NetIQ® Sentinel™ 7.2.1

Security Target

Date:	*November 14th, 2014*
Version:	*0.3*
Prepared By:	*NetIQ Corporation*
Prepared For:	*NetIQ Corporation* *515 Post Oak Blvd* *Suite 1200* *Houston, Texas 77027*

Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), Sentinel7.2.1. 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.

Table of Contents

1 Introduction 5
1.1 ST Reference 5
1.2 TOE Reference 5
1.3 Document Organization 5
1.4 Document Conventions 5
1.5 Document Terminology 6
1.6 TOE Overview 6
1.7 TOE Description 7
1.7.1 Overview 7
1.7.2 Console 10
1.7.3 Sentinel Server 11
1.7.4 Data Collector 12
1.7.5 Collector Manager 12
1.7.6 Sentinel Log Manager (SLM) 12
1.7.7 Correlation Engine (CE) 12
1.7.8 Physical Boundary 12
1.7.9 Hardware and Software Supplied by the IT Environment 14
1.7.10 Logical Boundary 14
1.7.11 TOE Security Functional Policies 15
1.7.12 TOE Product Documentation 15

2 Conformance Claims 16
2.1 CC Conformance Claim 16
2.2 PP Claim 16
2.3 Package Claim 16
2.4 Conformance Rationale 16

3 Security Problem Definition 17
3.1 Threats 17
3.2 Organizational Security Policies 17
3.3 Assumptions 17

4 Security Objectives 19
4.1 Security Objectives for the TOE 19
4.2 Security Objectives for the Operational Environment 19
4.3 Security Objectives Rationale 19
4.3.1 Rationale for Security Threats to the TOE 20

5 Extended Components Definition 22
5.1 Definition of Extended Components 22
5.1.1 Class SIEM: Incident Management 22

6 Security Requirements 24
6.1 Security Functional Requirements 24
6.1.1 Security Audit (FAU) 24
6.1.2 Information Flow Control (FDP) 25
6.1.3 Identification and Authentication (FIA) 25

6.1.4 Incident Management (SIEM) 27
6.2 Security Assurance Requirements *27*
6.3 Security Requirements Rationale *27*
6.3.1 Security Functional Requirements 27
6.3.2 Dependency Rationale 28
6.3.3 Sufficiency of Security Requirements 29
6.3.4 Security Assurance Requirements 30
6.3.5 Security Assurance Requirements Rationale 31
6.3.6 Security Assurance Requirements Evidence 31
7 TOE Summary Specification 33
7.1 TOE Security Functions *33*
7.2 Security Audit *33*
7.3 Identification and Authentication *34*
7.4 Security Management *34*

List of Tables

Table 1 – ST Organization and Section Descriptions 5
Table 2 – Acronyms Used in Security Target 6
Table 3 – Evaluated Configuration for the TOE 13
Table 4 – IT Environment 14
Table 5 – Logical Boundary Descriptions 15
Table 6 – Threats Addressed by the TOE 17
Table 7 – Organizational Security Policies 17
Table 8 – Assumptions 18
Table 9 – TOE Security Objectives 19
Table 10 – Operational Environment Security Objectives 19
Table 11 – Mapping of Assumptions, Threats, and OSPs to Security Objectives 20
Table 12 – Mapping of Threats, Policies, and Assumptions to Objectives 21
Table 13 – TOE Security Functional Requirements 24
Table 14 – Management of TSF data 26
Table 15 – Mapping of TOE Security Functional Requirements and Objectives 28
Table 16 – Rationale for TOE SFRs to Objectives 30
Table 17 – Security Assurance Requirements at EAL3 31
Table 18 – Security Assurance Rationale and Measures 32
Table 19 – Security Management Functions and SFRs 35

List of Figures

Figure 1 – Basic Sentinel 7.2.1 Configuration 7
Figure 2 – Sentinel 7.2.1 Configuration with Log Manager (SLM) and External Datastore 8
Figure 3 – Functional Block Diagram 8
Figure 4 – Sentinel Conceptual Architecture 9
Figure 5 – Sentinel Sample Data Flow 10
Figure 6 – TOE Boundary 13

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), Security Target organization, document conventions, and terminology. It also includes an overview of the evaluated product.

1.1 ST Reference

ST Title	Security Target: NetIQ® Sentinel™ 7.2.1
ST Revision	*0.2*
ST Publication Date	November 11th, 2014
Author	Michael F. Angelo (updated from Apex Assurance Group)

1.2 TOE Reference

TOE Reference	NetIQ® Sentinel™ 7.2.1 NetIQ Sentinel Log Manager 1.2.2

1.3 Document Organization

This Security Target follows the following format:

SECTION	TITLE	DESCRIPTION
1	Introduction	Provides an overview of the TOE and defines the hardware and software that make up the TOE as well as the physical and logical boundaries of the TOE
2	Conformance Claims	Lists evaluation conformance to Common Criteria versions, Protection Profiles, or Packages where applicable
3	Security Problem Definition	Specifies the threats, assumptions and organizational security policies that affect the TOE
4	Security Objectives	Defines the security objectives for the TOE/operational environment and provides a rationale to demonstrate that the security objectives satisfy the threats
5	Extended Components Definition	Describes extended components of the evaluation (if any)
6	Security Requirements	Contains the functional and assurance requirements for this TOE
7	TOE Summary Specification	Identifies the IT security functions provided by the TOE and also identifies the assurance measures targeted to meet the assurance requirements.

Table 1 – ST Organization and Section Descriptions

1.4 Document Conventions

The notation, formatting, and conventions used in this Security Target are consistent with those used in Version 3.1 of the Common Criteria. Selected presentation choices are discussed here to aid the Security Target reader. The Common Criteria allows several operations to be performed on

functional requirements: The allowable operations defined in Part 2 of the Common Criteria are *refinement, selection, assignment* and *iteration*.

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment operation is indicated by showing the value in square brackets, i.e. [assignment_value(s)].
- The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by bold text. Any text removed is indicated with a strikethrough format (Example: TSF).
- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by italicized text.
- Iterated functional and assurance requirements are given unique identifiers by appending to the base requirement identifier from the Common Criteria an iteration number inside parenthesis, for example, FMT_MTD.1.1 (1) and FMT_MTD.1.1 (2) refer to separate instances of the FMT_MTD.1 security functional requirement component.

When not embedded in a Security Functional Requirement, italicized text is used for both official document titles and text meant to be emphasized more than plain text.

1.5 Document Terminology

The following table describes the acronyms used in this document:

TERM	DEFINITION
CC	Common Criteria version 3.1
EAL	Evaluation Assurance Level
NTP	Network Time Protocol
OSP	Organizational Security Policy
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

Table 2 – Acronyms Used in Security Target

1.6 TOE Overview

The TOE is NetIQ® Sentinel™ 7.2.1. NetIQ® Sentinel™ 7.2.1 is a Security Information and Event Management Solution (SIEM) as well as a compliance monitoring solution. Sentinel acts as an aggregator, as well as a consolidator for information from multiple systems (applications, databases, servers, storage, and security devices). It analyzes and correlates the data, and reduces the data to the point where it can be acted on, either automatically or manually.

Sentinel automates log collection, analysis, and the reporting processes to ensure that IT controls are effective in supporting threat detection and audit requirements. Sentinel provides automated monitoring of security and compliance events as well as IT controls. Finally Sentinel provides real-time reporting which allows one to take immediate action if there is a security breach or non-compliant event.

Sentinel is different from an Intrusion Detection System (IDS) in that Sentinel monitors, analyzes, and reacts to events from multiple systems (applications, databases, servers, storage, and security devices).

Note: The official name of the product is: NetIQ® Sentinel™ 7.2.1 (aka Sentinel 7.2 SP1). The released product can be uniquely identified as: NetIQ® Sentinel™ 7.2.1.0_1561, or Sentinel 7.2.1.0_1561. The product name may also be referred to as or Sentinel 7.2 SP1 and abbreviated as Sentinel 7.2.1 simply Sentinel. For the purpose of this document all of the above references are equivalent, and the document may refer to the product simply as Sentinel or the TOE.

1.7 TOE Description

1.7.1 Overview

The TOE consists of the following components:

- Console
- Sentinel Server
- Data Collector
- Correlation Engine (CE)
- Sentinel Log Manager (SLM)

The basic configuration is depicted in the figure[1] below:

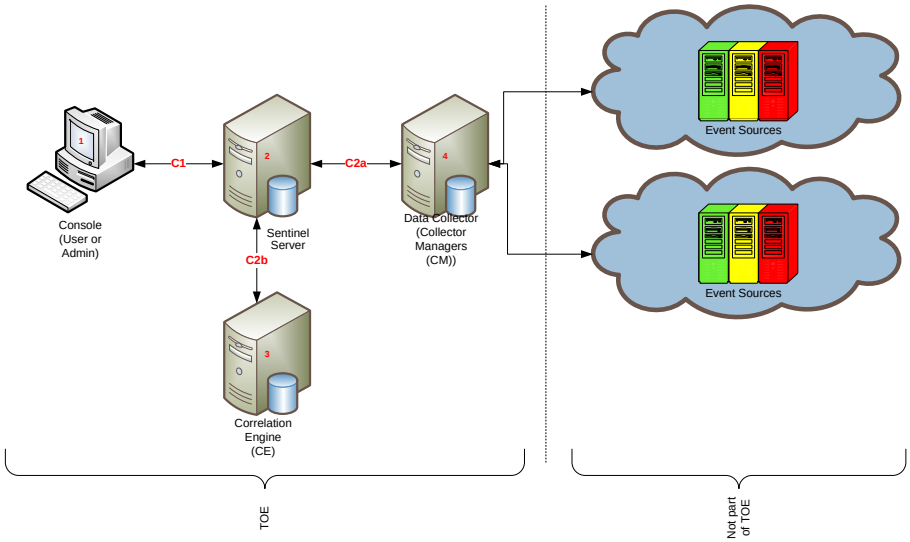


Figure 1 – Basic Sentinel 7.2.1 Configuration

The TOE can also be configured with an optional component called the NetIQ Sentinel Log Manager (SLM). The figure below depicts the placement of SLM in an environment.

[1] Components that are not part of the TOE are to the right of the dotted line. These components are included in this diagram for completeness of documentation.

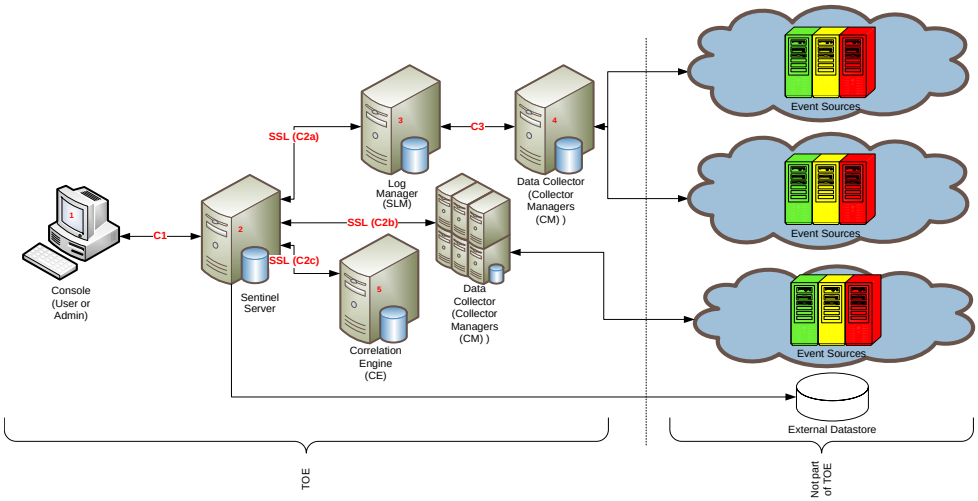


Figure 2 – Sentinel 7.2.1 Configuration with Log Manager (SLM) and External Datastore

It is important to note that all components in the Sentinel architecture can scale with multiple instances of the components.

The following diagram reflects the functional blocks in the configuration:

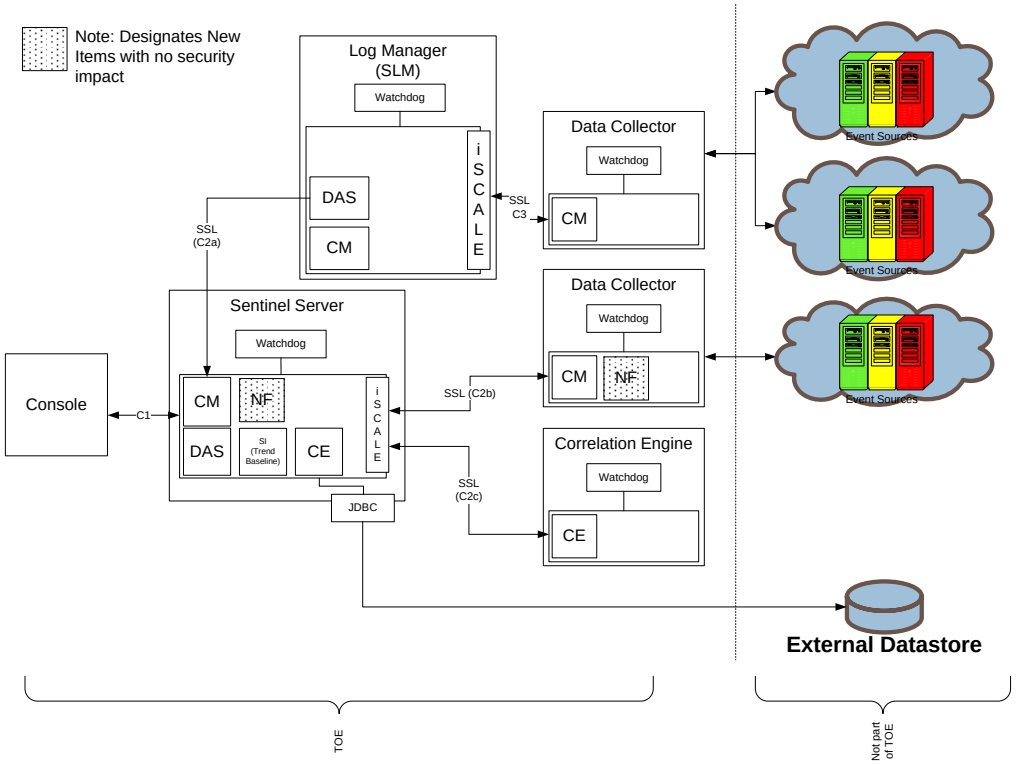


Figure 3 – Functional Block Diagram

Sentinel works by:

1. Gathering logs, events, and security information is from the configured event sources in the IT environment.

2. Normalizing the collected logs, events, and security information into a common format.
3. Adding the normalized information to a message bus (figure 4) that can move thousands of message packets per second. Scalability is achieved by allowing all of the Sentinel components to communicate through the message bus
4. Sentinel provides information by enabling the hierarchically linking of multiple Sentinel systems, including NetIQ Sentinel Log Manager, NetIQ Sentinel, and NetIQ Sentinel Rapid Deployment.

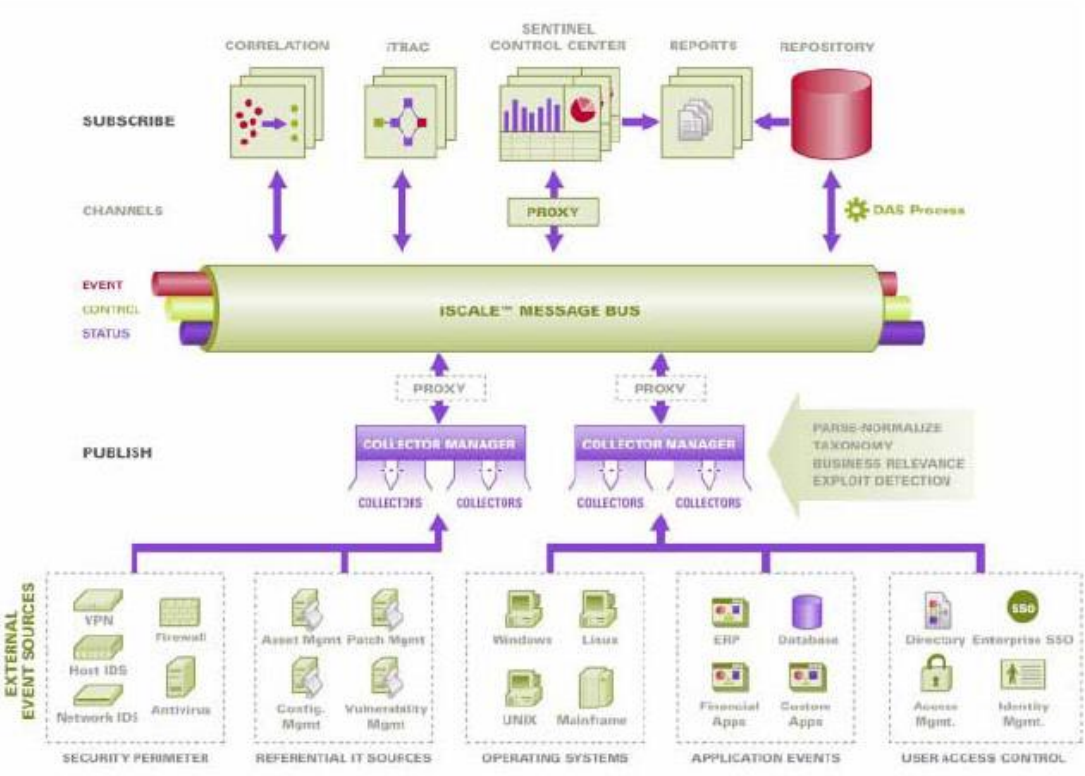


Figure 4 – Sentinel Conceptual Architecture

This architecture enables Sentinel to:

1. Provide event searches across the entire Sentinel infrastructure. i.e. on Sentinel servers distributed across the globe.
2. Perform statistical analysis to establish baselines. These can then be used to compare the events that are currently occurring to determine if there are masked or not obvious problems.
3. Correlate sets of similar, or comparable, events in a given period to determine a pattern.
4. Organization of events into incidents for efficient response management and tracking.
5. Report based on real time and historical events.

One of the key features of sentinel is a concept known as the iSCALE™ Message Bus. The iSCALE Message Bus allows for independent scaling of individual components while also allowing for standards-based integration with external applications. The key to scalability is that unlike other distributed software, no two peer components communicate with each other directly. All components communicate through the message bus, which is capable of moving thousands of message packets per second. Leveraging the message bus' unique features, the high-throughput communication channel can maximize and sustain a high data throughput rate across the independent components of the system. Events are compressed and encrypted on the wire for secure and efficient delivery from the edge of the network or collection points to the hub of the system, where real-time analytics are performed. The iSCALE message bus employs a variety of queuing services that improve the reliability of the communication beyond the security and performance aspects of the platform. Using a variety of transient and durable queues, the system offers unparalleled reliability and fault tolerance. For instance, important messages in transit are saved (by being queued) in case of a failure in the communication path. The queued message is delivered to the destination after the system recovers from failure state.

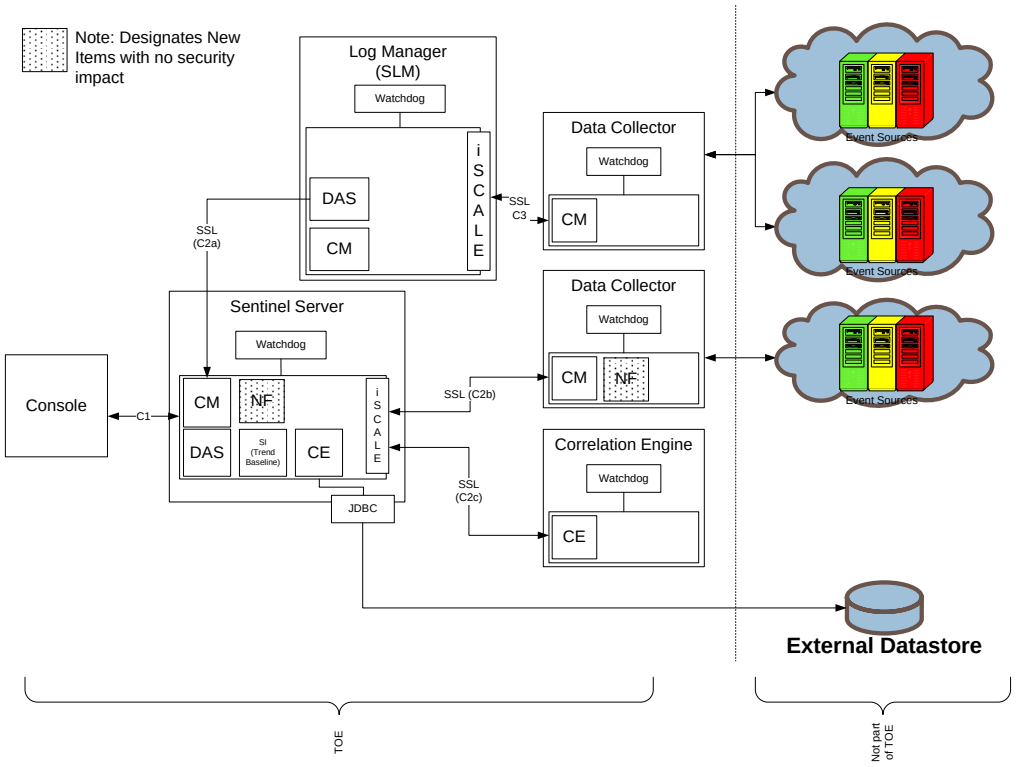


Figure 5 – Sentinel Sample Data Flow

1.7.2 Console

The Console serves two functions. The first is to enable the configuration of the system. The second is to allow for the review and output from the product. Outputs include alerts (indicating anomalies) and reports indicating status and events. The Console is a web-based interface accessed through supported web browsers. Access to Administrator or User functions are allowed based on user roles.

1.7.3 Sentinel Server

The Sentinel Server is used to aggregate information. The Sentinel Server is composed of several sub-components including:

- Sentinel Service Wrapper
- Collector Manager
- Data Access Service
- Correlation Engine
- iSCALE

1.7.3.1 Sentinel Service Wrapper

Wrapper is a Sentinel Process that manages other Sentinel Processes. If a process other than Wrapper stops, Wrapper will report this and will then restart that process.

If this service is stopped, it will stop all Sentinel processes on that machine. It executes and reports health of other Sentinel processes. This process is launched by the "Sentinel" UNIX service.

1.7.3.2 Collector Manager (CM)

Collector Manager manages the Collectors, monitors system status messages and performs event filtering as needed. Main functions of the Collector Manager include transforming events, adding business relevance to events through taxonomy, performing global filtering on events, routing events and sending health messages to the Sentinel server.

1.7.3.3 Data Access Service (DAS):

The Data Access Service (DAS) process is Sentinel Server's persistence service and provides an interface to the database. It provides data driven access to the database backend.

DAS receives requests from the different Sentinel processes, converts them to a search against the database, processes the result from the database and converts it that back to a reply. It supports requests to retrieve events for Search and Event Drill Down, to retrieve vulnerability information and advisor information and to manipulate configuration information. DAS also handles logging of all events being received from the Collector Manager and requests to retrieve and store configuration information.

1.7.3.4 Correlation Engine (CE)

The Correlation Engine process receives events from the Collector Manager and publishes correlated events based on user-defined correlation rules.

1.7.3.5 NetFlow Collector Manager (NF)

The NetFlow Collector manager receives NetFlow data from network devices and provides them to Sentinel for analysis.

1.7.3.6 iSCALE

The iSCALE is a message-oriented middleware that provides the communication platform for all other Sentinel processes.

1.7.4 Data Collector

To improve overall performance, Data Collectors service, process, and send events to the Sentinel Server. In addition there is a Wrapper service that monitors and manages the Data Collector. Data Collectors are distributed systems running the Collector Manager software.

1.7.5 Collector Manager

Collector Manager as a sub-component of the Data Collector has the same functionality as the Collector Manager sub-component of the Sentinel Server.

1.7.6 Sentinel Log Manager (SLM)

NetIQ Sentinel Log Manager (SLM) collects and manages data from a variety of devices and applications, including intrusion detection systems, firewalls, operating systems, routers, Web servers, databases, switches, mainframes, and antivirus event sources. NetIQ Sentinel Log Manager provides high event-rate processing, long-term data retention, policy-based data retention, regional data aggregation, and simple searching and reporting functionality for a variety of applications and devices.

The Sentinel Log Manager is composed of several sub-components including:

- Collector Manager
- Data Access Service
- iSCALE

1.7.7 Correlation Engine (CE)

While there is a Correlation Engine in the Sentinel Server, for load balancing there can be multiple correlation engines deployed on separate systems. In addition to the CE, there is also a Wrapper component that keeps track of the CE.

1.7.8 Physical Boundary

The TOE is a software TOE and includes the following components:

- Console
- Sentinel Server
- Data Collector
- Correlation Engine (CE)
- Log Manager (SLM)

The following figure presents the TOE diagram. The shaded elements are excluded from the TOE.

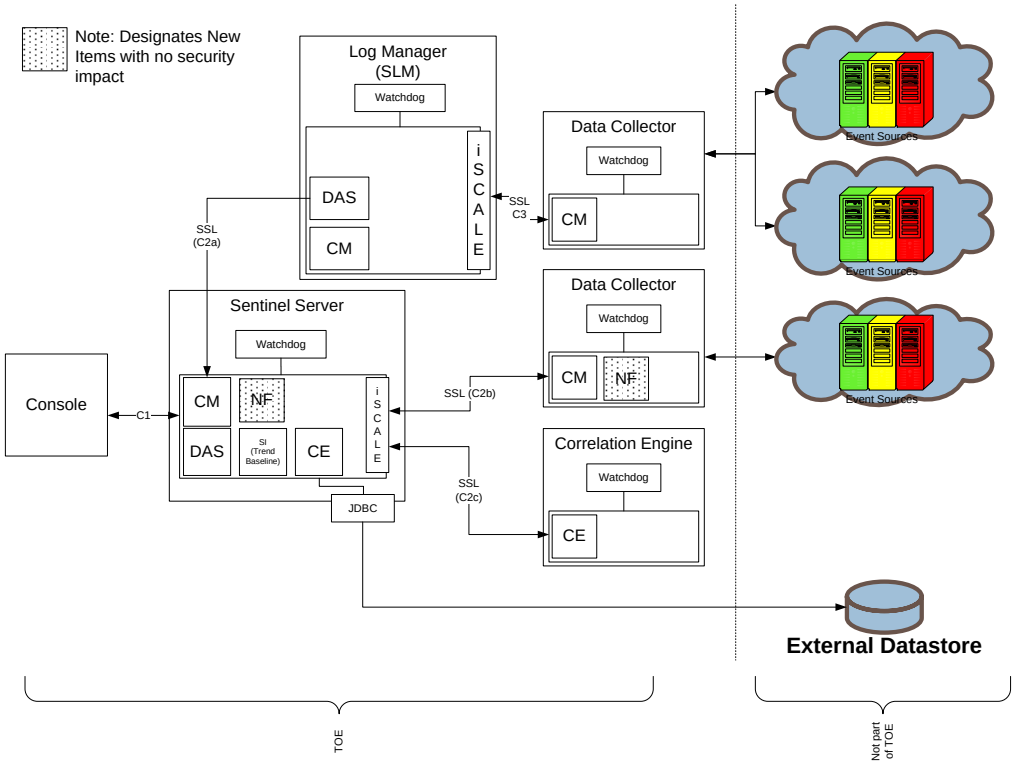


Figure 6 – TOE Boundary

In order to comply with the evaluated configuration, the following software component should be used:

COMPONENT	VERSION NUMBER
Sentinel Server (including Console, Sentinel Server, Data Collector, and Correlation Engine (CE) components)	Version 7.2.1.0_1561
Sentinel Log Manager (including Data Collector for Sentinel Log Manager)	Version 1.2.2.0_1014

Table 3 – Evaluated Configuration for the TOE

Note the following constraints for the evaluated configuration:

- The hardware, operating systems and third party support software (e.g. DBMS) on each of the systems are excluded from the TOE boundary.
- Sentinel plugins can be used in the evaluated configuration as they are not security relevant. Plugins are part of the TOE and are not a separate / distinct entity.
- The Report Development Utility is excluded from evaluation
- The Advisor functionality is excluded from evaluation.
- The command line interface is excluded from evaluation.

1.7.9 Hardware and Software Supplied by the IT Environment

The TOE consists of a set of software applications. The hardware, operating systems and all third party support software (e.g., DBMS) on the systems on which the TOE executes are excluded from the TOE boundary.

The TOE requires the following minimum hardware and software configuration:

TOE COMPONENT	TYPE	VERSION/MODEL NUMBER
Sentinel Server	Operating System	SUSE Linux Enterprise Server (SLES) 11 SP3 64-bit Red Hat Enterprise Linux Server (RHEL) 6.4 64-bit
	Virtual Platforms (With SLES-11 SP3 64-bit or RHEL 6.4 64-bit)	VMWare ESX 4.0 ESX 5.0 Xen 4.0 Hyper-V Server 2012 with the DVD ISO file only
	CPU	Intel(R) Xeon(R) CPU E5420 @ 2.50GHz (4 CPU cores), no hyper-threading
	Memory	4GB
	Storage	500 GB (no RAID required)
	Optional External Datastore	Oracle v 11g R2 or Microsoft SQL Server 2008 R2
Sentinel Log Manager	Operating System	SUSE Linux Enterprise Server (SLES) 11 SP3 64-bit
	Virtual Platforms (With SLES-11 SP3 64-bit and RHEL 6.4 64-bit)	VMWare ESX 5.0 Xen 4.0
	CPU	One Intel Xeon E550 3-GHZ (4core)
	Memory	4 GB
	Storage	2 x 500 GB
Data Collector	Operating System	SUSE Linux Enterprise Server (SLES) 11 SP3 64-bit
	CPU	Intel Xeon E5450 3-Ghz (4 cores)
	Memory	4 GB
	Storage	50 GB (RAID 1)
Correlation Engine	Operating System	SUSE Linux Enterprise Server (SLES) 11 SP3 64-bit
	CPU	Intel Xeon L5240 3-Ghz (2 core)
	Memory	8 GB
	Storage	50 GB
Console	Operating System	Windows 7 (Chrome, Firefox 5+, IE 9,10)
	Operating System	SLES 11 SP3 / RHEL 6 (Firefox 5+)

Table 4 – IT Environment

1.7.10 Logical Boundary

This section outlines the boundaries of the security functionality of the TOE; the logical boundary of the TOE includes the security functionality described in the following table:

TSF	DESCRIPTION
Security Management	The TOE provides administrators with the capabilities to configure, monitor and manage the TOE to fulfill the Security Objectives. Security Management principles relate to management of access control policies as well as management of events and incidents. Administrators configure the TOE with the Console via Web-based connection.
Security Audit	The TOE generates reports on the event analysis activities. Additionally, the TOE supports the provision of log data from each system component, such as user login/logout and incident/ticket management actions. It also records security events such as failed login attempts, etc. Audit trails can be stored for later review and analysis. Audit data is also collected by the TOE from the various devices that send event data, and the TOE analyzes this information against a set of correlation rules and filters.
Identification and Authentication	The TOE enforces individual I&A in conjunction with group/role based I&A mechanisms. Operators must successfully authenticate using a unique identifier and password prior to performing any actions on the TOE.

Table 5 – Logical Boundary Descriptions

1.7.11 TOE Security Functional Policies

The TOE supports the following Security Functional Policy:

1.7.11.1 Administrative Access Control SFP

The TOE implements an access control SFP named *Administrative Access Control SFP*. This SFP determines and enforces the privileges associated with operator roles. An authorized administrator can define specific services available to administrators and users via the Console.

1.7.12 TOE Product Documentation

The TOE includes the following product documentation[2,3]:

- Sentinel 7.2.1 Release Notes
- NetIQ Sentinel Administration Guide
- NetIQ Sentinel User Guide
- NetIQ Sentinel 7.2.1 Installation and Configuration Guide
- Sentinel Log Manager 1.2.2 Readme
- Sentinel Log Manager 1.2.2 Administration Guide
- Sentinel Log Manager 1.2.2 Installation Guide

[2] Sentinel documentation can be found here: https://www.netiq.com/documentation/sentinel72/
[3] Sentinel Log Manager can be found here: https://www.netiq.com/documentation/novelllogmanager12/

2 Conformance Claims

2.1 CC Conformance Claim

The TOE is Common Criteria Version 3.1 Revision 3 (July 2009) Part 2 extended and Part 3 conformant and augmented with ALC_FLR.1.

2.2 PP Claim

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

2.3 Package Claim

The TOE claims conformance to the EAL3 assurance package defined in Part 3 of the Common Criteria Version 3.1 Revision 3 (July 2009). The TOE does not claim conformance to any functional package.

2.4 Conformance Rationale

No conformance rationale is necessary for this evaluation since this Security Target does not claim conformance to a Protection Profile.

3 Security Problem Definition

In order to clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:

- Any known or assumed threats to the assets against which specific protection within the TOE or its environment is required
- Any organizational security policy statements or rules with which the TOE must comply
- Any assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used.

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

3.1 Threats

The following are threats identified for the TOE and the IT System the TOE monitors. The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all threats is unsophisticated.

The TOE addresses the following threats:

THREAT	DESCRIPTION
T.NO_AUTH	An unauthorized user may gain access to the TOE and alter the TOE configuration.
T.NO_PRIV	An authorized user of the TOE exceeds his/her assigned security privileges resulting in unauthorized modification of the TOE configuration and/or data.

Table 6 – Threats Addressed by the TOE

3.2 Organizational Security Policies

The TOE meets the following organizational security policies:

ASSUMPTION	DESCRIPTION
P.EVENTS	All events from network-attached devices shall be monitored and reported.
P.INCIDENTS	Security events correlated and classified as incidents should be managed to resolution

Table 7 – Organizational Security Policies

3.3 Assumptions

This section describes the security aspects of the environment in which the TOE is intended to be used. The TOE is assured to provide effective security measures in a co-operative non-hostile environment only if it is installed, managed, and used correctly. The following specific conditions are assumed to exist in an environment where the TOE is employed.

ASSUMPTION	DESCRIPTION
A.MANAGE	Administrators of the TOE are assumed to be appropriately trained to undertake the installation, configuration and management of the TOE in a secure and trusted manner.
A.NOEVIL	Administrators of the TOE and users on the local area network are not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the TOE documentation

ASSUMPTION	DESCRIPTION
A.LOCATE	The processing platforms on which the TOE resides are assumed to be located within a facility that provides controlled access
A.CONFIG	The TOE is configured to receive all events from network-attached devices.
A.TIMESOURCE	The TOE has a trusted source for system time via NTP server

Table 8 – Assumptions

4 Security Objectives

4.1 Security Objectives for the TOE

The IT security objectives for the TOE are addressed below:

OBJECTIVE	DESCRIPTION
O.CAPTURE_EVENT	The TOE shall collect data (in the form of events) from security and non-security products with accurate timestamps and apply analytical processes to derive conclusions about events.
O.MANAGE_INCIDENT	The TOE shall provide a workflow to manage incidents.
O.SEC_ACCESS	The TOE shall ensure that only those authorized users and applications are granted access to security functions and associated data.

Table 9 – TOE Security Objectives

4.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are addressed below:

OBJECTIVE	DESCRIPTION
OE.TIME	The TOE operating environment shall provide an accurate timestamp (via reliable NTP server).
OE.ENV_PROTECT	The TOE operating environment shall provide mechanisms to isolate the TOE Security Functions (TSF) and assure that TSF components cannot be tampered with or bypassed
OE.PERSONNEL	Authorized administrators are non-hostile and follow all administrator guidance and must ensure that the TOE is delivered, installed, managed, and operated in a manner that maintains the TOE security objectives. Any operator of the TOE must be trusted not to disclose their authentication credentials to any individual not authorized for access to the TOE.
OE.PHYSEC	The facility surrounding the processing platform in which the TOE resides must provide a controlled means of access into the facility

Table 10 – Operational Environment Security Objectives

4.3 Security Objectives Rationale

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions, threats, and Organizational Security Policies.

OBJECTIVES / ASSUMPTIONS/ THREATS/ POLICIES	O.CAPTURE_EVENT	O.MANAGE_INCIDENT	O.SEC_ACCESS	OE.TIME	OE.ENV_PROTECT	OE.PERSONNEL	OE.PHYSEC
A.CONFIG						✓	
A.MANAGE						✓	
A.NOEVIL						✓	

OBJECTIVES / ASSUMPTIONS/ THREATS/ POLICIES	O.CAPTURE_EVENT	O.MANAGE_INCIDENT	O.SEC_ACCESS	OE.TIME	OE.ENV_PROTECT	OE.PERSONNEL	OE.PHYSEC
A.LOCATE							✓
A.TIMESOURCE				✓			
T.NO_AUTH			✓		✓	✓	✓
T.NO_PRIV			✓				
P.EVENTS	✓			✓		✓	
P.INCIDENTS		✓		✓		✓	

Table 11 – Mapping of Assumptions, Threats, and OSPs to Security Objectives

4.3.1 Rationale for Security Threats to the TOE

ASSUMPTION/ THREAT/ POLICY	RATIONALE
A.CONFIG	This assumption is addressed by • OE.PERSONNEL, which ensures that the TOE is managed and administered by in a secure manner by a competent and security aware personnel in accordance with the administrator documentation. This objective also ensures that those responsible for the TOE install, manage, and operate the TOE in a secure manner
A.MANAGE	This assumption is addressed by • OE.PERSONNEL, which ensures that the TOE is managed and administered by in a secure manner by a competent and security aware personnel in accordance with the administrator documentation. This objective also ensures that those responsible for the TOE install, manage, and operate the TOE in a secure manner
A.NOEVIL	This assumption is addressed by OE.PERSONNEL, which ensures that the TOE is managed and administered by in a secure manner by a competent and security aware personnel in accordance with the administrator documentation. This objective also ensures that those responsible for the TOE install, manage, and operate the TOE in a secure manner
A.LOCATE	This assumption is addressed by OE.PHYSEC which ensures that the facility surrounding the processing platform in which the TOE resides provides a controlled means of access into the facility
A.TIMESOURCE	This assumption is addressed by OE.TIME, which ensures the provision of an accurate time source.

ASSUMPTION/ THREAT/ POLICY	RATIONALE
T.NO_AUTH	This threat is countered by the following: • O.SEC_ACCESS, which ensures that the TOE allows access to the security functions, configuration, and associated data only by authorized users and applications and • OE.ENV_PROTECT, which ensures that TSF components cannot be tampered with or bypassed and • OE.PERSONNEL, which ensures that the TOE is managed and administered by in a secure manner by a competent and security aware personnel in accordance with the administrator documentation. This objective also ensures that those responsible for the TOE install, manage, and operate the TOE in a secure manner and • OE.PHYSEC, which ensures that the facility surrounding the processing platform in which the TOE resides provides a controlled means of access into the facility
T.NO_PRIV	This threat is countered by O.SEC_ACCESS, which ensures that the TOE allows access to the security functions, configuration, and associated data only by authorized users and applications.
P.EVENTS	This organizational security policy is enforced by • O.CAPTURE_EVENT, which ensures that the TOE collects security events from security products and non-security products deployed within a network and applies analytical processes to derive conclusions about the events and • OE.TIME, which provides support for enforcement of this policy by ensuring the provision of an accurate time source and • OE.PERSONNEL, which ensures that authorized administrators are non-hostile and follow all administrator guidance and ensures that the TOE is delivered, installed, managed, and operated in a manner that maintains the TOE security objectives. Any operator of the TOE must be trusted not to disclose their authentication credentials to any individual not authorized for access to the TOE.
P.INCIDENTS	This organizational security policy is enforced by • O.MANAGE_INCIDENT, which ensures that the TOE will provide the capability to provide workflow functionality to manage the resolution of incidents and • OE.TIME, which ensures that the TOE operating environment shall provide an accurate timestamp (via reliable NTP server) and • OE.PERSONNEL, which ensures that authorized administrators are non-hostile and follow all administrator guidance and ensures that the TOE is delivered, installed, managed, and operated in a manner that maintains the TOE security objectives. Any operator of the TOE must be trusted not to disclose their authentication credentials to any individual not authorized for access to the TOE.

Table 12 – Mapping of Threats, Policies, and Assumptions to Objectives

5 Extended Components Definition

A class of Security Information and Event Management (SIEM) requirements was created to specifically address the data collected, analyzed, and managed by a SIEM solution. The purpose of this class is to address the unique nature of SIEM solutions and provide requirements about collecting events and managing incidents. These requirements have no dependencies since the stated requirements embody all the necessary security functions.

5.1 Definition of Extended Components

5.1.1 Class SIEM: Incident Management

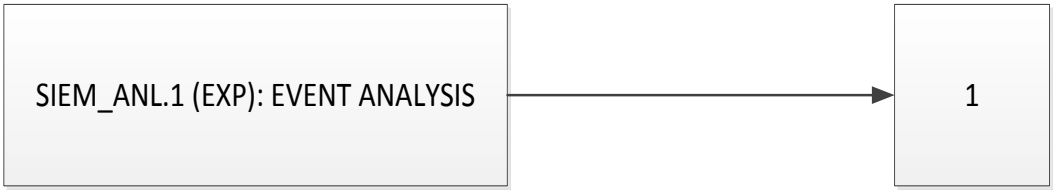
Incident Management functions provide the capability to analyze security event data and incident workflow.

5.1.1.1 Event Analysis SIEM_ANL.1 (EXP)

Family Behavior

This family defines the requirements for security event analysis functionality.

Component Leveling



SIEM_ANL.1 (EXP) Event Analysis provides the analysis of security event data.

Management: SIEM_ANL.1 (EXP)

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

a) Configuration of the analysis to be performed

Audit: SIEM_ANL.1 (EXP)

There are no auditable events foreseen.

SIEM_ANL.1 (EXP) Event Analysis

Hierarchical to: No other components
Dependencies: No dependencies

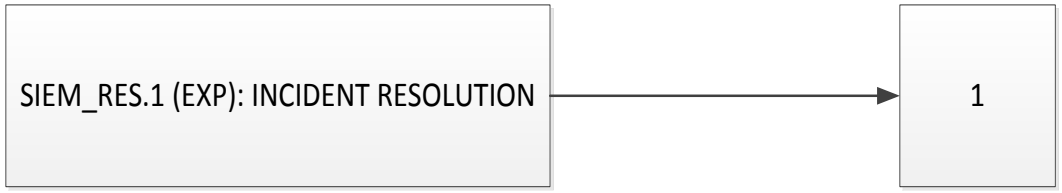
SIEM_ANL.1.1 (EXP) The TSF shall perform [assignment: list of analysis functions] analysis function(s) on data collected.

5.1.1.2 SIEM_RES.1 Incident Resolution (EXP)

Family Behavior

This family defines the requirements for security incident functionality.

Component Leveling



SIEM_RES.1 (EXP) provides the incident resolution workflow functionality.

Management: SIEM_RES.1 (EXP)

There are no management activities foreseen..

Audit: SIEM_RES.1 (EXP)

There are no auditable events foreseen.

SIEM_RES.1 (EXP) Incident Resolution

Hierarchical to: No other components
Dependencies: No dependencies

SIEM_RES.1.1 (EXP) The TSF shall provide a means to track work items that are necessary to resolve an incident.

6 Security Requirements

The security requirements that are levied on the TOE and the IT environment are specified in this section of the ST.

6.1 Security Functional Requirements

The functional security requirements for this Security Target consist of the following components from Part 2 of the CC, which are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_SAR.1	Audit Review
User Data Protection	FDP_ACC.1	Subset Access Control
	FDP_ACF.1	Security Attribute Based Access Control
Identification and Authentication	FIA_ATD.1	User Attribute Definition
	FIA_UAU.2	User Authentication before Any Action
	FIA_UID.2	User Identification before Any Action
Security Management	FMT_MSA.1	Management of Security Attributes
	FMT_MSA.3	Static Attribute Initialization
	FMT_MTD.1	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles
Incident Management	SIEM_ANL.1 (EXP)	Event Analysis
	SIEM_RES.1 (EXP)	Incident Resolution

Table 13 – TOE Security Functional Requirements

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 [*not specified*] level of audit; and

c) [User login/logout;

d) Login failures;]

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, [no other audit relevant information].

6.1.1.2 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide [the Administrator] with the capability to read [all audit data generated within the TOE] 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.

6.1.2 Information Flow Control (FDP)

6.1.2.1 FDP_ACC.1 Subset Access Control

FDP_ACC.1.1 The TSF shall enforce the [Administrative Access Control SFP] on [

Subjects: All users

Objects: System reports, component audit logs, TOE configuration, operator account attributes

Operations: all user actions]

6.1.2.2 FDP_ACF.1 Security Attribute Based Access Control

FDP_ACF.1.1 The TSF shall enforce the [Administrative Access Control SFP] to objects based on the following: [

Subjects: All users

Subject Attributes: User Identity, Authentication Status, Privileges

Objects: System reports, component audit logs, TOE configuration, operator account attributes

Object Attributes: None

Operations: all user actions]

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [verify the operator's User Identity, Authentication Status, Privileges].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [no additional rules].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [invalidation of username/password combination from the IT Environment].

6.1.3 Identification and Authentication (FIA)

6.1.3.1 FIA_ATD.1 – User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [User Identity, Password, Privileges].

6.1.3.2 FIA_UAU.2 User Authentication before Any Action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.3.3 FIA_UID.2 User Identification before Any Action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.3.4 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [Administrative Access Control SFP] to restrict the ability to [*query, modify, delete*] the security attributes [User accounts, privileges] to [Administrator].

6.1.3.5 FMT_MSA.3 Static Attribute Initialization

FMT_MSA.3.1 The TSF shall enforce the [Administrative Access Control SFP] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [Administrator] to specify alternative initial values to override the default values when an object or information is created.

Application Note: All access privileges must be explicitly granted by the Administrator. The default is to deny access to all privileges. The following Security Attributes have defaults – permissions to view/modify/delete/create:

- *Correlation Engine/Rules*
- *Reports*
- *Dashboards*
- *incidents*
- *Event Actions*

6.1.3.6 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to [control] the [data described in the table below] to [Administrator]:

DATA	CHANGE DEFAULT	QUERY	MODIFY	DELETE	CLEAR
User Privileges	✓	✓	✓	✓	✓
User Account Attributes		✓	✓		

Table 14 – Management of TSF data

6.1.3.7 FMT_SMF.1 Specification of Management Functions

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

a) Create accounts

b) Modify accounts

c) Define User privileges

d) Change Default, Query, Modify, Delete, Clear the attributes associated with the Administrative Access Control SFP

e) Modify the behavior of the Administrative Access Control SFP

f) Manage security incidents

g) Manage correlation rules].

Application Note: Security incidents are groups of events that represent an actionable security incident, plus associated state and meta-information. Incidents are created manually or through Correlation rules.

6.1.3.8 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [Administrator, User].

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

6.1.4 Incident Management (SIEM)

6.1.4.1 SIEM_ANL.1 Event Analysis (EXP)

SIEM_ANL.1.1 The TSF shall perform [filtering and correlation] analysis function(s) on data collected.

6.1.4.2 SIEM_RES.1 Incident Resolution (EXP)

SIEM_RES.1.1 The TSF shall provide a means to track work items that are necessary to resolve an incident.

6.2 Security Assurance Requirements

The Security Assurance Requirements for this evaluation are listed in Section 6.3.4 – Security Assurance Requirements.

6.3 Security Requirements Rationale

6.3.1 Security Functional Requirements

The following table provides the correspondence mapping between security objectives for the TOE and the requirements that satisfy them.

SFR \ OBJECTIVE	O.CAPTURE_EVENT	O.MANAGE_INCIDENT	O.SEC_ACCESS
FAU_GEN.1	✓	✓	
FAU_SAR.1	✓	✓	
FDP_ACC.1			✓
FDP_ACF.1			✓
FIA_ATD.1			✓
FIA_UAU.2			✓
FIA_UID.2			✓
FMT_MSA.1			✓
FMT_MSA.3			✓
FMT_MTD.1			✓
FMT_SMF.1			✓
FMT_SMR.1			✓
SIEM_ANL.1 (EXP)	✓		
SIEM_RES.1 (EXP)		✓	

Table 15 – Mapping of TOE Security Functional Requirements and Objectives

6.3.2 Dependency Rationale

This ST satisfies all the security functional requirement dependencies of the Common Criteria. The table below lists each SFR 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.

SFR CLAIM	DEPENDENCIES	DEPENDENCY MET	RATIONALE
FAU_GEN.1	FPT_STM.1	YES	Satisfied by the Operational Environment (OE.TIME)
FAU_SAR.1	FAU_GEN.1	YES	
FDP_ACC.1	FDP_ACF.1	YES	
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	YES	
FIA_ATD.1	N/A	N/A	
FIA_UAU.2	FIA_UAU.1	FIA_UID.1	Satisfied by FIA_UID.2, which is hierarchical to FIA_UID.1
FIA_UID.2	N/A	N/A	
FMT_MSA.1	FDP_ACC.1 FMT_SMF.1 FMT_SMR.1	YES	
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	YES	

SFR CLAIM	DEPENDENCIES	DEPENDENCY MET	RATIONALE
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	YES	
FMT_SMF.1	N/A	N/A	
FMT_SMR.1	FIA_UID.1	YES	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FPT_STM.1	N/A	N/A	
SIEM_ANL.1 (EXP)	N/A	N/A	
SIEM_RES.1 (EXP)	N/A	N/A	

6.3.3 Sufficiency of Security Requirements

The following table presents a mapping of the rationale of TOE Security Requirements to Objectives.

Objective	RATIONALE
O.CAPTURE_EVENT	The objective to ensure that the TOE will collect events from security products and non-security products deployed within a network and applies analytical processes to derive conclusions about the events is met by the following security requirements: • FAU_GEN.1 and FAU_SAR.1 define the auditing capability for events and administrative access control and requires that authorized users will have the capability to read and interpret data stored in the audit logs • SIEM_ANL.1 (EXP) ensures that the TOE performs analysis on all security events received from network devices
O.MANAGE_INCIDENT	The objective to ensure that the TOE provides a workflow to manage incidents is met by the following security requirements: • FAU_GEN.1 and FAU_SAR.1 define the auditing capability for incidents and administrative access control and requires that authorized users will have the capability to read and interpret data stored in the audit logs • SIEM_RES.1 (EXP) ensures that the TOE provides the capability to manage status and track action items in the resolution of incidents

Objective	RATIONALE
O.SEC_ACCESS	This objective ensures that the TOE allows access to the security functions, configuration, and associated data only by authorized users and applications. • FDP_ACC.1 requires that all user actions resulting in the access to TOE security functions and configuration data are controlled • FDP_ACF.1 supports FDP_ACC.1 by ensuring that access to TOE security functions, configuration data, audit logs, and account attributes is based on the user privileges and their allowable actions • FIA_UAU.2 requires the TOE to enforce authentication of all users prior to configuration of the TOE • FIA_UID.2 requires the TOE to enforce identification of all users prior to configuration of the TOE • FIA_ATD.1 specifies security attributes for users of the TOE • FMT_MTD.1 restricts the ability to query, add or modify TSF data to authorized users. • FMT_MSA.1 specifies that only privileged administrators can access the TOE security functions and related configuration data • FMT_MSA.3 ensures that all default values of security attributes are restrictive in nature as to enforce the access control policy for the TOE. The Administrator must explicitly grant access privileges to users – the default tis no access. • FMT_SMF.1 and FMT_SMR.1 support the security functions relevant to the TOE and ensure the definition of an authorized administrator role.

Table 16 – Rationale for TOE SFRs to Objectives

6.3.4 Security Assurance Requirements

The assurance security requirements for this Security Target are taken from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 3 (EAL3). The assurance components are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
ADV: Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.3	Functional Specification with Complete Summary
	ADV_TDS.2	Architectural Design
AGD: Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
ALC: Lifecycle Support	ALC_CMC.3	Authorization Controls
	ALC_CMS.3	Implementation representation CM coverage
	ALC_DEL.1	Delivery Procedures

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
	ALC_DVS.1	Identification of Security Measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_FLR.1	Flaw Remediation Procedures
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
AVA: Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

Table 17 – Security Assurance Requirements at EAL3

6.3.5 Security Assurance Requirements Rationale

The ST specifies Evaluation Assurance Level 3. EAL3 was chosen because it is based upon good commercial development practices with thorough functional testing. EAL3 provides the developers and users a moderate level of independently assured security in conventional commercial TOEs. The threat of malicious attacks is not greater than low, the security environment provides physical protection, and the TOE itself offers a very limited interface, offering essentially no opportunity for an attacker to subvert the security policies without physical access.

6.3.6 Security Assurance Requirements Evidence

This section identifies the measures applied to satisfy CC assurance requirements. Note that in some cases.

SECURITY ASSURANCE REQUIREMENT	EVIDENCE TITLE
ADV_ARC.1 Security Architecture Description	NetIQ® Sentinel™ 7.2.1 Security Architecture
ADV_FSP.3 Functional Specification with Complete Summary	NetIQ® Sentinel™ 7.2.1 Functional Specification
ADV_TDS.2 Architectural Design	NetIQ® Sentinel™ 7.2.1 Architectural Design
AGD_OPE.1 Operational User Guidance	NetIQ Sentinel Administration Guide[4][5] NetIQ Sentinel User Guide[6] NetIQ Sentinel Installation and Configuration Guide[7] Sentinel Log Manager 1.2.2 Administration Guide[8][9] NetIQ® Sentinel™ 7.2.1 Operational User Guidance and Preparative Procedures Supplement

[4] Documentation for Sentinel 7.2.1 can be found here: https://www.netiq.com/documentation/sentinel72/
[5] Found here: https://www.netiq.com/documentation/sentinel72/s721_admin/?page=/documentation/sentinel72/s721_admin/data/bookinfo.html
[6] Found here: https://www.netiq.com/documentation/sentinel72/s721_user/?page=/documentation/sentinel72/s721_user/data/bookinfo.html
[7] Found here: https://www.netiq.com/documentation/sentinel72/s721_install/?page=/documentation/sentinel72/s721_install/data/bookinfo.html
[8] Documentation for Sentinel Log Manager 1.2.2 can be found here: https://www.netiq.com/documentation/novelllogmanager12/
[9] Found here:
https://www.netiq.com/documentation/novelllogmanager12/log_manager_admin/?page=/documentation/novelllogmanager12/log_manager_admin/data/front.html

SECURITY ASSURANCE REQUIREMENT	EVIDENCE TITLE
AGD_PRE.1 Preparative Procedures	Sentinel 7.2.1Release Notes[10] NetIQ Sentinel Administration Guide[11] NetIQ Sentinel User Guide[12] NetIQ Sentinel Installation and Configuration Guide[13] NetIQ Sentinel Log Manager 1.2.2 Readme[14],[15] NetIQ® Sentinel™ 7.2.1 Operational User Guidance and Preparative Procedures Supplement
ALC_CMC.3 Authorization Controls	NetIQ® Sentinel™ 7.2.1 Configuration Management Processes and Procedures
ALC_CMS.3 Implementation representation CM coverage	NetIQ® Sentinel™ 7.2.1 Configuration Management Processes and Procedures
ALC_DEL.1 Delivery Procedures	Secure Delivery Processes and Procedures: NetIQ
ALC_DVS.1 Identification of Security Measures	Development Security Measures: NetIQ® Sentinel™ 7.2.1
ALC_LCD.1 Developer defined life-cycle model	Life Cycle Development Process: NetIQ® Sentinel™ 7.2.1
ALC_FLR.1: Flaw Remediation Procedures	Basic Flaw Remediation Procedures: NetIQ® Sentinel™ 7.2.1
ATE_COV.2 Analysis of Coverage	Test Plan and Coverage Analysis: NetIQ® Sentinel™ 7.2.1
ATE_DPT.1 Testing: Basic Design	Test Plan and Coverage Analysis: NetIQ® Sentinel™ 7.2.1
ATE_FUN.1 Functional Testing	Test Plan and Coverage Analysis: NetIQ® Sentinel™ 7.2.1

Table 18 – Security Assurance Rationale and Measures

[10] Found here: https://www.netiq.com/documentation/sentinel72/s721_release_notes/data/s721_release_notes.html
[11] Found here: https://www.netiq.com/documentation/sentinel72/s721_admin/?page=/documentation/sentinel72/s721_admin/data/bookinfo.html
[12] Found here: https://www.netiq.com/documentation/sentinel72/s721_user/?page=/documentation/sentinel72/s721_user/data/bookinfo.html
[13] Found here: https://www.netiq.com/documentation/sentinel72/s721_install/?page=/documentation/sentinel72/s721_install/data/bookinfo.html
[14] Note: Link on page is NetIQ Sentinel LogManager 1.2.2 Readme
[15] Found here: https://www.netiq.com/documentation/novelllogmanager12/log_manager_readme/data/log_manager_readme.html

7 TOE Summary Specification

This section presents the Security Functions implemented by the TOE.

7.1 TOE Security Functions

The security functions performed by the TOE are as follows:

- Security Audit
- Identification and Authentication
- Security Management

7.2 Security Audit

System Events is a means to report on the status and status change of the system. The TOE supports three types of events:

- Internal Events are informational and describe a single state or change of state in the system. They report when a user logs in or fails to authenticate, when a process is started or a correlation rule is activated.
- Performance Events are generated on a periodic basis and describe average resources used by different parts of the system
- Audit Events are generated internally. Each time an audited method is called or an audited data object is modified, audit framework generates audit events. There are two types of Audit Events. One which monitors user actions for example, user login/out, add/delete user and another which monitors system actions/health, for example, process start/stop. Audit Events can be logged into log files, saved into database, and sent out as Audit Event at the same time. (Internal Events are only sent out as events.).

System Events record the date and time of the event, type of event, subject identity and outcome.

The TOE generates the following audit data:

- Start-up and shutdown of the audit functions (instantiated by start-up of the TOE)
- User login/logout
- Login failures

The TOE provides the Administrator with the capability to read all audit data generated within the TOE via the Console. The GUI provides a suitable means for an Administrator to interpret the information from the audit log.

The TOE provides users with the capability to filter security event data queries and searches. Filter expressions are simple math expressions and simple evaluations. Filters work on selection sets

by matching events against the specified criteria. Filters are applied to data collected by the TOE. The Correlation Engine provides the capability for users to correlate security events. Correlation automates analysis of event data to find patterns of interest. The TOE enables users to define correlations between events through the definition of rules that define these patterns of interest.

The A.TIMESOURCE is added to the assumptions on operational environment, and OE.TIME is added to the operational environment security objectives. The time and date are provided by the operational environment. The TOE ensures that the audit trail data is stamped when recorded

with a dependable date and time received from the OE (operating system). In this manner, accurate time and date is maintained on the TOE.

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

- FAU_GEN.1
- FAU_SAR.1
- SIEM_ANL.1 (EXP)

7.3 Identification and Authentication

The Console provides user interfaces that administrators may use to manage TOE functions. The Console provides web-based access to TOE functions through supported web browsers. The TOE enforces individual identification and authentication and provides a centralized authentication mechanism. Operators with management access must successfully authenticate themselves using a unique identifier and authenticator prior to performing any actions on the TOE. The TOE maintains authorization information that determines which TOE functions an authenticated administrator or user (of a given role) may perform.

The TOE maintains the following list of security attributes belonging to individual users:

- User Identity (i.e., user name)
- Password
- Privileges

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

- FIA_ATD.1
- FIA_UAU.2
- FIA_UID.2

7.4 Security Management

The TOE provides the following management functions. The associated SFRs are noted in the table below.

Functional Description	SFR
The TOE enforces the Administrative Access Control SFP by only allowing Administrators to access system reports, component audit logs, TOE configuration, operator account attributes.	FDP_ACC.1
The TOE enforces the Administrative Access Control SFP by verifying user Identity, authentication status, and privileges. The TOE also explicitly denies access based on invalidation of username/password combination from the IT Environment.	FDP_ACF.1
Only Administrators have the capability to query, modify, or delete accounts and privileges.	FMT_MSA.1
The TOE provides restrictive default values for security attributes by requiring the Administrator to explicitly allow access to Users. Only the Administrator may be able to change defaults.	FMT_MSA.3
Only the Administrator can control user privileges and user accounts attributes.	FMT_MTD.1

Functional Description	SFR
The TOE supports the following management functions: a) Create accounts b) Modify accounts c) Define User privileges d) Change Default, Query, Modify, Delete, Clear the attributes associated with the Administrative Access Control SFP e) Modify the behavior of the Administrative Access Control SFP f) Manage security incidents g) Manage correlation rules.	FMT_SMF.1
The TOE provides only two user roles: Administrator and User and associates users to their roles. Administrator functions are defined in FMT_SMF.1. User privileges may be modified by the Administrator. By default, the User role allows limited viewing of events.	FMT_SMR.1
The TOE provides the capability for automating and tracking incident response processes. The TOE tracks security problems from identification through resolution by allowing the creation of "workflows". Workflows are designed to provide a simple, flexible solution for automating and tracking an enterprise's incident response processes. See NetIQ Sentinel User Guide for more information.	SIEM_RES.1 (EXP)

Table 19 – Security Management Functions and SFRs

End of Document