Prism Microsystems EventTracker Version 6.3 Build 93 Security Target

Version 1.6

June 22, 2010

Prism Microsystems, Inc.
8815 Centre Park Drive
Columbia, MD 21045

DOCUMENT INTRODUCTION

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Prism Microsystems EventTracker Version 6.3 Build 93. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

REVISION HISTORY

Rev	Description
1.0	July 15, 2009, Initial release
1.1	October 14, 2009, addressed issues from PETR v1.0
1.2	December 8, 2009, changed version to 6.3 Build 93 and addressed EWA Ors
1.3	January 15, 2010, updates for FSP and TDS consistency
1.4	March 1, 2010, addressed PET-ASE-INT-OR-3 and PET-ASE-INT-OR-2 from CSE
1.5	May 3, 2010, addressed PET-ALC-CMC-OR-1 from EWA
1.6	June 22, 2010 – Final version for submission to EWA

TABLE OF CONTENTS

LIST OF TABLES

ACRONYMS LIST

CC	**Common Criteria**
CM	**Configuration Management**
DBMS	**DataBase Management System**
EAL	**Evaluation Assurance Level**
GB	**Giga Byte**
GUI	**Graphical User Interface**
I&A	**Indentification & Authentication**
IDS	**Intrusion Detection System**
IP	**Internet Protocol**
IPS	**Intrusion Prevention System**
IT	**Information Technology**
OSP	**Organizational Security Policy**
PP	**Protection Profile**
RAM	**Random Access Memory**
SIEM	**Security Information and Event Management**
SIM	**Security Information Management**
SNMP	**Simple Network Management Protocol**
ST	**Security Target**
TCP	**Transmission Control Protocol**
TOE	**Target of Evaluation**
TSC	**TSF Scope of Control**
TSF	**TOE Security Function**
UDP	**User Datagram Protocol**

1. Security Target Introduction

This Security Target (ST) describes the objectives, requirements and rationale for the Prism Microsystems EventTracker Version 6.3 Build 93. The language used in this Security Target is consistent with the *Common Criteria for Information Technology Security Evaluation, Version 3.1*and all international interpretations through September 11, 2009. As such, the spelling of terms is presented using the internationally accepted English.

1.1 Security Target Reference

Prism Microsystems EventTracker Version 6.3 Build 93 Security Target, Version 1.6, June 22, 2010.

1.2 TOE Reference

Prism Microsystems EventTracker Version 6.3 Build 93

1.3 Evaluation Assurance Level

Assurance claims conform to EAL2 (Evaluation Assurance Level 2) augmented by ALC_FLR.2 from the *Common Criteria for Information Technology Security Evaluation*, Version 3.1 Release 3.

1.4 Keywords

Security information and event management, SIEM, security information management, SIM, threats, risk, collection, analysis, correlation.

1.5 TOE Overview

1.5.1 Usage and Major Security Features

EventTracker is an Enterprise-class Security Information and Event Management (SIEM) solution that provides real-time analysis of security information and event feeds from Windows systems and other devices that support the Syslog protocol. EventTracker also accepts batch feeds of event files.

EventTracker performs analysis of the real-time feeds. The feeds are also correlated to detect composite events. Alerts are generated for both single-feed events and composite events according to the configured policy. A cache of recent real-time and composite events is maintained for dashboard displays to administrators.

The events from all the sources (both real-time and batch) as well as composite events are stored in a database for later analysis and reporting. Reports may be used for long-term trend analysis or compliance.

Administrators have the ability to configure policies, display dashboard info for information from the event cache, or run reports and perform analysis of the event database (referred to as the EventVault). Configuration changes and processing of batch files cause audit records to be generated, and administrators may review the audit records. This functionality is provided by application programs executing on the same system that EventTracker is installed on.

1.5.2 TOE type

IDS/IPS (Analyzer)

1.5.3 Required Non-TOE Hardware/Software/Firmware

The TOE is a software application. The hardware, operating system (Windows) and DBMS (Microsoft Access) required by the TOE are part of the operational environment. The TOE also depends on the operational environment to protect the integrity of the communication between the TOE and the remote systems supplying real-time security events to the TOE. The minimum hardware and software requirements for the system hosting EventTracker are specified in the following table.

Table 1 - EventTracker System Hardware/Software Requirements

Item	Requirements
Processor	3 GHz
Memory	1 GB RAM
Hard Disk Free Space	10 GB
Operating System	Windows 2003 Server, Windows 2008 Server
Other Software	Microsoft .NET 2.0 Framework Microsoft Access

The TOE does not perform I&A. The system EventTracker is installed on must perform that function, and control what users have access to the EventTracker executables. EventTracker considers all users with access to it to be a single role – administrators.

The TOE receives security events from external systems, either via real-time feeds (e.g. syslog) or log (batch) files. Those external systems are responsible for generating the security events that are analyzed by the TOE. The network infrastructure used to connect the TOE with those remote systems is also part of the operational environment. The information sent from the external systems should be protected from modification. One mechanism for providing this protection is to use a separate management network with limited access for these interactions, but other mechanisms may be used.

Windows systems do not natively support the syslog protocol. An agent must be used on Windows systems to provide real-time feeds to the TOE. Prism Microsystems provides a Windows agent for this purpose, but that agent is not part of the TOE. Remedial action executable scripts are provided by Prism Microsystems to address specific conditions that may be discovered on Windows systems. Since these scripts are dependent on the Windows agent, they are not part of the TOE.

1.6 Definitions

Table 2 - Definitions

Term	Definition
Alert Event Cache	A cache of events received from real-time feeds, along with any composite events resulting from analysis of the real-time events. This information is used by Administrators when performing analysis via dashboards.
Analyser Data	Security information and event feeds from Windows systems and other devices that support the Syslog protocol, along with analytical results generated from the received data.

Term	Definition
Categories	A set of pre-configured groupings of multiple events (with qualifiers) into categories that are referenced when generating reports. An event may be included in any number of categories.
Composite Event	Event generated by EventTracker based upon rules for event correlation. Composite events are stored in the Alert Event Cache and the EventVault.
Correlation Rules	A set of pre-configured rules for correlation of events of different types or from different sources. If a rule is matched, a new (composite) event is generated.
EventVault	A database of all events (both real-time and batch) received from IT systems, along with any composite events that were generated. This information is used when performing analysis via reports.
Group	A logical grouping of systems. Groups may be referenced when defining reports to quickly select multiple systems. Systems may belong to more than one system group.
Normalized Event	Each event received from a remote IT system (both real-time and batch) is normalized into a standard format used by the TOE. This format is based upon Windows event definitions and contains the following fields: • Date the event occurred • User – the user on the IT system that caused the event to occur (if any) • Computer – the remote IT system on which the event occurred • Category - classification of the event by the event source, primarily used in the security log. • Event ID – TOE-specific identifier for each defined event • Source – Source of the event on the remote IT system • Event Type – Error, Warning, Information, Audit Success, Audit Failure, or Success • Log Type – System, Security, Application, DNS Server, File Replication Service, or Directory Service • Description – Text string providing the details of the event Events received from Windows systems may have all the fields filled in. Events received via syslog have the Date and Computer fields filled in.

1.7 TOE Description

EventTracker is a set of software services and applications that provide functionality to receive and normalize system information and events from remote systems, analyze the information, store the information, and generate reports based on the information. As part of the analysis step, information is correlated to detect specific conditions.

Information is received from remote systems either via real-time feeds (e.g. syslog) or as batch files. This information is normalized and saved in the EventVault for subsequent analysis. The information received via the real-time feeds is analyzed to generate alerts as specified by policies configured by Administrators.

Correlation of the information received via the real-time feeds is performed according to pre-configured policies to detect specific conditions. Any detected conditions generate an event (referred to as a composite event) and may also generate an alert.

An Alert Event Cache is maintained for short-term analysis (typically seven days). All events received from remote systems via real-time feeds and composite events are saved in the Alert Event Cache. This information may be queried against via dashboards available to Administrators.

All normalized data from the remote systems as well as composite events are stored for long-term analysis in the EventVault. Administrator may analyze this data via on-demand or scheduled reports as well as a search function for specific event criteria.

Management functionality is provided so that Administrators may configure the TOE and monitor its operation. Audit records are generated for specific Administrator actions and may be reviewed via the TOE.

1.7.1 Physical Boundary

The software components of the TOE include:

1. Event Correlator – A service that correlates events received from the real-time feeds according to rules configured by Administrators to detect specific conditions. The composite events resulting from this analysis are saved in the Alert Event Cache and EventVault and may generate alerts.
2. EventTracker Alerter – A service that sends configured alerts in response to detected real-time or composite events.
3. EventTracker EventVault – A service that stores normalized data from the remote systems and composite events for long-term analysis.
4. EventTracker Receiver – A service to receive Analyser data from remote systems via real-time feeds. The data is normalized and saved for subsequent analysis.
5. EventTracker Reporter – A service to manage report generation.
6. EventTracker Scheduler – A service to initiate scheduled activities such as purging of old analyser data and generation of scheduled reports.
7. Direct Log Archiver – An application program that processes log (batch) files from remote systems that have been moved to the system where EventTracker is running. The event records in the log file are normalized and saved in the EventVault.
8. EventTracker Management Console – An application program providing the primary user interface between Administrators and EventTracker. This program provides functionality to configure components and launch other component programs. It also provides the dashboard capability to analyze data stored in the Alert Event Cache.
9. EventTracker Control Panel – An application program providing a user interface to launch other component programs.
10. User Activity – An application program providing a user interface to view events specifically related to user activity as well as to configure the user activity monitoring functionality.
11. EventTracker Event-o-Meter – An application program providing a graphical display of the number of events received over a selected period of time.
12. EventVault Warehouse Manager - An application program providing the user interface to archive the events from the EventTracker database. The archives are stored as .mdb files compressed into .cab files and referred to as EventBoxes. This application also provides the functionality to configure archiving parameters.

13. Reports Console - An application program providing the user interface to view, configure and manage reports generated from the EventVault data.
14. EventTracker Log Search – An application program providing a GUI to search the EventVault for specific event criteria.
15. EventTracker Diagnostic & Support Tool - An application program that monitors the execution of EventTracker services and provides status information to administrators.

The operating system (Windows) and supporting software (e.g. Microsoft Access) are not within the TOE boundary.

The physical boundary includes the following guidance documentation:

1. *EventTracker User's Guide*
2. *EventTracker Installation Guide*
3. *EventTracker v6.3 Direct Log Archiver*
4. *EventTracker Common Criteria Installation Supplement*

1.7.2 Logical Boundary

1.7.2.1 Audit

Audit records are generated for specific actions performed by administrators as well as processing of log (batch) files. The audit records are saved and may be reviewed by administrators.

1.7.2.2 Management

The TOE provides functionality for Administrators to configure and monitor the operation of the TOE. Administrators are any authorized users of the Windows system on which EventTracker is installed that have been granted access to the EventTracker executables.

1.7.2.3 Security Information and Event Management (SIEM)

The TOE receives security information and event messages from external systems and normalizes them into a standard form for later analysis. This information may be received via real-time feeds (e.g. syslog) or via off-line (batch) files.

The real-time feeds are analyzed by a policy engine to determine if any alerts should be generated. Event correlation is also performed on the real-time feeds, which may result in additional (composite) events being generated.

Administrators may perform analysis against the real-time and composite events via dashboard displays. Analysis of all the events (saved in the EventVault) may be performed via reports or a log search tool.

1.7.3 TOE Data

The following table describes the TOE data.

Table 3 - TOE Data Descriptions

TOE Data	Description
Alert Actions	Specifies a portion of the rules for Alert Groups for the action(s) to be performed when all criteria are satisfied. The possible actions are Generate Sound, Send E-mail, Update RSS Feed, Send Net (console) Message, Syslog and Forward Events (SNMP Trap). For email, syslog and SNMP traps, the configuration for the actions includes the destination of the alert. For the other actions, the local system is the destination.
Alert Custom Details	Specifies a portion of the rules for Alert Groups for time interval and the number of occurrences. The options are a range of time (or no range), a number of occurrences, and a count/duration pair to specify the number of occurrences within a time period.
Alert Event Cache	A cache of events received from real-time feeds, along with any composite events resulting from analysis of the real-time events. This information is used by Administrators when performing analysis via dashboards.
Alert Event Cache Purge Time	Specifies the number of days that events and alerts are saved in the Alert Event Cache.
Alert Event Details	Specifies a portion of the rules for Alert Groups for matching received events. Alert Event Details may specify any of the following: • Event Type • Log Type • Match in Source – a string match against the Source field in the events • Category - classification of the event by the event source • Event ID – any single event ID defined within the TOE • Match in User – a string match against the User field in the events • Match in Event Descr – a string match against the Description field in the events • Event Descr Exception – a string match against the Description field in the events; a match indicates the event does not satisfy the alert condition
Alert Event Filters	Specifies a portion of the rules for Alert Groups for ignoring received events. Alert Event Filters may specify the same parameter types as Alert Event Details.
Alert Group	Defines the rules that generate a specific alert. The rules include matching alert event details, alert event filters, alert custom details, alert systems, and the alert actions.
Alert Storage and Analysis Configuration	Configuration parameters involving the storage and analysis of alerts, including: • Store Only Active Alert events – only events associated with active alerts are stored in the Alert Event Cache • Show Only Active Alert Events - only events associated with active alerts from the Alert Event Cache are displayed when analysis is performed using dashboards
Alert Systems	Specifies a portion of the rules for Alert Groups for applicable systems. The parameters are a list of systems. These may be specified by selecting all systems, selecting groups, or selecting individual systems.

TOE Data	Description
Categories	A set of pre-configured groupings of multiple events (with qualifiers) into categories that are referenced when generating reports.
Correlation Rules	A set of pre-configured rules for correlation of events of different types or from different sources. If a rule is matched, a new (composite) event is generated.
Direct Log Archiver Configuration	Configuration information used for processing log files, consisting of: • Whether Direct Log Archiver is enabled • Log file path – folder where log files to be processed are found • Log file extension – the extension used for the log files to be processed • Field separator – the character used in the file to delimit fields • Log type – one of the standard Windows log file types, if the extension is .evt
Direct Log Archiver Configuration File	Configuration information used for processing log files from a specific source system and specific types of events, consisting of: • Log source – source (e.g. Oracle) of the log file • Computer name - Name of the computer from where the logs originated • Computer IP - IP address of the computer where the logs originated • System type - operating system of the computer • System description - informative description for future reference • Comment line token - character that is used to comment a line in the event log file • Formatted description - parsed fields are mapped to the fields defined in the Message Fields • Entire row as description - the whole line will be considered as the description of the event • Log file format - specifies a standard log file format if appropriate • Message fields - fields to extract from the logs • Event Data and Time Fields – the fields in the log file records that specify the date and time of the event
Enable Alert Event Cache for Alert Analysis	Enables/disables the cache of real-time events and composite events for alert analysis via reports.
Enable User Activity Monitoring	Enables event correlation for individual users.
EventVault	A database of all events (both real-time and batch) received from IT systems, along with any composite events that were generated. This information is used when performing analysis via reports.
EventVault Configuration	Configuration parameters for the event storage, including: • The directory for storage of events • A purge period for archive files
Real-time Receiver Configuration	Parameters regarding the receiver for real-time feeds from other systems, including: • A list of UDP and/or TCP ports to be used • Whether the Syslog receiver is enabled

TOE Data	Description
Report Definitions	Templates defining report parameters. The templates can be referenced when scheduling a new report. The parameters include: • The systems to be included in the report • Matching and filtering criteria to limit the scope of the report •
Report Schedule	A set of reports to be generated at the configured times.
Reports Configuration	Parameters regarding reports generated by the TOE, including: • Length of time on-demand reports are saved • Length of time scheduled reports are saved • Whether a default report is generated if no matching event records are found
User Activity Monitoring Configuration	Parameters regarding user activity monitoring, including: • Whether this function is enabled • Users for which monitoring is not performed • Number of days user activity information is kept before being automatically purged.

1.8 Evaluated Configuration

The TOE is evaluated in the following configuration:

1. All of the TOE components are installed on a single Windows platform.
2. No add-in software modules are installed.
3. The standard console model is used (not the collection point model). An Enterprise license must be installed.
4. Remedial actions are not enabled since they are dependent on the Windows Agent (which is not in the TOE boundary).
5. Suspicious Network Activity alerts are disabled. This function has been deprecated in the TOE.
6. The EventVault data is stored on a different disk partition than EventTracker is installed on.

2. Conformance Claims

2.1 Common Criteria Conformance

Common Criteria version: Version 3.1 Revision 3

Common Criteria conformance: Part 2 extended and Part 3 conformant

2.2 Security Requirement Package Conformance

EAL2 augmented by ALC_FLR.2

The TOE does not claim conformance to any security functional requirement packages.

2.3 Protection Profile Conformance

The TOE does not claim conformance to any registered Protection Profile.

3. Security Problem Definition

3.1 Introduction

This chapter defines the nature and scope of the security needs to be addressed by the TOE. Specifically this chapter identifies:

A) assumptions about the environment,

B) threats to the assets and

C) organisational security policies.

This chapter identifies assumptions as A.*assumption*, threats as T.*threat* and policies as P.*policy*.

3.2 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 4 - Assumptions

A.Type	Description
A.ACCESS	The TOE has access to all the Analyser data it needs to perform its functions.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
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.NOTRUST	The TOE can only be accessed by authorized users.

3.3 Threats

The following are threats identified for the TOE and the operational environment in which the TOE resides. The assumed level of expertise of the attacker for all the threats is unsophisticated.

Table 5 - Threats

T.Type	Description
T.FALACT	The TOE may fail to react to identified or suspected inappropriate activity by an unsophisticated attacker on an IT system the TOE monitors.
T.FALASC	The TOE may fail to identify inappropriate activity by an unsophisticated attacker based on association of Analyser data received from one or many data sources.
T.IMPCON	A user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.
T.INFLUX	An unsophisticated attacker may attempt to disguise an attack on an IT system the TOE monitors by generating a large number of security events unrelated to the attack.
T.LOSSOF	A user may attempt to remove or destroy data collected and produced by the TOE.
T.MODIFY	Analyser data sent to the TOE may be modified in transit by an unsophisticated attacker.

3.4 Organisational Security Policies

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

Table 6 - Organizational Security Policies

P.Type	Description
P.ACCACT	Users of the TOE shall be accountable for their actions within the IDS.
P.ANALYZ	Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to Analyser data and appropriate response actions taken.
P.INTGTY	Data collected and produced by the TOE shall be protected from modification.
P.MANAGE	Authorized administrators of the TOE will be provided with all the management capabilities required to effectively manage the TOE.

4. Security Objectives

This section identifies the security objectives of the TOE and the TOE's Operational Environment. The security objectives identify the responsibilities of the TOE and the TOE's Operational Environment in meeting the security needs. Objectives of the TOE are identified as *O.objective*. Objectives that apply to the operational environment are designated as *OE.objective*.

4.1 Security Objectives for the TOE

The TOE must satisfy the following objectives.

Table 7 - TOE Security Objectives

Objective	Definition
O.AUDITS	The TOE must record audit records for security-relevant actions performed by administrators.
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.IDANLZ	The TOE must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).
O.OFLOWS	The TOE must appropriately handle potential audit and Analyser data storage overflows.
O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
O.RESPON	The TOE must respond appropriately to analytical conclusions.

4.2 Security Objectives for the Operational Environment

The TOEs operating environment must satisfy the following objectives.

Table 8 - Security Objectives of the Operational Environment

Objective	Definition
OE.COMM_PROTECTION	The IT Environment will protect the integrity of information transmitted to the TOE from remote IT systems.
OE.DATA_PROTECTION	The IT Environment will provide the capability to protect TOE data from modification from outside the TSC.
OE.IDAUTH	The IT Environment must be able to identify and authenticate users prior to allowing access to TOE functions and data.
OE.IDSENS	The IT Environment must collect and forward to the TOE information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets.
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 the TOE guidance documentation.
OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
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.RESTRICT	The IT Environment will restrict TOE access to administrators authorized to use the TOE.

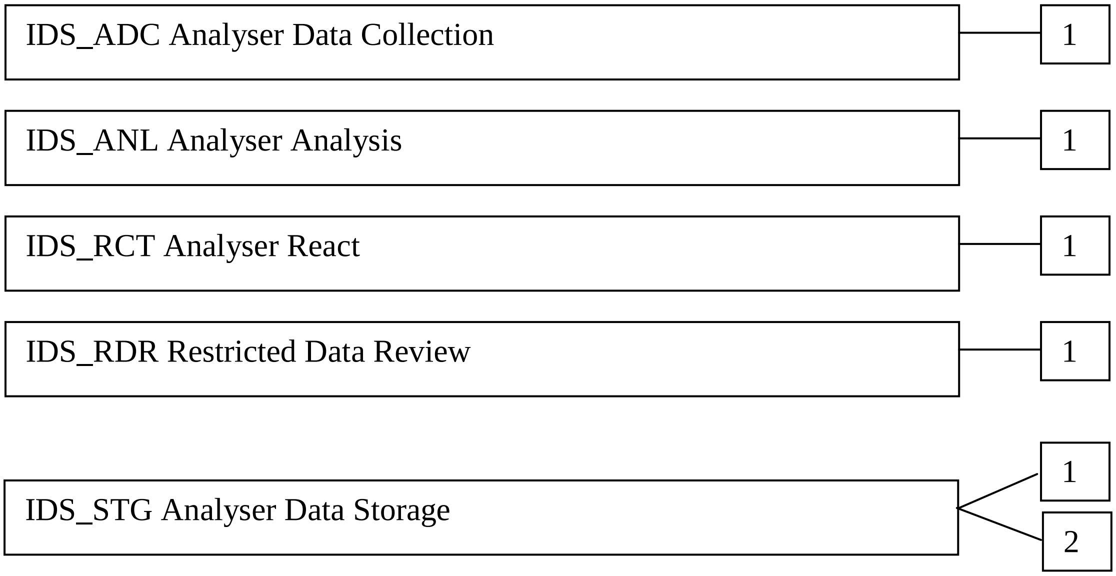
Objective	Definition
OE.TIME	The IT Environment will provide reliable timestamps to the TOE

5. Extended Components Definition

5.1 Class IDS: Intrusion Detection

All of the components in this section are based on the U.S. Government Protection Profile Intrusion Detection System Analyzer For Basic Robustness Environments.

This class of requirements is taken from the IDS Analyzer PP to specifically address the data analysed by an IDS analyzer. The audit class of the CC (FAU) was used as a model for creating these requirements. The purpose of this class of requirements is to address the unique nature of analyser data and provide for requirements about analyzing, reviewing and managing the data.


IDS_ADC Analyser Data Collection
1
IDS_ANL Analyser Analysis
1
IDS_RCT Analyser React
1
IDS_RDR Restricted Data Review
1
IDS_STG Analyser Data Storage
1
2

5.1.1 IDS_ADC Analyser Data Collection

Family Behaviour:

This family defines the requirements for the TOE regarding receipt of information related to security events from remote IT systems.

Component Levelling:

IDS_ADC Analyser Data Collection
1

IDS_ADC.1 Analyser Data Collection provides for the functionality to require TSF controlled processing of data received from remote IT systems regarding information related to security events.

Management:

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

a) Management of the configuration information for real-time feeds.

b) Management of the configuration information for processing of log (batch) files.

Audit:

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

a) Basic: Processing of log (batch) files.

IDS_ADC.1 Analyser Data Collection

Hierarchical to: No other components.

Dependencies: None

IDS_ADC.1.1 The TSF shall be able to normalize and store event information received via real-time feeds and/or log (batch) files.

5.1.2 IDS_ANL Analyser Analysis

Family Behaviour:

This family defines the requirements for the TOE regarding analysis of information related to security events received from remote IT systems.

Component Levelling:

IDS_ANL Analyser Analysis
1

IDS_ANL.1 Analyser Analysis provides for the functionality to require TSF controlled analysis of data received from remote IT systems regarding information related to security events.

Management:

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

a) Configuration of the analysis to be performed.

Audit:

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

a) Minimal: Enabling and disabling of any of the analysis mechanisms.

IDS_ANL.1 Analyser Analysis

Hierarchical to: No other components.

Dependencies: IDS_ADC.1 Analyser Data Collection

IDS_ANL.1.1 The TSF shall perform the following analysis function(s) on all security information and event feeds from Windows systems and other devices that support the Syslog protocol received:

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

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

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

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

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

5.1.3 IDS_RCT.1 Analyser React

Family Behaviour:

This family defines the requirements for the TOE regarding reactions to the analysis of information related to security events received from remote IT systems when an intrusion is detected.

Component Levelling:

IDS_RCT.1 Analyser React provides for the functionality to require TSF controlled reaction to the analysis of data received from remote IT systems regarding information related to security events when an intrusion is detected.

Management:

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

a) the management (addition, removal, or modification) of actions.

Audit:

There are no auditable events foreseen.

IDS_RCT.1 Analyser React

Hierarchical to: No other components.

Dependencies: IDS_ANL.1 Analyser Analysis

IDS_RCT.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 TSF 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.

5.1.4 IDS_RDR Restricted Data Review

Family Behaviour:

This family defines the requirements for the TOE regarding review of the analyser data collected by the TOE.

Component Levelling:

IDS_RDR.1 Restricted Data Review provides for the functionality to require TSF controlled review of the analyser data collected by the TOE.

Management:

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

a) maintenance (deletion, modification, addition) of the group of users with read access right to the analyser data records.

Audit:

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

a) Basic: Attempts to read analyser data that are denied.

b) Detailed: Reading of information from the analyser data records.

IDS_RDR.1 Restricted Data Review

Hierarchical to: No other components.

Dependencies: IDS_ANL.1 Analyser Analysis

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

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

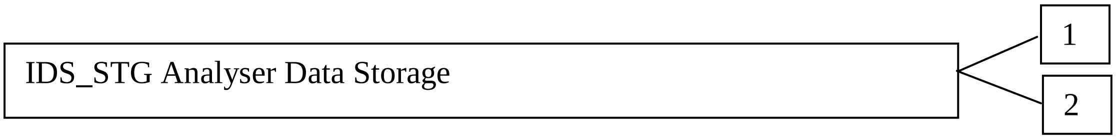
IDS_RDR.1.3 The TSF shall prohibit all users read access to the Analyser data, except those users that have been granted explicit read-access.

5.1.5 IDS_STG Analyser Data Storage

Family Behaviour:

This family defines the requirements for the TOE to be able to create and maintain a secure analyser data trail.

Component Levelling:



IDS_STG.1 Guarantee of Analyser Data Availability requires that the analyser data be protected from unauthorised deletion and/or modification and defines the behaviour when specific conditions occur.

IDS_STG.2 Prevention of Analyser Data Loss defines the actions to be taken if the analyser data storage capacity has been reached.

Management: IDS_STG.1

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

a) maintenance of the parameters that control the analyser data storage capability.

Management: IDS_STG.2

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

a) maintenance (deletion, modification, addition) of actions to be taken in case analyser data storage capacity has been reached.

Audit: IDS_STG.1

There are no auditable events foreseen.

Audit: IDS_STG.2

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

a) Basic: Actions taken if the storage capacity has been reached.

IDS_STG.1 Guarantee of Analyser Data Availability

Hierarchical to: No other components.

Dependencies: IDS_ANL.1 Analyser Analysis

IDS_STG.1.1 The TSF shall protect the stored Analyser data from unauthorised deletion.

IDS_ STG.1.2 The TSF shall protect the stored Analyser data from modification.

Application Note: Authorised deletion of data is not considered a modification of Analyser data in this context. This requirement applies to the actual content of the Analyser data, which should be protected from any modifications.

IDS_ STG.1.3 The TSF shall ensure that [assignment: *metric for saving Analyser data*] Analyser data will be maintained when the following conditions occur: [selection: *Analyser data storage exhaustion, failure, attack*].

IDS_STG.2 Prevention of Analyser data loss

Hierarchical to: No other components.

Dependencies: IDS_ANL.1 Analyser Analysis

IDS_STG.2.1 The TSF shall [selection: *'ignore Analyser data', 'prevent Analyser data, except those taken by the authorised user with special rights', 'overwrite the oldest stored Analyser data'*] and send an alarm if the storage capacity has been reached.

5.2 Extended Security Assurance Components

None

6. Security Requirements

This section contains the functional requirements that are provided by the TOE. These requirements consist of functional components from Part 2 of the CC.

The CC defines operations on security requirements. The font conventions listed below state the conventions used in this ST to identify the operations.

Assignment: indicated in italics

<u>Selection: indicated in underlined text</u>

<u>Assignments within selections: indicated in italics and underlined text</u>

Refinement: indicated with bold text

Iterations of security functional requirements may be included. If so, iterations are specified at the component level and all elements of the component are repeated. Iterations are identified by numbers in parentheses following the component or element (e.g., FAU_ARP.1(1)).

Explicitly stated requirements are included in this ST. The names of these requirements start with IDS_.

6.1 Security Functional Requirements for the TOE

The functional security requirements for the TOE consist of the following components, summarized below.

Table 9 - TOE SFRs

Functional Components	
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FAU_STG.1	Protected Audit Trail Storage
FAU_STG.4	Prevention of audit data loss
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
IDS_ADC.1	Analyser Data Collection
IDS_ANL.1	Analyser analysis
IDS_RCT.1	Analyser react
IDS_RDR.1	Restricted Data Review
IDS_STG.1	Guarantee of Analyser Data Availability
IDS_STG.2	Prevention of Analyser data loss

6.1.1 Security audit (FAU)

6.1.1.1 FAU_GEN.1 Audit data generation

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 <u>not specified</u> level of audit; and

c) *The auditable events specified in the following table.*

Table 10 - Auditable Events

Component	Event (Description)	Details
FAU_GEN.1	The EventTracker Manager service was started.	Event ID 2001
FMT_MTD.1	A scheduled report was added from EventTracker	Event ID 3283, Username, Name of the report, Report configuration details
	A scheduled report was modified from EventTracker	Event ID 3284, Username, Name of the report, Report configuration details
	A scheduled report was deleted from EventTracker	Event ID 3285, Username, Name of the report
	A report Configuration was modified from EventTracker	Event ID 3289, Username, Name of the report, Modified values
IDS_ADC.1	Direct log archiver started processing.	Event ID 3244
	DLA File not found for processing in last 24 hour.	Event ID 3254
	Direct log archiver successfully processed the following files: *filenames*	Event ID 3245, Names of the files processed
	Direct log archiver stopped processing.	Event ID 3246, Number of files processed
	Direct log archiver failed to process the following files: *filenames*	Event ID 3247, Names of the files not processed
IDS_RDR.1	Scheduled Report: *Report Name* was generated and published successfully.	Event ID 2012, Name of the report
	Scheduled Report: *Report Name* was not generated.	Event ID 2013, Name of the report

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *the additional information specified in the Details column of the previous table.*

6.1.1.2 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide *Administrators* with the capability to read *all 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.

6.1.1.3 FAU_STG.1 Protected Audit Trail Storage

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.

Application Note: Authorised deletion of data is not considered a modification of audit records in this context. This requirement applies to the actual content of the audit records, and the TOE does not provide any mechanism to modify audit records. The TOE is also dependent on the operational environment to prevent modification or deletion of audit records from outside the TSC.

6.1.1.4 FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 The TSF shall ignore audited events and *display a message in a pop-up window* if the audit trail is full.

6.1.2 Security Management (FMT)

6.1.2.1 FMT_MOF.1 Management of Security Functions Behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to disable, enable the functions *saving information in the Alert Event Cache for Alert Analysis, syslog receiving, processing log (batch) files, and user activity monitoring* to *Administrators*.

6.1.2.2 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to query, modify, and delete the *TSF data listed in the following table* to *Administrators*.

Table 11 - TSF Data Access Details

TSF Data	Operations
Alert Actions	Query, Modify
Alert Custom Details	Query, Modify
Alert Event Cache Purge Time	Query, Modify
Alert Event Details	Query, Modify
Alert Event Filters	Query, Modify
Alert Group	Query, Modify, Delete
Alert Storage and Analysis Configuration	Query, Modify
Alert Systems	Query, Modify
Direct Log Archiver Configuration	Query, Modify
Direct Log Archiver Configuration File	Query, Modify, Delete
Enable Alert Event Cache for Alert Analysis	Query, Modify
Enable User Activity Monitoring	Query, Modify
EventVault Configuration	Query, Modify
Real-time Receiver Configuration	Query, Modify
Report Definitions	Query, Modify, Delete
Report Schedule	Query, Modify
Reports Configuration	Query, Modify
User Activity Monitoring Configuration	Query, Modify

6.1.2.3 FMT_SMF.1 Specification of Management Functions

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

a) *Alert generation*

b) *Direct Log Archiver operation*

c) *User Activity Monitoring*

d) *Real-time event processing*

e) *EventVault storage*

f) *Reports generation.*

6.1.3 IDS Component Requirements (IDS)

6.1.3.1 IDS_ADC.1 Analyser Data Collection

IDS_ADC.1.1 The TSF shall be able to normalize and store event information received via real-time feeds and/or log (batch) files.

6.1.3.2 IDS_ANL.1 Analyser analysis

IDS_ANL.1.1 The TSF shall perform the following analysis function(s) on all security information and event feeds from Windows systems and other devices that support the Syslog protocol received:

a) statistical and

b) *no other analytical functions*.

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

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

b) *Event ID, Event Description, and the details specified for individual events in the following table*.

Table 12 - Event Details

Event ID	Event Description	Details
3251	Critical alert - Intrusion detected. An unauthorized and repeated logon request from *IP Address*	IP address of the system reporting the login requests
3252	Critical security alarm - Intrusion is detected - Excessive logon failures	None
3253	Intrusion is detected - Excessive logon failures due to bad password	None
3256	Intrusion Detection: Excessive network logon in your enterprise	None
3257	Intrusion Detection: Excessive network user lockout in your enterprise	None
3259	Intrusion Detection: Excessive network logon on computer *Computer Name*	Computer name of the system reporting the network logons
3260	Intrusion Detection: Excessive Authentication in your enterprise	None
3262	Critical security alarm - excessive amount of resource access failures on *Computer Name*	Computer name of the system reporting the resource access failures
3263	Intrusion detected: Unauthorized excessive file access failure on *Filename*	Name of the file being accessed
3264	Intrusion detected: Unauthorized user *Username* is persistently attempting to access resources which not permitted	Name of the user attempting the accesses
3265	High Security Alert: Too many files are being deleted from *Computer Name*	Computer name of the system reporting the deleted files

Event ID	Event Description	Details
3266	Critical Security alarm: Excessive logon on computer *Computer Name*	Computer name of the system reporting the logons
3268	Critical Security alarm: Excessive logon on domain *Domain Name*	Domain name of the domain experiencing the logons
3269	Unusual pattern: High user activity.	Name of the user generating the activity

6.1.3.3 IDS_RCT.1 Analyser react

IDS_RCT.1.1 The TSF shall send an alarm to *the alert destination configured by the Administrator* and take *no other action* when an intrusion is detected.

6.1.3.4 IDS_RDR.1 Restricted Data Review

IDS_RDR.1.1 The TSF shall provide *Administrators* with the capability to read *all information* from the Analyser data.

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

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

6.1.3.5 IDS_STG.1 Guarantee of Analyser Data Availability

IDS_STG.1.1 The TSF shall protect the stored Analyser data from unauthorised deletion.

IDS_ STG.1.2 The TSF shall protect the stored Analyser data from modification.

Application Note: Authorised deletion of data is not considered a modification of Analyser data in this context. This requirement applies to the actual content of the Analyser data, which should be protected from any modifications. The TOE is also dependent on the operational environment to prevent modification or deletion of Analyser data from outside the TSC.

IDS_ STG.1.3 The TSF shall ensure that *the oldest* Analyser data will be maintained when the following conditions occur: Analyser data storage exhaustion.

6.1.3.6 IDS_STG.2 Prevention of Analyser data loss

IDS_STG.2.1 The TSF shall ignore Analyser data and send an alarm if the storage capacity has been reached.

Application Note: The alarm is a message displayed in a pop-up window.

6.2 TOE Security Assurance Requirements

The TOE meets the assurance requirements for EAL2 augmented by ALC_FLR.2. These requirements are summarised in the following table.

Table 13 - EAL2 Assurance Requirements

Assurance Class	Component ID	Component Title
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification

Assurance Class	Component ID	Component Title
	ADV_TDS.1	Basic design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
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.2	Flaw Reporting Procedures
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

6.3 CC Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified SFRs include the appropriate hierarchy and dependencies. The following table lists the TOE SFRs and the SFRs each are hierarchical to, dependent upon and any necessary rationale.

Table 14 - TOE SFR Dependency Rationale

SFR	Hierarchical To	Dependency	Rationale
FAU_GEN.1	No other components.	FPT_STM.1	Satisfied by the operational environment (OE.TIME).
FAU_SAR.1	No other components.	FAU_GEN.1	Satisfied
FAU_STG.1	No other components.	FAU_GEN.1	Satisfied
FAU_STG.4	FAU_STG.3	FAU_STG.1	Satisfied
FMT_MOF.1	No other components.	FMT_SMF.1, FMT_SMR.1	Satisfied Not satisfied. The TOE supports a single role and all users have the same privileges. The IT Environment is required to restrict access to the TOE to authorized administrators (OE.RESTRICT).
FMT_MTD.1	No other components.	FMT_SMF.1, FMT_SMR.1	Satisfied Not satisfied. The TOE supports a single role and all users have the same privileges. The IT Environment is required to restrict access to the TOE to authorized administrators (OE.RESTRICT).
FMT_SMF.1	No other components.	None	n/a
FMT_SMR.1	No other components.	FIA_UID.1	Satisfied by the operational environment (OE.IDAUTH)
IDS_ADC.1	No other components.	None	n/a
IDS_ANL.1	No other components.	IDS_ADC.1	Satisfied
IDS_RCT.1	No other components.	IDS_ANL.1	Satisfied
IDS_RDR.1	No other components.	IDS_ANL.1	Satisfied
IDS_STG.1	No other components.	IDS_ANL.1	Satisfied
IDS_STG.2	No other components.	IDS_ANL.1	Satisfied

7. TOE Summary Specification

7.1 FAU_GEN.1

The TOE generates audit records for the events specified in the table included with FAU_GEN.1. The audit records are in the form of event records that are stored in the EventVault. All records include a time stamp (supplied by the operating system), event identifier (type of event), and EventTracker as the subject identifier. Different event types are used to indicate the success or failure of events. The Event IDs of these special events, as well as the additional information supplied with each event type, is identified in the table included with FAU_GEN.1.

7.2 FAU_SAR 1

Administrators may review the audit records using the TOE's report capability supplied by the Report Console application. The EventTracker category may be specified when generating the report to retrieve all the audit records.

Reports may be generated on demand or scheduled for periodic generation, as directed by the administrator. The EventTracker Scheduler monitors the list of scheduled reports and invokes the EventTracker Reports service as needed to generate a report.

Both on demand and scheduled reports are saved for later review. Administrators may use the Reports Console application to review previously generated reports.

Administrators may also use an interactive search tool (EventTracker Log Search) to search the EventVault for specific events.

The User Activity Viewer application provides another method to review the audit trail. This method provides a user-centric view of the events.

7.3 FAU_STG.1

The audit records are stored in the EventVault by the EventTracker EventVault service. The TOE does not provide any mechanism for administrators to modify or delete audit records, other than specifying a purge period for events.

7.4 FAU_STG.4

If storage space for the audit records (EventVault) is exhausted, a message is displayed in a pop-up window. If the storage issue is not corrected, new events are ignored.

7.5 FMT_MOF.1

Administrators enable or disable the operation of specific functions by modifying configuration parameters via the TOE application programs. The following table identifies the functions that may be enabled or disabled, along with the configuration parameters controlling them and the TOE application that provides management capability of the parameters.

Table 15 - Management of Security Functions Behaviour Details

Function	Parameter	Application
Saving information in the Alert Event Cache for Alert Analysis	Enable Alert Event Cache for Alert Analysis	EventTracker Management Console
Syslog receiving	Enable SYSLOG receiver	EventTracker Management Console

Function	Parameter	Application
Processing log (batch) files	Direct log file archiving from external sources	EventTracker Management Console
User activity monitoring	Monitor User Activity	User Activity Viewer

7.6 FMT_MTD.1

The table included with FMT_MTD.1 specifies the TSF data that may be modified by administrators as well as the operations that may be performed. These operations are performed via the GUIs provided by the TOE applications that provide the management access for these parameters. The TOE applications that provide management functionality for configuration parameters are:

1. EventTracker Management Console
2. User Activity Viewer
3. EventVault Warehouse Manager
4. Reports Console

7.7 FMT_SMF.1

The TOE provides administrators with the functionality to manage the following:

1. Alert generation (EventTracker Management Console)
2. Direct Log Archiver operation (EventTracker Management Console and EventTracker Warehouse Manager)
3. User Activity Monitoring (User Activity Viewer)
4. Real-time event processing (EventTracker Management Console)
5. EventVault storage (EventTracker Management Console and EventTracker Warehouse Manager)
5. Report generation (Report Console)

These functions are managed via the GUIs provided by the TOE applications that provide the ability to view and modify control parameters. The applications providing the GUIs are identified in parentheses in the list above.

7.8 IDS_ADC.1

The EventTracker Receiver service listens on the configured real-time feed ports for incoming events. The events are normalized and stored in the Alert Event Cache, forwarded to the Event Correlator service for event correlation, forwarded to the EventTracker Alerter service for generation of alerts as configured by the administrator, and stored in the EventVault.

The Direct Log Archiver (DLA) service is woken up by the EventTracker Scheduler process periodically to check for log (batch) files that have been added to a sub-folder for processing. The configuration file in each sub-folder directs DLA how to normalize the events contained in the file. As each event is normalized, it is saved in a temporary file that is later processed by the EventTracker EventVault service for storage in the EventVault.

7.9 IDS_ANL.1

The Event Correlator service performs correlation processing of all the events received via the real-time feeds (Analyser data). A set of pre-configured rules are used to analyze the events to detect specific conditions indicative of attempted intrusions. The list of events that are detected is specified in the table included with IDS_ANL.1. That table also specifies the information included in each type of event.

If a correlation rule is satisfied, a composite event is generated to record the result. The generated event is forwarded to an EventTracker Receiver via the configured network port for composite events. The standard processing for received events insures that the event is saved in the Alert Event Cache and EventVault, as well as causing any configured alerts to be generated.

7.10 IDS_RCT.1

Potential intrusions are indicated when specific events are received from remote systems or when a composite event is generated (Analyser data). Real-time events are received by the EventTracker Receiver and forwarded to the EventTracker Alerter service for generation of alerts as configured by the administrator.

7.11 IDS_RDR.1

Administrators may review the audit records using the TOE's report capability supplied by the Report Console application. The Alerts category may be specified when generating the report to retrieve all the composite event records.

Reports may be generated on demand or scheduled for periodic generation, as directed by the administrator. The EventTracker Scheduler monitors the list of scheduled reports and invokes the EventTracker Reports service as needed to generate a report.

Both on demand and scheduled reports are saved for later review. Administrators may use the Reports Console application to review previously generated reports.

Administrators may also use an interactive search tool (EventTracker Log Search) to search the EventVault for specific events.

The User Activity Viewer application provides another method to review Analyser data. This method provides a user-centric view of the events.

7.12 IDS_STG.1

All event records are stored in the EventVault by the EventTracker EventVault service. The TOE does not provide any mechanism for administrators to modify or delete these records, other than specifying a purge period for events.

7.13 IDS_STG.2

If storage space for the audit records (EventVault) is exhausted, a message is displayed in a pop-up window. If the storage issue is not corrected, new events are ignored.

8. Protection Profile Claims

The TOE does not claim conformance to any registered Protection Profile.

9. Rationale

This chapter provides the rationale for the selection of the IT security requirements, objectives, assumptions and threats. It shows that the IT security requirements are suitable to meet the security objectives, Security Requirements, and TOE security functional.

9.1 Rationale for IT Security Objectives

This section of the ST demonstrates that the identified security objectives are covering all aspects of the security needs. This includes showing that each threat and assumption is addressed by a security objective.

The following table identifies for each threat, OSP and assumption, the security objective(s) that address it.

Table 16 - Threats, OSPs and Assumptions to Security Objectives Mapping

	O.AUDITS	O.EADMIN	O.IDANLZ	O.OFLOWS	O.PROTCT	O.RESPON	OE.COMM_PROTECTION	OE.DATA_PROTECTION	OE.IDAUTH	OE.IDSENS	OE.INSTAL	OE.PERSON	OE.PHYCAL	OE.RESTRICT	OE.TIME
A.ACCESS										X					
A.LOCATE													X		
A.MANAGE												X			
A.NOEVIL											X	X			
A.NOTRUST									X				X		
P.ACCACT	X														X
P.ANALYZ			X			X									
P.INTGTY					X			X							
P.MANAGE		X												X	
T.FALACT						X									
T.FALASC			X												
T.IMPCON		X									X			X	
T.INFLUX				X											
T.LOSSOF					X			X							
T.MODIFY							X								

The following table describes the rationale for the mapping.

Table 17 - Mapping Rationale

Item	Security Objectives Rationale
A.ACCESS	The OE.IDSENS objective ensures the TOE has the needed data.
A.LOCATE	The OE.PHYCAL objective provides for the physical protection of the TOE.
A.MANAGE	The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.

Item	Security Objectives Rationale
A.NOEVIL	The OE.INSTAL objective ensures that the TOE is properly installed and operated and the OE.PERSON objective ensures all authorized administrators are qualified and trained to install and operate the TOE.
A.NOTRUST	The OE.PHYCAL objective provides for physical protection of the TOE to protect against unauthorized access. The OE.IDAUTH requires that logical access to the TOE is restricted to authorized users.
P.ACCACT	The O.AUDITS objective implements this policy by requiring auditing of security-relevant actions by administrators. The OE.TIME objective supports this policy by providing a time stamp for insertion into the audit records.
P.ANALYZ	The O.IDANLZ objective requires analytical processes be applied to data collected from remote IT systems. The O.RESPON objective requires appropriate reactions (as configured by administrators) by the TOE.
P.INTGTY	The O.PROTCT objective ensures the protection of data from modification within the TSC. The OE.DATA_PROTECTION objective requires the operational environment to protect TOE data from modification via mechanisms outside the TSC.
P.MANAGE	The O.EADMIN objective ensures there is a set of functions for administrators to use for effective management of the TOE. The OE.RESTRICT objective requires the IT Environment (operating system) to limit access to te TOE to authorized administrators.
T.FACCNT	Unauthorized attempts to access TOE data or security functions may go undetected. The O.AUDITS objective counters this threat by requiring the TOE to audit attempts for data accesses and use of TOE functions.
T.FALACT	The O.RESPON objective ensures the TOE reacts to suspected vulnerabilities or inappropriate activity.
T.FALASC	The O.IDANLZ objective provides the function that the TOE will recognize inappropriate activity from one or multiple data sources.
T.IMPCON	The OE.INSTAL objective states the authorized administrators will configure the TOE properly. The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product. The OE.RESTRICT objective requires the IT Environment (operating system) to limit access to te TOE to authorized administrators.
T.INFLUX	The O.OFLOWS objective counters this threat by requiring the TOE handle data storage overflows.
T.LOSSOF	The O.PROTCT objective addresses this threat by providing mechanisms in the TOE to protect TOE data. The OE.DATA_PROTECTION requires the operational environment to protect TOE data from unauthorized access outside the TSC.
T.MODIFY	The OE.COMM_PROTECTION objective addresses this threat by requiring the operational environment to protect the integrity of information sent to the TOE during transit.

9.2 Security Requirements Rationale

9.2.1 Rationale for Security Functional Requirements of the TOE Objectives

This section provides rationale for the Security Functional Requirements demonstrating that the SFRs are suitable to address the security objectives.

The following table identifies for each TOE security objective, the SFR(s) that address it.

Table 18 - TOE SFRs to Security Objectives Mapping

	O.AUDITS	O.EADMIN	O.IDANLZ	O.OFLOWS	O.PROTCT	O.RESPON
FAU_GEN.1	X					
FAU_SAR 1		X				
FAU_STG.1					X	
FAU_STG.4				X		
FMT_MOF.1		X			X	
FMT_MTD.1		X			X	
FMT_SMF.1		X			X	
IDS_ADC.1			X			
IDS_ANL.1			X			
IDS_RCT.1						X
IDS_RDR.1		X				
IDS_STG.1					X	
IDS_STG.2				X		

The following table provides the detail of TOE security objective(s).

Table 19 - TOE Security Objectives to SFR Rationale

Security Objective	SFR and Rationale
O.AUDITS	Security-relevant events that result in audit records are defined for the TOE [FAU_GEN.1].
O.EADMIN	The TSF must provide the ability to the administrator role review the audit trail of the System [FAU_SAR.1]. The TSF must provide the ability for authorized administrators to view all Analyser data collected and produced [IDS_RDR.1]. The management functions provided by the TOE are specified [FMT_SMF.1]. The specific access provided is defined and enforced by the TOE [FMT_MOF.1, FMT_MTD.1].
O.IDANLZ	The TSF collects information from remote systems [IDS_ADC.1] then performs intrusion analysis and generates conclusions [IDS_ANL.1].
O.OFLOWS	The TSF behavior if storage space is exhausted is defined [FAU_STG.4, IDS_STG.2].
O.PROTCT	The access provided to functions and data of the TOE is defined and enforced by the TSF [FMT_MOF.1, FMT_MTD.1, FMT_SMF.1]. The TSF is required to protect the audit trail and Analyser data from any modification and unauthorized deletion [FAU_STG.1, IDS_STG.1].
O.RESPON	The TOE is required to respond with an alert when configured to do so in the event an intrusion is detected [IDS_RCT.1].

9.2.2 Security Assurance Requirements Rationale

The TOE stresses assurance through vendor actions that are within the bounds of current best commercial practice. The TOE provides, primarily via review of vendor-supplied evidence, independent confirmation that these actions have been competently performed.

The general level of assurance for the TOE is:

A) Consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.

B) The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL2+ from part 3 of the Common Criteria.