ArcSight 3.0

Security Target

Version 1.0

29 September 2006

Prepared for:

ArcSight
1309 South Mary Avenue
Sunnyvale, CA 94087

Prepared By:

Science Applications International Corporation
Common Criteria Testing Laboratory
7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

Table of Contents

List of Figures

List of Tables

1. Security Target Introduction

The ArcSight product is a security management solution that allows a user to manage all enterprise activity from one centralized view. ArcSight integrates existing multi-vendor devices throughout the enterprise into its scope and gathers all generated events. ArcSight 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.

ArcSight product gathers events generated by multi-vendor devices, normalizes, and stores those events in the centralized ArcSight Database, and then filters and cross-correlates those events with rules to generate meta-events.

The ArcSight product is composed of several components;

- 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
- myArcSight
    - myArcSight is a personalized web-based interface that is accessed to monitor events, view cases, view Hotlists, acknowledge notifications, access reports, and access the Knowledge Base
- ArcSight Manager
    - ArcSight Manager is a high performance engine that manages, cross-correlates, filters, and processes all occurrences of security events in your enterprise
- ArcSight Database
    - The ArcSight Database is the relational database repository that is used to store all captured events, plus save all security management configuration information such as system users, groups, permissions, and defined rules, zones, assets, reports, displays, and preferences.
- ArcSight SmartAgents
    - ArcSight SmartAgents are collectors and processors of events generated by security devices throughout an enterprise

The Target of Evaluation (TOE) is ArcSight 3.0, a subset of components of the ArcSight product. The components that comprise the TOE are; ArcSight Console, ArcSight Manager, ArcSight Database, and ArcSight Agents. The following components are included in the product, which are outside the scope of the TOE;

- myArcSight (a Web-based UI to ArcSight which is part of the Manager and is disabled in the TOE);
- ArcSight Web (a Web-based UI to ArcSight which is a separately installed server which is only in beta for 3.0.2.8 and is not installed as part of the TOE);
- Pattern Discovery (which is a feature of the Manager that is licensed separately and is not enabled as part of the TOE);
- Database Agent (which is an Agent that may be installed on the database host and provides partition archiving services but is not installed as part of the TOE); and
- All Agents except for the three that are part of the TOE (Nessus, Checkpoint Firewall, and Snort).

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

  This section details the expectations of the environment, the threats that are countered by ArcSight 3.0 and the environment and the organizational policy that the ArcSight 3.0 must fulfill.

- Section 4 – TOE Security Objectives

  This section details the security objectives of the ArcSight 3.0 and the environment.

- Section 5 – IT Security Requirements

  This section presents the security functional requirements (SFR) for ArcSight 3.0 and the IT Environment that supports the TOE, and details the assurance requirements for EAL3.

- Section 6 – TOE Summary Specification

  This section describes the security functions represented in the ArcSight 3.0 that satisfy the security requirements.

- Section 7 – Protection Profile Claims

  This section presents any protection profile claims.

- Section 8 – Rationale

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

1.1 Security Target, TOE and CC Identification

ST Title – ArcSight 3.0 Security Target

ST Version – Version 1.0

ST Date – 29 September 2006

TOE Identification – ArcSight 3.0 comprised of the following components:

- ArcSight Console (ArcSight – 3.0.2.3939.0 – Console) with Patch-3.0.2.9.3939-Console
- ArcSight SmartAgents for Nessus, Check Point Firewall-1 NG OPSEC, and Snort IDS DB (ArcSight-3.5.1.4339.0 - Agent)
- ArcSight Manager (ArcSight-3.0.2.3939.0-Manager) with Patch-3.0.2.9.3939-Manager
- ArcSight Database (ArcSight-3.0.2.3939-DB) with Patch-3.0.2.6.3939-DB

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999, ISO/IEC 15408.

1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 2.1, August 1999, ISO/IEC 15408-2.
  - Part 2 Extended (with FPT_AVL.1, IDS_ANL.1, IDS_RCT.1, IDS_RDR.1, IDS_STG.1, and IDS_STG.2)

- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 2.1, August 1999, ISO/IEC 15408-3.
    - Part 3 Conformant
    - Evaluation Assurance Level 3 (EAL3) augmented with ALC_FLR.1

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

- U.S. Government Intrusion Detection System Analyzer Protection Profile, Version 1.2, April 27, 2005.

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 also includes Flaw Remediation. The resulting assurance level is therefore, EAL3 augmented with ALC_FLR.1.

1.3 Strength of Environment

The TOE, ArcSight 3.0, a subset of the ArcSight product provides data collection and storage system to consolidate network-wide alarms and alerts, analysis tools to detect multi-source and multi-target threats, and a display and report function to manage the results.

To ensure that the risks to the target environment are adequately addressed, the assurance requirements for EAL3 augmented with ALC_FLR.1, and the minimum strength of function, SOF-basic, were chosen.

1.4 Conventions, Terminology, and Acronyms

1.4.1 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 …").
- Explicitly stated Security Functional Requirements (i.e., those not found in Part 2 of the CC) are identified with "**(EXP)**".
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.4.2 Terminology and Acronyms

Reference the U.S. Government Intrusion Detection System Analyzer Protection Profile for a complete list of acronyms and terms used throughout the ST. In addition, the following acronyms may be used within this Security Target.

Acronym	Definition
API	Application programming interface
CC	Common Criteria
CEM	Common Evaluation Methodology
CCEVS	Common Criteria Evaluation and Validation Scheme
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
HLD	High-level Design
IA	Initial Assessment
IDS	Intrusion Detection Systems
NSS	Network Security System
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OS	Operating system
PP	Protection Profile
SAIC	Science Applications International Corporation
SOF	Strength of Function
SSL	Secure Socket Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

1.5 TOE Documentation

ArcSight offers a series of documents that describe the installation process for the TOE as well as guidance for subsequent use and administration of the applicable security features. Refer to Section 6.2 TOE Security Assurance Measures for information about these and other documentation associated with the TOE.

2. TOE Description

The TOE, ArcSight 3.0, a subset of the ArcSight product, 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). ArcSight 3.0 also includes the capability to provide enterprise-wide monitoring for sub-networks monitored by non-homogeneous network monitors. As such, ArcSight 3.0 provides a solution for managing all network events and/or activities in an enterprise from a centralized view. ArcSight 3.0 allows trusted users to monitor events, correlate events for in-depth investigation and analysis, and resolve events with automated escalation procedures and actions. For a list of ArcSight product components, refer to Section 1 Security Target Introduction.

The TOE can be installed on Microsoft Windows XP, Microsoft Windows 2000, Microsoft Windows 2003, Solaris 9, and Red Hat Enterprise Linux 3.0. All of the components can be installed either on the same machine or all on different machines. The Administrators, Analyzer Administrators, and Operators access the TOE locally. The TOE does not support or allow access to the TOE from external IT products.

2.1 TOE Physical Boundaries

The TOE, ArcSight 3.0, a subset of the ArcSight product comprises a number of different components that provide a comprehensive security event management system.

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 Administrators, Analyzer Administrators, and Operators with an intuitive interface to perform security management functions that includes viewing the audit data. 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 of the TOE. The underlying operating system is considered part of the environment.

ArcSight Manager

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 ArcSight 3.0 and acts as a link between the ArcSight Console, ArcSight Database, and ArcSight SmartAgent. 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. For pager notifications, firewalls (part of the environment) must be configured so that the pager can connect directly to the paging service provider. ArcSight 3.0 currently supports any provider that supports SNPP (Simple Network Paging Protocol).

ArcSight Database

The ArcSight Database is the logical access mechanism, particular schema, table spaces, partitioning, and disk layout. The ArcSight Database stores all captured events, plus save all security management configuration information such as system users, groups, permissions, and defined rules, zones, assets, reports, displays, and preferences in an Oracle database. The ArcSight Database relies on the environment to provide an Oracle database for its use. The Oracle database provided by the environment is referred to as the underlying database and is responsible for the security and integrity of information it stores. 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 underlying database system and by the underlying operating system of the database host.

ArcSight SmartAgent

ArcSight SmartAgent is collectors and processors of events generated by security devices 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 SmartAgent can be installed on the ArcSight Manager machine, a separate host machine, or, when supported, directly on a device. The three agents that are included in the TOE are;

- Nessus, a vulnerability scanner that delivers its data as a report file;
- Check Point Firewall-1 NG OPSEC, a firewall that delivers its data via a proprietary, push protocol (OPSEC); and
- Snort IDS DB, an intrusion detection system that delivers its data via a database (MySQL)).

The ArcSight SmartAgent relies 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. The ArcSight SmartAgent requires the underlying operating system to provide protection of the TOE. The underlying operating system is considered part of the environment.

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

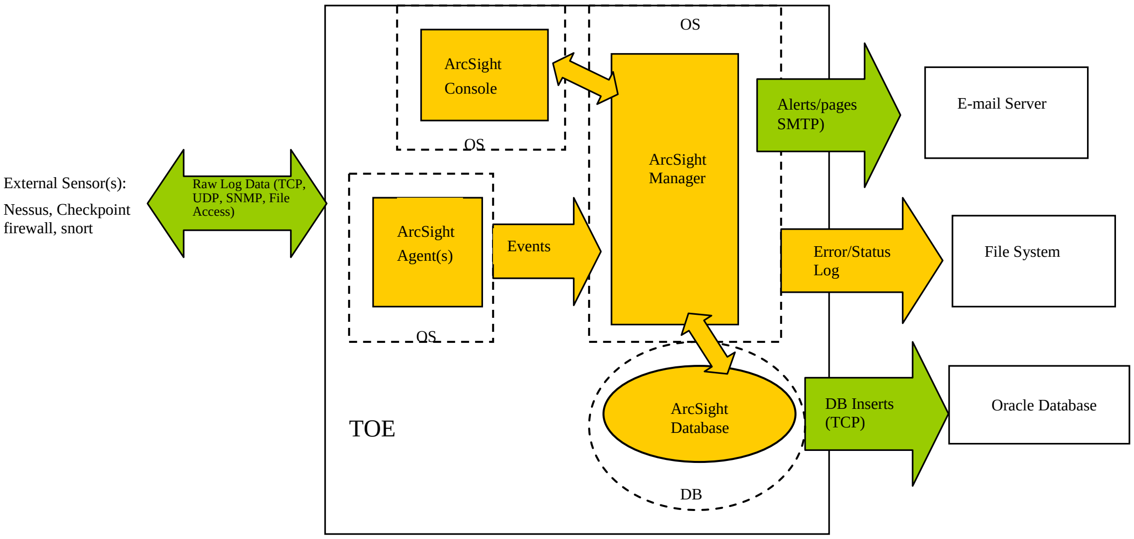

Figure 1: TOE Physical Boundaries

The following table outlines the system requirements for ArcSight 3.0

ArcSight Console		
Platform	**Supported Operating System**	**System Requirements**
Linux	Red Hat Enterprise Linux 3.0 (RHEL 3) WS Must have KDE or GNOME GUI and Desktop	- Pentium III 1.1 GHz - High Color (16-bit), 1024 x 768 resolution minimum. Higher recommended - 512 MB memory minimum. Higher recommended - 1 GB disk space
Windows	Microsoft Windows XP Professional	- Pentium III 1.1 GHz - High Color (16-bit), 1024 x 768 resolution minimum. Higher recommended - 512 MB memory minimum. Higher recommended - 1 GB disk space
Solaris	Sun Solaris 9	Sunblade 150 - 512 MB memory minimum. Higher recommended - 1 GB disk space
ArcSight Manager		
Platform	**Supported Operating System**	**System Requirements**
Linux	Red Hat Enterprise Linux 3.0 (RHEL 3) ES	- Pentium 4 Xeon 2.0 GHz or AMD Opteron 1.6 GHz - 2 GB memory - 2 GB disk space
Solaris	Sun Solaris 9	- UltraSparc IIi, 550 MHz or faster - 2 GB memory - 2 GB disk space
Windows	Windows 2000 Advanced Server	- Pentium 4 Xeon 2.0 GHz or AMD Opteron 1.6 GHz - 2 GB memory - 2 GB disk space
ArcSight Database		
Platform	**Supported Operating System**	**System Requirements**
Oracle 9.2.0.1	Windows 2000 Advanced Server	Pentium III, 1.1 GHz

Oracle 9.2.0.1	Solaris 9, 64-bit	UltraSparc IIi, 550 Mhz
Oracle 9.2.0.1	Red Hat Enterprise Linux 3.0 ES	Pentium III, 1.1 GHz
ArcSight Agent		
Platform	**Supported Operating System**	**System Requirements**
Linux	Red Hat Enterprise Linux 3.0 AS	- Pentium III 1.1 GHz or faster - 512 MB memory - 1 GB disk space
Solaris	Sun Solaris 9	- Ultra Sparc IIi, 550 MHz or faster - 512 MB memory - 1 GB disk space
Windows	Microsoft Windows 2000 Advanced Server	Pentium III 1.1 GHz or faster - 512 MB memory - 1 GB disk space

Table 1: System Requirements

2.2 TOE Logical Boundaries

The logical boundaries of the TOE include the functions of the TOE interfaces. These functions include audit, identification and authentication, security management, self-protection of the TOE, and intrusion detection.

Audit

Audit data comprises security relevant events such as user logging, service interruptions, server data accessed, etc. Audit data is also collected on the various devices that send their data to the SmartAgent that ArcSight 3.0 manages. Refer to 6.1.1 Security Audit for detailed information.

Identification & Authentication

ArcSight 3.0 requires users to provide unique identification and authentication data before any administrative access to the TOE is granted. ArcSight 3.0 provides an authentication mechanism for users through an authentication database. The only authentication mechanism supported by the TOE is passwords. Refer to 6.1.2 Identification and Authentication for detailed information.

Security Management

ArcSight 3.0 provides the authorized administrator with graphical user interfaces that can be used to configure and modify the options of the TOE. There are several modules available to the authorized users of the TOE, such as modify the behavior of the data collection and review, query audit data, and restrict access and/or the ability to query and modify all other TOE data to the appropriate authorized user/authorized role. Refer to 6.1.3 Security Management for detailed information.

Protection of the TSF

ArcSight 3.0 is not intended to make data available to other IT products and in the case of a distributed ArcSight 3.0 architecture; the components are expected to be connected with a benign, private, and protected communication network. The underlying operating system is required to provide protection of the TOE and its resources. The underlying operating is also responsible for providing a reliable timestamp. The underlying operating system is considered part of the environment. Refer to 6.1.4 Protection of the TSF for detailed information.

IDS Component Requirements; Analyzer Analysis, Analyzer React, and System Data Review, Availability and Loss

ArcSight 3.0 collects relevant information from one or more sources and performs analysis on the information that it collects by comparison against normal system activities and behavior. Refer to 6.1.5 Analyzer Analysis, 6.1.6 Analyzer React, and 6.1.7 System Data Review, Availability and Loss for detailed information.

3. Security Environment

The TOE security environment consists of threats to security and the secure usage assumptions as they relate to the TOE, ArcSight 3.0 components; ArcSight Agents, ArcSight Managers, ArcSight Database, and ArcSight Console.

The TOE, ArcSight 3.0, a subset of the ArcSight product provides for a level of protection that is appropriate for IT environments that require; a) continuous information about devices and information on a network and b) indications of vulnerabilities that exist on which network devices.

The TOE, ArcSight 3.0, a subset of the ArcSight product 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. ArcSight 3.0 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. The assumed level of expertise of the attacker for all the threats is unsophisticated.

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.

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.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.PROTECT 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 System Assumptions

A.SYSPROTECT The operating environment will provide protection to the TOE and its related data.

A.TIME The TOE’s IT environment will provide a reliable time source to enable the TOE to timestamp audit records.

3.3.3 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.

3.3.4 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 the supporting environment. The security objectives identify the responsibilities of the TOE and the environment in meeting the security needs.

4.1 Security Objectives for the TOE

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.

O.EXPORT When the TOE makes its Analyzer data available to other IDS components, the TOE will ensure the confidentiality of the Analyzer data.

4.2 Security Objectives for the IT Environment

The following security objectives for the IT environment of the TOE must be satisfied in order for the TOE to fulfill its own security objectives.

OE.AUDIT_PROTECTION The IT Environment will provide the capability to protect audit information.

OE.PROTECT The IT environment will protect itself and the TOE from external interference or tampering.

OE.TIME The IT environment will provide reliable timestamps to the TOE.

4.3 Security Objectives for the Non-IT Environment

The TOE's operating environment must satisfy the following objectives. These objectives do not levy any IT requirements but are satisfied by procedural or administrative measures.

O.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.

O.PHYCAL Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

O.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.

O.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the Analyzer.
O.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 and the Protection Profile (PP) identified in Protection Profile Claims section.

This ST includes a number of explicitly stated requirements. Each of the explicitly stated requirements is defined in the U.S. Government Intrusion Detection System Analyzer Protection Profile. The explicitly stated requirements can be identified by the use of the keyword "EXP" in the title.

Every SFR included in the PP is addressed in this Security Target. Each SFR, except as noted below, 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.

Security Functional Class	Security Functional Components
Security Audit (FAU)	Audit data generation (FAU_GEN.1)
	Audit review (FAU_SAR.1)
	Selectable audit review (FAU_SAR.3)
	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)[1]
	Security roles (FMT_SMR.1)
Protection of the TSF (FPT)	Inter-TSF data availability (FPT_AVL.1)[2]
	Basic internal TSF data transfer protection (FPT_ITT.1) [3]
IDS Component Requirements (IDS)	Analyzer analysis (IDS_ANL.1)
	Analyzer react (IDS_RCT.1)
	Restricted data review (IDS_RDR.1)

[1] This requirement has been added to conform to International Interpretation RI#65.

[2] This requirement has been added to address OD 250.

[3] This requirement has been added to protect inter-communications, replacing FPT_ITA.1, FPT_ITC.1, and FPT_ITI.1) per OD 250.

Security Functional Class	Security Functional Components
	Guarantee of analyzer data availability (IDS_STG.1)
	Prevention of analyzer data loss (IDS_STG.2)

Table 2: Security Functional Components

5.1.1 Security Audit (FAU)

5.1.1.1 FAU_GEN.1 Audit data generation

5.1.1.1.1 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].** FAU_GEN.1.1

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_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[5]	Use of the management functions	
FMT_SMR.1	Modifications to the group of users that are part of a role	User identity

Table 3: Auditable Events

5.1.1.1.2 FAU_GEN.1.2

The TSF shall record within each audit record at least the following information:

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**the additional information specified in the Details column of Table 2 Auditable Events**]. FAU_GEN.1.2

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

[5] FMT_SMF.1 is added to address International Interpretation RI #65

5.1.1.2 FAU_SAR.1 Audit review

5.1.1.2.1 FAU_SAR.1.1

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

5.1.1.2.2 FAU_SAR.1.2

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

5.1.1.3 FAU_SAR.2 Restricted audit review

5.1.1.3.1 FAU_SAR.2.1

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

5.1.1.4 FAU_SAR.3 Selectable audit review

5.1.1.4.1 FAU_SAR.3.1

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

5.1.1.5 FAU_SEL.1 Selective audit

5.1.1.5.1 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**]. FAU_SEL.1.1

5.1.1.6 FAU_STG.4 Prevention of audit data loss

5.1.1.6.1 FAU_STG.4.1

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

5.1.2 Identification and authentication (FIA)

5.1.2.1 FIA_ATD.1 User attribute definition

5.1.2.1.1 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;**

e) **Pager; and**

f) **no other security attributes**]. FIA_ATD.1.1

[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.

5.1.2.2 FIA_UAU.1 Timing of authentication

5.1.2.2.1 FIA_UAU.1.1

The TSF shall allow [**no administrative actions**] on behalf of the user to be performed before the user is authenticated. FIA_UAU.1.1

5.1.2.2.2 FIA_UAU.1.2

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

5.1.2.3 FIA_UID.1 Timing of identification

5.1.2.3.1 FIA_UID.1.1

The TSF shall allow [**no administrative actions**] on behalf of the user to be performed before the user is identified. FIA_UID.1.1

5.1.2.3.2 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. FIA_UID.1.2

5.1.3 Security management (FMT)

5.1.3.1 FMT_MOF.1 Management of security functions behavior

5.1.3.1.1 FMT_MOF.1.1

The TSF shall restrict the ability to [***modify the behavior of***] the functions [**of analysis and reaction**] to [~~**authorized Analyzer Administrator**~~ **Operator**[7]]. FMT_MOF.1.1

5.1.3.2 FMT_MTD.1 Management of TSF data

5.1.3.2.1 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 [**authorized Administrator can perform all functions and the Operator can query Analyzer data**]. FMT_MTD.1.1

5.1.3.3 FMT_SMF.1 Specification of Management Functions[8]

5.1.3.3.1 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**]. FMT_SMF.1.1

5.1.3.4 FMT_SMR.1 Security roles

5.1.3.4.1 FMT_SMR.1.1

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

[7] This refinement has been made to identify the role(s) supported by this TOE in Section 5.1.3.4.1.

[8] This is a required dependency of International Interpretation RI#65.

5.1.3.4.2 FMT_SMR.1.2

The TSF shall be able to associate users with roles. FMT_SMR.1.1

5.1.4 Protection of the TOE security functions (FPT)

5.1.4.1 Inter-TSF data availability (EXP) (FPT_AVL.1)

5.1.4.2 FPT_AVL.1.1

The TSF shall ensure the availability of audit and Analyser data provided to separate parts of the TOE given the following conditions; when the ArcSight database reaches capacity. (EXP) FPT_ITA_AVL.1.1

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

5.1.4.3.1 FPT_ITT.1.1

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

5.1.5 IDS Component Requirements (IDS)

5.1.5.1 IDS_ANL.1 Analyzer analysis (EXP)

5.1.5.1.1 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**]. (EXP) IDS_ANL.1.1

5.1.5.1.2 IDS_ANL.1.2

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

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

b) [**no other security relevant information about the result**]. (EXP) IDS_ANL.1.2

5.1.5.2 IDS_RCT.1 Analyzer react (EXP)

5.1.5.3 IDS_RCT.1.1

The TSF shall send an alarm to [**ArcSight database and to any monitoring ArcSight Console**] and take [**action specified by the rule that was triggered by the event**] when an intrusion is detected. (EXP) IDS_RCT.1.1

5.1.5.4 IDS_RDR.1 Restricted Data Review (EXP)

5.1.5.4.1 IDS_RDR.1.1

The Analyzer shall provide [**authorized Administrator (can perform all functions) and Operator (can query Analyzer data)**] with the capability to read [**audit data, reports (that includes the analytical results), configuration information, and other applicable Analyzer data**] from the Analyzer data. (EXP) IDS_RDR.1.1

5.1.5.4.2 IDS_RDR.1.2

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

5.1.5.4.3 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) IDS_RDR.1.3

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

5.1.5.5.1 IDS_STG.1.1

The Analyzer shall protect the stored Analyzer data from unauthorized deletion. (EXP) IDS_RDR.1.3

5.1.5.5.2 IDS_ STG.1.2

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

5.1.5.5.3 IDS_ STG.1.3

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

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

5.1.5.6.1 IDS_STG.2.1

The Analyzer shall [***overwrite the oldest stored Analyzer data***] and send an alarm if the storage capacity has been reached. (EXP) IDS_STG.2.1

5.2 IT Environment Security Functional Requirements

This section specifies the security functional requirements (SFRs) for the IT Environment. The SFRs are based on the SFRs in the CC Part 2 **Table 4: Security Functional Components for the IT Environment** identifies all SFRs implemented by the IT Environment and indicates the ST operations performed on each requirement.

Security Functional Class	Security Functional Components
Security Audit (FAU)	Restricted audit review (FAU_SAR.2)
Protection of the TSF (FPT)	Non-bypassability of the TSP (FPT_RVM.1)
	TSF domain separation (FPT_SEP.1)
	Reliable time stamps (FPT_STM.1)

Table 4: Security Functional Components for the IT Environment

5.2.1 Security Audit (FAU)

5.2.1.1 FAU_STG.2 Guarantees of audit data availability

5.2.1.1.1 FAU_STG.2.1

The ~~TSF~~ **IT Environment** shall protect the stored audit records from unauthorized deletion. FAU_STG.2.1

5.2.1.1.2 FAU_STG.2.2

The ~~TSF~~ **IT Environment** shall be able to [***detect***] modifications to the audit records. FAU_STG.2.2

5.2.1.1.3 FAU_STG.2.3

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

5.2.2 Protection of the TOE security functions (FPT)

5.2.2.1 FPT_RVM.1 Non-bypassability of the TSP

5.2.2.1.1 FPT_RVM.1.1

The ~~TSF~~ **IT Environment** shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed. FPT_RVM.1.1

5.2.2.2 FPT_SEP.1 TSF domain separation

5.2.2.2.1 FPT_SEP.1.1

The ~~TSF~~ **IT Environment** shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects. FPT_SEP.1.1

5.2.2.2.2 FPT_SEP.1.2

The ~~TSF~~ **IT Environment** shall enforce separation between the security domains of subjects in the TSC. FPT_SEP.1.2

5.2.2.3 FPT_STM.1 Reliable time stamps

5.2.2.3.1 FPT_STM.1.1

The ~~TSF~~ **IT Environment** shall be able to provide reliable time stamps for its own **and TOE** use. FPT_STM.1.1

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level 3 (EAL3) augmented with ALC_FLR.1 components as specified in Part 3 of the Common Criteria. Note that the EAL3 requirements that exceed EAL 2 are indicated in italics in the following table. No operations are applied to the assurance components. The SARs have been changed, when necessary, to conform to International Interpretations.

Assurance Class	Assurance Components
Configuration Management (ACM)	*ACM_CAP.3 Authorisation controls*
	ACM_SCP.1 TOE CM coverage
Delivery and Operation (ADO)	ADO_DEL.1 Delivery procedures
	ADO_IGS.1 Installation, generation, and start-up procedures
Development (ADV)	ADV_FSP.1 Informal functional specification
	ADV_HLD.2 Security enforcing high-level design
	ADV_RCR.1 Informal correspondence demonstration
Guidance Documents (AGD)	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Life cycle support (ALC)	*ALC_DVS.1 Identification of security measures* *ALC_FLR.1 Basic Flaw Remediation*

Assurance Class	Assurance Components
Tests (ATE)	*ATE_COV.2 Analysis of Coverage*
	ATE_DPT.1 Testing: high-level design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
Vulnerability assessment (AVA)	*AVA_MSU.1 Examination of analysis*
	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.1 Developer vulnerability analysis

Table 5: EAL3 Assurance Components

5.3.1 Configuration Management (ACM)

5.3.1.1 Authorisation controls (ACM_CAP.3)

5.3.1.1.1 ACM_CAP.3.1D

The developer shall provide a reference for the TOE.

5.3.1.1.2 ACM_CAP.3.2D

The developer shall use a CM system.

5.3.1.1.3 ACM_CAP.3.3D

The developer shall provide CM documentation.

5.3.1.1.4 ACM_CAP.3.1C

The reference for the TOE shall be unique to each version of the TOE.

5.3.1.1.5 ACM_CAP.3.2C

The TOE shall be labelled with its reference.

5.3.1.1.6 ACM_CAP.3.3C

The CM documentation shall include a configuration list and a CM plan.

5.3.1.1.7 ACM_CAP.3.RI3

The configuration list shall uniquely identify all configuration items that comprise the TOE.[9]

5.3.1.1.8 ACM_CAP.3.4C

The configuration list shall describe the configuration items that comprise the TOE.

5.3.1.1.9 ACM_CAP.3.5C

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

5.3.1.1.10 ACM_CAP.3.6C

The CM system shall uniquely identify all configuration items.

[9] This requirement element has been added to comply with International Interpretation RI #3.

5.3.1.1.11 ACM_CAP.3.7C

The CM plan shall describe how the CM system is used.

5.3.1.1.12 ACM_CAP.3.8C

The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

5.3.1.1.13 ACM_CAP.3.9C

The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

5.3.1.1.14 ACM_CAP.3.10C

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

5.3.1.1.15 ACM_CAP.3.1E

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

5.3.1.2 TOE CM coverage (ACM_SCP.1)

5.3.1.2.1 ACM_SCP.1.1D

~~The developer shall provide CM documentation~~ **The developer shall provide a list of configuration items for the TOE.**[10]

5.3.1.2.2 ACM_SCP.1.1C

~~The CM documentation shall show that the CM system, as a minimum, tracks the following: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, and CM documentation.~~ **The list of configuration items shall include the following: implementation representation and the evaluation evidence required by the assurance components in the ST.**[11]

5.3.1.2.3 ACM_SCP.1.2C

~~The CM documentation shall describe how configuration items are tracked by the CM system.~~~~[12]~~

5.3.1.2.4 ACM_SCP.1.1E

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

5.3.2 Delivery and Operation (ADO)

5.3.2.1 Delivery Procedures (ADO_DEL.1)

5.3.2.1.1 ADO_DEL.1.1D

The developer shall document procedures for delivery of the TOE or parts of it to the user.

5.3.2.1.2 ADO_DEL.1.2D

The developer shall use the delivery procedures.

[10] This requirement has been modified to comply with International Interpretation RI #4.

[11] This requirement has been modified to comply with International Interpretation RI #4.

[12] This requirement has been modified to comply with International Interpretation RI #4.

5.3.2.1.3 ADO_DEL.1.1C

The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

5.3.2.1.4 ADO_DEL.1.1E

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

5.3.2.2 Installation, generation, and start-up procedures (ADO_IGS.1)

5.3.2.2.1 ADO_IGS.1.1D

The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

5.3.2.2.2 ADO_IGS.1.1C

~~The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.~~ **The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.**[13]

5.3.2.2.3 ADO_IGS.1.1E

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

5.3.2.2.4 ADO_IGS.1.2E

The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.3.3 Development (ADV)

5.3.3.1 Informal functional specification (ADV_FSP.1)

5.3.3.1.1 ADV_FSP.1.1D

The developer shall provide a functional specification.

5.3.3.1.2 ADV_FSP.1.1C

The functional specification shall describe the TSF and its external interfaces using an informal style.

5.3.3.1.3 ADV_FSP.1.2C

The functional specification shall be internally consistent.

5.3.3.1.4 ADV_FSP.1.3C

The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

5.3.3.1.5 ADV_FSP.1.4C

The functional specification shall completely represent the TSF.

[13] This change has been made to conform to International Interpretation RI#51.

5.3.3.1.6 ADV_FSP.1.1E

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

5.3.3.1.7 ADV_FSP.1.2E

The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.2 Security enforcing high-level design (ADV_HLD.2)

5.3.3.2.1 ADV_HLD.2.1D

The developer shall provide the high-level design of the TSF.

5.3.3.2.2 ADV_HLD.2.1C

The presentation of the high-level design shall be informal.

5.3.3.2.3 ADV_HLD.2.2C

The high-level design shall be internally consistent.

5.3.3.2.4 ADV_HLD.2.3C

The high-level design shall describe the structure of the TSF in terms of subsystems.

5.3.3.2.5 ADV_HLD.2.4C

The high-level design shall describe the security functionality provided by each subsystem of the TSF.

5.3.3.2.6 ADV_HLD.2.5C

The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

5.3.3.2.7 ADV_HLD.2.6C

The high-level design shall identify all interfaces to the subsystems of the TSF.

5.3.3.2.8 ADV_HLD.2.7C

The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

5.3.3.2.9 ADV_HLD.2.8C

The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

5.3.3.2.10 ADV_HLD.2.9C

The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

5.3.3.2.11 ADV_HLD.2.1E

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

5.3.3.2.12 ADV_HLD.2.2E

The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.3.3.3 Informal correspondence demonstration (ADV_RCR.1)

5.3.3.3.1 ADV_RCR.1.1D

The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

5.3.3.3.2 ADV_RCR.1.1C

For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

5.3.3.3.3 ADV_RCR.1.1E

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

5.3.4 Guidance Documents (AGD)

5.3.4.1 Administrator Guidance (AGD_ADM.1)

5.3.4.1.1 AGD_ADM.1.1D

The developer shall provide administrator guidance addressed to system administrative personnel.

5.3.4.1.2 AGD_ADM.1.1C

The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

5.3.4.1.3 AGD_ADM.1.2C

The administrator guidance shall describe how to administer the TOE in a secure manner.

5.3.4.1.4 AGD_ADM.1.3C

The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

5.3.4.1.5 AGD_ADM.1.4C

The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

5.3.4.1.6 AGD_ADM.1.5C

The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

5.3.4.1.7 AGD_ADM.1.6C

The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

5.3.4.1.8 AGD_ADM.1.7C

The administrator guidance shall be consistent with all other documentation supplied for evaluation.

5.3.4.1.9 AGD_ADM.1.8C

The administrator guidance shall describe all security requirements on the IT environment that are relevant to the administrator.

5.3.4.1.10 AGD_ADM.1.1E

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

5.3.4.2 User Guidance (AGD_USR.1)

5.3.4.2.1 AGD_USR.1.1D

The developer shall provide user guidance.

5.3.4.2.2 AGD_USR.1.1C

The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

5.3.4.2.3 AGD_USR.1.2C

The user guidance shall describe the use of user-accessible security functions provided by the TOE.

5.3.4.2.4 AGD_USR.1.3C

The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

5.3.4.2.5 AGD_USR.1.4C

The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

5.3.4.2.6 AGD_USR.1.5C

The user guidance shall be consistent with all other documentation supplied for evaluation.

5.3.4.2.7 AGD_USR.1.6C

The user guidance shall describe all security requirements on the IT environment that are relevant to the user.

5.3.4.2.8 AGD_USR.1.1E

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

5.3.5 Life Cycle Support (ALC)

5.3.5.1 Identification of security measures (ALC_DVS.1)

5.3.5.1.1 ALC_DVS.1.1D

The developer shall produce development security documentation.

5.3.5.1.2 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.

5.3.5.1.3 ALC_DVS.1.2C

The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

5.3.5.1.4 ALC_DVS.1.1E

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

5.3.5.1.5 ALC_DVS.1.2E

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

5.3.5.2 Basic flaw remediation (ALC_FLR.1)

5.3.5.2.1 ALC_FLR.1.1D

The developer shall provide flaw remediation procedures addressed to TOE developers[14].

5.3.5.2.2 ALC_FLR.1.1C

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

5.3.5.2.3 ALC_FLR.1.2C

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.

5.3.5.2.4 ALC_FLR.1.3C

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

5.3.5.2.5 ALC_FLR.1.4C

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

5.3.5.2.6 ALC_FLR.1.1E

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

5.3.6 Security Testing (ATE)

5.3.6.1 Analysis of Coverage (ATE_COV.2)

5.3.6.1.1 ATE_COV.2.1D

The developer shall provide an analysis of the test coverage.

5.3.6.1.2 ATE_COV.2.1C

The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

[14] per Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, Supplement: ALC_FLR - Flaw Remediation (CEM-2001/0015R), Annex A: Flaw Remediation evaluation criteria

5.3.6.1.3 ATE_COV.2.2C

The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

5.3.6.1.4 ATE_COV.2.1E

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

5.3.6.2 Testing: high-level design (ATE_DPT.1)

5.3.6.2.1 ATE_DPT.1.1D

The developer shall provide the analysis of the depth of testing.

5.3.6.2.2 ATE_DPT.1.1C

The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

5.3.6.2.3 ATE_DPT.1.2E

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

5.3.6.3 Functional testing (ATE_FUN.1)

5.3.6.3.1 ATE_FUN.1.1D

The developer shall test the TSF and document the results.

5.3.6.3.2 ATE_FUN.1.2D

The developer shall provide test documentation.

5.3.6.3.3 ATE_FUN.1.1C

The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

5.3.6.3.4 ATE_FUN.1.2C

The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

5.3.6.3.5 ATE_FUN.1.3C

The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

5.3.6.3.6 ATE_FUN.1.4C

The expected test results shall show the anticipated outputs from a successful execution of the tests.

5.3.6.3.7 ATE_FUN.1.5C

The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

5.3.6.3.8 ATE_FUN.1.1E

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

5.3.6.4 Independent testing – sample (ATE_IND.2)

5.3.6.4.1 ATE_IND.2.1D

The developer shall provide the TOE for testing.

5.3.6.4.2 ATE_IND.2.1C

The TOE shall be suitable for testing.

5.3.6.4.3 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.

5.3.6.4.4 ATE_IND.2.1E

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

5.3.6.4.5 ATE_IND.2.2E

The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

5.3.6.4.6 ATE_IND.2.3E

The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.3.7 Vulnerability Assessment (AVA)

5.3.7.1 Examination of guidance (AVA_MSU.1)

5.3.7.1.1 AVA_MSU.1.1D

The developer shall provide guidance documentation.

5.3.7.1.2 AVA_MSU.1.1C

The guidance documentation 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.

5.3.7.1.3 AVA_MSU.1.2C

The guidance documentation shall be complete, clear, consistent and reasonable.

5.3.7.1.4 AVA_MSU.1.3C

The guidance documentation shall list all assumptions about the intended environment.

5.3.7.1.5 AVA_MSU.1.4C

The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

5.3.7.1.6 AVA_MSU.1.1E

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

5.3.7.1.7 AVA_MSU.1.2E

The evaluator shall repeat all configuration and installation procedures to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

5.3.7.1.8 AVA_MSU.1.3E

The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

5.3.7.2 Strength of TOE security function evaluation (AVA_SOF.1)

5.3.7.2.1 AVA_SOF.1.1D

The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

5.3.7.2.2 AVA_SOF.1.1C

For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

5.3.7.2.3 AVA_SOF.1.2C

For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

5.3.7.2.4 AVA_SOF.1.1E

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

5.3.7.2.5 AVA_SOF.1.2E

The evaluator shall confirm that the strength claims are correct.

5.3.7.3 Developer vulnerability analysis (AVA_VLA.1)

5.3.7.3.1 AVA_VLA.1.1D

~~The developer shall perform and document an analysis of the TOE deliverables searching for obvious ways in which a user can violate the TSP.~~ **The developer shall perform a vulnerability analysis.**[15]

5.3.7.3.2 AVA_VLA.1.2D

~~The developer shall document the disposition of obvious vulnerabilities.~~ **The developer shall provide vulnerability analysis documentation.** [16]

5.3.7.3.3 AVA_VLA.1.1C

~~The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.~~ **The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.**[17]

5.3.7.3.4 AVA_VLA.1.2C

The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.[18]

[15] This requirement has been modified to comply with International Interpretation #51.

[16] This requirement has been modified to comply with International Interpretation #51.

[17] This requirement has been modified to comply with International Interpretation #51.

[18] This requirement has been added to comply with International Interpretation #51.

5.3.7.3.5 AVA_VLA.1.3C

The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE. [19]

5.3.7.3.6 AVA_VLA.1.1E

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

5.3.7.3.7 AVA_VLA.1.2E

The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

[19] This requirement has been added to comply with International Interpretation #51.

6. TOE Summary Specification

This chapter describes the security functions and associated assurance measures.

6.1 TOE Security Functions

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

ArcSight 3.0 records two types of events; security events and analyzer events. The analyzer events are discussed separately in Section 6.1.7. Security events relate to the proper functioning and use of the system, and allow an administrator to track the management functions performed.

The ArcSight Manager relies on the underlying operating system to provide a file system to write audit and error logs. The security event audit data is written to a file system on the ArcSight Manager that is protected by the underlying operating system. The ArcSight Manager sits at the center of ArcSight 3.0 and acts as a link between the ArcSight Console, ArcSight Database, and ArcSight SmartAgent. The ArcSight Console provides the Administrator the ability to view security audit data for the system. The audit data displayed and the data contained in the audit record 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 obtains the date/timestamp from the IT environment. No security related actions can be taken without a successful user identification and authentication. The ArcSight Console allows only users who have the Administrator role to view the audit records.

Following are the events that are recorded;

- 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 is 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
- Modifications to the group of users that are part of a role

This audit data is presented in a readable format, as such the authorized Administrator can read and interpret the content of the information. In addition, the authorized Administrator can sort the audit data based on at least the following event attributes: date and time of the event, type of event, and success or failure of related event.

These Audit generation and review measures satisfy the following security requirements:

- **FAU_GEN.1**

- **FAU_SAR.1**
- **FAU_SAR.2**
- **FAU_SAR.3**

FAU_SEL.1 Selectable Audit

The ArcSight Console provides the Administrator the ability to include or exclude auditable events based on event type. The Administrator 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.

FAU_STG.4 Prevention of Audit Data Loss

To prevent audit data loss, a warning is sent to the designated administrator via e-mail should the ArcSight database begin to run out of storage space for the audit records. The capacity is set at 85% full (default setting), at which time e-mail is sent to the authorized Administrator. If the storage space for audit records reaches capacity, all incoming events from SmartAgents are stopped and all events that are currently being processed are stored temporarily in the local OS file system of the ArcSight Manager until the database 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 database failure. Until the database failure is cleared, no users are allowed to access the ArcSight Manager. The administrator accesses the database directly to free-up storage space that will clear the database failure. These measures ensure that very few events will need to be preserved on the local OS file system which in turn ensures that no audit information will be lost. The ArcSight Manager continues to monitor the database. Once space has been freed up, the ArcSight Manager will allow users to log in and will begin receiving events from SmartAgents, again.

6.1.2 Identification and Authentication

FIA_ATD.1 User Attribute Definition

The ArcSight Manager maintains user accounts on the authorized users of the system. The user account maintains the following attributes associated with the user, user identity; authentication data (passwords); authorizations (groups); e-mail address; and pager information. To protect the passwords, the ArcSight Manager only stores MD5 hashes of the passwords in the database. The ArcSight Console provides the graphical user interface (GUI) for administrators to create and maintain the user accounts.

FIA_UID.1 Timing of Identification and FIA_UAU.1 Timing of Authentication

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

To login to the ArcSight Console, the user provides the login name and password. The administrator console compares the password to that stored in the ArcSight database. If either the login name or the password is incorrect, the login request will fail and no administrator functions will be made available. As result of a successful login, the console session is established and the administrator functions are made available.

For non-administrative functions no authentication is required. The primary non-administrative function of the TOE is to collect data on network anomalies identified by third-party network monitoring devices (e.g. Intrusion Detection Systems (IDS) Sensors or IDS Scanners, firewalls, etc) by the ArcSight Smart Agents. The ArcSight Smart Agents then sends the data to the ArcSight Manager.

This security function has a strength of function claim of SOF-basic, more specifically the security functional requirement, FIA_UAU.1.

6.1.3 Security Management

FMT_MOF.1 Management of Security Functions Behavior

ArcSight 3.0 requires user authentication before any administrative actions can be performed (other than entry of identification and authentication data) on the Console, security-related or otherwise. As a result, only authorized

Administrators, Authors, and Operators can access any function on the TOE via the Console. The authorized Analyzer Administrator can create customized rules, but they do not have the authority to enable the rules, only the authorized Administrator can enable the rules and the course of action to take against events. Although, the authorized Operator can respond to events with preset automated actions.

FMT_MTD.1 Management of TSF Data

The ArcSight Console requires user authentication before any administrative actions can be performed (other than entry of identification and authentication data) on the TOE, security-related or otherwise. As a result, only authenticated users can access any functions on the system. Users with the Analyzer Administrator role have the ability to create custom rules to enforce security polices and procedures. Users with the Operator role have the ability to view, interpret, and respond to events with preset automated actions. Users with the Administrator role have the overall responsibility of managing and configuring the TOE. The Administrators create, modify, delete, configure, and implement the rules on the TOE. In addition, the Administrator is also the only role that can manage the security settings on the system, such as user accounts and audit settings.

FMT_SMF.1 Specification of Management Functions

The ArcSight Console provides a graphical user interface (GUI) that provides the Administrators, Analyzer Administrator, and Operators with an intuitive 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. Such as, modify the behavior of the data collection and review, query audit data, and restrict access and/or the ability to query and modify all other TOE data to the appropriate authorized user/authorized role.

FMT_SMR.1 Security Roles

ArcSight 3.0 supports the roles listed below. When a new user account is created, it must be assigned to one of these roles.

- Administrators – The Administrator uses the ArcSight Console to view the overall health of an enterprise and perform administrative tasks such as managing, configuring, and integrating ArcSight 3.0 with multi-vendor devices. Only the Administrator can implement the custom rules. The Administrator also manages users and sets authorizations.
- Analyzer Administrator – Analyzer Administrator use the ArcSight Console to create customized rules, escalation procedures, and Knowledge Base articles to enforce enterprise security policies and procedures.
- Operators – Operators use 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.

6.1.4 Protection of the TSF

FPT_AVL.1 Inter-TSF data availability (EXP)

If the ArcSight database fills up, the ArcSight Manager stops accepting new events from the ArcSight SmartAgents. The ArcSight SmartAgents will use the local operating system disk-based cache to temporarily store the events until the ArcSight Manager starts accepting events once again. Once the space has been freed on the ArcSight database, the ArcSight Manager is re-enabled so that the cached and live events may flow up from the ArcSight SmartAgents.

To prevent audit data loss if the ArcSight database reaches capacity, the ArcSight Manager will continue to create audit events for any scheduled actions or actions triggered by the processing of any events prior to the ArcSight database reaching capacity. The audit events are temporarily stored on the local operating system file system. Until the ArcSight database is cleared, no users are allowed access to the ArcSight Manager, ensuring that very few events will need to be preserved on the local operating system. Once the ArcSight database has been cleared, the ArcSight Manager will be re-enabled to accept the cached and live events and allow users to log in.

FPT_ITT.1 Internal TOE TSF data transfer

The ArcSight SmartAgent, ArcSight Manager, and ArcSight Console all protect TSF data from disclosure and modification, when it is transmitted between separate parts of the TOE, by communicating using SSL connections.

The SSL connection is the standard HTTP over SSL, often referred to as HTTPS (HyperText Transfer Protocol Secure). ArcSight uses X.509 certificates. The certificates must be a 128-bit X.509 Version 3 certificate. The maximum key size for the public key in the certificate is 1024 bits.

For SSL communication, all components of ArcSight 3.0 that are SSL endpoints, that is, ArcSight Console, ArcSight Manager, and ArcSight SmartAgents, 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 the ArcSight SmartAgents and the ArcSight Console that talk to the ArcSight Manager 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.

6.1.5 Analyzer Analysis

IDS_ANL.1 Analyzer Analysis

The ArcSight Manager uses a collection of tools that allows the Administrator to track, respond, and resolve security threats and attacks. The Cross-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 cross-correlate events using signatures and trigger automated response actions. The Cross-Correlation Engine in ArcSight Manager correlates events across vendor, across device, and across time. By cross-correlating different events, the Cross-Correlation Engine detects successful attacks, their criticality, and threat level. At a minimum, each analytical result is logged with following information; data and time and identification of data source.

The Cross-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 Cross-Correlation Engine generates a derived event and performs the other actions associated with the rule.

There are predefined threat level formula, 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 SmartAgent. 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

IDS_RCT.1 Analyzer React

Rule actions are automatic procedures that occur when all rule conditions and threshold settings have been met. The Administrator can choose to be notified of a triggered rule at the ArcSight Console or have information about the events that triggered the rule sent to a case or an active list. The following list describes some additional actions you can specify for a rule:

- Create an Active List rule action - The Active List rule action modifies the contents of an active list. Active Lists are tables of information, for instance a collection of IP addresses and zones, which are used to record prior actions from or intrusions on various devices. For instance, there are Active Lists to record hostile hosts, suspicious hosts, hosts that have performed prior recon on the protected network, and hosts that have been attacked, scanned, or compromised. Once a rule is triggered, the Active List rule action may add or remove an address mentioned in the derived event from an Active List. Rule conditions can also reference Active Lists. For instance, a rule may only match if the source address of an event appears in the Hostile Active List.

- Create an Execute Command rule action - The Execute Command rule action is used to execute a command line function when the rule is triggered. The command line function may be executed on the ArcSight Manager machine or an ArcSight SmartAgent machine.
- Create a Send to Console rule action - The Send to Console rule actions sends a meta-event to the ArcSight Console when the rule is triggered. A meta-event is generated by a rule when its conditions and threshold settings are met. The Send to Console rule action should always be used. Setting this action displays the lightning bolt-fired rule event on the Console. In the absence of a Send to Console, derived events are explicitly removed from the live stream of events before being presented to the Consoles. The lightning bolt is associated with all derived events displayed in the grid, whether they are displayed live or as part of a query result.
- Create a Case rule action – The Case rule actions create and modify cases, which are used to track the investigation of incidents. Rule actions may add the meta-event created when the rule triggered to a pre-existing case or the action may first create a new case.
- Create a Notification rule action – The Notification rule actions are used to inform ArcSight users that an incident has occurred. The notification may be delivered by email, pager, text message, or it may only be delivered to the user the next time the log into the ArcSight Manager using the ArcSight Console.

6.1.7 System Data Review, Availability and Loss

IDS_RDR.1 Restricted Data Review

In an ArcSight 3.0 environment, only successfully authenticated users can access the ArcSight Console and then only users who hold the appropriate authorization can vies the data. Using the ArcSight Console graphical user interface, authorized Administrators can view the overall health of the enterprise as well as the data colleted. The authorized Administrators can view the audit data, reports, to include the analytical results, configuration information, and other applicable analyzer data that is collected. In addition, Operators can query the data collected via the ArcSight Console. 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, be it the Administrator or the authorized Operator can understand the content of the information presented, hence the information is presented in a manner suitable for human interpretation.

IDS_STG.1 Guarantee of Analyzer Data Availability

All users must be identified and authenticated. In an ArcSight 3.0 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 the ArcSight SmartAgent. Only a properly identified and authenticated Administrator has the ability to read and delete the analyzer data log. Only the authorized administrator can delete and/or clear the audit trail, therefore preventing unauthorized deletion. The Administrators control the retention period of the audit logs that typically range from 30 to 90 days.

IDS_STG.2 Prevention of Analyzer Data Loss

To prevent analyzer data loss, a warning is sent to the designated administrator via e-mail should the database begin to run out of storage space for the analyzer data records. The capacity is set at 85% full (default setting), at which time e-mail is sent to the authorized Administrator.

If the ArcSight database fills up, the ArcSight Manager stops accepting new events from all ArcSight SmartAgent. Those ArcSight SmartAgent will use local operating system disk-based cache to preserve those events until the ArcSight Manager starts accepting events once again. Once space has been freed on the ArcSight database, the ArcSight Manager is re-enabled so that the cached and live events may flow up from the ArcSight SmartAgent.

If the ArcSight Manager fails, the ArcSight Agents 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 stores 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 ArcSight SmartAgent.

If an ArcSight SmartAgent fails, it will continue processing with the next log file line or database row. If the ArcSight SmartAgent is monitoring a live feed via, for example, SNMP, then all events that occurred while the ArcSight SmartAgent was down are lost.

6.2 TOE Security Assurance Measures

6.2.1 Configuration management

The configuration management measures applied by ArcSight ensure that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE. ArcSight ensures changes to the implementation representation are controlled. ArcSight performs configuration management on the TOE implementation representation, design documentation, tests and test documentation, user and administrator guidance, delivery and operation documentation, life-cycle documentation, vulnerability analysis documentation, and configuration management documentation and all of these items are identified in the CM Plan as configuration items.

These activities are documented in:

- Configuration Management (ACM_CAP-3) document
- Perforce and Branching document
- Perforce Configuration Items for ArcSight 3.0 document
- Perforce Naming Conventions document

The Configuration management assurance measure satisfies the following EAL 3 augmented with ALC_FLR.1 assurance requirements:

- ACM_CAP.3
- ACM_SCP.1

6.2.2 Delivery and operation

ArcSight provides delivery documentation and procedures to identify the TOE, secure the TOE during delivery, and provide necessary installation and generation instructions. ArcSight's delivery procedures describe all applicable procedures to be used to prevent in appropriate access to the TOE. ArcSight also provides documentation that describes the steps necessary to install ArcSight 3.0 in accordance with the evaluated configuration.

These activities are documented in:

- Delivery Procedures (ADO_DEL.1) document
- Installation, generation, and start-up procedures (ADO_IGS.1) document
- ArcSight Administrator's Guide, Version 3.0 SP2: Installation, Configuration, and Maintenance of the ArcSight System
- ArcSight SmartAgent Installation Guide, ArcSight Version 3.0
- SmartAgent Configuration Guide, Check Point FireWall-1, OPSEC Agent, NG OPSEC Agent
- SmartAgent Configuration Guide, Nessus Vulnerability Scanner, Report Agent
- SmartAgent Configuration Guide, Snort, Open Source Network Intrusion Detection System, Database Agent, Log-file Agent

- SmartAgent Readme March 17 2006
- Patch Readme files
  - Patch 9 [3.0.2.9.3939], March 22 2006
- ArcSight Version 3.0 Pre-installation Readme File
- Quick Start Guide ArcSight Version 3.0

The Delivery and operation assurance measure satisfies the following EAL 3 augmented with ALC_FLR.1 assurance requirements:

- ADO_DEL.1
- ADO_IGS.1

6.2.3 Development

ArcSight has numerous documents describing all facets of the design of the TOE. In particular, they have a functional specification that describes the accessible TOE interfaces; a high-level design that decomposes the TOE architecture into subsystems and describes each subsystem and their interfaces; and, correspondence documentation that explains how each of the design abstractions correspond from the TOE summary specification in the Security Target to the subsystems.

These activities are documented in:

- ArcSight 3.0 Combined Functional Specification and High-level Design with supporting documentations

The Development assurance measure satisfies the following EAL 3 augmented with ALC_FLR.1 assurance requirements:

- ADV_FSP.1
- ADV_HLD.2
- ADV_RCR.1

6.2.4 Guidance documents

ArcSight provides administrator and user guidance on how to utilize the TOE security functions and warnings to administrators and users about actions that can compromise the security of the TOE.

These activities are documented in:

- ArcSight Administrator’s Guide, Version 3.0 SP2
- Using the ArcSight Console, Version 3.0 SP2
- ArcSight Readme, November 12 2004
- ArcSight ESM Release Notes version 3.0 SP2
- ArcSight SmartAgent Installation Guide, ArcSight Version 3.0
- SmartAgent Configuration Guide, Check Point FireWall-1, OPSEC Agent, NG OPSEC Agent
- SmartAgent Configuration Guide, Nessus Vulnerability Scanner, Report Agent
- SmartAgent Configuration Guide, Snort, Open Source Network Intrusion Detection System, Database Agent, Log-file Agent
- SmartAgent Readme March 17 2006

- Patch Readme files
    - Patch 9 [3.0.2.9.3939], March 22 2006

The Guidance documents assurance measure satisfies the following EAL 3 augmented with ALC_FLR.1 assurance requirements:

- AGD_ADM.1
- AGD_USR.1

6.2.5 Life cycle support

ArcSight ensures the adequacy of the procedures used during the development and maintenance of the TOE through its life-cycle. ArcSight includes security controls on the development environment that are adequate to provide the confidentiality and integrity of the TOE design and implementation that is necessary to ensure the secure operation of the TOE. In addition, ArcSight identifies and tracks reported flaws, ensuring that they are addressed and corrections and corrective measures are made available as applicable.

These activities are documented in:

- Identification of Security Measures (ALC_DVS.1)
- Information Systems Access Policy
- Basic Flaw Remediation (ALC_FLR.1)

The Life cycle support assurance measure satisfies the following EAL 3 augmented with ALC_FLR.1 assurance requirements:

- ALC_DVS.1
- ALC_FLR.1

6.2.6 Tests

ArcSight has a test plan that describes how each of the necessary security functions is tested, along with the expected test results. ArcSight has documented each test as well as an analysis of test coverage and depth demonstrating that the security aspects of the design evident from the functional specification and high-level design are appropriately tested. Actual test results are created on a regular basis to demonstrate that the tests have been applied and that the TOE operates as designed.

These activities are documented in:

- ArcSight Inc. Common Criteria Test Plan
- ArcSight.CC.TestCases
- ArcSight.CC.TestResults.Sol.xls
- ArcSight.CC.TestResults.Win.xls

The Tests assurance measure satisfies the following EAL 3 augmented with ALC_FLR.1 assurance requirements:

- ATE_COV.2
- ATE_DPT.1
- ATE_FUN.1
- ATE_IND.2

6.2.7 Vulnerability assessment

The TOE administrator and user guidance documents describe the operation of ArcSight 3.0 and how to maintain a secure state. These guides also describe all necessary operating assumptions and security requirements outside the scope of control of the TOE. They have been developed to serve as complete, clear, consistent, and reasonable administrator and user references.

ArcSight has conducted a strength of function analysis wherein all permutational or probabilistic security mechanisms have been identified and analyzed resulting in a demonstration that all of the relevant mechanisms fulfill the minimum strength of function claim, SOF-basic.

ArcSight performs regular vulnerability analyses of the entire TOE (including documentation) to identify obvious weaknesses that can be exploited in the TOE.

These activities are documented in:

- Vulnerability Analysis
- ArcSight 3.0 Strength of Security Functions (AVA_SOF.1)

The Vulnerability assessment assurance measure satisfies the following EAL 3 augmented with ALC_FLR.1 assurance requirements:

- AVA_MSU.1
- AVA_SOF.1
- AVA_VLA.1

7. Protection Profile Claims

The TOE conforms to the U.S. Government Intrusion Detection System Analyzer Protection Profile, Version 1.2, April 27, 2005. Given the TOE is a software TOE, the ST follows the guidance included in the Errata section of the U.S. Government Intrusion Detection System Analyzer Protection Profile. In addition, ArcSight has elected to pursue a more vigorous assurance level as depicted in Section 1.2, Conformance Claims.

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

This Security Target includes all of the Security Objectives from the PP, verbatim.

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_SAR.1	*Assignment* – completed the assignment.
FAU_SEL.1	*Assignment* – completed the assignment.
FAU_STG.2	*Assignment* – completed the assignment. *Moved* – per the Errata Sheet, this requirement has been moved to the IT Environment *Refined* - to indicate the IT Environment enforces the security function and not the TSF
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 OD-250.
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.
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. 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	*Assignment* - completed the assignment. *Refinement* – to correctly identify the role(s) supported by the TOE.
FPT_ AVL.1	*Added* –The requirement ensures the audit data and Analyzer data are available when certain conditions occur. Reference OD 250.
FPT_ITA.1	*Removed* – this requirement was removed even though it is trivially satisfied since the TOE does not provide audit and analyzer data to external IT products. Reference OD 250
FPT_ITC.1	*Removed* – this requirement was removed even though it is trivially satisfied since the TOE does not transmit data to external IT products. Reference OD 250
FPT_ITI.1	*Removed* – this requirement was removed even though it is trivially satisfied since the TOE does not transmit data to external IT products. Reference OD 250
FPT_ITT.1	*Added* – this requirement was added to protect inter-communications between the

Requirement Component	Modification of Security Functional and Security Assurance Requirements
	distributed TOE components. This requirement replaces the following requirements: FPT_ITA.1, FPT_ITC.1, and FPT_ITI.1. *Selection* – completed the selection.
FPT_RVM.1	*Moved* – per the Errata Sheet, this requirement has been moved to the IT Environment
FPT_SEP.1	*Moved* – per the Errata Sheet, this requirement has been moved to the IT Environment *Refined* - to indicate the IT Environment enforces the security function and not the TSF
FPT_STM.1	*Moved* – per the Errata Sheet, this requirement has been moved to the IT Environment *Refined* - to indicate the IT Environment enforces the security function and not the TSF and the timestamp is used for the TOE.
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 environment requiring more assurance that the security functions are enforced, this Security Target has adopted the EAL3 security assurance requirements.

Table 6: Modification of PP claims

Interpretations

The following changes to the have been made based on National and International Interpretations.

a) Security Functional Requirements

- FMT_SMF.1 - this requirement was added in this Security Target to satisfy a dependency added to FMT_MOF.1 by International Interpretation RI#65.

b) Security Assurance Requirements

Note: These interpretations have no impact on conformance with the PP since they only serve to clarify three of the assurance claims.

- ACM_CAP.3 – this element was added per International Interpretation RI #03
- ACM_SCP.*.1D – this element was changed per International Interpretation RI #04
- ACM_SCP.*.1C – this element was changed per International Interpretation RI #04
- ADO_IGS.*.1C – this element was changed per International Interpretation RI #51
- AVA_VLA.1.*D and AVA_VLA.1.*C - these elements were changed per International Interpretation RI #51

8. Rationale

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

- Security Objectives;
- Security Requirements;
- Security Assurance;
- Explicitly Stated Requirements;
- Strength of Function;
- Security Functional Requirement Dependencies; and
- TOE Summary Specification

8.1 Security Objectives Rationale

The security objective rationale is presented in Section 7.1, Section 7.2, and Errata Sheets of the U.S. Government Intrusion Detection System Analyzer Protection Profile.

All of the assumptions, threats, and security objectives have been reproduced from the U.S. Government Intrusion Detection System Analyzer Protection Profile to this ST.

8.2 Security Requirements Rationale

The security requirements rationale is presented in Section 7.3 and the Errata Sheets of the U.S. Government Intrusion Detection System Analyzer Protection Profile.

All of the security functional requirements have been reproduced from the U.S. Government Intrusion Detection System Analyzer Protection Profile 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 in International Interpretation RI#65. 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_ AVL.1 (EXP) – this requirement was included to address OD 250 that requires the availability of all audit and Analyzer data when certain conditions occur. The requirement ensures the availability of audit data and Analyzer data if the ArcSight database reaches capacity. If the ArcSight database reaches capacity, the ArcSight Manager stops accepting events. The audit events and Analyzer data (events form the ArcSight SmartAgents) are temporarily stored on the local operating system. Once the space has been freed on the ArcSight database, the ArcSight Manager is re-enabled to accept the cached and live events and allow users to log in and to start accepting the cached and live events from the ArcSight SmartAgents. .
- 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 3.0 is not intended to make data available to other IT products and in the case of a distributed ArcSight 3.0 architecture, the components are expected to be connected with a benign, private, and protected communication network. Reference OD 250.

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 is requirement is not applicable. Reference OD 250.
- 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 OD 250.
- 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 OD 250.
- 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 OD 250.

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

8.3 Security Assurance Rationale

EAL3 was chosen to provide a low to 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 System 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. At EAL3, the System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

The ArcSight 3.0 appliances meet all the U.S. Government Intrusion Detection System Analyzer Protection Profile Functional and Assurance Requirements as so stated for EAL2. Additionally, the TOE conforms to all the Assurance Requirements for an EAL3 product. The resulting assurance level is therefore, EAL3.

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

ACM_CAP.3 Authorisation Controls

It is important that changes to the TOE be appropriately controlled. This requirement helps to ensure that unauthorized modifications are not made to the TOE.

ACM_SCP.1 TOE CM coverage

It is important that the changes to the TOE be controlled. This requirement helps to ensure that modifications to the TOE implementation representation, design, tests, user and administrator documentation, and CM documentation are performed in a controlled manner with proper authorizations.

ADV_HLD.2 Security enforcing high-level design

It is important to identify the basic structure of the TSF and the major hardware, firmware, and software elements of the product. This requirement will provide the necessary detail for supporting both thorough testing of the TOE and the assessment of vulnerabilities.

ALC_DVS.1 Identification of security measures

It is important to document the procedures that cover the physical, procedural, personnel, and other security measures that are used in the development environment. This requirement identifies the physical security of the development location, controls on the development staff, and other procedural security measures employed to protect the development environment.

ALC_FLR.1 Basic flaw remediation

It is important to document the established flaw remediation procedures that describe the tracking of security flaws, the identification of corrective actions, and the distribution of the corrective actions/solutions to the end-users.

ATE_COV.2 Analysis of Coverage

It is important to demonstrate that the TSF satisfies the TOE security functional requirements. This requirement ensures the completeness of the functional tests performed by the developer as well as the extent to which the TOE security functions are tested.

ATE_DPT.1 Testing: high-level design

It is important to demonstrate the level of detail to which the developer tests the TOE. This requirement ensures that the TSF operates in accordance with the high-level design.

AVA_MSU.1 Examination of guidance

It is important to demonstrate that the TOE is configured and operating in a manner that is secure. This requirement ensures that misleading, unreasonable and conflicting guidance is absent from the guidance documentation, and that secure procedures for all modes of operation have been addressed.

8.4 Explicitly Stated Requirements Rationale

The explicitly stated requirements rationale is presented in Section 7.4 of the U.S. Government Intrusion Detection System Analyzer Protection Profile.

The CC provides the Availability of exported TSF data (FPT_ITA.1) family within the Protection of the TSF (FPT) class of security functional requirements to address prevention of loss of availability of TSF data moving between the TSF and a remote trusted IT product; however, the TOE does not transmit data to external IT products. Therefore, an explicitly stated requirement was necessary to address OD 250.

The explicitly stated requirement, FPT_AVL.1 (EXP) ensures when the ArcSight database reaches capacity and the ArcSight Manager stops accepting events, the audit events and Analyzer data (events form the ArcSight SmartAgents) are temporarily stored on the local operating system until the ArcSight database is cleared and the ArcSight Manager is re-enabled to accept the cached and live audit events and Analyzer data.

The requirement has no dependencies since the stated requirement embodies all the necessary security functions.

The requirement is mapped to O.AUDITS and O.EXPORT security objectives.

8.5 Strength of Function Rationale

The TOE minimum strength of function of SOF-basic was chosen to be consistent with the TOE and its operating environment. This strength of function level was selected because it generally corresponds with the claimed assurance level of EAL3 augmented with ALC_FLR.1. The evaluated TOE is intended to operate in commercial and DoD environments processing unclassified information.

The SOF-basic claim is associated with the password mechanism, which is of a probabilistic or permutational nature. The password mechanism is used in the Identification and Authentication security function to authenticate user identity. The relevant security functional requirement is FIA_UAU.1. The intent is that the password mechanism meets or exceeds SOF-basic and the evidence can be found in the strength of function analysis included in ArcSight 3.0 Vulnerability Assessment.

8.6 Requirements Dependency Rationale

The dependency requirements rationale is presented in Section 7.7 of the U.S. Government Intrusion Detection System Analyzer Protection Profile.

This Security Target includes three Security Functional Requirements not included in the U.S. Government Intrusion Detection System Analyzer Protection Profile; FMT_SMF.1, FPT_ITA_AVL.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 in International Interpretation RI#65 and introduces no additional dependencies itself. The requirement, FPT_AVL.1 was included to address OD 250 that requires the availability of all audit and Analyzer data when certain conditions occur. 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.

8.7 TOE Summary Specification Rationale

Each subsection in TOE Summary Specification section, 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 TOE Summary Specification section 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).

The only security mechanism that is realized by a probabilistic or permutational implementation is the password mechanism that is associated with the Identification and Authentication security function. For an analysis of the Strength of Function claim, SOF-basic, refer to the ArcSight 3.0 Vulnerability Assessment document.

	SECURITY AUDIT	IDENTITY & AUTHENTICATION	SECURITY MANAGEMENT	PROTECTION OF TSF	IDS COMPONENT REQUIREMENTS
FAU_GEN.1	X				
FAU_SAR 1	X				
FAU_SAR.3	X				
FAU_SEL.1	X				
FAU_STG.4	X				
FIA_UAU.1		X			
FIA_ATD.1		X			
FIA_UID.1		X			
FMT_MOF.1			X		
FMT_MTD.1			X		

	SECURITY AUDIT	IDENTITY & AUTHENTICATION	SECURITY MANAGEMENT	PROTECTION OF TSF	IDS COMPONENT REQUIREMENTS
FMT_SMF.1			X		
FMT_SMR.1			X		
FPT_AVL.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

8.8 PP Claims Rationale

See Protection Profile Claims section.