National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

ArcSight ESM 4.5 SP3 Patch 2

Report Number: CCEVS-VR-VID10423-2012
Dated: 05 October 2012
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Dr. Patrick Mallett, The Mitre Corporation

Paul Bicknell CISM, CISSP, The Mitre Corporation

Common Criteria Testing Laboratory

SAIC
Columbia, MD

Table of Contents

List of Tables

1 Executive Summary

The evaluation of the ArcSight ESM 4.5 SP3 Patch 2 product was performed by Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America and was completed in October 2012. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1 Revision 3. The evaluation was consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The SAIC evaluation team determined that the product is Common Criteria Part 2 Extended and Common Criteria Part 3 Conformant, and that the Evaluation Assurance Level (EAL) for the product is EAL 3 augmented with ALC_FLR.2. The information in this Validation Report is largely derived from the Evaluation Technical Report (ETR) and associated test reports produced by the SAIC evaluation team. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The TOE 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 centralized ArcSight Database, and then filters and correlates those events with rules to generate meta-events. The TOE is comprised of the ArcSight Console, ArcSight Manager, ArcSight Database, and ArcSight SmartConnectors: NessusNSR, Checkpoint-OPSECNG, SnortDB, and Cisco Secure IPS SDEE.

The TOE, when configured as specified in the guidance documentation, satisfies all of the security functional requirements stated in the ArcSight ESM 4.5 SP3 Patch 2 Security Target (ST).

1.1 Evaluation Details

Table 1 – Evaluation Details

Evaluated Product:	ArcSight ESM 4.5 SP3 Patch 2, comprising:
	o ArcSight Console:
	  o ArcSight-4.5.3.6126.0-Console-Win.exe with Patch-4.5.3.6152.2-Console-Win.exe
	  o ArcSight-4.5.3.6126.0-Console-Linux.bin with Patch-4.5.3.6152.2-Console-Linux.bin
	  o ArcSight-4.5.3.6126.0-Console-Solaris.bin with Patch-4.5.3.6152.2-Console-Solaris.bin
	o ArcSight SmartConnectors (SnortDB, NessusNSR, Checkpoint-OPSECNG, Cisco Secure IPS SDEE)
	  o ArcSight-4.8.2.5516.0-Connector-Win.exe
	  o ArcSight-4.8.2.5516.0-Connector-Linux.bin
	  o ArcSight-4.8.2.5516.0-Connector-Solaris.bin
	o ArcSight Manager:
	  o ArcSight-4.5.3.6126.0-Manager-Linux.bin with Patch-4.5.3.6152.2-Manager-Linux.bin
	  o ArcSight-4.5.3.6126.0-Manager-Linux64.bin with Patch-4.5.3.6152.2-Manager-Linux64.bin
	  o ArcSight-4.5.3.6126.0-Manager-Solaris.bin with Patch-4.5.3.6152.2-Manager-Solaris.bin
	  o ArcSight-4.5.3.6126.0-Manager-Win.exe with Patch-4.5.3.6152.2-Manager-Win.exe
	  o ArcSight-4.5.3.6126.0-Manager-Win64.exe with Patch-4.5.3.6152.2-Manager-Win64.exe
	o ArcSight Database:
	  o ArcSight-4.5.3.6126.0-DB-Linux.bin with Patch-4.5.3.6152.2-DB-Linux.bin
	  o ArcSight-4.5.3.6126.0-DB-Solaris.bin with Patch-4.5.3.6152.2-DB-Solaris.bin
	  o ArcSight-4.5.3.6126.0-DB-Win.exe with Patch-4.5.3.6152.2-DB-Win.exe

Sponsor:	**ArcSight, an HP Company** 1140 Enterprise Way Sunnyvale, CA 94089
Developer:	**ArcSight, an HP Company** 1140 Enterprise Way Sunnyvale, CA 94089
CCTL:	Science Applications International Corporation 6841 Benjamin Franklin Drive Columbia, MD 21046
Kickoff Date:	January 2010

Completion Date:	5 October 2012
CC:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009
Interpretations:	None
CEM:	Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, Version 3.1, Revision 3, July 2009.
Evaluation Class:	EAL 3 augmented with ALC_FLR.2
Description:	ArcSight ESM 4.5 SP3 Patch 2 is an intrusion detection system (IDS) analyzer.
Disclaimer:	The information contained in this Validation Report is not an endorsement of the ArcSight ESM 4.5 SP3 Patch 2 product by any agency of the U.S. Government and no warranty of the product is either expressed or implied.
PP:	U.S. Government Protection Profile Intrusion Detection System Analyzer For Basic Robustness Environments, Version 1.3, July 25, 2007.
Evaluation Personnel:	Science Applications International Corporation: Katie Sykes Dawn Campbell Julie Cowan
Validation Body:	National Information Assurance Partnership CCEVS

1.2 Interpretations

Not applicable.

1.3 Threats

The ST identifies the following threats that the TOE and its IT environment are intended to counter:

- An unauthorized person may attempt to compromise the integrity of the data analyzed and produced by the TOE by bypassing a security mechanism.
- An unauthorized person may attempt to disclose the data analyzed and produced by the TOE by bypassing a security mechanism.
- An unauthorized person may attempt to remove or destroy data analyzed and produced by the TOE.
- An unauthorized person may attempt to compromise the continuity of the TOEs analysis functionality by halting execution of the TOE.

- An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
- The TOE may be susceptible to improper configuration by an authorized or unauthorized person causing potential intrusions to go undetected.
- An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.
- The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.
- The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.
- The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.

1.4 Organizational Security Policies

The ST identifies the following organizational security policies that the TOE and its IT environment are intended to fulfill:

- Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.
- 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.
- The TOE shall only be managed by authorized users.
- All data analyzed and generated by the TOE shall only be used for authorized purposes.
- Users of the TOE shall be accountable for their actions within the IDS.
- Data analyzed and generated by the TOE shall be protected from modification.
- The TOE shall be protected from unauthorized accesses and disruptions of analysis and response activities.

2 Identification

The evaluated product is **ArcSight ESM 4.5 SP3 Patch 2**, comprising:

- ArcSight Console:
  - ArcSight-4.5.3.6126.0-Console-Win.exe with Patch-4.5.3.6152.2-Console-Win.exe
  - ArcSight-4.5.3.6126.0-Console-Linux.bin with Patch-4.5.3.6152.2-Console-Linux.bin
  - ArcSight-4.5.3.6126.0-Console-Solaris.bin with Patch-4.5.3.6152.2-Console-Solaris.bin
- ArcSight SmartConnectors (SnortDB, NessusNSR, Checkpoint-OPSECNG, Cisco Secure IPS SDEE)
  - ArcSight-4.8.2.5516.0-Connector-Win.exe
  - ArcSight-4.8.2.5516.0-Connector-Linux.bin
  - ArcSight-4.8.2.5516.0-Connector-Solaris.bin
- ArcSight Manager:
  - ArcSight-4.5.3.6126.0-Manager-Linux.bin with Patch-4.5.3.6152.2-Manager-Linux.bin
  - ArcSight-4.5.3.6126.0-Manager-Linux64.bin with Patch-4.5.3.6152.2-Manager-Linux64.bin
  - ArcSight-4.5.3.6126.0-Manager-Solaris.bin with Patch-4.5.3.6152.2-Manager-Solaris.bin
  - ArcSight-4.5.3.6126.0-Manager-Win.exe with Patch-4.5.3.6152.2-Manager-Win.exe
  - ArcSight-4.5.3.6126.0-Manager-Win64.exe with Patch-4.5.3.6152.2-Manager-Win64.exe
- ArcSight Database:

- ArcSight-4.5.3.6126.0-DB-Linux.bin with Patch-4.5.3.6152.2-DB-Linux.bin
- ArcSight-4.5.3.6126.0-DB-Solaris.bin with Patch-4.5.3.6152.2-DB-Solaris.bin
- ArcSight-4.5.3.6126.0-DB-Win.exe with Patch-4.5.3.6152.2-DB-Win.exe

3 Security Policy

The TOE enforces the following security policies as described in the ST.

> ***Note:*** *Much of the description of the ArcSight ESM 4.5 SP3 Patch 2 security policy has been extracted and reworked from the ArcSight ESM 4.5 SP3 Patch 2 ST and Final ETR.*

3.1 Security Audit

The TOE 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 ArcSight Database, which is supported by the underlying Oracle RDBMS. 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.

3.2 Identification and Authentication

The TOE maintains accounts of the authorized users of the system. The user account includes the following attributes associated with the user: user identity: authentication data (passwords), authorizations (groups or roles), and e-mail address information. This information is stored in the ArcSight Database. 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.

3.3 Security Management

The TOE provides the authorized Administrator with graphical user interfaces (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).

3.4 Protection of the TSF

The TOE 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.

3.5 Analyzer Analysis, Reaction, Data Review, and Availability

The TOE 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 95% of capacity.

4 Assumptions

The ST identifies the following assumptions about the use of the product:

- The TOE has access to all the IT System resources necessary to perform its functions.
- The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
- The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
- There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
- The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
- The TOE can only be accessed by authorized users.

4.1 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (EAL 3 augmented with ALC_FLR.2).
2. This evaluation only covers the specific platforms and software version identified in this document, and not any earlier or later versions released or in process.
3. While is recommended that the TOE operate in FIPS 140-2 mode, this is not required for the evaluated configuration.
4. The TOE utilizes third-party software and hardware components in its operational environment, as follows:

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

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.
- Use of the System User role—this role was introduced in v4.0 of ESM. It has a special purpose (unlocking core content) and its capabilities are limited. The TOE guidance documentation includes a notice discouraging its use for regular administrative tasks.
- The ability of the TOE to use certificates to authenticate users (i.e., Password-Only authentication—either TOE-internal or external—is the only authentication option supported in the evaluated configuration).
- Use of the Partition Archiver and support for offline archiving of database partitions—users of the TOE in its evaluated configuration need to configure online storage to be adequate to support their required retention period. 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.

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 4.5 SP3.

SYSTEM REQUIREMENTS FOR ESM 4.5 SP3 Patch 2, NON-FIPS COMPLIANT

ArcSight Console		
Platform	**Supported Operating System**	**Typical System Configuration**
Linux	Red Hat Enterprise Linux 5.3 Desktop 32-bit	• x86-compatible multi-CPU system • 2-4 GB RAM memory, minimum • 2 GB disk space
Windows	Microsoft Windows Server 2003 R2 (SP2) 32-bit and 64-bit Microsoft Windows Server 2008 64-bit Microsoft Windows XP Professional SP3, 32-bit Microsoft Windows Vista, SP1, 32-bit and 64-bit	• x86-compatible multi-CPU system • 1-2 GB RAM memory, minimum • 2 GB disk space
Solaris	Sun Solaris 10 SPARC, 64-bit	• Sparc-compatible multi-CPU system • 2-4 GB RAM memory • 2 GB disk space
ArcSight Manager[1]		
Platform	**Supported Operating System**	**Typical System Configuration**
Linux	Red Hat Enterprise Linux 5.3 AS 32-bit and 64-bit	• x86-compatible multi-CPU system • 2-4 GB RAM memory, minimum • 2 GB disk space
Windows	Microsoft Windows Server 2003 R2 (SP2) 32-bit and 64-bit Microsoft Windows Server 2008 32-bit and 64-bit	• x86-compatible multi-CPU system • 2-4 GB RAM memory, minimum • 2 GB disk space
Solaris	Sun Solaris 10 SPARC, 64-bit	• Sparc-compatible multi-CPU system • 2-4 GB RAM memory • 2 GB disk space
ArcSight Database		
Platform	**Supported Operating System**	**Typical System Configuration**
Oracle 10.2.0.4	Microsoft Windows Server 2003 R2 (SP2), 32- and 64-bit	• x86-compatible multi-CPU system • 2-16 GB RAM memory
Oracle 10.2.0.4	Sun Solaris 10 SPARC, 64-bit	• Sparc-compatible multi-CPU system • 2-16 GB RAM memory
Oracle 10.2.0.4	Red Hat Enterprise Linux 5.3 AS 32-bit and 64-bit	• x86-compatible multi-CPU system • 2-16 GB RAM memory
ArcSight SmartConnectors		
Platform	**Supported Operating System**	**Typical System Configuration**
Linux	Red Hat Enterprise Linux 5.3 AS 32-bit and 64-bit	• x86-compatible CPU system • 512 MB memory • 1 GB disk space

[1] Note the ArcSight Manager component is supported on both 32-bit and 64-bit JVMs.

Windows	Microsoft Windows Server 2003, SP2, 32-bit	• x86-compatible CPU system • 512 MB memory • 1 GB disk space
Solaris	Sun Solaris 10 SPARC, 64-bit	• Sparc-compatible CPU system • 512 MB memory • 1 GB disk space

System Requirements for non-FIPS ArcSight ESM 4.5 SP3 Patch 2

SYSTEM REQUIREMENTS FOR ESM 4.5 SP3 Patch 2, FIPS 140-2 COMPLIANT

ArcSight Console		
Platform	**Supported Operating System**	**Typical System Configuration**
Linux	Red Hat Enterprise Linux 5.3 Desktop 32-bit	• x86-compatible, multi-CPU system • 2-4 GB RAM • 2 GB disk space
Windows	Microsoft Windows XP Professional SP2, 32-bit	• x86-compatible multi-CPU system • 1-2 GB RAM • 2 GB disk space
Solaris	Sun Solaris 10 SPARC, 64-bit	• Sparc-compatible multi-CPU system • 2-4GB memory • 2 GB disk space
ArcSight Manager[2]		
Platform	**Supported Operating System**	**Typical System Configuration**
Linux	Red Hat Enterprise Linux 5.3 AS 32-bit and 64-bit	• x86-compatible multi-CPU system • 2-4 GB memory • 2 GB disk space
Solaris	Sun Solaris 10 SPARC, 64-bit	• Sparc-compatible multi-CPU system • 2-4 GB memory • 2 GB disk space
ArcSight Database		
Platform	**Supported Operating System**	**Typical System Configuration**
Oracle 10.2.0.4	Sun Solaris 10 SPARC, 64-bit	• Sparc-compatible multi-CPU system • 2-16 GB RAM
Oracle 10.2.0.4	Red Hat Enterprise Linux 5.3 AS, 32-bit and 64-bit	• x86-compatible multi -CPU system • 2-16 GB RAM

[2] Note the ArcSight Manager is supported on both 32-bit and 64-bit JVMs.

ArcSight SmartConnectors		
Platform	**Supported Operating System**	**Typical System Configuration**
Linux	Red Hat Enterprise Linux 5.3 AS, 32-bit and 64-bit	• x86-compatible CPU system • 512 MB memory • 1 GB disk space
Solaris	Sun Solaris 10 SPARC, 64-bit	• Sparc-compatible CPU system • 512 MB memory • 1 GB disk space

System Requirements for FIPS 140-2 compliant ArcSight ESM 4.5 SP3 Patch 2

5 Architectural Information

This section provides a high level description of the TOE and its components as described in the Security Target and design documentation.

The TOE, ArcSight ESM 4.5 SP3 Patch 2 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 centralized ArcSight Database, and then filters and correlates those events with rules to generate meta-events.

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[3]. While it is recommended that the TOE operate in FIPS 140-2 mode, this is not required for the evaluated configuration.

The TOE, ArcSight ESM 4.5 SP3 Patch 2, comprises a number of different components that provide a comprehensive security event management system. Specifically, the TOE consists of the following components:

- ArcSight Console

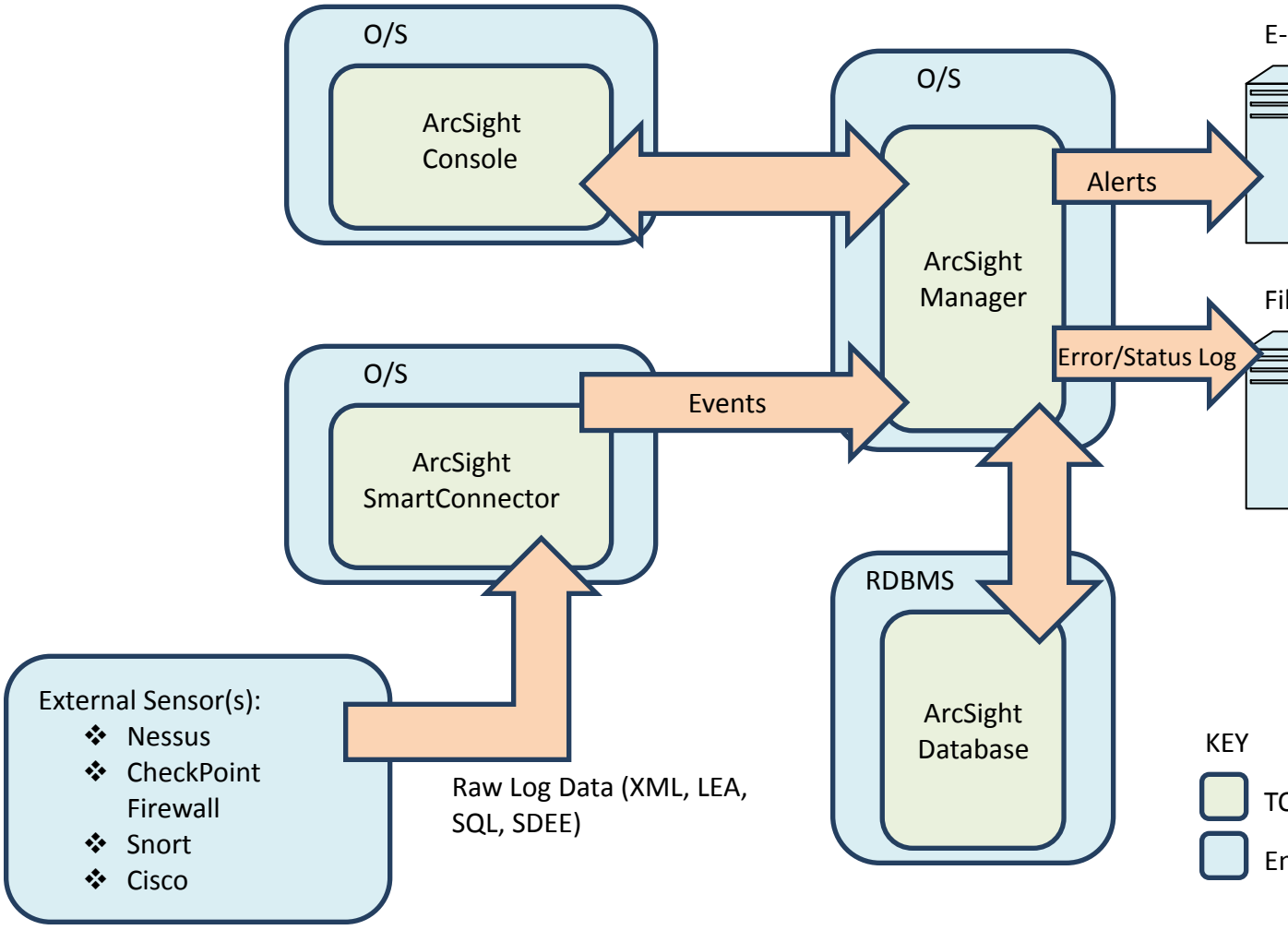
[3] Available at http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp814.pdf.

- ArcSight SmartConnectors
    - SnortDB
    - NessusNSR
    - Checkpoint-OPSECNG
    - Cisco Secure IPS SDEE
- ArcSight Manager
- ArcSight Database

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 that have not been subject to evaluation or part of the evaluation of the TOE will render the TOE out of its evaluated configuration.

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

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



5.1 ArcSight Console

The 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.

5.2 ArcSight Manager

The ArcSight Manager is a high performance engine that manages, cross-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, ArcSight Database, and ArcSight SmartConnectors. The ArcSight Manager relies on the underlying operating system to provide a file system to write audit 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. SMTP (Simple Mail Transfer Protocol and Simple Mail Transport Protocol) is used to send e-mail.

5.3 ArcSight Database

The ArcSight Database is the logical access mechanism, particular schema, table spaces, partitioning, and disk layout 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 ArcSight Database runs within the structure of an Oracle relational database management system (RDBMS), included in the ArcSight Database component installation. The Oracle RDBMS stores data in data files on the file system available to the operating system of the database host. The ArcSight Manager is the only component that communicates directly with the ArcSight Database. The data stored within the ArcSight Database is protected by the Oracle RDBMS and by the underlying operating system of the database host.

5.4 ArcSight SmartConnectors

The 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 included in the evaluated configuration are: SnortDB, NessusNSR, Checkpoint-OPSECNG, and Cisco Secure IPS SDEE.

5.4.1 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

5.4.2 NessusNSR

Nessus is a powerful, up-to-date, and easy-to-use remote security scanner. The Nessus Vulnerability Scanner lets the administrator 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.

5.4.3 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 VPN-1/FW-1. The ArcSight SmartConnector for Check Point VPN-1/FW-1 devices 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.

5.4.4 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.

6 Documentation

6.1 Product Guidance

The guidance documentation examined during the course of the evaluation and therefore delivered with the TOE is as follows:

- *Common Criteria Evaluated Configuration Guide: ArcSight ESM 4.5 SP3 Patch 3, Version 5.0, 08/30/2012*
- *Installation and Configuration Guide: ArcSight ESM Version 4.5 SP3, Revision 1, August 20, 2010*
- *ArcSight ESM User's Guide: ArcSight ESM 4.5 SP3, Revision 4, August 15, 2010*
- *Concepts for ArcSight ESM v4.5, Revision 3, November 6, 2009*
- *ArcSight ESM Administrator's Guide: ArcSight ESM Version 4.5 SP3, Revision 1, August 20, 2010*

- *Installing FIPS-Compliant SmartConnectors, Revision 2, February 11, 2010*
- *SmartConnector User's Guide: Topics Applicable to All ArcSight SmartConnectors, Revision 9, February 13, 2009*
- *SmartConnector Configuration Guide for Tenable Nessus NSR, Revision 8, February 11, 2010*
- *SmartConnector Configuration Guide for Check Point FW-1/VPN-1 OPSEC (Legacy), Revision 11, February 11, 2010*
- *SmartConnector Configuration Guide for Cisco Secure IPS SDEE, Revision 14, May 26, 2010*
- *SmartConnector Configuration Guide for Snort DB, Revision 20, February 11, 2010*
- *Patch Release Notes, ArcSight ESM 4.5 SP3, Build 4.5.3.6152.2, December 2010*
- *Release Notes, ArcSight ESM 4.5 SP3, Build 4.5.3.6126.0, August 24, 2010*
- *Release Notes, ArcSight SmartConnector, Build 4.8.2.5516, March 31, 2010*

7 Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Evaluation Team Test Report for the ArcSight ESM SP3 Patch 2.

Evaluation team testing was conducted at the vendor's development site August 20 through August 24, 2012.

7.1 Developer Testing

The vendor's test philosophy involves the use of manual test procedures that are primarily based on testing the claimed security functions of the TOE as represented by the SFRs specified in the ST. ArcSight used existing test cases and developed some new test cases that correspond to security functions claimed in the ST, ensuring that all security functions presented at the external interfaces are tested and that all TSFI are tested.

The test cases are grouped by security function and mapped to specific SFRs. Each test procedure targets the specific security behavior associated with that security function. The evaluation team completed a mapping of all test cases to TSFI and SFRS in the ATE ETR.

The vendor addressed test depth by analyzing the functionalities addressed in the TOE design and associating test cases that cover the addressed functionalities. The TOE design addressed the general functions of the TOE subsystems, identifying the security functionality of each subsystem as appropriate. The vendor test documentation maps specific tests to TSF subsystems and interfaces and to interactions between subsystems.

The ArcSight Test documentation consists of a Test Case Overview document (the test plan), a Test Coverage Analysis document, a Test Depth Analysis document and a set of Test Case documents which include both expected and actual test results. There is also a Test Case Results spreadsheet which contains the pass or fail status for all test cases.

The Test Case Overview document describes the overall approach of Testing and a description of how the Test Cases are presented. It also includes test configuration information such as test setup, test bed and test tools for the tests. The Test Cases are also divided into sets based on

security function. Each test case includes a Test Objective, Test Setup, Test Procedures and Expected and Actual Results.

The Test Cases are mapped to individual SFRs. The Test Coverage Analysis document provides the definitive mapping of test cases to individual shell commands and GUI interfaces. The Test Depth Analysis document maps the test cases to the subsystems and the subsystem interactions.

The vendor ran the TOE test suites, consistent with the test environment described in the testing documentation, and provided the evaluation team with the actual results.

7.2 Evaluation Team Independent Testing

The evaluation team used a sampling approach versus exercising the entire set of manual tests provided as evidence for the evaluation. The vender test suite is comprised of 298 manual test cases with approximately 200 test cases which are directly related and mapped to satisfy the TOE security functions. The vendor's test coverage is quite exhaustive in many cases and provides numerous examples of coverage of the same aspect of a particular security function. Therefore, the test sampling approach was not based on a percentage of test cases as this would not be necessary, nor time and cost efficient.

The tests were run across the test configurations described in the developer's test documentation. The documentation describes the different test configurations that were used in the test configurations.

The evaluation team performed the following sampling approach when determining the sample size:

- Exercised approximately 33 test cases from the test procedures across the three platforms dependent on time factors and repetition found amongst the chosen subset.
- Test cases included tests from each of the claimed security functions, security audit, identification and authentication, security management, protection of the TSF and IDS component requirements.
- Test cases included tests covering all TSFI (GUI, Shell commands and ArcSight Data Field
- Test cases included a generous sampling of the access via the SFR enforcing shell commands.

  Executed some test cases in both FIPS and non-FIPS mode (e.g., one configuration (Solaris) configured in FIPS mode).

In summary, the evaluation team performed its tests across three test bed configurations as follows:

- RH Linux Config: RH 5.3 64 bit (DB, Manager), RH 5.3 32 bit Desktop (Console) - Non-FIPS
- Windows Config: Windows Server 2003 R2 (SP2) 64 bit (DB, Manager, Console) - Non-FIPS
- Solaris Config: Sun Solaris SPARC 64 bit (DB, Manager, Console) – FIPS.

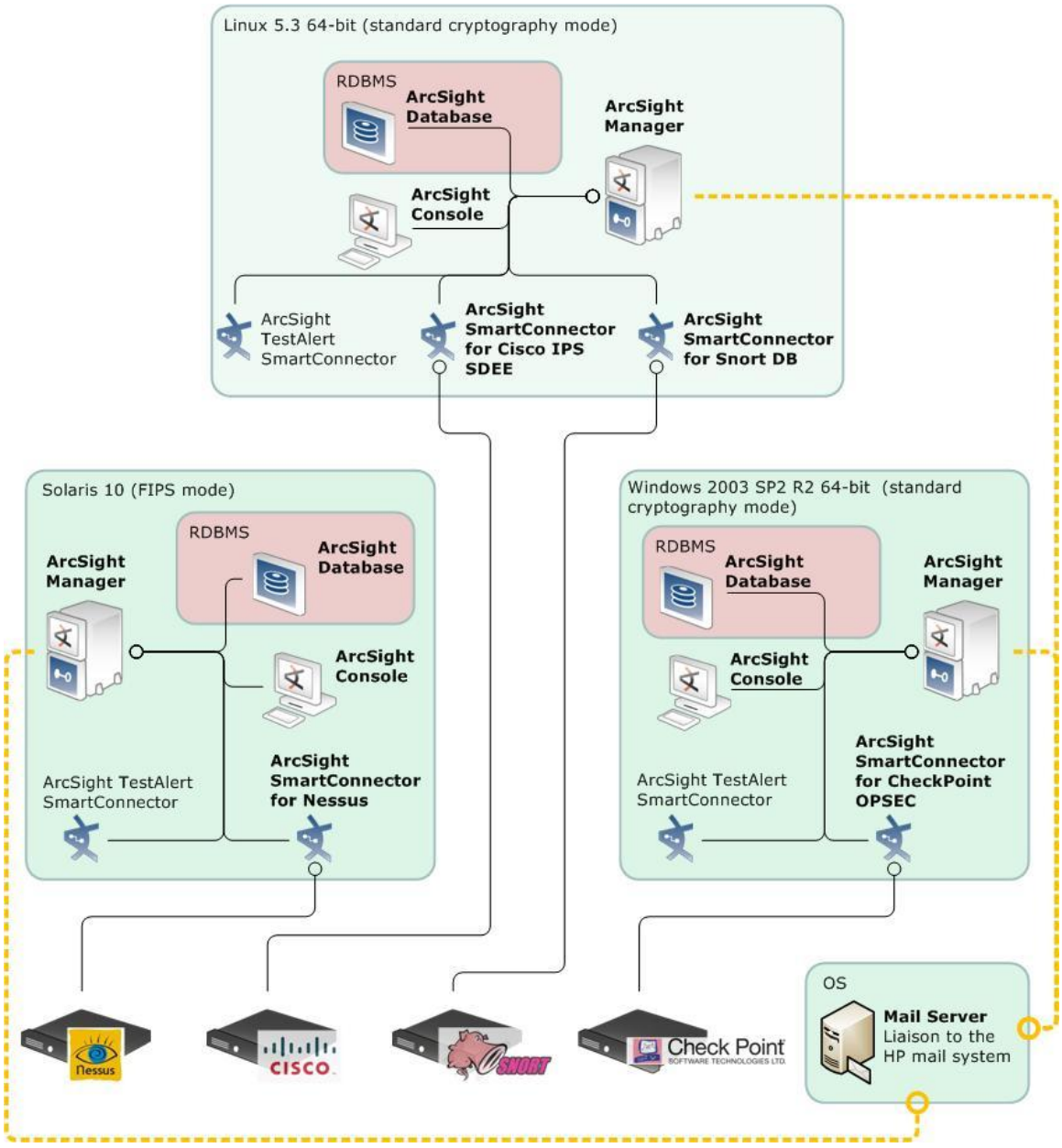
The following software was installed on the machines used for testing:

- ArcSight Console:
  - ArcSight-4.5.3.6126.0-Console-Win.exe with Patch-4.5.3.6152.2-Console-Win.exe
  - ArcSight-4.5.3.6126.0-Console-Linux.bin with Patch-4.5.3.6152.2-Console-Linux.bin
  - ArcSight-4.5.3.6126.0-Console-Solaris.bin with Patch-4.5.3.6152.2-Console-Solaris.bin
- ArcSight SmartConnectors (SnortDB, NessusNSR, Checkpoint-OPSECNG, Cisco Secure IPS SDEE)
  - ArcSight-4.8.2.5516.0-Connector-Win.exe
  - ArcSight-4.8.2.5516.0-Connector-Linux.bin
  - ArcSight-4.8.2.5516.0-Connector-Solaris.bin
- ArcSight Manager:
  - ArcSight-4.5.3.6126.0-Manager-Linux.bin with Patch-4.5.3.6152.2-Manager-Linux.bin
  - ArcSight-4.5.3.6126.0-Manager-Linux64.bin with Patch-4.5.3.6152.2-Manager-Linux64.bin
  - ArcSight-4.5.3.6126.0-Manager-Solaris.bin with Patch-4.5.3.6152.2-Manager-Solaris.bin
  - ArcSight-4.5.3.6126.0-Manager-Win.exe with Patch-4.5.3.6152.2-Manager-Win.exe
  - ArcSight-4.5.3.6126.0-Manager-Win64.exe with Patch-4.5.3.6152.2-Manager-Win64.exe
- ArcSight Database:
  - ArcSight-4.5.3.6126.0-DB-Linux.bin with Patch-4.5.3.6152.2-DB-Linux.bin
  - ArcSight-4.5.3.6126.0-DB-Solaris.bin with Patch-4.5.3.6152.2-DB-Solaris.bin
  - ArcSight-4.5.3.6126.0-DB-Win.exe with Patch-4.5.3.6152.2-DB-Win.exe

- RH Linux Config: RH 5.3 64 bit (DB, Manager), RH 5.3 32 bit Desktop (Console) - Non-FIPS
- Windows Config: Windows Server 2003 R2 (SP2) 64 bit (DB, Manager, Console) - Non-FIPS
- Solaris Config: Sun Solaris SPARC 64 bit (DB, Manager, Console) – FIPS
- ArcSight Test Alert Agent SmartConnector
- Wireshark

As documented in the vendor Test Case Overview, the Test Alert SmartConnector (shown in the diagram below) is an all-purpose utility that acts as a SmartConnector that sends base events to the Manager. These events are then viewed on the Console. Its behavior is the same as other ArcSight SmartConnectors. For test purposes, Test Alert was used to cover test cases involving general product functionality such as events fired by rule actions, notification triggers when the database fills up, etc.

The diagram below depicts the configurations used for the vender testing and also during onsite testing.



The evaluation team performed the following additional functional tests:

- **Password Structure Criteria**—the evaluation team confirmed the TOE enforces the following the following restrictions on passwords:
    - Minimum password length is 6 characters
    - Maximum password length is 20 characters
    - Password cannot be the same as the name of its User, cannot contain whitespace characters (spaces, tabs) and can have a maximum of three consecutive repeated characters

  - Passwords expire after 60 days and require the user to change the password.

- **Admin Guidance -** the evaluation team tested various procedures in the Admin Guidance and verified that they are complete and correct. Administrative instructions tested included: create a user, change a user password, and create a rule.
- **Secure Data Storage -** the evaluation team confirmed that the TOE stores only Md5 hashes of the passwords in the database; properties files are stored in the underlying file system of the OS; and that the underlying database authentication information is obfuscated and stored in the Manager's installation directory.
- **Consistent Time**—the evaluation team confirmed the consistency of timestamps when user login is performed via both the Console and the Shell commands.
- **Error Messages -** the evaluation team confirmed that appropriate error messages were displayed via the SFR enforcing shell commands and the Console.
- **ArcSight Manager Properties Files -** the evaluation team exercised the procedures in the ESM Installation Guide to restrict access to the server.properties file and verified that once the procedures were executed; only the owner of the file had access to read or write to the file.
- **Content Updates-** the evaluation team downloaded and installed content and vulnerability mapping updates and verified that they were successfully transmitted and installed and that this action is audited.

7.3 Penetration Testing

The evaluation team conducted an open source search for vulnerabilities in the TOE and identified a number of vulnerabilities reported against components that are not included in the TOE. No vulnerabilities in the TOE were located.

The evaluation team considered other potential vulnerabilities, based on a focused search of the evaluation evidence. Some of the ideas for vulnerability tests identified by the evaluation team were already covered by vendor functional tests or by the independent functional tests devised by the evaluation team. Others were determined, through analysis, not to present exploitable vulnerabilities. The evaluation team performed tests to confirm:

- **Port and Vulnerability Scan -** the evaluation team confirmed that the TOE only opened ports and services that were needed by the TOE.
- **Underlying File Permissions -** the evaluation team confirmed that the file permissions configured on the environmental components adequately protect the TOE, the binary image and file data stores.
- **User Account Harvesting** - the evaluation team confirmed that the TOE authentication mechanism returns the same error message for incorrect username or incorrect password.
- **User Input Validation** - the evaluation team confirmed that invalid data and SQL commands entered via the Console and command line returned appropriate error messages.
- **Log File Checking** - the evaluation team confirmed that the TOE logs did not contain any sensitive data.

- **Revoked User** - the evaluation team confirmed that user revocation is immediate when a user's permissions are revoked while they are logged in.

8 Evaluated Configuration

The evaluated version of the TOE is identified as the ArcSight Enterprise Security Management (ESM) Version 4.5 SP3 Patch 2, hereinafter referred to as "ESM" or "the TOE".

The TOE is composed of the following components: ArcSight Console, ArcSight Manager, ArcSight Database, and the ArcSight SmartConnectors. The evaluated configuration includes the following specific ArcSight SmartConnectors: SnortDB, NessusNSR, Checkpoint-OPSECNG, and Cisco Secure IPS SDEE.

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[4]. While is recommended that the TOE operate in FIPS 140-2 mode, this is not required for the evaluated configuration.

TOE relies on third-party software and hardware components in the operating environment as previously identified in Section 4.1.

9 Results of the Evaluation

The evaluation was conducted based upon version 3.1 Revision 3 of the CC and the CEM. A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each assurance component. For Fail or Inconclusive work unit verdicts, the evaluation team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the evaluation team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The validation team agreed with the conclusion of the evaluation team, and recommended to CCEVS management that an "EAL3 augmented with ALC_FLR.2" certificate rating be issued for ArcSight ESM 4.5 SP3 Patch 2.

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

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the SAIC CCTL. The security assurance requirements are listed in the following table.

Table 2 – TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ADV_ARC.1	Security Architecture Description
ADV_FSP.3	Functional specification with complete summary
ADV_TDS.2	Architectural Design
AGD_OPE.1	Operational User Guidance
AGD_PRE.1	Preparative Procedures
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_COV.2	Analysis of Coverage
ATE_DPT.1	Testing: basic design
ATE_FUN.1	Functional Testing
ATE_IND.2	Independent Testing – Sample
AVA_VAN.2	Vulnerability Analysis

10 Validator Comments/Recommendations

The validation team's observations support the evaluation team's conclusion that the ArcSight Enterprise Security Management (ESM) Version 4.5 SP3 Patch 2 meets the claims stated in the Security Target.

11 Annexes

Not applicable.

12 Security Target

The ST for this product's evaluation is ArcSight ESM 4.5 SP3 Patch 2 Security Target, Version 1.0, dated October 4, 2012.

13 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1, Revision 3, July 2009.

2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, Version 3.1, Revision 3, July 2009.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, Version 3.1, Revision 3, July 2009.
4. Common Methodology for Information Technology Security: Evaluation methodology, Version 3.1, Revision 3, July 2009.
5. ArcSight ESM 4.5 SP3 Patch 2 Security Target, Version 1.0, October 4, 2012.