RSA, The Security Division of EMC enVision® platform v4.0 SP 1

Security Target

Evaluation Assurance Level: 3+
Document Version: 0.8

Prepared for:	Prepared by:
RSA, The Security Division of EMC	Corsec Security, Inc.
174 Middlesex Turnpike Bedford, MA 01730	10340 Democracy Lane, Suite 201 Fairfax, VA 22030
Phone: (877) 772-4900	Phone: (703) 267-6050
Fax: (781) 515-5010	Fax: (703) 267-6810
http://www.rsa.com	http://www.corsec.com

Table of Contents

Table of Figures

Table of Tables

1 Security Target Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation is RSA enVision® platform v4.0 SP 1, and will hereafter be referred to as the TOE throughout this document. The TOE is a Security Information and Event Management (SIEM) platform. The TOE collects raw log data from monitored devices and formats the data into an Internet Protocol Data Base (IPDB). Users can access the IPDB through a web interface and perform deep analysis of monitored events in real time and generate detailed reports on their findings.

1.1 Purpose

This ST contains the following sections to provide mapping of the Security Environment to the Security Requirements that the TOE meets in order to remove, diminish or mitigate the defined threats:

- Security Target Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functions and describes the physical and logical scope for the TOE, as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), ST Protection Profile, and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem Definition (Section 3) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Extended Components Definition (Section 5) – Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3.
- Security Requirements (Section 6) – Presents the SFRs and SARs met by the TOE.
- TOE Summary Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- Rationale (Section 8) – Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms and Terminology (Section 9) – Defines the acronyms and terminology used within this ST.

1.2 Security Target and TOE References

Table 1 – ST and TOE References

ST Title	RSA, The Security Division of EMC enVision® platform v4.0 SP 1 Security Target
ST Version	Version 0.8
ST Author	Corsec Security, Inc. Greg Milliken and Amy Nicewick
ST Publication Date	2009-12-11
TOE Reference	RSA enVision® platform v4.0 SP 1[1] Build 0236
Keywords	SIEM, IPDB, Internet Protocol Database, Security Information and Event Management, log management, log analysis, forensics, compliance, RSA, enVision, LogSmart, All the Data, EMC.

1.3 TOE Overview

The TOE Overview summarizes the usage and major security features of the TOE. The TOE Overview provides a context for the TOE evaluation by identifying the TOE type, describing the product, and defining the specific evaluated configuration.

The TOE is software running on the "60 Series" family of appliances that provide corporations with the power to gather and use event data. The TOE is an Event Analyzer (EAN) that aggregates log data from a variety of systems and provides an analysis interface for users to interpret the information contained in the logs. Corporations can use the event data to understand security, compliance, or operational status of their organization in real-time or over any period of time. The TOE provides efficient collection, analysis, and management of event data from a wide range of Internet Protocol (IP) devices.

An LS deployment of enVision includes Local Collector (LC), Database Server (D-SRV), and Application Server (A-SRV) components. These components each have their own hardware platform and represent the distributed architecture of the LS deployment of the TOE. The LC appliance is dedicated to event collection, and stores collected data in Network Attached Storage (NAS). The D-SRV services requests for collected data. The A-SRV is responsible for performing analysis of data and generating reports. The LS deployment of the TOE has a highly scalable architecture; multiple appliances can be deployed in the same roles in order to increase capacity and performance.

An ES deployment of enVision includes all of the functionality present in the LS on a single hardware platform. ES deployments of the TOE can use a NAS device, a Direct Attached Storage (DAS) device, or local storage. Local storage is the hard disk on the ES hardware platform.

[1] The TOE version number 4.0 SP 1 indicates that this is the exact 4.0 SP 1 version without additional patches or service packs. RSA distributes only one build of the 4.0 SP 1 version.

The same software is installed on each appliance, with configuration options determining whether an appliance is an ES, an LC, a D-SRV, or an A-SRV. The software runs on top of a hardened installation of Microsoft Windows Server 2003 Release 2 Enterprise Edition with Service Pack 2.

Figure 1 shows the details of the deployment configuration of the LS deployment of the TOE. The evaluated LS configuration is a single enVision site that includes one LC, one A-SRV, and one D-SRV, with Network Attached Storage (NAS). The Web User Interface (UI) coordinates with the A-SRV and D-SRV to retrieve and analyze data on monitored devices. The A-SRV provides alerting, reporting, and data export capabilities—including execution of output actions and creation or escalation of incidents. Data sources reside on the Local Area Network (LAN).

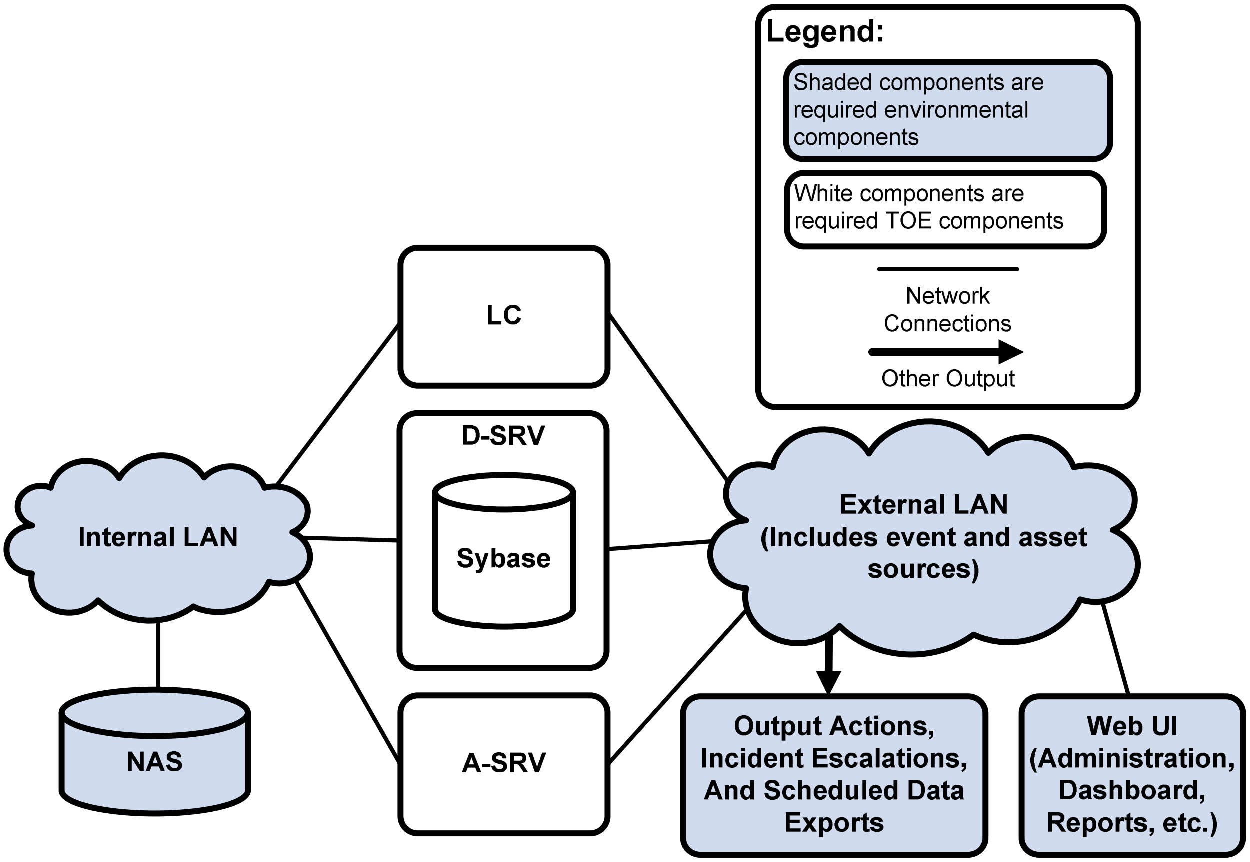
Legend:
Shaded components are required environmental components
White components are required TOE components
Network Connections
Other Output
LC
D-SRV
Sybase
A-SRV
Internal LAN
NAS
External LAN (Includes event and asset sources)
Output Actions, Incident Escalations, And Scheduled Data Exports
Web UI (Administration, Dashboard, Reports, etc.)

Figure 1 – LS Deployment Configuration of the TOE

Figure 2 shows the details of the ES deployment of the TOE. The evaluated ES configuration is a single enVision site that includes the ES system with a storage device. Each component operates as described above for the LS, except that the applicable A-SRV, D-SRV, and LC functionality is all provided through the single ES system.

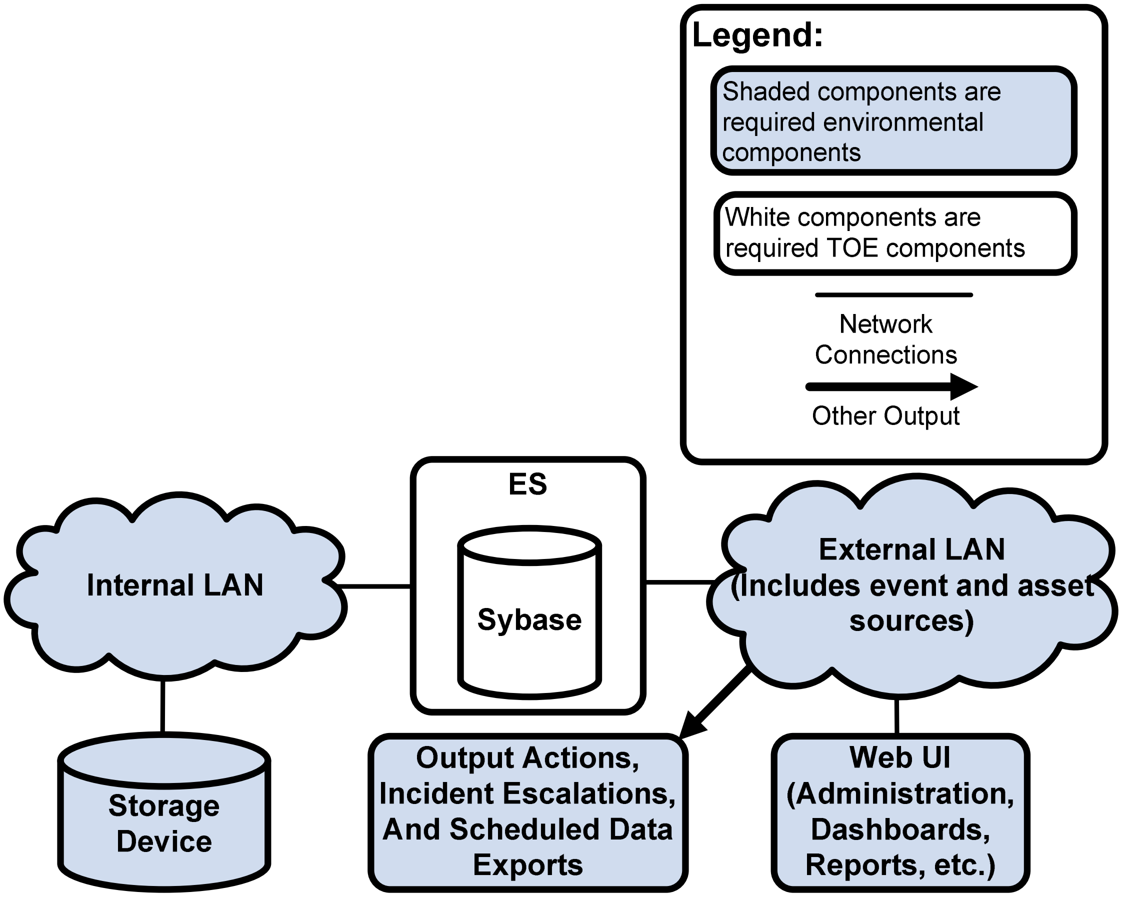
Legend:
Shaded components are required environmental components
White components are required TOE components
Network Connections
Other Output
ES
Sybase
Internal LAN
External LAN (Includes event and asset sources)
Storage Device
Output Actions, Incident Escalations, And Scheduled Data Exports
Web UI (Administration, Dashboards, Reports, etc.)

Figure 2 – ES Deployment Configuration of the TOE

1.3.1 Brief Description of the Components of the TOE

The TOE receives event data and stores the data on a storage device. An IPDB—an RSA proprietary flat file storage system designed to reduce overhead associated with entering new data into the database—contains the logs on the storage medium. IPDB is specifically designed to store and protect data from network source devices without filtering and – in most cases – without the need for intermediate agents. IPDB's advantage is that the data normalization process – the process by which data in a database is typically structured for general purpose querying – is removed. IPDB is designed with the understanding that log data from various sources is not homogenous and is thus able to store log data at a higher rate than general-purpose relational databases.

In addition to the IPDB, the TOE maintains an Asset database. Asset data is collected by the Asset Collector, then stored by the Asset Processor in a Sybase SQL AnyWhere 9.0.2.3480 Asset database. The Asset database contains information about vulnerabilities, services, and other properties of systems on the network ("assets"). The Asset database is capable of detecting major state changes in monitored assets.

The TOE includes an embedded copy of the National Vulnerability Database (NVD) issued by the Department of Homeland Security as well as the RSA Vulnerability and Asset Management (VAM) tool. The NVD is used to analyze events and their relevance to assets. VAM is a separate entity that contains an asset database containing a unified view of assets created by merging data from supported vulnerability assessment tools and imported asset information from asset tracking tools. Updated signatures for the embedded NVD are released periodically by the Department of Homeland Security. RSA provides these updated signatures, and updated signatures for the VAM tool, for administrators to download and install manually using the RSA SecurCare On-Line website. VAM and NVD content updates are not part of the TOE.

The TOE automatically analyzes event data and can send alerts when configurable patterns or events occur. Alerts can be sent in a variety of manners, including email notification, pager notification, Simple Network Management Protocol (SNMP) trap notification, and Syslog message notification. The analysis functionality is intelligent enough to suppress false-positives (events that match a pattern but are not actual security breaches). The TOE can perform stateful analysis of events and alert administrators when the pattern or event occurs.

TOE users (analysts) can create "watchlists" that facilitate configuration of reports and alerts in the TOE to keep track of specific items in event data.

The LC (and equivalent functionality on the ES) can collect event data via many protocols, including syslog, SNMP, database queries via Open Database Connectivity (ODBC), File Transfer Protocol (FTP), Secure File Transfer Protocol (SFTP)[2], Secure Hypertext Transfer Protocol (HTTPS)[3], and Microsoft Windows Event Collection. The event data collected by the TOE is stored in archive files[4] on the LC temporarily until they are transferred to the D-SRV for long-term storage. Each archive file receives a checksum[5] to ensure the integrity of the data stored within. The LC also runs an Asset Collector that collects data from third-party vulnerability scanners (such as Nessus or nCircle IP360). The LC converts vulnerability scanner data into an Extensible Markup Language (XML) format for storage and future analysis.

The D-SRV (and equivalent functionality on the ES) manages stored event data, and retrieves data upon request from an A-SRV. Multiple D-SRVs can distribute storage of event data. For distributed data, each D-SRV can communicate with other D-SRVs to retrieve needed data. The TOE stores the Asset DB and configuration data in an internal Sybase database that is replicated across all appliances. Sybase's built-in replication services allow each appliance to distribute Asset DB and configuration information.

The A-SRV (and equivalent functionality on the ES) runs a Tomcat version 5.5.26 web-application server that provides the main GUI. Tomcat enables a web-based user interface for reporting, alerting, and TOE management (the "Web User Interface (UI)") and a desktop application for event tracing and incident management ("Event Explorer"). The A-SRV also runs the enVision Alerter service, which performs stateful analysis of event data and sends alerts.

1.3.2 TOE Environment

The TOE requires the following environmental components in order to function properly:

- Network switch,
- NAS for LS, storage device (NAS, DAS, or local disk storage) for ES,
- Administrator workstation with a graphical web browser that supports Transport Layer Security (TLS),
- At least one monitored device,
- The 60 Series appliance hardware running a hardened installation of Microsoft Windows Server 2003.

1.4 TOE Description

This section primarily addresses the physical and logical components of the TOE included in the evaluation.

1.4.1 Physical Scope

Figure 3 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE and the constituents of the TOE Environment.

[2] This encryption protocol is provided by the TOE environment.
[3] This encryption protocol is provided by the TOE environment.
[4] These archive files are proprietary modifications of the ".zip" archive format.
[5] The checksum functionality is not included in the evaluated version of the TOE.

The TOE is a log aggregator and analyzer installed on 60 Series hardware appliances. The TOE is installed on a network in a distributed fashion as depicted in Figure 3 below for LS deployments. The essential physical components for the proper operation of the TOE in the evaluated LS configuration are:

- Application Server
- Database Server
- Local Collector

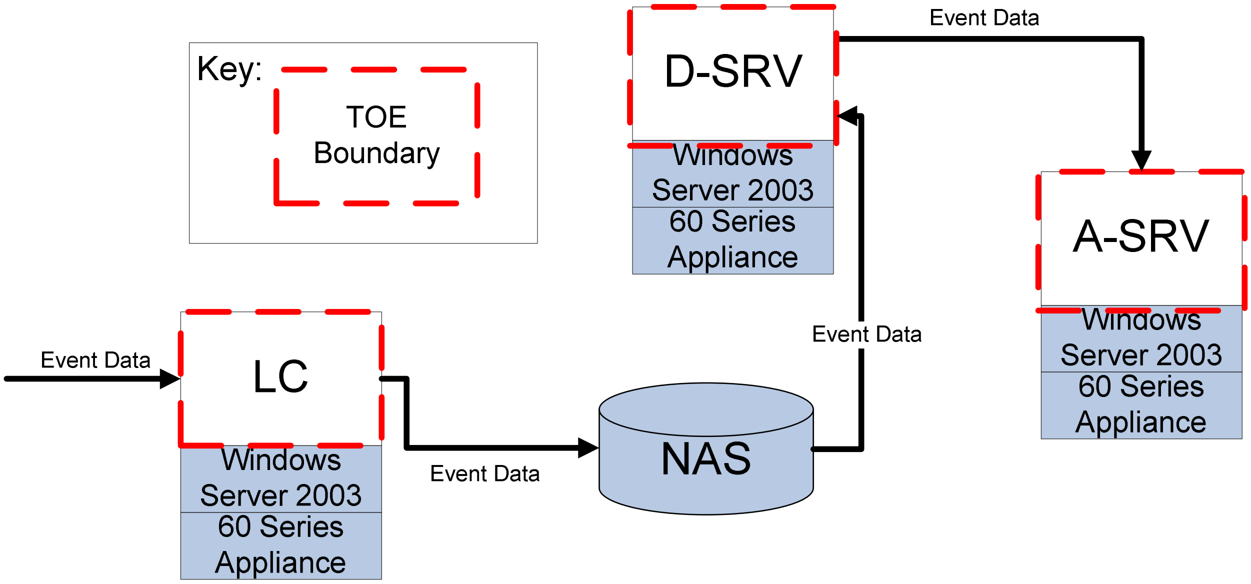

Figure 3 – LS Physical TOE Boundary

The TOE is installed on a network on a single appliance as depicted in Figure 4 below for ES deployments. The essential physical components for the proper operation of the TOE in the evaluated ES configuration are:

- ES Server

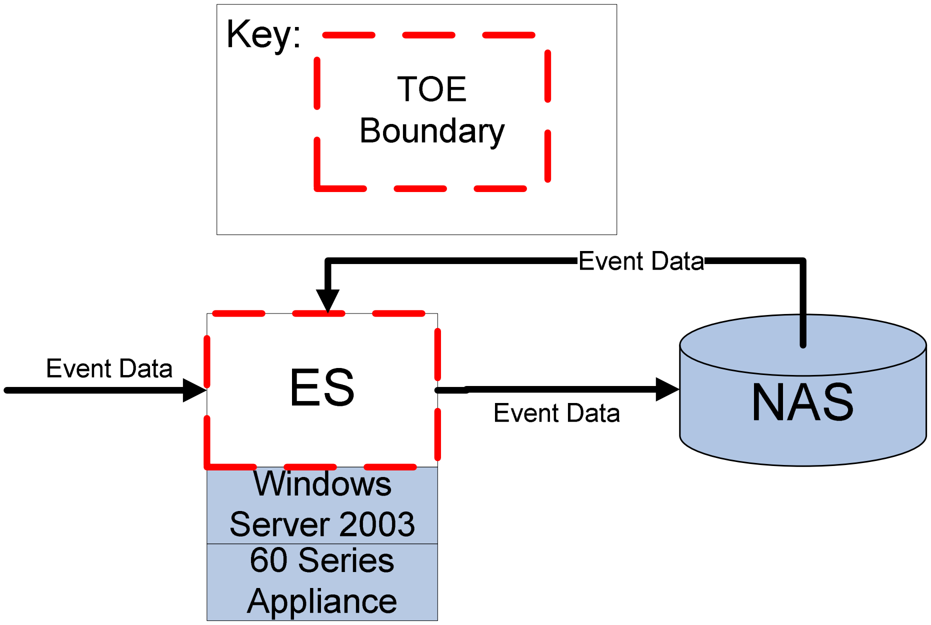

Figure 4 – ES Physical TOE Boundary

1.4.1.1 TOE Software

The TOE is application software running on one of the approved 60 Series appliances. The TOE is software only; the appliance hardware and operating system are not part of the TOE. The TOE runs on a hardened version of Microsoft Windows Server 2003 Release 2 Enterprise Edition with Service Pack 2. The TOE makes use of Sybase MySQL Anywhere version 9.0.2.3480. The TOE software in the LS deployment is distributed across at least three different appliances. The TOE software in the ES deployment runs on a single appliance.

1.4.1.2 Guidance Documentation

The following guides are required reading and part of the TOE:

- *RSA enVision™ Hardware Guide 60 Series*
- *RSA enVision™ Configuration Guide enVision® v4.0*
- *RSA enVision™ Migration Guide enVision® v4.0*
- *RSA enVision™ Release Notes enVision® v4.0 SP 1*
- *RSA enVision™ Administration and Operations Student Guide Rev A3*

1.4.2 Logical Scope

The security functional requirements implemented by the TOE are usefully grouped under the following Security Function Classes:

- Security Audit
- Identification and Authentication
- Security Management
- Protection of the TOE Security Function (TSF)
- Resource Utilization
- TOE Access
- EAN Component Requirements

1.4.2.1 Security Audit

The TOE can generate audit records for logging in, logging out, managing views, managing correlation rules, managing reports, and managing users. The TOE writes audit records to an audit trail that is stored in the IPDB. The audit records include information related to the audited event and when it occurred. A web Graphical User Interface (GUI) restricts access to the audit trail. Administrators can sort audit data based on several categories.

1.4.2.2 Identification and Authentication

The TOE manages a set of login credentials for all users and administrators. Each account is given an Identifier (ID), password, and a set of default or custom permissions. Users can also be assigned to groups that have custom permissions. Users and administrators must authenticate before performing any security-relevant actions on the TOE. Administrators can configure the TOE to automatically disable a user’s account after a configurable number of failed login attempts.

1.4.2.3 Security Management

The TOE provides a web GUI that administrators can use to manage the TSF behavior and TOE data. Administrators assign user permissions for managing security functions and data individually and through group assignment. Individual permissions override group permissions. Only administrators can modify users and groups.

1.4.2.4 Protection of the TSF

When a D-SRV, A-SRV, or equivalent service on an ES fails, the TOE continues to collect event data, thereby maintaining a secure state.

1.4.2.5 Resource Utilization

The TOE ensures that event data is still collected by the LC appliance or equivalent service on an ES when an A-SRV, D-SRV, or equivalent service on an ES fails.

1.4.2.6 TOE Access

The TOE displays an access banner to individuals attempting to connect, advising that unauthorized access is prohibited.

1.4.2.7 EAN Component Requirements

The TOE satisfies requirements that provide the functionality for and ensure the security of event data. This is accomplished by requiring TOE users to have a certain level of privilege and to authenticate to the TOE before access to TOE functionality and event data is granted. The TOE collects event data from various IP devices, including routers, switches, hubs, intrusion detection and prevention systems, and firewalls, using various protocols used by the devices. TOE event data includes information about IP devices collected by the TOE based on administrator configuration. Events include security infractions on network devices, users logging into and out of network devices, device startups and shutdowns, and related events that comprise network device event logs. Administrators can configure several aspects of event collection through the Web UI. The TOE can produce historical reports on event data and react to the results automatically. The TOE restricts access to the event data and displays reports through a graphical web interface.

The TOE can be configured by administrators to send information about certain events as alerts. These alerts include specific events that require immediate attention such as intrusion attempts, failed authentication, hardware errors, or software errors. Administrators can view alerts in many ways by using tools such as the enterprise dashboard, real-time detail views, alert history views, and alert configuration views. For more information about alerts, please see *Unit 5* of the *RSA enVision® Administration and Operations Student Guide Rev A3* document.

1.4.3 Product Physical/Logical Features and Functionality not included in the TOE

Features/Functionality that are not part of the evaluated configuration of the TOE are:

- Content updates,
- Event Explorer.

2 Conformance Claims

This section provides the identification for any CC, Protection Profile (PP), and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 2 – CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 2, September 2007; CC Part 2 extended; CC Part 3 conformant; Parts 2 and 3 Interpretations from the Interpreted Common Evaluation Methodology (CEM) as of 2009/02/12 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None.
Evaluation Assurance Level	EAL 3 (Augmented with Flaw Remediation (ALC_FLR.2))

3 Security Problem Definition

This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains all:

- Known and presumed threats countered by either the TOE or by the security environment
- Organizational security policies with which the TOE must comply
- Assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects

3.1 Threats to Security

This section identifies the threats to the Information Technology (IT) assets against which protection is required by the TOE or by the security environment. Note that while the identified threats are mitigated by the security functions implemented in the TOE, the overall assurance level (EAL 3+) also serves as an indicator of whether the TOE would be suitable for a given environment.

The following threats are applicable:

Table 3 – Threats

Name	Description
T.COMINT	An unauthorized person may attempt to compromise the integrity of the data analyzed and produced by the TOE by bypassing a security mechanism.
T.COMDIS	An unauthorized person may attempt to disclose the data analyzed and produced by the TOE by bypassing a security mechanism.
T.LOSSOF	An unauthorized person may attempt to remove or destroy data analyzed and produced by the TOE.
T.NOHALT	An unauthorized person may attempt to compromise the continuity of the TOEs analysis functionality by halting execution of the TOE.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
T.IMPCON	The TOE may be susceptible to improper configuration by an authorized or unauthorized person causing potential anomalies to go undetected.
T.FALACT	The TOE may fail to react to identified or suspected vulnerabilities to itself and monitored systems by external adversaries or inappropriate activity performed on it by TOE users or adversaries.
T.FALREC	The TOE may fail to recognize vulnerabilities or inappropriate activity based on event data received from each data source.
T.FALASC	The TOE may fail to identify vulnerabilities or inappropriate activity based on association of event data received from all data sources.

3.2 Organizational Security Policies

An Organizational Security Policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE. The following OSPs are presumed to be imposed upon the TOE or its operational environment by any organization implementing the TOE in the CC evaluated configuration:

Table 4 – Organizational Security Policies

Name	Description
P.ANALYZ	Analytical processes and information to derive conclusions about anomalies (past, present, or future) must be applied to event data and appropriate response actions must be taken.
P.DETECT	Static configuration information that might be indicative of the potential for a future anomaly or the occurrence of a past anomaly must be collected.
P.MANAGE	The TOE shall only be managed by authorized users.
P.ACCESS	All data analyzed and generated by the TOE shall only be used for authorized purposes.
P.ACCACT	Users of the TOE shall be accountable for their actions within the EAN.
P.INTGTY	Data analyzed and generated by the TOE shall be protected from modification.
P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of analysis and response activities.

3.3 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. The following specific conditions are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 5 – Assumptions

Name	Description
A.ACCESS	The TOE has access to all the IT System resources necessary to perform its functions.
A.CRYPTOGRAPHY	The TOE environment will provide cryptographic functionality for collection protocols and web browsers when needed.
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

Name	Description
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.NOTRST	The TOE can only be accessed by authorized users.
A.ENV_PRTCTN	The TOE environment will provide the necessary authentication mechanisms and firewall rules to prevent unauthorized access to the operating system the TOE is installed on and the network attached storage the TOE uses.
A.DATA_STG	The TOE environment will provide reliable storage for event data collected and used by the TOE.
A.TIME	The IT Environment will provide reliable time stamps to the TOE.
A.NETSEC	The TOE environment will provide sufficient protection against disclosure of sensitive data while it is being transmitted between separate TOE components or between TOE components and trusted IT entities. The level of protection will be appropriate to the environment where the TOE is placed.

4 Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 3). The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment.

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are as follows:

Table 6 – Security Objectives for the TOE

Name	Description
O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
O.IDACTS	The TOE must accept data from EAN Collectors and then apply analytical processes and information to derive conclusions about logged events.
O.RESPON	The TOE must respond appropriately to analytical conclusions.
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.IDAUTH	The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions and data.
O.AUDITS	The TOE must record audit records for data accesses and use of the EAN functions.
O.INTEGR	The TOE must ensure the integrity of all audit and event data.

4.2 Security Objectives for the Operational Environment

The following security objectives are to be satisfied by the environment:

Table 7 – Environmental Security Objectives

Name	Description
OE.TIME	The IT Environment will provide reliable timestamps to the TOE.
OE.AUDIT_PROTECTION	The IT Environment will provide the capability to protect audit information.
OE.AUDIT_SORT	The IT Environment will provide the capability to sort the audit information.

Name	Description
OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
OE.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
OE.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
OE.CRYPTOGRAPHY	The cryptographic functionality for cryptography-based collection protocols and for the web browsers used by TOE users is provided by the environment.
OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the EAN.
OE.INTROP	The TOE is interoperable with the IT Systems it monitors and other components used by the TOE that exist outside of the TOE boundary.
OE.OS_AUTH	The IT Environment will provide authentication for scheduled tasks, local storage on each appliance, network access to Sybase, and users attempting to run CLI utilities that can be run without authenticating with the TOE.
OE.FIREWALL	The IT Environment will provide a firewall configured to block network ports that allow unauthorized access to the network attached storage and functions on the TOE.
OE.DATA_STG	The IT Environment will provide adequate storage for event data collected and used by the TOE so that data is not lost or overwritten.
OE.NETSEC	The IT Environment will provide protection for TOE data being transmitted between separate TOE components and between trusted IT entities and TOE components. The level of protection will be appropriate to the environment.

5 Extended Components Definition

This section defines the extended SFRs and extended SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

5.1 Extended TOE Security Functional Components

This section specifies the extended SFRs for the TOE. The extended SFRs are organized by class. Table 8 identifies all extended SFRs implemented by the TOE

Table 8 – Extended TOE Security Functional Requirements

Name	Description
EAN_ANL.1 (EXP)	Analyzer analysis
EAN_COL.1 (EXP)	Event data collection
EAN_RCT.1 (EXP)	Analyzer react
EAN_RDR.1 (EXP)	Restricted data review

5.1.1 Class EAN: EAN Component Requirements

EAN Component Requirements involve functions that apply to an EAN system. The EAN Component Requirements function class was modeled after the CC FAU: Security audit class. The extended family EAN _ANL: Analyzer analysis was modeled after the CC family FAU_SAA: Security audit analysis. The extended family EAN_COL: Event data collection was modeled after the CC family FAU_GEN: Security audit data generation. The extended family and related components for EAN _RCT: Analyzer react were modeled after the CC family and related components for FAU_ARP: Security audit automatic response. The extended family and related components for EAN _RDR: Restricted data review were modeled after the CC family and related components for FAU_SAR: Security audit review.

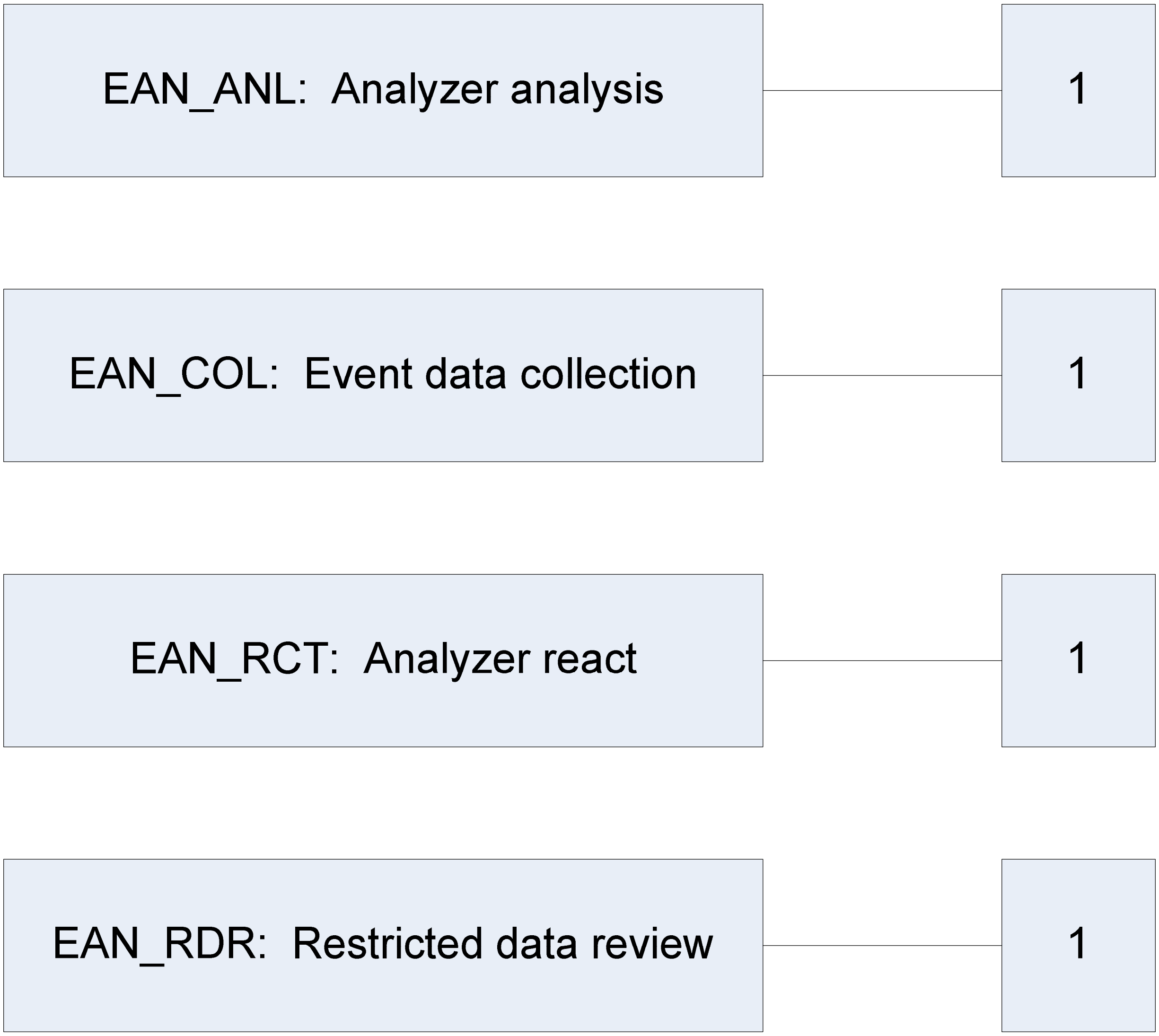
EAN_ANL: Analyzer analysis
1
EAN_COL: Event data collection
1
EAN_RCT: Analyzer react
1
EAN_RDR: Restricted data review
1

Figure 5 – EAN: EAN Component Requirements Class Decomposition

5.1.1.1 Analyzer analysis (EAN _ANL)

Family Behaviour

This family defines the requirements for what analytical functions the TOE can perform on event data.

Component Leveling

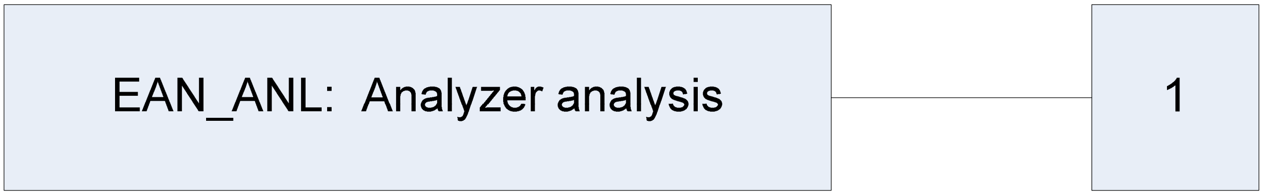

Figure 6 – EAN Analyzer analysis family decomposition

EAN _ANL.1 (EXP), Analyzer analysis, provides the capability to perform analytical functions on the event data.

Management: EAN _ANL.1 (EXP)

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

- Management of the event data by defining rules and filters to include or exclude data from the data being analyzed.

Audit: EAN _ANL.1 (EXP)

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

- Minimal: Enabling or disabling of any of the analysis mechanisms;
- Minimal: Automated responses performed by the tool.

EAN _ANL.1 Analyzer analysis (EXP)

Hierarchical to: No other components

Dependencies: No dependencies

This component defines the types of analytical functions that can be performed on event data.

EAN _ANL.1.1 (EXP)

The TSF shall be capable of performing the following reporting function(s) on event data received from non-TOE sources:

a) [selection: *detailed reports*]; and

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

EAN _ANL.1.2 (EXP)

The TSF shall be capable of recording within each detailed report:

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

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

5.1.1.2 Event data collection (EAN _COL)

Family Behaviour

This family defines the requirements for what event data the TOE can collect.

Component Leveling

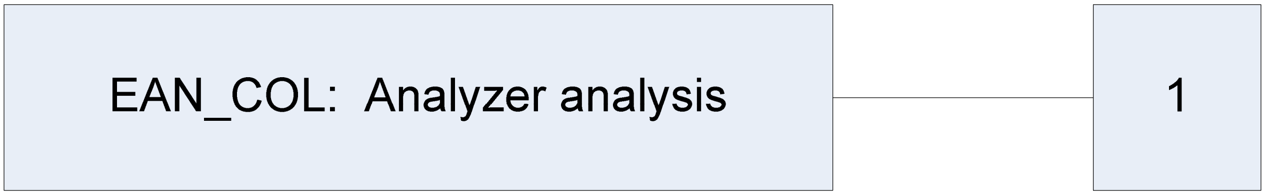

Figure 7 – EAN Event data collection family decomposition

EAN _COL.1 (EXP), Event data collection, provides the capability to collect event data.

Management: EAN _COL.1 (EXP)

There are no management activities foreseen.

Audit: EAN _COL.1 (EXP)

There are no auditable events foreseen.

EAN _COL.1 Event data collection (EXP)

Hierarchical to: No other components

Dependencies: No dependencies

This component defines the types of event data that the TOE can collect.

EAN _COL.1.1 (EXP)

The TSF shall be able to collect event data via the following protocols: [assignment: *list of protocols*].

5.1.1.3 Analyzer react (EAN _RCT)

Family Behaviour

This family defines the requirements for how the TOE reacts to anomalies detected during statistical analysis of event data.

Component Leveling

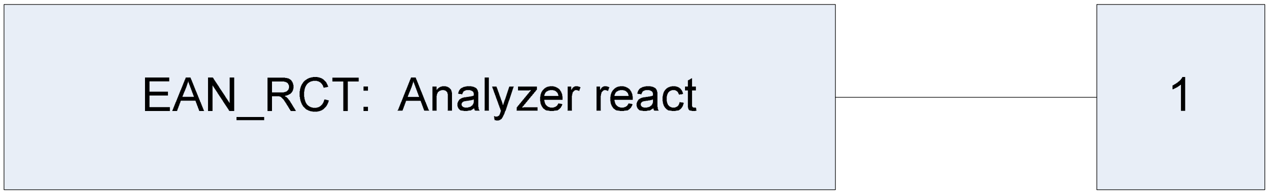

Figure 8 –Analyzer react family decomposition

EAN _RCT.1 (EXP), Analyzer react, defines the requirements for how the TOE reacts to anomalies detected during statistical analysis of event data.

Management: EAN _RCT.1 (EXP)

- The management (addition, removal, or modification) of actions.

Audit: EAN _RCT.1 (EXP)

- Minimal: Actions taken due to potential security violations.

EAN _RCT.1 Analyzer react (EXP)

Hierarchical to: No other components

Dependencies: EAN _RCT.1 (EXP)

This component defines the requirements for how the TOE reacts to anomalies detected during statistical analysis of event data.

EAN _RCT.1.1 (EXP)

The TSF shall be capable of generating an alert and taking [assignment: *appropriate actions*] when an anomaly is detected.

5.1.1.4 Restricted Data Review (EAN _RDR)

Family Behaviour

This family defines the requirements for who can access event data and ensures that event data is formatted in a manner suitable for the user to interpret the information.

Component Leveling

Figure 9 –Analyzer react family decomposition

EAN _RDR.1 (EXP), Restricted data review, defines the requirements for who can access event data and ensures that event data is formatted in a manner suitable for the user to interpret the information.

Management: EAN _RDR.1 (EXP)

- Maintenance (deletion, modification, addition) of the group of users with read access right to the event data.

Audit: EAN _RDR.1 (EXP)

- Basic: Reading of information from the event data.

EAN _RDR.1 Restricted Data Review (EXP)

Hierarchical to: No other components

Dependencies: No dependencies

This component defines the requirements for who can access event data and ensures that event data is formatted in a manner suitable for the user to interpret the information.

EAN _RDR.1.1 (EXP)

The Analyzer shall provide [assignment: *authorized users*] with the capability to read [assignment: *list of event data*] from the event data.

EAN _RDR.1.2 (EXP)

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

EAN _RDR.1.3 (EXP)

The Analyzer shall prohibit all users read access to the event data, except those users that have been granted explicit read-access.

5.2 Extended TOE Security Assurance Components

There are no extended SARs defined for this evaluation of the TOE.

6 Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

6.1 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the Security Target reader.

The CC allows for assignment, refinement, selection and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Parts 2 and 3 of the CC, and are shown as follows:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [<u>*underlined italicized text within brackets*</u>].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Extended Functional and Assurance Requirements are identified using "EXT_" at the beginning of the short name.
- Iterations are identified by appending a letter in parentheses following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 9 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 9 – TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit data generation	✓	✓		
FAU_SAR.1	Audit review		✓		
FAU_SAR.2	Restricted audit review				
FAU_SAR.3	Selectable audit review		✓		
FIA_AFL.1	Authentication failure handling	✓	✓		
FIA_ATD.1	User attribute definition		✓		
FIA_UAU.1	User authentication before any action		✓	✓	
FIA_SOS.1	Verification of Secrets		✓		
FIA_UID.1	User identification before any action		✓		
FMT_MOF.1	Management of security functions behaviour	✓	✓		

Name	Description	S	A	R	I
FMT_MTD.1	Management of TSF data	✓	✓		
FMT_SMF.1	Specification of Management Functions		✓		
FMT_SMR.1	Security roles		✓		
FPT_FLS.1	Failure with preservation of secure state		✓		
FRU_FLT.1	Degraded fault tolerance		✓		
FTA_TAB.1	TOE Access Banners				
EAN_ANL.1 (EXP)	Analyzer analysis	✓	✓		
EAN_COL.1 (EXP)	Event data collection		✓		
EAN_RCT.1 (EXP)	Analyzer react		✓		
EAN_RDR.1 (EXP)	Restricted data review		✓		

Note: S=Selection; A=Assignment; R=Refinement; I=Iteration

6.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

FAU_GEN.1.1

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

- Start-up and shutdown of the audit functions;
- All auditable events, for the [*not specified*] level of audit; and
- [*Logout, Login, View – add, View – delete, View – modify, CorrelationRule – add, CorrelationRule – delete, CorrelationRule – modify, Report – add, Report – delete, Report – modify, User – add, User – delete, User – modify*].

FAU_GEN.1.2

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

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*identification of the event source, severity*].

Dependencies: FPT_STM.1 Reliable time stamps

FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1

The TSF shall provide [*administrators*] 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.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

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.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

FAU_SAR.3.1

The TSF shall provide the ability to apply [*selection*] of audit data based on [*date and time, event category, and severity level of the event*].

Dependencies: FAU_SAR.1 Audit review

6.2.2 Class FIA: Identification and Authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

FIA_AFL.1.1

The TSF shall detect when [*a settable, non-zero number of*] unsuccessful authentication attempts occur related to [*a user attempting to authenticate*].

FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been [*met*], the TSF shall [*disable the user's account*].

Dependencies: FIA_UAU.1 Timing of authentication

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual users:

[

a) User identity;

b) Authentication data;

c) Authorizations; and

d) Group memberships.

].

Dependencies: No dependencies

FIA_SOS.1 Verification of Secrets

Hierarchical to: No other components.

FIA_SOS.1.1

The TSF shall provide a mechanism to verify that secrets meet [*an administrator-configurable password-strength policy*].

Dependencies: No dependencies

FIA_UAU.1 Timing of authentication

Hierarchical to: FIA_UAU.1 Timing of authentication

FIA_UAU.1.1

The TSF shall allow [*use of Command Line Interface (CLI) utilities by a user who has authenticated to the appliance operating system*] on behalf of the user to be performed before the user is authenticated **to the TOE**.

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.

Dependencies: FIA_UID.1 Timing of identification

FIA_UID.1 Timing of identification

Hierarchical to: No other components

FIA_UID.1.1

The TSF shall allow [*use of CLI utilities by a user who has authenticated to the appliance operating system*] 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.

Dependencies: No dependencies

6.2.3 Class FMT: Security Management

FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

FMT_MOF.1.1

The TSF shall restrict the ability to [*modify the behaviour of*] the functions [*the functions listed in the ‘Functions’ column of Table 10, restricted by the ‘Permissions’ column of Table 10*] to [*the roles listed in the ‘Role’ column of Table 10*].

Table 10 – Management Rules for Analysis and Reaction behavior

Role	Functions	Permissions
Users	• Reports	• Run, create, modify, and delete
	• Scheduled reports	• View
	• Alerts	• View
	• Rules	• Create, modify, and delete
	• Output actions	• Create, modify, and delete
Administrators	• Scheduled reports	• Schedule
	• Views	• Create, modify, and delete
	• Enterprise Dashboard collections	• Create, modify, and delete
	• Enterprise Dashboard	• Set up
	• Real-Time Details	• Set up

*Permissions applicable to users must be assigned by an administrator. All permissions applicable to administrators are always granted to all administrators.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1

The TSF shall restrict the ability to [*perform the actions listed in the 'Permissions' column of Table 11*] the [*types of data listed in the 'Type of Data' column of Table 11*] to [*the roles listed in the 'Role' column of Table 11*].

Table 11 – TOE Data Management

Role	Type of Data	Permissions
Users	• Watchlists	• Create, modify, and delete
Administrators	• Users	• Create, modify, and delete
	• User Groups	• Create, modify, and delete
	• Devices	• Create, modify, and delete
	• Device groups	• Create, modify, and delete
	• Message definitions	• Create, modify, and delete
	• Audit and Event data	• Create, modify, and delete

*Permissions applicable to users must be assigned by an administrator. All permissions applicable to administrators are always granted to all administrators.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions: [*Management of security function behaviour, management of TSF data*].

Dependencies: No Dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1

The TSF shall maintain the roles [*administrators, users with custom defined permissions*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

6.2.4 Class FPT: Protection of the TSF

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

FPT_FLS.1.1

The TSF shall preserve a secure state when the following types of failures occur: [*in an LS configuration, failure of an Application Server or Database Server appliance; in an ES configuration, shutdown of the NIC Web Server or NIC Server service*].

Dependencies: No dependencies

6.2.5 Class FRU: Resource Utilization

FRU_FLT.1 Degraded fault tolerance

Hierarchical to: No other components.

FRU_FLT.1.1

The TSF shall ensure the operation of [*collection of event data*] when the following failures occur: [*in an LS configuration, failure of an Application Server or Database Server appliance; in an ES configuration, shutdown of the NIC Web Server or NIC Server service*].

Dependencies: FPT_FLS.1 Failure with preservation of secure state

6.2.6 Class FTA: TOE Access

FTA_TAB.1 Default TOE access banners

Hierarchical to: No other components.

FPT_TAB.1.1

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

Dependencies: No dependencies

6.2.7 Class EAN: EAN Component Requirements (EXP)

EAN_ANL.1 Analyzer analysis (EXP)

Hierarchical to: No other components

EAN _ANL.1.1 (EXP)

The TSF shall be capable of performing the following reporting function(s) on event data received from non-TOE sources:

a) [*detailed reports*]; and

b) [*no other analytical functions*].

EAN _ANL.1.2 (EXP)

The TSF shall be capable of recording within each detailed report:

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

b) [*no other information*]

Dependencies: No dependencies

EAN_COL.1 Event data collection (EXP)

Hierarchical to: No other components

EAN _COL.1.1 (EXP)

The TSF shall be able to collect event data via the following protocols: [*syslog, SNMP, ODBC, SFTP, HTTPS, and Microsoft Windows Event Collection*].

Dependencies: No dependencies

EAN_RCT.1 Analyzer react (EXP)

Hierarchical to: No other components

EAN _RCT.1.1 (EXP)

The TSF shall be capable of executing output actions of various types , including: [

- *SNMP Trap notification*
- *Simple Mail Transport Protocol (SMTP) Email alert notification*
- *Simple Network Paging Protocol (SNPP) Pager alert notification*
- *Writing alerts to a text file (accessed through the operating system)*

- *Syslog redirects of alerts to another system as Syslog messages*
- *Script execution when an alert is triggered*
- *Send alert to task triage*[6]
- *Send alert to task triage for automatic escalation*
- *America Online (AOL) instant messenger*

] when an anomaly is detected.

Dependencies: EAN _ANL.1 (EXP)

EAN_RDR.1 Restricted Data Review (EXP)

Hierarchical to: No other components

EAN _RDR.1.1 (EXP)

The Analyzer shall provide [*administrators and users authorized with assigned permissions*] with the capability to read [*event data stored in the database*] from the event data.

EAN _RDR.1.2 (EXP)

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

EAN _RDR.1.3 (EXP)

The Analyzer shall prohibit all users read access to the event data, except those users that have been granted explicit read-access.

Dependencies: No dependencies

[6] Task Triage integrates enVision with external trouble ticket systems, but is excluded from the TOE.

6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL3 augmented with ALC_FLR.2. Table 12 – Assurance Requirements summarizes the requirements.

Table 12 – Assurance Requirements

Assurance Requirements	
Class ALC : Life Cycle Support	ALC_CMC.3 Authorisation controls
	ALC_CMS.3 Implementation representation CM coverage
	ALC_DEL.1 Delivery Procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_FLR.2 Flaw Reporting Procedures
Class ADV: Development	ADV_ARC.1 Security Architecture Description
	ADV_FSP.3 Functional specification with complete summary
	ADV_TDS.2 Architectural design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

7 TOE Summary Specification

This section presents information to detail how the TOE meets the functional requirements described in previous sections of this ST.

7.1 TOE Security Functions

Each of the security requirements and the associated descriptions correspond to the security functions. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions satisfy the necessary requirements.

Table 13 – Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
Security Audit	FAU_GEN.1	Audit data generation
	FAU_SAR.1	Audit review
	FAU_SAR.2	Restricted audit review
	FAU_SAR.3	Selectable audit review
Identification and Authentication	FIA_AFL.1	Authentication failure handling
	FIA_ATD.1	User attribute definition
	FIA_UAU.1	User authentication before any action
	FIA_SOS.1	Verification of Secrets
	FIA_UID.1	User identification before any action
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
Protection of the TSF	FPT_FLS.1	Failure with preservation of secure state
Resource Utilization	FRU_FLT.1	Degraded fault tolerance
TOE Access	FTA_TAB.1	TOE Access Banners
EAN Component Requirements	EAN_ANL.1 (EXP)	Analyzer analysis
	EAN_COL.1 (EXP)	Event data collection

TOE Security Function	SFR ID	Description
	EAN_RCT.1 (EXP)	Analyzer react
	EAN_RDR.1 (EXP)	Restricted data review

7.1.1 Security Audit

FAU_GEN.1

The TOE Logger Service generates audit logs that contain the following information:

- Date and time of the event;
- Type of event;
- Subject identity (if applicable,
- Outcome (success of failure) of the event,
- Identification of the event source,
- Severity.

The TOE records startup and shutdown of the audit function, logout, login, management of views, management of correlation rules, management of reports, management of users.

FAU_SAR.1, FAU_SAR.2, FAU_SAR.3

The TOE provides the audit logs for administrators to review in a format suitable for the administrators to interpret the information in the logs. The logs are available via a web GUI. Administrators can select the audit data based on the date and time, event category, and severity level of the event. Only authorized administrators are permitted to view the audit records.

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_SAR.1, FAU_SAR.2, FAU_SAR.3.

7.1.2 Identification and Authentication

FIA_AFL.1

The TOE implements an account locking mechanism. If a user makes (an administrator-defined) number of unsuccessful authentication attempts, the TOE disables the user account. The user can only successfully log in again after an administrator re-enables the user's account.

FIA_ATD.1

The TOE authenticates users and administrators who attempt to connect via the web GUI. Users and administrators authenticate with a login ID and password combination. The TOE stores IDs, hashed passwords, and permissions for users and groups in a local database.

FIA_SOS.1

The TOE enforces minimum password complexity requirements for administrator and user passwords. The password policy is administrator-configurable through editing a configuration file. The configuration file is edited with a text editor that is provided by the operating system.

FIA_UAU.1, FIA_UID.1

Users and administrators can access local storage on the appliance and run CLI utilities before the TOE identifies and authenticates them. Before performing any of these actions, the user or administrator must authenticate with the operating system the TOE is installed on. Authentication must take place before administrators can perform any actions on the web GUI.

TOE Security Functional Requirements Satisfied: FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.1, FIA_UID.1.

7.1.3 Security Management

FMT_MOF.1

The TOE is managed by individuals who can have one of two default roles, or an administrator-assigned set of custom permissions. The two default roles are administrator and users with limited privileges. Users can be assigned to customized groups and gain the permissions of groups they are assigned to. Individual permissions (applying to single users) override group permissions.

FMT_MTD.1

TOE administrators can assign permissions for who can query and add event and audit data. Only administrators can manage user permissions.

FMT_SMF.1, FMT_SMR.1

The TOE maintains the roles administrator, users with limited privileges, and a large number of customized users and groups with granular permissions. Users are associated with their roles and sets of permissions during authentication. Administrators can manage security function behavior and TSF data.

TOE Security Functional Requirements Satisfied: FMT_MOF.1, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1.

7.1.4 Protection of the TSF

FPT_FLS.1

The TOE preserves a secure state upon failure of an A-SRV or D-SRV. The secure state is preserved by maintaining the collection of event data at the LC.

TOE Security Functional Requirements Satisfied: FPT_FLS.1.

7.1.5 Resource Utilization

FRU_FLT.1

The TOE ensures the operation of collection of event data upon failure of an A-SRV or D-SRV.

TOE Security Functional Requirements Satisfied: FRU_FLT.1.

7.1.6 TOE Access

The TOE presents an access banner for individuals attempting to connect to the TOE that advises against unauthorized access. Administrators edit the access banner in a configuration file with a text editor that is provided by the operating system.

TOE Security Functional Requirements Satisfied: FTA_TAB.1.

7.1.7 EAN Component Requirements

EAN **_ANL.1**

The TOE can generate detailed reports from event data received from monitored systems. The TOE records the identification of the data source, date and time of the result, and the event category for each report.

EAN_COL.1

The TOE collects event data from various monitored systems using various protocols including: syslog, SNMP, ODBC, SFTP, HTTPS, and Microsoft Windows Event Collection. The TOE sends the data to the NAS for storage.

EAN **_RCT.1**

The TOE can detect anomalies in event data by comparing the data against a set of administrator-defined rules. Administrators can configure the rules so that the TSF takes administrator-defined actions in response to detection of an anomaly. This response includes alerts sent in a variety of manners, including email notification, pager notification, SNMP trap notification, and Syslog message notification.

EAN **_RDR.1**

Administrators can set permissions denying or granting user access to view event data. The event data is provided to the administrators through the web GUI in a manner that is easily interpreted. If a user does not have permission to view data, the TSF prevents that user from accessing the data.

TOE Security Functional Requirements Satisfied: EAN_ANL.1, EAN_COL.1, EAN_RCT.1, EAN_RDR.1.

8 Rationale

Section eight describes the rationale of this Security Target.

8.1 Conformance Claims Rationale

This Security Target extends Part 2 and conforms to part 3 of the Common Criteria Standard for Information Technology Security Evaluations, version 3.1 revision 2. Extended requirements from the EAN class are based on SFRs from the Security Audit (FAU) class.

8.2 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target. Sections 8.2.1, 8.2.2, and 8.2.3 demonstrate the mappings between the threats, polices, and assumptions to the security objectives is complete. The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

8.2.1 Security Objectives Rationale Relating to Threats

The following table describes the mapping of threats to objectives.

Table 14 – Threats:Objectives Mapping

Threats	Objectives	Rationale
T.COMINT An unauthorized person may attempt to compromise the integrity of the data analyzed and produced by the TOE by bypassing a security mechanism.	O.PROTCT The TOE must protect itself from unauthorized modifications and access to its functions and data.	The O.PROTCT objective addresses this threat by providing TOE self-protection.
	O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data.
	O.IDAUTH The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions and data.	The O.IDAUTH objective provides for authentication of users prior to any TOE data access.
	O.INTEGR The TOE must ensure the integrity of all audit and event data.	The O.INTEGR objective ensures no TOE data will be modified by unauthorized individuals.
T.COMDIS An unauthorized person may attempt to disclose the data analyzed and produced by the TOE by bypassing a security mechanism.	O.PROTCT The TOE must protect itself from unauthorized modifications and access to its functions and data.	The O.PROTCT objective addresses this threat by providing TOE self-protection.
	O.ACCESS The TOE must allow authorized users to access only appropriate TOE	The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access

Threats	Objectives	Rationale
	functions and data.	TOE data.
	O.IDAUTH The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions and data.	The O.IDAUTH objective provides for authentication of users prior to any TOE data access.
T.LOSSOF An unauthorized person may attempt to remove or destroy data analyzed and produced by the TOE.	O.PROTCT The TOE must protect itself from unauthorized modifications and access to its functions and data.	The O.PROTCT objective addresses this threat by providing TOE self-protection.
	O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data.
	O.IDAUTH The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions and data.	The O.IDAUTH objective provides for authentication of users prior to any TOE data access.
	O.INTEGR The TOE must ensure the integrity of all audit and event data.	The O.INTEGR objective ensures no TOE data will be deleted by unauthorized individuals.
T.NOHALT An unauthorized person may attempt to compromise the continuity of the TOEs analysis functionality by halting execution of the TOE.	O.IDACTS The TOE must accept data from EAN Collectors and then apply analytical processes and information to derive conclusions about logged events.	The O.IDACTS objective addresses this threat by requiring the TOE to collect all events, including those attempts to halt the TOE.
	O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.
	O.IDAUTH The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions and data.	The O.IDAUTH objective provides for authentication of users prior to any TOE function access.
T.PRIVIL An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.	O.PROTCT The TOE must protect itself from unauthorized modifications and access to its functions and data.	The O.PROTCT objective addresses this threat by providing TOE self-protection.
	O.ACCESS The TOE must allow authorized users to access only appropriate TOE	The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access

Threats	Objectives	Rationale
	functions and data.	TOE functions.
	O.IDAUTH The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions and data.	The O.IDAUTH objective provides for authentication of users prior to any TOE function access.
T.IMPCON The TOE may be susceptible to improper configuration by an authorized or unauthorized person causing potential anomalies to go undetected.	O.EADMIN The TOE must include a set of functions that allow effective management of its functions and data.	The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product.
	OE.INSTAL Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.	The OE.INSTAL objective states that authorized administrators will install and configure the TOE properly.
	O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	The O.ACCESS objective only permits authorized users to access TOE functions for which they are authorized.
	O.IDAUTH The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions and data.	The O.IDAUTH objective provides for authentication of users prior to any TOE function access.
T.FALACT The TOE may fail to react to identified or suspected vulnerabilities to itself and monitored systems by external adversaries or inappropriate activity performed on it by TOE users or adversaries.	O.RESPON The TOE must respond appropriately to analytical conclusions.	The O.RESPON objective ensures the TOE reacts to analytical conclusions about suspected vulnerabilities or inappropriate activity.
T.FALREC The TOE may fail to recognize vulnerabilities or inappropriate activity based on event data received from each data source.	O.IDACTS The TOE must accept data from EAN Collectors and then apply analytical processes and information to derive conclusions about logged events.	The O.IDACTS objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from a data source.
T.FALASC The TOE may fail to identify vulnerabilities or inappropriate activity based on association of event data received from all data sources.	O.IDACTS The TOE must accept data from EAN Collectors and then apply analytical processes and information to derive conclusions about logged events.	The O.IDACTS objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from multiple data sources.

Every Threat is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives counter all defined threats.

8.2.2 Security Objectives Rationale Relating to Policies

The following table describes the mapping of policies to objectives.

Table 15 – Policies:Objectives Mapping

Policies	Objectives	Rationale
P.ANALYZ Analytical processes and information to derive conclusions about anomalies (past, present, or future) must be applied to event data and appropriate response actions must be taken.	O.IDACTS The TOE must accept data from EAN Collectors and then apply analytical processes and information to derive conclusions about logged events.	The O.IDACTS objective requires analytical processes be applied to data collected by the EAN.
P.DETECT Static configuration information that might be indicative of the potential for a future anomaly or the occurrence of a past anomaly must be collected.	OE.TIME The IT Environment will provide reliable timestamps to the TOE.	The OE.TIME objective addresses this policy by ensuring that the audit records and event data will have reliable time stamps.
	O.IDACTS The TOE must accept data from EAN Collectors and then apply analytical processes and information to derive conclusions about logged events.	The O.IDACTS objective addresses this policy by requiring collection of event data.
	O.AUDITS The TOE must record audit records for data accesses and use of the EAN functions.	The O.AUDITS objective addresses this policy by requiring collection of audit data.
P.MANAGE The TOE shall only be managed by authorized users.	O.PROTCT The TOE must protect itself from unauthorized modifications and access to its functions and data.	The O.PROTCT objective ensures the TOE will be protected from unauthorized modifications and access to its functions and data..
	O.EADMIN The TOE must include a set of functions that allow effective management of its functions and data.	The O.EADMIN objective ensures there is a set of functions for administrators to use.
	OE.INSTAL Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.	The OE.INSTAL objective supports the P.MANAGE policy by ensuring the TOE is properly installed, managed, and operated, and administrators follow all provided documentation and procedures to maintain the security posture of the TOE.
	O.ACCESS The TOE must allow authorized users	The O.ACCESS objective builds upon the O.IDAUTH objective by only

Policies	Objectives	Rationale
	to access only appropriate TOE functions and data.	permitting authorized users to access TOE functions.
	O.IDAUTH The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions and data.	The O.IDAUTH objective provides for authentication of users prior to any TOE function access.
	OE.CREDEN Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.	The OE.CREDEN objective requires administrators to protect all authentication data.
	OE.PERSON Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the EAN.	The OE.PERSON objective ensures competent administrators will manage the TOE.
P.ACCESS All data analyzed and generated by the TOE shall only be used for authorized purposes.	O.PROTCT The TOE must protect itself from unauthorized modifications and access to its functions and data.	The O.PROTCT objective provides for TOE self-protection.
	OE.AUDIT_PROTECTION The IT Environment will provide the capability to protect audit information.	The OE.AUDIT_PROTECTION objective shall protect audit data.
	O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.
	O.IDAUTH The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions and data.	The O.IDAUTH objective provides for authentication of users prior to any TOE function access.
P.ACCACT Users of the TOE shall be accountable for their actions within the EAN.	OE.TIME The IT Environment will provide reliable timestamps to the TOE.	OE.TIME will provide a time stamp for each audit message.
	OE.AUDIT_SORT The IT Environment will provide the capability to sort the audit information.	The OE.AUDIT_SORT objective provides the capability to sort the audit information. This allows administrators to more easily find accountability information.
	O.IDAUTH The TOE must be able to identify and authenticate authorized users prior to	The O.IDAUTH objective supports this objective by ensuring each user is uniquely identified and authenticated.

Policies	Objectives	Rationale
	allowing access to TOE functions and data.	
	O.AUDITS The TOE must record audit records for data accesses and use of the EAN functions.	The O.AUDITS objective implements this policy by requiring auditing of all data accesses and use of TOE functions.
P.INTGTY Data analyzed and generated by the TOE shall be protected from modification.	O.INTEGR The TOE must ensure the integrity of all audit and event data.	The O.INTEGR objective ensures the protection of data from modification.
P.PROTCT The TOE shall be protected from unauthorized accesses and disruptions of analysis and response activities.	OE.PHYCAL Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.	The OE.PHYCAL objective protects the TOE from unauthorized physical modifications.

Every policy is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives enforce all defined policies.

8.2.3 Security Objectives Rationale Relating to Assumptions

The following table describes the mapping of assumptions to objectives.

Table 16 – Assumptions:Objectives Mapping

Assumptions	Objectives	Rationale
A.ACCESS The TOE has access to all the IT System resources necessary to perform its functions.	OE.INTROP The TOE is interoperable with the IT Systems it monitors and other components used by the TOE that exist outside of the TOE boundary.	The OE.INTROP objective ensures the TOE has the needed access to the IT Systems it monitors and other components used by the TOE that exist outside of the TOE boundary.
A.CRYPTOGRAPHY The TOE environment will provide cryptographic functionality for collection protocols and web browsers when needed.	OE.CRYPTOGRAPHY The cryptographic functionality for cryptography-based collection protocols and for the web browsers used by TOE users is provided by the environment.	The OE.CRYPTOGRAPHY objective supports this assumption by requiring that all cryptography for collection protocols and web browsers occur in the environment.
A.PROTCT The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.	OE.PHYCAL Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.	The OE.PHYCAL objective provides for the physical protection of the TOE hardware and software.
A.LOCATE	OE.PHYCAL	The OE.PHYCAL objective provides

Assumptions	Objectives	Rationale
The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.	for the physical protection of the TOE.
A.MANAGE There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.	OE.PERSON Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the EAN.	The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.
A.NOEVIL The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.	OE.INSTAL Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.	The OE.INSTAL objective ensures that the TOE is properly installed and operated.
	OE.PHYCAL Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.	The OE.PHYCAL objective provides for physical protection of the TOE by authorized administrators.
	OE.CREDEN Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.	The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.
A.NOTRST The TOE can only be accessed by authorized users.	OE.PHYCAL Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.	The OE.PHYCAL objective provides for physical protection of the TOE to protect against unauthorized access.
	OE.CREDEN Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.	The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.
A.ENV_PRTCTN The TOE environment will provide the necessary authentication mechanisms and firewall rules to prevent unauthorized access to the operating system the TOE is installed on and the network attached storage the TOE uses.	OE.OS_AUTH The IT Environment will provide authentication for scheduled tasks, local storage on each appliance, network access to Sybase, and users attempting to run CLI utilities that can be run without authenticating with the TOE.	The OE.OS_AUTH objective supports this assumption by ensuring that the operating system that the TOE is installed on will require authentication before allowing users to perform any actions.
	OE.FIREWALL The IT Environment will provide a firewall configured to block network	The OE.FIREWALL objective supports this assumption by preventing unauthorized access from vulnerable

Assumptions	Objectives	Rationale
	ports that allow unauthorized access to the network attached storage and functions on the TOE.	network ports.
A.DATA_STG The TOE environment will provide reliable storage for event data collected and used by the TOE.	OE.DATA_STG The IT Environment will provide adequate storage for event data collected and used by the TOE so that data is not lost or overwritten.	The OE.DATA_STG objective supports this assumption by requiring reliable storage of event data collected and used by the TOE.
A.TIME The IT Environment will provide reliable time stamps to the TOE.	OE.TIME The IT Environment will provide reliable timestamps to the TOE.	The OE.TIME objective supports this assumption by requiring reliable time stamps to be available for the TOE's use.
A.NETSEC The TOE environment will provide sufficient protection against disclosure of sensitive data while it is being transmitted between separate TOE components or between TOE components and trusted IT entities. The level of protection will be appropriate to the environment where the TOE is placed.	OE.NETSEC The IT Environment will provide protection for TOE data being transmitted between separate TOE components and between trusted IT entities and TOE components. The level of protection will be appropriate to the environment.	The OE.TIME objective supports this assumption by requiring adequate protection from the environment for sensitive information exposed to external entities.

Every assumption is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives uphold all defined assumptions.

8.3 Rationale for Extended Security Functional Requirements

A family of EAN requirements was created to specifically address the data collected and analyzed by an event analyzer. The audit family of the CC (FAU) was used as a model for creating these requirements. The purpose of this family of requirements is to address the unique nature of EAN data and provide for requirements about collecting, reviewing, and managing the data. These requirements have no dependencies since the stated requirements embody all the necessary security functions.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended SARs for this evaluation of the TOE.

8.5 Security Requirements Rationale

The following discussion provides detailed evidence of coverage for each security objective.

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

The following table describes the mapping of objectives to SFRs.

Table 17 – Objectives:SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.PROTCT The TOE must protect itself from unauthorized modifications and access to its functions and data.	FMT_MOF.1 Management of security functions behaviour	The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE.
	FMT_MTD.1 Management of TSF data	Only authorized administrators of the EAN may query and modify event and audit data, and authorized administrators of the TOE may query and modify all other TOE data.
	FMT_SMF.1 Specification of Management Functions	The TOE is required to provide management of security functions behaviour and management of TSF data.
	FPT_FLS.1 Failure with preservation of secure state	FPT_FLS.1 supports this objective by preserving a secure state upon failure of certain TOE components.
	FRU_FLT.1 Degraded fault tolerance	FRU_FLT.1 supports this objective by ensuring that event data is still collected upon failure of certain TOE components.
O.IDACTS The TOE must accept data from EAN Collectors and then apply analytical processes and information to derive conclusions about logged events.	EAN_ANL.1 (EXP) Analyzer analysis	The EAN is required to perform analysis of event data and generate conclusions.
	EAN_COL.1 (EXP) Event data collection	EAN_COL.1 supports this objective by ensuring that the TOE is capable of collecting event data from a variety of protocols.
O.RESPON The TOE must respond appropriately to analytical conclusions.	EAN_RCT.1 (EXP) Analyzer react	The TOE is required to respond appropriately to analytical conclusions.
O.EADMIN The TOE must include a set of functions that allow effective management of its functions and data.	FAU_SAR.1 Audit review	The TOE must provide the ability to review and manage the audit trail of an EAN.
	FAU_SAR.3 Selectable audit review	The TOE must provide the ability to review and manage the audit trail of an EAN.

Objective	Requirements Addressing the Objective	Rationale
	EAN_RDR.1 (EXP) Restricted data review	The EAN must provide the ability for authorized administrators to view the event data.
O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.	FAU_SAR.2 Restricted audit review	The TOE is required to restrict the review of audit data to those granted with explicit read-access.
	FIA_AFL.1 Authentication failure handling	The TOE must protect the management functions from unauthorized access.
	FIA_UAU.1 User authentication before any action	Users authorized to access the TOE are defined using an identification and authentication process.
	FIA_SOS.1 Verification of Secrets	FIA_SOS.1 supports this objective by defining minimum password strength requirements for TOE users and administrators.
	FIA_UID.1 User identification before any action	Users authorized to access the TOE are defined using an identification and authentication process.
	FMT_MOF.1 Management of security functions behaviour	The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE.
	FMT_MTD.1 Management of TSF data	Only authorized administrators of the EAN may query and add event and audit data, and authorized administrators of the TOE may query and modify all other TOE data.
	FMT_SMF.1 Specification of Management Functions	The TOE is required to provide the ability to manage security function behaviour and management of TSF data.
	FTA_TAB.1 TOE Access Banners	FTA_TAB.1 supports this objective by notifying unauthenticated individuals that unauthorized access is prohibited.
	EAN_RDR.1 (EXP) Restricted data review	The EAN is required to restrict the review of event data to those granted with explicit read-access.
O.IDAUTH The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions and data.	FAU_SAR.2 Restricted audit review	The TOE is required to restrict the review of audit data to those granted explicit read-access.
	FIA_AFL.1 Authentication failure handling	The TOE is required to protect the management functions and TSF data from unauthorized access.

Objective	Requirements Addressing the Objective	Rationale
	FIA_ATD.1 User attribute definition	Security attributes of subjects used to enforce the authentication policy of the TOE must be defined.
	FIA_UAU.1 User authentication before any action	Users authorized to access the TOE are defined using an identification and authorization process.
	FIA_UID.1 User identification before any action	Users authorized to access the TOE are defined using an identification and authentication process.
	FMT_MOF.1 Management of security functions behaviour	The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE.
	FMT_MTD.1 Management of TSF data	Only authorized administrators of the EAN may query and add event and audit data, and authorized administrators of the TOE may query and modify all other TOE data.
	FMT_SMF.1 Specification of Management Functions	The TOE is required to allow management of the security function behaviour and management of TSF data.
	FMT_SMR.1 Security roles	The TOE must be able to recognize the different administrative and user roles that exist for the TOE.
	EAN_RDR.1 (EXP) Restricted data review	The EAN is required to restrict the review of collected event data to those granted explicit read-access.
O.AUDITS The TOE must record audit records for data accesses and use of the EAN functions.	FAU_GEN.1 Audit data generation	Security-relevant events must be defined and auditable for the TOE.
O.INTEGR The TOE must ensure the integrity of all audit and event data.	FMT_MTD.1 Management of TSF data	Only authorized administrators of the EAN may query or add audit and event data.
	FMT_SMF.1 Specification of Management Functions	The TOE must allow for the management of security function behaviour and management of TSF data.

8.5.2 Security Requirements Rationale for Refinement

There are no refinements of Security Requirements for this evaluation of the TOE.

8.5.3 Security Assurance Requirements Rationale

EAL3+ was chosen to provide a moderate level of assurance that is consistent with good commercial practices. As such minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the EAN may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL3+ the EAN will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

The augmentation of ALC_FLR.2 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

This v4.0 certification is an EAL3, augmented with FLR.2, whereas the previous v3.3 evaluation was an EAL2.

8.5.4 Dependency Rationale

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 18 lists each requirement to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

Table 18 – Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	FPT_STM.1 is not included because time stamps are provided by the environment. An environmental objective states that the TOE will receive reliable time stamps.
FAU_SAR.1	FAU_GEN.1	✓	
FAU_SAR.2	FAU_SAR.1	✓	
FAU_SAR.3	FAU_SAR.1	✓	
FIA_AFL.1	FIA_UAU.1	✓	
FIA_ATD.1	None	N/A	
FIA_UAU.1	FIA_UID.1	✓	
FIA_SOS.1	None	N/A	
FIA_UID.1	None	N/A	
FMT_MOF.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1	FMT_SMR.1	✓	

SFR ID	Dependencies	Dependency Met	Rationale
	FMT_SMF.1	✓	
FMT_SMF.1	None	N/A	
FMT_SMR.1	FIA_UID.1	✓	
FPT_FLS.1	None	N/A	
FRU_FLT.1	FPT_FLS.1	✓	
FTA_TAB.1	None	N/A	
EAN_ANL.1 (EXP)	None	N/A	
EAN_COL.1(EXP)	None	N/A	
EAN_RCT.1 (EXP)	None	N/A	
EAN_RDR.1 (EXP)	None	N/A	

9 Acronyms and Terminology

9.1.1 Acronyms

Table 19 – Acronyms

Acronym	Definition
A-SRV	Application Server
AOL	America Online
CC	Common Criteria
CEM	Common Evaluation Methodology
CLI	Command Line Interface
CM	Configuration Management
D-SRV	Database Server
EAL	Evaluation Assurance Level
EAN	Event Analyzer
GUI	Graphical User Interface
HTTPS	Secure Hypertext Transfer Protocol
ID	Identifier
IP	Internet Protocol
IPDB	Internet Protocol Data Base
IT	Information Technology
LAN	Local Area Network
LC	Local Collector
NAS	Network Attached Storage
ODBC	Open Database Connectivity

Acronym	Definition
OSP	Organizational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SFTP	Secure File Transfer Protocol
SIEM	Security Information and Event Management
SMTP	Simple Mail Transport Protocol
SNMP	Simple Network Management Protocol
SNPP	Simple Network Paging Protocol
ST	Security Target
TOE	Target of Evaluation
TLS	Transport Layer Security
TSF	TOE Security Functionality
UI	User Interface
U.S.	United States
VAM	Vulnerability and Asset Management
XML	Extensible Markup Language

9.1.2 Terminology

Assets – Information or resources to be protected by the countermeasures of a TOE.

Attack – An attempt to bypass security controls on an IT System. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the IT System and the effectiveness of existing countermeasures.

Audit – The independent examination of records and activities to ensure compliance with established controls, policy, and operational procedures, and to recommend indicated changes in controls, policy, or procedures.

Audit Trail – In an IT System, a chronological record of system resource usage. This includes user login, file access, other various activities, and whether any actual or attempted security violations occurred, legitimate and unauthorized.

Authentication – To establish the validity of a claimed user or object.

Authorized Administrator – A subset of authorized users that manage an EAN component.

Authorized User – A user that is allowed to perform EAN functions and access data.

Availability – Assuring information and communications services will be ready for use when expected.

Compromise – An anomaly into an IT System where unauthorized disclosure, modification, or destruction of sensitive information may have occurred.

EAN component – a collector, database server, or application server.

EAN functions – The active part of the EAN responsible for performing anomaly analysis of information that may be representative of vulnerabilities in and misuse of IT resources, as well as reporting of conclusions.

Evaluation – Assessment of a PP, a ST, or a TOE against defined criteria.

Event data – Data collected by the EAN functions

Information Technology System – May range from a computer system to a computer network.

Integrity – Assuring information will not be accidentally or maliciously altered or destroyed.

IT Product – A package of IT software, firmware, and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems.

Network – Two or more machines interconnected for communications.

Protection Profile – An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Scanner data – Data collected by the Scanner functions.

Scanner functions – The active part of the Scanner responsible for collecting configuration information that may be representative of vulnerabilities in and misuse of IT resources (i.e., Scanner data).

Security – A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences.

Sensor data – Data collected by the Sensor functions.

Sensor functions – The active part of the Sensor responsible for collecting information that may be representative of vulnerabilities in and misuse of IT resources (i.e., Sensor data).

Security Policy – The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

Security Target – A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Target of Evaluation –An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation

Threat – The means through which the ability or intent of a threat agent to adversely affect an automated system, facility, or operation can be manifest. A potential violation of security.

TOE Security Functions – A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy – A set of rules that regulate how assets are managed, protected, and distributed within a TOE.

TSF data – Data created by and for the TOE, that might affect the operation of the TOE.

User – Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

Vulnerability – Hardware, firmware, or software flaw that leaves an IT System open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.