Swedish Certification Body for IT Security

Certification Report - OpenText ArcSight Logger 7.3

Issue: 1.0, 2026-Feb-26

Authorisation: Hans Sharma, Junior Certifier , CSEC

Table of Contents

1 Executive Summary

The TOE is the ArcSight Logger 7.3.0.8511.8 from OpenText. The TOE is a software only TOE. Logger is a data collection and storage engine that unifies log data collection, storage, and security data management in a scalable, high-performance software or appliance solution. It provides capabilities to collect machine data from any source (such as logs, clickstreams, sensors, stream network traffic, security devices, web servers, custom applications, social media, and cloud services) and to monitor and search that data for security intelligence.

The TOE ArcSight Logger is a log management solution designed to handle high event throughput, support data analysis, and provide efficient long-term storage. Logger receives and stores events, supports search, retrieval, and reporting, and can optionally forward selected events (e.g., to ArcSight ESM).

While the product is available in appliance and software form factors, the TOE is software only. The TOE software is provided to customers via secure download.

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

There are six assumptions made in the ST regarding the secure usage and environment of the ArcSight Logger 7.3. The TOE relies on these being met to counter the four threats and no organisational security policy in the ST. The assumptions and the threats are described in chapter 4 Assumptions and Clarifications of Scope.

The evaluation has been performed by Combitech AB at their premises in Bromma, Sweden, and Växjö, Sweden.

The evaluation was completed on 2026-02-16. The evaluation was conducted in accordance with the requirements of Common Criteria (CC), version 2022 revision 1 (of November 2022).

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.

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 the Common Methodology for evaluation assurance level EAL 2 augmented by e.g. ALC_FLR.3.

The technical information in this report is based on the Security Target (ST) and the Final Evaluation Report (FER) produced by Combitech AB.

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	CSEC2025011
Name and version of the certified IT product	ArcSight Logger 7.3.0.8511.8
Security Target Identification	ArcSight Logger 7.3.0.8511.8 Security Target, OpenText Corporation, 2026-02-10, Version 0.11
EAL	EAL 2 + ALC_FLR.3
Sponsor	OpenText Corporation
Developer	OpenText Corporation
ITSEF	Combitech AB
Common Criteria version	2022 revision 1
CEM version	2022 revision 1
QMS version	2.6.1
Scheme Notes Release	22.0
Recognition Scope	CCRA, SOGIS, EA/MLA
Certification date	2026-02-26

3 Security Policy

The TOE provides the following security functionality:

Security Audit

Cryptographic Support

Identification and Authentication

Security Management

Protection of the TSF

TOE Access

Trusted Path

3.1 Security Audit

The TOE generates the following audit data:

▪ Start-up and shutdown of the audit functions (instantiated by start-up of the TOE)

▪ User login/logout, Login failures [All User access and activities performed while accessing systems]

The TOE records the date, time and type of event as well as the subject identity and outcome of the event.

The TOE provides the Administrator with the capability to read all audit data generated within the TOE via the Console or via the external event sources. The Console provides a suitable means for an Administrator to interpret the information from either the audit log. The audit data is stored on the Logger server.

A.TIMESOURCE is added to the assumptions on operational environment, and OE.TIME is added to the operational environment security objectives. The time and date are provided by the operational environment. The TOE ensures that the audit trail data is stamped when recorded with a dependable date and time received from the OE (operating system). In this manner, accurate time and date is maintained on the TOE.

3.2 Cryptographic Support

Logger uses the environment cryptography to establish TLS v1.2 connections for secure communications.

If Logger is the Server, as in the case of the evaluated configuration, and FIPS mode is configured, Logger avails itself of the Voltage environment Cryptography. This is not part of the TOE, but it is invoked by TOE.

3.3 Identification and Authentication

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

3.4 Security Management

Security Management is provided by enforcing roles and rules. Each role consists of a series of privileges. Roles can have privileges added to or removed from them. These roles are then assigned to individuals. In addition, rules can be specified controlling where and when the privileges may be used. Note a user may only have one role at a time.

The table below describes the TOE management functions along with their SFRs.

3.5 Protection of the TSF

Reliable timestamps are provided by an NTP Server in the environment.

3.6 TOE Access

The TOE can terminate sessions either via a pre-configured inactivity timeout or via a user-initiated timeout. The TOE can also prevent TOE users (Administrators, Users), from accessing the system outside of their authorized time.

3.7 Trusted Path

The Environment provides the cryptographic algorithms needed to establish a trusted path using TLS v1.2. The Environment provides Bouncy Castle version 1.0.2.1 (CMVP certificate # 4616) to protect communications between Logger and the SmartConnectors and between Logger and the AD Server.

4 Assumptions and Clarification of Scope

4.1 Assumptions

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

A.PROTECT

The TOE software critical to security policy enforcement will be protected from unauthorized physical modification. TSF data shall be protected from disclosure.

A.HTTPS

Web browsers used to access the TOE shall support HTTPS using TLS. Communications between the TOE and trusted IT products are [WHAT?]

A.PLATFORM

The underlying operating system of each TOE software component will protect the component and its configuration from unauthorized access.

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

Administrators of the TOE are well-trained and non-hostile.

A.TIMESOURCE

The TOE has a trusted source for system time via NTP server

4.2 Clarification of Scope

The Security Target contains four 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.

T.NO_PRIV

An authorized user of the TOE exceeds their assigned security privileges resulting in unauthorized modification of the TOE configuration and/or data.

T.UNATTENDED_SESSION

An unauthorized user gains access to the TOE via an unattended authorized user session.

T.SENSDATA

An unauthorized user may be able to view sensitive data passed between the TOE and its remote users, and between the TOE and external web servers, and exploit this data to gain unauthorized privileges on the TOE.

There are no OSPs for this TOE.

5 Architectural Information

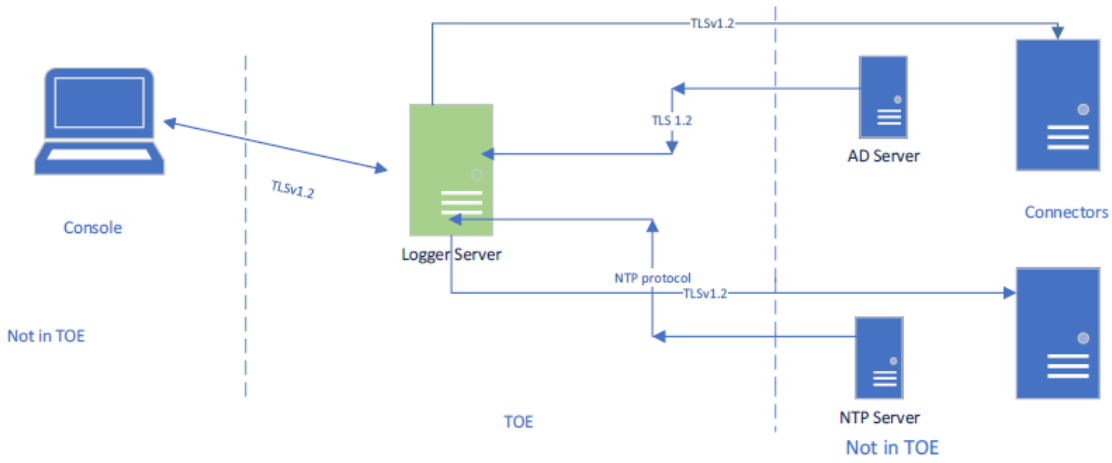
The TOE is a software only TOE. In its evaluated configuration it consists of the Logger software.

For the purpose of this certification, the TOE includes:

- A data collection and storage engine that unifies log data collection, storage, and security data management. It provides capabilities to collect machine data from any source (such as logs, clickstreams, sensors, stream network traffic, security devices, web servers, custom applications, social media, and cloud services) and to monitor and search that data for security intelligence.

- A browser-based GUI that enables Logger users to access functional capabilities.

- a Web Services Application Programming Interface (API) that exposes Logger functions as Web services. This enables Logger functionality to be integrated into other ArcSight products and third-party applications.



6 Documentation

The TOE includes the following guidance documentation:

Micro Focus Security ArcSight Logger, Software Version: 7.3, Installation and Configuration Guide

Micro Focus Security ArcSight Logger, Software Version: 7.3, Administrator's Guide

Additional TOE operational guidance and installation procedures will be provided in the TOE Operational Guidance and Installation Procedures (AGD-IGS.1).

7 IT Product Testing

7.1 Developer Testing

The developer’s testing covers the most of the security functional behaviour of the TSFIs and nearly all SFRs.

7.2 Evaluator Testing

The evaluator performed the installation of the TOE into the evaluated configuration, repeated a subset of the developer tests, and added two complementary tests (modification of test 10). One test per SFR was conducted. Tests relying on external services were excluded. The complementary tests failed to match evaluator expectations; this was mitigated by updates in the ST and guidance. All other test results were as expected

7.3 Penetration Testing

Since the TOE is placed in a physically secure location (A.LOCATE, OE.PHYSEC), the main focus was on the network connectivity, the active listening server ports.

The following types of penetration tests were performed:

• Vulnerability scanning, Nessus and Nmap

• TLS Scanning

8 Evaluated Configuration

The following software components are required for operation of the TOE in the evaluated configuration:

Supplied by the Environment	Environment Requirements
SmartConnector for Windows 25.1.1	Windows Server 2022
SmartConnector for Linux 25.1.1	RHEL 9.2
Browser	Firefox, Edge, Chrome
NTP Server	Chrony (RHEL 9 default) – Version chrony-4.6.1-1.el9.x86_64
AD Server	Windows Server 2019 Standard running LDAP version 3

The following functionality is excluded from the evaluated configuration:

• Hadoop functionality

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 evaluator's overall verdict is PASS.

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

Assurance Class/Family	Short name	Verdict
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
Life-Cycle Support	ALC	PASS
CM Capabilities	ALC_CMC.2	PASS
CM Scope	ALC_CMS.2	PASS
Delivery	ALC_DEL.1	PASS
Flaw Remediation	ALC_FLR.3	PASS
Development	ADV	PASS
Security Architecture	ADV_ARC.1	PASS
Functional Specification	ADV_FSP.2	PASS
TOE Design	ADV_TDS.1	PASS
Guidance Documents	AGD	PASS
Operational User Guidance	AGD_OPE.1	PASS
Preparative Procedures	AGD_PRE.1	PASS
Tests	ATE	PASS
Coverage	ATE_COV.1	PASS
Functional tests	ATE_FUN.1	PASS
Independent testing	ATE_IND.2	PASS
Vulnerability Analysis	AVA	PASS
Vulnerability analysis	AVA_VAN.2	PASS

10 Evaluator Comments and Recommendations

None.

11 Glossary

CC	Common Criteria
CEM	Common Methodology for Information Technology Security, document describing the methodology used in Common Criteria evaluations
FIPS	FIPS Federal Information Processing Standard
ITSEF	IT Security Evaluation Facility, test laboratory licensed to operate within a evaluation and certification scheme
PP	Protection Profile
SFR	Security Functional Requirements
ST	Security Target, document containing security requirements and specifications , used as the basis of a TOE evaluation
TOE	Target of Evaluation
TSF	TOE Security Functions

12 Bibliography

ST	ArcSight Logger 7.3.0.8511.8 Security Target, OpenText Corporation, 2026-02-10, version 0.11
CC/CEM	Common Criteria for Information Technology Security Evaluation, CC:2022, revision 1, parts 1-5, November 2022, and Common Methodology for Information Technology Security Evaluation, CEM:2022, revision 1, November 2022
AGD	ArcSight Logger 7.3.8 Operational User Guidance and Preparative Procedures Supplement (AGD_OPE and AGD_PRE), OpenText, 2025-09-09, document Version

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
2.6.1.	2025-10-16	None.
2.6	Application	Original version

A.2 Scheme Notes

Scheme Note	Version	Title	Applicability
SN-15	5.0	Testing	Compliant
SN-18	4.0	Highlighted Requirements on ST	Compliant
SN-22	4.0	Vulnerability assessment	Compliant
SN-25	2.0	Use of CAVP-tests in CC evaluation	Compliant
SN-27	1.0	ST requirements at the time of application	Compliant
SN-28	2.0	Updated procedures	Compliant
SN-31	1.0	New procedures for site-visit/testing oversight	Compliant