Micro Focus
ArcSight Data Platform
Security Target

Version 1.0
29 September 2017

Prepared for:

Micro Focus
1160 Enterprise Way
Sunnyvale CA, 94089

Prepared By:

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

TABLE OF CONTENTS

1. INTRODUCTION 1

1.1 SECURITY TARGET, TOE AND CC IDENTIFICATION 1
1.2 CONFORMANCE CLAIMS 1
1.3 CONVENTIONS 2
1.4 GLOSSARY 2
1.5 ABBREVIATIONS AND ACRONYMS 3

2. TOE DESCRIPTION 5

2.1 OVERVIEW 5
2.2 ARCHITECTURE 5
2.2.1 ArcSight Management Center 6
2.2.2 ArcSight Logger 6
2.2.3 ArcSight Data Platform (ADP) Event Broker 7
2.2.4 ArcSight SmartConnectors 7
2.3 PHYSICAL BOUNDARIES 7
2.3.1 Physical TOE Components 7
2.3.2 Operational Environment Components 8
2.4 LOGICAL BOUNDARIES 10
2.4.1 Audit 10
2.4.2 Identification & Authentication 10
2.4.3 Security Management 10
2.4.4 Protection of the TSF 11
2.4.5 TOE Access 11
2.4.6 Trusted Path/Channels 11
2.4.7 Intrusion Detection System 11
2.5 CAPABILITIES PROVIDED BY THE OPERATIONAL ENVIRONMENT 11
2.6 CAPABILITIES EXCLUDED FROM THE SCOPE OF EVALUATION 12
2.7 TOE DOCUMENTATION 12

3. SECURITY PROBLEM DEFINITION 13

3.1 ASSUMPTIONS 13
3.2 THREATS 13

4. SECURITY OBJECTIVES 14

4.1 SECURITY OBJECTIVES FOR THE TOE 14
4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT 14

5. IT SECURITY REQUIREMENTS 16

5.1 EXTENDED COMPONENTS DEFINITION 16
5.1.1 Intrusion Detection System (IDS) 16
5.2 TOE SECURITY FUNCTIONAL REQUIREMENTS 18
5.2.1 Security Audit (FAU) 19
5.2.2 Identification and Authentication (FIA) 20
5.2.3 Security Management (FMT) 21
5.2.4 Protection of the TSF (FPT) 22
5.2.5 TOE Access (FTA) 22
5.2.6 Trusted Path/Channels (FTP) 22
5.2.7 Intrusion Detection System (IDS) 23
5.3 TOE SECURITY ASSURANCE REQUIREMENTS 23
5.3.1 Development (ADV) 24
5.3.2 Guidance Documents (AGD) 25
5.3.3 Life-cycle Support (ALC) 26

5.3.4 Security Target Evaluation (ASE) 27
5.3.5 Tests (ATE) 29
5.3.6 Vulnerability Assessment (AVA) 30

6. TOE SUMMARY SPECIFICATION 31

6.1 SECURITY AUDIT 31
6.2 IDENTIFICATION AND AUTHENTICATION 32
6.3 SECURITY MANAGEMENT 33
6.4 PROTECTION OF THE TSF 35
6.5 TOE ACCESS 35
6.6 TRUSTED PATH/CHANNELS 36
6.7 INTRUSION DETECTION SYSTEM 36
6.7.1 Data Collection 36
6.7.2 Storage and Availability 38
6.7.3 Searching and Review 39
6.7.4 Alerting 41

7. RATIONALE 43

7.1 SECURITY OBJECTIVES RATIONALE 43
7.2 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE 46
7.3 SECURITY ASSURANCE REQUIREMENTS RATIONALE 49
7.4 REQUIREMENT DEPENDENCY RATIONALE 50
7.5 TOE SUMMARY SPECIFICATION RATIONALE 50

LIST OF TABLES

Table 1: Supported SmartConnector Environments 9
Table 2: TOE Security Functional Components 19
Table 3: TOE Security Assurance Components 24
Table 4: Supported Field-Based Search Operators 40
Table 5: Security Problem Definition to Security Objective Correspondence 43
Table 6: Objectives to Requirement Correspondence 47
Table 7: Requirement Dependencies 50
Table 8: Security Functions vs. Requirements Mapping 51

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 Data Platform (ADP) 2.11 from Micro Focus. ADP is a next-generation data collection and storage engine that unifies log data collection, storage, and security data management in a scalable, high-performance software or appliance solution. It provides capabilities to collect machine data from any source (such as logs, clickstreams, sensors, stream network traffic, security devices, web servers, custom applications, social media, and cloud services) and to monitor and search that data for security intelligence.

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 – Micro Focus ArcSight Data Platform Security Target

ST Version – Version 1.0

ST Date – 29 September 2017

TOE Identification – Micro Focus ArcSight Data Platform 2.11, comprising:

- ArcSight Management Center v2.6
- ArcSight Logger v6.4
- ArcSight Data Platform Event Broker 2.01
- ArcSight SmartConnectors v7.6, specifically:
  - Syslog NG Daemon
  - Microsoft Windows Event Log – Native (WINC).

TOE Developer – Micro Focus

Evaluation Sponsor – Micro Focus

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 and/or different fonts (such as `Courier`) to highlight text of special interest, such as captions, commands, or filenames specific to the TOE.

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.

Apache Flume	A distributed, reliable, and available service for efficiently collecting, aggregating, and moving large amounts of log data.
Apache Hadoop	An open-source software framework used for distributed storage and processing of very large data sets.
Apache Kafka	An open-source stream processing platform that provides a unified, high-throughput, low-latency platform for handling real-time data feeds.
Apache ZooKeeper	A distributed hierarchical key-value store, which is used to provide a distributed configuration service, synchronization service, and naming registry for large distributed systems.
ArcMC	The component of the TOE that provides the ability to centrally manage SmartConnectors and Loggers deployed in the enterprise network.
device	A device is a named event source, consisting of an IP address or hostname and a receiver name.
device group	A grouping of devices—device groups facilitate management of devices within the TOE. For example, device groups can be associated with storage rules.
event	A record of security-sensitive activity occurring on a device in an IT system.

Kubernetes	An open-source system for automating deployment, scaling and management of containerized applications.
IDS data	Refers to the raw data (i.e., events) collected by the TOE from IDS entities in the IT system being monitored by the TOE.
IDS	Intrusion Detection System—an application or device that monitors an IT system for malicious activities or policy violations and generates records of its findings.
IT system	A combination of computers, network infrastructure devices, cables, etc.
Logger	The component of the TOE that provides search, retrieval, and reporting capabilities for collected IDS data.
receiver	The Logger mechanism used to receive IDS data from SmartConnectors and event sources in the IT system.
SmartConnectors	TOE components that collect raw events from devices throughout the enterprise network, process them into ArcSight security events, and transmit them to destination devices, including Logger.
storage group	A Logger mechanism for grouping stored events with a shared retention policy, defined in terms of size (Allocation) and days (Maximum Age).
storage rule	A mapping between a device group and a storage group that enables storing of events from specific sources in specific storage groups.

1.5 Abbreviations and Acronyms

The following abbreviations and acronyms are used in this ST:

ADP	Micro Focus ArcSight Data Platform
API	Application Programming Interface
CC	Common Criteria
CEF	Common Event Format
DN	Distinguished Name—unique identifier of an entry in an X.500 directory
DNS	Domain Name System
DoS	Denial of Service
EAL	Evaluation Assurance Level
EPS	Events Per Second
ESM	Enterprise Security Management
GUI	Graphical User Interface
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IT	Information Technology
JBOD	Just a Bunch of Disks/Drives—an architecture using multiple hard drives exposed as individual devices
LDAP	Lightweight Directory Access Protocol
LVM	Logical Volume Management
NTP	Network Time Protocol
RADIUS	Remote Authentication Dial-In User Service
RAID	Redundant Array of Independent Disks
REST	Representational state transfer—a way of providing interoperability between computer systems on the Internet
SAR	Security Assurance Requirement

SFP	Security Function Policy
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol—a protocol specification for exchanging structured information in the implementation of web services
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Function
UDP	User Datagram Protocol
VPN	Virtual Private Network

2. TOE Description

2.1 Overview

The TOE, Micro Focus ArcSight Data Platform (ADP) 2.11, comprises data collection and storage engine functionality that unifies log data collection, storage, and security data management in a scalable, high-performance software or appliance solution.

2.2 Architecture

The TOE consists of the following components:

- ArcSight Management Center (ArcMC)
- ArcSight Logger
- ArcSight Data Platform (ADP) Event Broker
- ArcSight SmartConnectors, specifically:
    - Syslog NG Daemon
    - Microsoft Windows Event Log – Native (WINC).

SmartConnectors collect raw events from devices throughout the enterprise network, process them into ArcSight security events, and transmit them to destination devices, including ArcSight Logger and ADP Event Broker. Logger receives and stores events from SmartConnectors directly or via subscription to ADP Event Broker. Logger can also receive syslog messages and read events from text log files on remote hosts. Logger provides search, retrieval, and reporting capabilities for collected IDS data and can optionally forward selected events (e.g., to ArcSight ESM). ArcMC provides the ability to centrally manage the SmartConnectors, Loggers and Event Brokers deployed in the enterprise network.

The following figure illustrates how the TOE components can be deployed in a network. Note that communications between the TOE components are protected using TLS. In addition, although SmartConnectors collecting from IDS and firewall devices are depicted, only the Syslog NG Daemon and the Microsoft Windows Event Log – Native (WINC) SmartConnectors are formally included in the scope of the evaluation.

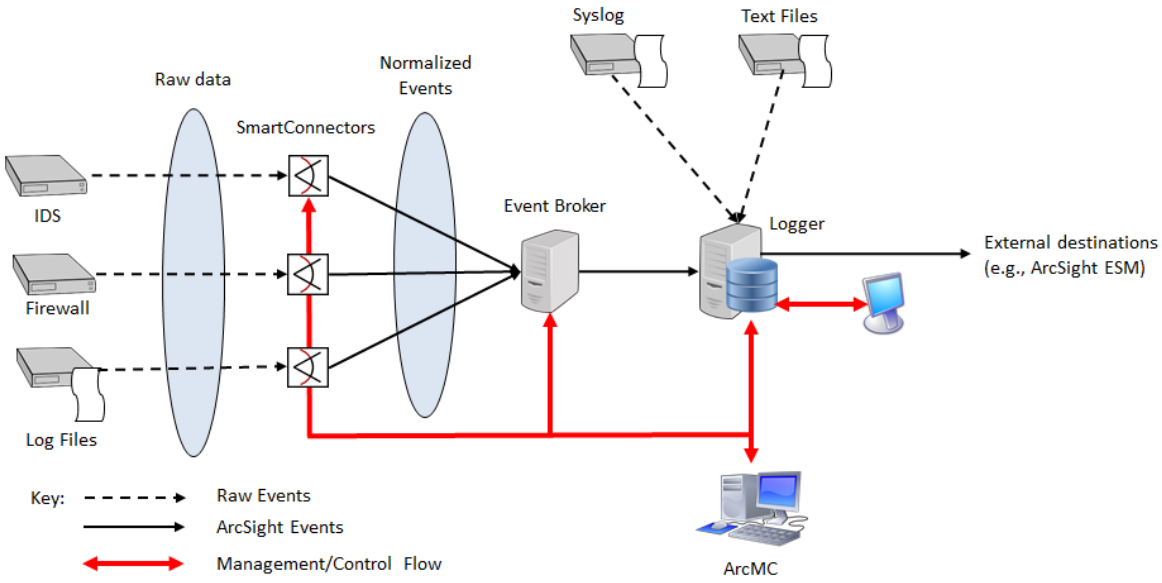

Figure 1: Example TOE Deployment

2.2.1 ArcSight Management Center

The ArcSight Management Center (ArcMC) is a centralized management tool that supports security policy configuration, deployment maintenance, and monitoring. It provides a single management interface to administer ArcSight managed nodes, including Loggers, SmartConnectors, Event Brokers, and other ArcMCs

ArcMC provides a browser-based graphical user interface (GUI) that enables ArcMC users to access the following functional capabilities:

- Manage the following node types:
  - SmartConnectors
  - Hardware or Software Loggers
  - Event Brokers
  - ArcSight Management Centers
- Create and manage node configurations
- View status of all nodes being managed
- Manage users across all managed nodes
- Administer ArcMC itself
- View statistics of total Events Per Second (EPS) in and out from all managed connectors.

2.2.2 ArcSight Logger

ArcSight Logger is a log management solution designed to handle high event throughput, support data analysis, and provide efficient long-term storage. Logger receives and stores events, supports search, retrieval, and reporting, and can optionally forward selected events (e.g., to ArcSight ESM).

Logger receives structured data in the form of normalized Common Event Format (CEF) events and unstructured data, such as syslog events. The file-type receivers configured on Logger only parse event time from an event. Although Logger is message-agnostic, it can do more with CEF.

Logger provides a browser-based GUI that enables Logger users to access the following functional capabilities:

- Manage IDS data (event) storage
- Manage receivers for collecting IDS data (events) from SmartConnectors, syslog over UDP or TCP, and text files
- Search and review collected IDS data
- Manage alerts
- Manage reports
- Manage IDS data (event) archiving
- Manage Logger users.

Logger also provides a Web Services Application Programming Interface (API) that exposes Logger functions as Web services. This enables Logger functionality to be integrated into other ArcSight products and third party applications. Capabilities provided by the Web Services API include executing searches on stored Logger events, running Logger reports, and feeding Logger reports back to the third party application. The Web Services API supports both SOAP-based and REST-based Web services.

Logger is available in two form factors—an appliance and software. The appliance-based solution is a hardened, dedicated, enterprise-class system that is optimized for extremely high event throughput, efficient long-term storage, and rapid data analysis. The software-based solution is similar in feature and functionality to the appliance-based solution, enabling the end customer to install ArcSight Logger on a supported platform of the customer's choice.

Multiple Loggers can work together to scale up to support extremely high event volume with search queries distributed across all Loggers.

2.2.3 ArcSight Data Platform (ADP) Event Broker

The ADP Event Broker centralizes event processing, enabling integration of ArcSight events to third party solutions. It enables scalable, high-throughput, multi-broker clusters for publishing and subscribing to event data.

The ADP Event Broker provides a packaged version of Apache Kafka. The Event Broker Kafka broker (or cluster of brokers) allows for the use of SmartConnectors to publish data, and to subscribe to that data with Logger, ArcSight ESM, ArcSight Investigate, Apache Hadoop, and/or a third party consumer. Event Broker utilizes Apache Flume as a data transfer channel to transfer events from Event Broker to Apache Hadoop or other storage systems. ArcSight ESM, ArcSight Investigate, Apache Hadoop and any third party consumers are considered to be in the operational environment and are not part of the TOE.

Administrators can manage topic routing and the Event Broker infrastructure through ArcMC. Additionally, Event Broker provides the Event Broker Manager (a version of Yahoo Kafka Manager) to monitor and manage Event Broker's Kafka services.

In the evaluated configuration, ADP Event Broker acts as a pipe or conduit between SmartConnectors and Logger, and provides support for clients and brokers to communicate securely over Transport Layer Security (TLS) using a dedicated port.

2.2.4 ArcSight SmartConnectors

ArcSight SmartConnectors collect and process events generated by devices throughout an enterprise. The devices are considered part of the environment in which the TOE operates. Devices can be routers, e-mail logs, anti-virus products, firewalls, Intrusion Detection Systems, access control servers, VPN systems, anti-DoS appliances, operating system logs, and other sources where information of security threats are detected and reported.

SmartConnectors are specifically developed to work with network and security products using multiple techniques, including simple log forwarding and parsing, direct installation on native devices, SNMP, and syslog.

The following specific SmartConnectors were tested as part of the evaluated configuration:

- Syslog NG Daemon—can collect syslog records from Syslog NG Daemon, an open source implementation of the syslog protocol for UNIX and UNIX-like systems that extends the original `syslogd` model and adds such features as support for the IETF Standard (RFC 5424) syslog header and TLS for secure communication
- Microsoft Windows Event Log – Native (WINC)—collects Windows Event Log events.

Other SmartConnectors may be deployed in an evaluated configuration, but no conclusions should be drawn regarding the efficacy of their event collection functionality.

2.3 Physical Boundaries

2.3.1 Physical TOE Components

The ArcSight Management Center (ArcMC) is a software component provided in the following form:

- `ArcSight-ArcMC-2.6.0.2005.bin` file, the installer file for ArcMC.

The Logger component is provisioned in the following form factors:

- `ArcSight-logger-6.4.0.8117.0.bin` file, the installer file for the Logger software form factor
- Logger L7600 series appliance with Logger 6.4 installed.

The ADP Event Broker is a software component provided in the following forms:

- `Arcsight_eb_images_17_4c2a6ccc0a553390488ceb56aeb1126c607fa293.tar` file, the offline installer file for Event Broker
- `Arcsight-installer-1.0.1-19.rc.x86_64.rpm`, the online installer file for Event Broker.

SmartConnectors are provisioned in a single installer file from which the desired SmartConnectors are selected and installed. The following SmartConnector installers are available for the relevant supported platforms:

- `ArcSight-7.6.0.8009.0-Connector-Win64.exe`
- `ArcSight-7.6.0.8009.0-Connector-Linux.bin`.

2.3.2 Operational Environment Components

ArcMC can be installed on Red Hat Enterprise Linux (RHEL) 6.8 or 7.3 and CentOS 6.8 or 7.3. The following browsers are supported for accessing ArcMC:

- Internet Explorer 11
- Microsoft Edge (latest version)
- Firefox ESR (latest version)
- Google Chrome (latest version).

The software Logger is supported on 64-bit RHEL 6.8 or 7.3, 64-bit CentOS 6.8 or 7.3, and as a virtual appliance on VMware ESXi server v5.5. Minimum recommended requirements for software Logger in these environments are as follows:

- software Logger installed on 64-bit RHEL or 64-bit CentOS:
    - CPU: 2 x Intel Xeon Quad Core or equivalent
    - Memory: 12–24 GB (24 GB recommended)
    - Disk Space: 65 GB (minimum) in the software Logger installation directory
    - Root partition: 40 GB (minimum)
    - Temp directory: 1 GB
- virtual appliance Logger installed on VMware ESXi server (the VM image includes the Logger installer on a 64-bit CentOS 7.3 configured with 12 GB RAM and four physical and eight logical cores):
    - CPU: 1 or 2 x Intel Xeon Quad Core or equivalent
    - Memory: 4–12 GB (12 GB recommended)
    - Disk Space: 10 GB (minimum) in the Logger installation directory
    - Temp directory: 1 GB

The following browsers are supported for accessing the Logger GUI (both the software and appliance form factors):

- Internet Explorer 11
- Microsoft Edge (latest version)
- Firefox 41 and 38.3.0 ESR
- Google Chrome (latest version).

The Event Broker is supported on 64-bit RHEL 7.3 and 64-bit CentOS 7.3. Event Broker is installed and deployed by the ArcSight Installer application using Kubernetes container management to enable elastic scaling. The Kubernetes master node controller resides on one system/node. A Kubernetes worker node hosts container management units called pods. A pod manages one or more containers with a shared namespace and shared volumes. Event Broker requires an Apache ZooKeeper ensemble and a Kafka cluster to be configured—ZooKeeper and Kafka are installed as part of the Event Broker installation. The Event Broker cluster must have an odd number of nodes and MICRO FOCUS recommends a minimum of three nodes in a production environment. ZooKeeper runs on these nodes, which should be dedicated to the Event Broker, as high throughput and low latency are required.

Minimum recommended requirements for the nodes in the Event Broker cluster are as follows:

- Minimum 10-Gigabit Ethernet, with full-speed interconnects between all nodes in the cluster. These must be reachable from all consumers and producers.
- All machines involved in the Event Broker (nodes, consumers, producers) must have forward and reverse DNS entries.
- For each server node:
  - 8-core 64-bit server-grade processor
  - 32 GB RAM
  - 8 or more TB of disk space, depending on how long data should be retained and expected throughput, sourced from at least 2 disks, using either hardware RAID or LVM to create a JBOD or striped array.

The following browsers are supported for accessing the Event Broker Manager GUI:

- Internet Explorer 11
- Microsoft Edge (latest version)
- Firefox 41 and 38.3.0 ESR
- Google Chrome (latest version)
- Safari 9.0.1 (OS X 10.9).

SmartConnectors are supported[1] on the operating systems and hardware processors listed in the following table. Note that individual SmartConnectors run only on the platforms that are useful for the connector type and specific device type. For example, the SmartConnector for Microsoft Windows Event Log runs on Windows platforms only. Each SmartConnector has its own specific configuration guide that provides connector-specific platform requirements and installation information.

Operating System	Hardware Platform
CentOS Linux 6.5, 6.6, 6.7, 6.8, 7.0, 7.1 and 7.2 64-bit	x86_64
CentOS Linux 6.9 and 7.3 64-bit	x86_64 (Certified)
Microsoft Windows Server 2008 SP1/SP2 32-bit	x86
Microsoft Windows Server 2008 SP1/SP2 64-bit	x86_64
Microsoft Windows Server 2008 R2 and 2008 R2 SP1 64-bit	x86_64
Microsoft Windows Server 2012 Standard and 2012 R2 64-bit	x86_64 (Certified)
Microsoft Windows Server 2016 Standard 64-bit	X86_64 (Certified)
Red Hat Enterprise Linux (RHEL) 6.5, 6.6, 6.7, 6.8, 7.0, 7.1 and 7.2 64-bit	x86_64
Red Hat Enterprise Linux (RHEL) 6.9 and 7.3 64-bit	x86_64 (Certified)
SUSE Linux 11 Enterprise Server 64-bit	x86_64
Oracle Solaris 10 64-bit	SPARC
Oracle Solaris 11 64-bit	SPARC (Certified)
Oracle Solaris 11 64-bit	x86_64 (Certified)

Table 1: Supported SmartConnector Environments

[1] "Supported" means that the platform has been sanity-tested by Micro Focus at a minimum. Micro Focus ArcSight will accept support calls and address bugs on the platform. Platforms marked as "Certified" have been tested and certified with regression tests with the 7.6.0 SmartConnector release by Micro Focus.

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

- IDS resources in the IT system monitored by the TOE generating IDS data (events) to be collected by the TOE's SmartConnectors
- SMTP Server to support e-mail notifications. POP3 and IMAP can be used to check for e-mail acknowledgments

The following components are also supported in the operational environment of the TOE, but are not required for the evaluated configuration:

- LDAP or RADIUS server to support user authentication
- NTP server to provide time synchronization to TOE appliances or hosting platforms
- ArcSight Load Balancer, which provides a "connector-smart" load balancing mechanism by monitoring the status and managing the load of SmartConnectors
- ArcSight ESM instances that can subscribe to the Event Broker component and can receive events and alert notifications from the Logger component of ADP
- Other non-TOE subscribers of Event Broker, including ArcSight Investigate, Apache Hadoop, and/or a third party consumer.

2.4 Logical Boundaries

This section summarizes the security functions provided by the TOE.

2.4.1 Audit

Both the ArcMC and Logger components of the TOE are able to generate and store audit records of security-relevant events. The stored audit records are protected from unauthorized modification and deletion. Audit records generated by ArcMC can be viewed only by users in the ArcMC Default System Admin or ArcMC Read Only System Admin roles, while audit records generated by Logger can be viewed only by users in the Logger System Admin or Logger Read Only System Admin roles. Both ArcMC and Logger provide the authorized roles with capabilities to review the generated audit records, including capabilities for selecting audit records based on date and time range and, optionally, subject identity and outcome, and ordering the selected records based on date and time, the subject associated with the audit event, and the type of audit 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. The TOE supports both passwords and certificates for authentication and users can be configured for password-only, certificate-only, or password and certificate-based authentication. The TOE additionally supports external LDAP and RADIUS authentication servers. 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 15 minutes. The TOE requires users to provide unique identification and authentication data before any administrative access to the TOE via the ArcMC GUI or Logger GUI is granted.

2.4.3 Security Management

The ArcMC component provides authorized ArcMC users with a GUI that can be used to configure and manage ArcMC security functions and TSF data, depending on the security management groups (or roles) a user is assigned. ArcMC supports the following security management groups: Default System Admin Group; Read Only System Admin Group; Default ArcMC Rights Group; and Read Only ArcMC Group.

The Logger component provides authorized Logger users with a GUI that can be used to configure and manage Logger security functions and TSF data, depending on the security management roles assigned to the user. Logger

supports the following security management roles: Logger System Admin; Logger Read Only System Admin; Logger Rights; Logger Search; and Logger Reports.

The Event Broker component provides the Event Broker Manager to support administration of the Event Broker. The Event Broker Manager can be accessed only by users that can log on to the Event Broker server, part of the operational environment of the TOE.

2.4.4 Protection of the TSF

Communications between distributed components of the TOE (i.e., ArcMC, Loggers, Event Broker, and SmartConnectors) occur over TLS, which provides confidentiality and integrity of transmitted data.

Appliance-based Logger components maintain time internally and use this internal time as the source for reliable timestamps. In addition, they can be configured to synchronize their clocks with external NTP servers. Software-based TOE components use the system clock maintained by the underlying operating system as the source for date and time information.

2.4.5 TOE Access

The TOE enforces a limit on the number of simultaneous active sessions for each user account. The maximum number is configurable by an administrator and has a default value of 15.

The TOE will terminate interactive sessions after a period of inactivity configurable by an administrator. The TOE also allows user-initiated termination of the user's own interactive session by explicitly logging off.

The TOE displays a banner message on the user login page. The content of the message can be configured by an administrator.

2.4.6 Trusted Path/Channels

The TOE provides a trusted channel to communicate securely with external ArcSight ESM destinations. The trusted channel is implemented using HTTPS (i.e., HTTP over TLS).

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 ArcMC GUI and Logger GUI. 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.

2.4.7 Intrusion Detection System

The TOE collects IDS data generated by devices in the IT system it is monitoring. The Logger component receives and stores events from SmartConnectors (directly or via the Event Broker), syslog, and text files. SmartConnectors collect raw events generated by devices in the operational environment, normalize them, process them into ArcSight security events, and transmit them to the Logger component (directly or via the Event Broker). The Logger component provides the repository for storing collected IDS data and capabilities for managing IDS data storage.

The TOE provides capabilities to search stored IDS data (events) using queries. Queries can be simple search terms or they can be complex enough to match events that include multiple IP addresses or ports, and that occurred between specific time ranges from a specific storage group.

The TOE provides capabilities to define queries that can trigger alerts if specified conditions are met.

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 software component is relied on to protect the component and its configuration from unauthorized access.
- The underlying operating system of each TOE software component is relied on to provide a reliable date and time stamp for use by the TOE.

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:

- Connector Hosting Appliances (also referred to as ArcMC appliances)
- Micro Focus ArcSight FlexConnectors
- Micro Focus ArcSight Load Balancer.

2.7 TOE Documentation

This section identifies the guidance documentation included in the TOE. **Note: All Hewlett Packard Enterprise (HPE) guidance documentation is effectively in process of being renamed to Micro Focus.** The contents of the documents are unaffected by the naming change.

The documentation comprises:

- HPE Security ArcSight Logger Installation and Configuration Guide, Software Version 6.4, April 14, 2017
- HPE Security ArcSight Logger Administrator's Guide, Software Version 6.4, April 14, 2017
- HPE Security ArcSight Logger Web Services API Guide, Software Version 6.4, April 14, 2017
- HPE Security ArcSight Logger Release Notes, Software Version 6.4, April 14, 2017
- HPE Security ArcSight ArcSight Data Platform Support Matrix, April 21, 2017
- HPE ArcSight Management Center Administrator's Guide, Software Version: 2.6, April 14, 2017
- HPE ArcSight Management Center Release Notes, Software Version 2.6, April15, 2017
- HPE Security ArcSight Data Platform Event Broker Deployment Guide, Software Version 2.01, September 29, 2017
- HPE Security ArcSight Data Platform Event Broker Administrator's Guide, Software Version: 2.01, June 13, 2017
- HPE Security ArcSight Data Platform Event Broker Release Notes, Software Version 2.01, June 13, 2017
- HPE Security ArcSight Connectors SmartConnector User Guide, May 15, 2017
- HPE Security ArcSight SmartConnectors SmartConnector for Microsoft Windows Event Log—Native Configuration Guide, May 15, 2017
- HPE Security ArcSight Connectors SmartConnector for Syslog NG Daemon Configuration Guide, May 15, 2017
- HPE Security ArcSight Connectors SmartConnector Release Notes 7.6.0.8009.0, May 15, 2017
- Common Criteria Evaluated Configuration Guide – ArcSight Data Platform (ADP) 2.11, Version 1.3, September 29, 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 software 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.INAPPROPRIATE_USE	Authorized users perform inappropriate actions on the TOE due to ignorance of their responsibilities or operational policies and procedures.
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	An unauthorized user may monitor the enterprise network in an attempt to obtain sensitive data, such as passwords, or to modify transmitted data.
T.NO_ACCOUNTABILITY	Authorized users of the TOE perform adverse actions on the TOE, or attempt to perform unauthorized actions, which go undetected.
T.UNATTENDED_SESSION	An unauthorized user gains access to the TOE via an unattended authorized user session.
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.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 require all users of the TOE to be identified and authenticated before gaining access to TOE services.
O.IDS_ALERT	The TOE shall provide capabilities to generate alerts based on results from IDS data searches.
O.IDS_COLLECT	The TOE shall provide capabilities to collect IDS data from IDS entities in the IT system it monitors.
O.IDS_REVIEW	The TOE shall provide capabilities for effective review of stored IDS data.
O.LOGON_BANNER	The TOE shall be able to display a configurable advisory warning message to potential users pertaining to appropriate use of the TOE.
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 its distributed components and between itself and external entities.
O.SECURITY_MANAGEMENT	The TOE shall restrict the ability to perform security management functions on the TOE to authorized administrators having appropriate privileges.
O.SESSION_LIMITS	The TOE shall provide capabilities to restrict the number of concurrent interactive sessions belonging to the same user.
O.SESSION_TERMINATION	The TOE shall provide mechanisms to terminate a user session after a period of inactivity or at the request of the user.
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 software component will protect the component and its configuration from unauthorized access.

OE.TIME	The underlying operating system of each TOE software component 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 specifically to address the nature of IDS data and specify requirements for: collecting IDS data from IT systems in a variety of forms; securely storing IDS data; searching and reviewing stored IDS data; and generating alerts if IDS data meet specified criteria. The FAU (Security audit) class defined in CC Part 2 was used as a model for creating these requirements.

5.1.1.1 IDS Data Collection (IDS_IDC)

This family defines requirements for being able to collect IDS data from external IT systems in a variety of forms.

Management: IDS_IDC.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_IDC.1

There are no auditable events foreseen.

IDS_IDC.1 – IDS data collection

Hierarchical to: No other components.

Dependencies: None

IDS_IDC.1.1 The TSF shall be able to collect IDS data from external IT systems in the following forms: **[selection:** ***syslog*****,** ***Windows Event Log*****,** ***text file*****,** ***SNMP*****,** ***database schema*****,** ***XML*****, [assignment:** ***other specifically defined forms*****]]**.

5.1.1.2 IDS Alert and Response (IDS_ARP)

This family defines how the TSF is to respond when it detects events matching specified criteria.

Management: IDS_ARP.1

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

a) maintenance of the parameters that control event alerting and response.

Audit: IDS_ARP.1

There are no auditable events foreseen.

IDS_ARP.1 – Alert definition and reaction

Hierarchical to: No other components.

Dependencies: IDS_IDC.1 – IDS data collection

IDS_ARP.1.1 The TSF shall be able to trigger an alert when [**assignment:** ***set of conditions***] are met.

IDS_ARP.1.2 The TSF shall send a notification to **[assignment:** ***alert destination*****]** when an alert is triggered.

Application Note: *The ST author specifies the set of conditions that constitute an alert in the context of the TOE and specifies the possible destinations for sending an alert notification the TOE supports.*

5.1.1.3 IDS Data Review (IDS_IDR)

This family defines requirements for reviewing IDS data.

Management: IDS_IDR.1

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

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

Management: IDS_IDR.2

There are no management actions foreseen.

Audit: IDS_IDR.1, IDS_IDR.2

There are no auditable events foreseen.

IDS_IDR.1 – Controlled data review

Hierarchical to: No other components.

Dependencies: IDS_IDC.1 – IDS data collection

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

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

IDS_IDR.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.*

IDS_IDR.2 – Selectable data review

Hierarchical to: No other components.

Dependencies: IDS_IDR.1 – Controlled data review

IDS_IDR.2.1 The TSF shall provide the ability to apply [**assignment: *methods of selection and/or ordering***] of IDS data based on [**assignment: *criteria with logical relations***].

5.1.1.4 IDS Data Storage (IDS_STG)

This family defines requirements for securely storing IDS data.

Management: IDS_STG.1

There are no management actions foreseen.

Management: IDS_STG.2

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

a) maintenance of the parameters that define storage limits.

Audit: IDS_STG.1, IDS_STG.2

There are no auditable events foreseen.

IDS_STG.1 – Protected IDS data storage

Hierarchical to: No other components.

Dependencies: IDS_IDC.1 – IDS data collection

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

IDS_STG.1.2 The TSF shall be able to [**selection, choose one of: *prevent*, *detect***] unauthorized modifications to stored IDS data.

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

Hierarchical to: No other components.

Dependencies: IDS_STG.1 – Protected IDS data storage

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

Application Note: *The ST author specifies the actions the TOE takes if the storage capacity has been reached. Anything that causes the TOE to stop collecting IDS data may not be the best solution, as this will only affect the TOE and not the IT resource(s) the TOE is monitoring, leaving those resources potentially open to intrusion.*

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.2: User authentication before any action
	FIA_UAU.5: Multiple authentication mechanisms
	FIA_UAU.6: Re-authenticating
	FIA_UID.2: User identification before any action
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
	FPT_STM.1: Reliable time stamps
FTA: TOE Access	FTA_MCS.1: Basic limitation on multiple concurrent sessions
	FTA_SSL.3: TSF-initiated termination
	FTA_SSL.4: User-initiated termination
	FTA_TAB.1: Default TOE access banners
FTP: Trusted Path/Channels	FTP_ITC.1: Inter-TSF trusted channel
	FTP_TRP.1: Trusted path
IDS: Intrusion Detection System	IDS_IDC.1: IDS data collection
	IDS_ARP.1: Alert definition and reaction

Requirement Class	Requirement Component
	IDS_IDR.1: Controlled data review
	IDS_IDR.2: Selectable data review
	IDS_STG.1: Protected IDS data storage
	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:**

- **All use of the user identification mechanism**
- **All use of the user authentication 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**
- **Modifications to the group of users that are part of a role**
- **Termination of an inactive user session by the TSF**
- **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(1) The TSF shall provide [**Default System Admin, Read Only System Admin**] with the capability to read [**all ArcMC-generated audit information**] from the audit records.

FAU_SAR.1.2(1) The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.1.1(2) The TSF shall provide [**Logger System Admin, Logger Read Only System Admin**] with the capability to read [**all Logger-generated audit information**] from the audit records.

FAU_SAR.1.2(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 [**selection and ordering**] of audit data based on [**the following criteria:**

- **Selection based on date and time range and, optionally, subject identity and outcome**
- **Ordering based on date and time, subject identity, or type of 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 [***3***] 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 for an administrator configurable period of time**].

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**
- **User Group membership**
- **Email 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**
- **Minimum number of numeric characters**
- **Minimum number of uppercase characters**
- **Minimum number of lowercase characters**
- **Minimum number of special characters**].

FIA_UAU.2 – User authentication before any action

FIA_UAU.2.1 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, LDAP, RADIUS**] 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**
  - **Certificate-based**
  - **Password-based and certificate-based**
  - **LDAP-based**
  - **RADIUS-based**
- **Users configured for "password-based and certificate-based" must satisfy the authentication requirements of both mechanisms in order to be successfully authenticated**].

FIA_UAU.6 – re-authenticating

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions [**user changes own password**].

FIA_UID.2 – User identification before any action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.2.3 Security Management (FMT)

FMT_MOF.1 – Management of security function behaviour

FMT_MOF.1.1(1) The TSF shall restrict the ability to [***determine the behavior of, modify the behavior of***] the functions [**authentication, authentication failure handling, user session behavior**] to [**Default System Admin, Logger System Admin**].

FMT_MOF.1.1(2) The TSF shall restrict the ability to [***determine the behavior of, modify the behavior of***] the functions [**IDS data collection**] to [**Logger Rights**].

FMT_MTD.1 – Management of TSF data

FMT_MTD.1.1(1) The TSF shall restrict the ability to [***modify, delete, [create]***] the [**nodes, node configurations, node users**] to [**Default ArcMC Rights**].

FMT_MTD.1.1(2) The TSF shall restrict the ability to [***[create]***] the [**storage groups**] to [**user with both Logger System Admin and Logger Rights**].

FMT_MTD.1.1(3) The TSF shall restrict the ability to [***modify***] the [**retention policies**] to [**Logger Rights**].

FMT_MTD.1.1(4) The TSF shall restrict the ability to [***modify, delete, [create]***] the [**event archives, alerts, alert notifications**] to [**Logger Rights**].

FMT_MTD.1.1(5) The TSF shall restrict the ability to [***query, [create, schedule, run, publish]***] the [**reports**] to [**Logger Reports**].

FMT_MTD.1.1(6) The TSF shall restrict the ability to [***modify***] the [**time, password settings, user session attributes, password of another user**] to [**Default System Admin, Logger System Admin**].

FMT_MTD.1.1(7) The TSF shall restrict the ability to [***modify, delete, [create]***] the [**TOE users**] to [**Default System Admin, Logger System Admin**].

FMT_SMF.1 – Specification of Management Functions

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

- **Manage nodes**
- **Manage node configurations**
- **Manage node users**
- **Manage IDS data collection**
- **Manage IDS data storage**
- **Manage IDS data archiving**
- **Manage alerts**
- **Manage reports**
- **Manage time**
- **Manage TOE users**
- **Manage password settings**
- **Manage authentication function**
- **Manage authentication failure handling**
- **Manage user session attributes**
- **Manage user session behavior**
- **Reset user password**].

FMT_SMR.1 – Security roles

FMT_SMR.1.1 The TSF shall maintain the roles: [

- **Default System Admin**
- **Read Only System Admin**
- **Default ArcMC Rights**
- **Logger System Admin**
- **Logger Read Only System Admin**

- **Logger Rights**
- **Logger Search**
- **Logger Reports**].

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.

FPT_STM.1 – Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

5.2.5 TOE Access (FTA)

FTA_MCS.1 – Basic limitation on multiple concurrent sessions

FTA_MCS.1.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same user.

FTA_MCS.1.2 The TSF shall enforce, by default, a limit of [**15**] sessions per user.

FTA_SSL.3 – TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [**time interval of user inactivity configured by an authorized administrator**].

FTA_SSL.4 – TSF-initiated termination

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

FTA_TAB.1 – Default TOE access banners

FTA_TAB.1.1 Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorized use of the TOE.

5.2.6 Trusted Path/Channels (FTP)

FTP_ITC.1 –Inter-TSF trusted channel

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

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

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [**transmission of events and alert notifications to an ArcSight ESM destination**].

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 [***modification***, ***disclosure***].

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_ARP.1 – Alert definition and reaction

IDS_ARP.1.1 The TSF shall be able to trigger an alert when [**the following conditions:**

- **A specified number of matches against a search query occur within a specified threshold (real time alert), or**
- **A specified number of matches against a search query occur within a specified threshold and time range (saved search alert)**

] are met.

IDS_ARP.1.2 The TSF shall send a notification to **[configured notification destinations, which can be:**

- **E-mail address**
- **SNMP server**
- **syslog server**
- **ArcSight Manager**

] when an alert is triggered.

IDS_IDC.1 – IDS data collection

IDS_IDC.1.1 The TSF shall be able to collect IDS data from external IT systems in the following forms: [***syslog***, ***Windows Event Log***, ***text file***].

IDS_IDR.1 – Controlled data review

IDS_IDR.1.1 The TSF shall provide **[Logger Search]** with the capability to read **[all IDS data]** from the IDS data.

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

IDS_IDR.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_IDR.2 – Selectable data review

IDS_IDR.2.1 The TSF shall provide the ability to apply [**selection and ordering**] of IDS data based on [**the following criteria:**

- **Selection based on text searches of IDS data fields**
- **Ordering based on receipt time and sort criteria (oldest first or newest first)].**

IDS_STG.1 – Protected IDS data storage

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

IDS_STG.1.2 The TSF shall be able to [***prevent***] unauthorized modifications to stored IDS data.

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

IDS_STG.2.1 The TSF shall **[delete the oldest stored IDS data in a storage group]** if the stored IDS data exceeds [**the configured retention policy of the storage group**].

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

Requirement Class	Requirement Component
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
- TOE Access
- Trusted Path/Channels
- Intrusion Detection System.

6.1 Security Audit

Both the ArcMC and the Logger components of the TOE generate audit records.

The ArcMC component generates the following types of audit event:

- Application events—related to ArcMC functions and configuration changes
- Platform events—related to the ArcMC system
- System health events—related to ArcMC health.

The Logger component generates the following types of audit event:

- Application events—related to Logger functions and configuration changes
- Platform events—related to the Logger hardware (for Logger appliance) or underlying operating system (for Logger software).

Both the ArcMC and the Logger components can generate audit records of the following security-relevant events:

- All use of the authentication mechanism
- All use of the user identification mechanism
- All modifications in the behavior of the functions of the TSF
- All modifications to the values of TSF data
- Modifications to the group of users that are part of a role
- Termination of an inactive user session by the TSF
- Termination of a user's interactive session by the user.

Note that the audit function automatically starts at system start-up and shuts down only at system shutdown—there is no capability to otherwise shut down or start up the audit function. As such, the requirement to audit start-up and shutdown of the audit function is satisfied vacuously because there is no startup or shutdown of the audit function to be audited.

All 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 manner in which the TOE is able to provide a reliable time stamp for audit records is described in Section 6.4 below.

The ArcMC GUI provides users in the Default System Admin and Read Only System Admin roles the ability to view the audit events generated by ArcMC. The GUI provides the capability to search the stored audit records based on

date and time range, user identity, and event description. Displayed audit records can be ordered based on date and time, subject identity, or type of event.

The Logger GUI provides users in the Logger System Admin and Logger Read Only System Admin roles the ability to view the audit events generated by Logger. The GUI provides the capability to search the stored audit records based on date and time range, user identity, and event description. Displayed audit records can be ordered based on date and time, subject identity, or type of event.

The audit events generated by ArcMC are stored in a PostgreSQL database that is installed along with ArcMC. The ArcMC GUI does not provide any interface or mechanism to modify or delete the audit records stored in the database.

The audit events generated by the Logger component are stored in the Logger Internal Storage Group. As such, they are handled in the same manner as IDS data (events) and the capabilities for viewing and searching events can equally be used to view and sort Logger audit records—see Section 6.7.3 below for further details. The manner in which Logger audit records are stored is described in Section 6.7.2.

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_GEN.2—the TOE associates each auditable event resulting from actions of identified users with the identity of the user that caused the event.
- FAU_SAR.1(*)—the TOE provides authorized users with the capability to read 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 select audit data for review based on date and time range, and optionally on subject identity and outcome, and to order the selected audit data based on date and time, subject identity, or type of event.
- FAU_STG.1—the TOE protects stored audit records from unauthorized modification and deletion.

6.2 Identification and Authentication

The Identification and Authentication security function is implemented on both the ArcMC component and the Logger component of the TOE. The implementation of the security function and its mechanisms is essentially the same on both components. In particular, the security functional requirements are satisfied identically on both components. As such, no further distinction between them is made here.

The TOE maintains accounts of its authorized users. A user account includes the following attributes associated with the user: user identity; authentication data; user group memberships (which define the user's security management role); email address.

In order to access the functions provided by the TOE via either the ArcMC GUI or the Logger GUI, the user must first be identified and authenticated. The TOE supports the following user authentication methods:

- Local password-based authentication—as part of the login process, the user submits a password that must match the password associated with the user account
- Certificate-based authentication—the user is authenticated by a digital certificate matching the user identity
- Local 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
- External authentication using LDAP—the user supplies a login name and password. The login name is mapped to the DN for that user (stored in the local database) and the DN and user password are used to authenticate to the LDAP server

- External authentication using RADIUS—the user is authenticated by a (RADIUS) password matching the submitted user name.

When the TOE is configured for local password-based authentication, users are able to change their own passwords. In order to do so, they must re-authenticate their identity by providing their current password along with the desired new password, which is entered twice as a form of verification. The TOE can be configured to enforce the following restrictions on passwords used for local password-based authentication:

- Minimum length
- Minimum number of numeric characters
- Minimum number of uppercase characters
- Minimum number of lowercase characters
- Minimum number of special characters.

To login to the TOE, the user provides the login name and associated authentication data. If either the login name or the authentication data is incorrect, the login request fails and no administrator functions are made available. As a result of a successful login, the interactive session is established and the administrator functions appropriate to the user's assigned roles are made available. The TOE can be configured to disable a user account for a specified time period after a specified number of consecutive authentication failures. The default maximum number of consecutive failed login attempts is three, while the default lockout period is 15 minutes.

Logger also provides a Web Services Application Programming Interface (API) that exposes Logger functions as Web services. The Web Services API supports both SOAP-based and REST-based Web services. The Web Services API is accessed using the Login Service, which requires the requestor to submit a user name for an existing Logger account and the associated password. The Login Service authenticates the claimed user identity, logs the user into Logger, and establishes a session ID to use when making subsequent API calls.

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 for a specified time period as configured by authorized administrator.
- FIA_ATD.1—the TOE maintains the following security attributes associated with each user: user identity; authentication data; user group memberships, email 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.2—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 multiple authentication mechanisms: local password; certificate; LDAP; and RADIUS.
- FIA_UAU.6—the TOE requires each user to re-authenticate prior to allowing the user to change their own password.
- FIA_UID.2—the TOE requires each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.3 Security Management

The Security Management security function is implemented partially on the ArcMC component of the TOE and partially on the Logger component.

ArcMC provides a browser-based GUI that enables ArcMC users to access the following security management functions:

- Manage nodes—a node is a networked ArcSight product that can be centrally managed by ArcMC. Each node is associated with a single networked host that has been assigned a hostname, IP address, or both. ArcMC can be used to manage the following node types: SmartConnectors; Loggers; Event Brokers; and other ArcMCs. ArcMC can be used to perform the following node management tasks:
    - View managed nodes by location, by host, or by node type
    - Add, view, edit, and delete locations for hosts
    - Add nodes from a host, import hosts from a CSV file, view and delete hosts, view all hosts in a location, update software on hosts, move hosts to different locations, and scan hosts for new connectors or containers
- Create and manage node configurations—a configuration is a group of related appliance or software settings and their associated values, which applies to one or more node types. A configuration created for a node can be pushed to nodes of the same type managed by ArcMC, assuring uniformity across a group of nodes
- View status of all nodes being managed
- Manage users across all managed nodes
- Administer ArcMC itself.

When an ArcMC administrator creates a user account, the account is created within a user group. User groups define privileges to specific functions on the system and serve to control and restrict access to those functions. The user is granted the authorizations associated with its containing user group(s) (a user can belong to more than one group). This is the mechanism for implementing security management roles. ArcMC provides the following default user groups (note that the Read Only ArcMC Group does not provide access to any of the security management functions of the TOE):

- Default System Admin Group—controls the system administration operations for ArcMC, including configuring network information, setting storage mounts, and user management
- Read Only System Admin Group—can view System Admin settings but cannot change them
- Default ArcMC Rights Group—controls the ArcSight Management Center application operations for ArcMC, including ArcMC dashboards, node management, configuration management and backup operations
- Read Only ArcMC Group—can view the tabs in the ArcMC GUI and the operations displayed on the tabs, and can perform operations such as refresh, view certificate list, and Logfu.

Logger provides a browser-based GUI that enables Logger users to access the following security management functions:

- Manage IDS data (event) storage—create storage groups, manage the size of storage groups, and manage storage group retention policies
- Manage receivers for collecting IDS data (events) from SmartConnectors, syslog over UDP or TCP, and text files—set up and manage (enable, disable, modify, delete) the receivers that will capture event data from SmartConnectors and the IT system
- Manage alerts—create and manage (enable, disable, modify, delete) alerts and alert notifications
- Manage reports—create, schedule, run, view and publish reports
- Manage IDS data (event) archiving—create, modify and delete event archives
- Manage Logger users.

As with ArcMC, Logger user groups define privileges to specific functions on Logger and serve to control and restrict access to those functions. Logger provides the following built-in security management roles:

- Logger System Admin—controls the system administration operations for Logger, such as configuring network information, setting storage mounts, and user management

- Logger Read Only System Admin—can view System Admin settings, but cannot change them
- Logger Rights—controls the Logger application operations, such as viewing the Logger dashboards and configuring all the settings in the Configuration menu, including event archives, storage groups, alerts, filters, and scheduling tasks
- Logger Search—controls local and peer searches through two privileges: search for events; search for events on remote peers. If the group is configured to allow users to run local and peer searches, users assigned to this group can perform those operations. Conversely, if the group is configured to prevent users from running local and peer searches, users assigned to this group cannot perform those operations
- Logger Reports—controls all report operations on Logger, including run, edit, delete, schedule, and view published reports.

The Security Management function satisfies the following security functional requirements:

- FMT_MOF.1(*)—the TOE is able to restrict the management of aspects of the TSF to users assigned specific administrative roles.
- FMT_MTD.1(*)—the TOE is able to restrict the management of TSF data to users assigned specific administrative roles.
- FMT_SMF.1—the TOE provides the capabilities necessary to manage the security of the TOE.
- FMT_SMR.1—the TOE defines security management roles based on the privileges assigned to user groups.

6.4 Protection of the TSF

Communications between distributed components of the TOE (i.e., ArcMC, Loggers, Event Broker and SmartConnectors) occur over TLS, which provides confidentiality and integrity of transmitted data. Confidentiality is provided through the use of AES, while integrity is provided through the use of HMAC-SHA-1 or HMAC-SHA-256 (depending on the configured ciphersuite).

More specifically, the ArcMC component communicates with Logger and other ArcMC components using HTTPS (HTTP over TLS). The Logger component communicates with peered Loggers using HTTPS, and SmartConnectors can be configured to send events to Logger over HTTPS (termed SmartMessage in the TOE guidance documentation). In addition, both SmartConnectors and Logger can be configured to communicate with Event Broker over TLS.

The appliance-based components of the TOE maintain time internally using a CMOS clock and this internal time is used as the source for reliable timestamps used by those components (e.g., for the date-time stamp recorded in audit events or for calculating interactive user session inactivity). In addition, appliance-based components of the TOE can be configured to synchronize their clocks against one or more configured NTP servers.

Software-based TOE components use the system clock maintained by the underlying operating system as the source for date and time information.

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

- FPT_ITT.1—the TOE uses TLS to protect TSF data from disclosure and modification when it is transmitted between distributed parts of the TOE.
- FPT_STM.1—the TOE is able to provide reliable time stamps, based on its own internal clock (for appliance-based components) or a time source in its operational environment. Appliance-based components can also be configured to synchronize with NTP servers.

6.5 TOE Access

The TOE Access security function is implemented on both the ArcMC component and the Logger component of the TOE. The implementation of the security function and its mechanisms is essentially the same on both components. In particular, the security functional requirements are satisfied identically on both components and management of the security function is restricted to the Default System Admin role on ArcMC and the Logger System Admin role on Logger. As such, no further distinction between them is made here.

The TOE tracks the number of simultaneous active sessions for each user account and will prevent a new active session from being established if the number of active sessions for a particular user has reached the configured maximum. Users in the System Admin role can configure the maximum number of simultaneous sessions for user accounts. By default, a single user account can have a maximum of 15 simultaneous active sessions.

The TOE can be configured to terminate an interactive user session after a specified time interval of user inactivity. Users in the System Admin role can configure the timeout value for an inactive session in terms of hours, minutes and seconds. By default, a user account is logged out after 15 minutes of inactivity.

The TOE allows user-initiated termination of the user's own interactive session by explicitly logging off.

The TOE defines a login banner that displays a message above the Username and Password fields on the login screen (i.e., prior to users completing the identification and authentication process). Users in the System Admin role can configure the content of the message and can also configure a confirmation message that the user must acknowledge (by clicking a check box on the login screen) in order to enable the Username and Password fields and proceed with login.

The TOE Access security function satisfies the following security functional requirements:

- FTA_MCS.1—the TOE restricts the maximum number of concurrent sessions that belong to the same user. The default maximum number is 15.
- FTA_SSL.3—the TOE terminates an interactive session after a time interval of user inactivity configured by an authorized administrator.
- FTA_SSL.4—the TOE allows user-initiated termination of the user's own interactive session.
- FTA_TAB.1—the TOE can be configured to display an advisory warning message regarding unauthorized use of the TOE.

6.6 Trusted Path/Channels

The TOE provides a trusted channel to communicate securely with external ArcSight ESM destinations. The trusted channel is implemented using HTTPS (i.e., HTTP over TLS). The Logger component uses the trusted channel to forward CEF events and alert notifications (see Section 6.7.4 below) to an ArcSight ESM instance. In addition, ArcSight SmartConnectors use the trusted channel to forward events to ArcSight ESM. The use of HTTPS ensures all communication over the trusted channel is protected from disclosure and modification.

The TOE provides a trusted path for administrators of the TOE to communicate with the TOE. The trusted path is implemented using HTTPS for access to the ArcMC and Logger GUIs. Administrators initiate the trusted path by establishing an HTTPS connection (using a supported web browser) to ArcMC or Logger as appropriate. 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 security function satisfies the following security functional requirements:

- FTP_ITC.1—the TOE provides a trusted channel for the TOE to transmit events and alert notifications to external ArcSight ESM destinations.
- FTP_TRP.1—the TOE provides a trusted path for administrators to communicate with the TOE, using HTTPS to access the ArcMC and Logger GUIs as appropriate.

6.7 Intrusion Detection System

6.7.1 Data Collection

The TOE collects IDS data generated by devices in the IT system it is monitoring. The Logger component receives and stores events from the following sources:

- SmartConnectors—send events to Logger either as encrypted SmartMessages or as Common Event Format (CEF) messages. See below for further information about SmartConnectors

- Syslog—Logger can receive syslog messages sent using User Datagram Protocol (UDP) or Transmission Control Protocol (TCP)
- Text files—Logger can read events from text log files on remote hosts. Logger can be configured to poll remote folders for new files matching a filename pattern. Once the events in the new file have been read, Logger can delete the file, rename it, or simply remember that it has been read. Logger can read remote files on network drives using Secure Copy (SCP), SSH File Transfer Protocol (SFTP), or FTP, or using a previously-established Network File System (NFS) or Common Internet File System (CIFS) mount.

The Logger uses "receivers" to collect events from each of the different sources listed above. Receiver types include UDP, TCP, SmartMessage, and three types of file based receivers: File Transfer; File Receiver; and Folder Follower Receiver. The System Admin can configure the following types of receiver:

- UDP Receiver—UDP receivers listen for User Datagram Protocol messages on a configured port. Logger comes pre-configured with a UDP Receiver on port 514 or 8514, enabled by default. For software Loggers, this port may vary based on the port numbers available at installation time.
- CEF UDP Receiver—UDP receivers that receive events in Common Event Format.
- TCP Receiver—TCP receivers listen for Transmission Control Protocol messages on a configured port. Logger comes pre-configured with a TCP receiver on port 515 or 8515, enabled by default. For software Loggers, this port may vary based on the port numbers available at installation time.
- CEF TCP Receiver—TCP receivers that receive events in Common Event Format.
- Event Broker Receiver—Event Broker receivers are consumers for the Event Broker's publish-subscribe messaging system. They subscribe to event topics and receive events in CEF from Event Broker.
- File Receiver—depending on the type of Logger, file receivers read log files from a local file system, Network File System (NFS), Common Internet File System (CIFS), or Storage Area Network (SAN). File receivers read single or multi-line log files. They provide a snapshot of a log file at a single point in time.
- Folder Follower Receiver—Folder follower receivers actively read the log files in a specified directory as they are updated. If the source directory contains different types of log files, the Logger System Admin can create a receiver for each type of file to be monitored. Logger comes pre-configured with folder follower receivers for Logger's Apache Access Error Log, the System Messages Log, and Audit Log (when auditing is enabled). The Logger System Admin must enable these receivers in order to use them.
- File Transfer—File Transfer receivers read remote log files using SCP, SFTP, or FTP. These receivers can read single- or multi-line log files. The System Admin can schedule the receiver to read a file or batch of files periodically.
- SmartMessage Receiver—SmartMessage receivers listen for encrypted messages from ArcSight SmartConnectors.

A SmartConnector is an application that collects raw events generated by devices in the operational environment of the TOE, normalizes them, processes them into ArcSight security events, and transmits them to Logger and potentially other destinations, such as ArcSight ESM Manager.

SmartConnectors normalize collected data in two ways. First, they normalize values (such as severity, priority, and time zone) into a common format. Second, they normalize the data structure into a common schema (the Common Event Format). SmartConnectors can also filter and aggregate events to reduce the volume sent to the Logger and other destinations, which increases efficiency and reduces event processing time.

In brief, SmartConnectors:

- Collect IDS data generated by IDS and IPS entities in the IT system
- Parse individual events and normalize event values (such as severity, priority and time zone) into a common schema for use by Logger and ESM Manager
- Optionally filter out data not needed for analysis, thus saving network bandwidth and storage space

- Optionally aggregate events to reduce the quantity of events sent to Logger or ESM Manager, increasing efficiency and reducing event processing time
- Categorize events using a common, human-readable format, facilitating using event categories to build filters, rules, reports, and data monitors
- Pass processed events to the Logger or ESM Manager.

Vendor device types for which SmartConnectors are available include:

- Network and host-based IDS and IPS
- VPN, firewall, router, and switch devices
- Vulnerability management and reporting systems
- Access and identity management
- Operating systems, Web servers, content delivery, log consolidators, and aggregators.

Data collection and event reporting formats for various SmartConnectors include:

- Log file readers (including text and log file)
- Syslog
- SNMP
- Database
- XML
- Proprietary protocols, such as OPSEC.

6.7.2 Storage and Availability

The Logger component of the TOE provides the repository for storing collected IDS data and capabilities for managing IDS data storage.

The storage volume, either external or local, can be divided into multiple storage groups, each with a separate retention policy. Storage groups support multiple retention policies by defining a maximum size (Allocated (GB)) and number of days (Maximum Age) to retain events. Once events are older than the specified Maximum Age or there are more events than the storage group will hold (as specified by Allocated size), the oldest events are deleted at the next retention cycle. The retention process triggers periodically on Logger, so events might not be deleted immediately when events get older than maximum age or the storage group size exceeds the allocated size.

Logger can have a maximum of six storage groups—two groups (Internal Storage Group and Default Storage Group) are built-in and an administrator can create up to four additional groups. Additional storage groups (up to the maximum of six) can be created at any time. The Internal Storage Group is intended for logger's internal events (audit records), so up to five storage groups are available for storage of collected IDS data.

Once a storage group is created, it cannot be deleted. However, its size can be increased or decreased any time. If the size of a storage group is decreased and the new size is less than the currently used space on the storage group, stored IDS data will need to be deleted to achieve the new size.

Logger uses "device groups" and "storage rules" to determine in which storage group IDS data is stored. The combination of a source IP address and a Logger receiver is termed a "device". As events are received, devices are automatically created for each IP/receiver pair. Devices can also be created manually.

Devices can be categorized by membership in one or more device groups. While an incoming event belongs to one and only one device, it can be associated with more than one device group.

Storage rules create a mapping between device groups and storage groups, allowing events from specific sources to be stored in specific storage groups. Storage rules are ordered by priority, and the first matching rule determines to which storage group an incoming event will be sent. The System Admin can configure storage groups with different retention policies, and thus retain event data based on the source of incoming events. For example, all events from

firewall devices can be subject to a short retention period. To accomplish this, the System Admin manually assigns the firewall devices to a device group and then creates a storage rule that maps the device group to a storage group with the desired short retention period.

Event Archives enable the System Admin to save the events for any day in the past, not including the current day. Archive Storage Settings must be configured before Event Archives can be created. Archive Storage Settings specify the location to which Event Archives will be written. Note:

- For Logger Appliances, the location needs to be an NFS mount, CIFS mount, or SAN, which is configured using the Logger user interface
- For Software Loggers, the location is a directory (either local or a mount point that has already been established on the Logger host).

Events in each storage group are archived separately. That is, one archive file is created for each storage group, for each day. In addition, the System Admin can bulk archive events—that is, specify a range of dates to archive events in a single archive operation.

Logger uses the receipt time of an event to determine its archival day. For example, an event with a timestamp of 11:55:00 PM on December 7 is received at 12:01:00 AM on December 8 on the Logger. This event is archived in the archive file created for December 8th and not December 7th. When an archive operation occurs, one archive file per storage group is created at the location specified in Archive Storage Settings. Each archive file contains events from 12:00:00 AM to 11:59:59 PM for a single storage group of any given day. When a range of dates is specified, an archive file for each specified day per storage group is created.

Events can be archived on a configured schedule or manually on demand. When events are archived manually, the System Admin specifies the start and end dates of the event archive and the storage groups that should be archived. This operation occurs once for the specified date range. When events are archived based on a schedule, the System Admin specifies the time at which the archive operation should occur every day and selects the storage groups that should be included.

When Logger starts archiving, it proceeds sequentially through the various storage groups, as listed on the Daily Task Settings page (for scheduled archives) or the Add Event Archives page (for manual archives).

Once the events have been archived, they are not deleted from the local storage until the events (and their related indexing information) age out due to the configured retention policy. These events continue to be included in search operations until they age out.

Once events that have been archived are deleted from Logger's local storage, they are not included in search operations. To include such events in search operations, it is necessary to load the archive in which those events exist back to the Logger. When an Event Archive is loaded, its events are included in searches, but the archive itself remains on the remote storage.

6.7.3 Searching and Review

The TOE provides capabilities to search stored events using queries. Queries can be simple search terms or they can be complex enough to match events that include multiple IP addresses or ports, and that occurred between specific time ranges from a specific storage group.

The search process uses an optimized search language that allows the specification of multiple search commands in a pipeline format, as follows:

```
<Indexed Search> | <Search Operators>
```

The query expression is evaluated from left to right in a pipeline fashion. First, events matching the specified `<Indexed Search>` portion of the query are found. The search operator after the first pipe ("|") character is then applied to the matched events, followed by the next search operator, and so on to further refine the search results.

The `<Indexed Search>` section of the query uses fields to search for relevant data. It can contain a search expression to specify keywords to search for in the event text or a field-based expression in a Boolean format.

A keyword is a text string to search for, such as `failed`, `login`, etc. Multiple keywords can be specified in one query expression by using Boolean operators (`AND`, `OR`, or `NOT`) between them. In addition, Boolean expressions can be nested, e.g., `(John OR Jane) AND Doe`.

A field-based search specifies operations on fields in the Logger schema that can be further combined using Boolean operators. The Logger schema contains a predefined set of fields and the TOE provides the capability to add fields to the schema that are relevant to the events being collected.

The following table identifies and briefly describes the operators that can be used in field-based searches.

Operator	Description	Example of Use
AND	Boolean AND operator	`name="Data List" AND message="Hello"`
OR	Boolean OR operator	`name="Data List" OR message="Hello"`
NOT	Boolean NOT operator	`NOT name="test 123"`
=	Is equal to	`bytesIn = 32`
!=	Is not equal to	`destinationPort != 100`
>	Is greater than in value	`bytesIn > 100`
>=	Is greater than or equal to in value	`endTime >="01/13/2015 07:07:21"`
<	Is less than in value	`bytesIn < 32`
<=	Is less than or equal to in value	`bytesIn <= 32`
IN	Is a member of the set	`priority IN [2,5,4,3]`
BETWEEN	Is in the inclusive range	`priority BETWEEN 1 AND 5`
STARTSWITH	Text string starts with specified text	`message STARTSWITH "failed"`
ENDSWITH	Text string ends with specified text	`message ENDSWITH "login"`
CONTAINS	Specified text is within the text string	`message CONTAINS "login"`
IS	Test for NULL value	`sessionId IS NULL`
INSUBNET	IP address is in the specified subnet	`sourceAddress insubnet "192.0.2.*"`

Table 4: Supported Field-Based Search Operators

Multiple field conditions can be specified in a single query expression by using Boolean operators between them, and conditions can be nested, e.g., `(name="John Doe" OR name="Jane Doe") AND message!="success"`.

The `<Search Operators>` section of the query can be used to further refine the data that matched the Indexed Search filter. The following operators can be used in the Search Operators portion of the query:

- Chart—displays search results in a chart form of specified fields
- Dedup—remove duplicate events from search results
- Eval—display events after evaluating the result of the specified expression
- Extract—extract key-value pairs from raw events
- Fields—include or exclude specified fields from search results
- Head—display the first <N> lines of the search results
- Keys—identify keys in raw events based on specified delimiters
- Lookup—return an augmented or filtered set of events based on whether they have identical values in the corresponding fields in an uploaded Lookup file

- Parse—apply the named parser to the matching events of a search query
- Regex—select events that match the specified regular expression
- Rename—rename a specified field name
- Replace—replace a specified string in specified fields with a specified new string
- Rex—extract a value based on the specified regular expression, or extract and substitute a value based on the specified "sed" expression
- Sort—sort search results as specified by the sort criteria
- Tail—display the last <N> lines of the search results
- Top—list the search results in a tabular form of the most common values for the specified field
- Transaction—group events that have the same values in the specified fields
- Where—display events that match the criteria specified in a valid field-based query expression.

Search queries can be saved for subsequent reuse, either as a filter or as a saved search:

- Filter—saving as a filter saves the query expression, but does not save the time range or the field set information
- Saved search—saving as a saved search saves the query expression and the specified time range.

The search results table displays the events that match the query as they are found. As additional events are matched, the search results table is refreshed. Certain search operators (such as `head` and `tail`) require a query to finish running before search results can be displayed.

Search results are sorted by the Logger receipt time. The events are displayed either oldest first or newest first, depending on the sort criterion selected when the search was run. The results of any search can be saved by exporting them in PDF or CSV format.

6.7.4 Alerting

The TOE provides capabilities to define queries that can trigger alerts if specified conditions are met.

The TOE supports two types of alerts:

- Real Time Alerts—Real time alerts search events continually and automatically send notifications if specified criteria are found. A real time alert is defined by specifying a query, a match count, a threshold, and one or more destinations. Whenever the specified number of matches occurs within the specified threshold, an alert is triggered.
- Saved Search Alerts—Saved search alerts search at a scheduled interval and send notifications if specified criteria are found. A saved search alert is defined by specifying a Saved Search (which is a query with a time range within which events are to be searched), a match count, a threshold, and one or more destinations. If the specified number of matches occurs within the specified threshold within the specified time range, an alert is triggered.

When either a real time or a saved search alert is triggered, the TOE creates an alert event containing the triggering events or event IDs, and sends a notification to the specified destinations—e-mail addresses, SNMP server, syslog server, or ArcSight Manager.

Alerts can be viewed via the Logger GUI.

The IDS Capabilities security function satisfies the following security functional requirements:

- IDS_ARP.1—the TOE is able to generate an alert and send a notification to a configured destination when it finds IDS data (an event) matching specified search criteria.
- IDS_IDC.1—the TOE is able to collect IDS data (events) in a variety of formats from the IT system it is monitoring.

- IDS_IDR.1—the TOE provides authorized users with the capability to read all information from the collected IDS data (events). The IDS data is displayed in a manner suitable for the authorized user to interpret the information. The TOE prohibits all users read access to the audit records, except those users that have been granted explicit read-access.
- IDS_IDR.2—the TOE provides capabilities for selecting IDS data for review based on text searches of IDS data fields and ordering IDS data for review based on receipt time and sort criteria
- IDS_STG.1—the TOE protects collected IDS data (events) stored in Logger storage groups from unauthorized modification and unauthorized deletion.
- IDS_STG.2—the TOE will delete the oldest events from a Logger storage group in the event the storage group's retention policy for allocated size or maximum age has been exceeded.

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.INAPPROPRIATE_USE	T.INTEGRITY_COMPROMISE	T.NETWORK_COMPROMISE	T.NO_ACCOUNTABILITY	T.UNATTENDED_SESSION	T. UNAUTHORIZED_ACCESS	T.UNAUTHORIZED_ACTIVITY	T.UNDETECTED_THREATS	A. MANAGE	A.PLATFORM	A. PROTECT
O.AUDIT					X							
O.AUDIT_REVIEW					X							
O.I_AND_A							X					
O.IDS_ALERT									X			
O.IDS_COLLECT									X			
O.IDS_REVIEW									X			
O.LOGON_BANNER		X										
O.PASSWORD_CONTROLS	X											
O.PROTECTED_COMMS				X								
O.SECURITY_MANAGEMENT								X				
O.SESSION_LIMITS						X						
O.SESSION_TERMINATION						X						
O.STORAGE			X									
O.THROTTLE	X											
OE.PERSONNEL										X		
OE.PHYSICAL												X
OE.PLATFORM											X	
OE.TIME					X							

Table 5: 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.INAPPRORIATE_USE

Authorized users perform inappropriate actions on the TOE due to ignorance of their responsibilities or operational policies and procedures.

This threat is countered by the following security objective:

- O.LOGON_BANNER—addresses this threat by displaying a configurable advisory warning message to potential users pertaining to appropriate use of the TOE.

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

An unauthorized user may monitor the enterprise network in an attempt to obtain sensitive data, such as passwords, or to modify transmitted data.

This threat is countered by the following security objective:

- O.PROTECTED_COMMS—addresses this threat by ensuring the TOE is able to protect communications between its distributed components and between itself and external entities.

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 software components with a reliable time source that can be used to generate time stamps for inclusion within generated audit records.

T.UNATTENDED_SESSION

An unauthorized user gains access to the TOE via an unattended authorized user session.

This threat is countered by the following security objectives:

- O.SESSION_TERMINATION—addresses this threat by providing users with a mechanism to terminate their interactive sessions with the TOE, and by ensuring sessions that have been inactive for a configurable period of time will be terminated by the TOE.
- O.SESSION_LIMITS—supports O.SESSION_TERMINATION in addressing this threat by ensuring the TOE provides capabilities to restrict the number of concurrent interactive sessions belonging to the same user, reducing the likelihood of a user having multiple unattended active sessions.

T.UNAUTHORIZED_ACCESS

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

This threat is countered by the following security objective:

- 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.

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.IDS_COLLECT—addresses this threat by providing capabilities to collect IDS data (events) from IDS entities in the IT system it monitors.
- O.IDS_REVIEW—supports O.IDS_COLLECT in addressing this threat by ensuring the TOE provides capabilities for effective review of stored IDS data.
- O.IDS_ALERT—supports O.IDS_COLLECT in addressing this threat by ensuring the TOE provides capabilities to generate alerts based on results from IDS data searches.

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 software 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 software 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 6 summarizes the correspondence of functional requirements to TOE security objectives.

	O.AUDIT	O.AUDIT_REVIEW	O.I_AND_A	O.IDS_ALERT	O.IDS_COLLECT	O.IDS_REVIEW	O.LOGON_BANNER	O.PASSWORD_CONTROLS	O.PROTECTED_COMMS	O.SECURITY_MANAGEMENT	O.SESSION_LIMITS	O.SESSION_TERMINATION	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.2			X											
FIA_UAU.5			X											
FIA_UAU.6			X											
FIA_UID.2			X											
FMT_MOF.1										X				
FMT_MTD.1										X				
FMT_SMF.1										X				
FMT_SMR.1										X				
FPT_ITT.1									X					
FPT_STM.1	X													
FTA_MCS.1											X			
FTA_SSL.3												X		
FTA_SSL.4												X		
FTA_TAB.1							X							
FTP_ITC.1									X					
FTP_TRP.1									X					
IDS_ARP.1				X										
IDS_IDC.1					X									
IDS_IDR.1						X								
IDS_IDR.2						X								

	O.AUDIT	O.AUDIT_REVIEW	O.I_AND_A	O.IDS_ALERT	O.IDS_COLLECT	O.IDS_REVIEW	O.LOGON_BANNER	O.PASSWORD_CONTROLS	O.PROTECTED_COMMS	O.SECURITY_MANAGEMENT	O.SESSION_LIMITS	O.SESSION_TERMINATION	O.STORAGE	O.THROTTLE
IDS_STG.1													X	
IDS_STG.2													X	

Table 6: Objectives to Requirement Correspondence

O.AUDIT

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

The following security functional requirements contribute 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.
- FPT_STM.1—the ST supports FAU_GEN.1 by including FPT_STM.1 to specify the capability to provide reliable time stamps, which are applied to generated audit records.

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, subject identity, type of event, or success or failure of event, which assists the authorized roles in reviewing the audit trail effectively.

O.I_AND_A

The TOE shall require all users of the TOE to be identified and authenticated before gaining access to TOE services.

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

- FIA_UID.2, FIA_UAU.2—the ST includes FIA_UID.2 and FIA_UAU.2 to specify that users 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.2 and FIA_UAU.2 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.2 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.

- FIA_UAU.6—the ST supports FIA_UAU.2 by including FIA_UAU.6 to specify that users must re-authenticate themselves prior to changing their own password.

O.IDS_ALERT

The TOE shall provide capabilities to generate alerts based on results from IDS data searches.

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

- IDS_ARP.1—the ST includes IDS_ARP.1 to specify the capability to generate alerts based on results from IDS data searches.

O.IDS_COLLECT

The TOE shall provide capabilities to collect IDS data from IDS entities in the IT system it monitors.

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

- IDS_IDC.1—the ST includes IDS_IDC.1 to specify the capability to collect IDS data from IDS entities in the IT system it monitors.

O.IDS_REVIEW

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

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

- IDS_IDR.1—the ST includes IDS_IDR.1 to specify which roles are to be able to read IDS data from the stored IDS data, and that only those roles have access to the IDS data.
- IDS_IDR.2—the ST supports IDS_IDR.1 by including IDS_IDR.2 to specify capabilities for selecting IDS data based on text searches of IDS data fields and ordering IDS data based on receipt time and sort criteria.

O.LOGON_BANNER

The TOE shall be able to display a configurable advisory warning message to potential users pertaining to appropriate use of the TOE.

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

- FTA_TAB.1—the ST includes FTA_TAB.1 to specify the capability to display an advisory warning message regarding unauthorized use of the TOE.

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 its distributed components and between itself and external entities.

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

- FPT_ITT.1—the ST includes FPT_ITT.1 to specify that TSF data communicated between distributed parts of the TOE will be protected from disclosure and modification.
- FTP_ITC.1—the ST includes FTP_ITC.1 to specify that data will be communicated between the TOE and external IT entities through a trusted channel that protects the data from disclosure and modification.
- FTP_TRP.1—the ST includes FTP_TRP.1 to specify that data will be communicated between the TOE and remote users through a trusted path that protects the data from disclosure and modification.

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.SESSION_LIMITS

The TOE shall provide capabilities to restrict the number of concurrent interactive sessions belonging to the same user.

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

- FTA_MCS.1—the ST includes FTA_MCS.1 to specify the capability for the TSF to restrict number of concurrent interactive sessions belonging to the same user.

O.SESSION_TERMINATION

The TOE shall provide mechanisms to terminate a user session after a period of inactivity or at the request of the user.

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

- FTA_SSL.3—the ST includes FTA_SSL.3 to specify the capability for the TSF to terminate an interactive user session after a period of inactivity.
- FTA_SSL.4—the ST includes FTA_SSL.4 to specify the capability for users to terminate their own interactive sessions.

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 that stored audit records will be protected from unauthorized modification and deletion.
- IDS_STG.1—the ST includes IDS_STG.1 to specify that IDS data will be protected from unauthorized modification and deletion.
- IDS_STG.2—the ST supports IDS_STG.1 by including IDS_STG.2 to specify the actions the TOE takes if the storage capacity for IDS data has been reached.

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	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.2
FIA_ATD.1	None	None
FIA_SOS.1	None	None
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UAU.5	None	None
FIA_UAU.6	None	None
FIA_UID.2	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.2
FPT_ITT.1	None	None
FPT_STM.1	None	None
FTA_MCS.1	FIA_UID.1	FIA_UID.2
FTA_SSL.3	None	None
FTA_SSL.4	None	None
FTA_TAB.1	None	None
FTP_ITC.1	None	None
FTP_TRP.1	None	None
IDS_ARP.1	IDS_IDC.1	IDS_IDC.1
IDS_IDC.1	None	None
IDS_IDR.1	IDS_IDC.1	IDS_IDC.1
IDS_IDR.2	IDS_IDR.1	IDS_IDR.1
IDS_STG.1	IDS_IDC.1	IDS_IDC.1
IDS_STG.2	IDS_STG.1	IDS_STG.1

Table 7: Requirement Dependencies

TimeStamp Note: The TOE comprises software components and Logger appliances. The software components operate as applications within a process provided by the environment. Thus, the environment is providing resources for components of 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 software components of the TOE from their 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	TOE Access	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.2		X					
FIA_UAU.5		X					
FIA_UAU.6		X					
FIA_UID.2		X					
FMT_MOF.1			X				
FMT_MTD.1			X				
FMT_SMF.1			X				
FMT_SMR.1			X				
FPT_ITT.1				X			
FPT_STM.1				X			
FTA_MCS.1					X		
FTA_SSL.3					X		
FTA_SSL.4					X		
FTA_TAB.1					X		
FTP_ITC.1						X	
FTP_TRP.1						X	
IDS_ARP.1							X
IDS_IDC.1							X
IDS_IDR.1							X
IDS_IDR.2							X
IDS_STG.1							X
IDS_STG.2							X

Table 8: Security Functions vs. Requirements Mapping