NetIQ® Security Manager™ 6.5.3

Security Target

Initial Draft Date:	*October 20th, 2008*
Last Updated:	*January 13, 2011*
Version:	*V1.04*
Prepared By:	*NetIQ Corporation*
Prepared For:	*NetIQ Corporation*
	Park Towers North
	1233 West Loop South
	Suite 810
	Houston, Texas 77027

Table of Contents

Figures:

Tables:

1. Security Target Introduction (ASE_INT)

This section presents the following information:

- Security Target Reference
- Target of Evaluation Reference
- TOE Overview
- CC Conformance Claims
- Specifies the Security Target conventions,
- Describes the Security Target Organization

1.1 Security Target Reference:

ST Title:	NetIQ® Security Manager™ 6.5.3 Security Target
ST Version:	1.04
ST Date:	January 13, 2011
ST Author:	Michael F. Angelo 713-418-5396 angelom@netiq.com

1.2 Target of Evaluation Reference:

TOE Reference:	NetIQ® Security Manager™ 6.5.3.149
TOE Version #:	6.5.3.149
TOE Developer:	NetIQ Corporation
Evaluation Assurance Level (EAL):	EAL3
Keywords:	Security Information and Event Management Solution (SIEM), sensitive data protection device, ST, EAL3, NetIQ Security Manager.

1.3 Product Overview:

Note: The official name of the product is: *NetIQ® Security Manager™ 6.5.3 (SM 6.5.3).* The released product can be uniquely identified as: *NetIQ® Security Manager™ 6.5.3.149 (SM 6.5.3.149).* The product name is also abbreviated as SM6.5.3 or SM 6.5.3 or simply SM. For the purpose of this document all of the above references are equivalent.

NetIQ® Security Manager™ Version 6.5.3 (SM 6.5.3) is a Security Information and Event Management Solution (SIEM). A SIEM can act as an aggregator/consolidator of information from IDS systems, as well as for operating systems, firewalls, and antivirus applications. While intrusion detection systems (IDS) monitor IT systems for activities that may inappropriately affect the IT systems' assets and react appropriately, this TOE analyzes the output of the IDS systems, as well as operating systems, firewalls, and antivirus applications. It also provides long term storage of events from these sources.

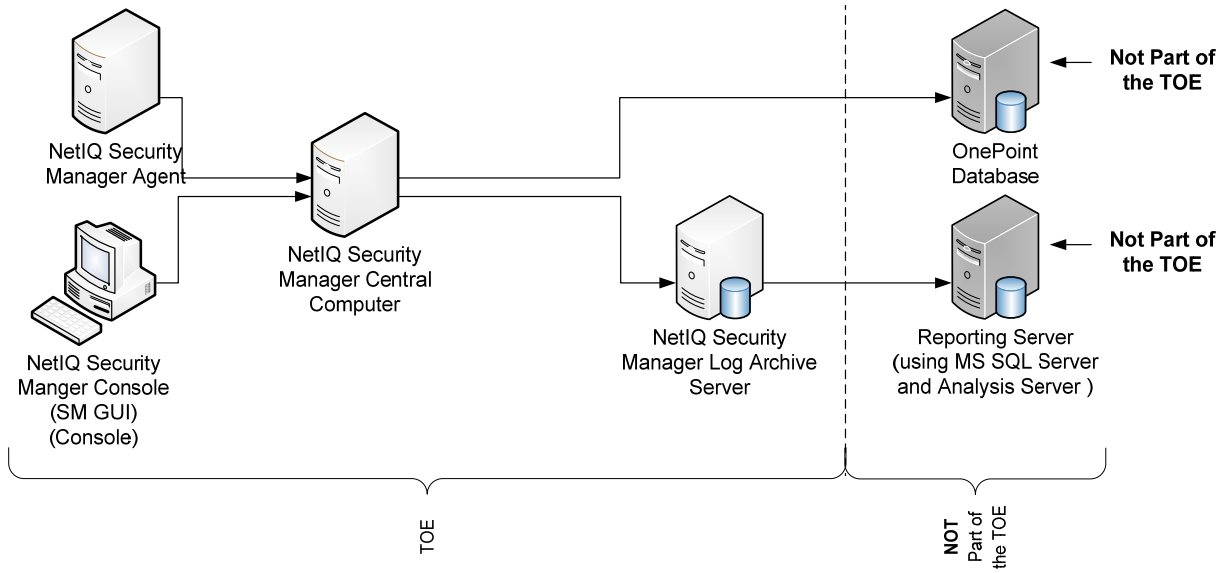

Figure 1: SM 6.5.3 Configuration

The Security Manager 6.5.3 (Figure 1[1] above) consists of the following components:

- NetIQ Security Manager Agent applications
- NetIQ Security Manager Console
- NetIQ Security Manager Central Computer applications
- NetIQ Security Manager Log Archive Server

1.4 Target of Evaluation Overview:

Note that this is a software only TOE.

1.4.1 TOE Description (Components):

NetIQ Security Manager Agent applications are responsible for executing specific tasks that may include gathering information and taking actions based on pre-defined metrics.

The NetIQ Agents can run on the following operating systems:

- Windows XP Professional
- VISTA
- Windows Server 2000
- Windows 2003 Server
- Windows 2008 Server
- IBM system i OS/400, i5/OS V5R3, V5R4, V6R1
- Sun Solaris 7,8,9,10
- IBM AIX 4.3, 5.1, 5.2, 5.3, 6.1
- HP HP-UX 11.0, 11.11, 11.23, 11.31
- Red Hat Enterprise Linux 2.1, 3, 4, 5
- Novell SuSE Linux for Enterprise Servers 9 and 10
- HP Tru64 5.1B
- SGI IRIX 6.5
- IBM Linux on POWER

[1] Components that are not part of the TOE are in grey boxes.

The NetIQ Security Manager Agent applications, with one exception[2], consist of components running on targeted IT systems. These agents send collected event data to the NetIQ Security Manager central computer in real-time.

NetIQ server components and/or agents (depending if an agent-based or an agent-less configuration is used to collect event data from a given targeted IT system) evaluate data collection rules in what is called an event workflow. This workflow is used to determine if a rule matches or not. In an agent-based configuration, there is a NetIQ client application called an agent running on the same machine as the targeted IT system. In an agent-less configuration, there is no TOE software running on the targeted IT system. The TOE in an agent-less configuration uses targeted IT system-specific interfaces (e.g. application-specific network interfaces, e.g. reading from a database [3]where a targeted IT system writes event data, etc.) to collect event data. In the event of a rule match the agent applies the corresponding response action associated with that rule. The NetIQ server components and/or agents generate alerts and in the case of agent-based configurations, send alert data to the NetIQ server components, along with the events that occurred on the targeted IT system that triggered the alert. At regular intervals the NetIQ agents check for new rules, or updates to existing rules, by initiating connections with NetIQ server components.

The TOE provides the ability to administratively configure the following types of rules:

Event rules – this type of rule can be used to monitor for a certain real-time event, and then send an alert to NetIQ server component user interfaces or trigger a response, such as running a script or paging a response team

Filtering rules – this type of rule can be used to manage the large number of real-time events that TOE collects. Filtering rules can specify whether Security Manager processes events or stores them in the database in the IT environment

Missing event rules – this type of rule can be used to monitor for a real-time event that one expects to occur within a specified time interval, but does not. For example, if one performs or automates routine tasks such as system backups, the TOE can generate alerts and responses if these tasks do not occur as planned

Consolidation rules – this type of rule can be used to group similar real-time events from an agent into one summary event. Event consolidation provides a combined event to replace many similar events generated in a short time to reduce event noise

Collection rules – this type of rule can be used to identify events to collect from specified sources to monitor in real-time. Collection rules do not generate alerts or provide other responses

Correlation rules – this type of rule can be used to monitor and analyze a stream of real-time events to look for patterns that indicate a security breach. Rather than detecting a single event, a correlation rule detects multiple events and identifies patterns using the elapsed time, the number of events, the event identification, matching event parameters, or the order in which the event occurred

Log collection rules – this type of rule can be used collect targeted IT system logs for archival and reporting. Log collection rules are similar to collection rules because they also do not generate alerts or respond to events. However, events that match a log collection rule are not further evaluated for other real-time processing rule matches

Log filter rules – this type of rule can be used to filter collected log data and prevent the TOE from storing it in the database. Administrators can create log filter rules to filter archival events that they have determined are too noisy or unimportant

Performance measuring rules - this type of rule can be used to provide real-time monitoring of Windows computers for system resource usage and performance thresholds. Also called performance processing rules.

Threshold rules – this type of rule can be used to compare sampled values, average values, or changes in values to a threshold that administrators supply. The TOE can use comparative performance data to initiate standard responses,

[2] The Windows operating system agent can run in one of two modes: an agent mode and a proxy agent mode. Windows agents installed on targeted IT Systems run in agent mode. Windows agents that are not installed on targeted systems run in proxy agent mode. Windows agents that are not installed on targeted systems can be used to collect information from targeted systems as if an agent had been installed on the targeted system. The Windows agents that are not installed on targeted systems forward collected information to the NetIQ Security Manager.

[3] Note that the database is not part of the TOE, but may be provided as input to the Security Manager Agent.

such as running a script or batch file, issuing an SNMP trap, notifying a specified notification group, or updating state variables

Alert processing rules – this type of rule differs in purpose from event and performance processing rules. Event and performance processing rules act on events or threshold data. Alert rules process the alerts that event and performance processing rules generate, including generating SMTP messages, SNMP messages, and running administrator-defined scripts. Alert processing rules define the real-time response the TOE takes when another rule issues a specified level of alert

The **NetIQ Security Manager Console application** allows administrators to view and manage collected event data and generated alerts and manage TOE functions. The console provides:

- interfaces that can be used by administrators to monitor alerts about real-time events.
- a web console function to monitor alerts about real-time events and view summary reports of archival log data using a web browser
- analysis functions
- a development environment to customize processing rules, computer groups, and other manager subcomponents.

The NetIQ Security Manager Console application includes the following functional components:

- Control Center (replaces Management Console / Monitor Console,)
- Development Console,
- Web Console.

These console components are described further in section 7.1.2 Security Management.

The **NetIQ Security Manager Central Computer** application receives data from the NetIQ Security Manager agent, in an agent-based configuration, or retrieves event data from targeted IT systems and sends real-time and log data to the log archive. The Central Computer can install, uninstall and configure Windows agents, distribute rules to Windows agents, and control the data flow between all agents and the log archive or database servers provides correlation services by applying correlation rules to received data, and generating responses when rule matches occur. The NetIQ Security Manager central computer also performs analysis on data from monitored log archives. NetIQ Security Manager central computer stores configuration data and data collected from targeted IT systems in a database[4] in the IT environment.

The **NetIQ Security Log Archive server** is the computer used by Log Manager to store daily log data in log archives. Each central computer sends log data to a log archive server. The **log archive partition** is a storage folder on the server used to store log data collected each day.

The User, Installation, and Administration guidance is provided with the TOE.

1.4.2 Major Security Features of the TOE:

The TOE provides the ability to:

- collect and react to event data from targeted IT systems using administrator configurable rules
- collect, standardize, and archive collected data from targeted IT systems
- generate reports to review collected data

The TSF provides the following security functions:

- Identification and authentication
- Security management
- Protection of the TSF
- Security information and event management

Please note: as can be seen in Figure 2 (below), the communications to the TOE components are either DCOM, .NET Remoting, MS SSL, MSMQ. In addition components of the TOE are secured by the Microsoft Infrastructure with the appropriate Account Creation, Group Membership Creation, and or file ACLs which are not part of the TOE.

[4] The database in this case refers to the OnePoint Database. This database is a SQL Database and is not part of the TOE.

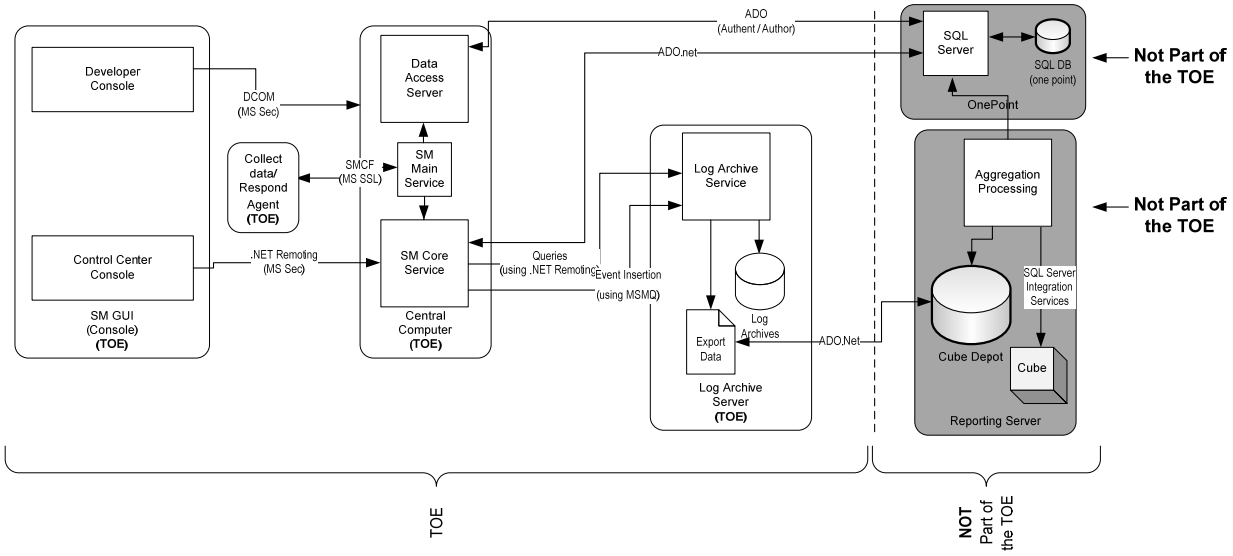

Figure 2: Security Manager Functional Architecture[56]

1.4.3 TOE Logical Boundary

1.4.3.1 Security Information and Event Management

The TOE can detect changes to both targeted IT system resource operation as well as configuration changes. Collected data from all targeted IT system resources is correlated by the TOE and interfaces are provided to authorized administrators to perform further analysis of the correlated data. When the TOE collects data from agents that are located on targeted IT system resources, the TOE passes the collected data into the following data streams (work flows):

- Real-time data streams
- Correlation data streams
- Log management data streams

DataStream processing is described further in section 5.1 (“Security Information and Event Management”).

1.4.3.2 Security management

The NetIQ Security Manager console application provides user interfaces that administrators may use to manage TOE functions. The TOE recognizes the following *operating system* groups, which each correspond to TOE roles:

- OnePointOp Reporting
- OnePointOp Users
- OnePointOp Operators
- OnePointOp ConfgAdms
- OnePointOp System
- OnePointOp TrustedServiceAccounts

The TOE recognizes the following *database*[7] groups:

- EeaDasLocator
- VigilEntUserAccess

[5] Components with-in larger boxes are functional components and not necessarily subcomponents.
[6] Objects that are in grey boxes are not part of the TOE.
[7] This is a generic group required to write to the OnePoint Database, and is not part of the TOE.

The standard SQL database groups do not correspond to TOE roles given that the user must also be a member of the OnePointOp groups for the set of TOE functions that require that the user be a member of any additional database groups, as described in section 6.1.2 (“Security Management”).

User accounts in the OnePointOp Reporting group have permission to use the Control Center Console to run reports.

User accounts in the OnePointOp Users group have permission to views in the Control Center. These users can monitor the information that Security Manager collects.

User accounts in the OnePointOp Operators group have all the permissions of the OnePointOp Users group. In addition, operators can modify the information that Security Manager collects and what the product does with the collected information. Operators typically use the Control Center and Development Console.

User accounts in the OnePointOp ConfgAdms group have all the permissions of the OnePointOp Operators group. In addition, users in the ConfgAdms group can also modify the list of computers where Security Manager installs agents (the Managed Computers list), as well as configure settings in the Configuration Wizard. Security Manager configuration administrators typically use the Control Center, Development Console Configuration snap-ins, Configuration Wizard, and Deployment Wizard.

Control Center (also referred to as Control Center Console), Development Console, and Web Console NetIQ Security Manager console application components are described further in section 6.1.2 (“Security Management”).

1.4.3.3 Identification and authentication

Users of targeted IT systems do not log into the TOE. The NetIQ Security Manager console application does not identify and authenticate individual administrators or users. The NetIQ Security Manager console application provides user interfaces that administrators may use to manage TOE functions. The operating system and the database in the IT Environment are queried to individually identify and authenticate administrators or users. The TOE maintains authorization information that determines which TOE functions an authenticated administrators or users (of a given role) may perform.

1.4.4 TOE Physical Boundary:

The NetIQ Security Manager is a software only TOE; hence the TOE physical boundary consists of the (previously described) NetIQ Security Manager Agent, NetIQ Security Manager Console, NetIQ Security Manager Central Computer, NetIQ Security manager Log Archive Server software components running on their supporting OSs. User installation and guidance documentation is supplied with the TOE.

1.4.5 TOE TYPE

The TOE is a Security Information and Event Management Solution (SIEM). A SIEM can act as an intrusion detection system for intrusion detection systems, as well as for operating systems, firewalls, and antivirus applications. While Intrusion detection systems (IDS) monitor IT systems for activities that may inappropriately affect the IT systems’ assets and react appropriately, this TOE correlates event data that the TOE collects from monitored systems. This in turn provides the TOE the ability to correlate events from otherwise disparate monitored systems.

1.4.6 Non-TOE hardware/software/firmware required by the TOE.

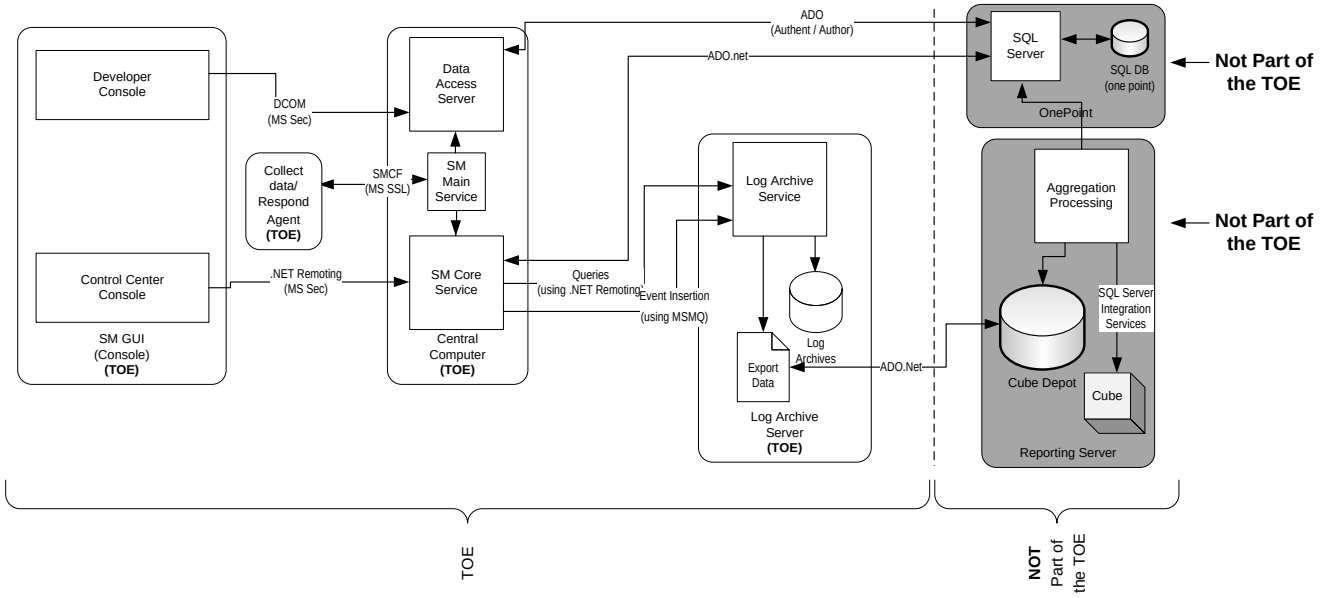

Figure 3: NetIQ Security Manager and IT Environment Component[89]

Those elements labeled **TOE** in Figure 4 are covered by this ST.

The NetIQ Central Computer (Central Computer) requires a server that is capable of supporting:

- Windows Server 2003

The NetIQ Log Archive Server (Log Archive Server) requires a server that is capable of supporting:

- Windows Server 2003

The NetIQ Security Manager Console can run on following operating systems:

- XP Professional
- VISTA
- Windows 2003 Server

The NetIQ Security Manager Agents can run on the following operating systems:

- XP Professional
- VISTA
- Windows 2003 Server
- Windows 2008 Server
- Linux

These environments (components) are not part of the TOE.

In addition the system requires a network which may consist of routers, switches, hubs, and other technology used in a TCP/IP based network, which are also not part of the TOE.

For those components that are resident on a Microsoft Operating System, the encryption technology is provided natively by Microsoft as part of the operating environment. The encryption technology has been certified by NIST to be FIPS validated.

Finally the system may employ SSL, MSMQ, DCOM, and .net Remoting for communications, which are provided by a third party and are not part of the TOE.

[8] Components with-in larger boxes are functional components and not necessarily subcomponents.
[9] Objects that are in grey boxes are not part of the TOE.

The operating system environment(s) are responsible for providing FIPS Certified encryption. Currently the following environments have FIPS certifications.

OS	Cert #	Description
Misc	888	Boot Manager (bootmgr)
	889	Winload OS Loader (winload.exe)
	890	Code Integrity (ci.dll)
	891	Microsoft Kernel Mode Security Support Provider Interface (ksecdd.sys)
	892	Microsoft Windows Cryptographic Primitives Library (bcrypt.dll)
XP	989	Windows XP Enhanced Cryptographic Provider (RSAENH)
	990	Windows XP Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)
	997	Microsoft Windows XP Kernel Mode Cryptographic Module (FIPS.SYS)
Vista	893	Windows Vista Enhanced Cryptographic Provider (RSAENH)
	894	Windows Vista Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)
	978	Windows Vista Boot Manager (bootmgr)
	979	Windows Vista Winload OS Loader (winload.exe)
	980	Windows Vista Code Integrity (ci.dll)
	1000	Microsoft Windows Vista Kernel Mode Security Support Provider Interface (ksecdd.sys)
	1001	Microsoft Windows Vista Cryptographic Primitives Library (bcrypt.dll)
	1002	Windows Vista Enhanced Cryptographic Provider (RSAENH)
	1003	Windows Vista Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)
W2K3	868	Windows Server 2003 Enhanced Cryptographic Provider (RSAENH)
	869	Windows Server 2003 Kernel Mode Cryptographic Module (FIPS.SYS)
	875	Windows Server 2003 Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)
	1012	Windows Server 2003 Enhanced Cryptographic Provider (RSAENH)
W2K8	1004	Windows Server 2008 Boot Manager (bootmgr)
	1005	Windows Server 2008 Winload OS Loader (winload.exe)
	1006	Windows Server 2008 Code Integrity (ci.dll)
	1007	Microsoft Windows Server 2008 Kernel Mode Security Support Provider Interface (ksecdd.sys)
	1008	Microsoft Windows Server 2008
	1009	Windows Server 2008 Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)

Table 1: FIPS Certificate Numbers

Additional documentation can be found in the AGD documentation which includes Chapter 6 of the User Guide (titled: Monitoring your environment). This chapter also included information on supported agents such as Anti-Virus applications, databases, firewalls, IDSs, and routers / switches.

1.4.7 Evaluated Configuration

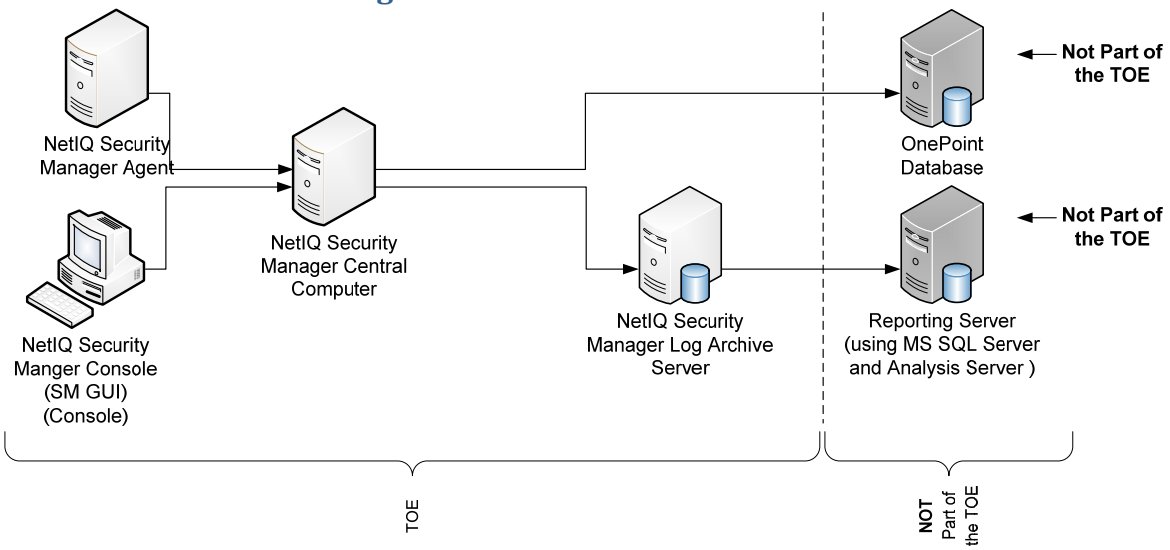

Figure 4: Evaluated Configuration[10]

The components that make up the evaluated configuration are:

- NetIQ Security Manager console (SM GUI)
- NetIQ Security Manager central computer (Central Computer)
- NetIQ Security Manager Log Archive Server (Log Archive Server)
- NetIQ Security Manager agent applications[11] (Agent)

While this system is modular and multiple components can be combined on one platform, the evaluated configuration separates these elements into individual discrete machines.

The NetIQ Security Manager central computer and Log Archive Server will be evaluated in the consolidated configuration with the following operating systems:

- Windows 2003 Server

The NetIQ Security Manager GUI (Console) will be evaluated on the following operating systems:

- Vista, [XP], and Windows Server 2003

The NetIQ Security Manager Agent will be evaluated on the following operating systems:

- Windows 2003 Server, Windows 2008 Server, [XP], and Vista, Linux (RedHat Enterprise Linux 5)

The NetIQ Agent will be tested in both the Agent and Agentless Configurations. The NetIQ Agent will generate and send alert messages using the following notification mechanisms:

- SNMP compatible management server

All other alarms defined in section 6.1.3.2 are also part of the evaluated configuration

1.4.8 References

Additional documentation can be found in the AGD documentation which includes Chapter 6 of the User Guide (titled: Monitoring your environment). This chapter also includes information on supported agents such as Anti-Virus applications, databases, firewalls, IDSs, and routers / switches. The complete list of guidance documentation is provided in Section 7.2.4 of this ST.

[10] Objects that are in grey boxes are not part of the TOE.

[11] The Windows and Unix agents support multiple Windows and Linux platforms as indicated.

1.5 Security Target Conventions:

This section specifies the formatting information used in the ST. The notation, conventions, and formatting in this security target are consistent with Version 3.1 of the Common Criteria for Information Security Evaluation. Clarifying information conventions, as well as font styles were developed to aid the reader.

- Security Functional Requirements – Part 1, section C.4, of the CC defines the approved set of operations that may be applied to functional requirements: assignment, iteration, refinement, and selection,.
  - Assignment: allows the specification of an identified parameter or parameter(s).
  - Iteration: allows a component to be used more than once with varying operations.
  - Refinement: allows the addition of details.
  - Selection: allows the specification of one or more elements from a list.

- Within section 6 of this ST the following conventions are used to signify how the requirements have been modified from the CC text.
  - Assignments are indicated using bold and are surrounded by brackets (e.g., **[assignment]**).
  - Iteration is indicated by a letter placed at the end of the component. For example FDP_ACC.1a and FDP_ACC.1b indicate that the ST includes two iterations of the FDP_ACC.1 requirement, a and b.
  - Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **every** object …" or "… ~~all~~ **things** …").
  - Selections are indicated using bold italics and are surrounded by brackets (e.g., **[*selection*]**).

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

1.5.1 Acronyms:

API	Application programming interface
CC	Common Criteria
CEM	Common Evaluation Methodology
CCEVS	Common Criteria Evaluation and Validation Scheme
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
HLD	High-level Design
IA	Initial Assessment
IDS	Intrusion Detection Systems
NSS	Network Security System
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OS	Operating system
PP	Protection Profile
SIEM	Security Information and Event Management Solution
SM	NetIQ® Security Manager™
SMTP	Simple Mail Transport Protocol
SNMP	Simple Network Monitoring Protocol
SSL	Secure Socket Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

1.6 Security Target Organization

The Security Target (ST) contains the following sections:

Section 1	Security Target Introduction (ASE_INT)	The ST introduction describes the Target of Evaluation (TOE) in a narrative with three levels of abstraction: A TOE reference, TOE overview, a TOE description (in terms of physical and logical boundaries) and scoping for the TOE.
Section 2	CC Conformance Claims (ASE_CCL)	This section details any CC and PP conformance claims.
Section 3	Security Problem (ASE_SPD)	This section summarizes the threats addressed by the TOE and assumptions about the intended environment.
Section 4	Security Objectives (ASE_OBJ	This section provides a concise statement in response to the security problem defined in definition.
Section 5	Extended Components Definition (ASE_ECD)	This section provides information about security requirements outside of components described in CC Part 2 or CC Part 3.
Section 6	IT Security Requirements (ASE_REQ)	This section provides a description of the expected security behavior of the TOE.
Section 7	TOE Summary Specification (ASE_TSS)	This section provides a general understanding of the TOE implementation.

2. CC Conformance Claims (ASE_CCL)

This TOE and ST are conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1 Release 3, July 2009. Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 3.1 Release 3, July 2009. Part 3 Conformant
- Evaluation Assurance Level 3 (EAL3)

This ST does not claim conformance to any Protection Profiles (PPs).

3. Security Problem (ASE_SPD)

This section summarizes the threats addressed by the TOE and assumptions about the intended environment of the TOE. Note that while the identified threats are mitigated by the security functions implemented in the TOE, the overall assurance level (EAL 3) also serves as an indicator of whether the TOE would be suitable for a given environment.

3.1 Introduction:

3.1.1 Assets:

The assets can be broken down into two classes – Primary and Secondary. The main aim of this TOE is to protect the primary assets against unauthorized access, manipulation, and disclosure. The primary assets are:

- Data stored on the *Central Computer* and the *Log Archive server*.
- Configuration information stored on the SM GUI (*Console)* and *Agents.*
- Data in transit from / to the *Central Computer*, SM GUI (*Console*) and *Agents*

The Secondary assets are themselves of minimal value, the possession of these assets enables or eases access to primary assets. Therefore these assets need to be protected as well.

- Credentials (i.e. account information and associated passwords)
- Security attributes (i.e. File access permissions) on the TOE.
- Signature keys

3.1.2 Roles:

3.1.2.1 OnePointOp ConfigAdms (Administrator):

User accounts in the OnePointOp ConfgAdms group have all the permissions of the OnePointOp Operators group. In addition, users in the ConfgAdms group can also modify the computers where Security Manager installs agents, as well as configure settings in the Configuration Wizard. Security Manager configuration administrators typically use the Control Center, Development Console Configuration snap-ins, Configuration Wizard, and Agent Administrator.

Warning:

Maintain tight control over members of the OnePointOp Operators and OnePointOp ConfgAdms groups. Members of these groups can define rules that can make widespread changes throughout your enterprise.

3.1.2.2 OnePointOp Reporting:

For Log Manager installations, user accounts in the OnePointOp Reporting group have permission to run and view reports in the Control Center. Reporting users can use the Control Center to run reports.

3.1.2.3 OnePointOp User:

User accounts in the OnePointOp Users group have permission to examine views in the Control Center. OnePointOp users can monitor the information that Security Manager collects and can resolve alerts but cannot modify product functionality.

3.1.2.4 OnePointOp Operator:

User accounts in the OnePointOp Operators group have all the permissions of the OnePointOp Users group. In addition, operators can modify the rules that configure Security Manager to monitor and collect events. Operators typically use the Control Center and the Development Console.

3.1.2.5 OnePointOp Trusted Service Accounts

Service accounts from a remotely connected configuration group that are members of the local OnePointOp TrustedServiceAccounts group have access to data in the local configuration group. A **service account** is a Windows security account used by services to log on to a Windows computer.
You cannot use the Access Configuration utility to add a service account to the OnePointOp TrustedServiceAccounts group. Instead use the Active Directory Users and Computers Administrative Tool to add user accounts to the TrustedServiceAccounts group.

3.1.2.6 OnePointOp System Group:

The OnePointOp System Group contains the local service account for the Central Computer and Log Archive Server. This group is assigned rights to files and directories and data in the OnePoint database.

3.1.2.7 Attacker:

An Attacker is a person (or persons) who is not a user or administrator, and has not physical access to any device in the infrastructure. This means that their only mode of access would be from outside the corporate environment (i.e. a machine on the Internet).

A successful attacker would be able to gain access to TOE resources. Assuming successful access that attacker would then attempt to:

- corrupt the configuration data on an monitored agent
- stop the monitoring of the agent
- gain access to data collected by the agent for the purpose of modification or deletion

3.2 Assumptions

3.2.1 Intended Usage Assumptions

A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions.
A.DYNMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
A.ASCOPE	The TOE is appropriately scalable to the IT System the TOE monitors.

3.2.2 Physical Assumptions

A.LOCATE	The server components of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

3.2.3 Personnel Assumptions

A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

3.2.4 Connectivity Assumptions:

A.AVAIL	The systems, networks and all components will be available for use.
A.CONFIG	The systems will be configured to allow for proper usage of the application.
A.NETCON	All networks will allow for communications between the components.
A.PROTCON	The TOE will be installed in an IT environment with that has the capability to provide private and authenticated network communications.

3.3 Threats

3.3.1 Threats to the TOE

T.ADMIN_ERROR	An authorized administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
T.MASQUERADE	An unauthorized user, process, or external IT entity may masquerade as an authorized entity to gain access to data or TOE resources.
T.NOHALT	An unauthorized person may attempt to compromise the continuity of the TOEs analysis functionality by halting execution of the TOE.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
T.TSF_COMPROMISE	A malicious user may cause configuration data to be inappropriately accessed (viewed, modified or deleted).
T.FALACT	The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity which would result in the TOE not capturing the inappropriate activity.
T.FALASC	The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources which would result in the TOE not capturing the associated events.
T.FALREC	The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source which would result in a failure to capture and or correlate the information.
T.INADVE	Inadvertent activity and access may occur on an IT System the TOE monitors could result in the TOE not capturing the data from the event.
T.INFLUX	An unauthorized user may cause a malfunction of the TOE by creating an influx of data that the TOE or the system cannot handle.
T.MISACT	An unauthorized user or program may deliberately introduce Viruses, Trojans or other Malware onto IT System the TOE monitors as the TOE does not prevent the introduction of such code to the system.
T.MISUSE	Unauthorized users may inadvertently accesses and perform activities indicative of misuse may occur on an IT System the TOE monitors which is outside the scope of the TOE.
T.SCNCFG	Improper security configuration settings may exist in the IT System the TOE monitors which could make the TOE ineffective.
T.SCNMLC	Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions.
T.SCNVUL	Vulnerabilities may exist in the IT System the TOE monitors which causes the TOE to become ineffective.

4. Security Objectives (ASE_OBJ)

4.1 Security Objectives for the TOE

O.ADMIN_ROLE	The TOE will define authorizations that determine the actions authorized administrator roles may perform.
O.IDANLZ	The TOE must accept data from Sensors (agents) or Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).
O.SIEMCAN	The TOE must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.
O.SIEMENS	The TOE must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the SIEM.
O.MANAGE	The TOE will allow administrators to effectively manage the TOE and its security functions, and must ensure that only authorized administrators are able to access such functionality.
O.OFLOWS	The TOE must appropriately handle potential System data storage overflows.
O.RESPON	The TOE must respond appropriately to analytical conclusions.

4.2 Security Objectives for the Non-IT Environment

OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
OE.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
OE.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
OE.INTROP	The TOE is interoperable with the IT System it monitors.

4.3 Security Objectives for the IT Environment

OE.ADMIN_ROLE	The IT Environment will provide authorized administrator roles to isolate administrative actions.
OE.USER_AUTHENTICATION	The IT Environment will verify the claimed identity of users.
OE.USER_IDENTIFICATION	The IT Environment will uniquely identify users.
OE.TIME	The IT environment will provide a time source that provides reliable time stamps.
OE.TOE_PROTECTION	The IT environment will protect the TOE and its assets from external interference or tampering.
OE.COM_PROT	The IT Environment will provide access to protected communications channels. The channels include SHTTP, SSL, .NET Remoting, DCOM, SMCF, and MSMQ.
OE_CRYPTO_PROT	The IT environment will protect the TOE communications using FIPS 140-2 validated cryptographic modules.
OE. AVAIL	The systems, networks and all components will be available for use.
OE. CONFIG	The systems will be configured to allow for proper usage of the application.
OE. NETCON	All networks will allow for communications between the components.

4.4

4.5 Rationale

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

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

4.6 Security Objectives Rationale

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

4.6.1 Security Objectives Rationale for the TOE and Environment

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

		O.ADMIN_ROLE	O.IDANLZ	O.SIEMCAN	O.SIEMENS	O.MANAGE	O.OFLOWS	O.RESPON	OE.ADMIN_ROLE	OE.USER_AUTHENTICATION	OE.USER_IDENTIFICATION	OE.TIME	OE.TOE_PROTECTION
Threats to the TOE	T.ADMIN_ERROR					x							
	T.MASQERADE	x							x	x	x		
	T.NOHALT	x											
	T.PRIVIL	x											
	T.TSF_COMPROMISE												x
	T.FALACT							x				x	
	T.FALASC		x									x	
	T.FALREC		x										
	T.INADVE				x								
	T.INFLUX						x						
	T.MISACT				x								
	T.MISUSE				x								
	T.SCNCFG			x									
	T.SCNMLC			x									
	T.SCNVUL			x									

Table 2: Environment to Objective Correspondence

4.6.1.1 T.ADMIN_ERROR

An authorized administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.

This Threat is countered by ensuring that:

O.MANAGE: The TOE will allow administrators to effectively manage the TOE and its security functions. The TOE will also provide guidance documentation in the effective and correct use of the TOE. Finally the TOE must ensure that only authorized administrators are able to access such functionality.

4.6.1.2 T.MASQUERADE

An unauthorized user, process, or external IT entity may masquerade as an authorized entity to gain access to data or TOE resources.

This Threat is countered by ensuring that:

O.ADMIN_ROLE: The TOE will define authorizations that determine the actions authorized administrator roles may perform.

OE.ADMIN_ROLE: The IT Environment will provide authorized administrator roles to isolate administrative actions.

OE.USER_AUTHENTICATION: The IT Environment will verify the claimed identity of users.

OE.USER_IDENTIFICATION: The IT Environment will uniquely identify users.

4.6.1.3 T.NOHALT

An unauthorized person may attempt to compromise the continuity of the TOEs analysis functionality by halting execution of the TOE.

This Threat is countered by ensuring that:

O.ADMIN_ROLE: The TOE will define authorizations that determine the actions authorized administrator roles may perform.

4.6.1.4 T.PRIVIL

An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.

This Threat is countered by ensuring that:

O.ADMIN_ROLE: The TOE will define authorizations that determine the actions authorized administrator roles may perform.

4.6.1.5 T.TSF_COMPROMISE

A malicious user may cause configuration data to be inappropriately accessed (viewed, modified or deleted).
This Threat is countered by ensuring that:

OE.TOE_PROTECTION: The IT environment will protect the TOE and its assets from external interference or tampering.

4.6.1.6 T. FALACT

The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity which would result in the TOE not capturing the inappropriate activity.

This Threat is countered by ensuring that:

O.RESPON: The O.RESPON objective ensures the TOE reacts to analytical conclusions about suspected vulnerabilities or inappropriate activity

OE.TIME: The IT environment will provide a time source that provides reliable time stamps.

4.6.1.7 T. FALASC

The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources which would result in the TOE not capturing the associated events.

This Threat is countered by ensuring that:

The O.IDANLZ objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from multiple data sources.

OE.TIME: The IT environment will provide a time source that provides reliable time stamps.

4.6.1.8 T. FALREC

The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source which would result in a failure to capture and or correlate the information.

This Threat is countered ensuring that:

O.IDANLZ: The O.IDANLZ objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from multiple data sources

4.6.1.9 T. INADVE

Inadvertent activity and access may occur on an IT System the TOE monitors could result in the TOE not capturing the data from the event.

This Threat is countered by ensuring that:

O.SIEMENS: The O.SIEMENS objective address this threat by requiring the TOE collect audit and Sensor data.

4.6.1.10 T. INFLUX

An unauthorized user may cause a malfunction of the TOE by creating an influx of data that the TOE or the system cannot handle.

This Threat is countered by ensuring that:

O.OFLOWS: The TOE will appropriately handle potential System data storage overflows.

4.6.1.11 T. MISACT

An unauthorized user or program may deliberately introduce Viruses, Trojans or other Malware onto IT System the TOE monitors as the TOE does not prevent the introduction of such code to the system

This Threat is countered by ensuring that:

O.SIEMENS: The O.SIEMENS objective address this threat by requiring the TOE collect audit and Sensor data.T. MISUSE

Unauthorized users may inadvertently accesses and perform activities indicative of misuse may occur on an IT System the TOE monitors which is outside the scope of the TOE.

This Threat is countered by ensuring that:

O.SIEMENS: The O.SIEMENS objective addresses this threat by requiring a TOE, that contains a Sensor, that can collect audit and Sensor data.

4.6.1.12 T. MISUSE

An unauthorized process or person can access, attempt to access, and or perform an activity indicative of misuse on an IT System the TOE monitors

This Threat is countered by ensuring that:

O.SIEMENS: The O.SIEMENS objective addresses this threat by requiring a TOE, that contains a Sensor, that can collect audit and Sensor data.

4.6.1.13 T. SCNCFG

Improper security configuration settings may exist in the IT System the TOE monitors which could make the TOE ineffective.

This Threat is countered by ensuring that:

O.SIEMCAN: The O.SIEMCAN objective counters this threat by requiring the TOE collects and stores static configuration information that might be indicative of a configuration setting change.

4.6.1.14 T. SCNMLC

Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions.

This Threat is countered by ensuring that:

O.SIEMCAN: The O.SIEMCAN objective counters this threat by requiring the TOE collects and stores static configuration information that might be indicative of a configuration setting change.

4.6.1.15 T. SCNVUL

Vulnerabilities may exist in the IT System the TOE monitors which causes the TOE to become ineffective.
This Threat is countered by ensuring that:

O.SIEMCAN: The O.SIEMCAN objective counters this threat by requiring the TOE collects and stores static configuration information that might be indicative of a configuration setting change.

4.7 Security Objectives Rationale for Environment Assumptions

This section provides evidence demonstrating coverage of the Non-IT security objectives by the environmental assumptions. The following table shows this assumption to objective mapping.

		O.ADMIN	O.AVAILABILITY	OE.CONFIG	OE.CONNECT	OE.INSTAL	OE.CREDEN	OE.PERSON	OE.PHYCAL	OE.INTROP	OE.COM_PROT	OE.CRYPTO_PROT
Intended usage assumptions	A.ACCESS									x		
	A.ASCOPE									x		
	A.DYNMIC							x		x		
Physical assumptions	A.LOCATE								x			
Personnel assumptions	A.MANAGE							x				
	A.NOEVIL					x	x					
Connectivity Assumptions	A.AVAIL	x	x									
	A.CONFIG			x								
	A.NETCON				x							
	A.PROTCON										x	x

Table 3: Complete coverage – environmental assumptions

4.7.1 A.ACCESS

The TOE has access to all the IT System data it needs to perform its functions.

This Assumption is satisfied by ensuring that:

OE.INTROP: The OE.INTROP objective ensures the TOE has the needed access.

4.7.2 A.ASCOPE

The TOE is appropriately scalable to the IT System the TOE monitors.

This Assumption is satisfied by ensuring that:

OE.INTROP: The OE.INTROP objective ensures the TOE has the necessary interactions with the IT System it monitors.

4.7.3 A.DYNIMC

The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors data collected and produced by the TOE shall be protected from modification.

This Assumption is satisfied by ensuring that:

OE.PERSON: The OE.PERSON objective ensures that the TOE will managed appropriately.
OE.INTROP: The OE.INTROP objective ensures the TOE has the proper access to the IT System.

4.7.4 A.LOCATE

The server components of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

This Assumption is satisfied by ensuring that:

OE.PHYCAL: The OE.PHYCAL provides for the physical protection of the TOE.

4.7.5 A.MANAGE

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

This Assumption is satisfied by ensuring that:

OE.PERSON: The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.

4.7.6 A.NOEVIL

The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

This Assumption is satisfied by ensuring that:

OE.INSTAL: The OE.INSTAL objective ensures that the TOE is properly installed and operated.
OE.CREDEN: The OE.CREDEN objective supports this assumption by requiring protection of all authentication data

4.7.7 A.AVAIL

The TOE will be installed in an IT environment built for complete system and data availability.

This Assumption is satisfied by ensuring that:
O.ADMIN: The O.ADMIN objective ensures that only Administrators can access the management functions for the TOE.
O.AVAILABILITY: The O.AVAILABILITY objective ensures that the system is fully available and fully redundant.

4.7.8 A.CONFIG

The TOE environment will be properly configured and maintained as defined in the MS Configuration Guidance Documentation.

This Assumption is satisfied by ensuring that:
OE.CONFIG: The OE.CONFIG objective ensures that the system is configured according to the MS Configuration Guidance Documentation.

4.7.9 A.NETCON

The TOE will be installed in an IT environment with network connectivity and availability.

This Assumption is satisfied by ensuring that:
OE.CONNECT addresses A.NETCON by ensuring the TOE is installed in an IT environment with network connectivity and availability.

4.7.10 A.PROTCON

The TOE will be installed in an IT environment with that has the capability to provide private and authenticated network communications.

This Assumption is satisfied by ensuring that:
OE.COMM_PROT: The OE_COMM_PROT objective ensures that the IT environment can protect communications between components.
OE.CRYPTO_PROT: The OE.CRYPTO_PROT objective ensures that the IT environment provides quality encryption.

4.8 Security Requirements Rationale

This section demonstrates how there is at least one functional component for each objective (and how all SFRs map to one or more objectives) by a discussion of the coverage for each objective.

	O.ADMIN_ROLE	O.IDANLZ	O.SIEMCAN	O.SIEMENS	O.MANAGE	O.OFLOWS	O.RESPON
FIA_ATD.1	x						
FMT_MOF.1					x		
FMT_MTD.1					x		
FMT_SMF.1					x		
FMT_SMR.1	x						
SIEM_ADM.1(EX)					x		
SIEM_ALR.1(EX)							x
SIEM_COL.1(EX)			x	x			
SIEM_COR.1(EX)		x					
SIEM_STG.1(EX)						x	

Table 4: Objective to Requirement Correspondence

4.8.1 O.ADMIN_ROLE

The TOE will define authorizations that determine the actions authorized administrator roles may perform.

This TOE Security Objective is satisfied by ensuring that:

FIA_ATD.1: The TOE maintains authorization information that determines which TOE functions a role may perform.

FMT_SMR.1: The TOE recognizes any user account that is assigned in the IT environment to one or more system-defined operating system user groups and database[12] roles as an "authorized administrator".

4.8.2 O.IDANLZ

The TOE must accept data from SIEM Sensors or SIEM Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).

This TOE Security Objective is satisfied by ensuring that:

SIEM_COR.1(EX): The TOE correlates event data collected from targeted IT system resources.

4.8.3 O.SIEMCAN

The TOE must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System

This TOE Security Objective is satisfied by ensuring that:

SIEM_COL.1(EX): The TOE collects targeted IT system resource operation information from agents that are installed on the targeted IT system resource.

4.8.4 O.SIEMENS

The TOE must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the SIEM

This TOE Security Objective is satisfied by ensuring that:

SIEM_COL.1(EX): The TOE collects targeted IT system resource operation and configuration information from agents that are installed on the targeted IT system resource.

4.8.5 O.MANAGE

The TOE will allow administrators to effectively manage the TOE and its security functions, and must ensure that only authorized administrators are able to access such functionality.
This TOE Security Objective is satisfied by ensuring that:

FMT_MOF.1: The TOE restricts the ability to manage SIEM settings to authorized administrators.

FMT_MTD.1: The TOE restricts the ability to query collected data and generated reports to authorized users.

FMT_SMF.1: The TOE provides authorized administrators with the ability to manage SIEM settings and review collected data and correlation reports.

SIEM_ADM.1(EX): The TOE provides authorized administrators with the ability to interactively analyze collected data and generated reports using the GUI of the console component.

4.8.6 O.OFLOWS

The TOE must appropriately handle potential System data storage overflows

This TOE Security Objective is satisfied by ensuring that:

SIEM_STG.1 (EX): The TOE generates alarms using a configured notification mechanism when storage capacity for collected System data has been reached.

[12] Database refers to the one point Database, as provided by SQL. This database is not part of the TOE.

4.8.7 O.RESPON

The TOE must respond appropriately to analytical conclusions

This TOE Security Objective is satisfied by ensuring that:

SIEM_ALR.1 (EX): The TOE generates alarms that notify authorized administrators using the console, using email, using SMTP, and/or executing a command in a configured script. Note that alarms are generated in response to administratively-configured processing rules.

4.8.8 OE.COM_PROT

The IT Environment will provide access to protected communications channels. The channels include SHTTP, SSL, .NET Remoting, DCOM, SMCF, and MSMQ.

4.8.9 OE.CRYPTO_PROT:

The IT Environment will provide access to FIPS 140-2 L1 certified encryption components.

4.8.10 OE.ADMIN_ROLE

The IT Environment will provide authorized administrator roles to isolate administrative actions.

This IT Environment Security Objective is satisfied by ensuring that:

The IT Environment provides roles that correspond to operating system user groups and database[13] roles. Any user account that is assigned in the IT environment to one or more system-defined operating system user groups and database roles is considered an "authorized administrator".

4.8.11 OE.USER_AUTHENTICATION

The IT Environment will verify the claimed identity of users.

This IT Environment Security Objective is satisfied by ensuring that:

The IT environment authenticates individual users as members of system-defined operating system user groups and/or database roles.

4.8.12 OE.USER_IDENTIFICATION

The IT Environment will uniquely identify users.

This IT Environment Security Objective is satisfied by ensuring that:

The IT environment identifies individual users.

4.8.13 OE.TIME

The IT environment will provide a time source that provides reliable time stamps.

This IT Environment Security Objective is satisfied by ensuring that:

4.8.14 OE.TOE_PROTECTION

The IT environment will protect the TOE and its assets from external interference or tampering.

This IT Environment Security Objective is satisfied by ensuring that:

HTTPS provided by the web server in the IT Environment is used to protect communication between TOE console and IT Environment web browser components.

4.9 Security Assurance Requirements Rationale

EAL3 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software

[13] Database Roles refer to roles in the one point Database – as implemented in SQL.

engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the System may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL3, the System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

4.9.1 Requirement Dependency Rationale

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

SFR	Dependencies	Met By
FIA_ATD.1	None	None
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_SMF.1	None	None
FMT_SMR.1	FIA_UID.1	Not included because Environment provides this function not the TOE.
SIEM_ADM.1(EX)	SIEM_COL.1(EX)	Included
SIEM_ALR.1(EX)	SIEM_COL.1 (EX)	Included
SIEM_COL.1(EX)	FPT_STM.1	Included
SIEM_COR.1(EX)	SIEM_COL.1 (EX)	Included
SIEM_STG.1(EX)	SIEM_COL.1 (EX)	Included
ADV_ARC.1	ADV_FSP.1, ADV_TDS.1	Included
ADV_FSP.3	ADV_TDS.1	Included
ADV_TDS.2	ADV_FSP.2	Included
AGD_OPE.1	ADV_FSP.1	Included
AGD_PRE.1	AGD_PRE.1	Included
ALC_CMC.3	ALC_CMS.1, ALC_DVS.1, ALC_LCD.1	Included
ALC_CMS.3	None	None
ALC_DEL.1	None	None
ALC_DVS.1	None	None
ALC_LCD.1	None	None
ASE_CCL.1	ASE_INT.1, ASE_ECD.1, ASE_REQ.1	Included
ASE_ECD.1	None	None
ASE_INT.1	None	None
ASE_OBJ.2	ASE_SPD.1	ASE_SPD.1
ASE_REQ.2	ASE_OBJ.1, ASE_ECD.1	ASE_OBJ.1, ASE_ECD.1
ASE_SPD.1	None	None
ASE_TSS.1	ASE_INT.1, ASE_REQ.1, ADV_FSP.1	ASE_INT.1, ASE_REQ.1, ADV_FSP.1
ATE_COV.2	ADV_FSP.2, ATE_FUN.1	ADV_FSP.2, ATE_FUN.1
ATE_DPT.1	ADV_ARC.1, ADV_TDS.2, ATE_FUN.1	ADV_ARC.1, ADV_TDS.2, ATE_FUN.1
ATE_FUN.1	None	None
ATE_IND.2	ADV_FSP.2, AGD_OPE.1, AGD_PRE.1, ATE_COV.1, ATE_FUN.1	Included
AVA_VAN.2	ADV_ARC.1, ADV_FSP.1, ADV_TDS.1, AGD_OPE.1, AGD.PRE.1	Included

Table 5: Requirement Dependency

4.10 Explicitly Stated Requirements Rationale

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

4.11 TOE Summary Specification Rationale

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

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

	Identification and authentication	Security management	Security Information \ Event Management
FIA_ATD.1	x		
FMT_MOF.1		x	
FMT_MTD.1		x	
FMT_SMF.1		x	
FMT_SMR.1		x	
SIEM_ADM.1(EX)			x
SIEM_ALR.1(EX)			x
SIEM_COL.1(EX)			x
SIEM_COR.1(EX)			x
SIEM_STG.1(EX)			x

Table 6: Security Functions vs. Requirements Mapping

5. Extended Components Definition (ASE_ECD)

This chapter defines a new class required by Security Information and Event Management systems called SIEM. The class consists of the following family members SIEM_ADM, SIEM_ALR, SIEM_COL, SIEM_COR, and SIEM_STG. This class is defined because the Common Criteria (Part 2 and Part 3) does not contain any SFRs which cover these functions. The families in this class address requirements for data review, alarms, collection controls, correlation, and loss prevention.

Class	Component
SIEM: Security Information and Event Management	SIEM_ADM.1(EX): Data Review
	SIEM_ALR.1(EX): Data Alarms
	SIEM_COL(EX): Data Collection
	SIEM_COR.1(EX): Data Correlation
	SIEM_STG.1(EX): Data Loss Prevention

Table 7: Extended Functional Components

5.1 Definition for SIEM_ADM.1 (EX)

For the TOE described in this ST it was necessary to provide authorized administrators with a mechanism to read and process information that has been gathered. This mechanism is covered by the SIEM_ADM family and contains the components as shown in Figure 5 below.

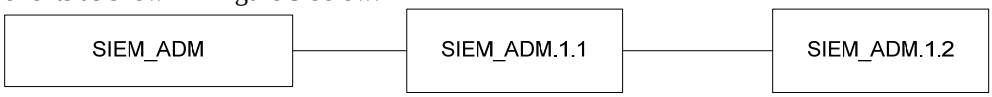

Figure 5: SIEM_ADM Component Leveling

5.1.1 Data Review (SIEM_ADM.1 (EX))

SIEM_ADM.1.1 defines a mechanism whereby authorized users have the capability to read collected data and generate reports.
SIEM_ADM.1.2 defines a mechanism requiring collected data and generated reports to be suitable for the user to interpret the information provided by them.

5.1.1.1 Dependencies

- SIEM_COL.1(EX)

5.2 Definition for SIEM_ALR.1 (EX)

For the TOE described in this ST it was necessary to define a new family (SIEM_ALR) that addresses the rules which control the generation and disposition of alarms. This family contains the component as shown in Figure 6 below.

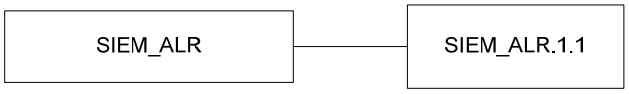

Figure 6: SIEM_ALR Component Leveling

5.2.1 Data Alarms (SIEM_ALR.1 (EX))

SIEM_ALR.1.1 defines groups or rules as well as rules for the generation of alarms using one or more notification mechanisms. This component may include:

- Display alarm information to the administrator console
- Send alarm information to administrators using email
- Send alarm information to administrators using SNMP
- Execute a command
- Execute a script
- in response to one or more of the following rule types:

- Event rules
- Filtering (database and conditional filters only) rules
- Missing event rules
- Alert rules
- Performance measuring rules
- Threshold rules

Application note: Scripts and commands can be used to support notification mechanisms for which there is no built-in support.

5.2.1.1 Dependencies

- SIEM_COL.1(EX)

5.3 Definition for SIEM_COL

For the TOE described in this ST it was necessary to define a new family (SIEM_COL) that addresses the collection of changes to the security mechanisms (operations and configuration) as well as additional event information. This family contains the components as shown in Figure 7 below.

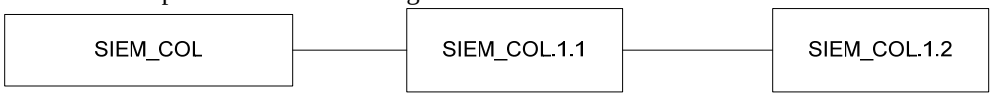

Figure 7: SIEM_COL Component Leveling

5.3.1 Data Collection (SIEM_COL (EX))

SIEM_COL.1.1 This component requires the targeted IT System resource(s) provide information about changes to the security mechanisms operation and security mechanisms configuration.

SIEM_COL.1.2 This component requires that the System shall collect and record date and time of an event, as well as the type of event, and the subject identity.

5.4 Definition for SIEM_COR.1 (EX)

For the TOE described in this ST, it is necessary that all collected SIEM data be correlated to events. In order to do this it was necessary that we define a new family (SIEM_COR). SIEM_COR must provide the ability to:

a. monitor and correlate a stream of events to identify patterns that indicate potential security breaches, and
b. monitor multiple events to identify patterns using the elapsed time, the number of events, the event identification, matching event parameters, or the order in which the event occurred to indicate potential security breaches.

This family contains the components as shown in Figure 8 below.

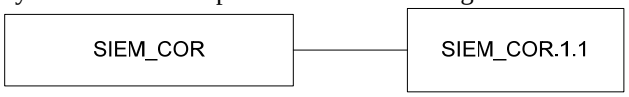

Figure 8: SIEM_COR Component Leveling

5.4.1 Data Correlation (SIEM_COR.1 (EX))

SIEM_COR.1.1 This component requires event correlation on all SIEM data received.

5.4.1.1 Dependencies

- SIEM_COL.1(EX)

5.5 Definition for SIEM_STG.1

For the TOE described in this ST it is necessary that the SIEM be able to handle the case in which the system has run out of storage capacity. In order to do this it was necessary that we define a new family (SIEM_STG). This family contains the components as shown in Figure 9 below.

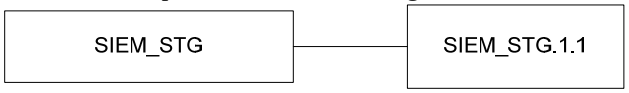

Figure 9: SIEM_STG Component Leveling

5.5.1 Data Loss Prevention (SIEM_STG.1 (EX))

SIEM_STG.1.1 This component requires an action be taken with respect to the collection of System data and the issuing of an alarm if the storage capacity has been reached.

5.5.1.1 Dependencies

- SIEM_COL.1(EX)

6. IT Security Requirements (ASE_REQ)

This section defines the security functional requirements for the TOE as well as the security assurance requirements against which the TOE has been evaluated. All of the requirements have been copied from version 3.1 of the applicable Common Criteria documents, with the exception of the explicitly stated Security Functional Requirements.

6.1 TOE Security Functional Requirements

Class	Component
FIA: Identification and Authentication	FIA_ATD.1: User attribute definition
FMT: Security management	FMT_MOF.1: Management of security functions behavior
	FMT_MTD.1: Management of TSF data
	FMT_SMF.1: Specification of management Functions
	FMT_SMR.1: Security management roles
SIEM: Security Information and Event Management	SIEM_ADM.1(EX): Data Review
	SIEM_ALR.1(EX): Data Alarms
	SIEM_COL1(EX): Data Collection
	SIEM_COR.1(EX): Data Correlation
	SIEM_STG.1(EX): Data Loss Prevention

Table 8: TOE Security Functional Requirements

6.1.1 Identification and authentication (FIA)

6.1.1.1 User attribute definition (FIA_ATD.1)

FIA_ATD.1 The TSF shall maintain the following list of security attributes belonging to individual ~~users~~: **roles**: **[authorizations]**.

6.1.2 Security management (FMT)

6.1.2.1 Management of security functions behavior (FMT_MOF.1)

FMT_MOF.1.1 The TSF shall restrict the ability to [***modify the behavior of***] the functions **[**
Data collection
Data correlation
Data alarms] to **[OnePointOp Operators, OnePointOp ConfigAdms**].

6.1.2.2 Management of TSF data (FMT_MTD.1)

FMT_MTD.1.1 The TSF shall restrict the ability to ***[query]*** the **[collected data and generated reports]** to **[OnePointOp Reporting,**
OnePointOp Users,
OnePointOp Operators,
OnePointOp ConfigAdms].

6.1.2.3 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: **[**
Modify the behavior of data collection,
Modify the behavior of data correlation,
Modify the behavior of data alarms,
Query collected data and generated reports]

6.1.2.4 Specification of Management Roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles [**OnePointOp Operators,**
OnePointOp ConfgAdms,
OnePointOp System,
OnePointOp Reporting,
OnePointOp Users,
OnePointOp TrustedServiceAccounts,
EeaDasLocator,
VigilEntUserAccess].

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

6.1.3 Security Information and Event Management (SIEM)

6.1.3.1 Data Review (SIEM_ADM.1 (EX))

SIEM_ADM.1.1 The TSF shall provide authorized users with the capability to read collected data and generated reports. (EX)
SIEM_ADM.1.2 The TSF shall provide collected data and generated reports in a manner suitable for the user to interpret the information. (EX)

6.1.3.2 Data Alarms (SIEM_ALR.1 (EX))

SIEM_ALR.1.1 The TSF shall generate an alarm using one or more of the following notification mechanisms:

- Display alarm information to the administrator console
- Send alarm information to administrators using email
- Send alarm information to administrators using SNMP
- Execute a command
- Execute a script
- in response to one or more of the following rule types:
- Event rules
- Filtering (database and conditional filters only) rules
- Missing event rules
- Alert rules
- Performance measuring rules
- Threshold rules (EX)

Application note: Scripts and commands can be used to support notification mechanisms for which there is no built-in support.

6.1.3.3 Data Collection (SIEM_COL (EX))

SIEM_COL.1.1 The TSF shall collect the following information from the targeted IT System resource(s):

Security mechanism operation and Security mechanism configuration changes. (EX)

SIEM_COL.1.2 At a minimum, the TSF shall collect and record date and time of the event, type of event, and subject identity. (EX)

6.1.3.4 Data Correlation (SIEM_COR.1 (EX))

SIEM_COR.1.1 The TSF shall perform event correlation on all SIEM data received based on rules configured by the administrator. (EX)

6.1.3.5 Data Loss Prevention (SIEM_STG.1 (EX)

SIEM_STG.1.1 The TSF shall ignore System data and send an alarm if the storage capacity has been reached. (EX)

7. TOE Summary Specification (ASE_TSS)

This chapter describes the security functions and associated assurance measures.

7.1 TOE Security Functions

7.1.1 Identification and Authentication

Users of targeted IT systems do not log into the TOE. The TOE provides user interfaces that administrators may use to manage TOE functions. The TOE does not identify and authenticate individual administrators. The TOE, when an administrator attempts to access its interfaces, first checks to see if the user has been authenticated by the operating system in the IT Environment.

If the user has been successfully identified and authenticated by the environment, and if the user has been successfully identified and authenticated as a member of an operating system and/or database [14]group that the TOE recognizes, the TOE provides access to its interfaces according to authorization data. Authorization data maintained by the TOE for each role that the TOE recognizes is used to determine the functions that a user possessing a given role (i.e. membership in an operating system and/or database group) may perform.

The TOE recognizes the following operating system groups, which each correspond to TOE roles:

- OnePointOp Reporting
- OnePointOp Users
- OnePointOp Operators
- OnePointOp ConfgAdms
- OnePointOp TrustedServiceAccounts
- OnePointOp System

The TOE recognizes the following database groups:

- EeaDasLocator
- VigilEntUserAccess

Operating system and database groups are described further in section 1.4.3 (“Security Management”).

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

- FIA_ATD.1: The TOE maintains authorization information that determines which TOE functions a role may perform.
- FMT_SMR.1: The TOE uses the operating system for the definition of different groups prior to allowing access.

[14] For the purposes of this section database refers to the OnePoint database as implemented in SQL.

7.1.2 Security Management

The TOE management functions are accomplished using the following components:

- Control Center
- Development Console
- Web Console

To use the TOE, the authorized administrator operating system account must be a member of one of the following groups:

- OnePointOp Operators
- OnePointOp ConfgAdms
- OnePointOp System

The authorized administrator account must also be a member of the EeaDasLocator role in the database[15]. Some tasks within the TOE require membership in other OnePointOp groups. The TOE allows authorized administrators to monitor real-time events and alerts for a configuration group. A configuration group has one database server storing information for a group of monitored computers or devices. The TOE also allows authorized administrators to configure Security Manager settings for a configuration group.

To use the TOE, the authorized administrator operating system account must be a member of the OnePointOp Operators group. The authorized administrator account must also be a member of the EeaDasLocator role in the database. The TOE GUI is available as an MMC. The TOE displays Windows computer groups, processing rule groups, notification groups, and advanced rule functionality for one configuration group. Authorized administrators can create or modify computer groups and processing rules using the TOE. Authorized administrators can create or modify computer attributes, which authorized administrators can use when creating Windows computer groups. Authorized administrators can also create or modify notification groups, scripts, and data providers, which can be used when creating processing rules.

To use the TOE, the authorized administrator operating system account must be a member of the OnePointOp Users group. The authorized administrator account must also be a member of the EeaDasLocator role in the database. The TOE provides remote monitoring and easy access for authorized administrators. The TOE allows authorized administrators to view real-time data and Summary reports using any Windows platform that supports Microsoft Internet Explorer.

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

- FMT_MOF.1: The TOE restricts the ability to manage SIEM settings to authorized administrators.
- FMT_MTD.1: The TOE restricts the ability to query collected data and generated reports to authorized users.
- FMT_SMF.1: The TOE provides authorized administrators with the ability to manage SIEM settings and review collected data and correlation reports.
- FMT_SMR.1: The TOE uses the operating system for the provisioning of different groups prior to allowing access.

7.1.3 Security Information and Event Management

The TOE provides the ability to monitor the security mechanisms of targeted IT system resources which can include intrusion detection systems, as well as operating systems, firewalls, and antivirus applications. The TOE can detect changes to both targeted IT system resource operation as well as configuration changes. Collected data from all targeted IT system resources is correlated by the TOE and interfaces are provided to authorized administrators. Authorized administrators have the ability to configure alarms using event processing rules. When the TOE collects data from agents that are located on targeted IT system resources, the console component passes the collected data into what are called real-time, correlation, log management, and “datastreams” or work flows.

[15] For the purposes of this section, database refers to the OnePoint database as implemented in SQL.

Real-time datastream processing starts when events occur on targeted IT system resources, when agents evaluate rules that are defined by, and administered using, the TOE. When a rule match occurs, the agent generates an alert and sends it to the TOE, along with the events that triggered the alert. If the rule specifies to notify an authorized administrator, TOE delivers alarm using the configured notification mechanism. The TOE stores alert and event data to the real-time database on the database server. The TOE console polls for updated information from the TOE by monitoring changes to the TOE database. The TOE initially displays an alert; authorized administrators can then perform further analysis of the alert.

Correlation datastream processing starts when the TOE applies event correlation rules to collected data from targeted IT system resource(s). The TOE evaluates collected alerts and events against correlation rules as data arrives. When a rule match occurs, the TOE responds as the rule defines and sends the source events and resultant alerts to the database server. Authorized administrators can define event correlation rules to evaluate events received from the real-time datastream from agents. To create event correlation rules, authorized administrators run the Correlation Wizard, which is an interface to the console component. The Correlation Wizard lets authorized administrators select multiple alerts and then define a relationship and time frame. Correlation rules can amplify the importance of alerts, suppress less important alerts, and alert authorized administrators to seemingly unrelated activities that may indicate a threat.

Processing of the log management datastream begins when the TOE normalizes event data collected from targeted IT system resource(s) and sends the normalized data to the database for storage.

The TOE is configured, by default, to retain log data in the TOE datastore for 90 days. However, if the datastore reaches storage capacity, any new collected event data that is presented by agents to the TOE is ignored and a warning is displayed in the TOE. When log data is older than the retention period, TOE deletes the oldest data to free space for newer data. Authorized administrators can configure the TOE datastore retention period using interactive GUI interfaces to the console component. Log management datastream processing also includes the TOE periodically summarizing the collected data and assembling dimension information.

When an event or threshold occurs that matches a processing rule, the TOE associates the specified alert and alert severity to that event and displays the alert in the TOE console's. Alert severity allows administrators monitoring alerts to quickly determine the importance of the indicated condition. Alert severities are defined when the processing rules are created. Possible alert severities are defined as follows:

- Service Unavailable – Identifies alerts generated for missed agent heartbeats and other events indicating that an application or service is unavailable to its users.
- Security Breach – Identifies an alert that indicates a security compromise has occurred. Systems on the network are at risk.
- Critical Error – Identifies an alert that indicates a serious problem needing attention immediately.
- Error – Identifies an alert that is important and needs attention soon.
- Warning – Identifies an alert that might indicate future problems or lower priority issues requiring research.
- Information – Identifies an alert that simply provides information.
- Success – Identifies an alert that indicates a successful event or operation.

Using processing rules, administrators can also define real-time responses to a detected condition. The following processing rule types allow administrators to define responses for a processing rule match:

- Event rules
- Filtering (database and conditional filters only) rules
- Missing event rules
- Alert rules
- Performance measuring rules
- Threshold rules

Administrators can define the following responses within processing rules:

- Display alarm information to the administrator console
- Send alarm information to administrators using email
- Send alarm information to administrators using SNMP
- Execute a command
- Execute a script

Scripts and commands can be used to support notification mechanisms for which there is no built-in support.

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

- SIEM_COL.1 (EX): The TOE collects targeted IT system resource operation and configuration information from agents that are installed on the targeted IT system resource.
- SIEM _STG.2 (EX): The TOE generates alarms using a configured notification mechanism when storage capacity for collected System data has been reached.
- SIEM_COR.1 (EX): The TOE correlates event data collected from targeted IT system resources.
- SIEM_ALR.1 (EX): The TOE generates alarms that notify authorized administrators using the console, using email, using SMTP, and/or executing a command in a configured script. Note that alarms are generated in response to administratively-configured processing rules.
- SIEM_ADM.1 (EX): The TOE provides authorized administrators with the ability to interactively analyze collected data and generated reports using the GUI of the console component.

7.2 TOE Security Assurance Requirements

The following assurance measures are applied to satisfy the Common Criteria EAL3 assurance requirements:

- Configuration Management Capabilities
- Configuration Management Scope
- Delivery Procedures
- Development Security
- Life-cycle definition
- Tests

7.2.1 Configuration Management (CM) Capabilities

The configuration management measures applied by NetIQ ensure that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to design documentation, tests and test documentation, user and administrator guidance, delivery and operation documentation, vulnerability analysis documentation, and configuration management documentation.

These activities are documented in:

- NetIQ Configuration Management Manual [16]
- NetIQ Product Management Process[17]

The Configuration management assurance measure satisfies the following EAL 3 assurance requirements:

- ALC_CMC.3 - Authorization controls

[16] NetIQ Configuration Management Manual - January / February 09
[17] NetIQ Product Management Process – February 09

- ALC_CMS.3 - Implementation representation CM coverage
- ALC_DVS.1 - Identification of security measures

7.2.2 Delivery Procedures

NetIQ provides delivery documentation and procedures to identify the TOE, secure the TOE during delivery, and provide necessary installation and generation instructions. NetIQ delivery procedures describe all applicable procedures to be used to prevent inappropriate access to the TOE. NetIQ also provides documentation that describes the steps necessary to install the TOE in accordance with the evaluated configuration.

- NetIQ Delivery and Operation Procedures [18]
- NetIQ Security Manager Installation Guide[19]

The Delivery and operation assurance measure satisfies the following EAL 3 assurance requirements:

- ALC_DEL.1 - Delivery procedures
- ALC_LCD.1 - Developer defined life-cycle model

7.2.3 Development Security

The Design Documentation provided for NetIQ Security Manager is provided in two documents:

- NetIQ Security Manager Functional Specification[20]
- NetIQ Development Security Process / Procedures[21]
- NetIQ Security Manager High-level Design[22]

These documents serve to describe the security functions of the TOE, its interfaces both external and between subsystems, the architecture of the TOE (in terms of subsystems), and correspondence between the available design abstractions (including the ST).

The Development assurance measure satisfies the following EAL 3 assurance requirements:

- ADV_ARC.1 - Security architecture description
- ADV_FSP.3 - Functional specification with complete summary
- ADV_TDS.2 - Architectural design

7.2.4 Life-Cycle definition

NetIQ provides guidance on how to properly utilize the TOE security functions, including function descriptions, warnings, effects, assumptions, etc. The installation and generation procedures, included in the administrator guidance, describe the steps necessary to install NetIQ SIEM products in accordance with the evaluated configuration. Note that there are no conventional “users” of NetIQ products. All users of the TOE must belong to one or more of the OnePointOp Security Manager Groups and are classified either as administrators (System Admin or Configuration Admin) or users (Operator, Reporting User and User). As such, all applicable guidance for “administrator” and “users” is embodied in a single guide:

- User Guide, Security Manager[23]
- Evaluation Guide, Security Manager[24]
- Installation Guide, Security Manager[25]

[18] NetIQ Delivery and Operation Procedures - January / February 09
[19] NetIQ Security Manager Installation Guide - March 09
[20] NetIQ Security Manager Functional Specification - February / March 09
[21] Document to be delivered in February 09
[22] Document to be delivered in February 09
[23] User Guide, Security Manager - April/May 09
[24] Evaluation Guide, Security Manager - April/May 09

- Programming Guide, Security Manager[26]

The Guidance documents assurance measure satisfies the following EAL 3 assurance requirements:

- AGD_OPE.1 - Operational user guidance
- AGD_PRE.1 - Preparative procedures

7.2.5 Tests

The Test Documentation is found in the following documents:

- NetIQ Security Manager Test Coverage[27]
- NetIQ Security Manager Test Plan[28]
- NetIQ Security Manager Test Procedures[29]

NetIQ has a test plan that describes how each of the necessary security functions is tested, along with the expected test results. NetIQ has documented each test as well as an analysis of test coverage and depth demonstrating that the security aspects of the design evident from the functional specification and high-level design are appropriately tested. Actual test results are created on a regular basis to demonstrate that the tests have been applied and that the TOE operates as designed.

The Tests assurance measure satisfies the following EAL 3 assurance requirements:

- ATE_COV.2 - Analysis of coverage
- ATE_DPT.1 - Testing: basic design
- ATE_FUN.1 - Functional testing
- ATE_IND.2 - Independent testing – sample

7.2.6 Vulnerability Assessment

The TOE administrator and user guidance documents describe the operation of NetIQ Security Manager and how to maintain a secure state. These guides also describe all necessary operating assumptions and security requirements outside the scope of control of the TOE. They have been developed to serve as complete, clear, consistent, and reasonable administrator and user references

- NetIQ performed a vulnerability analysis of the TOE to identify weaknesses that can be exploited in the TOE. The vulnerability analysis is documented in:
- NetIQ Security Manager Vulnerability Assessment[30]

The Vulnerability assessment assurance measure satisfies the following EAL 3 assurance requirements:

- AVA_VAN.2 - Vulnerability analysis

[25] Installation Guide, Security Manager - April/May 09
[26] Programming Guide, Security Manager - April/May 09
[27] NetIQ Security Manager, Test Coverage - March 09
[28] NetIQ Security Manager, Test Plan - March 09
[29] NetIQ Security Manager, Test Procedures - March 09
[30] NetIQ Security Manager Vulnerability Assessment - February 09 – if needed