RSA Security Analytics v10.6
Security Target

Version 1.0
March 17, 2016

Prepared for:

RSA The Security Division of EMC²

10700 Parkridge Blvd.
Suite 600
Reston, VA 20191

Prepared By:

Leidos Inc. (formerly Science Applications International Corporation)
Common Criteria Testing Laboratory
6841 Benjamin Franklin Drive, Columbia, Maryland 21046

TABLE OF CONTENTS

LIST OF TABLES

1 Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE), ST conventions, ST conformance claims, and the ST organization. The Security Target was undertaken at the request and under the direction of LMR Associates, LLC, acting as Project Director for RSA Security LLC, the Security Division of EMC, regarding the Security Analytics Version 10.6 Common Criteria Certification Project. The TOE is RSA Security Analytics (SA). SA is a collection of appliances that form a security infrastructure for an enterprise network. This architecture provides converged network security monitoring and centralized security information and event management (SIEM). SA provides real-time visibility into the monitored network and long-term network data storage to provide detection, investigation, analysis, forensics, and compliance reporting. SA's Capture infrastructure collects log and packet data from the network. Packet collection extracts metadata, reassembles, and globally normalizes all network traffic at layers 2 through 7 of the Open Systems Interconnection (OSI) model. This data allows SA to perform real-time session analysis; incident detection, drill-down investigation, reporting, and forensic analysis functions.

The Security Target contains the following additional sections:

- Security Target Introduction (Section 1)
- TOE Description (Section 2)
- Security Problem Definition (Section 3)
- Security Objectives (Section 4)
- IT Security Requirements (Section 5)
- TOE Summary Specification (Section 6)
- Rationale (Section 7)

1.1 Security Target, TOE and CC Identification

ST Title –RSA Security Analytics v10.6 Security Target

ST Version – Version 1.0

ST Date – March 17, 2016

TOE Identification –RSA Security Analytics 10.6

TOE Developer – RSA The Security Division of EMC[2]

Evaluation Sponsor – RSA The Security Division of EMC[2]

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

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 3.1 Revision 4, September 2012.
    - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012.
    - Part 3 Conformant
    - Assurance Level: EAL2 augmented with ALC_FLR.1

1.3 Conventions

The following conventions have been applied in this document:

Extended requirements – Security Functional Requirements not defined in Part 2 of the CC are annotated with a suffix of _EXT.

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 identified with a number in parentheses following the base component identifier. For example, iterations of FCS_COP.1 are identified in a manner similar to FCS_COP.1(1) (for the component) and FCS_COP.1.1(1) (for the elements).

Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).

Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are 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 …").

Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.4 Glossary

Acronym	Description
API	Application Programming Interface
CC	Common Criteria
EAL	Evaluation Assurance Level
EPS	Events per Second
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDS	Intrusion Detection System
LAN	Local Area Network
OS	Operating System
OSI	Open Systems Interconnection
PP	Protection Profile
SDEE	Security Device Event Exchange
SIEM	Security Information and Event Management
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function

1.5 Terminology

The terminology below is described in order to clarify the terms used in the ST as well as those used in the TOE product documentation.

Analyzer The function of an IDS that applies analytical processes to collected IDS data in order to derive conclusions about potential or actual intrusions.

Concentrator	A concentrator that receives network packet metadata.
Decoder	A decoder that captures network packets.
IDS	Intrusion Detection System —a combination of services or functions such as an Analyzer that monitors an IT System for activity that may inappropriately affect the IT System or its resources, and that can send alerts if such activity is detected.
IDS data	Refers both to raw data collected by the TOE and to the results of analysis applied by the TOE to that data.
Index	Indexes are internal RA data structures that organize for searching the metadata elements of sessions and are generated during data processing for a collection. The content of the index, and consequently the metadata elements that are displayed in the Navigation view, are controlled by settings in effect during collection processing.
Log Concentrator	A concentrator that receives log metadata,
Log Decoder	A decoder that captures log data.
Metadata	Specific data types (Service Type, Action Event, Source IP Address, etc.) created by the parsers which are counted and itemized in the captured data. A detailed list of metadata for each parser may be found in the SA Guidance.
Parser	A software module that defines tokens and instructions for lexical processing of network streams. Processing includes stream identification and metadata extraction.
Services	Components of the product that work together to provide the security functions of the TOE such as Analyzer, Concentrator, and Decoder

2 TOE Description

The Target of Evaluation (TOE) is RSA Security Analytics (SA), hereafter referred to as Security Analytics, SA or the TOE.

2.1 TOE Overview

SA is a collection of appliances that form a security infrastructure for an enterprise network. This architecture provides converged network security monitoring and centralized security information and event management (SIEM). SA provides real-time visibility into the monitored network and long-term network data storage to provide detection, investigation, analysis, forensics, and compliance reporting. SA's capture infrastructure imports log and collects packet data from the network. Packet collection extracts metadata, reassembles, and globally normalizes all network traffic at layers 2 through 7 of the OSI model. This data allows SA to perform real-time session analysis. SA recognizes over 250 event source types, which are aggregated, analyzed, and stored for long-term use.

Data is collected and aggregated by the Decoder and Concentrator appliances. Collected data is aggregated into a complete data structure across all network layers, logs, events, and applications. The Event Stream Analysis (ESA) appliance uses this data to provide advanced stream analytics such as correlation and complex event processing at high throughputs and low latency. ESA uses Event Processing Language to bring meaning to the event flows. SA Server's user interface uses this aggregated data to provide incident detection, and drill-down investigation[1]. The Archiver appliance is a specialized concentrator or variant that receives, indexes, and compresses logs. The Archiver is adapted to hold indexed and compressed raw log and metadata, and indices for an extended period of time. The Reporting Engine and SA Server's user interface use the data to provide compliance reporting and in-depth network analysis. Raw packets and packet metadata are not stored in the Archiver.

The TOE implements additional security functions such as identification and authentication of TOE users; auditing; security management; and trusted path.

The security management functions of the TOE are performed via the SA Server Interface, which is a web-based browser GUI. This interface allows authorized administrators to manage the user accounts, session lockout values and other TSF data, and view the IDS data and alerts.

2.2 TOE Architecture

2.2.1 SA Product Components

SA is composed of multiple components that can be combined on appliances or deployed with multiple appliances depending on network needs. The components are broken into the Capture Architecture and the Analysis Architecture.

2.2.1.1 Capture Architecture

The SA Capture architecture is composed of the Decoder, Concentrator, and Broker. Each component is described below.

Decoder: The Decoder performs capture for either packets or logs. When deployed, either the packet or log capture capability is enabled. A Decoder collects packets, extracts metadata, reassembles and normalizes network traffic. A Log Decoder imports logs by either retrieving (pulling) the log records from an event source or by receiving the log records from the event sources (pushed). Each appliance sends its collected data to an assigned Concentrator.

Within a Log Decoder appliance is a Log Collector service that imports logs from the following sources:

- Syslog
- SNMP Trap
- NetFlow
- File (pushed by SFTP and FTPS)

[1] The SA product provides additional capabilities for reporting, and forensic analysis functions, which are not included in the scope of evaluation.

- Windows (WinRM)
- Windows (Legacy)
- ODBC
- Check Point LEA
- VMWare
- SDEE

Concentrator: Concentrators are deployed as either a packet or log Concentrator. These appliances aggregate and store metadata received from multiple Decoders. Concentrators also perform queries to retrieve stored metadata, as requested by external users or the SA Server.

Broker: Brokers facilitate queries between Concentrators, allowing the SA Server access to metadata across the network.

2.2.1.2 Analysis Architecture

SA Server: The SA Server hosts the user interface. This interface enables an administrator to perform incident detection, management, investigation, and device and user administration. The SA Server User Interface (UI) is accessed through HTTPS only (i.e., HTTP over TLS in FIPS mode).

Archiver: The Archiver is a stand-alone appliance. Archiver receives, indexes, and compresses log data from Log Decoders. The Archiver is adapted to hold indexed and compressed raw log and metadata, and indices for an extended period of time. The Reporting Engine and SA Server's user interface use the data (via the Broker) to provide compliance reporting and in-depth network analysis..

ESA: ESA is a stand-alone appliance that provides advanced stream analytics such as correlation and event processing. ESA receives event data from multiple Concentrators. ESA uses an advanced Event Processing Language (EPL) to filter, aggregate, join, correlate, and recognize patterns across multiple disparate event streams. ESA provides incident detection and alerting[2].

Malware Analysis: The Malware Analysis service analyzes file objects to assess the likelihood the file is malicious. This service uses network session analysis and static file analysis[3] to check for malware. The service can perform continuous or on-demand polling of Decoders or Brokers to extract sessions identified as potentially carrying malware.

Incident Management: Collects Alerts and provides authorized users the ability to group them logically and start an Incident response workflow to investigate and remediate the security issues raised. Incident Management allows the user to configure rules to automate the aggregation of Alerts into Incidents. The IM service periodically runs rules to aggregate multiple Alerts into an Incident and set some attributes of the Incident (e.g. severity, category, etc.). Users can access these functions through the SA UI.

Reporting Engine: The Reporting Engine is deployed on the same appliance as the SA Server. The Reporting Engine supports the definition and generation of reports and alerts. Administrators can create rules that govern how data is represented in reports and alerts. The Reporting Engine also manages the alert queue, allowing administrators to enable and disable alerts.

Each appliance in the SA solution can also be deployed as a virtual appliance. The functionality of the virtual appliance is the same as the hardware-based solution, though there are differences in throughput.

[2] SA can send alerts over email, syslog or SNMP traps, but these types of alert notification are not within the scope of evaluation.
[3] The SA product provides additional capabilities for dynamic file analysis, and security community analysis, which are not included in the scope of evaluation.

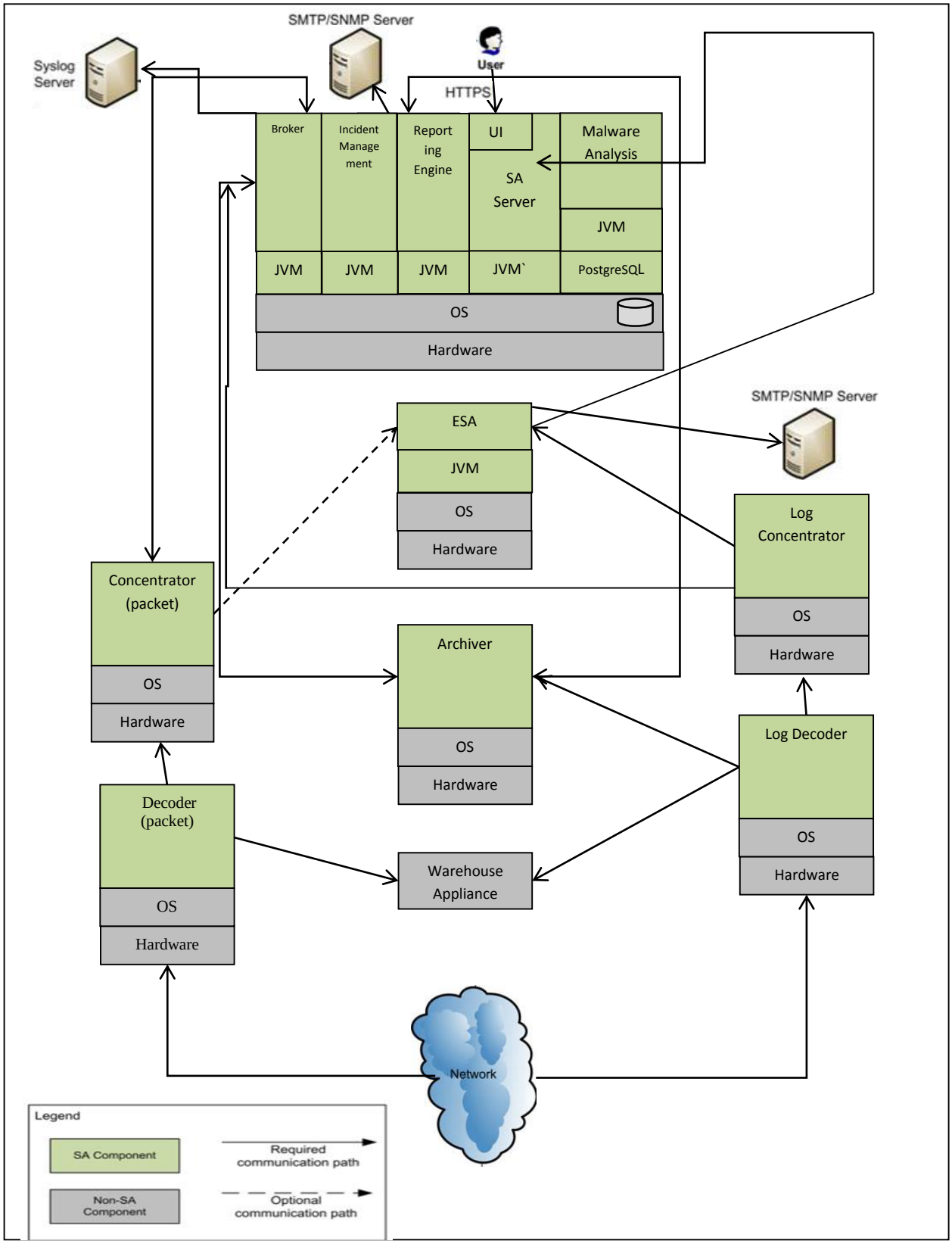

Figure 2-1 Evaluated Configuration

Communications between components are protected using TLS. The TOE configuration is described further in Section 2.2.2.4.

2.2.2 TOE Physical Boundaries

2.2.2.1 Included Product Components

Product components included in the TOE are listed below. **Error! Reference source not found.**shows a representative deployment of the TOE in its evaluated configuration.

1. Decoder (zero or more)
2. Log Decoder (zero or more)
   Note: A SA deployment includes at least one Decoder or Log Decoder.
3. Concentrator (zero or more)
4. Log Concentrator (zero or more)
   Note: A SA deployment that contains a Log Decoder must include a Log Concentrator. Likewise, a deployment that includes a Decoder for network packets must include a Concentrator for network packets.
5. Broker (One or more)
6. Event Stream Analysis (ESA) (one or more)
7. Archiver (one or more)
8. Security Analytics Server (one or more)
9. Incident Management (one or more)
10. Malware Analysis (one or more)
11. Reporting Engine (one per SA Server)
12. Java Virtual Machine (JVM) (one for each of the following services on the SA Server: Broker, Incident Management, Malware Analysis, Reporting Engine Services, and one for the UI and SA Server itself. Additionally, the ESM runs in its own JVM)
13. PostgreSQL database (one for each malware analysis)
14. TokuMX database (one for each SA Server and ESA)

2.2.2.2 Excluded Product Components

SA product components excluded from the TOE in the evaluated configuration are:

1. Warehouse appliance
2. RSA Live (content delivery)
3. Malware Community
4. Malware Sandbox
5. Virtual Log Collector
6. Legacy Windows Log Collector

SA product features excluded from the TOE in the evaluated configuration are:

1. Direct-Attached Capacity (DAC) storage for Archiver
2. Representational State Transfer, Application Programming Interface (REST API)
3. External authentication services (such as RADIUS, LDAP, and Windows Active Directory)
4. Export of security audit records to Syslog server
5. Sending SMTP, SNMP, or Syslog alerts
6. Integrated Dell Remote Access Controller (iDRAC) out-of-band appliance management capabilities
7. Serial and USB device connections (Used during installation and maintenance only)
8. Advanced Threat Detection (ATD)

2.2.2.3 Services and Products in the Operational Environment

The TOE relies on the services and products in operational environment:

1. Operating System: provides execution environment for SA components. The OS is CentOS version 6.5.
2. Hypervisor: provides virtualization for SA virtual appliances. The hypervisor is ESXi version 5.0 or later.
3. Administrator Workstation / Browser: provides human users access to SA Server user interface. SA supports Microsoft Internet Explorer (versions 10 and 11), Firefox (version 26 to 30), Safari (version 6), and Chrome (version 34 and 35.x).
4. Syslog server: SA Server can forward security audit records and alerts to an external Syslog server. **Note:** export to Syslog server was not tested in the evaluation.
5. SMTP Server: SA Server can send email messages via SMTP server. **Note:** the email message capability was not tested in the evaluation.
6. SNMP Server: SA Server can send SNMP traps. **Note:** the SNMP capability was not tested in the evaluation
7. Authentication Server: provides external authentication methods (such as Windows Active Director, RADIUS, and LDAP). **Note:** the external authentication capability was not tested in the evaluation
8. Network Traffic Sources: source of network traffic. **Note:** The TOE has a direct physical connection to a network traffic source (Decoder (packet) network connection)
9. Log Decoder Event Sources: provide log data to the TOE. SA supports event sources:
    a. Syslog
    b. SNMP Trap
    c. NetFlow
    d. File
    e. Windows (WinRM)
    f. Windows (Legacy)
    g. ODBC
    h. Check Point LEA
    i. VMWare
    j. SDEE

2.2.2.4 TOE Configurations

RSA deploys Security Analytics as a collection of appliances providing services. RSA provides the TOE as either hardware appliances or virtual appliances. The deployment of appliances varies from customer to customer. A customer with a small volume of network or log data would combine services onto a few appliances. A large enterprise customer would have appliances for each service with multiple Decoder, Concentrator, and Broker appliances. The evaluated configuration represents the range of deployments.

2.2.2.4.1 Hardware Appliance Deployments

The evaluated configuration includes the following appliances (see **Figure 2-1 Evaluated Configuration**):

1. Security Analytics Server (hosting SA Server UI, Broker, Incident Management, Malware Analysis, and Reporting Engine services)
    a. Broker, Incident Management, and Reporting Engine Services each have their own JVM. Malware Analysis has its own JVM and a PostgreSQL.
    b. Also contains a TokuMX High Performance MongoDB distribution.
2. One Decoder appliance
3. One Log Decoder appliance

    Note: A SA deployment includes at least one Decoder or Log Decoder with the following deployment.
    a. Can be deployed standalone or on appliance with Concentrator.
    b. Typical deployment is one-to-one Decoder/ Concentrator pairs; though multiple Decoders per Concentrators are technically possible.

4. One Concentrator appliance for packet data
5. One Concentrator appliance for log data
   Note: A SA deployment that contains a Log Decoder must include a Log Concentrator. Likewise, a deployment that includes a Decoder for network packets must include a Concentrator for network packets.
   a. Can be deployed standalone or on appliance with Decoder
   b. Typical deployment is one-to-one Decoder/ Concentrator pairs; though it is possible for a single Concentrator to aggregate from multiple Decoders.
6. One Event Stream Analysis appliance (and JVM)
   a. Deployed standalone
   b. Receives event data from multiple Concentrators
   c. Also contains a TokuMX High Performance MongoDB distribution

   Note: Deployments could have more than one ESA appliance.
7. One Archiver appliance
   Note: Deployments could have more than one Archiver.
   a. Deployed standalone
   b. Only aggregates capture data from Log Decoder

The deployment described above includes sufficient appliances to demonstrate the TOE security functions even when additional appliances are used in a deployment. The deployment uses each of the TOE components. The interactions between TOE components remain the same when multiple components are installed on a single appliance, albeit without the need for protected communication.

Note: The Malware Analysis component shipped with SA Server has a capacity limit of 100 file scans per day. The Malware Analysis appliance runs the same RSA-developed software but without license limitations on the number of file scans per day. The capability of the Malware Analysis component shipped with the SA Server was tested as part of the evaluation but the standalone Malware Analysis device was not.

Hardware Specifications per Appliance Model:

Series 4S Packet Decoder
Throughput: 2 Gbps
Form Factor: 1U, Full Depth
Processors: Dual Eight Core, 2.6GHz
RAM: 96GB
RAID Controller Card: 6Gb/s
Capacity Drive Count: 2 - 1TB HDD
Available Capacity: N/A

Series 4S Log Decoder
Throughput: up to 60K EPS
Form Factor: 1U, Full Depth
Processors:Dual Eight Core, 2.6GHz
RAM; 96GB
RAID Controller Card: 6Gb/s
Capacity Drive Count: 2 - 1TB HDD
Available Capacity: N/A

Series 4S Concentrator (both packet and Log)
Throughput: N/A
Form Factor: 1U, Full Depth
Processors: Dual Eight Core, 2.6GHz
RAM: 96GB
RAID Controller Card: 6Gb/s

Capacity Drive Count: 2 - 1TB HDD
Available Capacity: N/A

Series 4S Hybrid for Packets (Packet Decoder and Concentrator)
Throughput: 622 Mbps
Form Factor: 1U, Full Depth
Processors: Dual Eight Core, 2.6GHz
RAM: 96GB
RAID Controller Card: 6Gb/s
Capacity Drive Count: 10 - 1TB HDD
Available Capacity: 4.2 TB

Series 4S Hybrid for Logs (Log Collector, Log Decoder, and Concentrator)
Throughput: up to 20K EPS
Form Factor: 1U, Full Depth
Processors: Dual Eight Core, 2.6GHz
RAM: 96GB
RAID Controller Card: 6Gb/s
Capacity Drive Count: 10 - 1TB HDD
Available Capacity: 8 TB

Series 4S All-In-One for Packets
Throughput: 310 Mbps
Form Factor: 1U, Full Depth
Processors: Dual Eight Core, 2.6GHz
RAM: 96GB
RAID Controller Card: 6Gb/s
Capacity Drive Count: 10 - 1TB HDD
Available Capacity: 3.99TB

All In One for Packet includes Packet Decoder, Concentrator, Broker, SA Server, and Malware Analysis (free version)

Series 4S All-In-One for Logs
Throughput: up to 7,500 EPS
Form Factor: 1U, Full Depth
Processors: Dual Eight Core, 2.6GHz
RAM: 96GB
RAID Controller Card: 6Gb/s
Capacity Drive Count: 10 - 1TB HDD
Available Capacity: 2.6TB

All In One for Logs includes Log Decoder, Log Collector, Concentrator, Broker, SA Server, and Malware Analysis (free version)

Series 4S Broker
Throughput: N/A
Form Factor: 1U, Full Depth
Processors: Dual Eight Core, 2.6GHz
RAM: 96GB
RAID Controller Card: 6Gb/s
Capacity Drive Count: 2 - 1TB HDD
Available Capacity: N/A

Series 4S Security Analytics Server w/ Broker
Throughput: N/A

Form Factor: 1U, Full Depth
Processors: Dual Eight Core, 2.6GHz
RAM: 96GB
RAID Controller Card: 6Gb/s
Capacity Drive Count: 2 - 1TB HDD
Available Capacity: N/A

Series 4S Archiver
Throughput: N/A
Form Factor: 1U, Full Depth
Processors: Dual Eight Core, 2.6GHz
RAM: 96GB
RAID Controller Card: 6Gb/s
Capacity Drive Count: 2 - 1TB HDD
Available Capacity: N/A

Series 4S Event Stream Analytics
Throughput: N/A
Form Factor: 1U, Full Depth
Processors: Dual Eight Core, 2.6GHz
RAM: 96GB
RAID Controller Card: 6Gb/s
Capacity Drive Count: 10 - 1TB HDD
Available Capacity:10TB

2.2.2.4.2 Virtual Deployments

The TOE components can also be deployed as virtual appliances in the evaluated configuration. The virtual appliances are the same TOE image and operating system as the physical appliances. Virtual appliances differ from physical appliances in capacity. Hence evaluation on hardware appliances is adequate validation of virtual appliances.

Virtual ESA appliances are not offered. The SA Server, Incident Management, Reporting Engine and the collocated version of Malware Analysis services are to be hosted as one virtual appliance in the virtual environment. Broker is not included in this virtual appliance and must be deployed as a separate virtual appliance. The hardware requirements for the virtual machine are cumulative for these components.

The following table lists CPU, Memory, and OS Disk partition minimum requirements for the virtual appliances.

- The disk requirements are fixed sizes for the OVA packages.
- RAM and CPU metrics are minimums and are also dependent on the capture and ingest environment.

Virtual Appliance Type	Quantity of CPUs	CPU Specifications	RAM	Disk
Packet Decoder	4	Intel Xeon CPU @2.93 Ghz	16 GB	320 GB
Log Decoder	4	Intel Xeon CPU @2.93 Ghz	16 GB	320 GB
Concentrator	4	Intel Xeon CPU @2.93 Ghz	16 GB	320 GB
Archiver	4	Intel Xeon CPU @2.93 Ghz	16 GB	320GB
Broker	4	Intel Xeon CPU @2.93 Ghz	16 GB	320 GB
Security Analytics Server	4	Intel Xeon CPU @2.93 Ghz	16 GB	320 GB

The TOE relies on each hosting OS to protect its applications, processes, and any locally stored data. The TOE also relies on the hosting OS for reliable time to use with the audit, IDS data.

2.2.3 TOE Logical Boundaries

This section identifies the security functions that RSA Security Analytics v10.6 provides. The logical boundaries of the TOE include the security functions of the TOE interfaces. The TOE logically supports the following security functions:

- Security Audit
- Cryptographic Support
- Identification & Authentication
- Security Monitoring with Security Information and Event Management (SIEM)
- Security Management
- Protection of the TSF
- TOE Access
- Trusted path/channels

2.2.3.1 Security Audit

The TOE generates audit records of security relevant events that include at least date and time of the event, subject identity and outcome for security events. The TOE provides the default Administrator and Operator roles with the ability to read the audit events. The environment stores the audit records and also provides the system clock information that is used by the TOE to timestamp each audit record.

2.2.3.2 Cryptographic Support

The Transport Layer Security (TLS 1.2) protocol in FIPS mode is used to provide protection of the communications surrounding the remote administrative sessions from disclosure and from modification. TLS is also used for distributed internal TOE component communications. The TOE uses a FIPS-validated module for SSH protected communication pathways for the transfer of file event source data from log data sources to the TOE.

The TOE uses OpenSSL object module Red Hat Enterprise Linux 6.2 with RPM version file of 1.0.0-20.el6 (FIPS 140-2 validation certificate #1758) for both SSH and TLS communications.

The TOE uses the RSA BSAFE Crypto-J cryptographic library: BSAFE SSL-J 6.1.3.1 for Java applications, which incorporates BSAFE Crypto-J 6.1.2. The latter is certified under FIPS 140-2 Certificate #XXXX, which also falls under Consolidated Validation Certificate #XXXX.

2.2.3.3 Identification & Authentication

The TOE allows the users to acknowledge end-user license agreements and view warning banners prior to providing identification and authentication data. No other access to the TOE is permitted until the user is successfully authenticated. The TOE maintains the following security attributes belonging to individual human users: username, password and role.

The TOE provides authentication failure handling that allows administrators to configure the number of times a user may attempt to login and the time that the user will be locked out if the number of the configured number of attempts has been surpassed. The TOE detects when the defined number of unsuccessful authentication attempts has been met, and enforces the described behavior (locks the user account for a specified time period).

2.2.3.4 Security Monitoring with Security Information and Event Management (SIEM)

The TOE receives network packets, reconstructs network transactions, extracts metadata, and applies rules. The rules identify interesting events, effectively matching signatures. Likewise, the TOE receives log data, parses the data, extracts metadata, correlates events, and applies rules. Through signature analysis, the TOE can identify potential misuse or intrusions and send an alarm to incident management SA views. The incident management SA views provide the analytical results to authorized users in a manner suitable for the user to interpret the information. The analytical

results are recorded with information such as date and time. Only users with the Analysis and Administrator roles can read the metadata, raw logs, raw packet data, and incident management data from the IDS data.

2.2.3.5 Security Management

Authorized administrators manage the security functions and TSF data of the TOE via the web-based User Interface. The ST defines and maintains the administrative roles: Administrator, Analyst, and Operator. Authorized administrators perform all security functions of the TOE including starting and stopping the services and audit function, creating and managing user accounts, manage authentication failure handling and session inactivity values and read the audit and analyzer data.

2.2.3.6 Protection of the TSF

The TOE provides protection mechanisms for its security functions. One of the protection mechanisms is that users must authenticate and have the appropriate permissions before any administrative operations or access to TOE data and resources can be performed on the TSF. The TOE is a collection of special-purpose appliances. Each appliance provides only functions for the necessary operation of the TOE, and limits user access to authorized users with an administrative role.

Communication with remote administrators is protected by TLS in FIPS mode, protecting against the disclosure and undetected modification of data exchanged between the TOE and the administrator. The TOE runs in a FIPS compliant mode of operation and uses FIPS-validated cryptographic modules.

2.2.3.7 TOE Access

The TOE terminates interactive sessions after administrative configured period of time. The TOE also allows user-initiated termination of the user's own interactive session by closing the browser or explicitly logging off.

Before establishing a user session, the TOE displays an advisory warning message regarding unauthorized use of the TOE.

2.2.3.8 Trusted path/channels

The TOE requires remote users to initiate a trusted communication path using TLS for initial user authentication. The TOE also requires that the trusted path be used for the transmission of all SA interface session data. The use of the trusted path provides assured identification of end points and protection of the communicated data from modification, and disclosure. The TOE uses a FIPS-validated module for SSH protected communication pathways for the transfer of file event source data from log data sources to the TOE. TLS and SSH ensure the administrative session and file transfer communication pathways are secured from disclosure and modification.

2.3 TOE Documentation

RSA has a number of administration and configuration guides for SA which include the following:

- *System Security and User Management:* https://sadocs.emc.com/0_en-us/088_SA106/200_SecUsrMgt
- *Licensing Guide:* https://sadocs.emc.com/0_en-us/088_SA106/140_Lic
- *Host and Services Configuration Guides:* https://sadocs.emc.com/0_en-us/088_SA106/120_AppSerCon
- *Archiver Configuration Guide:* http://sadocs.emc.com/0_en-us/088_SA106/120_AppSerCon/ArcCon
- *Broker and Concentrator Configuration Guide:* http://sadocs.emc.com/0_en-us/088_SA106/120_AppSerCon/BrCnCon
- *Decoder/Log Decoder Configuration Guide: Broker and Concentrator Configuration Guide:* http://sadocs.emc.com/0_en-us/088_SA106/120_AppSerCon/DeLdCon
- *Event Stream Analysis (ESA) Configuration Guide:* http://sadocs.emc.com/0_en-us/088_SA106/120_AppSerCon/ESACon
- *List of Core ESA Rules or Alerts:* https://sadocs.emc.com/0_en-us/300_RSA_ContentAndResources/RSA_Content/RSA_Event_Stream_Analysis_Rules/01_List_of_Core_ESA_Rules_and_Alerts.

- *Malware Analysis Configuration Guide:* http://sadocs.emc.com/0_en-us/088_SA106/120_AppSerCon/MaCon
- *Incident Management Configuration Guide:* http://sadocs.emc.com/0_en-us/088_SA106/120_AppSerCon/IncManCon
- *Reporting Engine Configuration Guide:* http://sadocs.emc.com/0_en-us/088_SA106/120_AppSerCon/ReCon
- *Virtual Appliance Setup Guide:* https://sadocs.emc.com/0_en-us/088_SA106/110_VaSetup
- *Log Collection Getting Started Guide:* https://sadocs.emc.com/0_en-us/088_SA106/135_LCGds/00_LCGS
- *Log Collection Deployment Guide:* https://sadocs.emc.com/0_en-us/088_SA106/135_LCGds/10LCDG
- *Log Collection Configuration Guide:* https://sadocs.emc.com/0_en-us/088_SA106/135_LCGds/20_LCCG
- *Reporting Engine Configuration Guide:* http://sadocs.emc.com/0_en-us/088_SA106/120_AppSerCon/ReCon
- *Incident Management Configuration Guide* : http://sadocs.emc.com/0_en-us/088_SA106/120_AppSerCon/IncManCon
- *System Preferences:* https://sadocs.emc.com/0_en-us/088_SA106/210_SysPref
- *System Security and User Management:* https://sadocs.emc.com/0_en-us/088_SA106/200_SecUsrMgt

3 Security Problem Definition

The TOE security environment describes the security aspects of the intended environment in which the TOE is to be used and the manner in which it is expected to be employed. The statement of the TOE security environment defines the following:

- Threats that the TOE and the environment of the TOE counter
- Assumptions made about the operational environment and the intended method of use for the TOE

The statement of TOE security environment does not include any Organizational Policies.

The TOE is intended to be used in environments where the relative assurance that its security functions are enforced is commensurate with EAL 2 augmented with ALC_FLR.1 as defined in the CC.

3.1 Assumptions

The following conditions are assumed to exist in the operational environment.

3.1.1 Intended Usage Assumptions

A.AUDIT_PROTECTION	The operational environment will provide the capability to protect audit information.
A.DATA_SOURCES	The data sources in the environment provide complete and reliable data to the TOE.
A.TIME	The environment will provide reliable time sources for use by the TOE.

3.1.2 Physical Assumptions

A.DEPLOY	TOE Administrators will properly configure the network in the TOE operational environment and configure adequate network capacity for the deployed TOE components.
A.PHYSICAL	The TOE hardware and software critical to the security policy enforcement will be located within controlled access facilities which will prevent unauthorized physical access.

3.1.3 Personnel Assumptions

A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.TRUSTED_ADMIN	TOE Administrators will follow and apply all administrator guidance in a trusted manner.
A.USER	Users will protect their authentication data.

3.2 Threats

T.MALICIOUS_ACTIVITY	Malicious activity by an attacker may occur on the network the TOE monitors may go undetected.
T.INADVERTENT_ACTIVITY	Inadvertent activity and access by a user or a process that may occur on the network the TOE monitors may go undetected.
T.MISUSE	Unauthorized accesses and activity indicative of misuse by a user or a process that may occur on the network the TOE monitors may go undetected.
T.TSF_COMPROMISE	A user may cause, through an unsophisticated attack, TSF data, or security functions to be inappropriately accessed (viewed, modified, or deleted).
T.UNAUTHORIZED_ACCESS	An unauthorized user may gain access to the TOE Security functions and data.

T.UNACCOUNTABLE_USERS	Authorized users of the TOE might not be held accountable for their actions.

4 Security Objectives

This chapter identifies the security objectives of the TOE and its environment. Security objectives identify the responsibilities of the TOE and the support need by the TOE from its environment.

4.1 Security Objectives for the TOE

O.ANALYZE	The TOE will apply analytical processes and information to derive conclusions about potential unauthorized/malicious intrusions and send appropriate alerts.
O.AUDIT_GENERATION:	The TOE will provide the capability to detect and create records of security relevant events associated with users.
O.AUDIT_PROTECTION:	The TOE will provide the capability for protection of the audit information from unauthorized users via the TOE interfaces.
O.MANAGE:	The TOE will provide all the functions necessary to support the authorized administrators in their management of the security of the TOE, and restrict these functions from unauthorized use.
O.TOE_ACCESS	The TOE will provide mechanisms that control a user's logical access to the TOE.
O.PROTECTED_COMMS	The TOE will provide protected communication channels for remote administrators, IT entities and for TOE device to TOE device communications.

4.2 Security Objectives for the Operational Environment

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

OE.AUDIT_PROTECTION	The operational environment provides the capability to protect audit information.
OE.DATA_SOURCES	The data sources in the environment provide complete and reliable data to the TOE.
OE.DEPLOY	The TOE Administrators will properly configure the network in the TOE operational environment and configure adequate network capacity for the deployed TOE components
OE.MANAGE	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the TSF.
OE.PHYSICAL	The TOE hardware and software critical to the security policy enforcement will be located within controlled access facilities which will prevent unauthorized physical access.
OE.TIME	The environment provides reliable time sources for use by the TOE.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
OE.USER	Users must ensure that their authentication data is held securely and not disclosed to unauthorized persons.

5 IT Security Requirements

The security requirements for the TOE have been drawn from Parts 2 and 3 of the Common Criteria. The security functional requirements have been selected to correspond to the actual security functions implemented by the TOE while the assurance requirements have been selected to offer a low to moderate degree of assurance that those security functions are properly realized.

5.1 Extended Component Definition

This Security Target includes Security Functional Requirements (SFRs) that are not drawn from CC Part 2. These Extended SFRs are identified by having a label '_EXT' in the requirement name for TOE SFRs. The structure of the extended SFRs is modeled after the SFRs included in CC Part 2. The structure is as follows:

A. Class – The extended SFRs included in this ST are part of the identified classes of requirements.

B. Family – The extended SFRs included in this ST are part of several SFR families including the new families defined below.

C. Component – The extended SFRs are not hierarchical to any other components, though they may have identifiers terminating on other than "1". The dependencies for each extended component are identified in the TOE SFR Dependencies section of this ST (Section 7.3, Requirement Dependency Rationale).

5.1.1 Extended Family Definitions

5.1.1.1 **Transport Layer Security Components**

Class FCS: Cryptographic support

Family: Transport Layer Security (FCS_TLS)

Family Behavior

This family identifies the behavior of the TOE when the Transport Layer Transport Layer Security (TLS) protocol is implemented. The TOE must implement one or more of the identified protocols and ciphersuites.

The FCS_TLC family contains one component.

Management:

There are no management activities foreseen.

Audit:

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

Basic:

- Failure to establish an TLS Session
- Establishment/Termination of an TLS session

5.1.1.1.1 Definition

FCS_TLS_EXT.1 – Transport Layer Security Protocol

Hierarchical to: No other components.

Dependencies: None

FCS_TLS_EXT.1.1 The TSF shall implement the following protocols [selection: TLS 1.0, TLS 1.1, TLS 1.2)] supporting the following ciphersuites:

[selection:
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA

TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_ SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

].

5.1.1.1.2 Extended Requirements Rationale:

FCS_TLS_EXT.1 is modeled closely on the standard component FCS_CKM.1: Cryptographic key generation. FCS_TLS_EXT.1 needed to be defined as an extended family/component because the Transport Layer Security functionality does not exist in the CC part 2.

5.1.1.2 **SSH Protocol Components**

Class FCS: Cryptographic support

Family: SSH Protocol (FCS_SSH)

Family Behavior

This family identifies the behavior of the TOE when the SSH protocol is implemented. The TOE must implement one or more of the identified protocols and ciphersuites.

The FCS_SSH family contains six components.

Management:

There are no management activities foreseen.

Audit:

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

Basic:

- Failure to establish an SSH Session
- Establishment/Termination of an SSH session

5.1.1.2.1 Definition

FCS_SSH_EXT.1 – SSH Protocol

Hierarchical to: No other components.

Dependencies: None

FCS_SSH_EXT.1.1 The TSF shall implement the SSH protocol.

FCS_SSH_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following authentication method as described in RFC 4252: [**selection:** password, public key-based].

FCS_SSH_EXT.1.3 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms: AES-CBC-256, [**selection:** AES-CBC-128, AES-CBC-192, AES-CTR-128, AES-CTR-192, AES-CTR-256, 3DES-CBC, no other algorithms].

FCS_SSH_EXT.1.4 The TSF shall ensure that the SSH transport implementation uses [**selection:** SSH_RSA, SSH_DSS] and [**selection:** PGP-SIGN-RSA, PGP-SIGN-DSS, ecdsa-sha2-nistp384, no other public key algorithms,] as its public key algorithm(s).

FCS_SSH_EXT.1.5 The TSF shall ensure that data integrity algorithms used in SSH transport connection is [**selection**: hmac-sha1, hmac-sha1-96, hmac-sha2-256, hmac-sha2-512].

FCS_SSH_EXT.1.6 The TSF shall ensure that diffie-hellman-group14-sha1 is the only allowed key exchange method used for the SSH protocol.

5.1.1.2.2 Extended Requirements Rationale:

FCS_SSH_EXT.1 is modeled closely on the standard component FCS_CKM.1 Cryptographic key generation. FCS_SSH_EXT.1 needed to be defined as an extended family/component because the SSH Protocol functionality does not exist in the CC part 2

5.1.1.3 **Intrusion Detection System**

Class IDS: Intrusion Detection System

This class is defined specifically for the security functionality provided by the Security Analytics TOE that is not defined in CC Part 2. This class of requirements covers the security functions provided by the TOE regarding the analyzing and reporting (alerts) of the information from targeted IT System resource(s) (the IT network monitored by the TOE). This functionality is typical of an Intrusion Detection System (IDS).

The IDS Class, Families and Components are modeled on the FAU Class, Families and Components defined CC Part 2.

5.1.1.4 **Analyzer**

Family: Intrusion Detection System Analyzer analysis (IDS_ANL)

Family Behavior

This family defines the Security Analytics functionality to perform analysis on all log and network traffic in the monitored network (IDS traffic). The TOE must also derive conclusions about potential intrusions and record the result of the analysis.

The IDS_ANL family contains one component.

Management:

There are no management activities foreseen.

Audit:

There are no auditable events foreseen.

5.1.1.4.1 Definition

IDS_ANL_EXT.1 – Analyzer

Hierarchical to: No other components.

Dependencies: none

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

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

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

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

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

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

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

5.1.1.4.2 Extended Requirements Rationale:

IDS_ANL_EXT.1 is modeled closely on the standard components from CC part 2 and needed to be defined as an extended component because there is no requirement in the CC part 2 to cover this functionality of the TOE.

5.1.1.5 **Analyzer React**

Family: Intrusion Detection System Analyzer react (IDS_RCT)

Family Behavior

This family defines the Security Analytics functionality to send an alarm and perform other actions when analysis of the network traffic in the monitored network (performed in IDS_ANL) indicates there have been potential intrusions.

The IDS_RCT family contains one component.

Management:

There are no management activities foreseen.

Audit:

There are no auditable events foreseen.

5.1.1.5.1 Definition

IDS_RCT_EXT.1 – Analyzer React

Hierarchical to: No other components.

Dependencies: IDS_ANL_EXT.1

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

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

5.1.1.5.2 Extended Requirements Rationale:

IDS_RCT_EXT.1 is modeled closely on the standard components from CC part 2 and needed to be defined as an extended component because there is no requirement in the CC part 2 to cover this functionality of the TOE.

5.1.1.6 **Restricted Data Review**

Family: Intrusion Detection System Restricted Data Review (IDS_RDR)

Family Behavior

This family defines the Security Analytics functionality for data analyzing tools that must be available to authorized users to assist in the review of data collected from the monitoring network. This family indicates that the TOE must provide authorized users the capability to obtain, review and interpret the information.

This family consists of two components.

Management:

There are no management activities foreseen.

Audit:

There are no auditable events foreseen.

5.1.1.6.1 Definition

IDS_RDR_EXT.1 – Restricted Data Review

Hierarchical to: No other components.

Dependencies: IDS_ANL_EXT.1

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

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

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

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

5.1.1.6.2 Extended Requirements Rationale:

IDS_RDR_EXT.1 is modeled closely on the standard components from CC part 2 and needed to be defined as an extended component because there is no requirement in the CC part 2 to cover this functionality of the TOE

5.2 TOE Security Functional Requirements

The following table describes the SFRs that are candidates to be satisfied by RSA Security Analytics.

Requirement Class	Requirement Component
FAU: Security Audit	FAU_GEN.1: Audit data generation
	FAU_GEN.2: User identity association
	FAU_SAR.1: Audit review
	FAU_SAR.2: Restricted audit review
	FAU_STG.1: Protected audit trail storage
FCS: Cryptographic support	FCS_SSH_EXT.1: SSH Protocol
	FCS_TLS_EXT.1: Transport Layer Security Protocol
FIA: Identification and authentication	FIA_AFL.1: Authentication failure handling (Human user)
	FIA_ATD.1: User attribute definition
	FIA_UAU.1: Timing of authentication
	FIA_UAU.5: Multiple authentication mechanisms
	FIA_UID.1: Timing of identification
Security Monitoring with Security Information and Event Management (SIEM)	IDS_ANL_EXT.1: Analyser analysis
	IDS_RCT_EXT.1: Analyser react
	IDS_RDR_EXT.1: Restricted Data Review
FMT: Security management	FMT_MOF.1: Management of security functions behaviour
	FMT_MTD.1: Management of TSF data
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security roles
FPT: Protection of the TSF	FPT_ITT.1: Basic internal TSF data transfer protection
TOE Access	FTA_SSL.3: TSF-initiated Termination

	FTA_SSL.4: User-initiated Termination
	FTA_TAB.1: Default TOE access banners
FTP: Trusted path/channels	FTP_TRP.1: Trusted Path

Table 5-1 TOE Security Functional Components

5.2.1 Security audit (FAU)

5.2.1.1 Audit data generation (FAU_GEN.1)

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;
b) All auditable events for the [***not specified***] level of audit; and [
c) **The specifically defined auditable events listed in Table 5-2 Auditable Events**].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, 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, [**information specified in column three of Table 5-2 Auditable Events**].

Table 5-2 Auditable Events

Security Functional Requirement	RSA Identified Auditable Event	Additional Audit Record Contents
FIA_AFL.1	Each failed authentication attempt is audited	No additional information
FIA_UAU.1	Failed login	No additional information
FIA_UAU.5	An SFTP connection will generate logs for both failed and successful connections.	No additional information
FIA_UID.1	Failed login	No additional information
FMT_SMF.1	Create, modify, delete users	Module or Service where audit record originated Connection information (IP address)
FMT_SMF.1	Configuration of the banner	No additional information
FMT_SMF.1	Create, modify LockBox password	Module or Service where audit record originated
FMT_SMR.1	Creating/updating/enabling/disabling users; Creating/updating roles	No additional information
FTA_SSL.4	User logouts are audited, which terminates session	No additional information

Security Functional Requirement	RSA Identified Auditable Event	Additional Audit Record Contents
FTP_TRP.1	Initiation of trusted channel (Successful logins) FCS_TLS_EXT.1 or FIA_UAU.1 audit events serve here since TLS and authentication are the trusted path mechanisms.	No additional information
	Termination of trusted channel (User logouts) FTA_SSL.4 audit events serve here since TLS and authentication are the trusted path mechanisms.	No additional information
	Failures of the trusted path functions (Failed logins) FCS_TLS_EXT.1 or FIA_UAU.1 audit events serve here since TLS and authentication are the trusted path mechanisms.	No additional information

5.2.1.2 User identity association (FAU_GEN.2)

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.2.1.3 Audit review (FAU_SAR.1)

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

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

5.2.1.4 Restricted audit review (FAU_SAR.2)

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

5.2.1.5 Protected audit trail storage (FAU_STG.1)

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

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

5.2.2 Cryptographic Support (FCS)

5.2.2.1 SSH Protocol (FCS_SSH_EXT.1)

FCS_SSH_EXT.1.1 The TSF shall implement the SSH protocol.

FCS_SSH_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following authentication method as described in RFC 4252: [***public key-based***].

FCS_SSH_EXT.1.3 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms: AES-CBC-256, [***AES-CBC-128, AES-CBC-192, AES-CTR-128, AES-CTR-192, AES-CTR-256, 3DES-CBC***].

FCS_SSH_EXT.1.4 The TSF shall ensure that the SSH transport implementation uses [***SSH_RSA, SSH_DSS***] and [***no other public key algorithms***] as its public key algorithm(s).

FCS_SSH_EXT.1.5 The TSF shall ensure that data integrity algorithms used in SSH transport connection is [***hmac-sha1, hmac-sha1-96***].

FCS_SSH_EXT.1.6 The TSF shall ensure that diffie-hellman-group14-sha1 is the only allowed key exchange method used for the SSH protocol

5.2.2.2 Transport Layer Security Protocol (FCS_TLS_EXT.1)

FCS_TLS_EXT.1.1 The TSF shall implement the following protocols [***TLS 1.2***] supporting the following ciphersuites: [

TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA].

5.2.3 Identification and authentication (FIA)

5.2.3.1 Authentication failure handling (Human user) (FIA_AFL.1)

FIA_AFL.1.1 The TSF shall detect when [***[an administrator configurable positive integer within [0 and no maximum value]]***] unsuccessful authentication attempts occur related to [**SA UI user authentication**].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [***surpassed***], the TSF shall [**lock account for a specified time period as configured by authorized administrator**].

5.2.3.2 User attribute definition (FIA_ATD.1)

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [

- **Username;**
- **password; and**
- **role**].

5.2.3.3 Timing of authentication (FIA_UAU.1)

FIA_UAU.1.1 The TSF shall allow [**acknowledge end-user license agreement and view warning banner**] on behalf of the user to be performed before the user is authenticated.

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

5.2.3.4 Multiple authentication mechanisms (FIA_UAU.5)

FIA_UAU.5.1 The TSF shall provide [SSH public-key, and password-based authentication mechanisms] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [TOE users authenticate using password-based and authorized IT entities authenticate using SSH public-key authentication mechanisms].

5.2.3.5 Timing of identification (FIA_UID.1)

FIA_UID.1.1 The TSF shall allow [**acknowledge end-user license agreement and view warning banner**] on behalf of the user to be performed before the user is identified.

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

5.2.4 Security Monitoring with Security Information and Event Management

5.2.4.1 Analyzer analysis (IDS_ANL_EXT.1)

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

IDS_ANL_EXT.1.2 The TSF shall record within each analytical result at least the following information: a. Date and time of the result, type of result, identification of data source; and b. [**no additional information**]. _

5.2.4.2 Analyzer react (IDS_RCT_EXT.1)

IDS_RCT_EXT.1.1 The TSF shall send an alarm to [**incident management SA views**] and take [**no other action**] when an intrusion is detected.

5.2.4.3 Restricted data review (IDS_RDR_EXT.1)

IDS_RDR_EXT.1.1 The TSF shall provide [**Analyst and Administrator role**] with the capability to read [**all metadata, raw logs, raw packet data, and Incident Management data**] from the IDS data.

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

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

5.2.5 Security management (FMT)

5.2.5.1 Management of security functions behaviour (FMT_MOF.1)

FMT_MOF.1.1 The TSF shall restrict the ability to [**disable, enable**] the functions [**audit function**, **start/stop services (decoder, concentrator, broker, ESA, Archiver, Incident Management, Malware Analysis, and Reporting Engine)**] to [**Administrator, Operator**].

5.2.5.2 Management of TSF data (FMT_MTD.1)

FMT_MTD.1.1 The TSF shall restrict the ability to [***query, [manage]***] the [**TSF data**] to [**authorized identified roles in Table 5-3 Management of TSF Data**].

Table 5-3: Management of TSF Data

TSF data	Operation(s)	Role
Login failure limit	Change	Administrator
Lockout period	Change	Administrator
Session inactivity period	Change	Administrator
User accounts	Create, modify, delete	Administrator
Security audit	Read (query)	Operators, Administrator
Analyzer data	Read (query)	Analysts, SOC_Manager
Malware Analysis data	Read (query)	Malware Analyst
Text (system settings)	Enable/disable, customize	Administrator
Devices	Add. Remove	Administrator

Log Decoder event sources connections	Add, update, delete	Administrator and Operator
Signatures	Add, modify, remove	Administrator and Operator
LockBox password for Log Collectors	Create, modify	Administrator and Operator

5.2.5.3 Specification of Management Functions (FMT_SMF.1)

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

- **Manage TSF functions as specified in FMT_MOF.1**
- **Manage TSF data as specified in FMT_MTD.1**
- **Manage security audit as specified in FMT_MTD.1, FAU_STG.1**

].

5.2.5.4 Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles: [

- **Administrator**
- **Analyst**
- **Operator**
- **SOC_Manager**
- **Malware Analyst**].

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

5.2.6 Protection of the TSF (FPT)

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

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

5.2.7 TOE Access (FTA)

5.2.7.1 TSF-initiated termination (FTA_SSL.3)

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

5.2.7.2 TSF-initiated termination (FTA_SSL.4)

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

5.2.7.3 Default TOE access banners (FTA_TAB.1)

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

5.2.8 Trusted path/channels (FTP)

5.2.8.1 Trusted Path (FTP_TRP.1)

FTP_TRP.1.1 The TSF shall provide a communication path between itself and **[*remote administrative, authorized IT entities*]** users that is logically distinct from other communication paths and

provides assured identification of its end points and protection of the communicated data from **[*modification and disclosure*].**

FTP_TRP.1.2 The TSF shall permit [***remote users, authorized IT entities***] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [***initial user authentication [all SA interface session data, transfer of file event source data]***].

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL 2 augmented with ALC_FLR.1 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

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

Table 5-3 EAL2 Augmented with ALC_FLR.1 Assurance Components

5.3.1 Development (ADV)

5.3.1.1 Security architecture description (ADV_ARC.1)

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

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

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

ADV_ARC.1.1c The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2c The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3c The security architecture description shall describe how the TSF initialization process is secure.

ADV_ARC.1.4c The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5c The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

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

5.3.1.2 Security-enforcing functional specification (ADV_FSP.2)

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

5.3.1.3 Basic design (ADV_TDS.1)

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

5.3.2 Guidance documents (AGD)

5.3.2.1 Operational user guidance (AGD_OPE.1)

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

AGD_OPE.1.7c The operational user guidance shall be clear and reasonable.

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

5.3.2.2 Preparative procedures (AGD_PRE.1)

AGD_PRE.1.1d The developer shall provide the TOE including its preparative procedures.

AGD_PRE.1.1c The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2c The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

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

AGD_PRE.1.2e The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.3.3 Life-cycle support (ALC)

5.3.3.1 Use of a CM system (ALC_CMC.2)

ALC_CMC.2.1d The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.2.2d The developer shall provide the CM documentation.

ALC_CMC.2.3d The developer shall use a CM system.

ALC_CMC.2.1c The TOE shall be labelled with its unique reference.

ALC_CMC.2.2c The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.2.3c The CM system shall uniquely identify all configuration items.

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

5.3.3.2 Parts of the TOE CM coverage (ALC_CMS.2)

ALC_CMS.2.1d The developer shall provide a configuration list for the TOE.

ALC_CMS.2.1c The configuration list shall include the following: The TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE.

ALC_CMS.2.2c The configuration list shall uniquely identify the configuration items.

ALC_CMS.2.3c For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

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

5.3.3.3 Delivery procedures (ALC_DEL.1)

ALC_DEL.1.1d The developer shall document and provide procedures for delivery of the TOE or parts of it to the consumer.

ALC_DEL.1.2d The developer shall use the delivery procedures.

ALC_DEL.1.1c The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

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

5.3.3.4 Systematic flaw remediation (ALC_FLR.1)

ALC_FLR.1.1d The developer shall document and provide flaw remediation procedures addressed to TOE developers.

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.

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.

ALC_FLR.1.3c The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

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.

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

5.3.4 Tests (ATE)

5.3.4.1 **Evidence of coverage (ATE_COV.1)**

ATE_COV.1.1d The developer shall provide evidence of the test coverage.

ATE_COV.1.1c The evidence of the test coverage shall show the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

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

5.3.4.2 **Functional testing (ATE_FUN.1)**

ATE_FUN.1.1d The developer shall test the TSF and document the results.

ATE_FUN.1.2d The developer shall provide test documentation.

ATE_FUN.1.1c The test documentation shall consist of test plans, expected test results and actual test results.

ATE_FUN.1.2c The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3c The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4c The actual test results shall be consistent with the expected test results.

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

5.3.4.3 **Independent testing — sample (ATE_IND.2)**

ATE_IND.**2.1d** The developer shall provide the TOE for testing.

ATE_IND.2.1c The TOE shall be suitable for testing.

ATE_IND.2.2c The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

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

ATE_IND.2.2e The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

ATE_IND.2.3e The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.3.5 Vulnerability assessment (AVA)

5.3.5.1 **Vulnerability analysis (AVA_VAN.2)**

AVA_VAN.2.1d The developer shall provide the TOE for testing.

AVA_VAN.2.1c The TOE shall be suitable for testing.

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

AVA_VAN.2.2e The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.2.3e The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE.

AVA_VAN.2.4e The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

6 TOE Summary Specification

This chapter describes the following security functions:

- Security audit
- Cryptographic support
- Identification and authentication
- Security Monitoring with Security Information and Event Management (SIEM)
- Security management
- Protection of the TSF
- TOE Access
- Trusted path/channels

6.1 Security audit

The TOE generates audit records for the following auditable events:

- Start-up and shutdown of the audit function,
- Start-up and shutdown of the TOE,
- All auditable events as specified in Table 5-2 Auditable Events in Section 5.2.1.1..

Each audit record includes the date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event.

The operating system in the environment provides protection, and storage of the audit records. The operating system also provides the system clock information that is used by the TOE to timestamp each audit record. The audit records are stored on the local file system of the host appliance. The TOE is a multi-host distributed architecture, where the TOE subsystems run on a number of hosts. The audit records are stored on the local file system of the host on which the related auditable event is detected. Consequently, the aggregate audit record for an entire TOE system is distributed across multiple services, rather than being stored in a single location.

The TOE provides a web-based SA Server UI, through which an authorized user with the Operator or Administrator role has the ability to read all audit information from the audit records on each appliance. Additionally, the TOE does not provide any interfaces to delete or modify audit records.

The TOE relies upon the environment to provide typical operating system file services including protected data storage. The TOE relies upon the operating system in the operational environment to provide the file system which allows the TOE to store information securely. The TOE relies upon the environment to prevent unauthorized modification or deletion of the audit files.

The TOE does not provide the ability to start and stop the audit mechanism independently from the starting and stopping of the services. The audit mechanism is started and stopped when the service is started and stopped. The TOE generates an audit event when each service is started and stopped.

The Security audit function is designed to satisfy the following security functional requirements:

- FAU_GEN.1: Audit records are generated for security relevant events and include the date and time of the event, type of event, subject identity, outcome of the event, and other data identified above.
- FAU_GEN.2: The TOE associates each auditable event resulting from actions of identified users with the identity of the user that caused the event.
- FAU_SAR.1: The TOE provides users with the Operator and Administrator roles with the capability to read all audit information from the audit records. The TSF provides the audit records in a manner suitable for the user to interpret the information.
- FAU_SAR.2: The TOE prohibits all users read access to the audit records, except those users that have been granted explicit read-access.

- FAU_STG.1: The TOE does not provide the capability to delete or modify audit records. Hence, the TOE protects the stored audit records in the audit trail from unauthorised deletion. The TOE is able to prevent unauthorised modifications to the stored audit records in the audit trail.

6.2 Cryptographic support

The TOE uses cryptography to support the protection of the following types of communication pathways:

- Administrative login and management sessions, and
- TOE appliance to TOE appliance and
- File event source to Log Collector.

A remote administrative management session is initiated by a login and occurs only over HTTPS using TLS (TLS version 1.2 in FIPS mode). The TOE performs TLS cryptographic operations in a FIPS-compliant mode of operation using FIPS-validated cryptographic module. TOE to TOE communication occurs for the purpose of TOE device/appliance communication with one another. Each instance of the TOE ensures that such communication occurs only over a TLS in FIPS mode protected communication pathway.

The TOE uses the RSA BSAFE Crypto-J cryptographic library: BSAFE SSL-J 6.1.3.1 for Java applications, which incorporates BSAFE Crypto-J 6.1.2. The latter is certified under FIPS 140-2 Certificate #2058, which also falls under Consolidated Validation Certificate #0036. The Lockbox uses the Common Security Toolkit, version 3.1. RSA BSAFE Micro Edition Suite version 4.0.1 uses RSA BSAFE Crypto-C ME 4.0.1, and is covered by Certificates #2056 and 2097.[4] The lockbox uses TLS_RSA_WITH_AES_256_CBC_SHA and TLS_RSA_WITH_AES_256_CBC_SHA256.

The TOE uses a FIPS-validated module for SSH protected communication pathways for the transfer of file event source data from log data sources to the TOE. The TOE implements the SSH protocol and supports public key-based authentication as described in RFC 4252. The TSF uses the following encryption algorithms: AES-CBC-256, AES-CBC-128, AES-CBC-192, AES-CTR-128, AES-CTR-192, AES-CTR-256, 3DES-CBC for SSH transport. The SSH transport implementation uses SSH_RSA, SSH_DSS public key algorithms; and hmac-sha1 and hmac-sha1-96 data integrity algorithms for the SSH transport connection. Diffie-hellman-group14-sha1 is the key exchange method used for the SSH protocol.

The TOE uses OpenSSL object module Red Hat Enterprise Linux 6.2 with RPM version file of 1.0.0-20.el6 module which has undergone a FIPS 140-2 certification (certificate #1758) for both SSH and TLS. The TOE operates in FIPS mode in the evaluated configuration. The FIPS cryptographic functionality must be enabled to place the product into FIPS-compliant mode with strong cipher suite.

The TOE implements TLS version 1.2 as specified by RFC 5246 using the following ciphersuites.

- TLS_RSA_WITH_AES_128_CBC_SHA (used only by Archiver, Concentrator (packet and log), Decoder (packet and log (with collector)))
- TLS_RSA_WITH_AES_256_CBC_SHA (used by all TOE components: SA Server, ESA, Report Engine, Malware Analysis, Archiver, Incident Management, Concentrator (packet and log), Decoder (packet and log)
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA (used only by Archiver, Concentrator (packet and log), Decoder (packet and log(with collector)))
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA (used only by Archiver, Concentrator (packet and log), Decoder (packet and log (with collector)))

The Cryptographic support function is designed to satisfy the following security functional requirements:

- FCS_SSH_EXT.1.1: The TOE implements the SSH protocol according to RFC 4252 for public key-based and using the algorithms and key exchange method as described in the text above.

[4] Lockbox protects the passwords required for some Log Sources by encryption (using a FIPS-validated cryptographic module). This protection does not contribute to satisfying any TOE security functional requirements.

- FCS_TLS_EXT.1: The TOE implements TLS Version 1.2 protocol which is used as described in the text above. The TOE implementation of TLS provides the ciphersuites listed above.

6.3 Identification and authentication

The TOE maintains user accounts for the authorized users of the TOE and a list of security attributes for each user which includes the username, role membership, and password. The TOE maintains the security relevant roles of Administrator, Operator, and Analyst.

The TOE requires users to provide unique identification and passwords before any access to the TOE is granted other than acknowledging the end-user license agreement and viewing the warning banner. The TOE authenticates claimed identities for TOE users using password-based mechanisms and for authorized IT entities using SSH public-key authentication mechanisms. IT entities are log collection sources that have been configured to send logs to the TOE. SSH public-key authentication is used when log sources send file event sources (SFTP).

The TOE maintains role and user attributes on each device. The TOE associates attributes with a user through SA Server login and SA trusted connections. The SA server login authenticates the identity of a human user and SA trusted management connections initiated by administrators by providing the user identity from the SA server to other SA devices. SA trusted connections use client authentication for TLS connections. For example, when SA server establishes an SA trusted connection to a Concentrator, the Concentrator (TLS server) authenticates the SA server (TLS client). Once authenticated, the SA server provides the Concentrator with the user's authenticated identity and roles. TOE devices will trust the certificate of the SA server when an administrator has added the TLS client's PEM encoded certificate to the server's trusted peer list. When the Concentrator then subsequently establishes a connection to other devices, it will present an authentication token for the user, which contains the username, and role. If the device recognizes the TLS client device's certificate as trusted and if the role is defined locally, it will allow the user access. If the TLS server device does not accept the TLS client device's certificate, then the client must authenticate by providing the username and role(s) for that session. If a role is not defined locally, it is ignored. For example for Archiver, Log and Packet Decoder/Concentrator; if the device does not have the role defined it is ignored and SA Server has to connect using the legacy method (present usrname/passwd credentials). For all other devices/services (that is, Broker, ESA, Malware Analysis devices) trust is determined as follows. If the TLS client device reports user "tim" has roles "A", "B", "C" but the TLS server device only defines roles "X" and "Y" then when user tim makes an API call the API call will be rejected on any APIs that are controlled with roles "X" and "Y". The SA Server acts as the TLS client and the device acts as the TLS server. The device uses the SA Server certificate in the TLS exchange to authenticate the SA Server. The TLS client device does not authenticate the TLS server device.

Once access to the TOE is granted, authorization to access functions and data is implemented via the user's role membership. User roles are the central point of authorization in the TOE's security model. User roles are created with a specific set of permissions which apply to all users assigned to the role.

The TOE is able to detect when an administrator configurable positive integer of unsuccessful authentication attempts occur related to SA Server UI user authentication. When the defined number of unsuccessful authentication attempts has been surpassed, the TOE locks the user account for a specified time period as configured by authorized administrator. The range of time values which can be configured for the maximum number of login attempts is min 0, no max and default is 5 (Maximum number of login attempts allowed before an account is locked out is 5). The range of time values which can be configured for the lockout time is min 0, no max and default is 20 minutes (Period of time where locked out accounts remain locked out). Note that 0 means lockout is disabled. Once the session is locked and the timeframe for locking the session has passed the user may log back in by providing their username and password. When an unsuccessful authentication attempt has been detected the TOE audits the failed authentication attempt.

The Identification and authentication function is designed to satisfy the following security functional requirements:

- FIA_AFL.1: The TOE is able to detect when an administrator configurable positive integer of unsuccessful authentication attempts occur related to SA UI user authentication. When the defined number of unsuccessful authentication attempts has been surpassed, the TOE locks the user account for a specified time period as configured by authorized administrator.
- FIA_ATD.1: The TOE maintains a list of security attributes: Username, password, role for individual users.

- FIA_UAU.1: The TOE allows "acknowledge end-user license agreement and view warning banner" on behalf of the user to be performed before the user is authenticated. Otherwise the TOE requires each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
- FIA_UAU.5.1 The TOE provides SSH public-key, and password-based authentication mechanisms to support user authentication. The TOE authenticates claimed identities for TOE users using password-based and for authorized IT entities using SSH public-key authentication mechanisms.
- FIA_UID.1: The TOE allows "acknowledge end-user license agreement and view warning banner" on behalf of the user to be performed before the user is identified. Otherwise the TOE requires each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.4 Security Monitoring with Security Information and Event Management

The TOE accepts network and log data and analyzes the data for anomalous and inappropriate activity. The TOE:

- Reconstructs network traffic,
- Parses network traffic and log data to identify metadata,
- Indexes metadata for analysis,
- Analyzes metadata by applying Decoder rules, ESA rules, and Malware Analysis rules, and
- Generates an alert when a rule matches.

The parsers, indices, and rules encapsulate signatures of anomalous and inappropriate activity. The analysis process includes signature analysis and malware analysis when indicated. The TOE identifies known patterns based on parsed metadata from transactions. The out of the box rules identify patterns representing known attacks. Additional rule content is developed specifically for threats and can include a file type rule which when matched would result in Malware Analysis processing. Malware analysis uses network session analysis, and static file analysis to check for malware. The device can perform continuous or on-demand polling to extract sessions identified as potentially carrying malware.

There are three types of Decoder rules: Correlation, Network, and Application.

Basic Correlation Rules are applied at the session level and alert the user to specific activities that may be occurring in their environment. Correlation rules are applied over a configurable slice of time on a Decoder. When the conditions are met, alert metadata is created for this activity and there is a visible indicator of the suspicious activity.

Network rules do not apply to Log Decoders. Network layer rules are applied at the packet level on a Decoder and are made up of rule sets from Layer 2 - Layer 4. Network rules can apply to multiple network layers (for example, when a network rule filters out specific ports for a specific IP address).

Application rules can be applied to both Decoders and Log Decoders. Application layer rules are applied at the session level. Rule conditions trigger an action when matched. One of the following actions is applied when a matching packet is found depending on the defined rule.

- Keep: The packet payload and associated meta are saved when they match the rule.
- Filter: The packet is not saved when it matches the rule.
- Truncate: The packet payload is not saved when it matches the rule, but packet headers and associated meta are retained.

The TOE is capable of receiving events from different source types (e.g. Syslog, SNMP Trap, NetFlow…) covering over 350 specific devices. RSA content team authors rules for parsing content from a particular device (Log Decoder). These parser rules make up the signatures for log events (and network packets) to be collected (IDS_ANL.1). Parsing rules or signatures are included for the following event sources:

a. Syslog
b. SNMP Trap

c. NetFlow
d. File
e. Windows (WinRM)
f. Windows (Legacy)
g. ODBC
h. Check Point LEA
i. VMWare
j. SDEE

Note: LockBox protects credentials for log sources, but the functionality does not implement any security functional requirements. The TOE protects log source by encryption (using a FIPS-validated cryptographic module). This protection does not contribute to satisfying any TOE security functional requirements.

Categories of ESA Rules:

- Log Events with certain criteria
- Active Directory Policy Modification
- Adapter Events
- Backdoor Activity
- Brute Force Login
- Traffic detection with certain criteria
- Port Activity and port scan
- Login and attempted login activity including account lockouts
- DNS activity
- Account creation and password changes
- Connection attempts
- Scan Events
- P2P Software detection
- Privilege escalation
- Configuration changes
- Windows account creation with subsequent management activity
- Windows audit log cleared

Malware Analysis Rules / Methodologies (out of the box):

- Network Session Analysis: metadata check: attribution checks (e.g. from China, new domain, …) and scores metadata
- Static File Analysis: 2000 rules consisting of WinPE, Office, and PDF checks such as Payload, Header, High-Risk scripting, Obfuscation, Artifacts, Country, and Meta.

Analytical results are recorded with the following information: date and time of the result, type of result, and identification of data source. Type of result corresponds to rule that generates an alert. There are original data sources and metadata sources. The original sources are from the operational environment (Cisco, Juniper, etc.). The metadata sources are internal to SA and are also identified in the user interface. It is the original sources that correspond to data source in the requirement.

The TOE uses results of the analysis to determine whether or not to send an alarm. If analysis identifies potential intrusion, malware or misuse an alarm (alert) is sent to the incident management SA views (IDS_RCT.1). 'intrusions' are anomalous events or events that merit further investigation. Authorized administrators can view, and work with alarm notifications via the incident management menu available remotely through the SA Server User Interface (UI). The IDS data (metadata, raw logs, raw packet data, and incident management data) can also be viewed from the UI by users with the Analyst and Administrator administrative roles. The data are provided in a readable format to authorized users (IDS_RDR.1). Updates to the rules can be obtained by licensed customers at the vendor's website Live. Only authorized Administrators are permitted to download these updates.

The Security Monitoring with Security Information and Event Management function is designed to satisfy the following security functional requirements:

- IDS_ANL_EXT.1: The TOE performs signature analysis on all network and log data received. The TOE records within each analytical result the following information: date and time of the result, type of result, and identification of the data source.
- IDS_RCT_EXT.1: The TOE sends an alarm to incident management SA views when an intrusion is detected.
- IDS_RDR_EXT.1: The TOE provides the Analyst and Administrator roles with the capability to read all metadata, raw logs, raw packet data, rules, and incident management data from the IDS data. The TOE provides the IDS data in a manner suitable for the user to interpret the information. The TOE prohibits all users read access to the IDS data, except those users that have been granted explicit read-access.

6.5 Security management

The ST defines the Administrator, Analyst, Operator, SOC_Manager, and Malware Analyst roles to distinguish users who can perform various security management functions. The TOE defines roles with various security management functions protected with privileges. A user that is assigned a role has the associated privileges assigned to that role and can perform those associated security management functions. Note that internally, some TOE components associate groups to users. However these groups are essentially the same as the roles previously described differing only in reference (e.g. group rather than role).

Only authorized administrators with the Administrator role can create, modify, or delete users. The ability to query and manage the TSF data is restricted to the users as identified in Table 5-3: Management of TSF Data in Section 5.2.5.2.

The SA Server UI Interface provides the interface through which the authorized administrator manages the security functions of the TOE and the TSF data. There are no local administrative interfaces provided in the evaluated configuration for either management or installation. Only authorized administrators with the Administrator or Operator role can start/stop services and start or stop the Audit function. Users with the Operator role only have permissions to those services explicitly assigned to them by the user with the Administrator role. User accounts are per service. The Administrator should not create an account for the Analyst or Operator on services they should not have access to.

The Security management function is designed to satisfy the following security functional requirements:

- FMT_MOF.1: The TOE restricts the ability to disable, enable, the audit function, start/stop services (Decoder, Concentrator, Broker, ESA, …) functions to the authorised identified roles. Starting and stopping the services also starts and stops the Audit collection function as each TOE appliance/service generates its own audit records.
- FMT_MTD.1: The TOE restricts the ability to query and manage the TSF data to the authorised identified roles.
- FMT_SMF.1: The TOE provides management functions identified in the text above to support the authorised identified role's ability to manage the TSF data, functions, and security audit as described in the above section.
- FMT_SMR.1: The TOE maintains the security roles: Administrator, Analyst, Operator, SOC_Manager, and Malware Analyst. The TSF is able to associate users with roles.

6.6 Protection of the TSF

The TOE uses TLS in FIPS-compliant mode to protect the TSF data transmitted between distributed parts of the TOE. This protection is enforced across all TOE Device components/appliances (e.g. device to device). The data that is protected across the communication channel consist of audit data, and collected data: all metadata, raw logs, raw packet data, rules, and incident management data. TLS is automatically configured in FIPS mode which is the evaluated configuration mode.

The Protection of the TSF function is designed to satisfy the following security functional and assurance requirements:

- FPT_ITT.1: The TOE utilizes TLS to protect data transmitted between distributed parts of the TOE (Device to Device only).

6.7 TOE Access

The TOE terminates an interactive session after a time interval of user inactivity configured by an authorized administrator. Authorized administrators can configure the interval to be between min 0 and no max but default is 600 (Expiry for all sessions in minutes) via the remote administrative GUI interface. Note that zero is permitted, which disables lockout. An interactive remote session that is inactive (i.e., no commands issued and no activity from the remote client browser to the SA Server UI) for the defined timeout value will be terminated.

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

Before establishing an interactive user session, the TOE displays an advisory warning message regarding unauthorised use of the TOE.

The TOE access function is designed to satisfy the following security functional requirements:

- FTA_SSL.3: The TOE terminates an interactive session after a time interval of user inactivity configured by an authorized administrator.
- FTA_SSL.4: The TOE allows user-initiated termination of the user's own interactive session.
- FTA_TAB.1: Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorised use of the TOE.

6.8 Trusted path/channels

The TOE requires an HTTPS connection for remote users to authenticate to the TOE from a browser that is part of the environment. To successfully establish an interactive administrative session, the administrator must be able to provide acceptable user credentials (e.g., user id and password), after which they will be able to access the GUI interface. This initial authentication action occurs over TLS in FIPS mode negotiated using the ciphers defined as valid for a TLS in FIPS mode session as described in section 6.2. Subsequently, all SA interface session data transmission also occurs over TLS. The TOE uses a FIPS-validated module for SSH protected communication pathways for the transfer of file event source data from log data sources to the TOE. TLS and SSH ensure the administrative session and file transfer communication pathways are secured from disclosure and modification.

The Trusted path/channels function is designed to satisfy the following security functional requirements:

- FTP_TRP.1: The TOE provides a communication path between itself and remote administrative and authorized IT Entity users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification and disclosure.
- FTP_TRP.1: The TOE permits remote administrative and authorized IT Entity users to initiate communication via the trusted path.
- FTP_TRP.1: The TOE requires the use of the trusted path for initial user authentication, all SA interface session data, and for the transfer of file event source data from log data sources to the TOE.

7 Rationale

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

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

7.1 Security Objectives Rationale

This section shows that all secure usage assumptions, organizational security policies, and threats are completely covered by security objectives. In addition, each objective counters or addresses at least one assumption, organizational security policy, or threat.

7.1.1 Security Objectives Rationale for the TOE and Environment

This section provides evidence demonstrating the coverage of organizational policies and usage assumptions by the security objectives.

	T.MALICIOUS_ACTIVITY	T.INADVERTENT_ACTIVITY	T.MISUSE	T.TSF_COMPROMISE	T. UNAUTHORIZED_ACCESS	T.UNACCOUNTABLE_USERS	A.AUDIT_PROTECTION	A.DATA_SOURCES	A. DEPLOY	A. MANAGE	A. PHYSICAL	A.TIME	A.TRUSTED_ADMIN	A.USER
O.ANALYZE	X	X	X											
O.AUDIT_GENERATION					X	X								
O.AUDIT_PROTECTION				X										
O.MANAGE	X	X	X	X	X									
O.PROTECTED_COMMS				X	X									
O.TOE_ACCESS				X	X	X								
OE.AUDIT_PROTECTION							X							
OE. DATA_SOURCES								X						
OE.DEPLOY									X					
OE.MANAGE										X				
OE.PHYSICAL											X			
OE.TIME												X		
OE.TRUSTED_ADMIN													X	
OE.USER														X

7.1.1.1 T.MALICIOUS_ACTIVITY

Malicious activity by an attacker may occur on the network the TOE monitors may go undetected.

This Threat is countered by ensuring that:

- O.ANALYZE: The TOE applies analytical processes and collects information to derive conclusions and send alerts about potential unauthorized/malicious activities in the monitored network.
- O.MANAGE: The TOE provide tools necessary to support the authorized administrators in their management of the security of the TOE, this includes reviewing the alarms and IDS data.

7.1.1.2 T.INADVERTENT_ACTIVITY

Inadvertent activity and access by a user or a process that may occur on the network the TOE monitors may go undetected.

This Threat is countered by ensuring that:

- O.ANALYZE: The TOE applies analytical processes and collects information to derive conclusions and send alerts about potential unauthorized/malicious activities in the monitored network.
- O.MANAGE: The TOE provide tools necessary to support the authorized administrators in their management of the security of the TOE, this includes reviewing the alarms and IDS data.

7.1.1.3 T.MISUSE

Unauthorized accesses and activity indicative of misuse by a user or a process that may occur on the network the TOE monitors may go undetected.

This Threat is countered by ensuring that:

- O.ANALYZE: The TOE applies analytical processes and collects information to derive conclusions and send alerts about potential misuse in the monitored network.
- O.MANAGE: The TOE provide tools necessary to support the authorized administrators in their management of the security of the TOE, this includes reviewing the alarms and IDS data.

7.1.1.4 T.TSF_COMPROMISE

A user may cause, through an unsophisticated attack, TSF data, or security functions to be inappropriately accessed (viewed, modified, or deleted).

This Threat is countered by ensuring that:

- O.MANAGE: The TOE restricts access to the security functions and TSF data to authorized administrators.
- O.AUDIT_PROTECTION: The TOE helps to protect the audit records by not providing interfaces to modify or delete the audit records.
- O.PROTECTED_COMMUNICATION: Administrative communications with the TOE; IT entities (log sources) and TOE device to TOE Device communications are protected from disclosure and medication.
- O.TOE_ACCESS: To reduce the potential of unauthorized access to TOE security functions and data, the TOE ensures that only authorized administrators can log in and access security management functions and TOE data.

7.1.1.5 T.UNAUTHORIZED_ACCESS

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

This threat is satisfied by ensuring that:

- O.MANAGE: The TOE restricts access to the security functions and TSF data to authorized administrators.
- O.PROTECTED_COMMS: To reduce the potential that an unauthorized user might gain unauthorized access to the TOE or its data via data transmitted across a network, the TOE is expected to protect its administrator communication channels from disclosure, modification. The TOE also requires that TOE device to TOE device communications and log source to TOE communications are protected from disclosure, modification.
- O. AUDIT_GENERATION: To reduce the potential of unauthorized access attempts that might go unnoticed, the TOE is expected to log security relevant events.

- O.TOE_ACCESS: To reduce the potential of unauthorized access to TOE security functions and data, the TOE is expected to be designed to ensure that only authorized administrators can log in and access security management functions and TOE data.

7.1.1.6 T.UNACCOUNTABLE_USERS

Authorized users of the TOE might not be held accountable for their actions.

.

This threat is satisfied by ensuring that:

- O.AUDIT_GENERATION: To reduce the potential of security relevant actions occurring without notice, the TOE is expected to audit security relevant events and associates the user that the caused the event with the audit record. This helps to mitigate the threat by ensuring that the user that caused the security relevant events can be identified.
- O.TOE_ACCESS: This objective helps to mitigate this threat by ensuring each user is uniquely identified and authenticated.

7.1.1.7 A.AUDIT_PROTECTION

The operational environment will provide the capability to protect audit information.

This Assumption is satisfied by ensuring that:

- OE.AUDIT_PROTECTION: The operational environment provides the capability to protect audit information.

7.1.1.8 A.DATA_SOURCES

The data sources in the environment will provide complete and reliable data to the TOE.

This Assumption is satisfied by ensuring that:

- OE.DATA_SOURCES: The data sources in the environment provide complete and reliable data to the TOE.

7.1.1.9 A.DEPLOY

TOE Administrators will properly configure the network in the TOE operational environment and configure adequate network capacity for the deployed TOE components.

This assumption is countered by ensuring that:

OE.DEPLOY: The TOE Administrators will properly configure the network in the TOE operational environment and configure adequate network capacity for the deployed TOE components.

7.1.1.10 A.MANAGE

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

This assumption is countered by ensuring that:

OE.MANAGE: Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the TSF.

7.1.1.11 A.PHYSICAL

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

This assumption is countered by ensuring that:

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

7.1.1.12 A.TIME

The environment will provide reliable time sources for use by the TOE.

This assumption is countered by ensuring that:

OE.TIME: The environment must provide a time source for use by the TOE

7.1.1.13 A.TRUSTED_ADMIN

TOE Administrators will follow and apply all administrator guidance in a trusted manner.

This assumption is countered by ensuring that:

OE.TRUSTED_ADMIN: TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

7.1.1.14 A.USER

Users will protect their authentication data.

This assumption is countered by ensuring that:

OE.USER: Users must ensure that their authentication data is held securely and not disclosed to unauthorized persons.

7.2 Security Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the components (requirements) in the Security Target. Note Table 7-1 indicates the requirements that effectively satisfy the individual objectives.

7.2.1 Security Functional Requirements Rationale

All of the Security Functional Requirements (SFR) identified in this Security Target are fully addressed in this section and each SFR is mapped to the objective for which it is intended to satisfy.

	O.ANALYZE	O.AUDIT_PROTECTION	O.AUDIT_GENERATION	O.MANAGE	O.PROTECTED_COMMUNICATIONS	O.TOE_ACCESS
FAU_GEN.1			X			
FAU_GEN.2			X			
FAU_SAR.1				X		
FAU_SAR.2				X		
FAU_STG.1		X				
FCS_SSH_EXT.1					X	
FCS_TLS_EXT.1					X	
FIA_AFL.1						X
FIA_ATD.1						X
FIA_UAU.1						X
FIA_UAU.5						X
FIA_UID.1						X
FMT_MOF.1				X		
FMT_MTD.1				X		
FMT_SMF.1				X		

	O.ANALYZE	O.AUDIT_PROTECTION	O.AUDIT_GENERATION	O.MANAGE	O.PROTECTED_COMMUNICATIONS	O.TOE_ACCESS
FMT_SMR.1				X		
FPT_ITT.1					X	
FTA_SSL.3						X
FTA_SSL.4						X
FTA_TAB.1						X
FTP_TRP.1					X	
IDS_ANL_EXT.1	X					
IDS_RCT_EXT.1	X					
IDS_RDR_EXT.1				X		

Table 7-1 Objective to Requirement Correspondence

7.2.1.1 O.ANALYZE

The TOE will apply analytical processes and information to derive conclusions about potential unauthorized/malicious intrusions and send appropriate alerts.

This TOE Security Objective is satisfied by ensuring that:

- IDS_ANL_EXT.1: The TOE performs signature analysis functions on all data received through the data sources. The TOE records each analytical result and includes at least the following information in the record: Date and time of the result, type of result, identification of data source.
- IDS_RCT.1_EXT: The TOE sends an alarm to incident management SA views when an intrusion is detected.

7.2.1.2 O.AUDIT_GENERATION

The TOE will provide the capability to detect and create records of security relevant events associated with users.

This TOE Security Objective is satisfied by ensuring that:

- FAU_GEN.1: The TOE is required to provide a set of events that it is capable of recording. Among these events the TOE is able to audit must be security relevant events occurring within the TOE. This requirement also defines the information that must be recorded for each auditable event.
- FAU_GEN.2: The TOE is required to associate a user identity with the auditable events being recorded.

7.2.1.3 O.AUDIT_PROTECTION

The TOE will provide the capability for protection of the audit information from unauthorized users via the TOE interfaces.

This TOE Security Objective is satisfied by ensuring that:

- FAU_STG.1: The TOE is required to protect the stored audit records from unauthorized modification or deletion.

7.2.1.4 O.MANAGE

The TOE will provide all the functions necessary to support the authorized administrators in their management of the security of the TOE, and restrict these functions from unauthorized use.

This TOE Security Objective is satisfied by ensuring that:

- FAU_SAR.1: The TOE is required to provide authorized administrators with the capability to read all audit information from the audit records. The TOE is required to provide the audit records in a manner suitable for the user to interpret the information.
- FAU_SAR.2: The TOE is required to prohibit all users read access to the audit records, except those users that have been granted explicit read-access.
- FMT_MOF.1: The TOE is required to restrict the ability to enable disable on security functions to authorized administrators.
- FMT_MTD.1: The TOE is required to restrict to authorized administrators the ability to manipulate TOE data used to enforce the TOE security functions.
- FMT_SMF.1: The TOE is required to provide at least the identified management functions for use by the authorized administrators.
- FMT_SMR.1: The TOE is required to establish, maintain and enforce authorized administrator roles.
- IDS_RDR_EXT.1: The TOE is required to provide users with the Analyst and/or Administrator roles with the capability to read all metadata, raw logs, raw packet data, rules, and incident management data from the IDS data. The TOE provides the data in a manner suitable for the user to interpret the information; and prohibits all users read access to the IDS data, except those users that have been granted explicit read-access.

7.2.1.5 O.PROTECTED_COMMS

The TOE will provide protected communication channels for remote administrators, IT entities and for TOE device to TOE device communication channels.

This TOE Security Objective is satisfied by ensuring that:

- FCS_SSH_EXT.1: The TOE implements SSH to protect log data being sent to the TOE from authorized IT entities (log sources).
- FCS_TLS_EXT.1: The TOE is required to implement TLS to protect applicable network communication channels.
- FPT_ITT.1: The TOE is required to protect communications from disclosure and detect the modification of those communications when it is transmitted between distributed parts of the TOE.
- FTP_TRP.1: The TOE is required to protect communication between itself and its remote administrative users from disclosure and detect the modification of those communications. The TOE is required to use HTTP over TLS to provide these protections.

7.2.1.6 O.TOE_ACCESS

The TOE will provide mechanisms that control a user's logical access to the TOE.

This TOE Security Objective is satisfied by ensuring that:

- FIA_AFL.1: The TOE must detect when an administrator configurable positive integer within the configured timeframe of unsuccessful authentication attempts occur related to SA UI user authentication. When the defined number of unsuccessful authentication attempts has been met, the TSF shall lock account for a specified time period as configured by authorized administrator.
- FIA_ATD.1: The TOE maintains the following list of security attributes belonging to individual human users: Username, password, role. The attributes of users, are used by the TOE to determine a user's identity and role memberships and enforce what type of access the user has to the TOE.

- FIA_UAU.1: The TOE is required to ensure that users must be authenticated in order to access functions, other than those specifically identified (view the warning banner and acknowledging the end-user license).
- FIA_UAU.5: The TOE provides password-based authentication for administrative users and SSH public-key based authentication for authorized IT entities (log sources) sending log data to the TOE. Administrative users must successfully authenticate by providing a valid username and password in order to access functions, other than those specifically identified (view the warning banner and acknowledging the end-user license). IT entities must successfully authenticate using public key-based authentication prior to sending any log data to the TOE.
- FIA_UID.1: The TOE is required to ensure that users must be identified in order to access functions of the TOE other than those specifically identified (view the warning banner and acknowledging the end-user license).
- FTA_SSL.3: The TOE will terminate an interactive session after a time period configured by an authorized administrator.
- FTA_SSL.4: The TOE must allow user-initiated termination of the user's own interactive session.
- FTA_TAB.1: Before establishing a user session, the TOE shall display an advisory warning message regarding unauthorised use of the TOE.

7.2.2 Security Assurance Requirements Rationale

The security assurance requirements for the TOE are the EAL 2 augmented with ALC_FLR.1 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

EAL 2 augmented with ALC_FLR.1 was selected as the assurance level because the TOE is a commercial product whose users require a low to moderate degree of independently assured security. ALC_FLR.1 was selected to exceed EAL2 assurance objectives in order to ensure that identified flaws are addressed. The TOE is targeted at a relatively benign environment with good physical access security and competent administrators. Within such environments it is assumed that attackers will have little attack potential. As such, EAL 2 augmented with ALC_FLR.1 is appropriate to provide the assurance necessary to counter the limited potential for attack.

7.3 Requirement Dependency Rationale

The following table demonstrates the dependencies among the claimed security requirements. It shows that all dependencies are satisfied. Therefore the requirements work together to accomplish the overall objectives defined for the TOE.

ST Requirement	CC Dependencies	ST Dependencies
FAU_GEN.1	FPT_STM.1	See TimeStamp Note Below.
FAU_GEN.2	FAU_GEN.1 and FIA_UID.1	FAU_GEN.1 and FIA_UID.2
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FCS_SSH_EXT.1	None	None
FCS_TLS_EXT.1	None	None
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_ATD.1	None	None
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UAU.5	None	None
FIA_UID.1	None	None
FMT_MOF.1	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_MTD.1	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_SMF.1	None	None
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FPT_ITT.1	None	None

FTA_SSL.3	None	None
FTA_SSL.4	None	None
FTA_TAB.1	None	None
FTP_TRP.1	None	None
IDS_ANL_EXT.1	None	
IDS_RCT_EXT.1	IDS_ANL_EXT.1	IDS_ANL_EXT.1
IDS_RDR_EXT.1	IDS_ANL_EXT.1	IDS_ANL_EXT.1
ADV_FSP.1	None	None
AGD_OPE.1	ADV_FSP.1	ADV_FSP.1
AGD_PRE.1	None	None
ALC_CMC.1	ALC_CMS.1	ALC_CMS.1
ALC_CMS.1	None	None
ALC_FLR.1	None	None
ATE_COV.1	ADV_FSP.2 and ATE_FUN.1	ADV_FSP.2 and ATE_FUN.1
ATE_FUN.1	ATE_COV.1	ATE_COV.1
ATE_IND.2	ADV_FSP.2 and AGD_OPE.1 and AGD_PRE.1 and ATE_COV.1 and ATE_FUN.1	ADV_FSP.2 and AGD_OPE.1 and AGD_PRE.1 and ATE_COV.1 and ATE_FUN.1
AVA_VAN.2	ADV_ARC.1 and ADV_FSP.2 and ADV_TDS.1 and AGD_OPE.1 and AGD_PRE.1	ADV_ARC.1 and ADV_FSP.2 and ADV_TDS.1 and AGD_OPE.1 and AGD_PRE.1

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

7.4 TOE Summary Specification Rationale

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

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. **Table 7-2 Security Requirements to Security Functions** Mapping demonstrates the relationship between security requirements and security functions.

	Security audit	**Cryptographic support**	**Identification and authentication**	**Security Monitoring with SIEM**	**Security management**	**Protection of the TSF**	**TOE Access**	**Trusted path/channels**
FAU_GEN.1	X							
FAU_GEN.2	X							
FAU_SAR.1	X							
FAU_SAR.2	X							
FAU_STG.1	X							
FCS_SSH_EXT.1		X						

FCS_TLS_EXT.1		X						
FIA_AFL.1			X					
FIA_ATD.1			X					
FIA_UAU.1			X					
FIA_UAU.5			X					
FIA_UID.1			X					
IDS_ANL_EXT.1				X				
IDS_RCT_EXT.1				X				
IDS_RDR_EXT.1				X				
FMT_MOF.1					X			
FMT_MTD.1					X			
FMT_SMF.1					X			
FMT_SMR.1					X			
FPT_ITT.1						X		
FTA_SSL.3							X	
FTA_SSL.4							X	
FTA_TAB.1							X	
FTP_TRP.1								X

Table 7-2 Security Requirements to Security Functions Mapping