ArcSight ESM 6.0c Patch 1

Security Target

Version 2.0

12 February 2014

Prepared for:

ArcSight, an HP Company

1140 Enterprise Way

Sunnyvale, CA 94089

Prepared By:

Science Applications International Corporation

Common Criteria Testing Laboratory

6841 Benjamin Franklin Drive

Columbia, MD 21046

Table of Contents

List of Figures

List of Tables

1. Security Target Introduction

The Target of Evaluation (TOE) is ArcSight Enterprise Security Management (ESM) Version 6.0c Patch 1, hereinafter referred to as "ESM" or "the TOE". ESM is an intrusion detection system (IDS) analyzer able to concentrate, normalize, analyze, and report the results of its analysis of security event data generated by various IDS sensors and scanners in the operational environment. ESM integrates existing multi-vendor devices throughout the enterprise into its scope and gathers generated events. ESM allows users to monitor events in real-time, correlate events for in-depth investigation and analysis, and resolve events with automated escalation procedures and actions.

ESM gathers events generated by multi-vendor devices, normalizes, and stores those events in the CORR-Engine, and then filters and correlates those events with rules to generate meta-events.

The TOE is composed of the following components:

- ArcSight Console—provides the primary interface to the TOE for users to manage the TOE's resources and view and monitor the security events generated by the TOE.
- ArcSight Manager—the central engine of the TOE, it manages the TOE's resources and is responsible for processing, filtering, and correlation of security events.
- Correlation Optimized Retention and Retrieval (CORR)-Engine—provides the repository for storing resources and security events
- ArcSight SmartConnectors—import security event data generated by security scanners and sensors in the operational environment, normalize the imported data into the TOE's security event format, and forward the security events to the ArcSight Manager for storage and processing. The evaluated configuration includes the following specific ArcSight SmartConnectors:
    - SnortDB—Snort is an open-source network intrusion detection system, capable of performing realtime traffic analysis and packet logging on IP networks. It can perform protocol analysis and content searching/matching, and can be used to detect a variety of attacks and probes, including buffer overflows, stealth port scans, CGI attacks, SMB probes, and OS fingerprinting attempts. This ArcSight SmartConnector imports events generated by Snort (and stored in a database) into the TOE.
    - NessusXML—Nessus is a remote security scanner. The Nessus Vulnerability Scanner is able to remotely audit a given network and determine whether it has been broken into or misused in some way. This ArcSight SmartConnector imports events generated by the Tenable Nessus XML File device into the TOE.
    - Checkpoint-OPSECNG—Check Point's Open Platform for Security (OPSEC) integrates and manages all aspects of network security through an open, extensible management framework. The Check Point OPSEC Software Development Kit (SDK) provides Application Programming Interfaces (APIs) for open protocols. It includes the Log Export API (LEA), which lets ArcSight securely receive both realtime and historical auditing log data generated by Check Point OPSEC NG. The ArcSight SmartConnector for Check Point OPSEC NG devices uses LEA exclusively. The LEA allows Check Point log data to be exported to third-party applications such as the ArcSight SmartConnector. These applications are called LEA Clients. When the connection between the LEA Server (usually a FW-1 Management Server) and the SmartConnector (LEA Client) is established, the LEA Server sends all the records in the log file to the connector, one after the other.
    - Cisco Secure IPS SDEE—Cisco IPS Sensors are network security appliances that detect unauthorized activity over the network, analyzing traffic in real time, letting users quickly respond to security breaches. When unauthorized activity is detected, the sensors can send alarms providing details of the activity and can control other systems, such as routers, to terminate the unauthorized session or sessions. This ArcSight SmartConnector works as an IPS client and imports events generated by Cisco IPS sensors into the TOE.

The following components are included in the ESM software, but are outside the scope of the evaluated configuration:

- Pattern Discovery is a feature of the ArcSight Manager that is licensed separately and is not enabled as part of the TOE. The component mines historical trends to baseline and profile expected behavior. Pattern Discovery is used as a learning tool that an authorized user can use on the gathered information to create policies. The TOE itself offers the capabilities for the authorized users to define policies and rules without the use of this tool.
- All SmartConnectors except for the four listed above that have been chosen to be part of the TOE.
- Management Console is a web-based interface used to view dashboards, monitor events, manage users, and manage connectors. Connector management component is a separately licensed component of the Management Console. Note that these capabilities are still available through the ArcSight Console.
- ArcSight Web is a web-based interface used to monitor events, view dashboards, view cases, acknowledge notifications, access reports, and access the Knowledge Base. The ArcSight Web is a separate licensed component.
- ArcSight Express includes a set of rules, report templates, alerts and dashboards that allow smaller security teams to gain visibility into their environment on the first day, with no rule/report development required. ArcSight Express is marketed as 'Security in a box' and does not expose all of the functionality and security functions being claimed in this Security Target. ArcSight Express is a separate licensed product.

The remainder of this section identifies the Security Target (ST), the Target of Evaluation (TOE), and Security Target conventions, conformance claims, and organization.

The Security Target contains the following additional sections:

- Section 2 – Target of Evaluation (TOE) Description

  This section gives an overview of the TOE, describes the TOE in terms of physical and logical boundaries, and states the scope of the TOE.

- Section 3 – Security Problem Definition

  This section details the expectations of the environment, the threats that are countered by the TOE and its environment and the organizational security policies that the TOE must fulfill.

- Section 4 – TOE Security Objectives

  This section details the security objectives of the TOE and operational environment.

- Section 5 – IT Security Requirements

  This section presents the Security Functional Requirements (SFR) for the TOE, and details the assurance requirements for EAL3 augmented with ALC_FLR.2.

- Section 6 – TOE Summary Specification

  This section describes the security functions represented in the TOE that satisfies the security requirements.

- Section 7 – Protection Profile Claims

  This section presents any protection profile claims.

- Section 8 – Rationale

  This section closes the ST with justifications for security objectives, stated requirements, and TOE summary specifications as to their consistency, completeness, and suitability.

1.1 Security Target, TOE, and CC Identification

ST Title – ArcSight ESM Version 6.0c Patch 1 Security Target

ST Version – Version 2.0

ST Date – 05 November 2013

TOE Identification – The TOE is ArcSight ESM Version 6.0c Patch 1 comprising:

- ArcSight Console:
  - ArcSight-6.0.0.1333.0-Console-Win.exe with patch Patch-6.0.0.1378.1-Console-Win.exe
  - 6.0.0.1333.0-Console-Linux.bin with patch Patch-6.0.0.1378.1-Console-Linux.bin
- ArcSight SmartConnectors (SnortDB, NessusXML, Checkpoint-OPSECNG, Cisco Secure IPS SDEE)
  - ArcSight-6.0.1.6574.0-Connector-Win.exe
  - ArcSight-6.0.1.6574.0-Connector-Linux.bin
- ArcSight Manager with CORR-Engine:
  - ArcSightESMSuite-1208.tar, which includes ArcSight-6.0.0.1333.0-Manager-Linux.bin, and with patch ArcSightESMSuite-1254.tar, which includes ArcSight-6.0.0.1378.0-Manager-Linux.bin.

TOE Developer – ArcSight, an HP Company

Evaluation Sponsor – ArcSight, an HP Company

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009.

1.2 Conformance Claims

This ST and the TOE it describes are conformant to the following Common Criteria (CC) specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 3, July 2009
  - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, Revision 3, July 2009
  - Part 3 Conformant

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

- EAL 3 augmented with ALC_FLR.2

The TOE is further conformant to the following Protection Profile (PP):

- U.S. Government Protection Profile Intrusion Detection System Analyzer For Basic Robustness Environments, Version 1.3, July 25, 2007.

ArcSight has elected to pursue a more rigorous assurance evaluation. The product meets all the U.S. Government Intrusion Detection System Analyzer Protection Profile Functional and Assurance Requirements; additionally the TOE conforms to all the Assurance Requirements for an EAL3 product and includes Flaw Remediation. The resulting assurance level is therefore, EAL3 augmented with ALC_FLR.2.

1.3 Conventions, Terminology, and Acronyms

1.3.1 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 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 the ST, iteration is indicated by a letter in parenthesis placed at the end of the component. For example

FDP_ACC.1(a) and FDP_ACC.1(b) indicate that the ST includes two iterations of the FDP_ACC.1 requirement; a and b.

- Assignment: allows the specification of an identified parameter. Assignments are indicated using bold text surrounded by brackets (e.g., [**assignment**]).
- Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics text surrounded 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 …").

- Extended Requirements (i.e., those not found in Part 2 of the CC) are identified with "(EXT)" following the identification of the new functional class/name (i.e., Intrusion Detection System (IDS)) and the associated family descriptor. Example: Analyzer analysis (EXT) (IDS_ANL.1).
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.3.2 Terminology and Abbreviations

Refer to the U.S. Government Intrusion Detection System Analyzer Protection Profile for a glossary of terms associated with IDS Analyzer technology. In addition, the following terms are used within this Security Target.

Term	Definition
API	Application Programming Interface
authorized user	An ESM user, i.e., a user with an account managed by ESM. Every authorized user is assigned to one of the default roles provided by the TOE (Administrator, Analyzer Administrator, Operator, Analyst).
ESM	Enterprise Security Management—the name of the TOE described in this ST.
ESM Administrator	An **authorized user** assigned the Administrator role on the TOE, as distinct from **System Administrator** and **RDBMS Administrator**. Whenever this ST uses the term "Administrator" without qualification, "ESM Administrator" is meant.
GUI	Graphical User Interface
IDS	Intrusion Detection Systems
IMAP	Internet Message Access Protocol—an application layer Internet protocol that allows an e-mail client to access e-mail on a remote mail server.
JCE	Java Cryptography Extension—an officially released Standard Extension to the Java Platform. JCE provides a framework and implementation for encryption, key generation and key agreement, and Message Authentication Code (MAC) algorithms. The TOE uses the SunJCE as its default cryptographic provider.
JVM	Java Virtual Machine—a virtual machine capable of executing Java bytecode. It is the code execution component of the Java software platform.
LDAP	Lightweight Directory Access Protocol—an application protocol for querying and modifying data using directory services running over TCP/IP.
NSS	Network Security System
OS	Operating System
POP3	Post Office Protocol, Version 3—an application layer Internet standard protocol used by local e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection.

Term	Definition
RADIUS	Remote Authentication Dial in User Service—a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for computers to connect and use a network service.
Resources	Refers specifically in this ST and the TOE guidance documentation to the objects the TOE employs to manage the logic used to process events. Examples of TOE resources include: active channels; data monitors; filters; cases; assets; queries; trends; report templates; rules; and packages. A resource defines the properties, values, and relationships used to configure the functions the TOE performs. Resources can also be the output of such a configuration.
SMTP	Simple Mail Transfer Protocol—an Internet standard for email transmission across Internet Protocol (IP) networks.
SSL	Secure Sockets Layer
System Administrator	A user defined in the underlying operating system supporting the TOE that has been granted administrator privileges in that operating system (e.g., Windows Administrator, Unix root), as distinct from **ESM Administrator**.

1.4 TOE Documentation

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

- Installation and Configuration Guide: ArcSight ESM Version 6.0c, October 10, 2012
- ArcSight ESM Administrator's Guide: ArcSight ESM Version 6.0c, September 27, 2012
- ArcSight Console User's Guide: ArcSight ESM Version 6.0c, September 20, 2012
- SmartConnector Configuration Guide for Check Point OPSEC NG, December 21, 2012
- SmartConnector Configuration Guide for Cisco Secure IPS SDEE, September 28, 2012
- SmartConnector Configuration Guide for Tenable Nessus XML File, May 15, 2012
- SmartConnector Configuration Guide for Snort DB, May 15, 2012
- Common Criteria Evaluated Configuration Guide: ArcSight ESM 6.0c Patch 1.

2. TOE Description

The TOE, ArcSight ESM Version 6.0c Patch 1, is a security management software product designed to monitor, analyze, and report on network anomalies identified by third-party network monitoring devices (e.g. Intrusion Detection Systems (IDS) Sensors or IDS Scanners, firewalls, etc). ESM also includes the capability to provide enterprise-wide monitoring for sub-networks monitored by non-homogeneous network monitors. As such, ESM provides a solution for managing all network events and/or activities in an enterprise from a centralized view. ESM allows authorized users to monitor events, correlate events for in-depth investigation and analysis, and resolve events with automated escalation procedures and actions.

The TOE can be installed on a wide range of supported platforms, the details of which are provided below in section 2.1. All of the components can be installed on the same machine or all on different machines. The authorized users access the TOE locally via the ArcSight Console. The TOE in its evaluated configuration does not provide interfaces to other external IT products.

2.1 TOE Architecture

The TOE, ArcSight ESM 6.0c Patch 1, comprises a number of different components that provide a comprehensive security event management system.

2.1.1 ArcSight Console

ArcSight Console is a centralized view into an enterprise that provides real-time monitoring, in-depth investigative capabilities, and automated responses and resolutions to events. The ArcSight Console provides authorized users with a graphical user interface (GUI) to perform security management functions, including management of TOE resources, management of the TOE's analysis and reaction functions, and viewing audit data and analysis results. The ArcSight Console connects to a single ArcSight Manager at a time via the network. The ArcSight Console requires the underlying operating system to provide protection for the TOE. The underlying operating system is considered part of the environment.

2.1.2 ArcSight Manager

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

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

2.1.3 CORR-Engine

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

2.1.4 ArcSight SmartConnectors

ArcSight SmartConnectors collect and process events generated by security devices (Targeted IT systems) throughout an enterprise. The devices are considered part of the environment in which the TOE operates. The devices consist of routers, email 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. ArcSight SmartConnectors can be installed on the ArcSight Manager machine, a separate host machine, or, when supported, directly on a device.

ArcSight SmartConnectors rely on the underlying operating system to cache events (security events and error logs) if they cannot be delivered immediately to the ArcSight Manager due to communication problems, or if the ArcSight Manager is experiencing temporary bursts of events. ArcSight SmartConnectors require the underlying operating system to provide protection for the TOE. The underlying operating system is considered part of the environment.

The SmartConnectors that are included in the evaluated configuration are:

- SnortDB - Snort is an open-source network intrusion detection system, capable of performing realtime traffic analysis and packet logging on IP networks. It can perform protocol analysis and content searching/matching, and can be used to detect a variety of attacks and probes, including buffer overflows, stealth port scans, CGI attacks, SMB probes, and OS fingerprinting attempts. The ArcSight SmartConnector imports events generated by Snort (and stored in a database) into the ArcSight system.
- NessusXML - Nessus is a powerful, up-to-date, and easy-to-use remote security scanner. The Nessus Vulnerability Scanner is able to remotely audit a given network and determine whether it has been broken into or misused in some way. The ArcSight SmartConnector imports events generated by the Tenable Nessus XML File device into the ArcSight System
- Checkpoint-OPSECNG - Check Point's Open Platform for Security (OPSEC) integrates and manages all aspects of network security through an open, extensible management framework. The Check Point OPSEC Software Development Kit (SDK) provides Application Programming Interfaces (APIs) for open protocols. It includes the Log Export API (LEA), which lets ArcSight securely receive both realtime and historical auditing log data generated by Check Point. The ArcSight SmartConnector for Check Point devices (including VPN-1/FW-1) uses LEA exclusively. The LEA lets Check Point log data to be exported to third-party applications such as the ArcSight SmartConnector. These applications are called LEA Clients. When the connection between the LEA Server (usually a FW-1 Management Server) and the SmartConnector (LEA Client) is established, the LEA Server sends all the records in the log file to the connector, one after the other.
- Cisco Secure IPS SDEE - Cisco IPS Sensors are network security appliances that detect unauthorized activity over the network, analyzing traffic in real time, letting users quickly respond to security breaches. When unauthorized activity is detected, the sensors can send alarms providing details of the activity and can control other systems, such as routers, to terminate the unauthorized session or sessions. Sensor installation requires seven simple addressing parameters and no special training. When the sensor is installed, it immediately begins monitoring as a promiscuous device by default. The ArcSight SmartConnector works as an IPS client and imports events generated by Cisco IPS sensors into the ArcSight ESM System.

2.2 TOE Physical Boundaries

The ArcSight Console, ArcSight Manager and ArcSight SmartConnectors are implemented as Java applications and execute in the context of an underlying Java Virtual Machine (JVM). This allows the components to be supported on a wide range of platforms and specific operating systems, as indicated in Tables 1 and 2 below. The ArcSight Console and ArcSight Manager components are supported on JVM 1.6.0_20, while the ArcSight SmartConnectors are supported on JVM 1.6.0_26.

The following diagram is a representation of the physical boundaries of the TOE and its components.

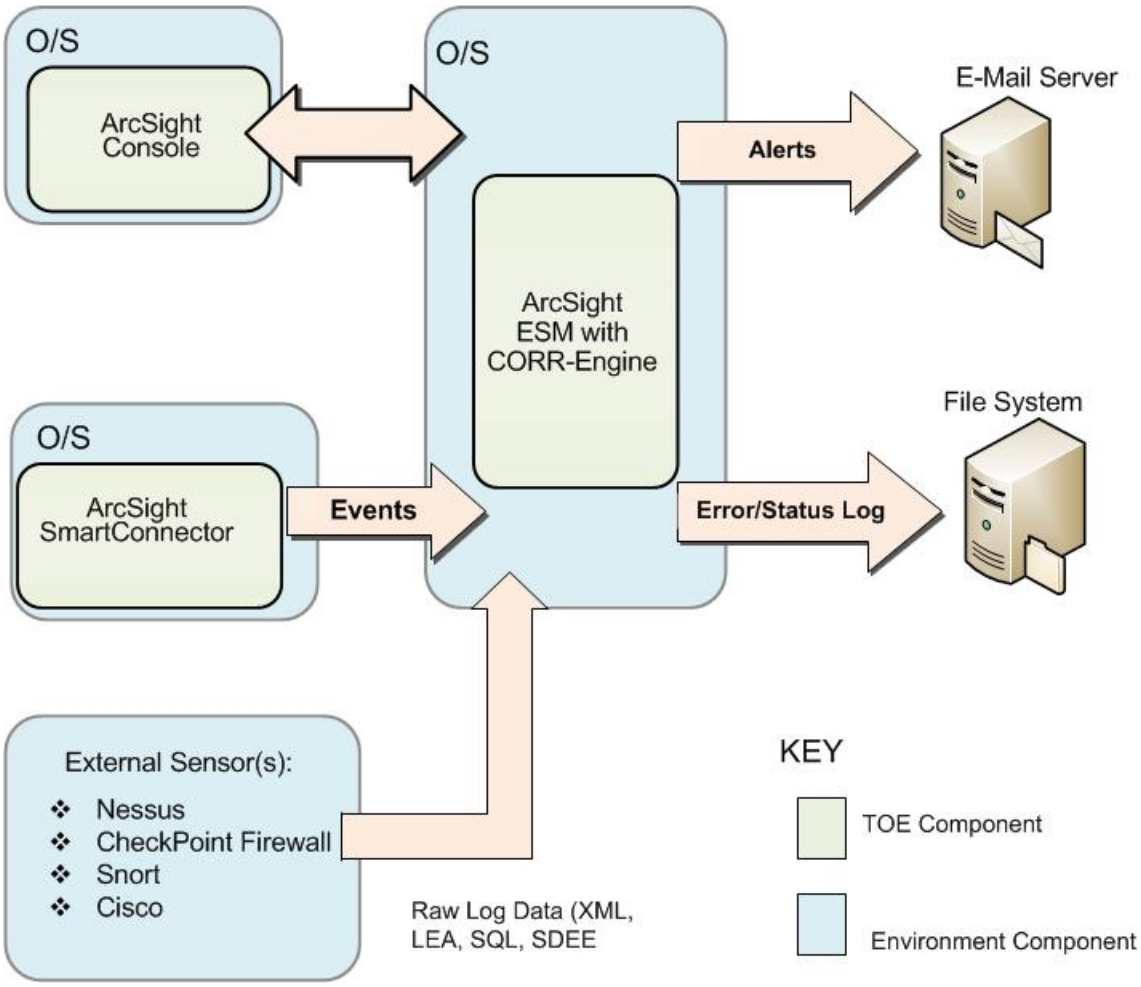

Figure 1: TOE Physical Boundaries

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

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

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

The TOE can be configured in either of two security modes: non-FIPS mode (the default mode); and FIPS 140-2 compliant mode. The configured security mode determines the cryptographic protocol and the underlying cryptographic provider the TOE uses to implement secure subsystem communications. In non-FIPS mode, communications between the SmartConnectors and the Manager, and between the Console and the Manager, are protected using SSL v3.0. In this mode, the TOE uses SunJCE and Bouncy Castle as the cryptographic providers—SunJCE is used for SSL and most other cryptographic needs, while Bouncy Castle is used for certificate generation in the TOE's setup wizard. The TOE uses X.509 Version 3 certificates. The maximum key size for the public key in the certificate is 1024 bits.

In FIPS 140-2 mode, the TOE uses the FIPS 140-2 validated Network Security Services (NSS) cryptographic module, version 3.11.4 (FIPS 140-2 certificate 814). Communications between the TOE components are protected using TLS v1.0. For additional information on the NSS cryptographic module, see the ArcSight™ ESM FIPS 140-2 Compliance Statement and the NSS Cryptographic Module Version 3.11.4 FIPS 140-2 Non-Proprietary Security Policy[1]. While is recommended that the TOE operate in FIPS 140-2 mode, this is not required for the evaluated configuration.

The following tables outline the system requirements for ESM for non-FIPS and FIPS 140-2 compliant modes. Specific system and installation requirements are documented in Installation and Configuration Guide: ArcSight ESM Version 6.0c.

ArcSight Console		
Platform	**Supported Operating System**	**Typical System Configuration**
Linux	Red Hat Enterprise Linux 6.2 Workstation, 64-bit	• x86-compatible multi-CPU system • 36-128 GB RAM memory, minimum • 250 GB disk space
Windows	Microsoft Windows 7 SP1, 64-bit	• x86-compatible multi-CPU system • 36-128 GB RAM memory, minimum • 250 GB disk space
ArcSight Manager (Includes CORR-Engine)		
Platform	**Supported Operating System**	**Typical System Configuration**
Linux	Red Hat Enterprise Linux 6.2, 64-bit	• 8-core processor • 36 GB RAM memory, minimum • 250 GB disk space (RAID 10), 15,000 RPM
ArcSight SmartConnectors		
Platform	**Supported Operating System**	**Typical System Configuration**
Linux	Red Hat Enterprise Linux 6.2, 64-bit	• x86-compatible CPU system • 512 MB memory • 1 GB disk space
Windows	Microsoft Windows Server 2008 R2, 64-bit	• x86-compatible CPU system • 512 MB memory • 1 GB disk space

Table 1: System Requirements for non-FIPS ArcSight ESM 6.0c Patch 1

ArcSight Console		
Platform	**Supported Operating System**	**Typical System Configuration**
Linux	Red Hat Enterprise Linux 6.2 Workstation, 64-bit	• x86-compatible, multi-CPU system • 2-4 GB RAM • 2 GB disk space
ArcSight Manager (includes CORR-Engine)		
Platform	**Supported Operating System**	**Typical System Configuration**

[1] Available at http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp814.pdf.

Linux	Red Hat Enterprise Linux 6.2 Workstation, 64-bit	• x86-compatible multi-CPU system • 36-128 GB memory • 250 GB disk space
ArcSight SmartConnectors		
Platform	**Supported Operating System**	**Typical System Configuration**
Linux	Red Hat Enterprise Linux 6.2 Workstation, 64-bit	• x86-compatible CPU system • 512 MB memory • 1 GB disk space

Table 2: System Requirements for FIPS 140-2 compliant ArcSight ESM 6.0c

In summary, the evaluated TOE configuration includes the following components:

- ArcSight Console
- ArcSight SmartConnectors
    - SnortDB
    - NessusXML
    - Checkpoint-OPSECNG
    - Cisco Secure IPS SDEE
- ArcSight ESM Suite which includes Manager and CORR-Engine

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

- SmartConnectors, except the four identified above
- Pattern Discovery
- Management Console
- ArcSight Web
- ArcSight Express

Other operating environment components in support of the TOE can be described in terms of the following components:

- Targeted IT systems (devices) in the environment sending and/or receiving network traffic and/or security relevant network operational data.
- SMTP Server to support e-mail notifications. POP3 and IMAP can be used to check for e-mail acknowledgments.

2.3 TOE Logical Boundaries

This section describes the logical scope of the TOE, i.e., the logical security features offered by the TOE, in terms of the following security functions: Audit; Identification and Authentication; Security Management; Protection of the TSF; and IDS Analyzer. In addition, this section identifies all capability to be provided by the operational environment, and those TOE capabilities excluded from the scope of evaluation.

2.3.1 TOE Security Features

2.3.1.1 Audit

ArcSight ESM 6.0c records two types of events, security events and analyzer events. The analyzer events include the events collected from the managed network via the SmartConnectors and discussed under the IDS Component Requirements. The security events relate to the proper functioning and use of the system, and allow authorized users to track the management functions performed. The TOE provides Administrators and Analyst Administrators with capabilities to review the generated security events. The Administrator and Analyst Administrator roles are able to select what security events are actually generated by the TOE. Generated security events are stored in the CORR-Engine. The TOE monitors the amount of space available for storing security events and sends a notification to a configured destination (e.g., an ESM Administrator) if the space drops below a configured level. In the event the security event storage space is exhausted, the Manager stops receiving events from SmartConnectors (which are then cached on the SmartConnector hosts) until such time as space becomes available.

2.3.1.2 Identification & Authentication

The ArcSight Manager maintains accounts of the authorized users of the system. The user account includes the following attributes associated with the user: user identity: authentication data (passwords), authorizations (groups or roles), and e-mail address information. This information is stored in the CORR-Engine. ESM requires users to provide unique identification and authentication data before any administrative access to the TOE is granted. ESM provides an authentication mechanism for users. The only authentication mechanism supported by the TOE is passwords.

2.3.1.3 Security Management

The ArcSight Console provides the authorized users with a graphical user interface (GUI) that can be used to configure and modify the functions of the TOE. The functions include the ability to manage user accounts, manage the Analyzer data, and manage the audit functions.

The TOE provides the following default security management roles: Administrator; Analyzer Administrator; Operator; and Analyst. The TOE enforces restrictions on which management capabilities are available to each role. Administrators and Analyzer Administrators are able to: modify the behavior of the analysis and reaction functions; determine which auditable events are included in the set of audited events; determine the analyzer events collected and processed by the TOE; and query and modify all other TOE data (except that Analyzer Administrators cannot modify user accounts).

2.3.1.4 Protection of the TSF

ESM is not intended to make data available to other IT products, in fact, in the case of a distributed ESM architecture, the components are expected to be connected with a benign, private, and protected communication network. ArcSight SmartConnectors, ArcSight Manager, and ArcSight Console all protect TSF data from disclosure and modification when transmitted between separate parts of the TOE, by communicating using SSL connections. The underlying operating system is required to provide protection for the TOE and its resources. The underlying operating system is also responsible for providing a reliable timestamp. The underlying operating system is considered part of the operational environment.

2.3.1.5 Analyzer Analysis, Reaction, Data Review and Availability

ESM collects relevant information from one or more network sources and subjects it to statistical and signature-based analysis, depending on configured rules. Rules trigger responses either on first match or after a given threshold has been passed. Notification destinations (e.g., authorized users) can be configured to be notified of a triggered rule at the ArcSight Console or e-mail. The authorized users can view the analyzer data, reports, to include the analytical results, query viewers, configuration information, and other applicable analyzer data that is collected. To prevent analyzer data loss, a warning is sent to a configured notification destination (e.g., ESM Administrator) should the database begin to run out of storage space for the Analyzer data records. The default setting for generating this notification is 90% of capacity.

2.3.2 Capabilities Provided by the Operational Environment

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

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

2.3.3 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:

- The ability of the TOE to send Security Events as SNMP traps.
- Support for external LDAP or RADIUS servers for user authentication.
- The ArcSight Manager, ArcSight Console, and ArcSight SmartConnector components all rely on properties files that are stored in the file system of the underlying operating system supporting each component. Each properties file is a text file containing pairs of keys and values. The keys determine which setting is configured and the value determines the configuration value. The TOE maintains two versions of each properties file—the default properties file and the user properties file. The default properties files are provided with the TOE. The user properties files are created during initial configuration of the TOE using the appropriate setup wizard (the Manager, Console and SmartConnector components each have their own setup wizard that is automatically launched as part of the component installation and configuration process). Settings in the user properties file for a component override settings in the defaults properties file for that component. The component first reads in the values in the default properties file, and then reads in the user properties file and updates any settings that have different values. Each component performs bounds and sanity checks on the configuration values before applying them to its configuration. The TOE is fully functional using the default properties set at install time. Manual modification of the properties files (e.g., using a text editor in the operational environment) is excluded for the evaluated configuration.

3. Security Problem Definition

The TOE security environment consists of threats to security, organizational security policies, and the secure usage assumptions as they relate to the TOE, ArcSight ESM 6.0c Patch 1 components; ArcSight SmartConnectors, ArcSight Manager with CORR-Engine, and ArcSight Console.

The TOE, ArcSight ESM 6.0c Patch 1, a subset of the ArcSight product[2] provides for a level of protection that is appropriate for IT environments that require:

a) Continuous information about devices and information on a network

b) Indications of vulnerabilities that exist on which network devices

The TOE is not designed to withstand physical attacks directed at disabling or bypassing security features; however, it is designed to withstand logical attacks originating from the attached network. The TOE is suitable for use in both commercial and government environments.

3.1 Threats to Security

The following are threats identified for the TOE and the IT System the TOE monitors. The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides.

[2] Refer to Section 1 for the list of the ArcSight ESM 6.0c Patch 1 software components included in the evaluated configuration and the components of the product that are not included within the scope of the evaluation.

3.1.1 TOE Threats

T.COMINT An unauthorized person may attempt to compromise the integrity of the data analyzed and produced by the TOE by bypassing a security mechanism.

T.COMDIS An unauthorized person may attempt to disclose the data analyzed and produced by the TOE by bypassing a security mechanism.

T.LOSSOF An unauthorized person may attempt to remove or destroy data analyzed and produced by the TOE.

T.NOHALT An unauthorized person may attempt to compromise the continuity of the TOEs analysis functionality by halting execution of the TOE.

T.PRIVIL An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.

T.IMPCON The TOE may be susceptible to improper configuration by an authorized or unauthorized person causing potential intrusions to go undetected.

T.INFLUX An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.

3.1.2 Analytical Threats

T.FALACT The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.

T.FALREC The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.

T.FALASC The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.

3.2 Organization Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address the security needs.

P.ANALYZ Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.

P.DETECT Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System must be collected.

P.MANAGE The TOE shall only be managed by authorized users.

P.ACCESS All data analyzed and generated by the TOE shall only be used for authorized purposes.

P.ACCACT Users of the TOE shall be accountable for their actions within the IDS.

P.INTGTY Data analyzed and generated by the TOE shall be protected from modification.

P.PROTCT The TOE shall be protected from unauthorized accesses and disruptions of analysis and response activities.

3.3 Secure Usage Assumptions

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

3.3.1 Intended Usage Assumptions

A.ACCESS The TOE has access to all the IT System resources necessary to perform its functions.

3.3.2 Physical Assumptions

A.PROTCT The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

A.LOCATE The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

3.3.3 Personnel Assumptions

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

A.NOEVIL The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

A.NOTRST The TOE can only be accessed by authorized users.

4. Security Objectives

This section identifies the security objectives of the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its environment in meeting the security needs. Modifications to the security objectives as described in the U.S. Government Protection Profile Intrusion Detection System Analyzer For Basic Robustness Environments, to which this ST claims compliance are identified in Section 7 Protection Profile Claims.

4.1 TOE Security Objectives

The following are the TOE security objectives:

O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
O.IDACTS	The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).
O.RESPON	The TOE must respond appropriately to analytical conclusions.
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.IDAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions and data.
O.OFLOWS	The TOE must appropriately handle potential audit and Analyzer data storage overflows.
O.AUDITS	The TOE must record audit records for data accesses and use of the Analyzer functions.
O.INTEGR	The TOE must ensure the integrity of all audit and Analyzer data.

4.2 Security Objectives for the Environment

The TOE's operating environment must satisfy the following objectives.

OE.TIME	The IT Environment will provide reliable timestamps to the TOE.
OE.AUDIT_PROTECTION	The IT Environment will provide the capability to protect audit information.
OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
OE.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
OE.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the Analyzer.
OE.INTROP	The TOE is interoperable with the IT System it monitors and other IDS components within its IDS.

5. IT Security Requirements

5.1 TOE Security Functional Requirements

This section specifies the security functional requirements (SFRs) for the TOE. All SFRs were drawn from Part 2 of the Common Criteria v3.1 Revision 3 and the Protection Profile (PP) identified in Protection Profile Claims section.

This ST includes a number of extended requirements. Each of the extended requirements is defined in the U.S. Government Protection Profile Intrusion Detection System Analyzer For Basic Robustness Environments. The extended requirements can be identified by the use of the keyword "EXT" in the title.

Every SFR included in the PP is addressed in this Security Target. Each SFR, except as noted in Section 7, was copied from the PP. Each SFR was changed in this ST to complete operations left incomplete by the PP or to make necessary refinements so that the intent of each SFR remains as specified in the PP. Each SFR was also changed, when necessary, to conform to International Interpretations and the version of the CC being claimed.

Security Functional Class	Security Functional Components
Security Audit (FAU)	Audit data generation (FAU_GEN.1)
	Audit review (FAU_SAR.1)
	Restricted audit review (FAU_SAR.2)
	Selectable audit review (FAU_SAR.3)
	Selective audit (FAU_SEL.1)
	Guarantees of audit data availability (FAU_STG.2)
	Prevention of audit data loss (FAU_STG.4)
Identification and authentication (FIA)	User attribute definition (FIA_ATD.1)
	Timing of authentication (FIA_UAU.1)
	Timing of identification (FIA_UID.1)
Security management (FMT)	Management of security functions behaviour (FMT_MOF.1)
	Management of TSF data (FMT_MTD.1)
	Specification of management functions (FMT_SMF.1)
	Security roles (FMT_SMR.1)
	Basic internal TSF data transfer protection (FPT_ITT.1) [3]
Protection of the TSF (FPT)	Analyzer analysis (EXT) (IDS_ANL.1)
IDS Component Requirements (IDS)	Analyzer react (EXT) (IDS_RCT.1)
	Restricted data review (EXT) (IDS_RDR.1)
	Guarantee of analyzer data availability (EXT) (IDS_STG.1)
	Prevention of analyzer data loss (EXT) (IDS_STG.2)

Table 3: Security Functional Components

[3] This requirement has been added to protect inter-communications, replacing FPT_ITA.1, FPT_ITC.1, and FPT_ITI.1) per PD-0127.

5.1.1 Security Audit (FAU)

5.1.1.1 Audit data generation (FAU_GEN.1)

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 [***basic***] level of audit; and
c) [**Access to the Analyzer and access to the TOE and Analyzer data]**.

Component	Event	Details
FAU_GEN.1	Start-up and shutdown of audit functions	
FAU_GEN.1	Access to Analyzer	
FAU_GEN.1	Access to the TOE Analyzer data	Object ID, Requested access
FAU_SAR.1	Reading of information from the audit records	
FAU_SAR.2	Unsuccessful attempts to read information from the audit records	
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating	
FAU_STG.4[4]	Actions taken due to audit storage failure	
FIA_UAU.1	All use of the authentication mechanism	User identity, location
FIA_UID.1	All use of the user identification mechanism	User identity, location
FMT_MOF.1	All modifications in the behavior of the functions of the TSF	
FMT_MTD.1	All modifications to the values of TSF data	
FMT_SMF.1	Use of the management functions	
FMT_SMR.1	Modifications to the group of users that are part of a role	User identity

Table 4: Auditable Events

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity **(if applicable)**, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**the additional information specified in the Details column of Table 4 Auditable Events**].

5.1.1.2 Audit review (FAU_SAR.1)

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

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

5.1.1.3 Restricted audit review (FAU_SAR.2)

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.

5.1.1.4 Selectable audit review (FAU_SAR.3)

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

[4] It appears the PP inadvertently omitted FAU_STG.4 from the table.

5.1.1.5 Selective audit (FAU_SEL.1)

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:
a) [***event type***]**;**
b) [**no additional attributes**].

5.1.1.6 Guarantees of audit data availability (FAU_STG.2)

FAU_STG.2.1 The TSF shall protect the stored audit records **in the audit trail** from unauthorized deletion.

FAU_STG.2.2 The TSF shall be able to [***prevent***] modifications to the audit records.

FAU_STG.2.3 The TSF shall ensure that [**the most recent, limited by available audit storage**] audit records will be maintained when the following conditions occur: [***audit storage exhaustion***]**.**

5.1.1.7 Prevention of audit data loss (FAU_STG.4)

FAU_STG.4.1 The TSF shall [***prevent auditable events, except those taken by the authorized user with special rights***[5]] and [**send an alarm**] [6] if the audit trail is full.

5.1.2 Identification and authentication (FIA)

5.1.2.1 User attribute definition (FIA_ATD.1)

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:
a) [**User identity;**
b) **Authentication data;**
c) **Authorizations (groups);**
d) **Email address; and**
e) **no other security attributes**].

5.1.2.2 Timing of authentication (FIA_UAU.1)

FIA_UAU.1.1 The TSF shall allow [**actions where the operational environment has authenticated the user**] on behalf of the user to be performed before the user is authenticated.

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

5.1.2.3 Timing of identification (FIA_UID.1)

FIA_UID.1.1 The TSF shall allow [**actions where the operational environment has identified the user**] on behalf of the user to be performed before the user is identified.

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

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

[5] The users with the "special rights" are those in one of the four security management roles (Administrator, Analyzer Administrator, Operator, Analyst).

[6] The PP indicates this operation as a selection, when in fact it is an assignment. The ST author has indicated the correct operation performed.

5.1.3 Security management (FMT)

5.1.3.1 Management of security functions behavior (FMT_MOF.1)

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

5.1.3.2 Management of TSF data (FMT_MTD.1)

FMT_MTD.1.1 The TSF shall restrict the ability to [***query* and add Analyzer and audit data, and shall restrict the ability to query and modify all other TOE data**] to [**Administrator, Analyzer Administrator (cannot modify user accounts)**].

Application Note: The statement "query and add Analyzer and audit data" in this requirement refers to the ability to look at and to change the set of events for which audit records and Analyzer data are actually collected. It does not refer to the capability of looking at and changing either the generated audit records or generated Analyzer results. The ability to look at the records within the audit trail is specified using FAU_SAR.1. The ability to look at the Analyzer data is specified using IDS_RDR.1. Furthermore, FMT_MTD.1 is included to satisfy a dependency of FAU_SEL.1. In order to satisfy this dependency, FMT_MTD.1 needs to address management of the selection of audited events from the set of auditable events.

5.1.3.3 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [**Management of Analyzer data, Management of Audit functions, Management of user accounts**].

5.1.3.4 Security roles (FMT_SMR.1)

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

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

5.1.4 Protection of the TOE security functions (FPT)

5.1.4.1 Basic internal TSF data transfer protection (FPT_ITT.1)

FPT_ITT.1 The TSF shall protect TSF data from [***disclosure***, ***modification***] when it is transmitted between separate parts of the TOE **by using SSL connections**.

5.1.5 IDS Component Requirements (IDS)

5.1.5.1 Analyzer analysis (EXT) (IDS_ANL.1)

IDS_ANL.1.1 The TSF shall perform the following analysis function(s) on all IDS data received:
a) [***statistical, signature***]; and
b) [**no other analytical functions**].

IDS_ANL.1.2 The TSF shall record within each analytical result at least the following information:
a) Date and time of the result, type of result, identification of data source; and
b) [**no other security relevant information about the result**].

5.1.5.2 Analyzer react (EXT) (IDS_RCT.1)

5.1.5.3 IDS_RCT.1.1

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

5.1.5.4 Restricted Data Review (EXT) (IDS_RDR.1)

IDS_RDR.1.1 The Analyzer shall provide [**Administrator, Analyzer Administrator, Operator, Analyst**] with the capability to read [**Analyzer events, reports (that includes the analytical results), query viewers, configuration information, and other applicable Analyzer data**] from the Analyzer data.

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

IDS_RDR.1.3 The Analyzer shall prohibit all users read access to the Analyzer data, except those users that have been granted explicit read-access. (EXP)

5.1.5.5 Guarantee of Analyzer Data Availability (EXT) (IDS_STG.1)

IDS_STG.1.1 The Analyzer shall protect the stored Analyzer data from unauthorized deletion. (EXP)

IDS_STG.1.2 The Analyzer shall protect the stored Analyzer data from modification. (EXP)

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

5.1.5.6 Prevention of Analyzer data loss (EXT) (IDS_STG.2)

IDS_STG.2.1 The Analyzer shall [***prevent Analyzer data, except those taken by the authorized user with special rights***[7]] and send an alarm if the storage capacity has been reached. (EXP)

5.2 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level 3 (EAL3) augmented with ALC_FLR.2 components as specified in Part 3 of the Common Criteria. Note that the EAL3 requirements that exceed EAL2 are indicated in italics in the following table. No operations are applied to the assurance components.

Requirement Class	Requirement Component
ADV: Development	ADV_ARC.1: Security architecture description
	ADV_FSP.3: Functional specification with complete summary
	ADV_TDS.2: Architectural design
AGD: Guidance documents	AGD_OPE.1: Operational user guidance
	AGD_PRE.1: Preparative procedures
ALC: Life-cycle support	*ALC_CMC.3: Authorisation controls*
	ALC_CMS.3: Implementation representation CM coverage
	ALC_DEL.1: Delivery procedures
	ALC_DVS.1: Identification of security measures
	ALC_FLR.2: Flaw reporting procedures
	ALC_LCD.1: Developer defined life-cycle model
ATE: Tests	*ATE_COV.2: Analysis of coverage*
	ATE_DPT.1: Testing: basic design
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing - sample

[7] The only user with the special rights is the authorized Administrator.

Requirement Class	Requirement Component
AVA: Vulnerability assessment	AVA_VAN.2: Vulnerability analysis

Table 5: EAL3 Assurance Components

5.2.1 Development (ADV)

5.2.1.1 Security architecture description (ADV_ARC.1)

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.

5.2.1.2 Functional specification with complete summary (ADV_FSP.3)

ADV_FSP.3.1D The developer shall provide a functional specification.

ADV_FSP.3.2D The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.3.1C The functional specification shall completely represent the TSF.

ADV_FSP.3.2C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.3.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.3.4C For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.

ADV_FSP.3.5C For each SFR-enforcing TSFI, the functional specification shall describe direct error messages resulting from security enforcing effects and exceptions associated with invocation of the TSFI.

ADV_FSP.3.6C The functional specification shall summarise the SFR-supporting and SFR-non-interfering actions associated with each TSFI.

ADV_FSP.3.7C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

ADV_FSP.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.3.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.2.1.3 Architectural design (ADV_TDS.2)

ADV_TDS.2.1D The developer shall provide the design of the TOE.

ADV_TDS.2.2D 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.2.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.2.2C The design shall identify all subsystems of the TSF.

ADV_TDS.2.3C The design shall describe the behaviour of each SFR non-interfering subsystem of the TSF in detail sufficient to determine that it is SFR non-interfering.

ADV_TDS.2.4C The design shall describe the SFR-enforcing behaviour of the SFR-enforcing subsystems.

ADV_TDS.2.5C The design shall summarise the SFR-supporting and SFR-non-interfering behaviour of the SFR-enforcing subsystems.

ADV_TDS.2.6C The design shall summarise the behaviour of the SFR-supporting subsystems.

ADV_TDS.2.7C The design shall provide a description of the interactions among all subsystems of the TSF.

ADV_TDS.2.8C The mapping shall demonstrate that all behaviour described in the TOE design is mapped to the TSFIs that invoke it.

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

ADV_TDS.2.2E The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

5.2.2 Guidance documents (AGD)

5.2.2.1 Operational user guidance (AGD_OPE.1)

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.

5.2.2.2 Preparative procedures (AGD_PRE.1)

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.

5.2.3 Life-cycle support (ALC)

5.2.3.1 Authorisation controls (ALC_CMC.3)

ALC_CMC.3.1D The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.3.2D The developer shall provide the CM documentation.

ALC_CMC.3.3D The developer shall use a CM system.

ALC_CMC.3.1C The TOE shall be labelled with its unique reference.

ALC_CMC.3.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.3.3C The CM system shall uniquely identify all configuration items.

ALC_CMC.3.4C The CM system shall provide measures such that only authorised changes are made to the configuration items.

ALC_CMC.3.5C The CM documentation shall include a CM plan.

ALC_CMC.3.6C The CM plan shall describe how the CM system is used for the development of the TOE.

ALC_CMC.3.7C The evidence shall demonstrate that all configuration items are being maintained under the CM system.

ALC_CMC.3.8C The evidence shall demonstrate that the CM system is being operated in accordance with the CM plan.

ALC_CMC.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.2 Implementation representation CM coverage (ALC_CMS.3)

ALC_CMS.3.1D The developer shall provide a configuration list for the TOE.

ALC_CMS.3.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; the parts that comprise the TOE; and the implementation representation.

ALC_CMS.3.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.3.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

ALC_CMS.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.3 Delivery procedures (ALC_DEL.1)

ALC_DEL.1.1D The developer shall document 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.

5.2.3.4 Identification of security measures (ALC_DVS.1)

ALC_DVS.1.1D The developer shall produce development security documentation.

ALC_DVS.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.1.2E The evaluator shall confirm that the security measures are being applied.

5.2.3.5 Flaw reporting procedures (ALC_FLR.2)

ALC_FLR.2.1D The developer shall document flaw remediation procedures addressed to TOE developers.

ALC_FLR.2.2D The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.

ALC_FLR.2.3D The developer shall provide flaw remediation guidance addressed to TOE users.

ALC_FLR.2.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.2.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.2.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.2.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

ALC_FLR.2.5C The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.

ALC_FLR.2.6C The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users.

ALC_FLR.2.7C The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

ALC_FLR.2.8C The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.

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

5.2.3.6 Developer defined life-cycle model (ALC_LCD.1)

ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2D The developer shall provide life-cycle definition documentation.

ALC_LCD.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

ALC_LCD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4 Tests (ATE)

5.2.4.1 Analysis of coverage (ATE_COV.2)

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that all TSFIs in the functional specification have been tested.

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

5.2.4.2 Testing: basic design (ATE_DPT.1)

ATE_DPT.1.1D The developer shall provide the analysis of the depth of testing.

ATE_DPT.1.1C The analysis of the depth of testing shall demonstrate the correspondence between the tests in the test documentation and the TSF subsystems in the TOE design.

ATE_DPT.1.2C The analysis of the depth of testing shall demonstrate that all TSF subsystems in the TOE design have been tested.

ATE_DPT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4.3 Functional testing (ATE_FUN.1)

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.

5.2.4.4 Independent testing - sample (ATE_IND.2)

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.

5.2.5 Vulnerability assessment (AVA)

5.2.5.1 Vulnerability analysis (AVA_VAN.2)

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 security functions implemented by the TOE to satisfy the SFRs.

6.1 Introduction

Each of the security function descriptions is organized by the security requirements corresponding to the security function. Each description serves to explain how the corresponding function specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions are suitable to satisfy the necessary requirements.

6.1.1 Security Audit

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

- External events—generated by IDS and IPS sensors and scanners in the TOE's operational environment and imported by the TOE for analysis. External events provide the source of the TOE's Analyzer data; they are discussed separately in Section 6.1.7.
- Internal events—these are divided into **audit events** and **status monitor events**. Status monitor events provide information on the status and performance of the TOE; they are not discussed further. Audit events provide information on TOE activity, including security-related activity.

6.1.1.1 Audit Data Generation (FAU_GEN.1)

The ArcSight Manager and the various SmartConnectors generate audit events—the SmartConnectors forward their audit events to the Manager. All audit events are stored in CORR-Engine, which is a component of the ESM Suite. ESM is relied upon to protect the data stored in the CORR-Engine, including the audit events.

The audit events the TOE can generate include:

- The start-up and shutdown of audit functions (the audit function automatically starts at system start-up and can only be shutdown at system shutdown. In both instances, a record of the event is recorded.)
- Access to Analyzer
- Access to the TOE Analyzer data
- Reading of information from the audit records
- Unsuccessful attempts to read information from the audit records
- All modifications to the audit configuration that occur while the audit collection functions are operating
- 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
- Use of the management functions
- Modifications to the group of users that are part of a role
- Actions taken by the TOE when the storage space for audit records reaches capacity.

6.1.1.2 Audit Data Review (FAU_SAR.1, FAU_SAR.2, FAU_SAR.3)

The ArcSight Console provides users in the Administrator and Analyzer Administrator roles the ability to view the audit events—these users are expected to view the audit events using the ArcSight Console. Access to the audit events via the ArcSight Console is restricted to the Administrator and Analyzer Administrator roles.

The audit events include the date and time of the event, the type of event, the subject identity, and the outcome of the event, such as whether it was a success or failure. The TOE relies on and obtains a reliable date/timestamp from

the operational environment. The audit events are presented by the ArcSight Console in a readable format—as such, Administrators and Analyzer Administrators can read and interpret the content of the information. In addition, Administrators and Analyzer Administrators can sort the audit events based on the following event attributes: date and time of the event; subject identity; type of event; and success or failure of the related event.

6.1.1.3 Selectable Audit (FAU_SEL.1)

The ArcSight Console provides Administrators and Analyzer Administrators the ability to include or exclude auditable events based on event type. Administrators and Analyzer Administrators can select to record or not record activity based on a particular event—for example, all use of the authentication mechanism or all modifications in the behavior of the functions of the TSF.

6.1.1.4 Protection of Stored Audit Records (FAU_STG.2, FAU_STG.4)

The ArcSight Manager does not provide any interfaces to modify the audit records. To prevent audit data loss, a warning is sent to a configured notification destination (e.g., an ESM Administrator) should the database begin to run out of storage space for the audit records. Events are stored on a 30-day retention period based on Manager Receipt Time (MRT) of the event. As events age out, the oldest events are removed to make room for the day's events. The default setting for generating the first notification is at 90% of capacity. If the storage space for audit records reaches 98% capacity, space-based retention, which is 26 Gb maximum for events, automatically takes over and another notification is sent. At this time, the oldest events are deactivated to free up space. All incoming ArcSight SmartConnectors events are stopped and all events that are currently being processed are stored temporarily in memory of the underlying operating system of the ArcSight Manager until the storage space problem is cleared. The ArcSight Manager continues to create audit events for any scheduled actions or actions triggered by the processing of any events received prior to the storage failure. Once space is free, the ArcSight Manager begins receiving events from active ArcSight SmartConnectors.

6.1.2 Identification and Authentication

6.1.2.1 User Attribute Definition (FIA_ATD.1)

The ArcSight Manager maintains accounts of the authorized users of the TOE. The user account includes the following attributes associated with the user: user identity; authentication data (password); authorizations (groups, which equate to roles); and e-mail addressinformation. To protect the passwords, the ArcSight Manager stores only MD5 hashes of the passwords in the database. The ArcSight Console provides the GUI for Administrators to create and maintain the user accounts.

6.1.2.2 User Identification and Authentication (FIA_UID.1, FIA_UAU.1)

The ArcSight Console requires authorized users to provide unique identification and authentication data (password) before any administrative access to the ArcSight Console is granted. Each authorized user must be successfully authenticated by providing the correct password associated with the user identity. The TOE enforces the following restrictions on passwords:

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

To login to the ArcSight Console, the user provides the login name and password. The ArcSight Console compares the SHA 256 hash of the password to that stored in the CORR-Engine. If either the login name or the password is incorrect, the login request fails and no administrator functions are made available. As result of a successful login, the console session is established and the administrator functions appropriate to the user's assigned roles are made available. The TOE allows a maximum three consecutive failed login attempts, after which the user account is locked for 10 minutes.

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

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

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

6.1.3 Security Management

6.1.3.1 Security Management Roles (FMT_SMR.1)

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

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

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

6.1.3.2 Management of Security Functions Behavior (FMT_MOF.1)

The TOE requires user authentication before any administrative actions, security-related or otherwise, can be performed (other than entry of identification and authentication data) on the ArcSight Console. As a result, only users belonging to one of the security management roles (Administrator, Analyzer Administrator, Operator or

Analyst) can access any function on the TOE via the ArcSight Console. The Administrator and Analyzer Administrator roles have the capabilities to modify the behavior of the TOE's analysis and reaction functions, by virtue of having read and write access to the various TOE resources that control how the TOE analyzes and reacts to security events.

6.1.3.3 Management of TSF Data (FMT_MTD.1)

Users with the Administrator or Analyzer Administrator role have the ability to query and modify the configuration of the TOE as it relates to the generation of Analyzer data. The Administrators and Analyzer Administrators can create, modify, delete, configure, and implement the rules on the TOE and the filters that determine which auditable events are actually audited. The Administrator is the only role that can create and modify user accounts.

6.1.3.4 Specification of Management Functions (FMT_SMF.1)

The ArcSight Console implements the GUI that provides the Administrators, Analyzer Administrators, Operators and Analysts with the interface to perform essential security management tasks. The tasks include the ability to manage user accounts, manage the Analyzer data, and manage the audit functions.

6.1.4 Protection of the TSF

6.1.4.1 Internal TOE TSF data transfer (FPT_ITT.1)

The TOE can be configured in either of two security modes: non-FIPS mode (the default mode); and FIPS 140-2 compliant mode. The configured security mode determines the cryptographic protocol and the underlying cryptographic provider the TOE uses to implement secure subsystem communications. In non-FIPS mode, communications between the SmartConnectors and the Manager, and between the Console and the Manager, are protected using SSL v3.0. In this mode, the TOE uses SunJCE and Bouncy Castle as the cryptographic providers—SunJCE is used for SSL and most other cryptographic needs, while Bouncy Castle is used for certificate generation in the TOE's setup wizard. The TOE uses X.509 Version 3 certificates. The maximum key size for the public key in the certificate is 1024 bits.

In FIPS 140-2 mode, the TOE uses the FIPS 140-2 validated Network Security Services (NSS) cryptographic module, version 3.11.4 (FIPS 140-2 certificate 814). Communications between the TOE components are protected using TLS v1.0.

For SSL communication, all TOE components that are SSL endpoints (i.e., ArcSight Console, ArcSight Manager, and ArcSight SmartConnectors) need to store two types of key material:

- Key Pairs, consisting of a private key and the matching public key wrapped in a X.509 certificate
- X.509 Certificates of certificate authorities (CAs) whose certificates are trusted.

ArcSight Manager is always the SSL server, and ArcSight SmartConnectors and the ArcSight Console that communicates with it, always represent the SSL client. When a SSL connection is established, the client and server authenticate one another, using the key pairs and certificates in their key stores and trust stores.

The server authentication mechanism in SSL requires the ArcSight Manager to have a valid SSL certificate. An SSL certificate contains the ArcSight Manager's public key. The public key is used by the client to encrypt information. Only the ArcSight Manager (using its private key) can decrypt this information. ArcSight Manager's SSL certificate contains a date range for which it is valid as well as the ArcSight Manager's host name.

The SunJCE provider used in non-FIPS mode supplies the following cryptographic services:

- An implementation of the DES and Triple DES symmetric encryption algorithms in Cipher Block Chaining (CBC) mode
- An implementation of the RSA asymmetric encryption algorithm
- An implementation of the HMAC-MD5 and HMAC-SHA1 keyed-hashing algorithms
- An implementation of the Diffie-Hellman key agreement algorithm between two or more parties
- Key generators for generating keys suitable for the DES, Triple DES, HMAC-MD5, and HMAC-SHA1 algorithms

- A Diffie-Hellman key pair generator for generating a pair of public and private values suitable for the Diffie-Hellman algorithm.

The NSS cryptographic module used in FIPS 140-2 mode supplies the following cryptographic services:

- An implementation of the AES (FIPS 197) symmetric encryption algorithm
- Implementations of the Secure Hash Standard (SHA-1, SHA-256, SHA-384, and SHA-512) (FIPS 180-2) for hashing
- An implementation of HMAC (FIPS 198) for keyed hash
- A random number generator (FIPS 186-2 with Change Notice 1) to support encryption key generation
- Implementations of Diffie-Hellman, EC Diffie-Hellman, and Key Wrapping using RSA keys for key establishment
- Implementations of DSA (FIPS 186-2 with Change Notice 1) and RSA (PKCS #1 v2.1) for signature generation and verification.

The following cipher suites are enabled by default:

- TLS_RSA_WITH_AES_128_CBC_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_WITH_RC4_128_MD5
- SSL_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5

Other supported cipher suites are:

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_WITH_DES_CBC_SHA
- SSL_DHE_RSA_WITH_DES_CBC_SHA
- SSL_DHE_DSS_WITH_DES_CBC_SHA
- SSL_RSA_EXPORT_WITH_RC4_40_MD5
- SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
- SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
- SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
- SSL_RSA_WITH_NULL_MD5
- SSL_RSA_WITH_NULL_SHA
- SSL_DH_anon_WITH_RC4_128_MD5
- TLS_DH_anon_WITH_AES_128_CBC_SHA
- SSL_DH_anon_WITH_3DES_EDE_CBC_SHA
- SSL_DH_anon_WITH_DES_CBC_SHA
- SSL_DH_anon_EXPORT_WITH_RC4_40_MD5
- SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA

The following are the only ciphersuites available in FIPS mode:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA

The TOE does not provide the protection described above for the data transmitted to the CORR-Engine. Since the CORR-Engine is part of the ArcSight Manager installation, no additional form of physical security is required.

6.1.5 Analyzer Analysis

6.1.5.1 Analyzer Analysis (IDS_ANL.1)

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

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

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

6.1.6 Analyzer React

6.1.6.1 Analyzer React (IDS_RCT.1)

Rule actions are automatic procedures that occur when all rule conditions and threshold settings have been met. A rule is a programmed procedure that can analyze network events and generate additional correlation events, as determined by security policy. When creating rules, the Analyzer Administrators[8] define the rule events and conditions, thresholds, and rule actions. Conditions define which events trigger the rule, thresholds set when a correlation event is generated, and actions state which responses are taken when a correlation event is generated. A rule requires at least one event and one condition. The Analyzer Administrator can also assign more than one rule action to any rule. For example, the notification rule actions are used to inform ArcSight users that an incident has occurred. The notification may be delivered to the user on the ArcSight Console or by email. Rule actions can also be set to send information about the event to a case or active list.

- Cases are entries in an event-tracking system used to track, investigate, and resolve suspicious events in a workflow-type environment. When suspicious events occur, cases are created and assigned to users, who then investigate and resolve them based on enterprise policies and practices.
- Active list can be used to create a configurable data store that can hold information derived from events or other sources. Active lists can monitor activity based on any rule-driven combination of event attributes or set of custom fields. For example, active lists are very useful for tracking suspicious or hostile IP addresses as well as targets of attacks that may be compromised. The main uses of active lists are to:
    - Maintain information, such as in the system content provided “Hostile List” or “Trusted List”, which maintain information on hostile and trusted IP addresses (and corresponding zones)
    - Check for the existence of particular information in lists using the InActiveList condition. For example, when a system is compromised (such as in a security breach), it can be added to the compromise list using rule actions. The information in the active list can then be used to collect all the events that occur on the asset while it is compromised. This can be used for tracking and further investigation on other systems that have come into contact with the compromised system.

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

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

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

6.1.7 Analyzer Data Review and Availability

6.1.7.1 Restricted Data Review (IDS_RDR.1)

In an ArcSight ESM 6.0c Patch 1 environment, only successfully authenticated users can access the ArcSight Console and only users who hold the appropriate authorization can view the data. Using the ArcSight Console GUI, Administrators can view the overall health of the enterprise as well as the data collected. The Administrators can also view the analyzer event data, reports, to include the analytical results, query viewers, configuration information, and other applicable analyzer data that is collected. In addition, the Analyzer Administrator can view analyzer configuration and analyzer data. The Operators and Analysts can view the analyzer data collected via the ArcSight Console. The Operator can also create reports or query viewers, as can the Analyzer Administrator and Administrator.

- The reports are captured views or summaries of data that can be viewed in the ArcSight Console or exported for sharing in a variety of file formats. Authorized users can create reports by pulling together the result sets from one or more queries (a query is an ArcSight resource that defines the parameters of data to gather from an ArcSight data source) or trends (a trend is an ArcSight resource that defines how and over what time period data will be evaluated for trends. A trend is always based on a query).
- The query viewers are a type of resource for defining and running SQL queries on other TOE resources, including trends, assets, cases, connectors, events, and so forth. Each query viewer contains an SQL query along with other logic for establishing and comparing baseline results, analyzing historical data to find patterns in network activity, and performing drill-down investigation on a particular aspect of the results.

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

6.1.7.2 Guarantee of Analyzer Data Availability (IDS_STG.1)

All users must be identified and authenticated. In an ESM environment, only successfully identified and authenticated users can access the ArcSight Console, and then only users who hold the appropriate authorization can view the data that is collected and analyzed by ArcSight SmartConnectors.

The TOE provides a mechanism for managing database storage of the potentially large amount of events that can be collected and generated by the TOE. The TOE is able to "package" chronological sections of past data for reasonable retrieval and reuse through database partition management. Partition management is established and configured during installation of the TOE. The Partitions tree in the ArcSight Console provides the Administrator role with capabilities to manage partitions.

A time-based retention is a time-delimited record of database activity. The default 30 days. The TOE uses partitions as a means of controlling and storing volumes of past events to facilitate subsequent analysis.

Events remain active according to the time-based retention set initially during installation. The events stored during the oldest day within the given retention period are removed to make room for newer events.

Along with time-based retention period, ESM is also configured for space-based retention, the default is 26 GB of event storage. Space-based retention automatically executes when capacity is reached at 98%.

6.1.7.3 Prevention of Analyzer Data Loss (IDS_STG.2)

To prevent analyzer data loss, two warnings are sent to a configured notification destination (e.g., Administrator) in the event the database begins to run out of storage space for the analyzer data records. The first notification comes in the form of a warning and is sent at 90% of capacity. The second notification comes in the forn of an error and is sent at 98% of capacity.

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

If the ArcSight Manager fails, the ArcSight SmartConnectors cache the data and wait for the ArcSight Manager to return. Analyzer data in memory at the time of the crash may be lost. The correlation facility of the product periodically writes a checkpoint of its state. When the checkpoint is reloaded, all previously stored events that occurred between the time of the checkpoint and the crash are replayed in order to restore the state of correlation prior to the crash. At which time when the ArcSight Manager comes back on-line, it will receive all cached and live events from the ArcSight SmartConnectors.

If an ArcSight SmartConnector fails, it will on re-starting resume processing with the next log file line or database row.

7. Protection Profile Claims

The TOE conforms to the U.S. Government Protection Profile Intrusion Detection System Analyzer For Basic Robustness Environments, Version 1.3, July 25, 2007. In addition, ArcSight has elected to pursue a more vigorous assurance level as depicted in Section 1.2, Conformance Claims.

Section 1.3 of the U.S. Government Protection Profile Intrusion Detection System Analyzer For Basic Robustness Environments, Version 1.3, July 25, 2007 states "…STs that claim conformance to this PP shall meet a minimum standard of demonstrable-PP conformance…". This ST is a suitable solution to the generic security problem described in the PP. Following are the changes to the PP defined security problem definition, security objectives, and security requirements. All changes in the ST are equivalent to or more restrictive than stated in the PP.

This Security Target includes all of the assumptions, organizational security policies, and threats statements described in the PP, verbatim.

This Security Target includes all of the Security Objectives from the PP, verbatim, except as noted below.

> The security objective, O.EXPORT was removed from the ST since the TOE does not transmit data to external IT products
>
> The operational environment security objective, OE.AUDIT_SORT was removed since the TOE performs this function and does not rely on the operating environment.

This Security Target includes all of the Security Functional and Security Assurance Requirements from the PP verbatim, except as noted below.

Requirement Component	Modification of Security Functional and Security Assurance Requirements
FAU_GEN.1	Refined to be compliant with CC v3.1, Revision 3.
FAU_SAR.1	Assignment – completed the assignment.
FAU_SEL.1	Assignment – completed the assignment.
FAU_STG.2	Assignment – completed the assignment. Selection - Changed the selection to prevent since the TOE does not offer any interfaces to modify audit records.
FAU_STG.4	Selection – completed the selection. Assignment - completed the assignment. In addition, the PP indicates this operation as a selection, when in fact the operation is an assignment. The ST author has indicated the correct operation performed.
FIA_AFL.1	Removed – the requirement was removed from the ST since the TOE does not allow or support access from external IT products. In addition, the authentication mechanism is SSL, and therefore this requirement is not applicable. Reference PD-0127.
FIA_ATD.1	Assignment - completed the assignment.
FIA_UAU.1	Assignment – completed the assignment.
FIA_UID.1	Assignment – completed the assignment.
FMT_MOF.1	Refinement – to correctly identify the role(s) supported by the TOE.
FMT_MTD.1	Assignment – completed the assignment.

Requirement Component	Modification of Security Functional and Security Assurance Requirements
FMT_SMF.1	Added – this requirement was added in this Security Target to satisfy a dependency added to FMT_MOF.1 by International Interpretation RI#65 that was adapted in CC Part 2, v2.3. This requirement simply requires that security functions actually be present in addition to being protected if they are present and therefore does not impact PP conformance.
FMT_SMR.1	Refinement - replaced the PP-defined roles of authorized Administrator and authorized Analyzer administrator with the TOE-defined roles of Administrator, Analyzer Administrator, Operator, and Analyst. The Administrator and Analyzer Administrator roles defined by the TOE satisfy the PP requirement for the authorized Analyzer Administrator, while the Operator and Analyst roles defined by the TOE satisfy the PP requirement for the authorized Administrator.
FPT_ITA.1	Removed – The TOE does not transmit data to external IT products, and therefore this requirement is not applicable.
FPT_ITC.1	Removed – The TOE does not transmit data to external IT products, and therefore this requirement is not applicable
FPT_ITI.1	Removed – The TOE does not transmit data to external IT products, and therefore this requirement is not applicable
FPT_ITT.1	Added – Since the TOE does not does not communicate with IDS components outside of the IDS system TOE the FPT_ITA.1, FPT_ITC.1, and FPT_ITI.1 SFRs were removed. The requirement, FPT_ITT.1 was added to protect inter-communications between the distributed TOE components. Selection – completed the selection.
FPT_STM.1	Removed – The TOE relies on the operational environment to provide a reliable timestamp as indicated by the security objective for the environment OE.TIME.
IDS_ANL.1	Selection – completed the selection. Assignment - completed the assignment.
IDS_RCT.1	Assignment - completed the assignment.
IDS_RDR.1	Assignment - completed the assignment.
IDS_STG.1	Assignment – completed the assignment. Selection – completed the selection.
IDS_STG.2	Selection – completed the selection.
EAL3	Added – the PP requires only EAL2. However, to satisfy the assurance requirements of the environment which requires more assurance that the security functions are enforced, this Security Target has adopted the EAL3 security assurance requirements.

Table 6: Modification of PP claims

8. 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;
- Extended Requirements;
- TOE Summary Specification; and,
- PP Claims

8.1 Security Objectives Rationale

The TOE conforms to the U.S. Government Protection Profile Intrusion Detection System Analyzer For Basic Robustness Environments, Version 1.3, July 25, 2007.

This Security Target includes all of the Security Objectives for the TOE from the PP, verbatim, except as noted below.

> The security objective, O.EXPORT was removed from the ST since the TOE does not transmit data to external IT products. Reference PD-0127.

This Security Target includes all of the Security Objectives for the Environment from the PP, verbatim, except as noted below.

> The operational environment security objective OE.AUDIT_SORT is not applicable to the environment for this TOE and was removed from the ST. The security objectives for the TOE provide the ability to sort the audit logs and provide protection of the audit trail.

The security objective rationale is presented in Section 6.1 and Section 6.2 of the U.S. Government Protection Profile Intrusion Detection System Analyzer For Basic Robustness Environments.

8.2 Security Requirements Rationale

The security requirements rationale is presented in Section 6.3 of the U.S. Government Protection Profile Intrusion Detection System Analyzer For Basic Robustness Environments.

All of the security functional requirements have been reproduced from the U.S. Government Protection Profile Intrusion Detection System Analyzer For Basic Robustness Environments to this ST, except as noted below:

The following security functional requirements were added to the ST:

- FMT_SMF.1 – this requirement was included to satisfy a dependency of FMT_MOF.1 introduced by International Interpretation RI#65 that was adapted in CC Part 2, v2.3. FMT_SMF.1 requires that a defined set of security management functions are made available so that an administrator can effectively manage the security configuration of the TOE. This security functional requirement provides direct support for the O.EADMIN security objective.
- FPT_ITT.1 – this requirement was included to protect inter-communications in lieu of FPT_ITA.1, FPT_ITC.1, and FPT_ITI.1. ArcSight ESM 6.0c is not intended to make data available to other IT products. In fact, the distributed ArcSight ESM 6.0c architecture components should be connected with a benign, private, and protected communication network. This security functional requirement provides direct support for the O.PROTCT and O.INTEGR security objectives. Reference PD-0127.

The following security functional requirements were removed from the ST:

- FIA_AFL.1 – this requirement is intended to detect attempts to access the TOE by untrusted external IT products. The TOE supports SSL authentication mechanism when transmitting data between TOE components. The TOE does not support or allow access to the TOE from external IT products, therefore this requirement is not applicable. Reference PD-0127.
- FPT_ITA.1 – this requirement is intended to specify how audit and Analyzer data are made available to external (trusted) IT products that would provide audit and Analyzer data services. Since the TOE provides these functions internally, no external IT products are necessary. Even though this requirement is trivially satisfied, it is not applicable. Note that when the TOE is distributed, TSF data is transferred over a network that is protected from associated threats. Reference PD-0127.
- FPT_ITC.1 – this requirement is intended to specify how TSF data is protected while transmitted to external (trusted) IT products. Since the TOE provides all functionality for the Analyzer in a self-contained manner, no data is transferred to external products. Even though this requirement is trivially satisfied, it is not applicable. Note that when the TOE is distributed, TSF data is transferred over a network that is protected from associated threats. Reference PD-0127.
- FPT_ITI.1 - this requirement is intended to specify how modifications to TSF data can be detected when it is transmitted to external (trusted) IT products. This includes both integrity checks and detection of modification during transmission. Since the TOE does not transmit data to external products. Even though this requirement is trivially satisfied, it is not applicable. Note that when the TOE is distributed, TSF data is transferred over a network that is protected from associated threats. Reference PD-0127.

Removal of these requirements does not have any impact on other security functional requirements.

8.3 Security Assurance Requirements Rationale

ArcSight has elected to pursue a more rigorous assurance level than as specified in U.S. Government Protection Profile Intrusion Detection System Analyzer For Basic Robustness Environments to EAL3 augmented with ALC_FLR.2, as specified in section 1.2 of this ST. EAL3 was chosen to provide a moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the TOE may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. In addition, augmentation was chosen to provide the added assurances that result from having flaw remediation procedures and correcting security flaws as they are reported.

The TOE meets all the U.S. Government Protection Profile Intrusion Detection System Analyzer For Basic Robustness Environments assurance requirements as stated in Section 6.5 for EAL2. Additionally, the TOE conforms to all the assurance requirements for an EAL3 product. The resulting assurance level is therefore, EAL3 augmented with ALC_FLR.2.

The EAL3 requirements that exceed EAL2 by the U.S. Government Protection Profile Intrusion Detection System Analyzer For Basic Robustness Environments are rationalized below:

- ADV Development; ADV_FSP.3 Functional specification with complete summary
  - It is important to document the SFR-supporting and SFR-non-interfacing actions and error messages to demonstrate they are not SFR-enforcing.
- ADV Development; ADV_TDS.2 Architectural design
  - It is important to provide sufficient information to determine the TSF boundary and to describe how the TSF implements the security functional requirements.
- ALC Life-cycle support; ALC_CMC.3 Authorisation controls
  - It is important to demonstrate the CM operates in accordance with the CM Plan.
- ALC Life-cycle support; ALC_CMS.3 Implementation representation CM coverage

  - It is important to demonstrate that the parts that comprise the TOE that are under CM control are in fact modified in a controlled manner with proper authorization.

- ALC Life-cycle support; ALC_DVS.1 Identification of security measures
  - It is important to demonstrate the physical security of the development facility as well as personnel, procedural, and other security measures as deemed appropriate.
- ALC Life-cycle support; ALC_LCD.1 Developer defined life-cycle model
  - It is important to demonstrate the controlled development and maintenance of the TOE.
- ATE Tests; ATE_COV.2 Analysis of coverage
  - It is important to demonstrate the TSF has been tested against the functional specification and that the test documentation corresponds to all the TSFIs in the functional specification.
- ATE Tests; ATE_DPT.1 Testing basic design
  - It is important to demonstrate the TSF subsystems behave and interact as described in the architectural description.

8.4 Requirements Dependency Rationale

The dependency requirements rationale is presented in Section 6.6 of the U.S. Government Intrusion Detection System Analyzer Protection Profile.

This Security Target includes two Security Functional Requirements not included in the U.S. Government Intrusion Detection System Analyzer Protection Profile; FMT_SMF.1 and FPT_ITT.1. The requirement, FMT_SMF.1 was included to satisfy a dependency of FMT_MOF.1 and FMT_MTD.1 introduced by International Interpretation RI#65 that was adapted in CC Part 2, v2.3 and is included CC v3.1. The SFR introduces no additional dependencies itself. The requirement FPT_ITT.1 was included to support inter-communications in lieu of FPT_ITA.1, FPT_ITC.1, and FPT_ITI.1. The requirement FPT_ITT.1 does not introduce any dependency requirements.

8.5 Extended Requirements Rationale

There are no extended requirements beyond those in the U.S. Government Protection Profile Intrusion Detection System Analyzer For Basic Robustness Environments.

The extended requirements rationale is presented in Section 6.4 of the U.S. Government Protection Profile Intrusion Detection System Analyzer For Basic Robustness Environments.

8.6 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is organized by requirement with rationale that indicates how each requirement is satisfied by aspects of the corresponding security function. This set of security functions work together in order to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to fulfill the TOE security requirements. The following table identifies the relationship between security requirements and security functions, showing that all security requirements are addressed and all security functions are necessary (i.e., they correspond to at least one security requirement).

	Security Audit	Identification & Authentication	Security Management	Protection of the TSF	IDS Analyzer
FAU_GEN.1	X				
FAU_SAR 1	X				
FAU_SAR.2	X				
FAU_SAR.3	X				
FAU_SEL.1	X				
FAU_STG.2	X				
FAU_STG.4	X				
FIA_UAU.1		X			
FIA_ATD.1		X			
FIA_UID.1		X			
FMT_MOF.1			X		
FMT_MTD.1(a)			X		
FMT_MTD.1(b)			X		
FMT_SMF.1			X		
FMT_SMR.1			X		
FPT_ITT.1				X	
IDS_ANL.1					X
IDS_RCT.1					X
IDS_RDR.1					X
IDS_STG.1					X
IDS_STG.2					X

Table 7: Security Functions vs. Requirements Mapping

8.7 PP Claims Rationale

See the *Protection Profile Claims* section.