**Swedish Certification Body for IT Security**

# Certification Report - LogPoint™ 6.8.0

**Issue: 1.0, 2021-Feb-17**

*Authorisation: Helén Svensson, Lead Certifier , CSEC*

Table of Contents

# 1 Executive Summary

The Taget of Evaluation (TOE) is LogPoint™ 6.8.0.

The TOE is a Security Information and Event Management (SIEM) system. It is part of an enterprise network and collects and analyses log information from devices on this network.

The TOE receives this log information (referred to as events) and then it is normalized, indexed and stored according to well-defined policies. Alert rules are used to automatically identify and inform users of suspicious activity on the network indicated by analysing the log information. In addition, the TOE provides an extensive forensic capability to enable an authorized user to search for vulnerabilities on the network.

The TOE is a software-only TOE. The TOE can be operated as a single machine or as multiple TOEs in a distributed configuration.

No PP claims are being made.

There are twelve assumptions being made in the ST regarding the secure usage and environment of the TOE. The TOE relies on these to counter the six threats and comply with the five organisational security policies (OSPs) in the ST. The assumptions, threats and OSPs are described in chapter 4 Assumptions and Clarification of Scope.

The evaluation has been performed by atsec information security AB in their premises in Danderyd, Sweden. The evaluation was completed on 2021-02-11. The evaluation was conducted in accordance with the requirements of Common Criteria (CC), version. 3.1 release 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 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 3 augmented by ALC_FLR.1.

| |
|---|
| 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.<br>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 | CSEC2020004 |
| Name and version of the certified IT product | LogPoint™ 6.8.0 |
| Security Target Identification | LogPoint A/S LogPoint™ 6.8.0 Common Criteria EAL3+ Security Target, LogPoint A/S, 21 Septemeber 2020, document version 0.11 |
| EAL | EAL 3 + ALC_FLR.1 |
| Sponsor | LogPoint A/S |
| Developer | LogPoint A/S |
| ITSEF | atsec information security AB |
| Common Criteria version | 3.1 release 5 |
| CEM version | 3.1 release 5 |
| QMS version | 1.24.1 |
| Scheme Notes Release | 17.0 |
| Recognition Scope | CCRA, SOGIS, EA/MLA |
| Certification date | 2021-02-17 |

# 3 Security Policy

The security functional requirements implemented by the TOE are usefully grouped under the following Security Function Classes:

- SIEM
- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- Trusted path/channels

## 3.1 SIEM

Broadly the SIEM security features of LogPoint™ can be described as:

- Data collection
- Data normalization
- Data storage
- Data indexing
- Data enrichment
- Search
- Dashboard
- Alert
- Correlation
- Incident
- Report
- Anomaly (optional as it requires UEBA)

Each of them is described in more detail in the Security Target [ST].

## 3.2 Security Audit

The TOE performs auditing of authentication attempts and administrative actions, and stores these audit data. The TOE audit logs include all of the following: date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event. These audit logs can be reviewed by an authorized user (including sorting audit output). Audit records are protected against unauthorized deletion and modification.

## 3.3 User Data Protection

The TOE uses access control to protect the TOE user data. The TOE user data that is protected is the event data. However, the access control policy also applies to the audit data (TSF data). Identity based access control in the form of user identification and authentication is used to provide access control. The access control policy is described below.

### 3.3.1 Multiple Access Control SFP

The TOE enforces an access control mechanism. TOE access control decisions are made based on the permission information available for a given subject and a given object. When a TOE user requests an operation to be performed on a particular object, the TOE access control determines if the user role has sufficient permission to perform the requested operation on behalf of the requesting user. If sufficient permission is found, the requested operation is performed. Otherwise, the operation is disallowed. An authorized LogPoint administrator can define the specific services for all TOE users. An authorized User

Account administrator can define the specific services for all TOE users in the user groups Operator and Admin.

## 3.4 Identification and Authentication

The TOE requires that the TOE authenticate all TOE users prior to being granted access to the TOE functionality. The TOE can perform the identification and authentication of users, but may also be configured to use an LDAP server (TOE environment) for user authentication.

## 3.5 Security Management

The TOE provides authorized 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. Authorized administrators configure the TOE with the Console via a web-based connection.

There are a number of different roles associated with the TOE. These roles are realized through user groups. A user assumes a specific role by being a member of a specific user group. By default there are two built-in user groups: LogPoint Administrator and User Account Administrator. In order to conform to this Security Target, two additional user groups must be created, based on two built-in permission groups, Admin and Operator. The Admin user group must be created based on the Admin permission group and the Operator user group must be created based on the Operator permission group

## 3.6 Trusted Channels

Whenever the TOE connects to a separate remote TOE for the purpose of transferring event data, the OpenVPN establishes a virtual private network (VPN) for the purpose. This ensures the confidentiality and integrity of TSF Data when it leaves the TOE boundary.

A HTTP connection is also used between TOE and a separate remote TOE to transfer the UUID/Identifier of the client to the server. An UUID is a unique value for each LogPoint installation and created/calculated during the installation of the LogPoint and remain unchanged during the lifetime of the LogPoint. An HTTP connection, which is established inside the VPN tunnel, is used to provide same static tunnel IP address to the OpenVPN client each time it connects to the OpenVPN server.

In regards to OpenVPN configuration and events on client side, as the configuration details (Private IP for VPN tunnel, IP address of Open Door server reachable from DLP and the password) from the VPN server is saved in the Distributed LogPoint, this starts operating as an OpenVPN client. In case of HTTP communication, a python module named “request” acts as HTTP client and initiate HTTP connection to get static tunnel IP address for the OpenVPN session.

Similarly, in regards to OpenVPN configuration and events on the server side, when open door is enabled in the LogPoint, it behaves as an OpenVPN server, listening on UDP port 1194 for OpenVPN connection request from the client. In case of HTTP communication, gunicorn, a python application server, acts as HTTP server and listens on TCP port 18000 for HTTP request. No additional setting needs to be configured for LogPoint to make it listen to the TCP port 18000.

# 4 Assumptions and Clarification of Scope

## 4.1 Assumptions

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

A.MANAGEMENT

It is assumed that LogPoint administrators are trained, qualified, non-hostile and follow all guidance.

A.USERS

It is assumed that authorized users have the authorization to access at least some of the information managed by the TOE and that they act in a cooperating manner.

A.LOCATE

It is assumed that the TOE is physically secure, i.e. no unauthorized persons have physical access to the TOE and its underlying system.

A.FIREWALL

The IT environment shall provide a firewall or other suitable means to protect the TOE from untrusted networks.

A.INTEROPERATIVE

The TOE shall be used in a way that it is interoperable with the network it monitors.

A.TIME

The IT environment shall provide reliable timestamps to the TOE.

A.ENRICHMENT

The IT environment shall provide appropriate data enrichment sources.

A.KEYS

It is assumed that private RSA keys used for the VPN nodes and the VPN tunnel are of high quality and not disclosed.

A.LDAP

The IT environment shall provide a trusted and reliable LDAP server to provide user authentication. The IT Environment shall provide a secure connection from the TOE to the LDAP server. LDAP is an optional component.

A.NET

The network that the authorized administrator uses to access the LogPoint Console is trusted.

A.SMTP

The IT environment shall provide a trusted and reliable SMTP server for email exchange. The IT Environment shall provide a secure connection from the TOE to the SMTP server

A.UEBA

The IT environment shall provide a trusted and reliable UEBA cluster for anomaly detection. The UEBA cluster is an optional component.

## 4.2 Clarification of Scope

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

T.INSIDER

An authorized user may intentionally or unintentionally remove or destroy TOE user data, disclose TOE user data or halt the TOE without being detected.

T.UNAUTH

An unauthorized user may gain access to the TOE security functions, TSF data or user data that is under the control of the TOE so that it is being disclosed, compromised or destroyed.

T.ACCESS

An authorized user of the TOE could gain unauthorized access to resources or information protected by the TOE, or performs operations for which no access rights have been granted.

T.OVERFLOW

An unauthorized entity may halt the execution of the TOE or cause malfunction of the TOE by creating an influx of user data that the TOE cannot handle.

T.FAIL_TO_DETECT

The TOE may analyze event data received from each device and fail to recognize vulnerabilities or inappropriate activity by an unauthorized user.

T.FAIL_TO_REACT

The TOE may fail to react to identified or suspected vulnerabilities or malicious attack on the enterprise network by an unauthorized user.

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

P.MANAGE

The TOE shall provide the means to configure and manage the TOE security functions.

P.SIEM_COLLECT

All events from devices are collected and stored.

P.SIEM_ANALYZE

All events from devices are monitored and reported upon.

P.SIEM_MANAGE

Events correlated and classified as incidents are managed to resolution.

P.SIEM_PURPOSE

Event data collected and/or generated by the TOE is used for authorized purposes only.

# 5 Architectural Information

The TOE consists of a set of software applications that collectively make up the TOE. The hardware platform on which the TOE is installed is dedicated to functioning as the TOE with no secondary function. The TOE can also be installed on a virtual machine with the same restriction that the machine only functions as the TOE.

For a TOE installation that consists of more than one appliance operating as a distributed system, each appliance has the same hardware and software requirements as described below. The TOE runs on any Linux-based operating system. However, for the purpose of evaluation, the following hardware and software configuration is used:

| Item | Identification | Description |
|---|---|---|
| Operating System | Ubuntu 16.04.1 LTS | |
| Hardware | Intel-compatible quad core CPU, 2GHz minimum<br>Memory: 8GB or more recommended<br>Disk Space 100GB (RAID-1 protected) recommended<br>Network adapter: 1GB network adapter | |
| Software | Mongo DB v4.0.10 | an open-source document database, and leading NoSQL database |
| | Nginx v1.18.0 | an HTTP and reverse proxy server, as well as a mail proxy server |
| | Gunicorn v19.19.0 | a Python WSGI HTTP Server for UNIX |

All of the required software, including the TOE, Operating system and other software is provided as an ISO image file/patch that is delivered electronically to the customer.

To access the TOE web interface, an authorized user requires a network-attached computer with a compatible browser installed (Google Chrome 68.x or later, Mozilla Firefox 62.x or later, Microsoft Internet Explorer 11 or later, Apple Safari 12.x or later).

If LDAP is used for user authentication then a suitable LDAP server needs to be installed. OpenLDAP is included in Ubuntu's default repositories under the package "slapd". Appropriate measures shall be employed to ensure the security of user credentials delivered from the TOE to the LDAP server.

If UEBA is used for advance analytics then a UEBA license will be required to communicate with the UEBA cluster. After UEBA is enabled and configured, the UEBA connector present in the TOE will manage the communication with UEBA cluster. Appropriate measures are employed to ensure the security of log data delivered from the TOE to the UEBA cluster.

# 6 Documentation

The following documentation comprises the TOE guidance:

- LogPoint™ 6.8.0 Release Notes [NOTES]
- LogPoint™ 6.8.0 Installation Manual [INST]
- LogPoint™ 6.8.0 Administrator Manual [ADM]
- LogPoint™ 6.8.0 User Manual [USR]
- LogPoint™ 6.8.0 Security Guide [CCGUIDE]

# 7 IT Product Testing

## 7.1 Developer Testing

The testing approach of the developer is to test all TOE interfaces, as well as all TOE subsystems.

The developer has provided the results of all test cases. All tests were successful.

## 7.2 Evaluator Testing

The evaluator performed negative testing to verify the proper function of the authentication mechanisms. The evaluator performed test cases specific for the selected protocol / functionality, and observed the results that were logged by the TOE.

All test cases completed successfully, i.e., no errors were observed.

## 7.3 Penetration Testing

The evaluator did not create any penetration tests based on the independent search for potential vulnerabilities. The developer testing and evaluator testing did sufficiently cover the possible candidates for penetration testing. While such tests are usually of functions, the evaluator found that the testing did take into account malformed or tampered input which could originate from an attacker.

These tests all passed, showing that no such malformed input would result in an issue within the TOE.

# 8 Evaluated Configuration

The requirements on the evaluated configuration are described below:

1. First, the hardware and software requirements are presented.
2. Boot the system with the LogPoint v6.3.0 ISO image and start the installation. The procedures describe how to set up systems storage.
3. Log in as user "li-admin" and default password "changeme", and immediately change the password.
4. Follow the list of initial configuration tasks in the "README.TXT"-file in the home directory.
5. Check the IP and log in to the LogPoint user interface as user "admin" and default password "changeme", and immediately change the password.
6. Activate the LogPoint with a valid license file.
7. Upload and install the required patches (6.4.0, 6.5.0, 6.6.0, 6.6.6, 6.7.2, and 6.8.0)
8. Enable NTP within system settings.
9. Configure permission groups, user groups and users.
10. Configure the TOE in the desired mode: Single LogPoint appliance or Multiple LogPoint appliances in a distributed configuration.
11. Configure collectors and fetchers
12. Verify the installed software to conclude the installation procedure

# 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* | *Component* | *Verdict* |
|---|---|---|
| Development | ADV | PASS |
| Security Architecture | ADV_ARC.1 | PASS |
| Functional Specification | ADV_FSP.3 | PASS |
| TOE 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 |
| CM Capabilities | ALC_CMC.3 | PASS |
| CM Scope | ALC_CMS.3 | PASS |
| Delivery | ALC_DEL.1 | PASS |
| Development security | ALC_DVS.1 | PASS |
| Life-cycle definition | ALC_LCD.1 | PASS |
| Flaw Remediation | ALC_FLR.2 | PASS |
| 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 |
| Tests | ATE | PASS |
| Coverage | ATE_COV.2 | PASS |
| Depth | ATE_DPT.1 | PASS |
| Functional Tests | ATE_FUN.1 | PASS |
| Independent Testing | ATE_IND.2 | PASS |
| Vulnerability Assessment | AVA | PASS |
| Vulnerability Analysis | AVA_VAN.2 | PASS |

# 10 Evaluator Comments and Recommendations

None.

# 11 Glossary

| | |
|---|---|
| Authorized administrator | An authenticated TOE user in either the LogPoint Administrator or User Account Administrator user group |
| CC | Common Criteria |
| CEM | Common Methodology for Information Technology Security |
| Device | Network entity such as a firewall or web server that provides event data to the TOE |
| Device Group | A cluster of log forwarding devices. A device can be associated to multiple device groups. |
| EAL | Evaluation Assurance Level |
| Event | Single data item received from a device |
| LDAP | Lightweight Directory Access Protocol |
| NTP | Network Time Protocol |
| OSP | Organizational Security Policy |
| IT | Information Technology |
| ITSEF | IT Security Evaluation Facility |
| PP | Protection Profile |
| SFP | Security Function Policy |
| SIEM | Security Information and Event Management |
| ST | Security Target |
| TOE | Target of Evaluation |
| TSF | TOE Security Functionality |
| User | A TOE user from one of the four TOE user groups: LogPoint Administrator, User Account Administrator, Admin or Operator. |
| UEBA | User and Entity Behavior Analytics |
| UEBA Connector | Component responsible for communicating with the external UEBA cluster to send/receive data to/from UEBA cluster. |
| UEBA Cluster | A cluster where UEBA analytics is generated. |

# 12 Bibliography


| | |
|---|---|
| ST | LogPoint A/S LogPoint™ 6.8.0 Common Criteria EAL3+ Security Target, LogPoint A/S, 21 Septemeber 2020, document version 0.11 |
| ADM | LogPoint Administration Manual, Logpoint A/S, 2020-08-14, Release 6.8.0 |
| CCGUIDE | Security Guide – Supplement for Common Criteria, Logpoint A/S, 2020-07-31,document version 0.11 |
| INST | LogPoint Installation Manual, Logpoint A/S, 2020-06-02, Release 6.8.0 |
| NOTES | LogPoint User Manual, Logpoint A/S, 2020-08-14, Release 6.8.0 |
| USR | LogPoint User Manual, Logpoint A/S, 2020-05-15, Release 6.8.0 |
| 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 |
| SP-002 | SP-002 Evaluation and Certification, CSEC, 2020-11-30, document version 32.0 |

# 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

During the certification project, the following versions of the quality management system (QMS) have been applicable since the certification application was received:

QMS 1.23.1 valid from 2020-03-06

QMS 1.23.2 valid from 2020-05-11

QMS 1.24 valid from 2020-11-19

QMS 1.24.1 valid from 2020-12-03

In order to ensure consistency in the outcome of the certification, the certifier has examined the changes introduced in each update of the quality management system.

The changes between consecutive versions are outlined in "Ändringslista CSEC QMS 1.24.1". The certifier concluded that, from QMS 1.23.1 to the current QMS 1.24.1, there are no changes with impact on the result of the certification.

## A.2 Scheme Notes

The following Scheme interpretations have been considered during the certification.

- Scheme Note 15 - Demonstration of test coverage
- Scheme Note 18 - Highlighted Requirements on the Security Target
- Scheme Note 22 - Vulnerability assessment
- Scheme Note 28 - Updated procedures for application, evaluation and certification
- Scheme Note 30 - CM of Third Party Components
- Scheme Note 31 - New procedures for site visit oversight and testing oversight