Swedish Certification Body for IT Security

Certification Report - Sentinel™ 8.5.1.0

Issue: 1.0, 2023-feb-27

Authorisation: Helén Svensson, Lead certifier , CSEC

Table of Contents

1 Executive Summary

The target of evaluation (TOE) is the security information and event management (SIEM) software Sentinel™ 8.5.1.0-5968. It provides centralized aggregated logs from different sources and can be setup to react upon defined scenarios.

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

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

The TOE components can be installed on separate hardware or as a virtual appliance.

The TOE is delivered as software with documentation.

It is important to verify the integrity of the TOE for secure acceptance of the TOE in accordance with the preparative procedures of the guidance, i.e. verify the TLS connection, the CA certificate and the file hash. It is also important to update the TOE (including 3rd party software) and the operational environment of the TOE in accordance with the preparative procedures of the guidance to mitigate known vulnerabilities.

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 in Bromma and Växjö, Sweden (critical locations), and by Intertek/EWA-Canada in Ottawa, Canada (foreign location).

The evaluation was completed on 2023-02-17. The evaluation was conducted in accordance with the requirements of Common Criteria (CC), version. 3.1 release 5.

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 according to ISO/IEC 17025 for Common Criteria. Intertek/EWA-Canada 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 and by observing site-visit and testing. The certifier determined that the evaluation results confirm the security claims in the Security Target (ST) and the Common Methodology for evaluation assurance level:

EAL3 + ALC_FLR.1.

The evaluation was performed as a re-evaluation of the previous evaluation of NetIQ® Sentinel™ 8.1.0.1-4309, CSEC2017007, according to FMV/CSECs scheme publication EP-003 Assurance Continuit [EP-003].

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

2 Identification

Certification Identification	
Certification ID	CSEC2022010
Name and version of the certified IT product	Sentinel™ 8.5.1.0, Version 8.5.1.0-5968 components: • Console • Sentinel Server • Data Collector • Correlation Engine (CE)
Security Target Identification	NetIQ® Sentinel™ 8.5.1.0 Security Target, OpenText, 2023-02-10, document version 0.15
EAL	EAL 3 + ALC_FLR.1
Sponsor	OpenText
Developer	OpenText
ITSEF	Combitech AB, Intertek/EWA-Canada
Common Criteria version	3.1 release 5
CEM version	3.1 release 5
QMS version	2.3
Scheme Notes Release	20.0
Recognition Scope	CCRA, SOGIS, EA/MLA
Certification date	2023-02-27

3 Security Policy

The security functions performed by the TOE are as follows:

- 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 with the Console via 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 Clarification 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

The Security Target [ST] makes five assumptions on the operational environment of the TOE.

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 Clarification of Scope

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

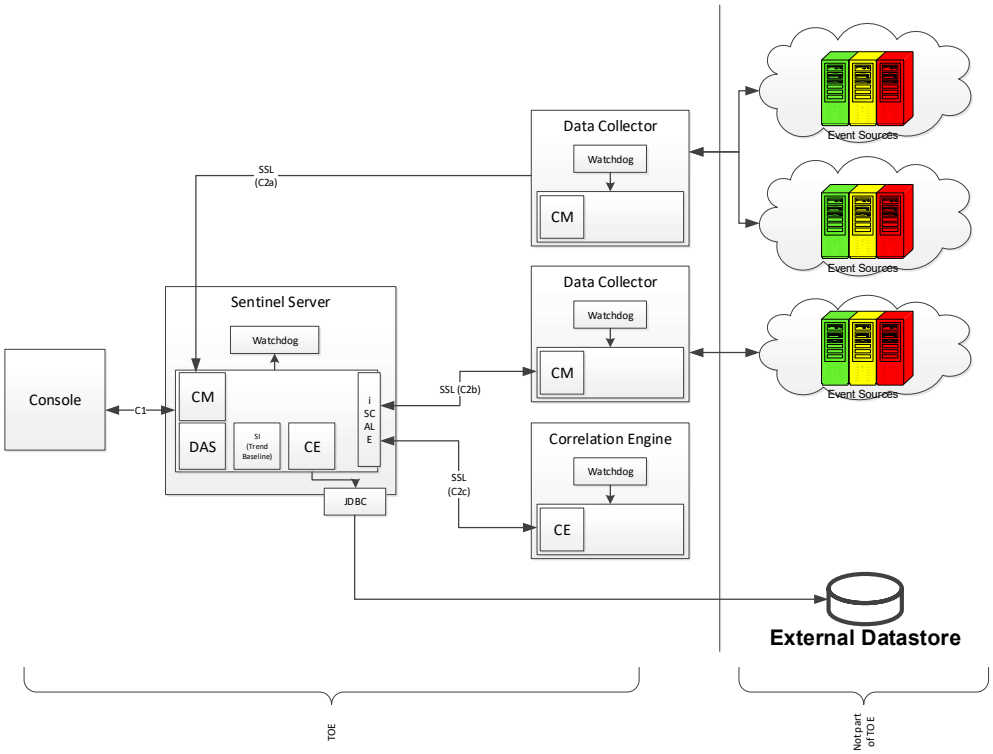
The Security Target contains two Organisational Security Policies (OSPs), which have been considered during the evaluation.

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.

5 Architectural Information

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

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



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

5.1 Console[1]

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

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

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 (CM)
- Data Access Service (DAS)
- Correlation Engine (CE)
- iSCALE

5.2.1 Sentinel Service Wrapper (Watchdog)

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

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

5.2.2 Collector Manager (CM)

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

5.2.3 Data Access Service (DAS):

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

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

5.2.4 Correlation Engine (CE)

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

5.2.5 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.

5.3.1 Collector Manager

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

5.4 Correlation Engine (CE)

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

6 Documentation

The TOE includes the following product documentation:

- Sentinel™ 8.5.1.0 Release Notes, October 2022 [REL]
- Sentinel™ 8.5.1.0 Administration Guide, October 2022 [ADM]
- Sentinel™ 8.5.1.0 User Guide, October 2022 [USER]
- Sentinel™ 8.5.1.0 Installation and Configuration Guide, October 2022 [INST]
- Sentinel™ 8.5.1.0 System Requirements, October 2022 [REQ]

7 IT Product Testing

7.1 Developer Testing

There are 22 test cases covering all SFRs with at least one test.

Tested configurations:

OS	Sentinel Server	Data Collector (DCE)	Correlation Engine
SLES12 SP5 64 bit	SLES12 SP5 64 bit	SLES12 SP5 64 bit	SLES12 SP5 64 bit
RHEL 7.9 64 bit	RHEL 7.9 64 bit	RHEL 7.9 64 bit	RHEL 7.9 64 bit

All tests were successful with a pass verdict.

7.2 Evaluator Testing

The evaluator repeated ten of the developer tests.

With one minor remark, the evaluator concludes that all actual test results (repeated tests) are consistent with the expected test results.

An issue was discovered were the Visualization tab (/visual-analytics/-page) remained open both after a user initiated log out (from any other tab than Visualization) and after a session timeout has passed. The behaviour appeared both for Administrators and Users. The screen was locked for input without further authentication but the screen content was exposed. The behaviour is noted in [ST] and the user is instructed to manually wipe this specific screen by initiate a new authentication after log out.

The evaluator accepts this work around until the problem is fixed in coming releases of the TOE.

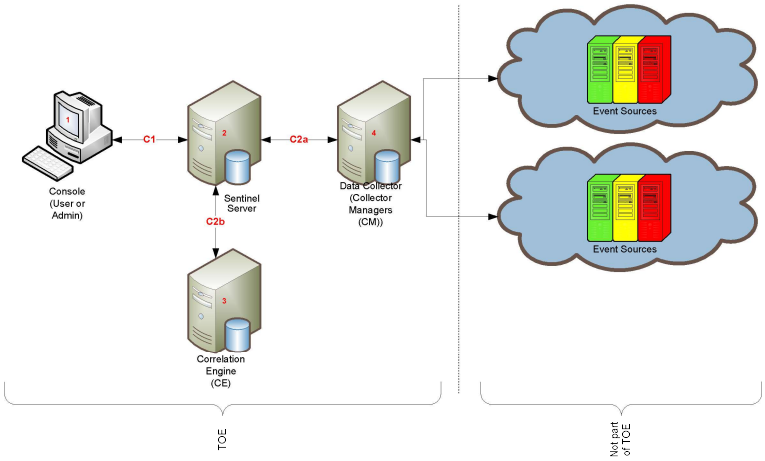
7.3 Penetration Testing

The evaluator performed vulnerability scanning with Nessus, nmap and port enumeration and service mapping using netstat and ps.

No potential vulnerabilities were found to devise specific penetration tests against.

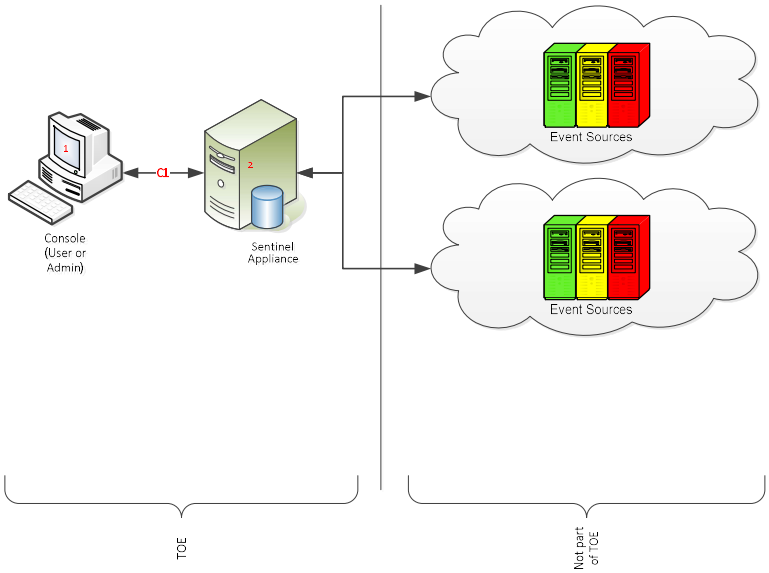
8 Evaluated Configuration

The evaluation consists of two configurations for the product. 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 figure below.



Note the following constraints for the evaluated configuration:

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

- The command line interface is excluded from evaluation.
  Note the 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 SP5 64-bit Red Hat Enterprise Linux Server (RHEL) 7.9 64-bit
	CPU	Two lntel(R) Xeon(R) CPU ES2650 O@ 2.00GHz (4 core) CPUs (8 cores total), without Intel HT Technology
	Memory	24GB
	Storage	500 GB 7.2k RPM drive
	Optional External Datastore	Microsoft SQL Server 2017
Data Collector	Operating System	SLES 12 SP5 64-bit
	CPU	lntel(R) Xeon(R) CPU E5-2650 O@ 2.00GHz, 4 cores (virtual machine)
	Memory	4 GB
	Storage	100 GB (RAID 1)
Correlation Engine	Operating System	SLES 12 SP5 64-bit
	CPU	lntel(R) Xeon(R) CPU E5-2650 O@ 2.00GHz, 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 SP5 / RHEL 7.9 64 (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 6.7 (OVF)
	Operating System	SUSE Linux Enterprise Server (SLES) 12 SP5 64-bit
	CPU	lntel(R) Xeon(R) CPU E5420@ 2.50GHz (8 CPU cores), without Intel HT Technology
	Memory	24 GB
	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 evaluators and determined that the evaluation was conducted in accordance with the Common Criteria [CC].

The evaluators' overall verdict is PASS.

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

Assurance components	*Short name*	*Verdict*
Development	ADV	PASS
Security architecture description	ADV_ARC.1	PASS
Functional specification with complete summary	ADV_FSP.3	PASS
Architectural 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
Authorisation controls	ALC_CMC.3	PASS
Implementation representation CM coverage	ALC_CMS.3	PASS
Delivery procedures	ALC_DEL.1	PASS
Identification of security measures	ALC_DVS.1	PASS
Developer defined life-cycle model	ALC_LCD.1	PASS
Basic flaw remediation	ALC_FLR.1	PASS
Security Target evaluation	ASE	PASS
Conformance claims	ASE_CCL.1	PASS
Extended components definition	ASE_ECD.1	PASS
ST introduction	ASE_INT.1	PASS
Security objectives	ASE_OBJ.2	PASS
Derived security requirements	ASE_REQ.2	PASS
Security problem definition	ASE_SPD.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Tests	ATE	PASS
Analysis of coverage	ATE_COV.2	PASS
Testing: basic design	ATE_DPT.1	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing - sample	ATE_IND.2	PASS
Vulnerability assessment	AVA	PASS
Vulnerability analysis	AVA_VAN.2	PASS

10 Evaluator Comments and Recommendations

Since the TOE contains several 3rd party components and since the TOE relies upon the security of the underlying Linux OS it is important for the administrator to update the TOE and the operational environment of the TOE in accordance with the guidance to mitigate know vulnerabilities.

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	NetIQ® Sentinel™ 8.5.1.0 Security Target, OpenText, 2023-02-10, document version 0.15
USER	Sentinel™ 8.5.1.0 User Guide, Micro Focus, October 2022
ADM	Sentinel™ 8.5.1.0 Administration Guide, Micro Focus, October 2022
INST	Sentinel™ 8.5.1.0 Installation and Configuration Guide, Micro Focus, October 2022
REQ	Sentinel™ 8.5.1.0 System Requirements, Micro Focus, October 2022
REL	Sentinel™ 8.51.0 Release Notes, Micro Focus, October 2022
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
EP-002	EP-002 Evaluation and Certification, CSEC, 2021-10-26, document version 34
EP-003	EP-003 Assurance Continuity, CSEC, 2021-10-26, document version 16.0

Appendix A Scheme Versions

During the certification the following versions of the Swedish Common Criteria Evaluation and Certification scheme have been used.

A.1 Scheme/Quality Management System

Version	Introduced	Impact of changes
2.3	2023-01-26	None.
2.2	Application	Original version

A.2 Scheme Notes

The following Scheme Notes have been considered during the evaluation:

- Scheme Note 15 - Testing
- Scheme Note 18 - Highlighted Requirements on the Security Target
- Scheme Note 22 - Vulnerability assessment
- Scheme Note 27 - ST requirements at the time of application for certification
- Scheme Note 28 - Updated procedures for aplication, evaluation ad certification
- Scheme Note 31 - New procedures for site visit oversight and testing oversight