

NetIQ® Sentinel™ 8.1

Security Target

Date: August 8, 2018
Version: 2.0
Prepared By: NetIQ Corporation
Prepared For: NetIQ Corporation
Suite 1200
515 Post Oak Blvd
Houston, Texas 77027

Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), Sentinel 8.1. 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	<i>ST Reference</i>	5
1.2	<i>TOE Reference</i>	5
1.3	<i>Document Organization</i>	5
1.4	<i>Document Conventions</i>	6
1.5	<i>Document Terminology</i>	6
1.6	<i>TOE Overview</i>	7
1.7	<i>TOE Description</i>	7
1.7.1	<i>Overview</i>	7
1.7.2	<i>Console</i>	11
1.7.3	<i>Sentinel Server</i>	12
1.7.4	<i>Data Collector</i>	13
1.7.5	<i>Correlation Engine (CE)</i>	13
1.7.6	<i>Physical Boundary</i>	13
1.7.7	<i>Hardware and Software Supplied by the IT Environment</i>	15
1.7.8	<i>Logical Boundary</i>	16
1.7.9	<i>TOE Security Functional Policies</i>	16
1.7.10	<i>TOE Product Documentation</i>	16
2	Conformance Claims	17
2.1	<i>CC Conformance Claim</i>	17
2.2	<i>PP Claim</i>	17
2.3	<i>Package Claim</i>	17
2.4	<i>Conformance Rationale</i>	17
3	Security Problem Definition	18
3.1	<i>Threats</i>	18
3.2	<i>Organizational Security Policies</i>	18
3.3	<i>Assumptions</i>	18
4	Security Objectives	20
4.1	<i>Security Objectives for the TOE</i>	20
4.2	<i>Security Objectives for the Operational Environment</i>	20
4.3	<i>Security Objectives Rationale</i>	21
4.3.1	<i>Rationale for Security Threats to the TOE</i>	21
5	Extended Components Definition	24
5.1	<i>Definition of Extended Components</i>	24
5.1.1	<i>Class SIEM: Incident Management</i>	24
5.1.2	<i>Class FTA: TOE Access</i>	25
6	Security Requirements	27
6.1	<i>Security Functional Requirements</i>	27
6.1.1	<i>Security Audit (FAU)</i>	27
6.1.2	<i>Information Flow Control (FDP)</i>	28
6.1.3	<i>Identification and Authentication (FIA)</i>	28
6.1.4	<i>Security Management (FMT)</i>	29

- 6.1.5 TOE Access (FTA).....30
- 6.1.6 Incident Management (SIEM)30
- 6.2 *Security Assurance Requirements*30
- 6.3 *Security Requirements Rationale*31
 - 6.3.1 Security Functional Requirements.....31
 - 6.3.2 Dependency Rationale.....31
 - 6.3.3 Sufficiency of Security Requirements32
 - 6.3.4 Security Assurance Requirements33
 - 6.3.5 Security Assurance Requirements Rationale34
 - 6.3.6 Security Assurance Requirements Evidence34
- 7 TOE Summary Specification..... 36**
 - 7.1 *TOE Security Functions*.....36
 - 7.2 *Security Audit*36
 - 7.3 *Identification and Authentication*37
 - 7.4 *Security Management*.....37
- 8 Appendix A – Default Sentinel Roles 39**
- 9 Appendix B 41**
- 10 Appendix C 42**

List of Tables

Table 1 – ST Organization and Section Descriptions	6
Table 2 – Acronyms Used in Security Target	6
Table 3 – Evaluated Configurations for the TOE	14
Table 4 – IT Environment	15
Table 5 - Appliance Minimum Hardware	15
Table 6 – Logical Boundary Descriptions	16
Table 7 – Threats Addressed by the TOE	18
Table 8 – Organizational Security Policies	18
Table 9 – Assumptions	19
Table 10 – TOE Security Objectives	20
Table 11 – Operational Environment Security Objectives	20
Table 12 – Mapping of Assumptions, Threats, and OSPs to Security Objectives	21
Table 13 – Mapping of Threats, Policies, and Assumptions to Objectives	23
Table 14 – TOE Security Functional Requirements	27
Table 15 – Management of TSF data	29
Table 16 – Mapping of TOE Security Functional Requirements and Objectives.....	31
Table 17 – Rationale for TOE SFRs to Objectives	33
Table 18 – Security Assurance Requirements at EAL3.....	34
Table 19 – Security Assurance Rationale and Measures	35
Table 20 – Security Management Functions and SFRs	38

List of Figures

Figure 1 – Basic Sentinel 8.1 Configuration	7
Figure 2 – Sentinel 8.1 Configuration with External Datastore	8
Figure 3 – Sentinel 8.1 Appliance Configuration	8
Figure 4 – Functional Block Diagram	9
Figure 5 – Sentinel Conceptual Architecture	10
Figure 6 – Sentinel Sample Data Flow	11
Figure 7 – TOE Boundary	14

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™ 8.1
ST Revision	2.0
ST Publication Date	August 8, 2018
Author	Michael F. Angelo

1.2 TOE Reference

TOE Reference	NetIQ® Sentinel™ 8.1.0.1_4309
----------------------	-------------------------------

Note: The official name of the product is: NetIQ Sentinel Enterprise 8.1 (aka Sentinel 8.1 Enterprise). The released product can be uniquely identified as: NetIQ Sentinel Enterprise 8.1.0.1_4309, or Sentinel 8.1.0.1_4309. The product name may also be referred to as or Sentinel 8.1.0 and abbreviated as 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.

1.3 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
EOE	Events Originating External to the TOE
ISO	International Standards Organization. When referring to a CD or DVD it means ISO-9660
NTP	Network Time Protocol
OSP	Organizational Security Policy
OVF	Open Virtualization Format
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™ 8.1. NetIQ® Sentinel™ 8.1 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).

1.7 TOE Description

1.7.1 Overview

The TOE consists of the following components:

- Console
- Sentinel Server
- Data Collector
- Correlation Engine (CE)

The basic configuration is depicted in the figure¹ below:

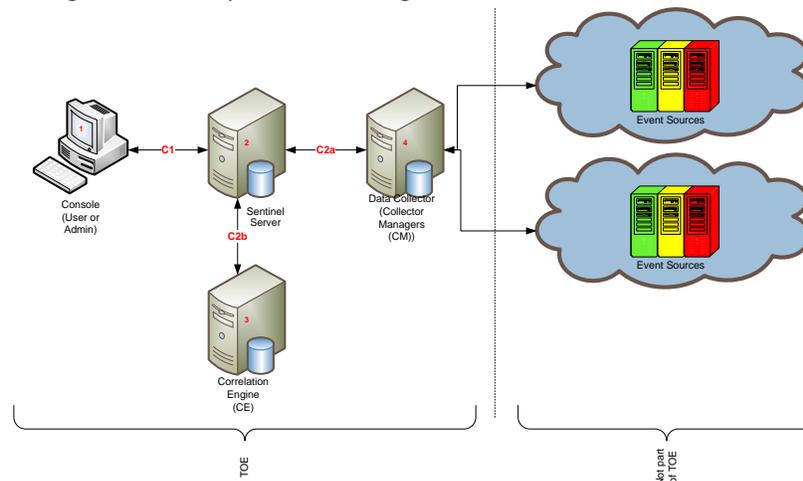


Figure 1 – Basic Sentinel 8.1 Configuration

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.

The figure below depicts the TOE in a complex environment.

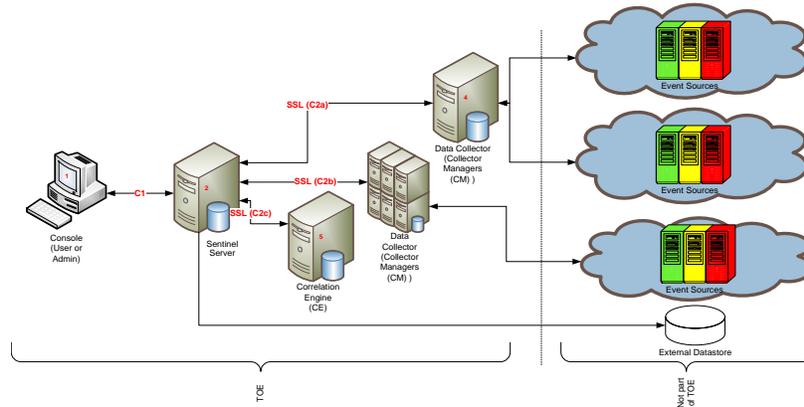


Figure 2 – Sentinel 8.1 Configuration with External Datastore

The following depicts the TOE in an appliance configuration:

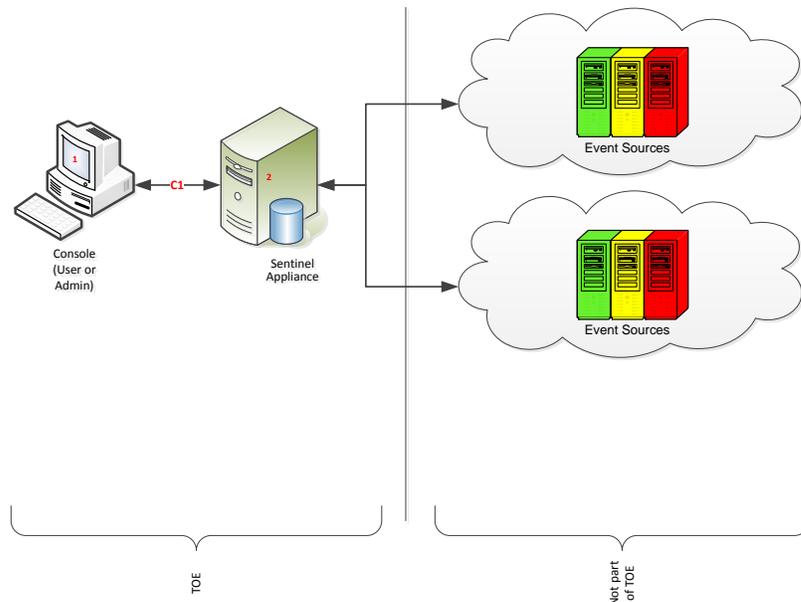
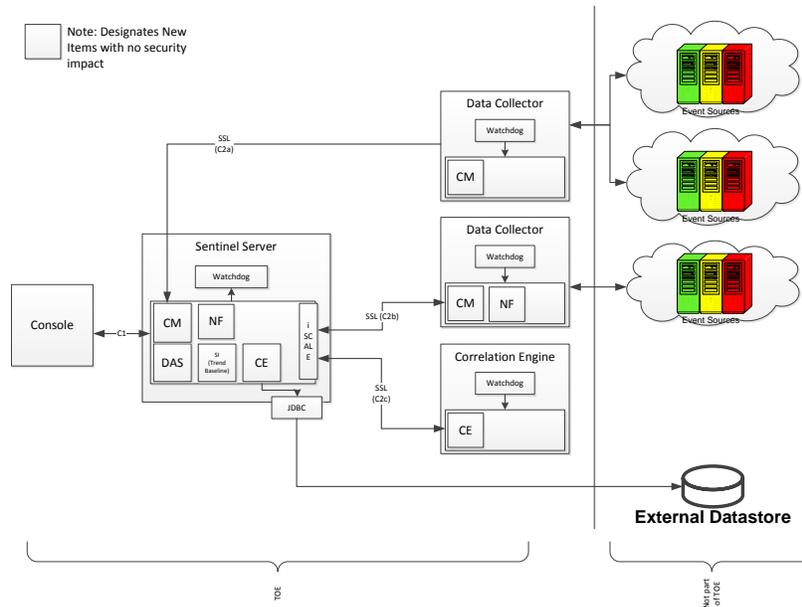


Figure 3 – Sentinel 8.1 Appliance Configuration

It is important to note that all components in the Sentinel architecture can scale with multiple instances of the components. Note the appliance contains all components in the Sentinel Architecture (Sentinel Server, Data Collector, and Correlation Engine (CE)).

The following diagram reflects the functional blocks in the configuration:



Sentinel works by:

1. Gathering logs, events, and security information 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, NetIQ Sentinel, and NetIQ Sentinel Rapid Deployment.

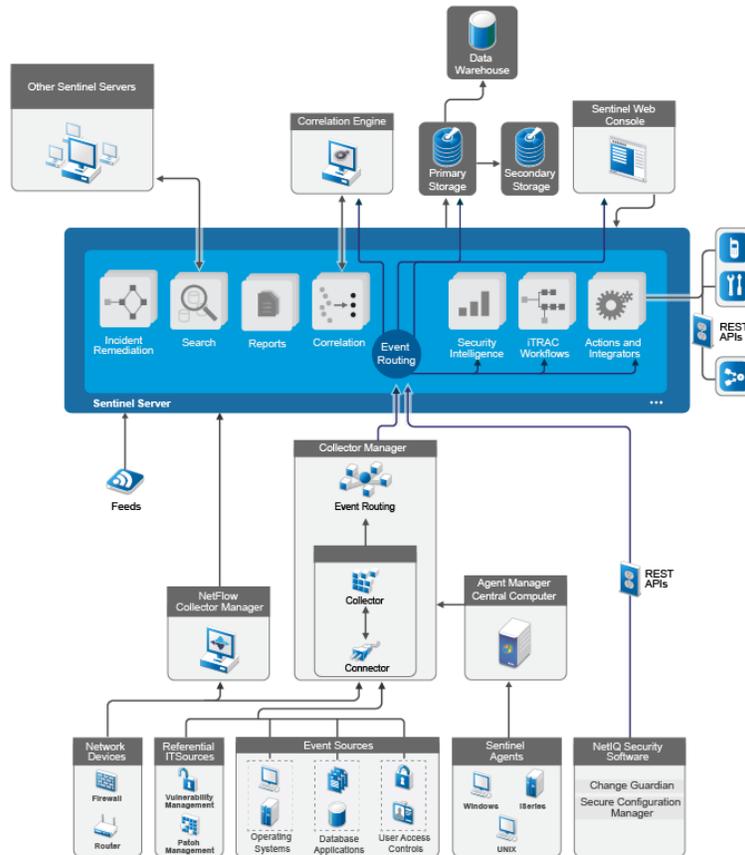


Figure 5 – Sentinel Conceptual Architecture

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's 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.

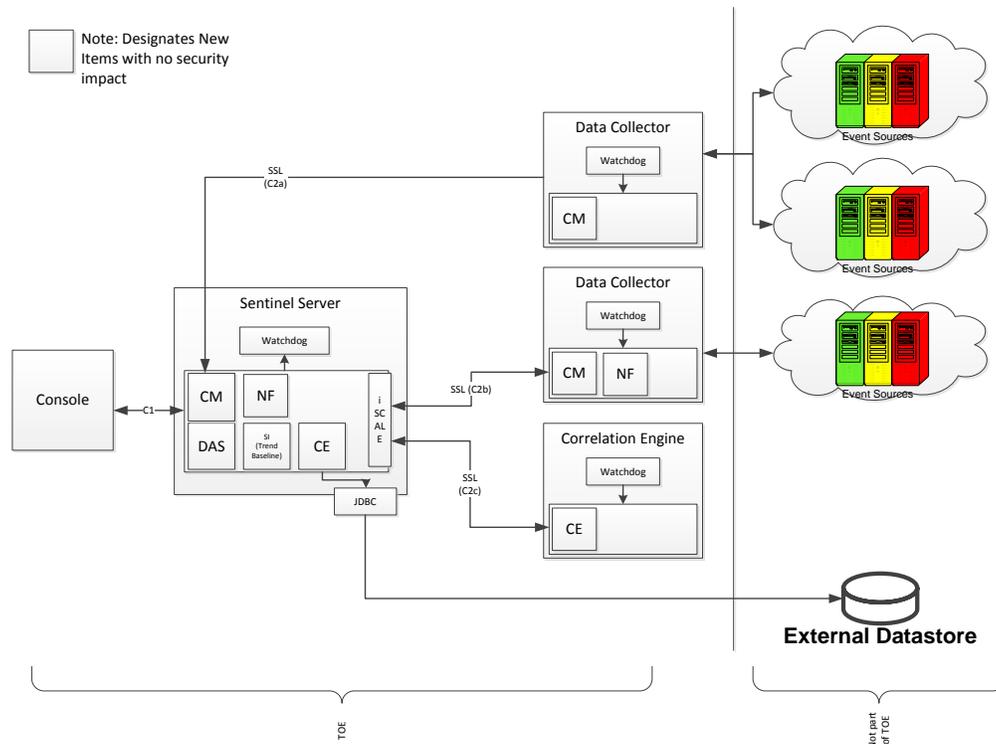


Figure 6 – Sentinel Sample Data Flow

1.7.2 Console²

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.

² Note: The console is used for management and operational user functions and may be referred to as User Console or Administrator Console depending on the functions it is performing. It may also be referred to as the Sentinel Web Interface in a generic form.

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 (Watchdog)
- Collector Manager (CM)
- Data Access Service (DAS)
- Correlation Engine (CE)
- NetFlow Collector Manager (NF)
- iSCALE

1.7.3.1 Sentinel Service Wrapper (Watchdog)

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, receives events from external event sources, 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.

1.7.4.1 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.

1.7.5 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, the watchdog component also keeps track of the CE.

1.7.6 Physical Boundary

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

- Console
- Sentinel Server
- Data Collector
- Correlation Engine (CE)

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

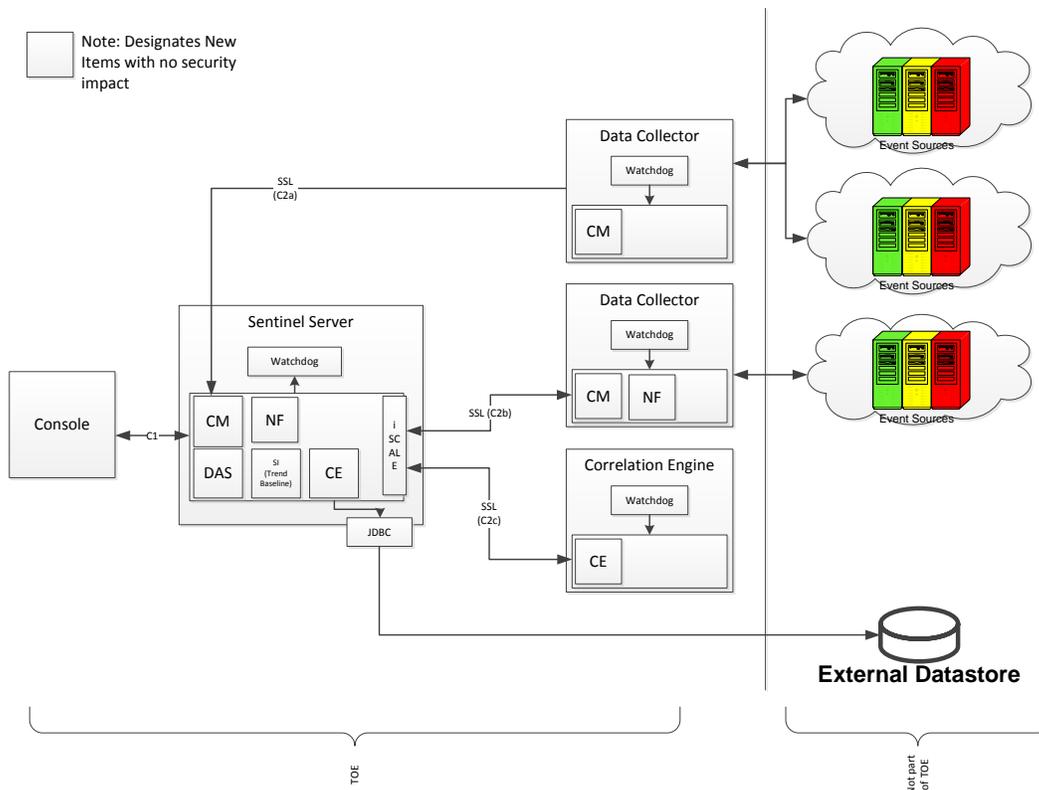


Figure 7 – TOE Boundary

The evaluation consists of two configurations for the product. The first configuration consists of the Basic Sentinel Server product as depicted in Figure 1. The second configuration is a virtual appliance in the form of an OVF as depicted in Figure 3.

COMPONENT	VERSION NUMBER
Sentinel Server	Version 8.1.0.1_4309 ³
Sentinel Appliance	Version 8.1.0.1_4309 ⁴

Table 3 – Evaluated Configurations 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.

Note the external Datastore is explicitly excluded from the certification configuration.

Note the Webyast and SSHD facilities are explicitly excluded from the certification configuration.

³ The appliance and server numbers are the same as they are just deployment configurations.

⁴ The appliance was updated and re-tested with a ‘buddy drop’ to address a security issue. Since the testing appliance was not registered as a customer owned product it needed to be updated out of band with patch: 8.1.1.0-4313.

1.7.7 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) 12 SP2 64-bit Red Hat Enterprise Linux Server (RHEL) 7.3 64-bit
	CPU	Intel(R) Xeon(R) CPU E5420@ 2.50GHz (8 CPU cores), without Intel HT Technology
	Memory	16GB
	Storage	500 GB 7.2k RPM drive
	Optional External Datastore	Microsoft SQL Server 2012
Data Collector	Operating System	SLES 12 SP2 64-bit or SLES 11 SP4
	CPU	Intel Xeon E5450 3-Ghz (4 cores)
	Memory	4 GB
	Storage	50 GB (RAID 1)
Correlation Engine	Operating System	SLES 12 SP2 64-bit or SLES 11 SP4
	CPU	Intel(R) Xeon(R) CPU E5-2650 O@2.00 GHz, 4 cores (virtual machine)
	Memory	8 GB
	Storage	100 GB
Console	Operating System	Windows 10 (Microsoft Edge, Google Chrome, Mozilla Firefox, Microsoft Internet Explorer 11)
	Operating System	SLES 12 SP2 or SLES 11 SP4 / RHEL 7.3 (Mozilla Firefox)

Table 4 – IT Environment

The Sentinel appliance requires the following minimum hardware configuration:

TOE COMPONENT	TYPE	VERSION/MODEL NUMBER
Sentinel Server Appliance	Appliance installation:	VMware ESX 6.5 (OVF)
	Operating System	SUSE Linux Enterprise Server (SLES) 12 SP2 64-bit or SLES 11 SP4 Red Hat Enterprise Linux Server (RHEL) 7.3 64-bit
	CPU	Intel(R) Xeon(R) CPU E5420@ 2.50GHz (8 CPU cores), without Intel HT Technology
	Memory	16GB
	Storage	500 GB 7.2k RPM drive

Table 5 - Appliance Minimum Hardware

1.7.8 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. The TOE provides an inactivity timeout mechanism.
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 6 – Logical Boundary Descriptions

1.7.9 TOE Security Functional Policies

The TOE supports the following Security Functional Policy:

1.7.9.1 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 user roles. An authorized administrator can define specific privileges available to administrators and users via the Console.

1.7.9.2 User Roles SFP

The TOE implements user roles via defined collections of privileges. These privileges are defined and assigned by the administrator. Users can only have a single role at one time.

1.7.10 TOE Product Documentation

The TOE includes the following product documentation⁵:

- Sentinel 8.1.0.1 Release Notes July 2017
- NetIQ® Sentinel™ Administration Guide June 2017
- NetIQ® Sentinel™ User Guide June 2017
- NetIQ® Sentinel™ Installation and Configuration Guide June 2017

⁵ <https://www.netiq.com/documentation/sentinel-80/>

2 Conformance Claims

2.1 CC Conformance Claim

The TOE is conformant to Common Criteria Version 3.1 CC Revision 5, April 2017 Part 2 extended and Part 3 conformant.

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 5 (April 2017)). The TOE does not claim conformance to any functional package. The TOE EAL3 assurance package is augmented with ALC_FLR.1.

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. The asset is the configuration of the TOE.
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. The asset are the configuration of the TOE, data that is collected, and the resultant analysis by the TOE.

Table 7 – 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. This enables the detection of potential events that may represent a security issue or other issues that may require additional analysis and mitigation.
P.INCIDENTS	Security events correlated and classified as incidents should be managed to resolution. This enables the detection and potential prevention of harm to the TOE or the infrastructure the TOE is used to monitor and or protect.

Table 8 – 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 (and competent) 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
A.LOCATE	The processing platforms on which the TOE resides are assumed to be located within a facility that provides controlled access
A.DS_PROTECT	The External Datastore(s) are located within a facility that provides physical and logical 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
A.UPDATE	The TOE environment is regularly updated to address potential and actual vulnerabilities.

Table 9 – 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. The collected data is critical to the analysis and tracking of events in the environment which might indicate security issues.
O.MANAGE_INCIDENT	The TOE shall provide a workflow to manage events and incidents. This workflow enables the TOE to provide responses that authorized users may execute to analyze and expedite potential security events and issues. Thus enabling TOE users to respond faster.
O.SEC_ACCESS	The TOE shall ensure that only those authorized users and applications are granted access to security functions and associated data. This prevents unauthorized users from performing actions that may disable the TOE and result in undetected security events and issues.

Table 10 – 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 to not disclose their authentication credentials. Authorized administrators are also required to manage and administer the TOE in a secure manner. Authorized administrators must be competent and security aware personnel in accordance with the administrator documentation.
OE.PHYSEC	The facility surrounding the processing platform in which the TOE resides must provide a controlled means of access into the facility
OE.DS_PROTECT	The facility surrounding the External Datastore platform must provide physical and logical controlled access.
OE.UPDATE	The TOE environment is regularly updated to address potential and actual vulnerabilities.

Table 11 – 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	O.CAPTURE_EVENT	O.MANAGE_INCIDENT	O.SEC_ACCESS	OE.TIME	OE.ENV_PROTECT	OE.PERSONNEL	OE.PHYSEC	OE.DS_PROTECT	OE.UPDATE
ASSUMPTIONS/ THREATS/ POLICIES									
A.CONFIG						✓			
A.MANAGE						✓			
A.NOEVIL						✓			
A.LOCATE							✓		
A.TIMESOURCE				✓					
A.DS_PROTECT								✓	
A.UPDATE									✓
T.NO_AUTH			✓		✓	✓	✓		
T.NO_PRIV			✓						
P.EVENTS	✓			✓		✓			
P.INCIDENTS		✓		✓		✓			

Table 12 – 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 <ul style="list-style-type: none"> OE.PERSONNEL, which ensures that the TOE is managed and administered in a secure manner by 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 <ul style="list-style-type: none"> OE.PERSONNEL, which ensures that the TOE is managed and administered 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 in a secure manner by 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

ASSUMPTION/ THREAT/ POLICY	RATIONALE
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.
A.DS_PROTECT	This assumption is addressed by OE.DS_PROTECT, which ensures that the facility surrounding the External Datastore platform has both physical and logical controlled access.
A.UPDATE	This assumption is addressed by OE.UPDATE. <ul style="list-style-type: none"> • OE.UPDATE which requires the TOE environment be updated regularly to address potential and actual operational security issues.
T.NO_AUTH	This threat is countered by the following: <ul style="list-style-type: none"> • 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 in a secure manner by 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 <ul style="list-style-type: none"> • 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.

ASSUMPTION/ THREAT/ POLICY	RATIONALE
P.INCIDENTS	<p>This organizational security policy is enforced by</p> <ul style="list-style-type: none"> • 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 13 – 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

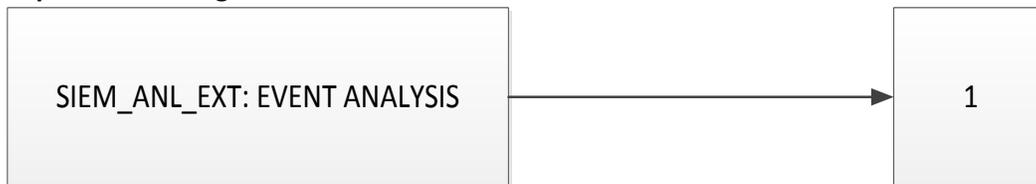
Incident Management functions provide the capability to analyze security event data and incident workflow.

5.1.1.1 Event Analysis SIEM_ANL_EXT

Family Behavior

This family defines the requirements for security event analysis functionality.

Component Leveling



SIEM_ANL_EXT Event Analysis provides the analysis of security event data.

Management: SIEM_ANL_EXT.1

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

- a) Configuration of the analysis to be performed

Audit: SIEM_ANL_EXT.1

There are no auditable events foreseen.

SIEM_ANL_EXT.1 Event Analysis

Hierarchical to: No other components

Dependencies: No dependencies

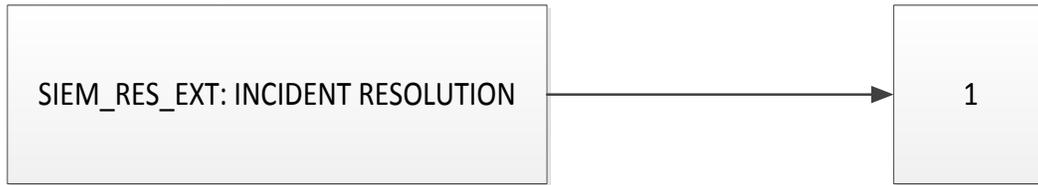
SIEM_ANL_EXT.1.1 The TSF shall perform [assignment: list of analysis functions] analysis function(s) on data collected from security and non-security products within a network.

5.1.1.2 Incident Resolution SIEM_RES_EXT

Family Behavior

This family defines the requirements for security incident functionality.

Component Leveling



SIEM_RES_EXT provides the incident resolution workflow functionality.

Management: SIEM_RES_EXT.1

There are no management activities foreseen.

Audit: SIEM_RES_EXT.1

There are no auditable events foreseen.

Incident Resolution: SIEM_RES_EXT.1

Hierarchical to: No other components

Dependencies: No dependencies

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

5.1.2 Class FTA: TOE Access

TOE Access functions provide facilities and controls for access to the TOE.

5.1.2.1 Session locking and termination FTA_SSL_EXT

Component Leveling



FTA_SSL_EXT TSF-initiated session locking includes system initiated locking of an interactive session after an administrator configured of user inactivity time interval has expired, but does not include clearing or overwriting the display.

Management: FTA_SSL_EXT.1

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

- a) specification of the time of user inactivity after which termination of the interactive session occurs for an individual user;

Audit: FTA_SSL_EXT.1

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

- a) Minimal: Locking of an interactive session by the session locking mechanism.
- b) Minimal: Successful unlocking of an interactive session.
- c) Basic: Any attempts at unlocking an interactive session.

FTA_SSL_EXT.1

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Timing of authentication

FTA_SSL_EXT.1.1 The TSF shall lock an interactive session [after an administrator-configured user inactivity time interval has expired] by disabling any users actions other than unlocking the session

FTA_SSL_EXT.1.2 The TSF shall require the following events to occur prior to unlocking the session [the user must re-authenticate to the TOE].

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
	FTA_SSL_EXT.1	TSF-initiated session locking
	FTA_SSL.4	User-initiated termination
Incident Management	SIEM_ANL_EXT.1	Event Analysis
	SIEM_RES_EXT.1	Incident Resolution

Table 14 – 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 of the TOE;
- d) Login failures;
- e) Events from security products and non-security products]

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, and designated operators] with the capability to read [all audit data generated within the TOE, all data received / processed] 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, configuration
Operations: all user actions⁶]

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, Roles
Objects: System reports, component audit logs, configuration⁷,
Object Attributes: source of data.
Operations: View, Manage, Search, Run Reports, Share]

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [Role association based on user authentication and source of data (i.e. role)].

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: [No Additional Rules].

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, Roles].

⁶ For example - Run report, schedule report, create role, create a user,

⁷ Configurations include the establishment and access to Correlation Engine/Rules, Reports, incidents, Event Actions

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.

6.1.4 Security Management (FMT)

6.1.4.1 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 [change_default values, query, modify, delete] the security attributes [User identity or Roles] to [Administrator].

6.1.4.2 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 Roles must be explicitly granted by the Administrator. The default is to deny access to privileges not associated with Roles. <see Appendix B>

6.1.4.3 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to [perform the functions listed in Table 15] the [data described in the Table 15] to [Administrator]:

ROLE DATA	CHANGE_DEFAULT	QUERY	MODIFY	DELETE
User Role	✓	✓	✓	✓
User Account Attributes		✓	✓	

Table 15 – Management of TSF data

6.1.4.4 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 Rolls
- d) Change Default, Query, Modify 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

- h) Manage Reports and Searches
- i) Change the user inactivity timeout ⁸interval].

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.

6.1.4.5 **FMT_SMR.1 Security Roles**

FMT_SMR.1.1 The TSF shall maintain the roles [Administrator, Other Roles as described in Appendix A].

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

6.1.5 **TOE Access (FTA)**

6.1.5.1 **FTA_SSL_EXT.1 TSF-initiated session locking**

FTA_SSL_EXT.1.1 The TSF shall lock an interactive session [after an administrator-configured user inactivity time interval has expired] by disabling any user actions other than unlocking the session

FTA_SSL_EXT.1.2 The TSF shall require the following events to occur prior to unlocking the session: [the user must re-authenticate to the TOE].

6.1.5.2 **FTA_SSL.4 User-initiated termination**

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

6.1.6 **Incident Management (SIEM)**

6.1.6.1 **SIEM_ANL_EXT.1 Event Analysis**

SIEM_ANL_EXT.1.1 The TSF shall perform [filtering and correlation] analysis function(s) on data collected from security and non-security products within a network.

6.1.6.2 **SIEM_RES_EXT.1 Incident Resolution**

SIEM_RES_EXT.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.

⁸ The variable is userSessionManager expireTime in server.xml – note for ATE work. TBR prior to publication.

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.

OBJECTIVE SFR	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			✓
FTA_SSL_EXT.1			✓
FTA_SSL.4			✓
SIEM_ANL_EXT.1	✓		
SIEM_RES_EXT.1		✓	

Table 16 – 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	

SFR CLAIM	DEPENDENCIES	DEPENDENCY MET	RATIONALE
FIA_UAU.2	FIA_UID.1	YES	Although FIA_UID.1 is not included, FIA_UAU.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
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	
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	
FTA_SSL_EXT.1	FIA_UAU.1	Yes	Satisfied by FIA_UAU.2, which is hierarchical to FIA_UAU.1
FTA_SSL.4	N/A	N/A	
SIEM_ANL_EXT.1	N/A	N/A	
SIEM_RES_EXT.1	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	<p>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:</p> <ul style="list-style-type: none"> 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_EXT.1 ensures that the TOE performs analysis on all security events received from network devices

Objective	RATIONALE
O.MANAGE_INCIDENT	<p>The objective to ensure that the TOE provides a workflow to manage incidents is met by the following security requirements:</p> <ul style="list-style-type: none"> • 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_EXT.1 ensures that the TOE provides the capability to manage status and track action items in the resolution of incidents
O.SEC_ACCESS	<p>This objective ensures that the TOE allows access to the security functions, configuration, and associated data only by authorized users and applications.</p> <ul style="list-style-type: none"> • 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 roles 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 perform the functions listed in Table 15 on TSF data to the Administrator. • FMT_MSA.1 specifies that only privileged administrators can manage security attributes. • 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 can specify alternative initial values that will override default values. • FMT_SMF.1 and FMT_SMR.1 support the security functions relevant to the TOE and ensure the definition of an authorized administrator role. • FTA_SSL_EXT.1 requires the TSF lock after a period of inactivity. • FTA_SSL.4 requires the user be able to initiate a session termination.

Table 17 – 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

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
ALC: Lifecycle Support	ALC_CMC.3	Authorization Controls
	ALC_CMS.3	Implementation representation CM coverage
	ALC_DEL.1	Delivery Procedures
	ALC_DVS.1	Identification of Security Measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_FLR.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 18 – 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.

SECURITY ASSURANCE REQUIREMENT	EVIDENCE TITLE
ADV_ARC.1 Security Architecture Description	NetIQ® Sentinel™ 8.1 Security Architecture (ADV_ARC)
ADV_FSP.3 Functional Specification with Complete Summary	NetIQ® Sentinel™ 8.1 Functional Specification
ADV_TDS.2 Architectural Design	NetIQ® Sentinel™ 8.1 Architectural Design
AGD_OPE.1 Operational User Guidance	NetIQ® Sentinel™ Administration Guide June 2017 NetIQ® Sentinel™ User Guide June 2017 NetIQ® Sentinel™ Installation and Configuration Guide June 2017 NetIQ® Sentinel™ 8.1 Operational User Guidance and Preparative Procedures Supplement

SECURITY ASSURANCE REQUIREMENT	EVIDENCE TITLE
AGD_PRE.1 Preparative Procedures	Sentinel 8.1.0.1 Release Notes July 7, 2017 ⁹ NetIQ® Sentinel™ Administration Guide June 2017 ¹⁰ NetIQ® Sentinel™ User Guide June 2017 ¹¹ NetIQ® Sentinel™ Installation and Configuration Guide June 2017 ¹² NetIQ® Sentinel™ 8.1 Operational User Guidance and Preparative Procedures Supplement
ALC_CMC.3 Authorization Controls	NetIQ® Sentinel™ 8.1 Configuration Management Processes and Procedures (ALC_CM)
ALC_CMS.3 Implementation representation CM coverage	NetIQ® Sentinel™ 8.1 Configuration Management Processes and Procedures (ALC_CM)
ALC_DEL.1 Delivery Procedures	NetIQ® Sentinel™ Secure Delivery Processes and Procedures: (ALC_DEL)
ALC_DVS.1 Identification of Security Measures	NetIQ® Sentinel™ Development Security Measures (ALC_DVS)
ALC_LCD.1 Developer defined life-cycle model	NetIQ® Sentinel™ Life Cycle Development Process (ALC_LCD)
ALC_FLR.1: Flaw Remediation Procedures	NetIQ® Sentinel™ Basic Flaw Remediation Procedures(ALC_FLR)
ATE_COV.2 Analysis of Coverage	NetIQ® Sentinel™ Test Plan and Coverage Analysis
ATE_DPT.1 Testing: Basic Design	NetIQ® Sentinel™ Test Plan and Coverage Analysis
ATE_FUN.1 Functional Testing	NetIQ® Sentinel™ Test Plan and Coverage Analysis

Table 19 – Security Assurance Rationale and Measures

⁹Found here: https://www.netiq.com/documentation/sentinel-81/sentinel8101_release_notes/data/sentinel8101_release_notes.html

¹⁰Found here: <https://www.netiq.com/documentation/sentinel-81/pdfdoc/admin/admin.pdf>

¹¹ Found here: <https://www.netiq.com/documentation/sentinel-81/pdfdoc/user/user.pdf>

¹² Found here: <https://www.netiq.com/documentation/sentinel-81/pdfdoc/install/install.pdf>

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

Events Originating External to the TOE (EOE): These external events are collected, either via a push or pull, from the various event sources. Event sources may include and are not limited to, remote operating systems, firewalls, routers, and other security devices.

These event are consumed by the TOE, and are normalized into a common schema and classification taxonomy. This data is then correlated and used to detect abnormal behavior and anomalies within your infrastructure. These may also include alerts that indicate interesting events such as those dealing with security or threshold violations.

EOE includes timestamps, origin, event information, completion status of the event, and other data as specified in the report.

System Events: System events are a means to report on the status and status change of the TOE. While the TOE accepts events from outside, it can generate three classes of events:

- **Internal Events:** These 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:** These are generated on a periodic basis and describe average resources used by different parts of the system
- **Audit Events:** These 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/logout, 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, event subject identity and outcome of the event.

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

Audit Handing: The TOE provides the Administrator with the capability to read all audit data generated within the TOE via the Console or via the external event sources. The GUI provides a

suitable means for an Administrator to interpret the information from either the audit log or EOE as configured.

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_EXT.1

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
- Roles

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

Security Management is provided by enforcement of roles. Each role consists of a series of privileges. Roles can have privileges added to or removed from them. These roles are then assigned to individuals. Note a user may only have one role at a time.

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 or accounts with appropriate roles (Appendix A) to perform activities (Appendix B).	FDP_ACC.1
The TOE enforces the Administrative Access Control SFP by verifying user identity and roles.	FDP_ACF.1
Only Administrators have the capability to change default values, query, modify, or delete users or roles.	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
The TOE supports the following management functions: <ul style="list-style-type: none"> a) Create accounts b) Modify accounts c) Define User Roles <p>Note: Roles allow you define user actions and what data they can view. Permissions are granted to the role, and then the user is assigned to the role.</p> 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. h) Manage Reports and Searches i) Change the user inactivity timeout ¹³interval] 	FMT_SMF.1
The TOE provides multiple user roles. For a complete list of default roles, refer to Appendix A. 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 TSF initiated locking of interactive sessions after a specified period of user inactivity.	FTA_SSL_EXT.1
The TOE provides the capability for user initiated termination of interactive sessions.	FTA_SSL.4
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_EXT.1

Table 20 – Security Management Functions and SFRs

¹³ The variable is userSessionManager expireTime in server.xml – note for ATE work. TBR prior to publication.

8 Appendix A – Default Sentinel Roles¹⁴

Role	Description
Administrator:	A user in this role has administrative rights in the Sentinel system. You cannot delete users in this role. Administrative rights include the ability to perform user administration, data collection, data storage, search operations, rules, report, dashboard, and license management. You cannot modify or delete the administrator role.
Database Administrator:	A user in this role has access to events coming from database event sources. The Collector parsing the data from the event source determines the type of the event source (database). A user in this role can view data that matches filter <code>rv32:"DB"</code> and search data targets.
Data Proxy User:	This is a system role for proxy users. This role is critical to setting up another Sentinel system to access your local Sentinel system using the Data Federation feature.
Incident Administrator:	A user in this role can manage incidents in the system and control incidents being handled by other users.
NetFlow Provider:	A user in this role can send NetFlow data to Sentinel and manage NetFlow Collector Managers. A user in this role can also view and analyze the NetFlow data.
Network Administrator:	A user in this role can administer network infrastructure devices, such as routers, switches, and VPNs. This role has access to events coming from devices in the category <code>NETD</code> or <code>VPN</code> (as determined by the Collector parsing the data) or from event sources with the <code>Network</code> tag. Set the <code>Network</code> tag on network infrastructure event sources to allow users in this role to view the events. A user in this role can view data that matches filter <code>rv32:"NETD" OR rv32:"VPN" OR rv145:"Network"</code> , and can search data targets.
Network Security Administrator:	A user in this role can administer network security infrastructure devices, such as firewalls, Ides, and Web proxies. This role has access to events coming from devices in the category <code>AV</code> , <code>FW</code> , or <code>IDS</code> (as determined by the Collector parsing the data) or from event sources with the <code>NetworkSecurity</code> tag. Set the <code>NetworkSecurity</code> tag on network infrastructure event sources to allow users in this role to view the events. A user in this role can view data that matches filter <code>rv32:"AV" OR rv32:"FW" OR rv32:"IDS" OR rv145:"NetworkSecurity"</code> , and can search data targets.
Operator:	A user in this role can manage alerts, view Security Intelligence Dashboards, share alert and event views, run reports, view and rename reports, and delete report results. The Threat Response Dashboard allows Operators to triage alerts quickly and efficiently.
PCI Compliance Auditor:	A user in this role has access to view events that are tagged with at least one of the regulation tags such as <code>PCI</code> , <code>SOX</code> , <code>HIPAA</code> , <code>NERC</code> , <code>FISMA</code> , <code>GLBA</code> , <code>NISPOM</code> , <code>JSOX</code> , and <code>ISO/IEC_27002:2005</code> , and can view system events, view the Sentinel configuration data, and search data targets.

¹⁴ Section 4 Administrative Manual. Configuring Roles and Users, Overview

Role	Description
Report Administrator:	A user in this role can run reports, view, rename and delete report results, add and delete report templates and report results, run reports on configuration database, export all reports, and save search results as a report. A Report Administrator can also tag report templates and report results. The Report Administrator can search report templates and report results based on these tags.
Security Policy Administrator:	A user in this role can implement the security policies within the system for users to access anomaly detection, correlation, incident remediation, and iTRAC workflows.
System Event Monitor:	A user in this role can monitor the Sentinel system for errors or outages. This role has access only to events coming from Sentinel systems. A user in this role can also access data coming from event sources that Sentinel is dependent on. For example, you can tag operating systems on which Sentinel and the Collector Managers are running with a Sentinel event source tag so that the users in this role can monitor problems in the operating systems. A user in this role can view data that matches filter <code>rv145:"Sentinel"</code> , view system events, and search data targets.
Unix Administrator:	A user in this role has access to events from operating system event sources that are not Windows computers. The type of the event source is determined by verifying the Collector parsing data and also by verifying if a <code>Windows</code> tag is present. A user in this role can view data that matches filter <code>(rv32:"OS" NOT ("Microsoft?Active?Directory*" NOT msg:"Microsoft?Active?Directory*") OR ("Microsoft?Windows*" NOT msg:"Microsoft?Windows*")) NOT rv145:"Windows"</code> and search data targets.
User:	A user in this role can manage dashboards, run reports, view and rename reports, and delete report results.
Windows Administrator:	A user in this role can administer Windows computers. This role has access to data generated by Windows event sources. The type of the event source is determined by verifying the Collector parsing the data. If data from a Windows event source is not being processed by the Active Directory or the Windows Collector, add the <code>Windows</code> tag to event sources to indicate that Windows data is being collected from the event source. This enables the Windows administrator to access the data. A user in this role can view data that matches filter <code>(rv32:"OS" AND ("Microsoft?Active?Directory*" NOT msg:"Microsoft?Active?Directory*") OR ("Microsoft?Windows*" NOT msg:"Microsoft?Windows*")) OR rv145:"Windows"</code> and search data targets.

9 Appendix B

Listed Privileges that can be assigned to a role.

Events

- View all event data (including raw data and NetFlow data)
 - Manage Correlation Engines/Rules
 - Manage and View Security Intelligence Dashboards
 - View Security Intelligence Dashboards

View the following data:

- Only events matching the criteria: <Custom Filter>
- Search Data Targets
- View NetFlow data
- View asset data
- View asset vulnerability data
- View data in the embedded database
- View people browser
- View system events

Reports

- Allow users to access reports
 - Manage reports
 - Import reports
 - Run reports

Alerts

- Allow users to manage alerts
 - Manage all alerts
 - Manage only alerts that match the following criteria: <Custom alert>

Incidents

- View incidents (restricted)
- Create incidents (restricted)
- Modify incidents (restricted)
- Manage incidents (all)

Sharing

- Share alert views
- Share event views
- Share reports
- Share search filters

Miscellaneous

- Create and use Event Views
- Edit knowledge base
- Manage Tags
- Manage roles and users
- Proxy for Authorized Data Requestors
- Send NetFlow data
- Solution Designer access
- View and execute event actions
- View detailed internal system state data
- View knowledge base

10 Appendix C

Setting auto timeout

The *server.xml*, *collector_mgr.xml*, and *correlation_engine.xml* files include advanced configuration options. If you need to modify the default values, it is important to set the values using the instructions described in this section because these XML files automatically get replaced during upgrade, which results in any modifications getting overwritten.

Consider an example where you want to customize the `tokenExpireTime` property in the `AuthenticationService` component below, which is present in the `server.xml` file:

```
<obj-component id="AuthenticationService">
<class>esecurity.ccs.comp.auth.AuthenticationService</class>
<property name="handler">esecurity.login.request</property>
<property name="maxThreads">100</property>
<property name="tokenExpireTime">86400000</property>
</obj-component>
```

To ensure that the modifications do not get overwritten during the upgrade, create a file in the `/etc/opt/novell/sentinel/config/` directory with its name in the format: `obj-component.<objcomponent id>.properties`. In the properties file, set the property to the value you desire in the format `<property name>=<value>`.