CSEC

Swedish Certification Body for IT Security

Certification Report NetIQ® Sentinel™ 8.1

Issue: 1.0, 2018-October-12

Table of Contents

1 Executive Summary

The Target of Evaluation, TOE, is a Security Information and Event Management Solution (SIEM) as well as a compliance monitoring solution. The TOE's intended usage is to collect log information from other sources and to provide real-time analysis of security alerts generated by applications and network hardware. The TOE is a software TOE, NetIQ® Sentinel™ 8.1, and includes the following components:

- Sentinel Server (featuring console functionality through a web interface)
- Data Collector
- Correlation Engine

The TOE is downloaded from NetIQ's web site either as install files, ISO images, or as OVF virtual machines.

The ST does not make conformance claims to any protection profile.

There are seven assumptions being made in the Security Target (ST) regarding the secure usage and environment of the TOE. The TOE relies on these to counter the two threats and comply with the two organisational security polices (OSPs) in the ST. The assumptions, the threats and the OSPs are described in chapter 4 Assumptions and Clarification of Scope.

The evaluation has been performed by Combitech AB and EWA-Canada Ltd. The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1, release 5, and the Common Methodology for IT Security Evaluation, version 3.1, release 5. The evaluation was performed at the evaluation assurance level EAL 3, augmented by ALC_FLR.1 Basic flaw remediation.

Combitech AB is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. Combitech AB is also accredited by the Swedish accreditation body SWEDAC according to ISO/IEC 17025 for Common Criteria evaluation. EWA-Canada Ltd. operates as a Foreign location for Combitech AB within scope of the Swedish Common Criteria Evaluation and Certification Scheme.

The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports. The certifier determined that the evaluation results confirm the security claims in the Security Target [ST], and have been reached in agreement with the requirements of the Common Criteria and the Common Methodology for evaluation assurance level:

EAL 3 + ALC_FLR.1.

The certification results only apply to the versions of the products indicated in the certificate, and on the condition that all the stipulations in the Security Target [ST] are met.
This certificate is not an endorsement of the IT product by CSEC or any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by CSEC or any other organization that recognizes or gives effect to this certificate is either expressed or implied.

2 Identification

Certification Identification

Certification ID	CSEC2017007
Name and version of the certified IT product	NetIQ® Sentinel™ 8.1 components: - Sentinel Server, version 8.1.0.1_4309 - Data Collector, version 8.1.0.1_4309 - Correlation Engine, version 8.1.0.1_4309 or - Sentinel Appliance, version 8.1.0.1_4309 (all components and OS as a virtual machine)
Security Target	Security Target: NetIQ® Sentinel™ 8.1, NetIQ Corporation, 2018-08-08, document version 2.0
Assurance level	EAL 3 + ALC_FLR.1
Sponsor	NetIQ Corporation
Developer	NetIQ Corporation
ITSEF	Combitech AB, EWA-Canada Ltd.
Common Criteria version	3.1 release 5
CEM version	3.1 release 5
Certification date	2018-10-12

3 Security Policy

The TOE provides the following security services:

- Security Management
- Security Audit
- Identification and Authentication

3.1 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 using the Console functionality via a web-based connection. The TOE provides an inactivity timeout mechanism.

3.2 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.

3.3 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.

4 Assumptions and Clarifications of Scope

4.1 Usage Assumptions

The Security Target [ST] makes two assumptions on the usage of the TOE.

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

4.2 Environmental Assumptions

Five assumptions on the environment are made in the Security Target.

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.

4.3 Organizational Security Policies

The Security Target [ST] places two organizational Security Policies on the usage of -the TOE.

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.

4.4 Clarification of Scope

The Security Target [ST] contains two threats, which have been considered during the evaluation.

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.

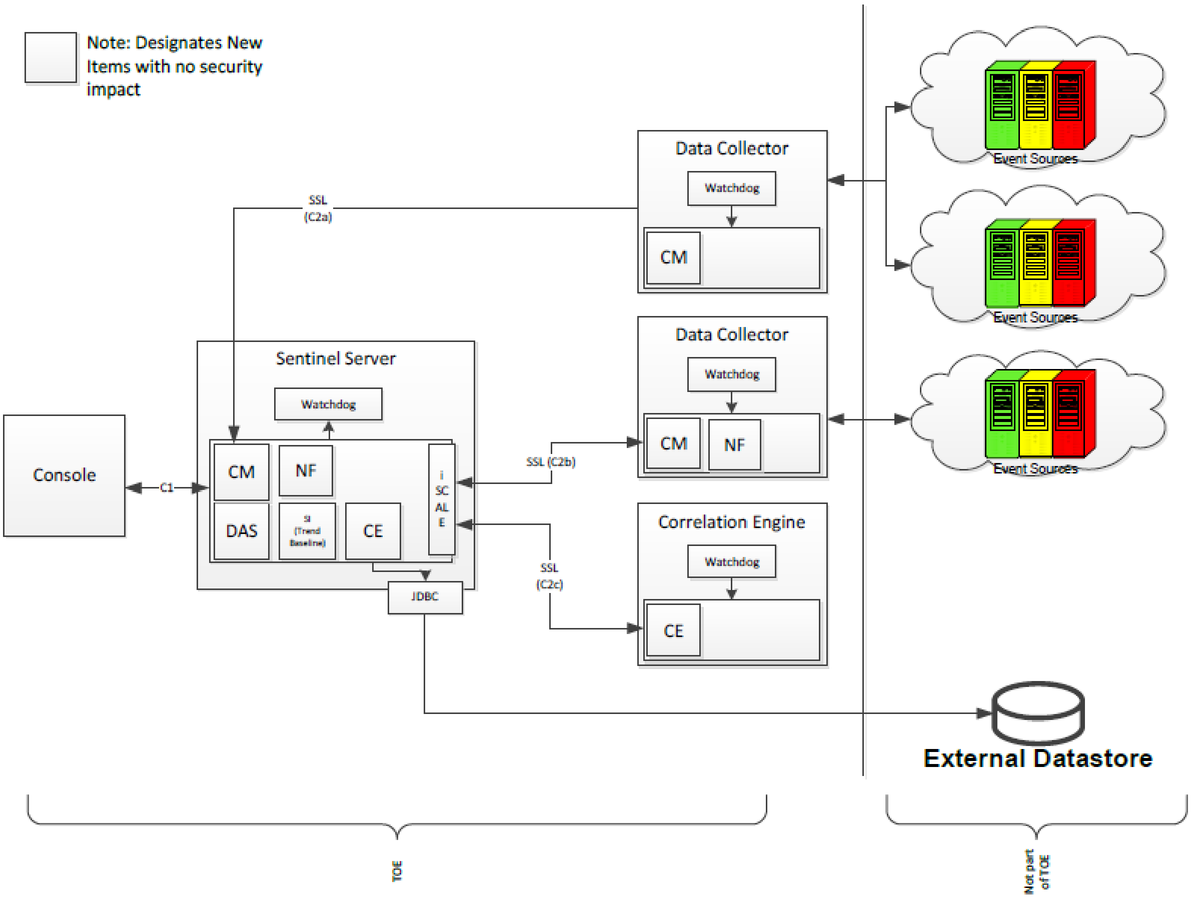
T.NO_PRIV - An authorized user of the TOE exceeds his/her assigned security privileges resulting in unauthorized modification of the TOE configuration and/or data. The asset are the configuration of the TOE, data that is collected, and the resultant analysis by the TOE.

.

5 Architectural Information

The TOE consists of the following components:

- Console
- Sentinel Server
- Data Collector
- Correlation Engine



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

The following diagram reflects the functional blocks in the configuration:

5.1 Console

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

5.2 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
- Data Access Service
- Correlation Engine
- NetFlow Collector Manager
- iSCALE

5.2.1 Sentinel Service Wrapper

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

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

5.2.2 Collector Manager

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.

5.2.3 Data Access Service:

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

5.2.4 Correlation Engine

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

5.2.5 NetFlow Collector Manager

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

5.2.6 iSCALE

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

5.3 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.

5.4 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.

5.5 Correlation Engine

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.

6 Documentation

The TOE includes the following product documentation:

- Sentinel 8.1.0.1 Release Notes
- NetIQ® Sentinel™ Administration Guide
- NetIQ® Sentinel™ User Guide
- NetIQ® Sentinel™ Installation and Configuration Guide June 2017
- NetIQ® Sentinel™ 8.1 Operational User Guidance and Preparative Procedures Supplement
- NetIQ® Sentinel™ 8.1 Secure Delivery Processes and Procedures

7 IT Product Testing

7.1 Developer Testing

The developer testing covers all SFRs, and all combinations of SUSE Linux Enterprise Server 12 SP2 64 bit, and Red Hat Enterprise Linux 7.3 64 bit operating systems in the system components.

The developer testing was performed in the developer site in Houston, USA.

7.2 Evaluator Testing

The evaluators have reproduced a selection of developer tests on a virtual appliance, and run complementary tests.

During the complementary testing the evaluators discovered the following:

After user session time-out, when a user has forgotten to log out, an information leakage between users may occur, where the previous users display is visible, but not usable, when another user logs in. In the evaluated configuration, without untrusted and remote users, this is not a problem.

The developer testing was performed in the evaluator's premises in Växjö, Sweden.

7.3 Evaluator Penetration Testing

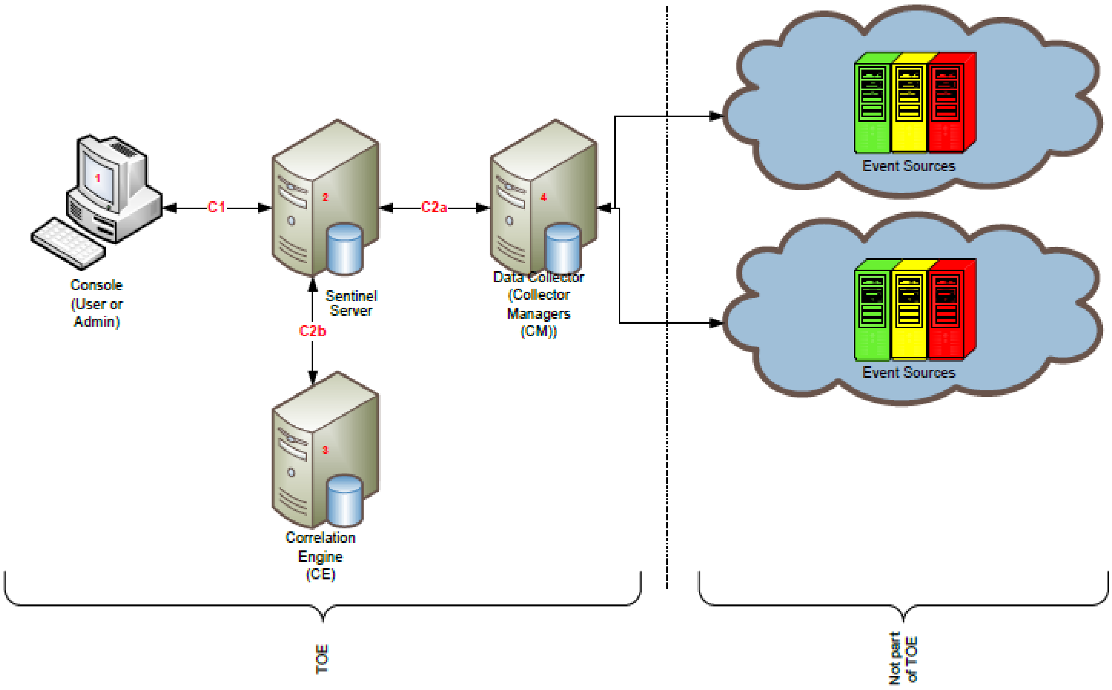
The evaluators penetration tested a hardware appliance TOE at the developer site in Houston, USA, and a virtual appliance TOE in the evaluator's premises in Växjö, Sweden.

Vulnerability scans were run with Nessus and Nmap, port enumeration and service mapping with Netstat and ps.

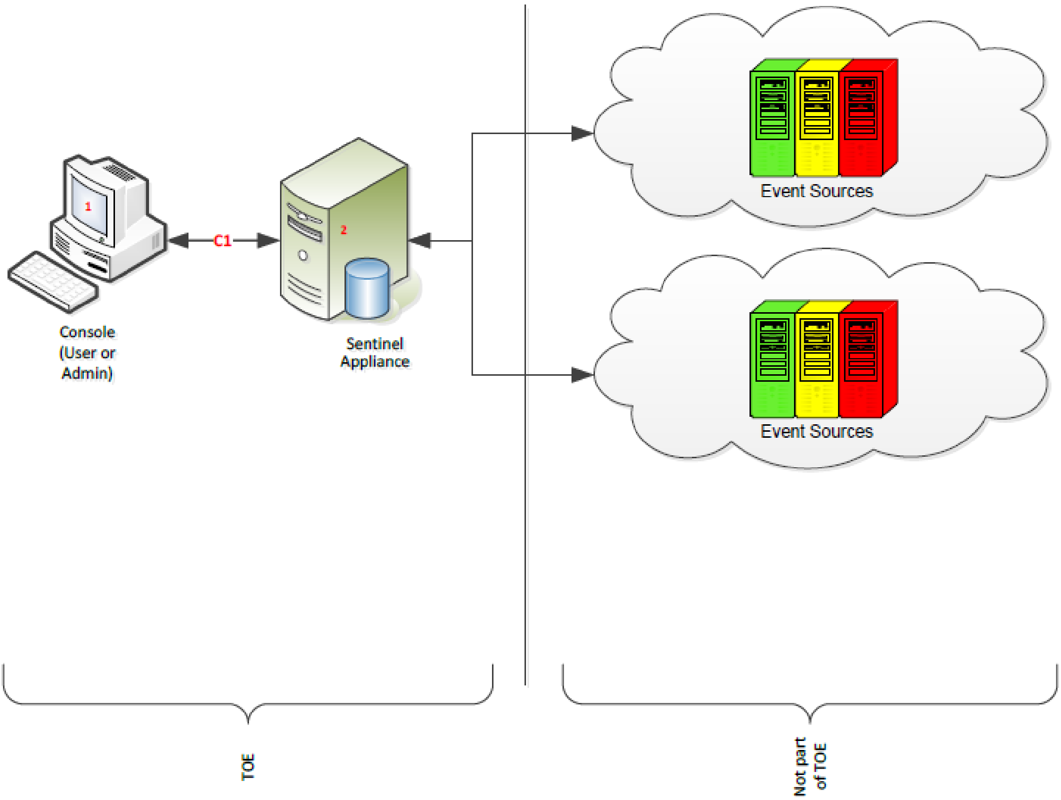
No vulnerabilities were found in the TOE, but there are complex IT products in the operating environment where new vulnerabilities are likely to be discovered frequently. Some of these may be updated regularly by NetIQ patches, but the users should make sure to patch the operating systems and Oracle Java JRE promptly when new vulnerabilities are found.

8 Evaluated Configuration

Two different configurations of the TOE have been evaluated. The first configuration consists of the Basic Sentinel Server product as depicted in the figure below..



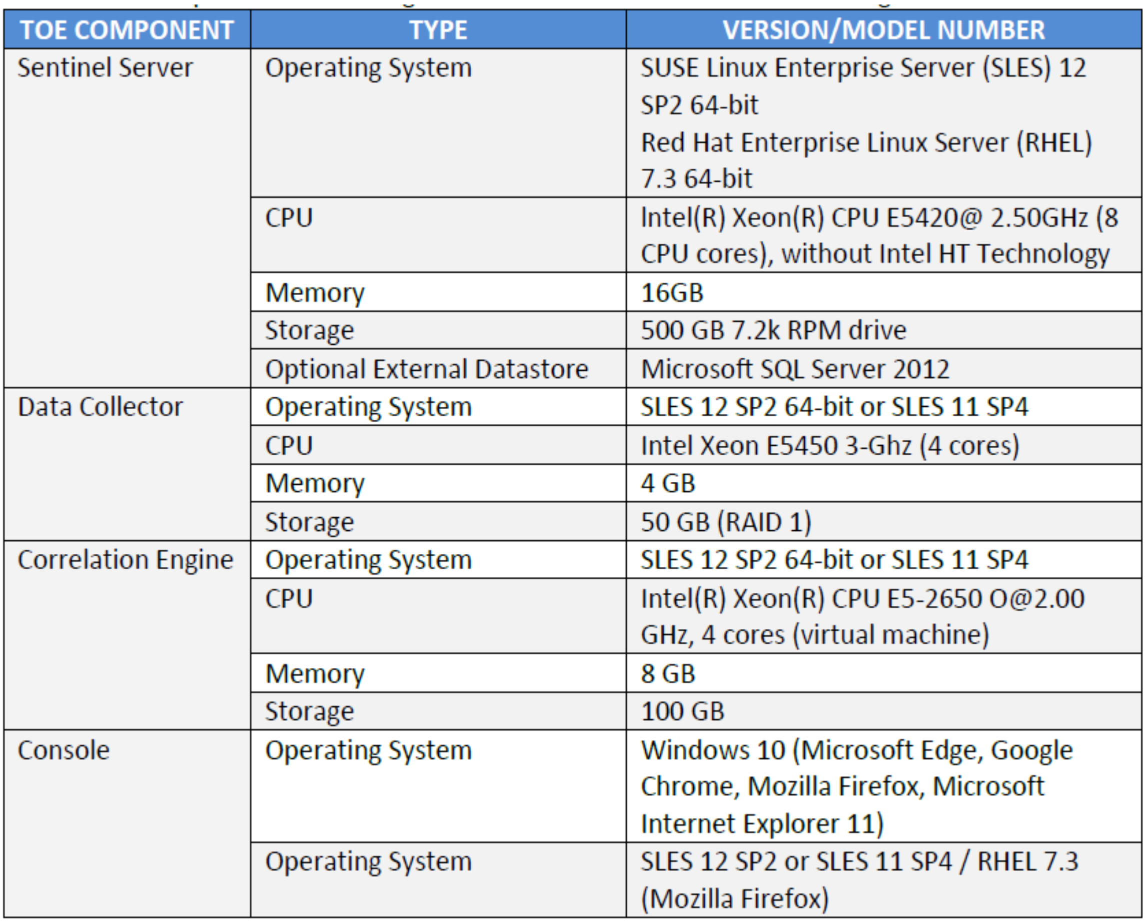
The second configuration is a virtual appliance in the form of an OVF as depicted in the figure below.



The following constraints exists for the two evaluated configurations:

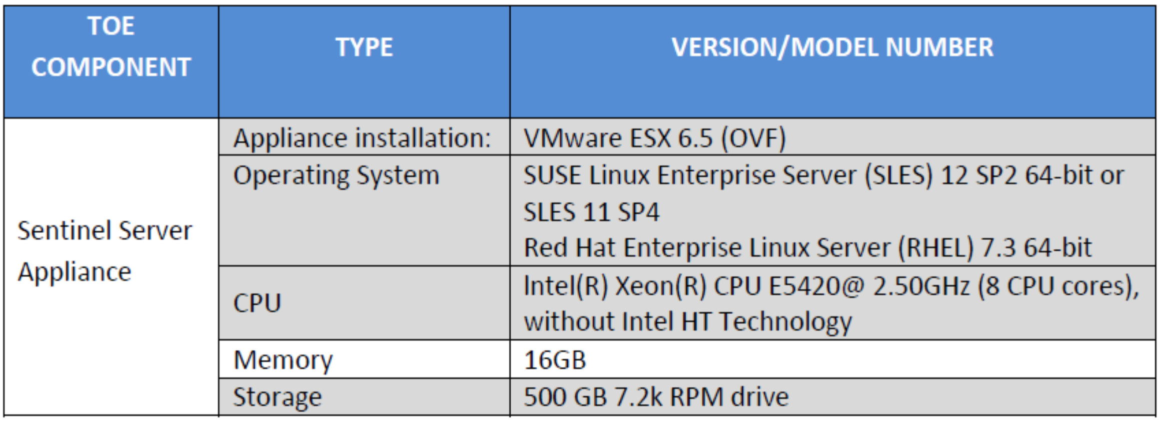
- The hardware, operating systems and third party support software (e.g. DBMS) on each of the systems are excluded from the TOE scope.
- Sentinel plugins can be used in the evaluated configuration as they are not security relevant. Plugins are part of the TOE and are not a separate / distinct entity.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

The Sentinel Server configuration 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 0@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)

The Sentinel Appliance configuration 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

9 Results of the Evaluation

The evaluators applied each work unit of the Common Methodology [CEM] within the scope of the evaluation, and concluded that the TOE meets the security objectives stated in the Security Target [ST] for an attack potential of Basic.

The certifier reviewed the work of the evaluator and determined that the evaluation was conducted in accordance with the Common Criteria [CC].

The evaluators overall verdict is PASS.

The verdicts for the respective assurance classes and components are summarised in the following table:

Assurance Class/Family		*Short name*	*Verdict*
Development		ADV	PASS
	Security Architecture	ADV_ARC.1	PASS
	Functional Specification	ADV_FSP.3	PASS
	TOEl Design	ADV_TDS.2	PASS
Guidance Documents		AGD	PASS
	Operational User Guidance	AGD_OPE.1	PASS
	Preparative Procedures	AGD_PRE.1	PASS
Life-cycle Support		ALC	PASS
	CM Capabilities	ALC_CMC.3	PASS
	CM Scope	ALC_CMS.3	PASS
	Delivery	ALC_DEL.1	PASS
	Development Security	ALC_DVS.1	PASS
	Life-cycle Definition	ALC_LCD.1	PASS
	Flaw Remediation	ALC_FLR.1	PASS
Security Target Evaluation		ASE	PASS
	ST Introduction	ASE_INT.1	PASS
	Conformance Claims	ASE_CCL.1	PASS
	Security Problem Definition	ASE_SPD.1	PASS
	Security Objectives	ASE_OBJ.2	PASS
	Extended Components Definition	ASE_ECD.1	PASS
	Security Requirements	ASE_REQ.2	PASS
	TOE Summary Specification	ASE_TSS.1	PASS
Tests		ATE	PASS
	Coverage	ATE_COV.2	PASS
	Depth	ATE_DPT.1	PASS
	Functional Tests	ATE_FUN.1	PASS
	Independent Testing	ATE_IND.2	PASS
Vulnerability Assessment		AVA	PASS
	Vulnerability Analysis	AVA_VAN.2	PASS

10 Evaluator Comments and Recommendations

The evaluators do not have any comments or recommendations concerning the product or using the product.

11 Glossary

CC	Common Criteria version 3.1
CE	Correlation Engine
CM	Collector Manager
DAS	Data Access Service
DBMS	Database Management System
EAL	Evaluation Assurance Level
EOE	Events Originating External to the TOE
I&A	Identification and Authentication
ISO	International Standards Organization. When referring to a CD or DVD it means ISO-9660
NF	NetFlow Collector Manager
NTP	Network Time Protocol
OSP	Organizational Security Policy
OVF	Open Virtualization Format
SFR	Security Functional Requirement
SSHD	Solid-State Hard Drive
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TSF Interface

12 Bibliography

ST Security Target: NetIQ® Sentinel™ 8.1, NetIQ Corporation, 2018-08-08, document version 2.0

USER NetIQ® Sentinel™ User Guide, NetIQ Corporation, June 2017

ADM NetIQ® Sentinel™ Administration Guide, NetIQ Corporation, June 2017

INST NetIQ® Sentinel™ Installation and Configuration Guide, NetIQ Corporation, June 2017

PREP NetIQ® Sentinel™ 8.1 Operational User Guidance and Preparative Procedures Supplement, NetIQ Corporation, 2018-08-07, document version 1.0

DEL NetIQ® Sentinel™ 8.1 Secure Delivery Processes and Procedures, NetIQ Corporation, 2017-08-07, document version 1.0

REL Sentinel 8.1.0.1 Release Notes, NetIQ Corporation, July 2017

CCpart1 Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1 revision 5, CCMB-2017-04-001

CCpart2 Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1 revision 5, CCMB-2017-04-002

CCpart3 Common Criteria for Information Technology Security Evaluation, Part 3, version 3.1 revision 5, CCMB-2017-04-003

CC CCpart1 + CCpart2 + CCpart3

CEM Common Methodology for Information Technology Security Evaluation, version 3.1 revision 5, CCMB-2017-04-004

SP-002 SP-002 Evaluation and Certification, CSEC, 2018-04-24, document version 29.0

SP-188 SP-188 Scheme Crypto Policy, CSEC, 2017-04-04, document version 7.0

Appendix A - QMS Consistency

During the certification project, the following versions of the quality management system (QMS) have been applicable since the certification application was received 2017-05-06:

QMS 1.20.3	valid from 2017-04-24
QMS 1.20.4	valid from 2017-05-11
QMS 1.20.5	valid from 2017-06-28
QMS 1.21	valid from 2017-11-15
QMS 1.21.1	valid from 2018-03-09
QMS 1.21.2	valid from 2018-03-09 SIC!
QMS 1.21.3	valid from 2018-05-24
QMS 1.21.4	valid from 2018-09-13

In order to ensure consistency in the outcome of the certification, the certifier has examined the changes introduced in each update of the quality management system.

The changes between consecutive versions are outlined in “Ändringslista CSEC QMS 1.21.4”.

The certifier concluded that, from QMS 1.20.3 to the current QMS 1.21.4, there are no changes with impact on the result of the certification.