Ärendetyp 5.3 Diarienummer: 23FMV1756-25

Dokument ID CSEC2023004

CSEC

Swedish Certification Body for IT Security

Certification Report Vectra Platform

Issue: 1.0, 2026-feb-11

Authorisation: Theodora Arvanitidis, Junior Certifier , CSEC

SWEDAC ACKREDITERING

Accred. no. 1917
Certification of
Products
ISO/IEC 17065

Table of Contents

1 Executive Summary

The Target of Evaluation (TOE) is a threat detection platform categorized as a Network Detection and Response (NDR) platform.

The Vectra Platform release 9.3.0-13-36 deployment consists of two main components, i.e., Vectra Brain and Vectra Sensor. Both of the components can be deployed either in a data center or a cloud environment. Only the data center deployment scenario is included in the evaluated configuration.

The Security Target [ST] claims conformance to Common Criteria security functional components, extended and conformant, version 3.1 revision 5. The [ST] claims the assurance level EAL2 augmented with ALC_FLR.1.

There are seven assumptions being made in the ST regarding the secure usage and the operational environment of the TOE. The TOE relies on these to counter the three threats and comply with the four organisational security policy (OSP) in the ST.

The assumptions, threats, and the OSP are described in chapter 3 Security Problem Definition and chapter 4 Security Objectives.

The evaluation has been performed by atsec information security AB and was completed in 2026-01-27. The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1, revision 5.

atsec information security AB is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. atsec information security AB is also accredited by the Swedish accreditation body SWEDAC according to ISO/IEC 17025 for Common Criteria evaluation.

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].

The technical information in this report is based on the Security Target and the Final Evaluation Report (FER) produced by atsec information security 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	CSEC2023004
Name and version of the certified IT product	Vectra Platform Release 9.3.0-13-36
Security Target Identification	Vectra Platform Security Target, Vectra AI Inc., 21-November-2025, version 1.27
EAL	EAL2 augmented with ALC_FLR.1
Sponsor	Vectra AI Inc.
Developer	Vectra AI Inc.
ITSEF	atsec information security AB
Common Criteria version	3.1 revision 5
CEM version	3.1 revision 5
QMS version	2.6.1
Scheme Notes Release	22.0
Recognition Scope	CCRA, SOG-IS, EA-MLA
Certification date	2026-02-11

3 Security Policy

The TOE provides the following security features:

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Channels

3.1 Security Audit

The TOE provides extensive auditing capabilities, by generating a comprehensive set of audit logs that identify specific TOE operations. For each event, the TOE records the date and time of each event, the type of event, the subject identity, and the outcome of the event. The audit logs are stored locally and can be sent out over syslog to an external system like a SIEM.

3.2 Cryptographic Support

The TOE provides cryptography in support of remote administrative management via SSH and TLS/HTTPS. TOE components communicate with each other using SSH. Vectra Brain utilizes file integrity checking during boot where it verifies cryptographic checksums of critical system files against the known expected values. If verification succeeds the system proceeds to decrypt the encrypted file system and continue the boot process normally to enter operational mode. If the verification fails, the boot process is halted with error message, and the application code remains encrypted.

Vectra Sensor does not utilize Secure Boot, as it is considered an untrusted asset. Instead, it performs a file system integrity check as part of the Ubuntu operating system to verify the absence of file system or hardware corruption. If a file system integrity issue is discovered, it will run a File System Integrity repair attempt automatically. If it is successful it will boot, if not it will not. If there is Hardware corruption, it will fail to boot.

3.3 Identification and Authentication

The TOE provides authentication services for local and remote users wishing to connect to the TOEs secure Web UI or REST API administrator interfaces. The TOE requires authorized administrators to authenticate prior to being granted access to any of the management functionality. After successful authentication, the TOE determines the permitted level of access for a user based on the local authorization setting for that user and provides role-based access (RBAC).

3.4 Security Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either through a secure SSH or TLS/HTTPS session. The TOE supports various administrator roles out of the box and custom roles can be created as needed, but only the Super Admin role has a user defined out of the box.

3.5 Protection of the TSF

The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls to limit configuration to only authorized administrators.

3.6 TOE Access

Administrative interfaces present a configurable access banner before authentication. The banner is shown on all interactive connections and provides the organization’s required warning or advisory notice.

3.7 Trusted Channels

The TOE provides trusted channel between the Sensors and the Brain (encrypted, authenticated over SSH). The TOE also provides trusted channels on remote administrative management via SSH and TLS/HTTPS. SSHv2 and TLS 1.2 and TLS 1.3 are supported.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

The Security Target [ST] makes seven assumptions on the usage and the operational environment of the TOE.

A.NETWORK

There will be a network that supports communication between instances of the TOE and between the TOE and IT systems used to manage the TOE. This network functions properly.

A.NOGENPURP

There are no general-purpose computing capabilities (e.g., compilers or applications) available on the TOE, other than those services necessary for the operation, administration, and support of the TOE.

A.PHYSICAL

The TOE shall presumably be located in physically secure environment that can be accessed only by the authorized administrators.

A.TRUSTADMIN

The administrators of the TOE shall not have any malicious intention, shall receive proper training on the TOE management, and shall follow the administrator guidelines.

A.TIME

It is assumed that the Operational Environment provides the TOE with reliable time

A.KEYS

It is assumed that random bits provided by the underlying platform are of good quality and have sufficient entropy.

A.SYSLOG_PROTECTION

It is assumed that the Operational Environment ensures the confidentiality and integrity of audit data transmitted from the TOE to external Syslog servers through secure network configurations and mechanisms.

4.2 Clarification of Scope

The Security Target contains three threats, which have been considered during the evaluation.

T.UNAUTHORIZE DACCESS

Threat agents may attempt to gain Administrator access to the TOE by nefarious means such as masquerading as an Administrator to the TOE, masquerading as the TOE to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the TOE.

T.HACKACCESS

An attacker may get undetected system access to the TOE. The attacker may use hacking methods to exploit access control in the TOE.

T.MALFUNCTION

The TOE may malfunction that may compromise information and data processing, implying risk of data exploiting. The attacker may get unauthorized access to TOE resources. The TOE may malfunction that may compromise roles and permissions, implying risk of data exploiting. An administrator may gain unauthorized roles and permissions in TOE.

The Security Target contains four Organisational Security Policy (OSP), which have been considered during the evaluation.

P.ACCOUNTABILITY

The authorized administrators of the TOE shall be held accountable for their actions.

P.ADMINACCESS

An authorized administrator must manage the TOE securely.

P.DETECT

To trace all security-related responsibilities, security-related events shall be documented, maintained, and analyzed, and such records can be checked.

P.M2MSECURE

The TOE shall ensure that all machine-to-machine communication between the Sensor and Brain is secure, authenticated, and encrypted to protect the confidentiality and integrity of transmitted data.

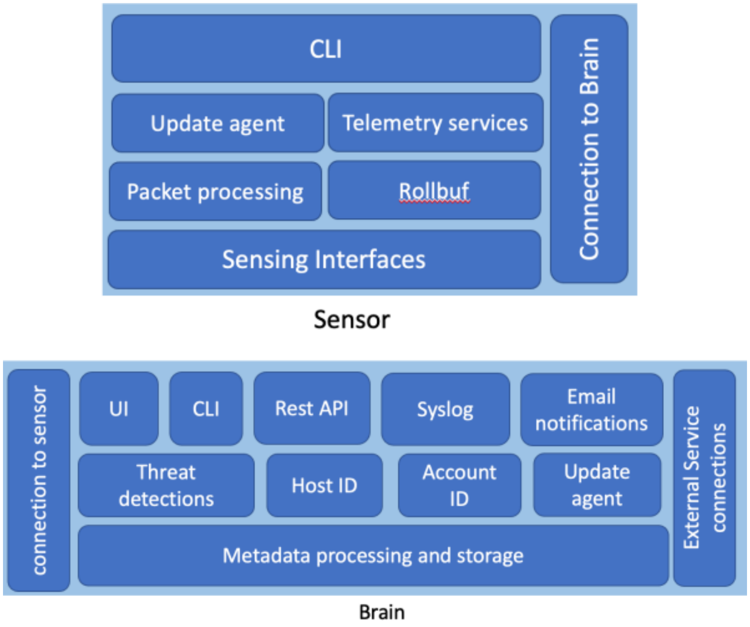
5 Architectural Information

The TOE is separated into two components, Vectra Brain and Vectra Sensor, in the form of virtual SW component deployed on Virtual Machines. The Brain is where all the algorithms are executed to detect and prioritize threats using AI, as well as interfaces to send the data out in syslog, email, or API. The Brain has a management interface over which it communicates with the Sensors, receives software updates, and provides Web UI and REST API access. The Web UI and the REST API are used to manage the TOE and to view the surfaced threats and take action. The Sensors can be physical, virtual (deployed on ESXi, KVM or Hyper-V) and cloud (deployed in the customer's AWS, Azure or GCP environments). Only the virtual Sensor deployment (on ESXi, KVM or Hyper-V) will be in the scope of the evaluation.

The TOE implements and supports the following network protocols: HTTPS, SSH and TLS (client and server). The TOE uses SSH to provide the trusted path (with protection from disclosure and detection of modification) for all local administration sessions. The Brain uses TLS/HTTPS to provide the trusted path (with protection from disclosure and detection of modification) for all remote administration sessions. The TOE includes OpenSSL 1.1.1f-1ubuntu2.24 which is used for the TLS implementation and underlying cryptographic operations for OpenSSH 8.2p1-4ubuntu0.13 which is used for SSH.

The TOE is divided into the following subsystems:

- CLI,
- Updated agent,
- Telemetry services,
- Packet processing,
- Rollbuf,
- Sensing Interfaces,
- Connection to Brain,
- Connection to Sensor,
- User interface (UI),
- Rest API,
- Syslog,
- Email notifications,
- Threat detection,
- Host ID,
- Account ID,
- Update agent,
- External Service connections,
- Metadata processing and storage.



Vectra Platform

6 Documentation

The TOE includes the following supporting documents:

- Vectra_AGD_v1.5.pdf
- Hyper-V vSensor Deployment Guide - 2025_Mar_5.pdf
- KVM vSensor Deployment Guide - 2025_Aug_27.pdf
- Permissions - Feb2025.xlsx
- SSL Certificate Installation - 2025_Nov_11.pdf
- Vectra Quadrant UX Deployment Guide - 2024_Oct_9.pdf
- Vectra_REST_API_Guide_v2.5 - Aug2025.pdf
- VMware Brain Deployment Guide - 2025_Oct_7.pdf
- VMware vSensor Deployment Guide - 2025_Oct_8.pdf

The TOE images can be downloaded from the Vectra Customer Support Portal. The static documentation is available publicly without any restrictions, and static links can be requested for documentation access.

7 IT Product Testing

7.1 Developer Testing

Developer testing was performed on the 9.3.0-13-36 TOE version running on VMWare ESXi. The tests have a reasonable coverage of the TSFI.

The automated integration testing was performed on September 8th, 2025 by Jenkins automation in Vectra’s datacenter in Austin, TX for version 9.3.0-13-36 of Vectra’s software. The manual testing was performed on October 31st 2025 by Oscar Ibatullin at Vectra’s office in San Jose, CA, USA for version 9.3.0-13-36 of Vectra’s software.

7.2 Evaluator Testing

The evaluator re-run a sample of the developer tests on the TOE as part of the and performed 9 evaluator tests to widen the coverage on TSF.

The evaluator also performed additional tests related to Machine-to-machine, Syslog, SSH, NTP, RestAPI, WebGUI, HTTPS and TLS, with a focus on syslog server, RestAPI function management, encrypted channels, Login Caption, User inactivity, User authentication feedback, NTP time handling, SSH communication for machine-to-machine and Audit log capability to make the coverage on TSF broader.

Testing was performed in Stockholm, Sweden, between 24th September 2025 to November 2025

7.3 Penetration Testing

An automated TLS and SSH scanner was used to verify the setup of the TLS service and SSH service. Injection, fuzzing and enumeration was performed on the HTTPS endpoint. Testing was also conducted using negative tests, i.e. that no outputs are expected in the case that no vulnerability was present.

Testing was performed in Stockholm, Sweden, between 24th September 2025 to November 2025

8 Evaluated Configuration

The following configuration specifics apply to the evaluated configuration of the TOE:

- The appliance is in an air-gapped environment
- Brain is in the form of software deployed in the customer data center on a VMware ESXi platform
- Sensor is in the form of software deployed virtually in a customer data center
- SSL certificate is added to the TOE for the TLS communications
- Banners and lockout mechanisms are configured
- Sensor pairing is performed manually
- Updates to the TOE software is to be performed manually

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 Class/Family		Short name	Verdict
Security Target Evaluation		ASE	PASS
	ST Introduction	ASE_INT.1	PASS
	Conformance Claims	ASE_CCL.1	PASS
	Security Objectives	ASE_OBJ.2	PASS
	Extended Components Definition	ASE_ECD.1	PASS
	Security Requirements	ASE_REQ.2	PASS
	Security Problem Definition	ASE_SPD.1	PASS
	TOE Summary Specification	ASE_TSS.1	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
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.1	PASS
Tests		ATE	PASS
	Coverage	ATE_COV.1	PASS
	Functional tests	ATE_FUN.1	PASS
	Independent Testing	ATE_IND.2	PASS
Vulnerablity Assessment		AVA	PASS
	Vulnerability Analysis	AVA_VAN.2	PASS

10 Evaluator Comments and Recommendations

None.

11 Glossary

CC	Common Criteria
CEM	Common Evaluation Methodology
LTM	Local Traffic Manager
PP	Protection Profile
SSH	Secure Shell
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TSF Interface

12 Bibliography

ST Vectra Platform Security Target, Vectra AI Inc., 2025-11-21, version 1.27

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

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

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	2025-03-27	None
2.5.2	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 application, evaluation and Certification