LogPoint A/S
LogPoint™ 6.8.0
Common Criteria EAL3+
Security Target

LogPoint A/S
Jagtvej 169B
2100 Copenhagen O
Denmark

www.logpoint.com
Telephone: +45 7060 6100

Contents

Figures

Introduction

SECTION	TITLE	DESCRIPTION
1	ST Introduction	Provides an overview of the TOE and defines the hardware and software that make up the TOE as well as the physical and logical boundaries of the TOE
2	Conformance Claims	Lists evaluation conformance to Common Criteria versions, Protection Profiles, or Packages where applicable
3	Security Problem Definition	Specifies the threats, assumptions and organizational security policies that affect the TOE
4	Security Objectives	Defines the security objectives for the TOE/operational environment and provides a rationale to demonstrate that the security objectives satisfy the threats
5	Extended Components Definition	Describes extended components of the evaluation (if any)
6	Security Requirements	Contains the functional and assurance requirements for this TOE
7	TOE Summary Specification	Identifies the IT security functions provided by the TOE and also identifies the assurance measures targeted to meet the assurance requirements.

Figure 1 Document Organization

0.1 Document Conventions

The notation, formatting, and conventions used in this Security Target are consistent with those used in Version 3.1 of the Common Criteria. Selected presentation choices are discussed here to aid the Security Target reader.

0.1.1 Use of language

Certain words within this document are used to convey a most specific meaning as defined in the ISO/IEC Directives, Part 2.

TERM	DEFINITION
shall	is used to indicate a requirement
will	is used to indicate a statement of fact
should	is used to indicate that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required.
not necessarily required	the choice of another possibility requires a justification of why the preferred option was not chosen.

0.1.2 Operations

The Common Criteria allows several operations to be performed on functional requirements: The allowable operations defined in Part 2 of the Common Criteria are *refinement*, *selection*, *assignment* and *iteration*.

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment operation is indicated by underlined text.

- The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**. Any text removed is indicated with a strikethrough format (Example: ~~TSF~~).

- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by *italicized* text.

- Iterated functional and assurance requirements are given unique identifiers by appending to the base requirement identifier from the Common Criteria an iteration number inside parenthesis, for example, FIA_UAU.1.1 (A) and FIA_UAU.1.1 (B) refer to separate instances of the FIA_UAU.1 security functional requirement component.

Outside the SFRs, italicized text is used for both official document titles and text meant to be emphasized more than plain text.

0.2 Document Terminology

TERM	DESCRIPTION
Authorized administrator	An authenticated TOE user in either the LogPoint Administrator or User Account Administrator user group
CC	Common Criteria
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
Knowledge Base	The collection of normalization rules, reports, alert rules, dashboards and searches that a user creates
LDAP	Lightweight Directory Access Protocol
NTP	Network Time Protocol
OSP	Organizational Security Policy
IT	Information Technology
LPA	LogPoint Administrator
OE	Operational Environment
PP	Protection Profile
Repo	Short for repository. A repository is a storage location used for holding log data.
SAR	Security Assurance Requirement
SFP	Security Function Policy

SFR	Security Functional Requirement
SIEM	Security Information and Event Management
ST	Security Target
Support Connection	A trusted channel used for remote administration. This feature is not part of the evaluated configuration. It can only be enabled by an authorized administrator.
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functionality
TSP	TOE Security Policy
UAA	User Account Administrator
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.

Figure 2 Glossary

0.3 References

[RFC5246]	RFC 5246: The Transport Layer Security (TLS) Protocol, Version 1.2, Internet Engineering Task Force, August 2008
[FIPS180-4]	FIPS 180-4: Secure Hash Standard (SHS), National Institute of Standards and Technology, August 2015
[FIPS186-4]	FIPS 186-4: Digital Signature Standard (DSS), National Institute of Standards and Technology, July 2013
[FIPS197]	FIPS 197: Advanced Encryption Standard (AES), National Institute of Standards and Technology, November 2001
[FIPS198]	FIPS 198: The Keyed-Hash Message Authentication Code (HMAC), National Institute of Standards and Technology, July 2008
[RFC5280]	RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, National Institute of Standards and Technology, May 2008
[RSASSAPKCSv1.5]	RFC 3447: Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1,Network Working Group, February 2003
[PKCS1v2.1]	RFC 3447: Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1,Network Working Group, February 2003
[PKCS12v1.1]	RFC 7292: Personal Information Exchange Syntax v1.1, Internet Engineering Task Force (IETF), July 2014
[PKCS5v2.1]	RFC 8018: Password-Based Cryptography Specification Version 2.1, Internet Engineering Task Force (IETF), January 2017

[NIST SP 800-38D]	NIST SP 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, November 2007

1 ST Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), Security Target organization, document conventions, and terminology. It also includes an overview of the evaluated product.

1.1 ST Reference

ST Title	LogPoint A/S LogPoint™ 6.8.0 Common Criteria EAL3+ Security Target
ST Revision	0.11
ST Publication Date	21 September 2020
Author	LogPoint A/S

1.2 TOE Reference

TOE Reference	LogPoint A/S LogPoint™ 6.8.0
TOE Type	Security Information and Event Management (SIEM) Software-only TOE

In this document, the terms TOE and LogPoint are used interchangeably.

1.3 TOE Overview

1.3.1 Usage and major security features of the TOE

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 analyzing 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 can also utilize UEBA for advance analytics to monitor user and entity activities in the network. This helps to detect potential threats before they emerge and also manage any potential breaches efficiently. The TOE also provides tools to further inspect the detected anomalies. Here, UEBA is an optional component of the TOE security features, where UEBA connector is the part of the TOE and UEBA cluster is the part of TOE environment.

An authorized user can access the TOE using its web interface via a web browser. TOE Role-based authentication is used to restrict access to TOE functionality to authorized users. The various user roles are discussed in section 1.4.1.5.

1.3.2 Required non-TOE hardware/software/firmware

The TOE consists of a set of software applications that collectively make up the TOE as identified in section 1.2.

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 Memory: 8GB or more recommended Disk Space 100GB (RAID-1 protected) recommended Network adapter: 1GB network adapter	
Other 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

Figure 3 LogPoint TOE Operational Environment

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. Regarding guidance document, customers can access them via Help Center (https://servicedesk.logpoint.com/hc) with valid credentials.

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.

1.4 TOE Description

The TOE is a software-only TOE.

The TOE can be operated on a single machine or as multiple TOEs in a distributed configuration.

The evaluated configurations of the TOE are illustrated in section 0 and consist of the following:

- Single LogPoint appliance
- Multiple LogPoint appliances working together in a distributed configuration

The TOE can also be configured as LogPoint Collector, with a subset of the full LogPoint components. But neither LogPoint Collector nor the use of LogPoint Collector in a distributed configuration is part of the evaluated configurations.

The TOE can also be integrated with UEBA analytics platform for both single machine and distributed configuration.

1.4.1 Logical Scope of the TOE Security Features

LogPoint is a SIEM system that collects, stores, analyzes and responds to log data from devices on an enterprise network.

LogPoint collects data from a wide range of sources, normalizes, indexes and stores it, making the data ready for analysis and reporting. Analysis is done on the indexed data using LogPoint's advanced search capabilities.

For the purposes of this document, there are two distinct types of log data:

- audit log data is collected to allow the security behavior of the TOE itself to be monitored
- event log data is collected by the TOE from network devices and allows the TOE to perform its SIEM functions

If the term "log data" is used without explicitly differentiating between audit and event data then the description shall be relevant to both types of log data.

The Physical scope of the TOE is shown in Figure 5, Figure 6. The logical boundary of the TOE encompasses the security functionality of the TOE.

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

1.4.1.1 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 below.

1.4.1.1.1 Data collection

The TOE acquires event data in a number of distinct ways.

Network based devices send events to the TOE. The TOE collects events from a number of different devices using collectors listening on specific network ports. Some of these operate in real-time, such as the Syslog, SNMP Trap, and Netflow collectors. Others are batch oriented, such as the FTP Collector.

Other devices require LogPoint to actively retrieve event information. For such devices, a dedicated fetcher polls the device for information at scheduled intervals.

LogPoint supports a number of collectors and fetchers. However, only the collectors and fetchers listed below are part of the evaluated configuration:

COLLECTORS	FETCHERS
Syslog Collector	FTP Fetcher
SNMP Trap Collector	SCP Fetcher
FTP Collector	WMI Fetcher
SFlow Collector	SNMP Fetcher
Snare Collector	SDEE Fetcher
FileSystem Collector	Checkpoint Firewall
Netflow Collector	ODBC Fetcher
	Vulnerability Management

Figure 4 Collectors and Fetchers

Note: The FileSystem Collector is only applied to the localhost device and is the means by which TOE Audit data is collected.

The collectors and fetchers provide the TOE with the raw event log data that the SIEM uses. They are tailored to obtain the event log data from the TOE environment. The collectors and fetchers themselves are part of the TOE operational environment. The File System collector is also used to obtain audit log data for the TOE and in this instance it is included within the TOE boundary.

1.4.1.1.2 Data normalization

The log data is normalized by applying templates to the log messages, extracting the metadata from the textual log messages.

Normalized data contains all the fields that were collected, with additional fields and values added after signature matching.

1.4.1.1.3 Data storage

Once the signature matching is completed, the log data is stored. Raw log messages are stored in text files. Fields and values extracted after normalization are stored separately.

1.4.1.1.4 Data indexing

The TOE uses indexes to facilitate the searching of log data. As the data is unstructured text, and the TOE handles such large amounts of data, indexing is crucial to the functionality of the TOE.

1.4.1.1.5 Data enrichment

The TOE uses external enrichment sources to enhance the value of the stored log data.

It does this by augmenting the event data it receives from devices by cross referencing it with data that it imports from external databases. In this way, an IP address can be matched to a more meaningful name, or a user identifier can be mapped to a user's name, for instance, to make the event data more meaningful.

1.4.1.1.6 Search

The TOE provides an intuitive query language that can be used to search the indexed log data.

Search results can be used to power real-time, self-updating dashboard widgets, create custom reports in order to monitor various compliance requirements, configure different correlation intelligence and write alert rules to act on the incidents requiring prompt response.

1.4.1.1.7 Dashboard

The Dashboard is a data visualization monitor that updates automatically in real time. Each dashboard contains one or more tabs.

A Dashboard can have multiple tabs. A tab can hold multiple widgets. A widget can hold charts, tables, and graphs generated by a search query. The width, height and positioning of each widget is user configurable.

1.4.1.1.8 Alert

Alerts are defined to continuously monitor data. Alert rules fire incidents that enable users to execute appropriate actions.

Alerts of different incidents can be created by using search queries. Users may be notified of alerts via either Email, Syslog, SSH, SNMP or HTTP. However, only notification via Email is included in the evaluated configuration.

1.4.1.1.9 Correlation

Correlation allows users to connect apparently disparate events to build up a pattern that may indicate inappropriate activity.

1.4.1.1.10 Incident

Incidents are used to identify, analyze, correct and prevent information hazards.

An authorized TOE user can identify one or more events and create an incident for each of these events.

An Incident can be created either on ad hoc basis from the search logs or by pre-defining alert rules. When the specified criteria are met, an incident is created. The incident is assigned to a user who is then responsible for it. The user is expected to resolve the incident through investigation and where necessary take remedial action.

1.4.1.1.11 Report

The TOE allows all authenticated users to create reports. These are exported from search.

The generated reports are listed with their name and format (pdf, html, xls, docx or csv).

When reports are created, the user responsible assigns a recipient for the report and a schedule for it. The report is then automatically delivered via email to the email address configured in the report settings recipient according to the defined schedule.

1.4.1.1.12 Anomaly (optional as it requires UEBA)

The TOE can also be configured with UEBA for analysis of anomalous behavior in the network. UEBA uses behavior and peer group analysis instead of predefined rules to ensure system only flags the abnormal behavior and reduce the false positives.

The analytics from UEBA can be viewed from UEBA dashboard. UEBA dashboard contains two pages: Overall Risk and Explore. Overall risk page provides an overview of the overall risk status based on the analyzed network events. Explore page displays the information for all the risky entities in the network. It also allows analysis of all the anomalies and potential threats associated with the entities.

1.4.1.2 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.

1.4.1.3 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.

1.4.1.3.1 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.

1.4.1.4 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.

1.4.1.5 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.

The four TOE user groups (roles) and their associated permissions are as follows:

- LogPoint Administrator
  - Can perform system related tasks
  - User account administration
  - Full Knowledge Base and Configuration Permissions
  - User functions (search, dashboard, correlation, alerts, reports)
- User Account Administrator
  - User account administration
  - Full Knowledge Base and Configuration Permissions
  - User functions (search, dashboard, correlation, alerts, reports)
- Admin
  - Full Knowledge Base and Configuration Permissions
  - User functions (search, dashboard, correlation, alerts, reports)
- Operator
  - Read-only Knowledge Base and Configuration Permissions
  - User functions (search, dashboard, correlation, alerts, reports)

TOE users are distinct from the users of the Operating System; such as the TOE users are not users in the Operating System. For more details see section 8.

1.4.1.6 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.

Following events takes place between the client and the server before the client is connected to the server with a static tunnel IP.

- The Distributed LogPoint acts as OpenVPN client (a TLS client) and initiates a VPN connection to the OpenVPN server.
- The server searches an existing association between the UUID/Identifier of the OpenVPN client and its tunnel IP address. If existing association is found then it creates a tunnel between itself and the client and provides the existing tunnel IP address to the OpenVPN client. If an association is not found then it provides an IP address from DHCP pool to the OpenVPN client. It only does so only if Tunnel IP Address and Password match on both side.
- Next the Client sends its UUID/Identifier through a HTTP POST request using a python module named “request”. The HTTP request is transmitted to the server inside the VPN tunnel.
- The server searches an existing association between the UUID/Identifier of the OpenVPN client and its tunnel IP address. If existing association is found then it sends the static IP address to the client. If existing association is not found then it adds one to the client specific file (the filename is tracked/identified with the Identifier of the client) and sends the tunnel IP information to the client in the HTTP response.
- After the client gets the HTTP response from the OpenVPN Server it starts its OpenVPN client to reconnect to the OpenVPN server.
- The server allows the client to connect by creating a VPN tunnel with static IP address.

RSA 2048 private key, a Diffie Hellman Key and the X.509 certificate is generated during the installation of each LogPoint instance. These entities are used to secure the OpenVPN channel between the OpenVPN Client and the Server.

TLSv1.2 is the TLS protocol and DHE_RSA_AES256_SHA256 is the cipher suite explicitly defined for TLS handshake protocol on both OpenVPN client and server. In addition, AES256 with CBC (Cipher Block Chaining) with SHA256 are explicitly defined as data channel protocol used for OpenVPN.

After the end of TLSv1.2 handshake protocol both OpenVPN client and server possesses a shared master secret, which is used to encrypt the bulk data i.e. actual LogPoint event data.

OpenSSL command line tool is used to create a private key, a Diffie-Hellman key and a X.509 certificate. OpenSSL uses “libcrypto”, which is a general-purpose cryptographic library, and “libssl”, which is a SSL specific cryptographic library.

The cryptographic library “libcrypto v1.0.0” and “libssl v1.0.0”, relied upon by the OpenSSL, which is relied upon by OpenVPN, which ultimately relied upon, by the TOE has been tested by the developers of “LogPoint A/S”.

In case of UEBA, when UEBA is enabled the TOE uses configuration present in the cloud.env file to identify the respective UEBA cluster and unlock the PKCS12 file using the passphrases. The TSF then uses the PKCS12 file which represents the keystore to authenticate itself to the cluster using the certificate. Similarly, it uses the other PKCS12 file representing the truststore which contains the CA certificate of the cluster to authenticate the server and establish trust between the UEBA cluster and the LogPoint UEBA connector. TLSv1.2 is the TLS protocol and TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 are the cipher suites explicitly defined for TLS handshake protocol on UEBA cluster whereas no specific cipher suite is defined on UEBA connector. After successful authentication, the UEBA connector can send data only at port 6667 of the UEBA cluster and can retrieve the data only from port 443.

The TOE then uses the configuration present in the on-prem.env file. The value of the OEM_ANON_PASSPHRASE key from the configuration is used in anonymization of event data to be sent to the UEBA cluster. This passphrase is a SHA256 hash of the random string of length 20-30 characters.

The TOE also specifies the cryptography algorithm (AES/CBC/PKCS5Padding) with hashing algorithm (SHA256) along with 128-bit keylen. The UEBA connector generates fixed salt and IV for the encryption and creates an instance of the cipher using the salt, IV, cryptography algorithm, hash algorithm, keylen bit, and SHA256 passphrase.

For each received payload, the UEBA connector generates digest of the plaintext and combines the byte array of the payload hash and the payload itself. The byte array is then encrypted using the cipher and then base64 encoded before sending to the UEBA cluster. When receiving data from the UEBA cluster the reverse steps are applied for de-anonymization of the data. This way it is ensured that the data is always encrypted before leaving the TOE premise. However, anonymization described above is not considered a TOE security feature.

1.4.2 TOE architecture and the Operational Environment (OE)

The TOE operates in an enterprise network. This is its operational environment. There are a number of different deployment scenarios for the TOE: It may be deployed as a single appliance, or with two or more appliances operating as a distributed system.

The operational environment includes all of the source machines and other network devices such as firewalls that provide event data to the TOE.

For the purposes of defining the TOE configuration, two specific scenarios are presented:

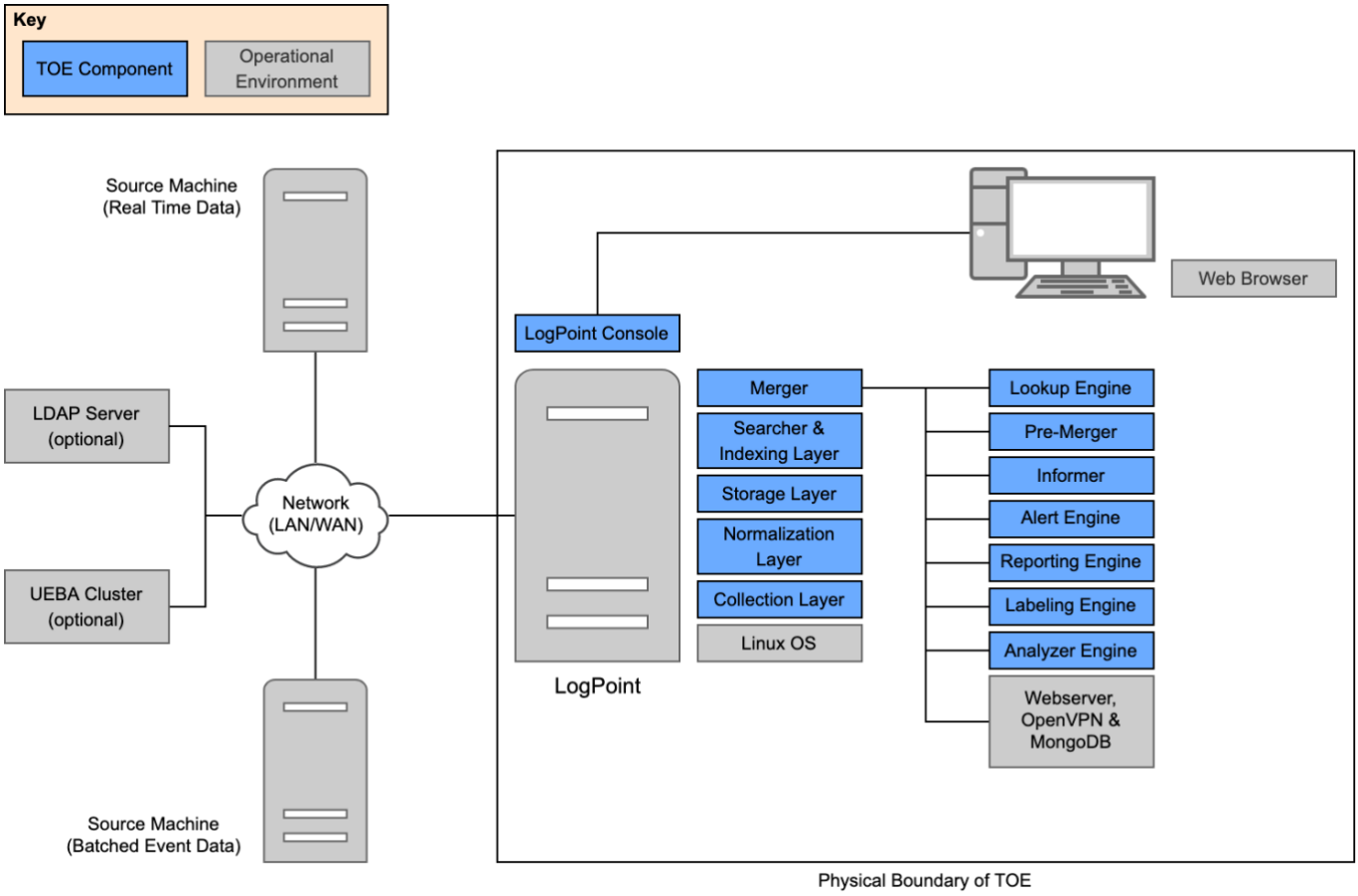


Figure 5 Single Appliance LogPoint Deployment

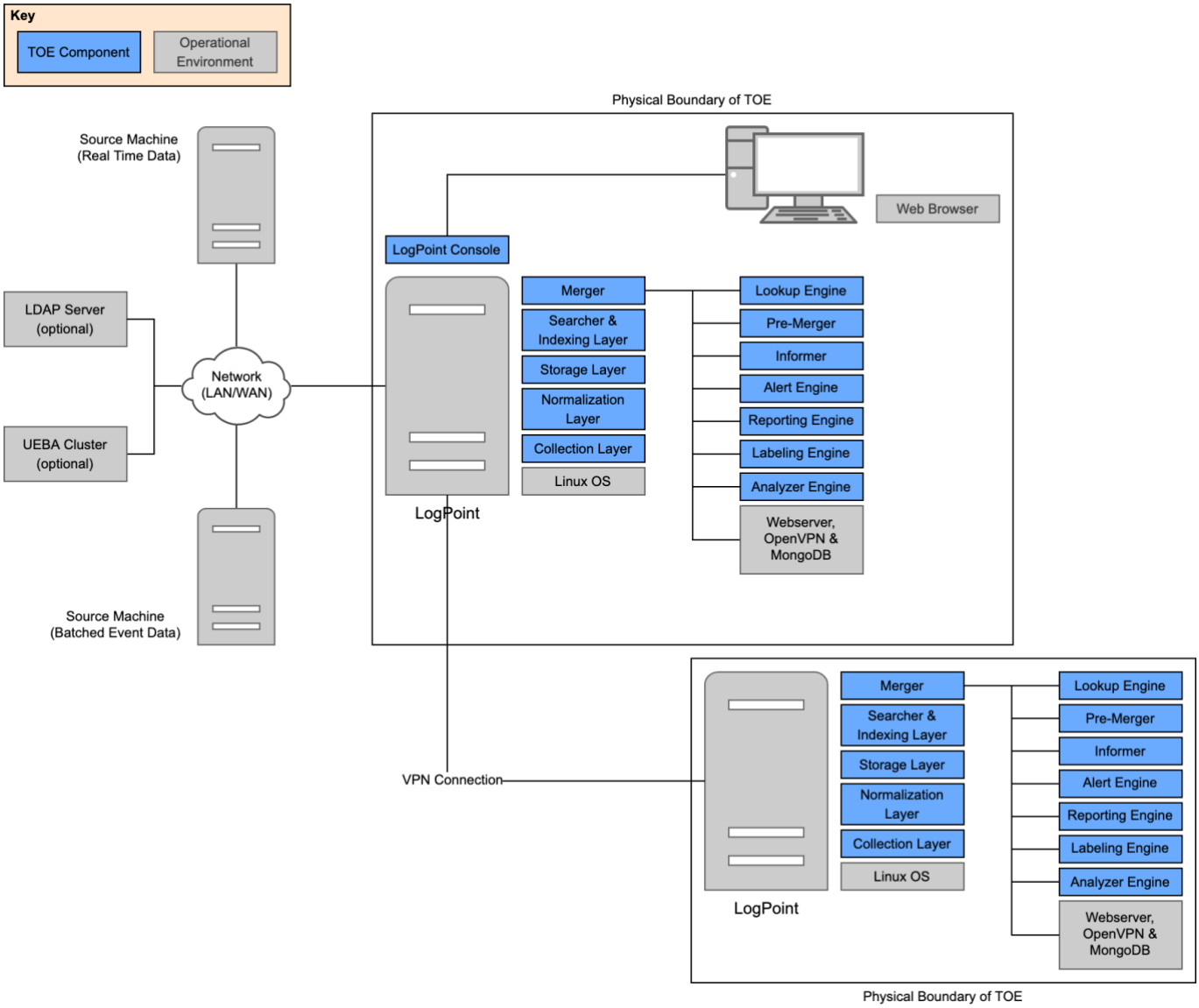


Figure 6 Multiple Appliance LogPoint Deployment

The Operational Environment must be protected to the level of security needed to protect the data that is stored on the LogPoint system. This requires current network administration best practice.

Similarly, if LogPoint receives events from devices on untrusted networks, then these must be shielded from LogPoint's operational environment using a firewall or other suitable means.

If LogPoint is deployed in a distributed configuration, there are a number of different scenarios that are possible with full-featured LogPoint appliances:

- LogPoint can be configured so that one LogPoint can access a repository from another LogPoint
- Logs can be forwarded from one LogPoint to another
- Two or more LogPoint appliances can be configured so that the same event data is stored in each LogPoint appliance

1.4.3 Guidance Documentation

The TOE provides the following administrative guidance documentation that is included as part of the TOE and customer can access them from Help Center (https://servicedesk.logpoint.com/hc) with valid credentials.

- LogPoint™ 6.8.0 Release Notes
- LogPoint™ 6.8.0 Installation Manual
- LogPoint™ 6.8.0 Administration Manual
- LogPoint™ 6.8.0 User Manual
- LogPoint™ 6.8.0 Security Guide
- LogPoint™ 6.8.0 UEBA Manual (optional)
- UEBA PreConfiguration Plugin v5.0.0 Manual
- Checkpoint Firewall v5.0.2 Manual
- ODBC Fetcher v5.0.0 Manual
- Vulnerability Management v5.0.0 Manual
- CSVEnrichmentSource v5.0.0 Manual
- LDAPEnrichmentSource v5.0.0 Manual
- GeoIP v5.0.1 Manual
- Evaluation Process Plugin v3.0.0 Manual
- Lookup Process Plugin v5.0.0 Manual
- Threat Intelligence v5.1.1 Manual
- Recorded Future v5.0.1 Manual
- StixTaxii v5.1.0 Manual
- Regex v5.0.0 Manual
- NetFlow Collector v3.0.0 Release Notes
- AsciiConverter Process Plugin v3.0.0 Release Notes
- Clean Char Process Plugin v3.1.0 Release Notes
- Codec Process Plugin v3.0.0 Release Notes
- Compare Process Plugin v3.1.0 Release Notes
- Compare Network Process Plugin v3.1.0 Release Notes
- Count Char Process Plugin v3.1.0 Release Notes
- Current Time Process Plugin v3.1.0 Release Notes
- DNS Process Plugin v3.1.0 Release Notes
- DNS Cleanup Process Plugin v3.1.0 Release Notes
- Experimental Median Quartile Quantile Plugin v3.0.0 Release Notes
- InRange Process Plugin v3.1.0 Release Notes
- IP Lookup Process Plugin v5.0.0 Release Notes
- Randomize Process Plugin v3.4.0 Release Notes
- ODBC Enrichment Source v5.0.0 Release Notes
- IPtoHost Enrichment Source v5.0.0 Release Notes

2 Conformance Claims

2.1 Common Criteria Conformance Claim

The TOE is Common Criteria Version 3.1 Revision 5 (April 2017) Part 2 extended and Part 3 conformant.

2.2 Protection Profile Conformance Claim

The TOE does not claim conformance to a Protection Profile.

2.3 Packages Conformance Claim

The TOE claims conformance to **Evaluation Assurance Level 3 (EAL3)** and augmented by **ALC_FLR.1 – Basic Flaw remediation**.

3 Security Problem Definition

3.1 Introduction

Enterprise Networks are complex. The demands placed on them by cloud-based computing and increasingly disparate appliances, in the form of mobile devices, tablets and more traditional computer technology makes it very difficult to maintain security while providing a usable working environment.

Against this, the threats from both outside and inside the network from malicious agents are changing and becoming more prevalent.

The TOE collects event data from network devices, analyzes it and responds to patterns and anomalies that it finds there. By identifying anomalous or malicious activity, user error, misconfigurations and security breaches, the TOE is able to identify threats to its assets and the assets of the OE, raise alarms and provide a means of managing an incident to resolution.

TOE assets are the events that it collects. In some use cases, these assets must be retained for legal compliance. The TOE has been designed to protect these assets by restricting access to them and protecting them against deletion.

OE assets are defined by the network administrators and owners, but would typically be the files and data stored on the network, transactions on the network and the physical network itself.

3.2 Threats

This section describes the threats to the assets of the TOE against which specific protection within the TOE or its environment is required.

This section describes the threat profile that the TOE addresses. This profile needs to be considered in the context of a global system security policy. The TOE is a Security Information and Event Management product and the threats it addresses are selected in order to fulfill these objectives.

THREAT	DESCRIPTION
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.

THREAT	DESCRIPTION
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.

3.3 Organizational Security Policies

This section describes the complete set of organizational security policy statements or rules with which the TOE must comply. Policies consist of rules, procedures and guidelines imposed by the organization that governs the OE and/or TOE implementation.

POLICY	DESCRIPTION
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.

3.4 Assumptions

This section describes the assumptions about the operational environment in which the TOE is used, including assumptions about personnel and the physical environment in which the TOE resides. The TOE operates in a secure manner and provides its countermeasures as long as it is utilized in a manner that adheres to the intended environment.

3.4.1 Personnel Assumptions

This section describes the assumptions about how the staff that are authorized to use the TOE behave.

ASSUMPTION	DESCRIPTION
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.

3.4.2 Physical Assumptions

This section describes the assumptions made about the physical environment in which the TOE operates.

ASSUMPTION	DESCRIPTION
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.

3.4.3 System Assumptions

This section describes the assumptions made about the whole system of which the TOE forms a component. The assumptions are made in relation to the TOE.

ASSUMPTION	DESCRIPTION
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 Security Objectives

This section identifies the security objectives of the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its environment in meeting the security needs.

These objectives reflect the intended method of use of the TOE and its operational environment and are suitable to counter all identified threats and cover all identified organizational security policies and assumptions.

4.1 Security Objectives for the TOE

This section describes the IT security objectives for the TOE.

OBJECTIVE	DESCRIPTION
O.AUDITS	The TOE must be able to provide audit evidence of TOE security relevant actions performed by the authorized administrator and user of the TOE.
O.AUTHENTICATE	The TOE must ensure that all users are identified and authenticated prior to allowing user access to TOE functions and data.
O.ACCESS	The TOE must allow authorized users to access only the TOE functions and data for which they have been given access.
O.OVERFLOW	The TOE must appropriately handle potential event data collection and storage overflows to ensure continuous operation in case of message flooding.
O.MANAGE	The TOE must provide the means for an authorized administrator to configure and manage the TOE security functions.
O.SIEM_COLLECT	The TOE must collect and store events from security and non-security products with accurate timestamps.
O.SIEM_ANALYZE	The TOE must apply analytical processes and rules to stored events in order to derive conclusions about them.
O.SIEM_MANAGE	The TOE must react to identified or suspected vulnerabilities or malicious attack on the enterprise network by an unauthorized entity.
O.EXPORT	The TOE must protect the event data against disclosure and tampering when it is transferred between distributed TOEs.

4.2 Security Objectives for the Operational Environment

4.2.1 Security Objectives for the IT Environment

This section describes the security objectives for the IT operational environment.

OBJECTIVE	DESCRIPTION
OE.FIREWALL	The IT environment shall provide a firewall or other suitable means to protect the TOE from untrusted networks.
OE.INTEROPERATIVE	The TOE shall be used in a way that it is interoperable with the network it monitors.
OE.TIME	The IT environment shall provide reliable timestamps to the TOE.
OE.ENRICHMENT	The IT environment shall provide appropriate data enrichment sources.
OE.KEYS	The IT environment shall provide high quality private RSA keys used for the VPN nodes and the VPN tunnel and maintain their confidentiality while doing so.
OE.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.
OE.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.
OE.UEBA	The IT environment shall provide a trusted and reliable UEBA cluster for anomaly detection. UEBA is an optional component.

4.2.2 Security Objectives for the Non-IT Environment

This section describes the security objectives for the non-IT aspects of the operational environment.

OBJECTIVE	DESCRIPTION
OE.MANAGEMENT	The operational environment must ensure that administrators are trained, qualified, non-hostile and follow all guidance.
OE.USERS	The operational environment must ensure that authorized users possess the necessary authorization to perform their tasks and have access at least some of the information managed by the TOE and are expected to act in a cooperating manner.
OE.LOCATE	The operational environment must ensure that the TOE is physically secure, i.e. no unauthorized persons have physical access to the TOE and its underlying system.
OE.NET	The operational environment must ensure that the network that the authorized administrator uses to access the LogPoint Console is trusted.

4.3 Security Objectives Rationale

The following table demonstrates that each threat identified in the TOE security environment is countered by one or more security objectives. Conversely, each security objective (either solely or in collection with other objectives) matches at least one assumption, threat or procedure.

This complete mapping demonstrates that the defined security objectives meet all defined threats, uphold all assumptions and enforce all organizational security policies.

Below the table, each mapping is considered in detail.

SECURITY OBJECTIVES / THREAT/ POLICY/ ASSUMPTION	OE.FIREWALL	OE.INTEROPERATIVE	OE.TIME	OE.ENRICHMENT	OE.KEYS	OE.LDAP	OE.SMTP	OE.UEBA	OE.MANAGEMENT	OE.USERS	OE.LOCATE	OE.NET	O.AUDITS	O.AUTHENTICATE	O.ACCESS	O.OVERFLOW	O.MANAGE	O.SIEM_COLLECT	O.SIEM_ANALYZE	O.SIEM_MANAGE	O.EXPORT
A.MANAGEMENT									X												
A.USERS										X											
A.LOCATE											X										
A.FIREWALL	X																				
A.INTEROPERATIVE		X																			
A.TIME			X																		
A.ENRICHMENT				X																	
A.KEYS					X																
A.LDAP						X															
A.NET												X									
A.SMTP							X														
A.UEBA								X													
T.INSIDER						X			X				X	X							
T.UNAUTH						X					X			X							X
T.ACCESS						X								X	X						
T.OVERFLOW																X					
T.FAIL_TO_DETECT																		X	X		
T.FAIL_TO_REACT																				X	
P.MANAGE																	X				
P.SIEM_COLLECT		X	X															X			
P.SIEM_ANALYZE								X											X		
P.SIEM_MANAGE																				X	
P.SIEM_PURPOSE																	X				

Figure 7 Matching Assumptions, Threats and Organizational Security Policies with OE and TOE Security Objectives

A.MANAGEMENT

The OE.MANAGEMENT objective ensures that LogPoint administrators are trained, qualified, non-hostile and follow all guidance.

A.USERS
The OE.USERS objective ensures 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
The OE.LOCATE objective ensures that the TOE is physically secure, i.e. no unauthorized persons have physical access to the TOE and its underlying system.

A.FIREWALL
The OE.FIREWALL objective ensures that the IT environment shall provide a firewall or other suitable means to protect the TOE from untrusted networks.

A.INTEROPERATIVE
The OE.INTEROPERATIVE objective ensures that the TOE is used in a way that it is interoperable with the network it monitors.

A.TIME
The OE.TIME objective ensures that the IT environment provides reliable timestamps to the TOE.

A.ENRICHMENT
The OE.ENRICHMENT objective ensures that the IT environment provides appropriate data enrichment sources.

A.KEYS
The OE.KEYS objective ensures that the IT environment provides high quality private RSA keys used for the VPN nodes and the VPN tunnel and maintain their confidentiality while doing so.

A.LDAP
The OE.LDAP ensures that the IT environment provides a trusted and reliable LDAP server for user authentication, and that the IT environment provides a secure connection from the TOE to the LDAP server (if required).

A.NET
The OE.NET objective will ensure that the network used by the authorized administrator to access the LogPoint Console is trusted.

A.SMTP
The OE.SMTP ensures that the IT environment provides a trusted and reliable SMTP server for email exchange, and that the IT environment provides a secure connection from the TOE to the SMTP server.

A.UEBA
The OE.UEBA ensures that the IT environment provides a trusted and reliable UEBA cluster for anomaly detection (if required).

T.INSIDER
The O.AUDITS ensure that audit evidence is provided for security relevant action performed by the authorized administrators and users of the TOE. Security actions that may include remove or destroy

TOE user data that may be intentionally or unintentionally performed. While the LogPoint administrator is considered to be non-hostile (OE.MANAGEMENT) so only unintentional, i.e. non-hostile actions are relevant, other users may try to act with bad intentions. Since all authorized user activity is logged, this will ensure that the actions of any malicious insider are recorded and so detected. This also acts as a deterrent measure. The O.AUTHENTICATE will ensure that all users are identified and authenticated so that accountability can be ensured. If LDAP is being used for the user authentication OE.LDAP will ensure the reliable LDAP authentication.

T.UNAUTH
The O.AUTHENTICATE will ensure that all users are identified and authenticated prior to allowing user access to TOE functions and data. The physical protection of the TOE ensured by OE.LOCATE, will ensure that the user authentication cannot be physically bypassed and the protection of event data transferred between the TOE and another TOE is ensured by O.EXPORT that protects exported event data against disclosure or tampering. If LDAP is being used for the user authentication OE.LDAP will ensure the reliable LDAP authentication.

T.ACCESS
The O.ACCESS will ensure that only authorized users are given to access only the TOE functions and data for which they have been given access. This will effectively prevent unauthorized users or user with no explicit access permission to gain access to resources or information protected by the TOE, or perform operations for which no access rights have been granted. The O.AUTHENTICATE will ensure that all users are identified and authenticated so that access rights are determined. If LDAP is being used for the user authentication OE.LDAP will ensure the reliable LDAP authentication.

T.OVERFLOW
The O.OVERFLOW will ensure that continuous operation can be ensured in case of message flooding. It is clear that data collection is sometimes performed in a hostile environment that may allow an attacker to create massive data generation that would potentially halt operation of the TOE. An attack that otherwise would have been detected may then go undetected. The O.OVERFLOW will ensure that such a message flooding attack will not result in halting the operation of the TOE.

T.FAIL_TO_DETECT
The O.SIEM_COLLECT and O.SIEM_ANALYZE will ensure that the TOE collects and store events with accurate timestamps (O.SIEM_COLLECT) and that the TOE applies analytical processes and rules to stored events in order to derive conclusions about them (O.SIEM_ANALYZE). It ensures that the TOE will analyze event data received from each device and will not fail to recognize vulnerabilities or inappropriate activity by unauthorized entities.

T.FAIL_TO_REACT
The O.SIEM_MANAGE will ensure that the TOE will react to identified or suspected vulnerabilities or malicious attack on the enterprise network by an unauthorized entity.

P.MANAGE
The O.MANAGE will ensure that the TOE will provide the means for an authorized administrator to configure and manage the TOE security functions.

P.SIEM_COLLECT

The O.SIEM_COLLECT will ensure that the TOE will collect and store events from security and non-security products with accurate timestamps. It ensures that all events from devices are collected and stored. The OE.INTEROPERATE will ensure the interoperability with the networks it monitors and OE.TIME will provide reliable timestamps.

P.SIEM_ANALYZE
The O.SIEM_ANALYZE will ensure that the TOE will apply analytical processes and rules to stored events in order to derive conclusions about them. It ensures that all events from devices are monitored and reported upon. If UEBA is being used for analysis OE.UEBA will ensure the reliable anomaly detection.

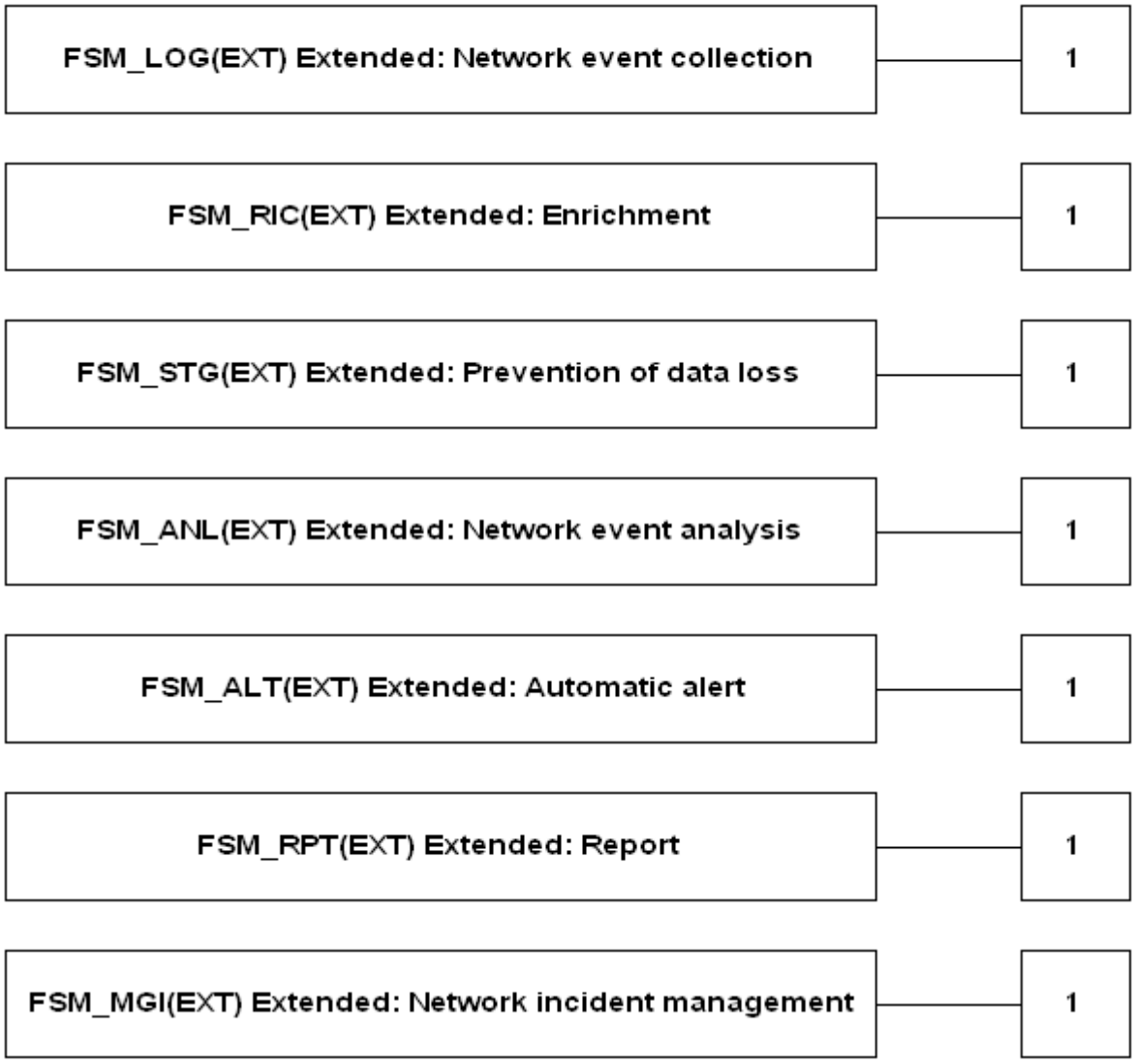
P.SIEM_MANAGE
The O.SIEM_MANAGE will ensure that the TOE will react to identified or suspected vulnerabilities or malicious attack on the enterprise network by an unauthorized entity. It ensures that events correlated and classified as incidents are managed to resolution.

P.SIEM_PURPOSE
The O.MANAGE will ensure that TOE will provide the means for an authorized administrator to configure and manage the TOE security functions. It ensures that event data collected and/or generated by the TOE is used for authorized purposes only.

5 Extended Components Definition

5.1 Class FSM: Security Information and Event Management

Security information and event management (SIEM) involves collecting, storing, analyzing and reporting on events generated by network and security devices; identity and access management applications; vulnerability management and policy compliance tools; operating system, database and application logs; and external threat data. The resulting data is handled in such a way as to facilitate a workflow that provides incident management as a means of maintaining and enhancing enterprise network security.

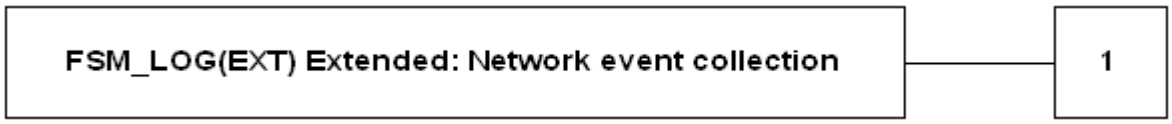


5.1.1 FSM_LOG(EXT) Extended: Network event collection

Family behavior

This family defines how event data is collected from network devices and stored.

Component leveling



FSM_LOG(EXT) Extended: Network event collection defines how SIEM events are collected and stored by the TSF.

Management: FSM_LOG(EXT).1

The following management actions could be considered for management functions in FMT:

a) The management of normalization rules.

Audit: FSM_LOG(EXT).1

There are no auditable events foreseen.

FSM_LOG(EXT).1 Extended: Network event collection

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FSM_LOG(EXT).1.1 The TSF shall collect [assignment: *list of event types*] from [assignment: *list of network devices*].

FSM_LOG(EXT).1.2 The TSF shall normalize the collected events using [assignment: *define rules used for normalization*].

FSM_LOG(EXT).1.3 The TSF shall store the normalized events. For each event, the TSF shall store at least the following information:

a) collection timestamp, collection type, device identifier, message counter, raw event message; and
b) [assignment: *other security relevant information about the event*].

5.1.2 FSM_RIC(EXT) Extended: Enrichment

Family behavior

This family defines how external enrichment sources are used to improve the quality of event data.

Component levelling

FSM_RIC(EXT) Extended: Enrichment defines how the TSF interfaces with and uses external enrichment sources.

Management: FSM_RIC(EXT).1

The following management actions could be considered for management functions in FMT:

a) The management of enrichment sources.

Audit: FSM_RIC(EXT).1

There are no auditable events foreseen.

FSM_RIC(EXT).1 Extended: Enrichment

Hierarchical to: No other components.

Dependencies: FSM_LOG(EXT).1 Extended: Network event collection

FSM_RIC(EXT).1.1 The TSF shall use [assignment: *list of enrichment sources*] to improve the value of SIEM event data.

5.1.3 FSM_STG(EXT) Extended: Prevention of data loss

Family behavior

This family defines how event data is protected against loss or modification once it has been stored.

Component levelling

FSM_STG(EXT) Extended: Prevention of data loss defines how stored SIEM events are protected by the TSF.

Management: FSM_STG(EXT).1

There are no management activities foreseen.

Audit: FSM_STG(EXT).1

There are no auditable events foreseen.

FSM_STG(EXT).1 Extended: Prevention of data loss

Hierarchical to: No other components.

Dependencies: FSM_LOG(EXT).1 Extended: Network event collection.

FSM_STG(EXT).1.1 The TSF shall protect the stored SIEM event data from unauthorized deletion.

FSM_STG(EXT).1.2 The TSF shall protect the stored SIEM event data from modification.

FSM_STG(EXT).1.3 The TSF shall [selection, choose one of: *ignore new SIEM event data*, *overwrite the oldest stored SIEM event data*] if the storage capacity has been reached.

5.1.4 FSM_ANL(EXT) Extended: Network event analysis

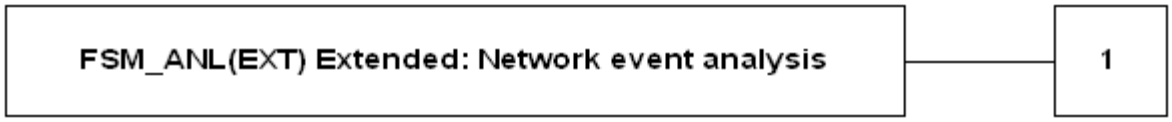
Family behavior

This family defines how stored event data is analyzed. Due to the ever changing threat profile that a SIEM tool has to meet, it is important that it is able to adapt to these changing threats.

The knowledge of the SIEM users is crucial for guiding the analysis process. The user is able to create searches that can be continually or periodically applied to all of the event data or a portion of it.

This analysis facilitates the discovery of potential security incidents.

Component levelling



FSM_ANL(EXT) Extended: Network event analysis defines how SIEM events can be manipulated and displayed for the user by the TSF.

Management: FSM_ANL(EXT).1

The following management actions could be considered for management functions in FMT:

a) The management of saved searches.

Audit: FSM_ANL(EXT).1

There are no auditable events foreseen.

FSM_ANL(EXT).1 Extended: Network event analysis

Hierarchical to: No other components.

Dependencies: FSM_LOG(EXT).1 Extended: Network event collection.

FSM_ANL(EXT).1.1 The TSF shall index SIEM event data according to [assignment: *define indexing policy*] to facilitate analysis.

FSM_ANL(EXT).1.2 The TSF shall perform [assignment: *list of analysis functions*] analysis on stored SIEM event data.

5.1.5 FSM_ALT(EXT) Extended: Automatic alert

Family behavior

This family defines how the TOE behaves when a potential security violation is detected. The alert may take the form of a visual indicator on-screen or take an action such as sending an email.

The purpose of an alert is to bring a user's attention to a potential violation as it occurs so that it can be dealt with in a timely manner.

Component levelling

FSM_ALT(EXT) Extended: Automatic alert defines how the TOE responds to potential security violations.

Management: FSM_ALT(EXT).1

The following management actions could be considered for management functions in FMT:

a) The management of alert rules.

Audit: FSM_ALT(EXT).1

There are no auditable events foreseen.

FSM_ALT(EXT).1 Extended: Automatic alert

Hierarchical to: No other components.

Dependencies: FSM_ANL(EXT).1 Extended: Network event analysis,
FSM_LOG(EXT).1 Extended: Network event collection.

FSM_ALT(EXT).1.1 The TSF shall [assignment: *list of actions*] upon detection of a potential security violation.

5.1.6 FSM_RPT(EXT) Extended: Report

Family behavior

This family defines how reports are generated. Reports provide a mechanism where anomalous behavior, vulnerabilities and potential violations, once detected can be communicated to the relevant individuals so that the appropriate remedial actions can be performed.

This family is concerned with how security incidents are reported.

Component levelling

FSM_RPT(EXT) Extended: Report defines how the TSF uses analysis and incident management outputs to provide reports to identified individuals.

Management: FSM_RPT(EXT).1

The following management actions could be considered for management functions in FMT:

a) The management of the recipient and schedule for a report.

Audit: FSM_RPT(EXT).1

There are no auditable events foreseen.

FSM_RPT(EXT).1 Extended: Report

Hierarchical to: No other components.

Dependencies: FSM_ANL(EXT).1 Extended: Network event analysis,
FSM_MGI(EXT).1 Extended: Network incident management,
FSM_LOG(EXT).1 Extended: Network event collection.

FSM_RPT(EXT).1.1 The TSF shall deliver [assignment: *list of reports*] exported from [assignment: *define source of report*] to [assignment: *report recipients*] according to a defined delivery schedule.

5.1.7 FSM_MGI(EXT) Extended: Network incident management

Family behavior

This family defines how incidents are managed to resolution by the TOE. An incident dashboard provides a convenient way to display incident data in the format chosen by the user. Data can be displayed graphically or passed through a post-processing function, such as applying statistical analysis.

The dashboard also allows a user to apply notes and to create new searches, view data and to change the status of an incident.

Component levelling

FSM_MGI(EXT) Extended: Network incident management defines the requirements for security incident management.

Management: FSM_MGI(EXT).1

The following management actions could be considered for management functions in FMT:

a) The management of incident dashboard.

Audit: FSM_MGI(EXT).1

There are no auditable events foreseen.

FSM_MGI(EXT).1 Extended: Network incident management

Hierarchical to: No other components.

Dependencies: FSM_ANL(EXT).1 Extended: Network event analysis,
FSM_LOG(EXT).1 Extended: Network event collection.

FSM_MGI(EXT).1.1 The TSF shall track [assignment: *list of work items*] that are necessary to resolve an incident.

6 Security Requirements

This section describes the security requirements levied on the TOE and the Operational Environment (OE).

6.1 Security Functional Requirements

The following are the conventions used for the operations applied to the Security Functional Requirements: Assignment is indicated in underscore, selection in italics and refinement is indicated in **bold**. Iterations are indicated with adding a capital letter in brackets.

This section defines the TOE SFRs derived from the CC Version 3.1 or from the extended components defined in Section 5. The TOE satisfies the SFRs stated in Figure **8** below, which list the names of the SFR components. Each individual functional requirement, with any TOE specific parts completed (see underlined text) is included following Figure **8.**

FUNCTIONAL CLASS	FUNCTIONAL COMPONENTS
FAU: Security Audit	FAU_GEN.1 Audit data generation
	FAU_SAR.1 Audit review
	FAU_SAR.2 Restricted audit review
	FAU_SAR.3 Selectable audit review
	FAU_STG.1 Protected audit trail storage
	FAU_STG.3 Action in case of possible audit data loss
FCS: Cryptographic Support	FCS_CKM.1(A) Cryptographic key generation (AES)
	FCS_CKM.1(B) Cryptographic key generation (HMAC)
	FCS_CKM.2(A) Cryptographic key distribution
	FCS_CKM.2(C) Cryptographic key distribution (X.509 certificates)
	FCS_CKM.4 Cryptographic key destruction
	FCS_COP.1(A) Cryptographic operation (AES-CBC)
	FCS_COP.1(B) Cryptographic operation (SHA)
	FCS_COP.1(C) Cryptographic operation (RSA)
FDP: User Data Protection	FDP_ACC.1 Subset access control
	FDP_ACF.1 Security attribute based access control
FIA: Identification and authentication	FIA_ATD.1 User attribute definition
	FIA_UAU.2 User authentication before any action
	FIA_UID.2 User identification before any action
	FIA_AFL.1(A) Authentication failure handling
	FIA_AFL.1(B) Authentication failure handling
FMT: Security Management	FMT_MOF.1 (A) Management of security functions behavior (user)
	FMT_MOF.1 (B) Management of security functions behavior (administrator)
	FMT_MSA.1 Management of Security Attributes

FUNCTIONAL CLASS	FUNCTIONAL COMPONENTS
	FMT_MSA.3 Static Attribute Initialization
	FMT_MTD.1(A) Management of TSF data (User Identity)
	FMT_MTD.1(B) Management of TSF data (Permissions)
	FMT_SMF.1 Specification of Management Functions
	FMT_SMR.1 Security roles
FTP: Trusted path/channels	FTP_ITC.1 Inter-TSF trusted channel
FSM: Security information and event management	FSM_LOG(EXT).1 Extended: Network event collection
	FSM_RIC(EXT).1 Extended: Enrichment
	FSM_STG(EXT).1 Extended: Prevention of data loss
	FSM_ANL(EXT).1 Extended: Network event analysis
	FSM_ALT(EXT).1 Extended: Automatic alert
	FSM_RPT(EXT).1 Extended: Report
	FSM_MGI(EXT).1 Extended: Network incident management

Figure 8 Security Functional Requirements of the TOE

6.1.1 Security Audit (FAU)

FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the *not specified* level of audit; and

1. User management
   - Add/Edit/Delete Users, User Groups and Permissions
2. Identification and authentication
   - Logon attempts
   - Logon success
   - Logon failures
   - User lock/unlock
3. User actions
   - Add/Edit/Delete Knowledge Base items,
   - Configuration (Device, Device Group, Log Collection Policies, Repos, Distributed LogPoint, UEBA)
   - Add/Edit/Delete Search, Report, Dashboard and Incident management.
4. Inter-TSF trusted channel
   - Connect to/Disconnect from another TOE
5. System
   - Disk Usage

Application Note: The audit records of the above auditable events are collected by TOE using file system collector.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

- Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, no other relevant information

Application note: The audit functions within the TOE cannot be disabled, as long as the TOE is active, the audit functions are running.

Application note: FAU_GEN1.2 records map to TOE records as follows:

FAU_GEN.1.2 RECORD FIELD	TOE FIELD
Date and time of the event	log_ts
type of event	type
subject identity	user
outcome (success or failure) of the event	action

Figure 9 FAU_GEN.1.2 information mapping to TOE

FAU_SAR.1 Audit review
FAU_SAR.1.1 The TSF shall provide authorized users with the capability to read all audit information from the audit records.
FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Application note: The authorized users could be any users that have been given permission to read all audit information. The permission is managed using universal query and object permission.

A universal query is a search item that can be used to restrict the set of data that a user has access to. It defines the extent of their universe with respect to the TSF data.

Object permission allows users to search logs from only those repos and devices that are assigned to them. And all the audit logs are stored in "_logpoint" repo.

FAU_SAR.2 Restricted audit review
FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

FAU_SAR.3 Selectable audit review
FAU_SAR.3.1 The TSF shall provide the ability to apply sorting of audit data based on date and time, the type of the event, the subject identity and the outcome of the event.

Application Note: Audit Review and Selectable Audit Review are only accessible to an authorized user through the LogPoint Console.

FAU_STG.1 Protected audit trail storage
FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.
FAU_STG.1.2 The TSF shall be able to *prevent* unauthorized modifications to the stored audit records in the audit trail.

FAU_STG.3 Action in case of possible audit data loss

FAU_STG.3.1 The TSF shall notify the LogPoint Administrator if the audit trail exceeds 90% disk space of each mounted partition where audit data is stored.

Application Note: By default, LogPoint and audit data are stored in a single disk partition. In case a new disk is mounted, only audit data along with event data can be configured to be stored in that partition. In case, audit records exceeds 90% disk space of any of the mentioned partitions where either LogPoint and audit data or only audit data are stored, TOE would notify the LogPoint Administrator.

The predefined limit for notification by default is 90% and this is user configurable. In addition to sending a notification an audit log is also generated when the disk usage exceeds the predefined limit. After that notification an audit log is generated every hour. Users can also define multiple disk usage notification rules with custom disk usage percent and message.

6.1.2 Cryptographic Support (FCS)

FCS_CKM.1(A) Cryptographic key generation (AES)

FCS_CKM.1.1(A) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm as defined in the TLS v1.2 standard [RFC5246] for AES-128 [FIPS197] and AES-256 [FIPS197] keys and specified cryptographic key sizes 128 bit (AES-128) and 256 bit (AES-256) that meet the following: generation and exchange of session keys as defined in the TLS v1.2 standard with the cipher suites defined in FCS_COP.1(A).

Application Note: The session keys are negotiated and established during a TLS session. The TLS standard allows other cryptographic algorithms and key sizes, but only AES-256 and SHA256 are supported. The TOE can act both as a TLS client and a TLS server. The TLS server provides this functionality. The client provides corresponding functionality on the TLS client's side. The key destruction of session keys is covered by FCS_CKM.4

In case of OpenVPN, two LogPoint instances are mutually authenticated using a TLS v1.2 encrypted connection. The DHE_RSA_AES256_SHA256 is the only supported TLS cipher suite.

In case of UEBA, the TOE and the UEBA cluster are mutually authenticated using a TLS v1.2 encrypted connection. A password protected PKCS12 file [PKCS12v1.1] containing TLS client credentials (certificate and it's matching 2048 bit RSA private key) representing the keystore and another password protected PKCS12 file [PKCS12v1.1] containing CA certificate for the cluster representing the truststore is used during two-way TLS authentication. The TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 are the list of supported cipher suites.

FCS_CKM.1(B) Cryptographic key generation (HMAC)

FCS_CKM.1.1(B) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm as defined in the TLS v1.2 standard [RFC5246] for HMAC with SHA256 [FIPS198] and SHA384 [FIPS180-4] keys and specified cryptographic key sizes 256 bit (HMAC-SHA256) and 384 bit (HMAC-SHA384) that meet the following: generation and exchange of session keys as defined in the TLS v1.2 standard with the cipher suites defined in FCS_COP.1(B).

Application Note: TLS uses the HMAC algorithm, a keyed-hash message authentication code (HMAC), for calculating a message authentication code (MAC) involving a cryptographic hash function in

combination with a secret cryptographic key. The key destruction of session keys is covered by FCS_CKM.4

In case of OpenVPN, two LogPoint instances are mutually authenticated using a TLS v1.2 encrypted connection. The DHE_RSA_AES256_SHA256 is the only supported TLS cipher suite.

In case of UEBA, the TOE and the UEBA cluster are mutually authenticated using a TLS v1.2 encrypted connection. A password protected PKCS12 file [PKCS12v1.1] containing TLS client credentials (certificate and it's matching 2048 bit RSA private key) representing the keystore and another password protected PKCS12 file [PKCS12v1.1] containing CA certificate for the cluster representing the truststore is used during two-way TLS authentication. The TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 are the list of supported cipher suites.

FCS_CKM.2(A) Cryptographic key distribution
FCS_CKM.2.1(A) The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method TLS using 2048 bit Ephemeral Diffie-Hellman key exchange of AES-128, AES-256 session keys and HMAC keys that meets the following: TLS v1.2 [RFC5246].

Application note: This requirement addresses the exchange of AES-256 session keys and HMAC keys as part of the TLS handshake protocol using Ephemeral Diffie-Hellman for the VPN connection using TLS. No other cipher suite is accepted.

In case of UEBA, the requirement addresses the exchange of AES-128 or AES-256 session keys and HMAC keys as part of the TLS handshake protocol using Ephemeral Diffie-Hellman for the TLS connection with UEBA cluster. No other cipher suite is accepted.

FCS_CKM.2(C) Cryptographic key distribution (X.509 certificates)
FCS_CKM.2.1(C) The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method of digital certificates that meets the following: X.509 Version 3 [RFC5280]**.**

Application note: This requirement addresses the exchange of X.509 certificates as part of the TLS authentication used by the OpenVPN protocol when VPN Tunnel is established between two LogPoint instances and by UEBA connector when TLS channel is established between the TOE and UEBA cluster.

FCS_CKM.4 Cryptographic key destruction
FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method zeroization or erase that meets the following: as per the OpenSSL version 1.0.2g or erased by the docker container.

Application Note: Zeroization of cryptographic keys is performed automatically by API function calls of OpenSSL cryptographic library.

In case of UEBA, the cryptographic keys are temporarily stored in the memory of docker container. Hence, after the communication terminates the containers are cleaned up removing the cryptographic keys as well.

FCS_COP.1(A) Cryptographic operation (AES)

FCS_COP.1.1(A) The TSF shall perform encryption and decryption in accordance with a specified cryptographic algorithm AES-CBC or AES-GCM and cryptographic key sizes 128 bit or 256 bit that meet the following: FIPS 197 or NIST SP 800-38D.

Application note: AES-CBC cryptographic algorithm with key size 256 bit is used by TLS for the VPN channel. If a client or a VPN node tries to use any other cipher suite, the client or VPN node will be rejected by the TOE.

In case of UEBA, the TLS uses AES-GCM cryptographic algorithm with key size 128 bit or 256 bit for encryption and decryption. No other cipher suite is accepted.

FCS_COP.1(B) Cryptographic operation (SHA)
FCS_COP.1.1(B) The TSF shall perform message digest generation and verification in accordance with a specified cryptographic algorithm HMAC with SHA256 or SHA384 and cryptographic key sizes 256 bit or 384 bit that meet the following: [FIPS198] or [FIPS180-4].

Application note: The TLS standard allows other ciphers, but the TOE supports only SHA256. If a client or VPN node tries to use any other cipher suite for the message digest, the client or peer will be rejected by the TOE.

In case of UEBA, the TOE supports both SHA256 and SHA384 cipher suite for the message digest. No other cipher suite is accepted.

FCS_COP.1(C) Cryptographic operation (Signature Generation and Verification)
FCS_COP.1.1(C) The TSF shall perform digital signature generation and verification in accordance with a specified cryptographic algorithm RSA [RSASSAPKCS1v1.5] or ECDSA and cryptographic key sizes 2048 bit or 256 bit, 384 bit that meet the following: [PKCS1v2.1] or [FIPS186-4].

Application note: RSA keys are generated only once during installation. And this requirement addresses the RSA digital signature generation and verification operations using the RSA algorithm as required by the TLS session establishment protocol.

In case of UEBA, either RSA or ECDSA keys with the specified key sizes 2048 bit or 256 bit, 384 bit can be used to generate and verify the digital signature as required by the TLS session establishment protocol.

6.1.3 User Data Protection (FDP)

FDP_ACC.1 Subset access control
FDP_ACC.1.1 The TSF shall enforce the Multiple Access Control SFP on

a) Subjects: All users
b) Objects: Audit logs, Dashboards, Reports, Incidents
c) Operations: All user actions.

Application note: user actions are the ones listed in FAU_GEN.1.1 b) 1,3.

FDP_ACF.1 Security attribute based access control
FDP_ACF.1.1 The TSF shall enforce the Multiple Access Control SFP to objects based on the following:

a) Subjects: All users

b) Subject Attributes: Permissions
c) Objects: Audit logs, Dashboards, Reports, Incidents
d) Object Attributes: None
e) Operations: all user actions

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: based on User's Permissions.
FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: no such rules.
FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: no such rules.

6.1.4 Identification and Authentication (FIA)

FIA_ATD.1 User attribute definition
FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

a) User Identity,
b) Password,
c) user group and permissions,
d) name (first name and last name),
e) email address,
f) time zone

Application note: The attribute "Password" is only in case the TOE is using LP password authentication and not when the TOE is using LDAP. In case of LDAP, the attribute "Password" is maintained by the LDAP Server.

FIA_UID.2 User identification before any action
FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.2 User authentication before any action
FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application Note: User authentication is applicable for both LogPoint and LDAP user.

FIA_AFL.1(A) Authentication failure handling
FIA_AFL.1.1(A) The TSF shall detect when *3* unsuccessful authentication attempts occur related to user logon.
FIA_AFL.1.2(A) When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall display a captcha for each subsequent logon attempt and require this to be completed correctly before the logon attempt is allowed.

Application Note: The use of a captcha protects against an automated, dictionary attack on a user's password.

FIA_AFL.1(B) Authentication failure handling

FIA_AFL.1.1(B) The TSF shall detect when 5 unsuccessful authentication attempts occur related to user logon.
FIA_AFL.1.2(B) When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall lock the user account for next 30 minutes after which user gets one additional logon attempt. If this logon attempt fails, then the user account is locked for additional 30 min. This process continues until the user logon with valid credentials.

Application Note: The lockout threshold and lockout time is user configurable. However, the values defined in FIA_AFL.1.2(B) are the recommended default values with in Common Criteria evaluated configuration.

6.1.5 Security Management (FMT)

FMT_MOF.1(A) Management of security functions behavior (user)
FMT_MOF.1.1(A) The TSF shall restrict the ability to *determine the behavior of, disable, enable, modify the behavior of* the functions Knowledge Base items, Configuration items, Security Incidents, Alert and Correlation rules, Dashboards, Reports and Saved Search to Authorized users.

Application Note: searches are saved during event analysis and reporting (FSM_RPT(EXT).1 and FSM_ANL(EXT).1).

FMT_MOF.1(B) Management of security functions behavior (administrator)
FMT_MOF.1.1(B) The TSF shall restrict the ability to *determine the behavior of, disable, enable, modify the behavior of* the functions Connections to other TOEs to Authorized administrators.

FMT_MSA.1 Management of security attributes
FMT_MSA.1.1 The TSF shall enforce the Multiple Access Control SFP to restrict the ability to *change_default, modify, delete, clear, create* the security attributes Permissions to Authorized administrators.

FMT_MSA.3 Static attribute initialization
FMT_MSA.3.1 The TSF shall enforce the Multiple Access Control SFP to provide *permissive* default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2 The TSF shall allow the authorized administrators to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1(A) Management of TSF data (User Identity)
FMT_MTD.1.1(A) The TSF shall restrict the ability to *query, modify, delete,* create the User identity to authorized administrators.

FMT_MTD.1(B) Management of TSF data (Permissions)
FMT_MTD.1.1(B) The TSF shall restrict the ability to *query, delete,* create the User Permissions to authorized administrators.

FMT_SMF.1 Specification of Management Functions
FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: Security Attribute Management and Security Functions Management

Application Note: Security attribute management is defined in FMT_MSA.1 and Security functions management is defined in FMT_MOF.1(A) and FMT_MOF.1(B).

FMT_SMR.1 Security roles
FMT_SMR.1.1 The TSF shall maintain the roles: LogPoint Administrator, User Account Administrator, Admin, Operator
FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.1.6 Trusted path/channels (FTP)

FTP_ITC.1 Inter-TSF trusted channel
FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2 The TSF shall permit *the TSF or another trusted IT product* to initiate communication via the trusted channel.
FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for to allow one LogPoint to exchange event data with another LogPoint in a distributed configuration and to provide secure communication between LogPoint and UEBA cluster.

Application note: The trusted channel is used: (a) to provide secure communication between LogPoint appliances. Either party can initiate the connection; (b) to provide secure communication between LogPoint and UEBA cluster for exchange of event data. However, UEBA is an optional component in the evaluated configuration. The TOE will initiate all connection but will only accept connection request from another instance of the TOE in a distributed configuration.

6.1.7 Security information and event management (FSM)

FSM_LOG(EXT).1 Extended: Network event collection
FSM_LOG(EXT).1.1 The TSF shall collect raw event data as binary data or text from connected network devices.
FSM_LOG(EXT).1.2 The TSF shall normalize the collected events using administrator defined normalization rules.
FSM_LOG(EXT).1.3 The TSF shall store the normalized events. For each event, the TSF shall store at least the following information:

a) collection timestamp, collection type, device identifier, message counter, raw event message; and
b) no other security relevant information about the event.

FSM_RIC(EXT).1 Extended: Enrichment
FSM_RIC(EXT).1.1 The TSF shall use the configured enrichment sources to improve the value of SIEM event data.

Application Note: see section 7.1.2 for details of the (optional) enrichment sources that a user may employ.

FSM_STG(EXT).1 Extended: Prevention of data loss
FSM_STG(EXT).1.1 The TSF shall protect the stored SIEM event data from unauthorized deletion.
FSM_STG(EXT).1.2 The TSF shall protect the stored SIEM event data from modification.
FSM_STG(EXT).1.3 The TSF shall *ignore new SIEM event data* if the storage capacity has been reached.

FSM_ANL(EXT).1 Extended: Network event analysis
FSM_ANL(EXT).1.1 The TSF shall index SIEM event data according to configured indexing rules to facilitate analysis.
FSM_ANL(EXT).1.2 The TSF shall perform search, correlation based on user-defined search queries, and anomaly detection to perform analysis on stored SIEM event data.

Application Note: When UEBA is enabled and configured, TSF will perform anomaly detection on the selected SIEM event data.

FSM_ALT(EXT).1 Extended: Automatic alert
FSM_ALT(EXT).1.1 The TSF shall employ user-defined alerts to alert the assigned user upon detection of a potential security violation.

FSM_RPT(EXT).1 Extended: Report
FSM_RPT(EXT).1.1 The TSF shall deliver user-defined reports exported from Search to identified report recipients according to a defined delivery schedule.

FSM_MGI(EXT).1 Extended: Network incident management
FSM_MGI(EXT).1.1 The TSF shall track searches and correlations (using the incident dashboard) that are necessary to resolve an incident.

6.2 Security Assurance Requirements

The security assurance requirements for this Security Target are reproduced from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 3 (EAL3) augmented by ALC_FLR.1. Figure 10 summarizes the assurance requirements.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.3 Functional specification with complete summary
	ADV_TDS.2 Architectural design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.3 Authorization Controls
	ALC_CMS.3 Implementation representation CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_FLR.1 Basic flaw remediation
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification

ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

Figure 10 Security Assurance Requirements

6.3 Security Requirements Rationale

This section provides rationale for the Security Functional Requirements demonstrating that the SFRs are suitable to address the security objectives.

6.3.1 Security Functional Requirements for the TOE

The table in Figure 11 provides a high level mapping of coverage for each security objective for the TOE and the IT components of the operational environment.

Each SFR traces back to at least one security objective demonstrating that there are no spurious SFRs. Each security objective for the TOE has at least one SFR tracing to it and so the mapping is complete with respect to the security objectives for the TOE.

Below the table in Figure 11 is a discussion of the correspondence between the objectives and the SFRs that completes the rationale.

SECURITY OBJECTIVES / SECURITY FUNCTIONAL REQUIREMENT	O.AUDITS	O.AUTHENTICATE	O.ACCESS	O.OVERFLOW	O.MANAGE	O.SIEM_COLLECT	O.SIEM_ANALYZE	O.SIEM_MANAGE	O.EXPORT
FAU_GEN.1	X								
FAU_SAR.1	X								
FAU_SAR.2	X		X						
FAU_SAR.3	X								
FAU_STG.1	X		X						
FAU_STG.3	X								
FCS_CKM.1(A)									X
FCS_CKM.1(B)									X
FCS_CKM.2(A)									X
FCS_CKM.2(C)									X
FCS_CKM.4									X
FCS_COP.1(A)									X
FCS_COP.1(B)									X

SECURITY OBJECTIVES / SECURITY FUNCTIONAL REQUIREMENT	O.AUDITS	O.AUTHENTICATE	O.ACCESS	O.OVERFLOW	O.MANAGE	O.SIEM_COLLECT	O.SIEM_ANALYZE	O.SIEM_MANAGE	O.EXPORT
FCS_COP.1(C)									X
FDP_ACC.1			X						
FDP_ACF.1			X						
FIA_ATD.1		X							
FIA_UAU.2		X							
FIA_UID.2		X							
FIA_AFL.1(A)		X							
FIA_AFL.1(B)		X							
FMT_MOF.1(A)					X				
FMT_MOF.1(B)					X				
FMT_MSA.1					X				
FMT_MSA.3					X				
FMT_MTD.1(A)					X				
FMT_MTD.1(B)					X				
FMT_SMF.1					X				
FMT_SMR.1		X			X				
FTP_ITC.1									X
FSM_LOG(EXT).1						X			
FSM_RIC(EXT).1						X			
FSM_STG(EXT).1			X	X					
FSM_ANL(EXT).1							X		
FSM_ALT(EXT).1							X		
FSM_RPT(EXT).1							X		
FSM_MGI(EXT).1								X	

Figure 11 Matching Security Functional Requirements to TOE Security Objectives and IT-related OE objectives

O.AUDITS

Security-relevant events must be audited for the TOE [FAU_GEN.1]. Time stamps associated with an audit record must be reliable [OE.TIME]. The TOE must provide a capability to review audit records [FAU.SAR.1] but this must be restricted to user that have explicitly been given explicit read access [FAU_SAR.2]. The TOE must provide sorting of audit data [FAU_SAR.3]. The audit records in the stored audit trail must be protected from unauthorized deletion and modification [FAU_STG.1]. The TOE must

notify the LogPoint Administrator if the audit trails exceeds 90% disk space of each mounted partitions where audit data is stored [FAU_STG.3].

O.AUTHENTICATE
Users must be successfully identified [FIA_UID.2] and authenticated [FIA_UAU.2] before they can perform any TSF mediated actions. Users will then be associated the roles [FMT_SMR.1] and rights according the attributes associated with the user identity [FIA_ATD.1]. The TOE must display a captcha for each subsequent logon attempt when 3 failed authentication attempts occur [FIA_AFL.1(A)]. The TOE must respond accordingly when a user fails 5 authentication attempts by locking out the user account so an attacker cannot gain access and by notifying the administrator of the possible attack [FIA_AFL.1(B)].

O.ACCESS
The TOE must ensure restricted audit review [FAU_SAR.2] and protect the audit trail against unauthorized modifications [FAU_STG.1]. The access to user data is ensured by the Multiple Access Control SFP between the subjects and the objects and is applicable to all user actions [FDP_ACC.1] and [FDP_ACF.1]. Protection of SIEM event data from unauthorized deletion and modification must be ensured [FSM_STG(EXT).1]

O.OVERFLOW
The TOE must protect stored data from unauthorized deletion and modification, and also ignore SIEM event data if the storage capacity has been reached [FSM_STG(EXT).1] to ensure continuous operation of the SIEM.

O.MANAGE
Different management functions [FMT_SMF.1] and rights are given to different roles [FMT_SMR.1]. The management of security functions behavior is restricted to users [FMT_MOF.1(A)] and administrators [FMT_MOF.1(B)]; the management of security attributes (permissions) [FMT_MSA.1] and the static attribute initialization [FMT_MSA.3] is restricted to authorized administrators; there is also management of TSF data for user identities [FMT_MTD.1(A)] and user permissions [FMT_MTD.1(B)].

O.SIEM_COLLECT
The TOE must collect and store events [FSM_LOG(EXT).1], events that are enriched to improve the value of these events [FSM_RIC(EXT).1].

O.SIEM_ANALYZE
The TOE must index the collected and stored events to allow user-defined search queries and analysis [FSM_ANL(EXT).1]. By using UEBA, the TOE can also optionally employ anomaly detection techniques to perform analysis on the events. Based on the analysis the TOE must employ user-defined alerts to alert the assigned user upon detection of a potential security violation [FSM_ALT(EXT).1]. The TOE must then deliver user-defined reports to identified report recipients according to a defined delivery schedule [FSM_RPT(EXT).1].

O.SIEM_MANAGE
The TOE must track searches and correlations that are necessary to resolve incidents [FSM_MGI(EXT).1].

O.EXPORT

The TOE must provide a trusted channel to protect the event data from disclosure and modification when the event data is transmitted to another IT product [FTP_ITC.1] The trusted channel is provided using cryptographic primitives for identification and authentication, encryption and decryption and for key management [FCS_CKM.1(A), FCS_CKM.1(B), FCS_CKM.2(A),FCS_CKM.2(C), FCS_COP.1(A), FCS_COP.1(B), FCS_COP.1(C)]. Object reuse if used to ensure the protection of the keys [FCS_CKM.4].

6.3.2 Rationale for TOE Assurance Requirements Selection

The TOE stresses assurance through vendor actions that are within the bounds of current best commercial practice. The TOE provides, via review of vendor-supplied evidence, independent confirmation that these actions have been competently performed.

The general level of assurance for the TOE is:

1. Consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.
2. The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL3 from part 3 of the Common Criteria.
3. Consistent with current best practice for tracking and fixing flaws as well as providing fixes to customers.

The augmentation of ALC_FLR.1 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

6.3.3 CC Component Hierarchies and Dependencies

This section of the Security Target demonstrates that all of the SFRs hierarchical to or dependent on the identified SFRs are also included within the Security Target. Where there are dependencies outside of the TOE within the IT environment, a rationale as to how this dependency is satisfied is included.

SFR	HIERARCHICAL TO	DEPENDENCIES	DEPENDENCY SATISFIED	NOTES
FAU_GEN.1	No other components	FPT_STM.1	See note	Satisfied by OE.TIME in the IT environment.
FAU_STG.1	No other components	FAU_GEN.1	X	
FAU_STG.3	No other components	FAU_STG.1	X	
FAU_SAR.1	No other components	FAU_GEN.1	X	
FAU_SAR.2	No other components	FAU_SAR.1	X	
FAU_SAR.3	No other components	FAU_SAR.1	X	
FCS_CKM.1(A)	No other components	FCS_COP.1 FCS_CKM.4	See note	The FCS_COP.1 dependency is on FCS_COP.1(A).
FCS_CKM.1(B)	No other components	FCS_COP.1 FCS_CKM.4	See note	The FCS_COP.1 dependency is on FCS_COP.1(B).

SFR	HIERARCHICAL TO	DEPENDENCIES	DEPENDENCY SATISFIED	NOTES
FCS_CKM.2(A)	No other components	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	See note	Depends on FCS_CKM.4 and FCS_CKM.1
FCS_CKM.2(C)	No other components	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	See note	Certificates are not sensitive data so FCS_CKM.4 is not applicable. FCS_CKM.1 is also not applicable as RSA key are generated only once during initial installation.
FCS_CKM.4	No other components	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	See note	Depends on FCS_CKM.1
FCS_COP.1(A)	No other components	FCS_CKM.1 FCS_CKM.4	See note	The FCS_CKM.1 dependency is on FCS_CKM.1(A).
FCS_COP.1(B)	No other components	FCS_CKM.1 FCS_CKM.4	See note	The FCS_CKM.1 dependency is on FCS_CKM.1(B).
FCS_COP.1(C)	No other components	FCS_CKM.1 FCS_CKM.4	See note	FCS_CKM.1 is not applicable as RSA key are generated only once during initial installation. And FCS_CKM.4 is not applicable, as keys are not deleted.
FDP_ACC.1	No other components	FDP_ACF.1	X	
FDP_ACF.1	No other components	FDP_ACC.1 FMT_MSA.3	X	
FIA_ATD.1	No other components	None	X	
FIA_UAU.2	FIA_UAU.1	FIA_UID.1	See note	The FIA_UID.1 requirement is a subset of the FIA_UID.2 requirement.
FIA_UID.2	FIA_UID.1	None	X	
FIA_AFL.1(A)	No other components	FIA_UAU.1	X	
FIA_AFL.2(B)	No other components	FIA_UAU.1	X	
FMT_MOF.1(A)	No other components	FMT_SMR.1 FMT_SMF.1	X	
FMT_MOF.1(B)	No other components	FMT_SMR.1 FMT_SMF.1	X	
FMT_MSA.1	No other components	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	See note	Depends on FDP_ACC.1, FMT_SMR.1 and FMT_SMF.1

SFR	HIERARCHICAL TO	DEPENDENCIES	DEPENDENCY SATISFIED	NOTES
FMT_MSA.3	No other components	FMT_MSA.1 FMT_SMR.1	X	
FMT_MTD.1(A)	No other components	FMT_SMR.1 FMT_SMF.1	X	
FMT_MTD.1(B)	No other components	FMT_SMR.1 FMT_SMF.1	X	
FMT_SMF.1	No other components	None	X	
FMT_SMR.1	No other components	FIA_UID.1	See note	The FIA_UID.1 requirement is a subset of the FIA_UID.2 requirement.
FTP_ITC.1	No other components	None	X	
FSM_LOG(EXT).1	No other components	FPT_STM.1	See note	Satisfied by OE.TIME in the IT environment.
FSM_RIC(EXT).1	No other components	FSM_LOG(EXT).1	X	
FSM_STG(EXT).1	No other components	FSM_LOG(EXT).1	X	
FSM_ANL(EXT).1	No other components	FSM_LOG(EXT).1	X	
FSM_ALT(EXT).1	No other components	FSM_LOG(EXT).1 FSM_ANL(EXT).1	X	
FSM_RPT(EXT).1	No other components	FSM_LOG(EXT).1 FSM_ANL(EXT).1 FSM_MGI(EXT).1	X	
FSM_MGI(EXT).1	No other components	FSM_LOG(EXT).1 FSM_ANL(EXT).1	X	

Figure 12 SFR dependencies

7 TOE Summary Specification

The objective for the TOE summary specification is to provide potential consumers of the TOE with a description of how the TOE satisfies all the SFRs. The TOE summary specification provides the general technical mechanisms that the TOE uses for this purpose.

More details are provided in the guidance documents, specifically the Administrator Manual and the User Manual.

7.1 Security Information and Event Management

7.1.1 Log data collection and storage

Raw, unaltered log data is collected from across the enterprise and stored by the TOE.

Data can be collected from any network device that supports syslog, SNMP Trap or NetFlow, or that can send batch data using FTP.

LogPoint also supports other devices that require LogPoint to actively retrieve event information. For such devices, a dedicated fetcher polls the device for information at scheduled intervals.

The list of currently supported collectors and fetchers is given in section 1.4.1.1.1. The individual collectors and fetchers are outside the logical boundary of the TOE, which focuses on the raw data delivered by these collectors and fetchers. The FileSystem collector is however a special case as this is used to collect audit data and is part of the TOE.

Normalization applications focus on data from specific network devices:

- Windows
- Palo Alto
- Firewalls
- Cisco
- CheckPoint
- Active Directory
- “Default”

The normalization packages use knowledge about how log data is represented in specific networks or appliances in order to convert the collected log data to a standard form within the TOE.

Two copies of each item of event data are stored. The raw data is stored alongside the normalized data in a named repository. A Repository or “Repo” is a logical storage location within the TOE akin to a file.

Indexing is used to facilitate the search process.

This TSF is mapped to the following SFR: FSM_LOG(EXT).1

7.1.2 Enrichment

The TOE supports enrichment. Data is imported into tables within LogPoint from an external source. This allows the event data to be enhanced by cross-referencing information from the event data, such as a user name or IP address with a database that contains additional relevant information. So, a user name

from event data can be used as a key into an enrichment table to add a telephone number or geographical address to the event data, for instance. A number of different formats for enrichment data are supported: CSV, ODBC, LDAP, IPtoHost, GeoIp, and Threat Intelligence.

Other enrichment data such as mapping an IP address to a distinguished name using DNS can be done on an ad hoc basis as required or fetched periodically. Some other enrichment data that can be mapped on an ad hoc basis are Ascii Converter, Clean Char, Codec, Compare, Compare Network, Count Char, Current Time, DNS, DNS Cleanup, Evaluation (Eval), Experimental Median Quartile Quantile, InRange, IP Lookup, Lookup, and Randomize, and Regex.

This TSF is mapped to the following SFR: FSM_RIC(EXT).1

7.1.3 Prevention of data loss

The event data is stored as text files on the TOE hard drive. TOE users have no direct access to this storage. TOE users only have limited read access to the event data mediated by TOE functionality. The event data storage is managed by the operating system administrator.

If the TOE detects that the amount of available storage has dropped below a critical level, then the existing event data is retained, and new events are discarded. The default critical level is 90%. The TOE will issue a notification to alert LogPoint Administrators that there is a problem. Also the audit log of disk usage is generated and stored within TOE.

This TSF is mapped to the following SFR: FSM_STG(EXT).1

7.1.4 Analysis

The TOE indexes event data to facilitate searching. The event data is indexed as non-structured data. The Lucene library is used to provide full-text indexing. MongoDB is used as the database engine.

Signatures are rules to capture important field values from the raw logs. These field values are then indexed to simplify search, compare, aggregate, correlate and report on the log data. As with normalization, signatures use templates that embody knowledge of the underlying structure of raw data to extract key fields from that data.

Searches are used to power the analysis functions of the TOE.

There is a sophisticated, proprietary search language that the TOE supports. Within the syntax, there are a number of options to allow a user to build complex search queries:

- search for single words, multiple words and phrases
- field values
- logical operators, braces and wildcards can be used to structure queries and combine search elements
- numerical fields can be grouped
- time functions can be used to select event data based on when events occur
- search results can be displayed as lists, tables and charts
- other built-in functions

Searches can be made on an ad hoc basis, or any search can be converted into a permanent alert or dashboard. Searches can also be reported for easy future reference. Log analytics make it easy to display data in the best possible fashion.

Additionally, if UEBA is enabled, the event data can also be sent to the UEBA cluster for behavioral analytics of user and other entities (device, host, etc). The UEBA will provide an overview of the overall risk status of the network infrastructure and also displays the information for all the risky entities in the network. Filtering can be applied on the entities and anomalies for further inspection. UEBA also enables report generation using the data presented in the Overall Risk and Explore pages of the UEBA dashboard. The events responsible for anomaly can be explored by drilling down to search page from the anomalies window.

The built-in intelligent log analysis engine automatically detects and issues notifications of all critical incidents. Events monitored are dynamically defined within the system. Typical incidents might be: an ongoing attack; a compromised system; a system breakdown; or failed user authentication.

This includes an advanced labeling structure that allows for highly efficient log tagging.

This TSF is mapped to the following SFR: FSM_ANL(EXT).1

7.1.5 Alerts

The TOE alerts users in a number of ways:

- E-mail alerts for detected security incidents
- Integration into existing ticketing and support systems

Alerts are defined to continuously monitor data. Alert rules fire incidents that enable users to execute appropriate actions.

Alerts of different incidents are created directly from the execution of a search query. When configuring an alert as part of a search query, it is possible for a user to select how notification occurs: either via Email, Syslog, SSH, SNMP or HTTP. However, only notification via Email is included in the evaluated configuration.

This TSF is mapped to the following SFR: FSM_ALT(EXT).1

7.1.6 Reports

Common reporting templates for compliance such as PCI, SOX, ISO2700x, HIPAA and more are standard to the LogPoint solution – and can be modified or created from scratch using an intuitive LogPoint Report Wizard.

Reports can also be generated for a specific search and delivered to a configured email address according to a configured delivery schedule.

This TSF is mapped to the following SFR: FSM_RPT(EXT).1

7.1.7 Network incident management

The Dashboard displays critical events and security incidents in real-time and facilitates incident management. LogPoint presents information through a structured overview, where information can be

grouped into charts and graphs to make it easier for a human operator to quickly discern anomalous data to focus on for further investigation.

This TSF is mapped to the following SFR: FSM_MGI(EXT).1

7.2 Audit

7.2.1 Generation

The TSF generates an audit record of the following auditable events:

- Start-up and shutdown of the audit functions;
- All auditable events for the not specified level of audit; and
- User management
- Identification and authentication
- User actions
- Inter-TSF trusted channel
- System

The audit records of the above auditable events are collected by TOE using file system collector. The generated audit data is collected by the file system collector, normalized by the "_logpoint" normalization policy then indexed and stored under "_logpoint" repository.

For each log entry, the TOE stores the date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event. The audit functions within the TOE cannot be disabled. As long as the TOE is active, the audit functions are running.

This TSF is mapped to the following SFR: FAU_GEN.1

7.2.2 Review

Access to audit records is a user permission that can be assigned to a user only by authorized administrators of the TOE.

Audit records can be displayed, searched and ordered on any field. However, access to audit records is only accessible to an authorized user through the LogPoint Console.

The Authorized users could be any users that have been given permission to read all the audit information. The permission is managed using Universal Query and object Permission.

A universal query is a search item that can be used to restrict the set of data that a user has access to. It defines the extent of their universe with respect to the TSF data. Similarly, object permission allows users to search logs from only those repos and devices that are assigned to them. And all the audit logs are stored in "_logpoint" repo.

Sorting of audit data based on date and time, the type of event, the subject identity and the outcome of the event are handled by client side JavaScript and have no implication on the data in the server side.

The TSF is mapped to the following SFRs: FAU_SAR.1, FAU_SAR.2, FAU_SAR.3

7.2.3 Prevention of data loss

As previously described for event data in section 7.13 above, audit records cannot be modified, deleted by TOE users. They are written to storage and once stored, can be read by authorized users. By default LogPoint and audit data are stored in a single disk partition. In case a new disk is mounted, only audit data along with event data can be configured to be stored in that partition. In case, audit records exceeds 90% disk space of any of the above mentioned partitions where either LogPoint and audit data or only audit data are stored, TOE would notify the LogPoint Administrator. The predefined limit for notification by default is 90% and this is user configurable. In addition to sending a notification an audit log is also generated when the disk usage excess the predefined limit. After that notification and audit log is generated every hour. Users can also define multiple disk usage notification rules with custom disk usage percent and message.

The TSF is mapped to the following SFRs: FAU_STG.1, FAU_STG.3

7.3 Cryptographic Support

In case of OpenVPN, the client and the server are mutually authenticated using X.509 certificates. The DHE_RSA_AES256_SHA256 is the only supported TLS cipher suite for OpenVPN communication.

RSA 2048 bit private key is generated during the installation of the LogPoint and is not changed during the lifetime of the LogPoint Instance. A 2048 bit Diffie Hellman key is also generated during the same time using OpenSSL tool.

A X.509 digital certificate is also generated with the help of OpenSSL tools and it is signed with self-signed CA certificate shipped with the LogPoint. In this process, the SHA256 sum of the server digital certificate is calculated and the resulting value is signed with the CA private key. OpenSSL does this process and it complies with Digital Signature Generation with RSASSAPKCS1v1.5.

The RSA private key, X.509 SSL certificate and the Diffie Hellman key mentioned above are used during the OpenVPN communication.

In case of OpenVPN Communication, the OpenVPN Client initiates the connection with a cipher suite DHE_RSA_AES256_SHA256 defined in its configuration file and the Server also determine to use the same cipher suite. This communication is the part of TLSv1.2 handshake protocol.

After the initiation process, the server sends its certificate to the client as part of TLSv1.2 Handshake Protocol. This method of key certificate distribution meets X.509 version 3 standard.

In the next Step, the client sends Diffie Hellman parameters. This step takes place in accordance to Ephemeral Diffie-Hellman Key exchange used in TLSv1.2.

In the final step of TLSv1.2 handshake protocol client and the server calculates master secret key, which is used to encrypt the data in actual communication channel.

After the end of TLSv1.2 handshake protocol, the record protocol starts where the bulk data is encrypted with AES256 with CBC (Cipher Block Chaining) encryption algorithm and SHA256 is used as hashing algorithm.

After the OpenVPN session teardown, destruction of cryptographic keys is done using zeroization method as per the OpenSSL version 1.0.2g. Zeroization of cryptographic keys is performed automatically by API function calls of OpenSSL cryptographic library.

In case of UEBA, the UEBA connector and UEBA cluster are also mutually authenticated using X.509 certificates following the PKCS12 [PKCS12v1.1] PKI standard.

UEBA connector initiates the connection with an empty list of cipher suite as no explicit cipher suite is defined in its configuration. The UEBA cluster has explicitly defined the following list of supported cipher suites TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 in its configuration. Upon receiving connection request from UEBA connector any one of the above cipher suites will be used.

The TLS client certificate and its matching RSA 2048 bit private key is generated when the tenant is provisioned. They are enclosed in a password-protected PKCS12 file which is the keystore. Similarly, the CA certificate of the UEBA cluster is also generated during the same time and is enclosed inside another password-protected PKCS12 file which is the truststore. These two files along with the cloud.env configuration file are the contents of the Client Customer Package (zip).

The RSA public key and the X.509 SSL certificate mentioned above are used during the TLS handshake.

The TSF is mapped to the following SFRs: FCS_CKM.1(A), FCS_CKM.1(B), FCS_CKM.2(A),FCS_CKM.2(C), FCS_COP.1(A), FCS_COP.1(B), FCS_COP.1(C), FCS_CKM.4

7.4 User Data Protection

The TOE uses access control to ensure that users have appropriate access to the TSF. The access control policy also applies to the audit data (TSF data).

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 to all TOE users in the user groups Operator and Admin.

In LogPoint, User Groups setting item includes creating a group, configuring different permissions, and assigning users into appropriate groups. The group settings are applied to only the users in this group.

Similarly Permission Groups setting item gives the ability to define user permissions. An authorized LogPoint Administrator can control and manage features of LogPoint assigned to the authorized users. Also different permissions can be grouped into a permission group and, later assigned it to the user group.

Both User and Permission group details are stored in MongoDB.

The TSF is mapped to the following SFRs: FDP_ACC.1, FDP_ACF.1

7.5 Identification and Authentication

For each user, the TOE stores a user name, password, user group, name (first name and last name), email address and time zone.

This is stored within the MongoDB database, which is part of the TOE environment. The username and Permissions are stored in plain text, but the password is stored hashed using SHA-1. However, the attribute password is only in case the TOE is using LP password authentication and not when the TOE is using LDAP. In case of the LDAP, the password is maintained by LDAP Server.

Successful authentication is required prior to accessing user functionality. The user must present credentials in the form of user name and password to the TOE Console and have these verified. The TOE performs the authentication itself by verifying the credentials against values held in its database.

LDAP can also be used as a means of authenticating users. If an LDAP user wishes to gain access to the TOE, the TOE requests details of the user's group name. If this maps to one of the four LogPoint user groups (see section 1.4.1.5), then the user is granted appropriate access to the TOE. If the LDAP user does not belong to a LogPoint user group, then they are not permitted access to the TOE.

The TOE requires each user to be successfully identified using authentication before allowing any other TOE-mediated actions on behalf of that user.

In case of authentication failure with 3 unsuccessful authentication attempts, TOE would display a captcha for each subsequent logon attempt and require this to be completed correctly before the logon attempt is allowed. Similarly, in case of 5 unsuccessful authentication attempts, TOE would lock the user account for next 30 minutes after which user gets one additional logon attempt. If this logon attempt also fails, then the user account is locked for additional 30 minutes. This process continues until the user logon with valid credentials.

The TSF is mapped to the following SFRs: FIA_ATD.1, FIA_UID.2, FIA_UAU.2, FIA_AFL.1(A), FIA_AFL.1(B)

7.6 Management

Authorized users are able to create, destroy and configure their own alert and correlation rules, dashboards, and reports, saved searches, while they can only create and configure their own security incidents using the LogPoint Console via a browser. Similarly, authorized administrators are able to create, destroy and configure normalization rules.

Authorized administrators are able to create, destroy and modify user accounts and to assign permissions to these accounts up to and including their own access level.

The LogPoint Console suggests default access rights to new users when these are created using default values. The Console provides full Knowledge Base and Configuration access by default for all new users, but this can be altered by an authorized administrator.

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. 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.

The four TOE user groups (roles) and their associated permissions are as follows:

- LogPoint Administrator
  - Can perform system related tasks
  - User account administration
  - Full Knowledge Base and Configuration Permissions
  - User functions (search, dashboard, correlation, alerts, reports)
- User Account Administrator
  - User account administration
  - Full Knowledge Base and Configuration Permissions
  - User functions (search, dashboard, correlation, alerts, reports)
- Admin
  - Full Knowledge Base and Configuration Permissions
  - User functions (search, dashboard, correlation, alerts, reports)
- Operator
  - Read-only Knowledge Base and Configuration Permissions
  - User functions (search, dashboard, correlation, alerts, reports)

Both default user Groups (LogPoint Administrator and User Account Administrator) are created by running the Fixtures script by inserting the group details in the collection for User Groups in MongoDB.

Similarly, both default Permission Groups (Admin and Operator) are created by running the Fixtures script by inserting the Permission details in the collection for Permission Groups in MongoDB.

TOE functions are described in section 8

The TSF is mapped to the following SFRs: FMT_MOF.1(A), FMT_MOF.1(B), FMT_MSA.1, FMT_MSA.3, FMT_MTD.1(A), FMT_MTD.1(B), FMT_SMF.1, FMT_SMR.1

7.7 Trusted Channels

Whenever the TOE connects to a separate remote TOE for the purpose of transferring event data or configuring the remote TOE, OpenVPN establishes a virtual private network (VPN) for the purpose using 2048-bit RSA authentication within SSL. This ensures the confidentiality and integrity of TSF Data when it leaves the TOE boundary.

The TSF accept the connection from other LogPoint via a trusted channel. This is accomplished by enabling open door in the LogPoint. When the open door is enabled in a LogPoint it behaves as an OpenVPN server, listening on UDP port 1194 for connection request from the client.

The TSF also initiates a connection to other LogPoint via a trusted channel. This is done by configuring it as a distributed LogPoint. 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 DLP, this starts operating as an OpenVPN client.

OpenVPN on both sides, the Client and the Server, are configured with the specific TLS version, TLSv1.2 and a specific cipher suite, DHE_RSA_AES256_SHA256. Both sides uses X.509 certificate to mutually authenticate.

HTTP communication channel is used to transmit the UUID/Identifier of the client to the Server. The gunicorn server, which is listening on TCP port 18000 on the server side, responds to the request from the HTTP client and provides a static tunnel IP address that remain same each time the client connects to the server. This step is necessary to maintain the identity of the distributed LogPoint and consistency of data transfer between the server and the client should there be network connectivity issue during the data transfer. The HTTP communication is encapsulated inside the VPN tunnel therefore it is transparent to any firewall in front of the LogPoint instances.

In case of UEBA, when UEBA is enabled the TOE uses configuration present in the cloud.env file to identify the respective UEBA cluster and unlock the PKCS12 file using the passphrases. The TSF then uses the certificate present in the PKCS12 file of its keystore to authenticate itself to the cluster. Similarly, it uses the other PKCS12 file representing the truststore which contains the CA certificate of the cluster to authenticate the server and establish trust between the UEBA cluster and the LogPoint UEBA connector.

UEBA connector and UEBA cluster are configured with the specific TLS version, TLSv1.2 and UEBA cluster explicitly supports the cipher suites TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, however, no specific cipher suite is defined on UEBA connector.

The TSF is mapped to the following SFR: FTP_ITC.1

8 Appendix A - TOE Functions

A user performing user account administration can only administer users at the same level of user permission or below.

System functions are:

- System Monitor
- System Settings
- LogPoint License
- Updates
- Backup and Restore
    - Creation of configuration/repository backups and restore them as required
- Applications
- Open Door
    - Used for establishing a distributed LogPoint
- Plugins
- Sync
    - Import/Export configuration used for synchronization
- LogPoint Director
- Snapshots

Permissions:

- Knowledge Base
    - Normalization Packages (Read/Create/Delete)
    - Lists and Tables (Read/Create/Delete)
    - Fields (Read/Create/Delete)
    - Macros (Read/Create/Delete)
- Configuration
    - Devices, DeviceGroups, Log Collection Policy and Parsers (Read/Create/Delete)
    - Distributed Collectors (Read/Create/Delete)
    - Processing Policy (Read/Create/Delete)
    - Distributed LogPoints (Read/Create/Delete)
    - Export Management (Read/Create/Delete)
    - Raw Syslog Forwarder (Read/Create/Delete)

User functions are user specific, that is, if one user creates a dashboard or a report, it is specific to that user and is not available to any other user unless shared.

8.1 Users, roles and permissions

There are four roles defined for the TOE, as defined in section 6.1.5 that are associated with users.

However, there are a number of functions within the TOE that are similar to user roles and also ways of changing the permissions available to users that define their capabilities within the four basic roles.

Permission groups define site permissions. There are two default permission groups for an out of the box installation, admin (full access to knowledge base and configuration items) and operator (read-only access to knowledge base and configuration items). To operate in a manner that is compliant with this

Security Target (Common Criteria mode of operation), two user groups are created, the Operator user group is created using the operator permission group and Admin user group is created using the admin permission group.

The scope of permission groups is the knowledge base and configuration only. The scope of the user's access to event data can further be controlled using universal query. A universal query is a search item that can be used to restrict the set of data that a user has access to. It defines the extent of their universe with respect to the TSF data.

Certain administration functions within the TOE are performed by built-in "users". These maintenance operations are delivered by "li-admin" and the "support" user.

li-admin is an authenticated console-based function that requires the operator to be locally, physically present at the TOE, and so access to li-admin functionality is restricted by A.LOCATE. li-admin can perform a number of high level operations including:

- Reboot TOE
- Shutdown the TOE system
- Change the system IP address
- Start/Stop support
- Change system date/time
- Create a directory for repositories
- Upload a software patch
- Add/Remove Eth bonding
- TCP Dump
- Route
- Install VMware Tools
- Add/Remove Firewall ports
- Enable/Disable SSH users
- Mount/Unmount
- ZFS operations
- Create/Manipulate Interactive/Command-line GUID partition table
- Up/down network interface
- Change LogPoint identifier
- Create/delete/display disk partition
- Create filesystem on formatted storage device
- Retry log backup
- Change syslog SSL port
- Load kernel keymap for console
- Detect and coalesce multiple paths to devices
- Docker
- Change UEBA network (optional)
- Start/stop tuning of LogPoint services

The li-admin is not needed or used for the operation in the evaluated configuration.