CERTIFICATION REPORT
issued by an
Accredited Certification Body

Ackred. nr 1914
Produktcertifiering
ISO/IEC 17065

Ref. No/Order No
CAB-260408-140202-276

Unit/Issued by	Date	Distribution
IQTR / Anders Staaf	2026-04-27	Public
Unit/Appoint	Classification	
IQTR / Peter Döös	Unclassified	

Subject

Certification Report OpenText ArcMC 3.2.5 and Connectors 8.5.1

Version number	File name	Product name	Sponsor
1.0	CR OpenText ArcMC and Connectors v1.0.pdf	ArcSight Management Center 3.2.5 and SmartConnectors 8.5.1	OpenText
ITSEF	**Reviewed by**	**Certification body**	**Certification ID**
COMBITECH	David Carlysle	Combitech	CAB2026001

Contents

1 Executive Summary

Certification id	CAB2026001
TOE identification	ArcSight Management Center 3.2.5 and SmartConnectors 8.5.1
Security Target identification	ArcSight Management Center 3.2.5 and SmartConnectors 8.5.1 Security Target, version 0.18, 2026-04-13
Assurance package	EAL3 augmented with ALC_FLR.3
Assurance level	Substantial, AVA_VAN.2
Protection Profile	N/A
Sponsor	OpenText Inc.
Developer	OpenText Inc.
ITSEF	Combitech EC/ITSEF
Certification Body	Combitech Certification Center
National Cybersecurity Certification Authority	FMV/ICC
Evaluation completion date	2026-04-13
Final Evaluation Report	Final Evaluation Report – OpenText ArcSight Management Centre (ArcMC) 3.2.5 and SmartConnectors 8.5.1, version 1.2, 2026-04-13, CAB-260330-153704-169:002, Combitech AB
Common Criteria version	CC:2022, Revision 1
CEM version	CEM:2022, Revision 1
Scheme version	Combitech EUCC Certification and Evaluation Scheme, v1.3
Recognition Scope	EUCC, CCRA, EA/MLA
Certification date	2026-04-27
Certificate validity	5 years from certification date

2 Certified ICT Product

The TOE is ArcSight Management Center 3.2.5 and SmartConnectors 8.5.1 from OpenText Inc.

Component	Support	Operating Environment
ArcSight Management Center 3.2.5	Tested	Red Hat Enterprise Linux (RHEL) 9.2,8.8,7.9.
	Supported	Rocky Linux 9.2, 8.8
SmartConnector 8.5.1	Tested	RHEL 8.6 and 9.2 Rocky Linux 8.9 CentOS Linux 7.9 Oracle Solaris 11, 64-bit MS Windows Server 2022 Standard 64-bit SUSE Linux Enterprise Server (SLES) 15 SP 5
	Supported	CentOS Linux 8.x and 7.x 64-bit RHEL 9.x, 8.x and 7.x 64 bit MS Windows Server 2022 Standard 64 bit MS Windows Server 2019 Standard 64 bit MS Windows Server 2016 Standard 64 bit MS Windows Server 2012 R2 Standard 64 bit Oracle Solaris 11, 64 bit (SPARC) Oracle Solaris 10, 64 bit (SPARC) Oracle Solaris 11, 64 bit (x86_64) SUSE Linux Enterprise Server 15 SP 3, 15 SP2, 15 SP1, 15, 12 SP2 and 11 64-bit

Table 1, Requirements on the operating environment

3 Security Policy

3.1 Security Services

Security Audit

The TOE is able to generate and store audit records of security relevant events. The stored audit records are protected from unauthorized modification and deletion. Audit records generated by the TOE can be viewed only by users in the System Admin roles. The TOE provides the authorized roles with capabilities to review the generated audit records, including capabilities for selecting audit records based on date and time range and, optionally, subject identity and outcome, and ordering the selected records based on date and time, the subject associated with the audit event, and the type of audit event. The stored audit records are protected from unauthorized modification and deletion. Reliable time is provided by the operational environment.

Cryptographic Support

Cryptography for TLS connections is supplied by the operational environment by a FIPS 140-2 certified crypto module. Communications between the TOE and trusted IT entities are protected by TLS v1.2. Format preserving encryption is provided for data encryption by the crypto module. A trusted path protected by HTTPS is provided between the TOA and a web browser for the administrative GUI.

Protection of the TSF

Communications between distributed components of the TOE occur over TLS v1.2 provided by a FIPS 140-2 certified crypto module in the operational environment, which provides confidentiality and integrity of transmitted data over the trusted channel.

Identification and Authentication

The TOE maintains accounts of the authorized users of the system. The user account includes the following attributes associated with the user: user identity; authentication data; authorizations (groups or roles); and e-mail address information. The TOE enforces restrictions on password structure, including minimum length and minimum number of different character types (i.e., alphabetic, numeric, special). The TOE requires users to provide unique identification and authentication data before any administrative access to the TOE is granted.

Security Management

The TOE provides authorized users with privileges to configure and manage the TOE security functions and TSF data. Authorized users may configure user authentication data and configuration settings and also:

- create users
- query users
- delete users
- define network settings
- review audit logs.

TOE Access

The TOE will terminate interactive sessions after a period of inactivity configurable by an authorized user. The TOE also allows user-initiated termination of the user's own interactive session by explicitly logging off.

3.2 Vulnerability Management Policy

The following vulnerability and patch management policies has been identified as applicable to the TOE.

The developer identified measures in place, including:

Reporting a Security Vulnerability

OpenText reviews all reports of security vulnerabilities affecting OpenText products and services. Customers can report a vulnerability in one of the products or solutions by contacting Customer Support with details of the vulnerability.
To report a vulnerability in one of the corporate websites, products, or services, security@opentext.com is used for the details. For critical issues, a company PGP key can be used to encrypt the details of the disclosure. Users can also report flaws through the web at https://opentext.com/support. This is the OpenText preferred method. An alternate method to report a flaw is to call support at 1-800-499-6545.

Tracking a Security Vulnerability

All security flaws are tracked in a professional tool, ValueEdge, with

- Name
- Description – includes actual versus expected results and steps to reproduce
- Product – selection list to identify the product
- Detected in Release – selection list to identify the version where defect was found
- Post Release – Yes/No to identify if an escaped defect in a released version
- Severity – selection list of Critical, High, Medium, Low based on CVSS score
- Security Impact – selection list of Yes, No, Unknown

Resolving Issues: Normally, Security Issues must be resolved within the following timelines, resolved meaning available to the customers:

Security Severity	Critical	High	Medium	Low
CVSS Score	9.0-10.0	7.0-8.9	4.0-6.9	0.0-3.9
Time to Resolution	30 days	30 days	90 days	180 days

Triage and Planning

It is determined whether the security flaw is legitimate and requires mitigation. This is done within seven days for customer-encountered defects. If legitimate a mitigation is planned.

Implementation and Testing

When a mitigation is determined and coded, the mitigation is tested for functionality by a QA team. It is also scanned for vulnerabilities to ascertain that it is flaw free. Changes are managed through formal change control and follow the EUCC process for changes to a certified ICT product.

Release

Fixes can be made available to customer through a new product release, a patch release, or with a hot fix depending on severity. Patches and Hot Fixes are published and available to all customers. Customer Support will provide Hot Fixes to a customer when requested and as appropriate.

The vulnerability management is considered to follow the guidelines in [EUCC Vuln].

3.3 Assurance Continuity Policy

This is a new product certification. An assurance continuity policy was not provided.

4 Assumptions and Clarification of Scope

4.1 Assumptions

The following assumption on the TOE operational environment are made.

ASSUMPTION	DESCRIPTION
A.AUDIT_PROTECT	The Audit data is protected from modification and disclosure.
A.HTTPS	HTTPS using TLS is used to access the TOE. The TOE uses environment Crypto to communicate with parts of the TOE and trusted IT products.
A.LOCATE	The processing platforms on which the TOE resides are assumed to be located within a facility that provides controlled access.
A.MANAGE	Privileged users (Administrators and Users) 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	Privileged users (Administrators, Users) of the TOE, are not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the TOE documentation. Privileged Users (Administrators and Users) will not leave their systems unattended and unlocked.
A.TIMESOURCE	The TOE has a trusted source for system time via the OS.
A.UPDATE	The TOE environment is patched by the administrator as patches are available to minimize the effects of vulnerabilities that may arise.

Table 2, Assumptions

The user guidance as outlined in [ST] section 1.7.8 contains necessary information about the usage of the TOE and its configuration in the environment to fulfil all Assumptions and Objectives for the operational environment described in the [ST]. Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE.

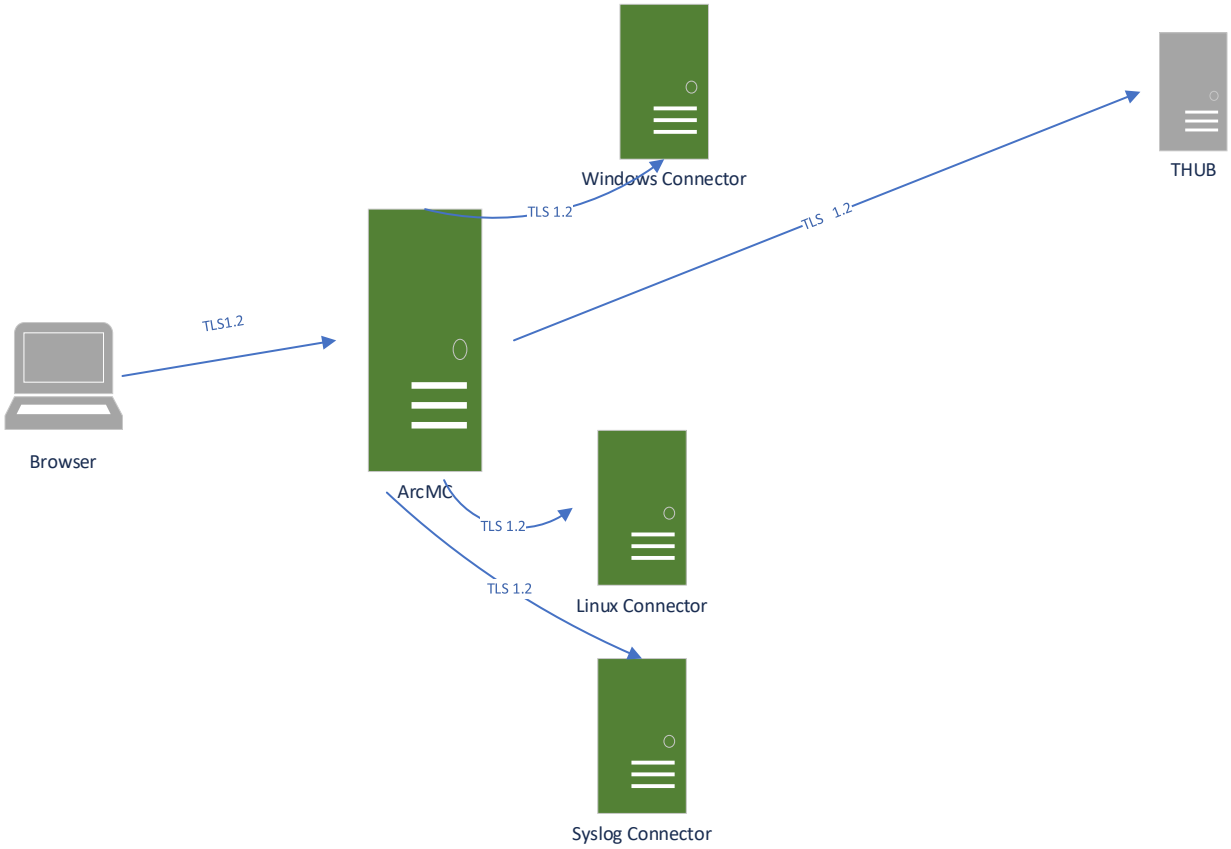
All threats identified in the Security Target, [ST] section 3.1 have been countered by the evaluated security functions of the TOE.

4.2 Clarification of Scope

Supported functionality excluded from the evaluated configuration is Hadoop functionality.

5 Architectural Information

The TOE consists of the components ArcSight Management Center 3.2.5 and SmartConnectors 8.5.1 and is dependent on the software component Transformation Hub, THUB, in the environment for its operation.



Arcsight Management Center (ArcMC) is a centralized management tool that simplifies security policy configuration, deployment maintenance, and monitoring in an efficient and cost-effective manner. ArcMC offers these key capabilities:

- Management and Monitoring: deliver the single management interface to administrate and monitor ArcSight managed nodes, such as Connector Appliances, Loggers, Connectors, Collectors, other ArcMCs, and Transformation Hub.
- SmartConnector Hosting: for the hardware appliance, as a platform to host and execute SmartConnectors ArcMC includes these benefits:
    - Rapid implementation of new and updated security policies. l Increased level of accuracy and reduction of errors in configuration of managed nodes
    - Reduction in operational expenses.

Note that individual SmartConnectors run only on the platforms that are useful for the connector type and specific device type. For example, the SmartConnector for Microsoft Windows Event Log runs on Windows platforms only. Each SmartConnector has its own

specific configuration guide that provides connector-specific platform requirements and installation information.
SmartConnectors can:

- Collect all the data from a source device, which eliminates the need to return to the device during an investigation or audit.
- Parse individual events and normalize event values such as severity, priority, and time zone into a common schema (format) for use by other products.
- Filter out data that is not needed for analysis, thus saving network bandwidth and storage space (optional).
- Filter and aggregate events to reduce the volume sent to the Manager, ArcSight Logger, or other destinations, which reduces event processing time and increases efficiency of ArcSight.
- Categorize events by using a common, human-readable format, saving time, and making it easier to use the event categories to build filters, rules, reports, and data monitors.
- Add device and event information to it to complete the message and send it to the configured destination.

The communication between TOE parts internally and communication to other trusted IT components in the environment is protected by TLS v1.2. Communication with the web browser used for administration of the TOE is protected by HTTPS/TLS v1.2. The TOE relies on FIPS 140-2 certified crypto components in the environment.

6 Supplementary Cybersecurity Information

The Sponsor and Developer web site is reached at:
https://www.opentext.com/

7 TOE Evaluation and Configuration

The TOE was evaluated according to Common Criteria, CC:2022, and Common Methodology, CEM:2022, [CCpart1], [CCpart2], [CCpart3], [CCpart4], [CCpart5], and [CEM].

No protection profile was claimed. No EUCC state-of-the-art documents were used for this evaluation.

The evaluation was done according to EAL3 augmented with ALC_FLR.3.

The assessment classifications used during this evaluation are: PASS, FAIL, and INCONCLUSIVE which have been drawn from [CEM]. In addition, the classification REMARK has been used. REMARK is used for errors that are not judged serious enough to cause the work unit to receive a FAIL verdict.

The overall result of the evaluation is Pass with remark[1]. The following assurance components was used.

Assurance Components	Action Element	Verdict
ASE_INT.1		Pass with remark
	ASE_INT.1.1E	Pass with remark
	ASE_INT.1.2E	Pass with remark
ASE_CCL.1		Pass
	ASE_CCL.1.1E	Pass
ASE_SPD.1		Pass
	ASE_SPD.1.1E	Pass
ASE_OBJ.2		Pass
	ASE_OBJ.2.1E	Pass
ASE_ECD.1		Pass
	ASE_ECD.1.1E	Pass
	ASE_ECD.1.2E	Pass
ASE_REQ.2		Pass with remark
	ASE_REQ.2.1E	Pass with remark
ASE_TSS.1		Pass
	ASE_TSS.1.1E	Pass
	ASE_TSS.1.2E	Pass
ALC_CMC.3		Pass
	ALC_CMC.3.1E	Pass
ALC_CMS.3		Pass
	ALC_CMS.3.1E	Pass
ALC_DEL.1		Pass
	ALC_DEL.1.1E	Pass
ALC_DVS.1		Pass
	ALC_DVS.1.1E	Pass
	ALC_DVS.1.2E	Pass
ALC_LCD.1		Pass
	ALC_LCD.1.1E	Pass
ALC_FLR.3		Pass
	ALC_FLR.3.1E	Pass
ADV_ARC.1		Pass
	ADV_ARC.1.1E	Pass

[1] See chapter 9 *Comments and Recommendations*

Assurance Components	Action Element	Verdict
ADV_FSP.3		Pass
	ADV_FSP.3.1E	Pass
	ADV_FSP.3.2E	Pass
ADV_TDS.2		Pass
	ADV_TDS.2.1E	Pass
	ADV_TDS.2.2E	Pass
AGD_OPE.1		Pass
	AGD_OPE.1.1E	Pass
AGD_PRE.1		Pass
	AGD_PRE.1.1E	Pass
	AGD_PRE.1.2E	Pass
ATE_COV.2		Pass
	ATE_COV.2.1E	Pass
ATE_DPT.1		Pass
	ATE_DPT.1.1E	Pass
ATE_FUN.1		Pass
	ATE_FUN.1.1E	Pass
ATE_IND.2		Pass
	ATE_IND.2.1E	Pass
	ATE_IND.2.2E	Pass
	ATE_IND.2.3E	Pass
AVA_VAN.2		Pass
	AVA_VAN.2.1E	Pass
	AVA_VAN.2.2E	Pass
	AVA_VAN.2.3E	Pass
	AVA_VAN.2.4E	Pass

Table 3, Assurance components and evaluation verdict

7.1 Testing

Both the developer's and the evaluator's independent tests were performed on a configuration similar with the configuration described in chapter 5.

7.1.1 Developer Testing

The developer testing effort covered all security related external interfaces, TSFIs, and all Security Functional Requirements, SFRs, stated in the [ST]. The test approach,

configuration, coverage, depth, and results are described in the developer's Test Plan and Coverage Analysis.

All developer tests are in the form of test cases to be followed through steps which specify interactions with the browser interface and Wireshark commands.

The actual results from each test step are compared with the expected results specified.

The developer testing was done between the 28th of February 2026.

All developer tests results were Pass.

7.1.2 Evaluator Independent Testing

Testing was performed on the TSFIs and all SFRs. All tests had a pass result.

The tests were divided into the following test groups:

- **Test Group 1 Installation**
  TOE Installation, verification of installation and configuration of the TOE as stated in the user guidance.
- **Test Group 2 Re-testing of developer tests**
  Re-run of a chosen subset of developer tests, a number of developer tests were sampled and re-tested by the evaluator. This activity was performed as part of the assessment of the developer test effort and test accuracy.
- **Test Group 3 Evaluator devised tests**
  Tests devised by the evaluator with the purpose to broaden the test coverage.
- **Test Group 4 Vulnerability scanning**
  Tests that complements the vulnerability assessment, this activity comprises mainly of vulnerability scanning, assessment of exposed services etc.

Each test case contained descriptions of the test steps, expected result of each test step, and if the test met this expected result or not. Additional evidence of the test steps and result was reported under each test case's table of test execution description.

8 Result of the Evaluation

The certificate for Common Criteria Certificate OpenText ArcSight Management Center 3.2.5 and SmartConnectors 8.5.1 was issued 2026-04-27. The certificate is valid for a maximum of five years but can be changed over time. For information regarding the current status of the certificate, please contact Combitech, Ljungadalsgatan 2B, Växjö, //www.combitech.com/certificationcenter.

9 Comments and Recommendations

The definition of TSF data, user data, user roles and permissions in the [ST] could be improved further on. The evaluator does not deem the observation severe enough to judge the work unit as inconclusive or failed, but resulted in the work unit receiving a pass with remark verdict

10 Security Target

The evaluate Security Target is: ArcSight Management Center 3.2.5 and SmartConnectors 8.5.1 Security Target, revision 0.18, 2026-04-13.

11 Scheme Mark and Label

EU CC Common Criteria
CYBERSECURITY CERTIFICATION

HIGH
SUBSTANTIAL
BASIC

AVA_VAN.2, Combitech EUCC Certification and Evaluation Scheme, Combitech Certification Center, 2026-04-27, CAB2026001

12 Glossary

CCRA	Common Criteria Recognition Arrangement
EA/MLA	European Accreditation Multilateral Agreement
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
PGP	Pretty Good Privacy
TLS	Transport Layer Security

13 References

[CCpart1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, version CC:2022, revision 1, November 2022, CCMB-2022-11-001

[CCpart2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, version CC:2022, revision 1, November 2022, CCMB-2022-11-002
[CCpart3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, version CC:2022, revision 1, November 2022, CCMB-2022-11-003
[CCpart4]	Common Criteria for Information Technology Security Evaluation, Part 4: Framework for the specification of evaluation methods and activities, version CC:2022, revision 1, November 2022, CCMB-2022-11-004
[CCpart5]	Common Criteria for Information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements, version CC:2022, revision 1, November 2022, CCMB-2022-11-005
[ISO]	ISO/IEC 15408:2022, Fourth edition, 2022-08
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation methodology, version CEM:2022, Revision 1, November 2022, CCMB-2022-11-006
[ERR]	Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), version 1.2, 2025-10-15
[CSA]	Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)
[EUCC]	Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC)
[EUCC-amd-1]	Commission Implementing Regulation (EU) 2024/3144 of 18 December 2024 amending Implementing Regulation (EU) 2024/482 as regards applicable international standards and correcting that Implementing Regulation
[EUCC-amd-2]	Commission Implementing Regulation (EU) 2025/2462 of 8 December 2025 amending Implementing Regulation (EU) 2024/482 as regards applicable international standards and correcting that Implementing Regulation
[EUCC Vuln]	EUCC Scheme GUIDELINES on Vulnerability Management and Disclosure, Version 1.1, January 2025
[STAFS]	2020:1, Styrelsens för ackreditering och teknisk kontroll (SWEDAC) föreskrifter och allmänna råd om ackreditering
[QM]	Quality Manual 17065, issue 1.3, CAB-23-8937-8630-87-00, Combitech AB

[FER]	Final Evaluation Report – OpenText ArcSight Management Centre (ArcMC) 3.2.5 and SmartConnectors 8.5.1, version 1.2, 2026-04-13, CAB-260330-153704-169, Combitech AB
[AGD]	ArcSight Management Center 3.2.5 and SmartConnectors 8.5.1 Operational User Guidance and Preparative Procedures Supplement (AGD-IGS), version 0.8, 2026-03-10, OpenText
[INSTALL]	ArcSight SmartConnectors, Software Version: CE 25.1, SmartConnector Installation and User Guide, February 2025, OpenText
[ADMIN]	Micro Focus Arcsight Management Center Software Version: 3.0.0 Administrator's Guide, March 2021, OpenText
[CIL]	ArcSight Management Center 3.2.5 and SmartConnectors 8.5.1 Configuration Management Processes & Procedures (ALC_CM), version 0.14, 2026-04-13, OpenText