Certification Report

ArcSight Enterprise Security Manager (ESM) 7.6.6.18296.0

Sponsor and developer: ***Open Text Corporation***
275 Frank Tompa Drive
Waterloo, ON, N2L 0A1
Canada

Evaluation facility: ***SGS Brightsight B.V.***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number:	**NSCIB-CC-2300078-01-CR**
Report version:	**1**
Project number:	**NSCIB-2300078-01**
Author(s):	**Brian Smithson**
Date:	**19 January 2026**
Number of pages:	**11**
Number of appendices:	**0**

Reproduction of this report is authorised only if the report is reproduced in its entirety.

CONTENTS

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TrustCB B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TrustCB B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TrustCB B.V. to perform Common Criteria evaluations; a significant requirement for such a licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TrustCB B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

Reproduction of this report is authorised only if the report is reproduced in its entirety.

Recognition of the Certificate

Presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the ArcSight Enterprise Security Manager (ESM) 7.6.6.18296.0. The developer of the ArcSight Enterprise Security Manager (ESM) 7.6.6.18296.0 is Open Text Corporation located in Waterloo ON, Canada and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE is ArcSight Enterprise Security Management (ESM) 7.6.6. ArcSight ESM is a Security Information and Event Management (SIEM) solution that combines event correlation and security analytics to identify and prioritize threats in real time and remediate incidents early.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 2026-01-19 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the ArcSight Enterprise Security Manager (ESM) 7.6.6.18296.0, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the ArcSight Enterprise Security Manager (ESM) 7.6.6.18296.0 are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]* [1] for this product provide sufficient evidence that the TOE meets the EAL3: augmented (EAL3+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_FLR.3 (Systematic flaw remediation).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CC]* (Parts I, II and III).

TrustCB B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. Note that the certification results apply only to the specific version of the product as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the ArcSight Enterprise Security Manager (ESM) 7.6.6.18296.0 from Open Text Corporation located in Waterloo ON, Canada.

The TOE is composed of the following main components:

Delivery item type	Identifier	Version
Hardware	N/A	N/A
Software	ArcSight Console	7.6.6.0.18303.0
	ArcSight Command Center	7.6.6.18296.0
	Manager	7.6.6.18296.0
	Correlation Engine	7.6.6.18296.0

To ensure secure usage a set of guidance documents is provided, together with the ArcSight Enterprise Security Manager (ESM) 7.6.6.18296.0. For details, see section 2.5 “Documentation” of this report.

2.2 Security Policy

The TOE implements the following security policy:

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.

User Data Protection

The TOE provides a mechanism to segment access control and enable security attributes for access controls.

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.

Security Management

The TOE provides administrators with the capabilities to configure, monitor and manage the TOE. 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.

TOE Access

The TOE provides a mechanism to automatically lock access and require re-authentication prior to reenabling access.

Protection of the TSF

The TOE provides protected communications between the parts of the TOE. The TOE supports TLS v1.2 as configured by the Administrator. The data is protected from modification and disclosure.

Trusted Path / Channels

The TOE provides trusted channels between itself and external components (connectors) from disclosure and modification via HTTPS/TLS. The Trusted path is established (via HTTPS/TLS) for initial authentication and subsequent actions. The use of HTTPS/TLS protects communications from disclosure or modification.

Incident Management

The TOE provides Incident Management functions provide the capability to analyze security event data and incident workflow and alert. Audit data is 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.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.2 of the *[ST]*.

2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

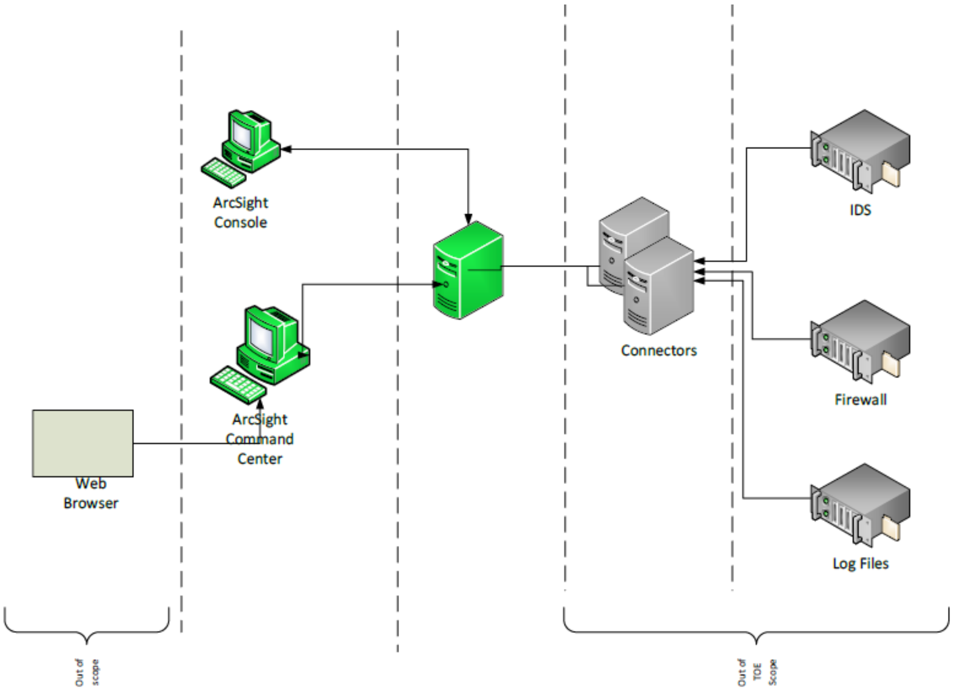
2.4 Architectural Information

ArcSight ESM is an enterprise network tool. It requires ArcSight SmartConnectors to gather events from the network and normalize them into a standard scheme for correlation. SmartConnectors are not within the scope of this evaluation.

The TOE consists of the following components:

- Manager
- CORR-Engine (Correlation Optimized Retention and Retrieval Engine)
- ArcSight Console
- ArcSight Command Center (ACC)

The basic configuration is depicted in the figure below:



2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version
ArcSight ESM Operational User Guidance and Preparative Procedures Supplement (AGD-IGS)	V0.14, 11 December 2025

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

The developer provided test documentation which describes the test strategy as follows:

- Each SFR is mapped to one or a subset of tests.
- Different tests use different TSFIs to perform the test and this is manifested in the test procedure.

This demonstrates all the SFRs (and therefore TSFIs and subsystems) are covered by the developer test cases.

The repeated tests are selected based on:

- The functionality of the tests. Such as testing on managing correlation rules and managing security incidents.
- How much security relevant they are. Such as audit record protection from delete and modification.

Four (4) developer tests were repeated..

2.6.2 Independent penetration testing

The evaluator has analyzed the developer test plan against the SFRs and based on the completeness of the tests the evaluator test plan is devised. Independent tests are chosen to cover:

- AGD_PRE.1.2 requirements.
- Negative test cases, such as tests that a non-administrator user performs activities that need administrators privileges.
- Communication related SFRs such as:
  - TLS for communication between ESM (command center) and Web browser (admin).
  - TLS for communication between ESM and SmartConnector.
- Verify secure initialization.
- Nessus/NMAP scan.

Fifteen (15) independent tests were devised and performed.

To identify potential vulnerabilities the evaluator performed the following activities:

- SFR design analysis: SFR implementation details were examined in the SFR design analysis. During this examination potential vulnerabilities were identified.
- CWE vulnerability focus: Using the CWE weaknesses collection, the evaluator collected a list of security questions and related answers. This approach ensured that the evaluator was forced to think in terms of vulnerabilities from all different angles and improved completeness in the vulnerability analysis. Also during this examination several potential vulnerabilities were identified.

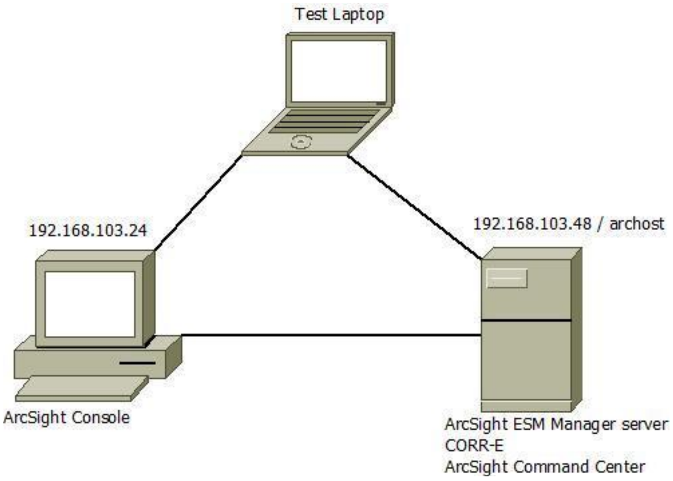
- Use of Scanning tools: The evaluator runs vulnerability scanning tools to identify potential vulnerabilities
- Public vulnerability search: Several additional potential vulnerabilities were identified during a search in the public domain.

Ten (10) penetration tests were devised and performed.

The evaluator performed all the tests (independent tests and penetration tests) in the period between 12 March 2024 and 13 May 2024, and then from 01 December 2025 to 11 December 2025, with 140 hours of effort in total for testing and reporting. All of the test effort was on the logical tests.

2.6.3 Test configuration

The test configuration is shown in the following figure:



The TOE component is as follows:

- ArcSight ESM Manager server, CORR-E, ArcSight Command Center: v7.6.6.18296.0 with patch 25.2, running on RHEL 8.10
- ArcSight ESM Console: v7.6.6.0.18303.0 running on RHEL 8.10

2.6.4 Test results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

The algorithmic security level of cryptographic functionality has not been rated in this certification process, but the current consensus on the algorithmic security level in the open domain, i.e., from the current best cryptanalytic attacks published, has been taken into account.

The TOE is vulnerable to the following public domain vulnerabilities:

- CVE-2025-8997 / EUVD-2025-25660
- CVE-2025-3478 / EUVD-2025025074
- CVE-2024-0967

However, the evaluator assessed the attack potential to exploit the TOE using these vulnerabilities above the required attack potential of AVA_VAN.2. Therefore, the evaluator concluded these are residual vulnerabilities.

2.7 Reused Evaluation Results

There is no reuse of evaluation results in this certification.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number ArcSight Enterprise Security Manager (ESM) 7.6.6.18296.0.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents.

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the ArcSight Enterprise Security Manager (ESM) 7.6.6.18296.0, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 3 augmented with ALC_FLR.3**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 "Documentation" contains necessary information about the usage of the TOE.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. For the evolution of attack methods and techniques to be covered, the customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: <*none*>, which are out of scope as there are no security claims relating to these.

3 Security Target

The ArcSight Enterprise Security Manager (ESM) 7.6.6 Security Target, v1.29, 11 December 2025 *[ST]* is included here by reference.

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
RHEL	Red Hat Enterprise Linux
TOE	Target of Evaluation

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report.

[CC] Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017

[CEM] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017

[ETR] Evaluation Technical Report “ArcSight Enterprise Security Manager (ESM) 7.6.6” – EAL3+, 23-RPT-771, v3.0, 22 December 2025

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022

[ST] ArcSight Enterprise Security Manager (ESM) 7.6.6 Security Target, v1.29, 11 December 2025

(This is the end of this report.)