the authorized roles in effectively reviewing the audit trail.

O.I_AND_A

The TOE shall provide a means for users to be identified and authenticated before gaining access to TOE services.

The following security functional requirements contribute to satisfying this security objective:

- FIA_UID.1, FIA_UAU.1—the ST includes FIA_UID.1 and FIA_UAU.1 to specify that users may perform actions where the operational environment has identified and authenticated the user and must be successfully identified and authenticated by the TOE before being able to perform any other TSF-mediated actions.
- FIA_ATD.1—the ST supports FIA_UID.1 and FIA_UAU.1 by including FIA_ATD.1 to ensure user identity and authentication data security attributes are associated with individual users.
- FIA_UAU.5—the ST supports FIA_UAU.1 by including FIA_UAU.5 to specify the authentication mechanisms supported by the TOE and the rules by which the TOE authenticates a user's claimed identity.
- FTA_SSL.4—the ST supports FIA_UID.1 and FIA_UAU.1 by including FTA_SSL.4 to specify the capability for users to terminate their own interactive sessions, thus requiring subsequent users to again identify and authenticate themselves prior to gaining access to TOE services via the ArcSight Console or ArcSight Command Center.

O.PASSWORD_CONTROLS

The TOE shall provide a mechanism to reduce the likelihood that users choose weak passwords.

The following security functional requirement contributes to satisfying this security objective:

- FIA_SOS.1—the ST includes FIA_SOS.1 to specify that passwords must meet minimum construction requirements, in terms of length and character set.

O.PROTECTED_COMMS

The TOE shall protect communications between distributed parts of the TOE, and between the TOE and external entities, from disclosure and modification.

The following security functional requirements contribute to satisfying this security objective:

- FPT_ITT.1—the ST includes FPT_ITT.1 to specify that communications between distributed parts of the TOE will be protected from disclosure and modification.

- FTP_ITC.1, FTP_TRP.1—the ST includes FTP_ITC.1 and FTP_TRP.1 to specify that communications between the TOE and external entities (both trusted IT entities and remote users) will be protected from disclosure and modification.

O.RESPONSE

The TOE shall respond to misuse and unauthorized or malicious activity it identifies based on its configuration.

The following security functional requirement contributes to satisfying this security objective:

- IDS_RCT.1—the ST includes IDS_RCT.1 to specify the capability for the TOE to respond to detected misuse, unauthorized or malicious activity by sending an alarm to a configured destination and taking other actions as specified by the TOE's configuration.

O.REVIEW

The TOE shall provide capabilities for effective review of stored IDS data.

The following security functional requirement contributes to satisfying this security objective:

- IDS_RDR.1—the ST includes IDS_RDR.1 to specify the capability for the TOE to provide authorized users with the capability to read all event information from the stored IDS data.

O.SECURITY_MANAGEMENT

The TOE shall restrict the ability to perform security management functions on the TOE to authorized administrators having appropriate privileges.

The following security functional requirements contribute to satisfying this security objective:

- FMT_SMF.1, FMT_SMR.1, FMT_MOF.1, FMT_MTD.1(*)—the ST includes these requirements to specify the security management functions to be provided by the TOE (FMT_SMF.1), to specify security management roles and privileges (FMT_SMR.1), and to specify the restrictions on management of security function behavior and TSF data (FMT_MOF.1, FMT_MTD.1(*)).

O.STORAGE

The TOE shall protect stored audit records and IDS data from unauthorized modification or deletion.

The following security functional requirements contribute to satisfying this security objective:

- FAU_STG.1—the ST includes FAU_STG.1 to specify the capability to protect audit records stored in the audit trail from unauthorized deletion and to prevent unauthorized modification of these records.
- IDS_STG.1—the ST includes IDS_STG.1 to specify the capability to protect stored IDS data from modification and unauthorized deletion. It additionally specifies a capability to ensure that the most recent stored IDS data, limited only by available storage, will be maintained in the event that storage space for IDS data is exhausted.
- IDS_STG.2(*)—the ST supports IDS_STG.1 by including IDS_STG.2(*) to specify capabilities to send warning and error notifications to a configured e-mail address in the event the IDS storage exceeds configured warning and error threshold values.

O.THROTTLE

The TOE shall limit the rate at which consecutive unsuccessful authentication attempts can be performed.

The following security functional requirement contributes to satisfying this security objective:

- FIA_AFL.1—the ST includes FIA_AFL.1 to specify the capability to limit the rate at which consecutive failed authentication attempts (which may indicate a password-guessing attack) can be made.

7.3 Security Assurance Requirements Rationale

EAL 2 was selected as the assurance level because the TOE is a commercial product whose users require a low to moderate level of independently assured security. The TOE is intended for use in an environment with good physical access security where it is assumed that attackers will have Basic attack potential. The target assurance level of EAL 2 is appropriate for such an environment.

7.4 Requirement Dependency Rationale

The following table identifies the SFRs claimed in the ST, their dependencies as defined in CC Part 2, and how the dependency is satisfied in the ST. It can be seen that all dependencies have been satisfied by inclusion in the ST of the appropriate dependent SFRs.

Requirement	Dependencies	How Satisfied
FAU_GEN.1	FPT_STM.1	See TimeStamp Note below.
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_ATD.1	None	None
FIA_SOS.1	None	None
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UAU.5	None	None
FIA_UID.1	None	None
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1(*)	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_SMF.1	None	None
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FPT_ITT.1	None	None
FTA_SSL.4	None	None
FTP_ITC.1	None	None
FTP_TRP.1	None	None
IDS_ANL.1	IDS_SDC.1	See IDS Data Collection Note below
IDS_RCT.1	IDS_ANL.1	IDS_ANL.1
IDS_RDR.1	IDS_SDC.1, IDS_ANL.1	See IDS Data Collection Note below. IDS_ANL.1
IDS_STG.1	IDS_SDC.1, IDS_ANL.1	See IDS Data Collection Note below. IDS_ANL.1
IDS_STG.2(*)	IDS_STG.1	IDS_STG.1

Table 6: Requirement Dependencies

TimeStamp Note: The TOE is not a physical device and operates as an application within a process provided by the environment. Thus, the environment is providing resources for the TOE. The environmental objective OE.TIME requires that the TOE's environment provide a reliable timestamp which the TOE can use as needed (e.g., within audit records). Therefore, the functionality specified in the dependency of FAU_GEN.1 upon FPT_STM.1 is available to the TOE from its environment.

IDS Data Collection Note: The TOE provides the capability of an IDS analyzer. It relies on agents in its operational environment (termed SmartConnectors) to collect IDS data from the IT system the TOE is monitoring. The environmental objective OE.SENSORS requires that the TOE's environment has the capability to provide IDS data to the TOE in a form suitable for the TOE to analyze. Therefore, the functionality specified in the dependency of IDS_ANL.1, IDS_RDR.1 and IDS_STG.1 upon IDS_SDC.1 is available to the TOE from its environment.

7.5 TOE Summary Specification Rationale

Section 6, the TOE Summary Specification, describes how the security functions of the TOE meet the claimed SFRs. The following table provides a mapping of the SFRs to the security function descriptions to support the TOE Summary Specification.

	Security Audit	Identification and Authentication	Security Management	Protection of the TSF	Trusted Path/Channels	Intrusion Detection System
FAU_GEN.1	X					
FAU_SAR.1	X					
FAU_SAR.2	X					
FAU_SAR.3	X					
FAU_STG.1	X					
FIA_AFL.1		X				
FIA_ATD.1		X				
FIA_SOS.1		X				
FIA_UAU.1		X				
FIA_UAU.5		X				
FIA_UID.1		X				
FMT_MOF.1			X			
FMT_MTD.1(*)			X			
FMT_SMF.1			X			
FMT_SMR.1			X			
FPT_ITT.1				X		
FTA_SSL.4		X				
FTP_ITC.1					X	
FTP_TRP.1					X	
IDS_ANL.1						X
IDS_RCT.1						X
IDS_RDR.1						X
IDS_STG.1						X
IDS_STG.2(*)						X

Table 7: Security Functions vs. Requirements Mapping