Bastille Enterprise Fusion Center Version 3.6 Security Target

Document ID: UL15574582-ST

Version: 1.8

January 09, 2026

Prepared For:

Bastille Networks, Inc

499 Lake Ave,

Santa Cruz CA, 95062

Prepared By:

Dylan Lyman

UL Verification Services Inc.

Notices:

ST Change Log

Version	Date	Author	Changes
1.0	January 27, 2025	D. Lyman	Initial release
1.1	June 11, 2025	D. Lyman	Updates in response to NIAP validator comments
1.2	July 9, 2025	D. Lyman	Updates in response to round 1 ATE evaluator comments
1.3	July 28, 2025	D. Lyman	Updates in response to round 1 of ASE evaluator comments
1.4	October 2, 2025	D. Lyman	Fixed typos and updated TDs
1.5	October 28, 2025	D. Lyman	Updated SFR selections and list of packages
1.6	October 30, 2025	D. Lyman	Minor updates
1.7	December 22, 2025	C. Sepulveda	Minor updates
1.8	January 09, 2026	C. Sepulveda	Minor updated for ECR

Table of Contents

1. Security Target (ST) Introduction

This Security Target (ST) is the statement of security needs for the specified Target of Evaluation (TOE). The structure of this document is defined by CC v3.1r5 Part 1 Annex A.2, “Mandatory contents of an ST”:

- Section 1 contains the ST Introduction, including the ST reference, Target of Evaluation (TOE) reference, TOE overview, and TOE description.
- Section 2 contains conformance claims to the Common Criteria (CC) version, Protection Profile (PP) and package claims, as well as rationale for these conformance claims.
- Section 3 contains the security problem definition, which includes threats, Organizational Security Policies (OSP), and assumptions that must be countered, enforced, and upheld by the TOE and its operational environment.
- Section 4 contains statements of security objectives for the TOE, and the TOE operational environment as well as rationale for these security objectives.
- Section 5 contains definitions of any extended security requirements claimed in the ST.
- Section 6 contains the security function requirements (SFR), the security assurance requirements (SAR), as well as the rationale for the claimed SFR and SAR.
- Section 7 contains the TOE summary specification, which includes the detailed specification of the IT security functions.

1.1 Security Target Reference

The Security Target reference shall uniquely identify the Security Target.

ST Title:	Bastille Enterprise Fusion Center Version 3.6 Security Target
ST Version Number:	1.8
ST Author(s):	Dylan Lyman
ST Publication Date:	January 09, 2026
Keywords	Application Software

1.2 Target of Evaluation Reference

TOE Developer:	Bastille Networks, Inc. 499 Lake Ave, Santa Cruz CA, 95062
TOE Name:	Bastille Enterprise Fusion Center
TOE Version:	3.6

1.3 Target of Evaluation Overview

1.3.1 TOE Product Type

The TOE is classified as Application Software running in a virtual appliance.

1.3.2 TOE Usage

The Bastille Enterprise Fusion Center analyzes observed wireless device data to detect devices, their metadata, and their locations (the data collection component is not part of the evaluation). The Fusion Center provides real time feeds of this enriched device data. This data enables users to make security decisions by leveraging the real time wireless device inventory the Fusion Center provides and site policies of the organization. Sites can include one or more floors of a building, multiple buildings, or entire organization campuses.

The Fusion Center provides secure access to the data through the use of APIs available to users via the TLS/HTTPS protected network connections. There are several web-based (single page) applications that are built into the TOE and these are built exclusively with the aforementioned APIs. Usage of these APIs is outside of scope of this evaluation. The TOE can optionally also provide notifications to subscriber applications through the use of webhooks via secured TLS/HTTPS protocol. Webhook subscribers are outside the scope of the evaluation (except for the TOE's configuration of webhook endpoints and the TOE's protected transmission of notifications to those endpoints).

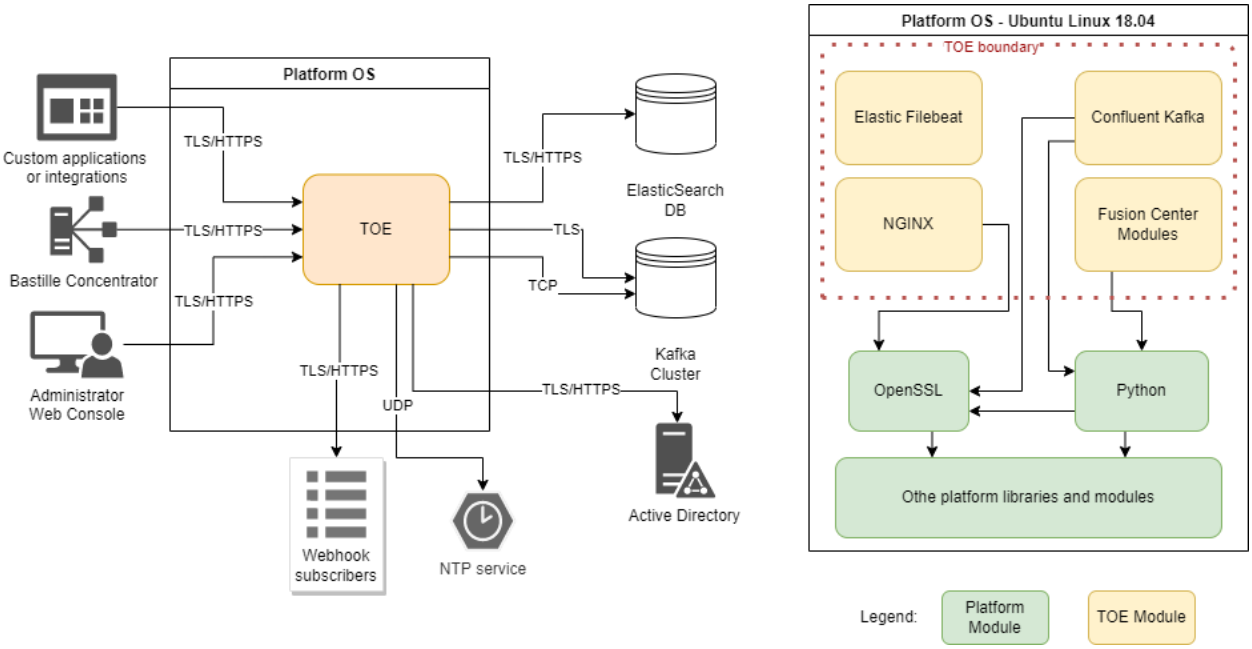

Figure 1: TOE and TOE Environment

1.3.3 TOE Major Security Features Summary

TOE performs secure collection, processing and presentation of data collected on customer location. Security of this functions is ensured by the following TOE security features, further detailed in TOE Logical Scope section below:

- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Privacy
- Protection of the TSF
- Trusted Path/Channel

1.3.4 TOE IT environment hardware/software/firmware requirements

IT environment should contain the following hardware and services that are not considered parts of the TOE, but required for correct functioning of the TOE:

Table 1: Non-TOE Software and Hardware		
Component	Purpose	Specific Requirements.
Bastille Concentrator or other compatible data source	Source of data for the TOE.	Support of the TOE API
Network equipment	Enabling TOE connection to non-TOE entities listed in this table over network.	None
Microsoft Windows Server 2019, running Active Directory Federation Service (MS ADFS)	Authentication that uses OAuth, specifically, OIDC.	Microsoft Windows Server 2019 or 2022
NTP Server	Synchronizes the clocks on computers and networks across the Internet.	Any NTPv4-compliant server
VMware ESXi Virtualization Server (vCenter®, vSphere®)	Hosts Fusion Center virtual appliance.	VMware ESXi 7 or higher (Virtual Hardware Version 17 or higher) running Intel® Xeon® Gold 6242 CPU @ 2.80GHz. Minimum virtual machine resources: − 32 GB RAM − 100 GB disk (local to VM) − 100 GB network mounted partition (NFS/external to VM)
Database Elasticsearch Cluster	Storage for data, data at rest.	Version 7.12 or higher 500 GB storage for index data
Data Queue Apache Kafka	Ephemeral data buffer or queue.	Version 2.7.0 or higher 20 GB storage or higher Minimum retention: 2 days

The TOE is running on Ubuntu Linux LTS 18.04 and 22.04, running on VMware ESXI Virtualization Server. Ubuntu Linux is not part of the TOE but is provided together with the TOE as a virtual appliance. Ubuntu Pro ESM long term support (LTS) subscription is prepaid by Bastille.

1.4 Target of Evaluation Description

1.4.1 Physical Scope

The TOE consists of the following modules and scripts: core Fusion Center Modules, NGINX web server, Elastic Filebeat, Confluent Kafka Python client, libraries as described in Appendix B.

The TOE is delivered to the customer in the form of a virtual appliance with all TOE parts already pre-installed to the /opt/bastille folder in a virtual appliance virtual drive. The appliance is provided through the developer support website, https://bastille.net/support/, and contacting Bastille support, to receive the VM in the OVA file format. Appliance integrity is verified using a digital signature of the file.

The TOE runs on an Ubuntu Linux LTS 18.04 or 22.04 virtual machine running on a VMware ESXI virtualization server.

The Guidance documentation that is part of the TOE is listed in Section 9 “References” within Table 9: TOE Guidance.

Guidance documentation is delivered to the customer in the form of PDF documents through the developer support website together with the appliance.

1.4.2 Logical Scope

The logical security features of the TOE are listed in Section 1.3.3 above and are further described in the following subsections. A more detailed description of the implementation of these security functions are provided in Section 7 “TOE Summary Specification”.

1.4.2.1 Cryptographic Support

The TOE does not directly perform cryptographic services, but rather calls the platform-provided crypto library, so cryptographic operations are out of the TOE logical scope.

1.4.2.2 User Data Protection

The TOE protects confidential data using platform provided mechanisms and does not collect sensitive information from the platform or users. The TOE restricts its access to platform resources to network connections.

1.4.2.3 Identification and Authentication

The TOE uses x509 certificates to verify the authenticity of the remote services when initiating secure communications with them.

1.4.2.4 Security Management

The TOE provides security management functionality for users to perform initial configuration and to configure external connections. Configuration is stored in a way recommended by the platform. The TOE requires users to change the built-in OS credentials during initial configuration of the TOE. TOE configures file permissions for its binaries to protect from modification by unprivileged users.

1.4.2.5 Privacy

The TOE does not collect or transmit Personal Identifiable Information.

1.4.2.6 Protection of the TSF

The TOE employs built-in anti-exploitation capabilities and uses only supported platform APIs and a limited number of 3rd party libraries. The TOE uses SemVer format to track TOE versions.

The TOE provides its current version number and capabilities to check for existing updates to the TOE. The TOE is distributed with the OS as a Virtual Appliance, and updates are distributed as a complete virtual appliance image.

1.4.2.7 Trusted Path/Channels

The TOE performs encryption of transmitted sensitive data using platform provided functionality.

1.5 Notation, formatting, and conventions

The notation, formatting, and conventions used in this Security Target are defined below; these styles and clarifying information conventions were developed to aid the reader.

Where necessary, the ST author has added application notes to provide the reader with additional details to aid understanding; they are italicized and usually appear following the element needing clarification.

The CC permits four SAR and SFR component operations (assignment, iteration, refinement, and selection) to be performed. These operations defined in Common Criteria, Part 1; section 8.1, are:

- Iteration: allows a component to be used more than once with varying operations;
- Assignment: allows the specification of parameters;
- Selection: allows the specification of one or more items from a list; and
- Refinement: allows the addition of details.

The notation conventions that refer to iterations, assignments, selections, and refinements made in this Security Target are in reference to SARs and SFRs taken directly from CC Part 2 and Part 3 as well as from the Protection Profiles, modules, packages and extensions this ST claims conformance to.

Iterations are indicated by an identifier or number in parenthesis following the requirement number, e.g., FIA_X509_EXT.1.1(Server); the iterated requirement titles are similarly indicated, e.g., FIA_X509_EXT.1(Server).

Assignments made by the ST author are identified with **[bold text].**

Selections are identified with [underlined text]**.** Selections within selections are identified with [double underlined text].

Refinements that add text use ***bold and italicized text*** to identify the added text***.*** Refinements that performs a deletion, identify the deleted text with ***~~strikeout, bold, and italicized text~~***.

2. Conformance Claims

2.1 Common Criteria Conformance Claims

This Security Target and TOE are conformant to the Common Criteria Version 3.1 Revision 5, CC Part 2 extended [C2], and CC Part 3 extended [C3].

2.2 Conformance to Protection Profiles

This Security Target claims exact conformance to the Protection Profile for Application Software, Version 1.4, dated 2021-10-07 [PP]. This Protection Profile will be referred to as PP for convenience throughout this Security Target.

The TOE conforms with the following related NIAP Technical Decisions:

Table 2 Technical Decisions implemented

Technical Decision	Details
0964 -Clarifications to FMT_MEC_EXT.1 Windows Test	Clarification of test activity, not applicable to ST
0945 – Adding FIPS 186-5 in PP_APP_V1.4	SFR not included in ST
0931 – Clarification when CTR_DRBG is Selected for FCS_RBG_EXT.2.2 in PP_APP_V1.4	SFR not included in ST
0914 – Addition of PKG_TLS_V2.0 to Conformance Claims	Package not supported by the TOE, not applicable to ST
0865 – Consistency of Cryptographic Key Sizes	SFR, FCS_STO_EXT.1.1
0844 – Addition of Assurance Package for Flaw Remediation V1.0 Conformance Claim	PP modification, not applicable to ST
0823 – Update to Microsoft Windows Exploit Protection link in FPT_AEX_EXT.1.3	Additional test activity, not applicable to ST
0822 – Correction to Windows Manifest File for FDP_DEC_EXT.1	Additional test activity, not applicable to ST
0815 – Addition of Conditional TSS Activity for FPT_AEX_EXT.1.5	Additional TSS evaluation activity, considered for ST generation
0798 – Static Memory Mapping Exceptions	Additional TSS evaluation activity, considered for ST generation
0780 – FIA_X509_EXT.1 Test 4 Clarification	Modification to test activity, not applicable to ST
0756 – Update for platform-provided full disk encryption	Modification to test activity, not applicable to ST
0747 – Configuration Storage Option for Android	Platform is not Android
0743 – FTP_DIT_EXT.1.1 Selection exclusivity	SFR, FTP_DIT_EXT.1, was modified to include assignment.
0736 – Number of elements for iterations of FCS_HTTPS_EXT.1	SFR not included in the ST
0719 – ECD for PP APP V1.3 and 1.4	PP modification, not applicable to ST
0717 – Format changes for PP_APP_V1.4	SFRs not included in the ST
0664 – Testing activity for FPT_TUD.2.2	SFR not included in the ST
0650 – Conformance claim sections updated to allow for MOD_VPNC_V2.3 and 2.4	Not part of conformance claims
0628 – Addition of Container Image to Package Format	SFR not included in the ST

2.3 Conformance to Security Packages

This Security Target does not claim conformance to any security function requirements or security assurance requirements packages, neither as package-conformant or package-augmented.

This Security Target does not claim conformance to any PP modules.

2.4 Conformance Claims Rationale

This ST claims exact conformance and as such no conformance claims rationale is required. The threats, OSPs, assumptions and security objectives are identical to the PP this ST is conformant to.

3. Security Problem Definition

3.1 Threats

This section defines the security threats for the TOE, characterized by a threat agent, an asset, and an adverse action of that threat agent on that asset. These threats are taken directly from the PP unchanged.

T.NETWORK_ATTACK

An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with the application software or alter communications between the application software and other endpoints in order to compromise it.

T.NETWORK_EAVESDROP

An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between the application and other endpoints.

T.LOCAL_ATTACK

An attacker can act through unprivileged software on the same computing platform on which the application executes. Attackers may provide maliciously formatted input to the application in the form of files or other local communications.

T.PHYSICAL_ACCESS

An attacker may try to access sensitive data at rest.

3.2 Organizational Security Policies

There are no Organizational Security Policies for the application.

3.3 Assumptions

This section describes the assumptions on the operational environment in which the TOE is intended to be used. It includes information about the physical, personnel, and connectivity aspects of the environment. The operational environment must be managed in accordance with the provided Guidance. The following defines specific conditions that are assumed to exist in an environment where the TOE is deployed. These assumptions are taken directly from the PP unchanged.

A.PLATFORM

The TOE relies upon a trustworthy computing platform with a reliable time clock for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE.

A.PROPER_USER

The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy.

A.PROPER_ADMIN

The administrator of the application software is not careless, willfully negligent or hostile, and administers the software in compliance with the applied enterprise security policy.

4. Security Objectives

4.1 Security Objectives for the TOE

O.INTEGRITY

Conformant TOEs ensure the integrity of their installation and update packages, and also leverage execution environment-based mitigations. Software is seldom, if ever, shipped without errors. The ability to deploy patches and updates to fielded software with integrity is critical to enterprise network security. Processor manufacturers, compiler developers, execution environment vendors, and operating system vendors have developed execution environment-based mitigations that increase the cost to attackers by adding complexity to the task of compromising systems. Application software can often take advantage of these mechanisms by using APIs provided by the runtime environment or by enabling the mechanism through compiler or linker options.

O.QUALITY

To ensure quality of implementation, conformant TOEs leverage services and APIs provided by the runtime environment rather than implementing their own versions of these services and APIs. This is especially important for cryptographic services and other complex operations such as file and media parsing. Leveraging this platform behavior relies upon using only documented and supported APIs.

O.MANAGEMENT

To facilitate management by users and the enterprise, conformant TOEs provide consistent and supported interfaces for their security-relevant configuration and maintenance. This includes the deployment of applications and application updates through the use of platform-supported deployment mechanisms and formats, as well as providing mechanisms for configuration. This also includes providing control to the user regarding disclosure of any PII.

O.PROTECTED_STORAGE

To address the issue of loss of confidentiality of user data in the event of loss of physical control of the storage medium, conformant TOEs will use data-at-rest protection. This involves encrypting data and keys stored by the TOE in order to prevent unauthorized access to this data. This also includes unnecessary network communications whose consequence may be the loss of data.

O.PROTECTED_COMMS

To address both passive (eavesdropping) and active (packet modification) network attack threats, conformant TOEs will use a trusted channel for sensitive data. Sensitive data includes cryptographic keys, passwords, and any other data specific to the application that should not be exposed outside of the application.

4.2 Security Objectives for the Operational Environment

The following security objectives for the operational environment assist the TOE in correctly providing its security functionality. These track with the assumptions about the environment.

OE.PLATFORM

The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying operating system and any discrete execution environment provided to the TOE.

OE.PROPER_USER

The user of the application software is not willfully negligent or hostile, and uses the software within compliance of the applied enterprise security policy.

OE.PROPER_ADMIN

The administrator of the application software is not careless, willfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy.

5. Extended Components Definition

As stated in Section 2, this Security Target claims exact conformance to the referenced PP. As such, the extended components definition is contained in the PP.

6. Security Requirements

This section describes the security functional and assurance requirements for the TOE.

6.1 Security Function Requirements

This section describes the functional requirements for the TOE. Operations that were performed in the PP are not signified in this section. Operations performed by the ST are denoted according to the formatting conventions in Section 1.5.

Table 3: Security Functional Requirements	
SFR	Description
FCS_CKM_EXT.1	Cryptographic Key Generation Services
FCS_RBG_EXT.1	Random Bit Generation Services
FCS_STO_EXT.1	Storage of Credentials
FDP_DAR_EXT.1	Encryption of Sensitive Application Data
FDP_DEC_EXT.1	Access to Platform Resources
FDP_NET_EXT.1	Network Communications
FIA_X509_EXT.1	X.509 Certificate Validation
FIA_X509_EXT.2	X.509 Certificate Authentication
FMT_CFG_EXT.1	Secure by Default Configuration
FMT_MEC_EXT.1	Supported Configuration Mechanism
FMT_SMF.1	Specification of Management Functions
FPR_ANO_EXT.1	User Consent of Transmission of Personally Identifiable Information
FPT_AEX_EXT.1	Anti-Exploitation Capabilities
FPT_API_EXT.1	Use of Supported Services and APIs
FPT_IDV_EXT.1	Software Identification and Versions
FPT_LIB_EXT.1	Use of Third Party Libraries
FPT_TUD_EXT.1	Integrity for Installation and Update
FTP_DIT_EXT.1	Protection of Data in Transit

6.1.1 Cryptographic Support (FCS)

6.1.1.1 FCS_CKM.1 Cryptographic Key Generation Services

FCS_CKM.1.1

The application shall [

- generate no asymmetric cryptographic keys].

6.1.1.2 FCS_RBG_EXT.1 Random Bit Generation Services

FCS_RBG_EXT.1.1

The application shall [

- Use no DRBG functionality

] for its cryptographic operations.

6.1.1.3 FCS_STO_EXT.1 Storage of Credentials

FCS_STO_EXT.1.1

The application shall [

- invoke the functionality provided by the platform to securely store [**TLS server private key**]

] to non-volatile memory.

6.1.2 User Data Protection (FDP)

6.1.2.1 FDP_DEC_EXT.1 Access to Platform Resources

FDP_DEC_EXT.1.1

The application shall restrict its access to [

- network connectivity

].

FDP_DEC_EXT.1.2

The application shall restrict its access to [

- no sensitive information repositories

].

6.1.2.2 FDP_NET_EXT.1 Network Communications

FDP_NET_EXT.1.1

The application shall restrict network communication to [

- user-initiated communication for [**updates availability check**],
- respond to [**connections from data source devices, users and custom applications to TOE API**],
- [**application-initiated connections to CRL servers, Elasticsearch Database Server, Apache Kafka server, Active Directory Server, event feed subscribers**]

].

6.1.2.3 FDP_DAR_EXT.1 Encryption of Sensitive Application Data

FDP_DAR_EXT.1.1

The application shall [

- protect sensitive data in accordance with FCS_STO_EXT.1

] in non-volatile memory.

6.1.3 Identification and Authentication (FIA)

6.1.3.1 FIA_X509_EXT.1 X.509 Certificate Validation (Selection-based)

FIA_X509_EXT.1.1

The application shall [invoke platform-provided functionality] to validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certificate path validation.
- The certificate path must terminate with a trusted CA certificate.
- The application shall validate a certificate path by ensuring the presence of the basicConstraints extension and that the CA flag is set to TRUE for all CA certificates and that any path constraints are met.
- The application shall validate that any CA certificate includes caSigning purpose in the key usage field.
- The application shall validate the revocation status of the certificate using [CRL as specified in RFC 5280 Section 6.3].
- The application shall validate the extendedKeyUsage (EKU) field according to the following rules:
    - Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
    - Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the EKU field.
    - Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the EKU field.
    - S/MIME certificates presented for email encryption and signature shall have the Email Protection purpose (id-kp 4 with OID 1.3.6.1.5.5.7.3.4) in the EKU field.
    - OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the EKU field.
    - Server certificates presented for EST shall have the CMC Registration Authority (RA) purpose (id-kp-cmcRA with OID 1.3.6.1.5.5.7.3.28) in the EKU field.

FIA_X509_EXT.1.2

The application shall treat a certificate as a CA certificate only if the basicConstraints extension is present and the CA flag is set to TRUE.

6.1.3.2 FIA_X509_EXT.2 X.509 Certificate Authentication (Selection-based)

FIA_X509_EXT.2.1

The application shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [HTTPS, TLS].

FIA_X509_EXT.2.2

When the application cannot establish a connection to determine the validity of a certificate, the application shall [not accept the certificate].

6.1.4 Security Management (FMT)

6.1.4.1 FMT_CFG_EXT.1 Secure by Default Configuration

FMT_CFG_EXT.1.1

The application shall provide only enough functionality to set new credentials when configured with default credentials or no credentials.

FMT_CFG_EXT.1.2

The application shall be configured by default with file permissions which protect the application binaries and data files from modification by normal unprivileged users.

6.1.4.2 FMT_MEC_EXT.1 Supported Configuration Mechanism

FMT_MEC_EXT.1.1

The application shall [

- invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.]

6.1.4.3 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions [

- **set up connections to external webhook subscribers**

].

6.1.5 Privacy (FPR)

6.1.5.1 FPR_ANO_EXT.1 User Consent of Transmission of Personally Identifiable Information

FPR_ANO_EXT.1.1

The application shall [

- not transmit PII over a network

] .

6.1.6 Protection of the TSF (FPT)

6.1.6.1 FPT_API_EXT.1 Use of Supported Services and APIs

FPT_API_EXT.1.1

The application shall use only documented platform APIs.

6.1.6.2 FPT_AEX_EXT.1 Anti-Exploitation Capabilities

FPT_AEX_EXT.1.1

The application shall not request to map memory at an explicit address except for [**no exceptions**].

FPT_AEX_EXT.1.2

The application shall [

- not allocate any memory region with both write and execute permissions]

] .

FPT_AEX_EXT.1.3

The application shall be compatible with security features provided by the platform vendor.

FPT_AEX_EXT.1.4
The application shall not write user-modifiable files to directories that contain executable files unless explicitly directed by the user to do so.

FPT_AEX_EXT.1.5
The application shall be built with stack-based buffer overflow protection enabled.

6.1.6.3 FPT_IDV_EXT.1 Software Identification and Versions
FPT_IDV_EXT.1.1

The application shall be versioned with [[**Semantic Versioning ("SemVer") version format**]]

6.1.6.4 FPT_LIB_EXT.1 Use of Third Party Libraries
FPT_LIB_EXT.1.1

The application shall be packaged with only [**3rd party libraries as listed in Appendix B**].

6.1.6.5 FPT_TUD_EXT.1 Integrity for Installation and Update
FPT_TUD_EXT.1.1

The application shall [provide the ability] to check for updates and patches to the application software.

FPT_TUD_EXT.1.2
The application shall [provide the ability] to query the current version of the application software.

FPT_TUD_EXT.1.3
The application shall not download, modify, replace or update its own binary code.

FPT_TUD_EXT.1.4
Application updates shall be digitally signed such that the application platform can cryptographically verify them prior to installation.

FPT_TUD_EXT.1.5
The application is distributed [with the platform OS]

6.1.7 Trusted path/channels (FTP)

6.1.7.1 FTP_DIT_EXT.1 Protection of Data in Transit
FTP_DIT_EXT.1.1[1]

The application shall [
- invoke platform-provided functionality to encrypt all transmitted sensitive data with [HTTPS, TLS] for [**external API communication and database access**].

] between itself and another trusted IT product.

[1] TD0743 has been applied.

6.2 Security Assurance Requirements

The TOE satisfies Security Assurance requirements as required by the [PP]. The TOE claims conformance to:

Table 4: Security Assurance Requirements	
SAR	Description
ADV_FSP.1	Basic functional specification
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.1	Labeling of the TOE
ALC_CMS.1	TOE CM coverage
ALC_TSU_EXT.1	Timely Security Updates
ASE_CCL.1	Conformance claims
ASE_ECD.1	Extended components definition
ASE_INT.1	ST introduction
ASE_OBJ.1	Security objectives for the operational environment
ASE_REQ.1	Stated security requirements
ASE_TSS.1	TOE summary specification
ATE_IND.1	Independent testing – conformance
AVA_VAN.1	Vulnerability survey

7. TOE Summary Specification

This section provides evaluators and potential consumers of the TOE with a high-level description of each SFR, thereby enabling them to gain a general understanding of how the TOE is implemented. These descriptions are intentionally not overly detailed, thereby disclosing no proprietary information. These sections refer to SFRs defined in Section 6.1.

The TOE consists of the following Security Functions:

- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Privacy
- Protection of the TSF
- Trusted Path/Channels

7.1 Cryptographic Support

7.1.1 Cryptographic Key Generation

The TOE does not directly generate asymmetric keys. Asymmetric keys used in a HTTPS/TLS connection as server certificates are generated outside of the TOE by the administrator and are imported to the TOE during the initial configuration process. Asymmetric keys that are used as part of the TLS handshake process are generated without TOE control by the underlaying platform cryptographic module that implements TLS encryption and decryption, as described in Section 7.7 below.

FCS_CKM_EXT.1.1

7.1.2 Random Bit Generation Services

The TOE does not directly use a DRBG to support TSF. A DRBG is called by the underlying platform cryptographic module that implements TLS encryption and decryption, as described in Section 7.1.4 below.

FCS_RBG_EXT.1.1

7.1.3 Storage of Credentials (Selection-based)

The TOE uses a Linux Keyring to securely store the TLS server private key. The TOE does not store other credentials in non-volatile memory. To authenticate external users, the TOE relies on JSON Web Tokens authorized by Active Directory Services and does not verify credentials based on locally stored values or keys. To verify JWT validity the TOE will establish a connection to the ADFS service, as described in section 7.7 below. Verification of credentials is out of the scope of the evaluation. Signature verification of the JWT token is performed by platform-provided OpenSSL crypto library.

FCS_STO_EXT.1

7.1.4 Platform provided cryptographic services.

The TOE relies on the platform-provided OpenSSL module to perform trusted channel encryption and other required cryptographic operations as required by the TOE.

7.2 User Data Protection

7.2.1 Encryption of Sensitive Application Data

The TOE does not store sensitive data other than TLS Server private keys in non-volatile memory. This is covered by FCS_STO_EXT.1.

FDP_DAR_EXT.1

7.2.2 Network Connectivity

The TOE uses the network to perform its primary functionality – receiving, processing, storing, and presenting of data.

The TOE accepts incoming network communications on port 443 using TLS protocol for:

- API or Web Interface Users
- Data collection from Concentrator (or other compatible data source devices)

The TOE establishes outgoing network connections to:

- MS AFDS Service for access token verification
- ElasticSearch database to store data
- Kafka cluster to queue messages for processing
- External applications using webhooks
- Developer portal to perform version check
- Kafka to send performance logs
- CRL server for revocation checking

FDP_NET_EXT.1

7.3 Identification and Authentication

7.3.1 Digital certificates for TLS and HTTPS

The TOE uses x509 certificates to verify the authenticity of remote servers that it connects to. The TOE uses the platform-provided OpenSSL module to perform the certificate validation checks in accordance with RFC 5280. Validation is performed for every certificate in the certificate trust chain up to the root certificate that is stored in the platform-managed root store. The TOE will reject a certificate without key usage or an incorrect key usage field. A revocation check for certificates is performed using CRLs as per RFC 5280 Section 6.3. If revocation status is impossible to verify, the certificate is considered invalid.

TOE uses only one certificate chain configured by the administrator. Section 6 of administrative guidance [G1] describes how to upload those certificates to the trust store during TOE configuration.

FIA_X509_EXT.1, FIA_X509_EXT.2

7.4 Security Management

7.4.1 Secure by Default Configuration

The TOE uses no credentials. The Application cannot be used until initial configuration has been performed. The customer is expected to follow the user guidance to perform initial configuration and secure the underlying OS.

FMT_CFG_EXT.1

7.4.2 Supported Configuration Mechanism

The TOE stores the following settings on the platform:

- List of domain names of external non-TOE entities the TOE will need to perform a network connection when functioning as listed in FDP_NET_EXT.1:
  - NTP server FQDN or IP
  - ADFS server FQDN or IP
  - ADFS web application id value
  - Kafka Server FQDN or IP
- Domain names the TOE will be using to accept incoming connections
- x509 certificates and private key for use with TLS connections, defined in FTP_DIT_EXT.1
  - X.509 certificate chain / certificates are stored in /var/lib/bastille/etc/certs/
  - TLS server private key stored in the Linux keyring (persists across reboots)

These settings are created at initial deployment and are not modified during normal operation. These configuration files are stored in /var/lib/bastille/ and /etc/opt/bastille/.

Settings for connection to external webhooks subscribers are stored by the TOE in the Elasticsearch database.

FMT_MEC_EXT.1

7.4.3 Management functions.

When the TOE is installed and initial configuration is performed, connection details for external IT entities are provided, together with hostnames for the services the TOE will be providing and TLS certificates that these services will be using. Those settings can be changed only when the TOE is re-initialized. During normal TOE operation, an authorized user can only enable and configure connection details for external webhooks subscribers using the web-interface provided by the TOE.

FMT_SMF.1

7.5 Privacy

7.5.1 User Consent of Transmission of Personally Identifiable Information

The TOE does not request or collect Personally Identifiable Information from the users.

FPR_ANO_EXT.1

7.6 Protection of the TSF

7.6.1 Anti-Exploitation Capabilities

The TOE consists of Python scripts and several compiled binaries and libraries. Binary code has been compiled using compilation flags to ensure exploit prevention capabilities:

Table 5: TOE module compilation flags

TOE Modules	Compilation flags
NGINX	C language compilation flags: -g -O2 -fdebug-prefix-map=/<<PKGBUILDDIR>>=. -fstack-protector-strong -Wformat -Werror=format-security -g -O2 -fdebug-prefix-map=/<<PKGBUILDDIR>>=. -fstack-protector-strong -Wformat -Werror=format-security -fPIC -Wdate-time

	-D_FORTIFY_SOURCE=2
FileBeat	GO language compilation flags: -D_FORTIFY_SOURCE=2 -O3 -fstack-protector-all CGO_ENABLED:1 -buildmode=pie -ldflags -s -linkmode=external -X
Confluent	C++ compilation flags: -g -O2 -fPIC -Wall -Wsign-compare -Wfloat-equal -Wpointer-arith -Wcast-align

In the table above "-fPIC" and "buildmode=pie" ensure binaries are compiled with ASLR support.

The underlying platform (Ubuntu 18.04 or 22.04) is able to perform ASLR when running TOE binaries. Python scripts are not susceptible to buffer overflow attacks.

The TOE does not interfere with the AppArmor security feature of the Linux platform.

FPT_AEX_EXT.1

7.6.2 Use of Supported Services and APIs

The TOE uses only documented APIs provided by the platform. The list is provided in Appendix A.

FPT_API_EXT.1

7.6.3 Software Identification and Versions

The TOE uses Semantic Versioning ("SemVer") versioning methodology to track TOE versions Major.Minor.Patch (e.g. 2.1.0). (For more on SemVer see https://semver.org/)

FPT_IDV_EXT.1

7.6.4 Integrity for Installation and Update

The TOE is distributed to customers from a secure developer portal or via a tracked courier delivery service. The Developer publishes the public key on a developer support website https://www.bastille.net/support.

Delivery package also contains a detached digital signature in the .sig file. Customers are required to verify integrity of the package using this detached signature and developers public key obtained from developer support website prior to installation of the package.

The delivery package is a virtual appliance image (.OVA), which contains Ubuntu Linux 18.04 or 22.04 operating system with the TOE pre-installed. Customers can import this OVA image to their VMware ESXi server, run it, and perform initial TOE configuration without installing any additional packages.

The Developer can issue an update to the TOE to address discovered flaws and vulnerabilities. This update will be similarly provided to customers as a packaged OVA virtual appliance image, with Platform OS and the updated TOE pre-installed. The TOE is not updated by applying patches or installing packages. In order to update the TOE, customers decommission the virtual appliance with the previous version of the TOE, then import and initialize the new version of the appliance obtained from the Developer as described above.

Users can query the current version of the TOE using the TOE web interface. Users can check for existing updates to the TOE using the TOE web interface (this functionality requires an internet connection).

FPT_TUD_EXT.1

7.6.5 Timely Security Updates

The TOE developer has implemented internal processes for receiving reports of security flaws, tracking product vulnerabilities, and distributing software updates to customers in a timely manner.

Customers can submit support issues, including discovered security vulnerabilities via email to support@bastille.io. Sensitive information should be encrypted using the PGP key published on the developer support website.

Any implementation flaws are expected to be addressed within 90 days of reporting. Issues that necessitate a fix to the TOE will result in a release of an updated version of the TOE, as there is no process of applying targeted patches or updates. The updated version will be released as a new software distribution package (virtual appliance). Customers are notified of security related fixes via email or can check for existing updates using the functionality built into the TOE. When a security fix affects security properties or the configuration, updated guidance documentation will be issued. Issues in the third-party libraries comprising the OVA image will be resolved in the same manner.

ALC_TSU_EXT.1

7.7 Trusted Path/Channels

7.7.1 Protection of Data in Transit

The TOE supports various network activities as described in Section 7.2.2 above. The network connections transmit sensitive and non-sensitive data as enumerated in the following table:

Table 6: TOE communication channels

Direction	Description	Data classification	Protection	TOE Module
Incoming	API Users/Web Interface	Sensitive	Platform TLS/HTTPS	NGINX
Incoming	Data Collection	Sensitive	Platform TLS/HTTPS	NGINX
Outgoing	MS AFDS connection	Sensitive	Platform TLS/HTTPS	Fusion Center
Outgoing	ElasticSearch DB	Sensitive	Platform TLS/HTTPS	Fusion Center
Outgoing	Kafka message queue	Sensitive	Platform TLS	Confluent
Outgoing	External Applications	Sensitive	Platform TLS/HTTPS	Fusion Center
Outgoing	Developer Portal	Sensitive	Platform TLS/HTTPS	Fusion Center
Outgoing	FileBeat logs	Non-Sensitive	Platform TLS	FileBeat
Outgoing	CRL check	Non-Sensitive	No	Fusion Center

TOE does not transmit user credentials over the network.

The TOE uses the platform-provided OpenSSL library to perform encryption of sensitive communications with other IT products or users.

For incoming connections, NGINX module accepts incoming network connection to the TOE. When this connection is being established, NGINX calls the platform-provided OpenSSL library to perform HTTPS/TLS channel establishment and ongoing decryption/encryption of transmitted data. The TOE uses the documented platform library API calls to obtain an established TLS channel, using a TOE-provided x509 certificate, private key, TOE-prescribed TLS version and ciphersuites. The platform library is expected to perform all necessary low-level cryptographic operations (including calls to the DRBG for key generation and establishment) transparently for the TOE. The API the TOE uses to communicate with the platform-provided OpenSSL library are provided in Table 7 below. The TOE does not request or verify client certificates for incoming connections.

Table 7: NGINX API Calls for channel encryption	
API	Description
BIO_free	https://www.openssl.org/docs/man1.1.1/man3/BIO_free.html
BIO_new_file	https://www.openssl.org/docs/man1.1.1/man3/BIO_new_file.html
CRYPTO_get_ex_new_index	https://www.openssl.org/docs/man1.1.1/man3/CRYPTO_get_ex_new_index.html
EVP_DigestFinal_ex	https://www.openssl.org/docs/man1.1.1/man3/EVP_DigestFinal_ex.html
EVP_DigestInit_ex	https://www.openssl.org/docs/man1.1.1/man3/EVP_DigestInit_ex.html
EVP_DigestUpdate	https://www.openssl.org/docs/man1.1.1/man3/EVP_DigestUpdate.html
EVP_MD_CTX_free	https://www.openssl.org/docs/man1.1.1/man3/EVP_MD_CTX_free.html
EVP_MD_CTX_new	https://www.openssl.org/docs/man1.1.1/man3/EVP_MD_CTX_new.html
EVP_sha1	https://www.openssl.org/docs/man1.1.1/man3/EVP_sha1.html
OPENSSL_init_ssl	https://www.openssl.org/docs/man1.1.1/man3/OPENSSL_init_ssl.html
OPENSSL_sk_num	https://github.com/openssl/openssl/blob/605856d72cbd4720ad9ccb20c8fd5afbee2ad1a4/crypto/stack/stack.c#L379
PEM_read_bio_X509	https://www.openssl.org/docs/man1.1.1/man3/PEM_read_bio_X509.html
PEM_read_bio_X509_AUX	https://www.openssl.org/docs/man1.1.1/man3/PEM_read_bio_X509_AUX.html
SSL_CIPHER_description	https://www.openssl.org/docs/man1.1.1/man3/SSL_CIPHER_description.html
SSL_CTX_callback_ctrl	https://www.openssl.org/docs/man1.1.1/man3/SSL_CTX_callback_ctrl.html
SSL_CTX_clear_options	https://www.openssl.org/docs/man1.1.1/man3/SSL_CTX_clear_options.html
SSL_CTX_ctrl	https://www.openssl.org/docs/man1.1.1/man3/SSL_CTX_ctrl.html
SSL_CTX_free	https://www.openssl.org/docs/man1.1.1/man3/SSL_CTX_free.html
SSL_CTX_get_client_CA_list	https://www.openssl.org/docs/man1.1.1/man3/SSL_CTX_get_client_CA_list.html
SSL_CTX_get_ex_data	https://www.openssl.org/docs/man1.1.1/man3/SSL_CTX_get_ex_data.html
SSL_CTX_get_options	https://www.openssl.org/docs/man1.1.1/man3/SSL_CTX_get_options.html
SSL_CTX_get_verify_callback	https://www.openssl.org/docs/man1.1.1/man3/SSL_CTX_get_verify_callback.html
SSL_CTX_get_verify_depth	https://www.openssl.org/docs/man1.1.1/man3/SSL_CTX_get_verify_depth.html
SSL_CTX_get_verify_mode	https://www.openssl.org/docs/man1.1.1/man3/SSL_CTX_get_verify_mode.html
SSL_CTX_new	https://www.openssl.org/docs/man1.1.1/man3/SSL_CTX_new.html
SSL_CTX_set_alpn_select_cb	https://www.openssl.org/docs/man1.1.1/man3/SSL_CTX_set_alpn_select_cb.html
SSL_CTX_set_cipher_list	https://www.openssl.org/docs/man1.1.1/man3/SSL_CTX_set_cipher_list.html
SSL_CTX_set_default_passwd_cb	https://www.openssl.org/docs/man1.1.1/man3/SSL_CTX_set_default_passwd_cb.html
SSL_CTX_set_ex_data	https://www.openssl.org/docs/man1.1.1/man3/SSL_CTX_set_ex_data.html
SSL_CTX_set_info_callback	https://www.openssl.org/docs/man1.1.1/man3/SSL_CTX_set_info_callback.html
SSL_CTX_set_next_protos_advertised_cb	https://www.openssl.org/docs/man1.1.1/man3/SSL_CTX_set_next_protos_advertised_cb.html
SSL_CTX_set_options	https://www.openssl.org/docs/man1.1.1/man3/SSL_CTX_set_options.html
SSL_CTX_set_session_id_context	https://www.openssl.org/docs/man1.1.1/man3/SSL_CTX_set_session_id_context.html
SSL_CTX_set_timeout	https://www.openssl.org/docs/man1.1.1/man3/SSL_CTX_set_timeout.html
SSL_CTX_set_verify_depth	https://www.openssl.org/docs/man1.1.1/man3/SSL_CTX_set_verify_depth.html
SSL_CTX_use_certificate	https://www.openssl.org/docs/man1.1.1/man3/SSL_CTX_use_certificate.html
SSL_CTX_use_PrivateKey_file	https://www.openssl.org/docs/man1.1.1/man3/SSL_CTX_use_PrivateKey_file.html
SSL_do_handshake	https://www.openssl.org/docs/man1.1.1/man3/SSL_do_handshake.html
SSL_free	https://www.openssl.org/docs/man1.1.1/man3/SSL_free.html
SSL_get_current_cipher	https://www.openssl.org/docs/man1.1.1/man3/SSL_get_current_cipher.html
SSL_get_error	https://www.openssl.org/docs/man1.1.1/man3/SSL_get_error.html
SSL_get_ex_data	https://www.openssl.org/docs/man1.1.1/man3/SSL_get_ex_data.html
SSL_get_rbio	https://www.openssl.org/docs/man1.1.1/man3/SSL_get_rbio.html
SSL_get_servername	https://www.openssl.org/docs/man1.1.1/man3/SSL_get_servername.html
SSL_get_shutdown	https://www.openssl.org/docs/man1.1.1/man3/SSL_get_shutdown.html
SSL_get_wbio	https://www.openssl.org/docs/man1.1.1/man3/SSL_get_wbio.html
SSL_in_init	https://www.openssl.org/docs/man1.1.1/man3/SSL_in_init.html
SSL_is_server	https://www.openssl.org/docs/man1.1.1/man3/SSL_is_server.html
SSL_new	https://www.openssl.org/docs/man1.1.1/man3/SSL_new.html
SSL_read	https://www.openssl.org/docs/man1.1.1/man3/SSL_read.html

SSL_select_next_proto	https://www.openssl.org/docs/man1.1.1/man3/SSL_select_next_proto.html
SSL_session_reused	https://www.openssl.org/docs/man1.1.1/man3/SSL_session_reused.html
SSL_set_accept_state	https://www.openssl.org/docs/man1.1.1/man3/SSL_set_accept_state.html
SSL_set_ex_data	https://www.openssl.org/docs/man1.1.1/man3/SSL_set_ex_data.html
SSL_set_fd	https://www.openssl.org/docs/man1.1.1/man3/SSL_set_fd.html
SSL_set_options	https://www.openssl.org/docs/man1.1.1/man3/SSL_set_options.html
SSL_set_quiet_shutdown	https://www.openssl.org/docs/man1.1.1/man3/SSL_set_quiet_shutdown.html
SSL_set_shutdown	https://www.openssl.org/docs/man1.1.1/man3/SSL_set_shutdown.html
SSL_set_SSL_CTX	https://github.com/openssl/openssl/blob/6d4313f03eddd39ca8d06a5e1d20fc1adcb207c5/ssl/ssl_lib.c#L4235
SSL_set_verify	https://www.openssl.org/docs/man1.1.1/man3/SSL_set_verify.html
SSL_set_verify_depth	https://www.openssl.org/docs/man1.1.1/man3/SSL_set_verify_depth.html
SSL_shutdown	https://www.openssl.org/docs/man1.1.1/man3/SSL_shutdown.html
SSL_write	https://www.openssl.org/docs/man1.1.1/man3/SSL_write.html
TLS_method	https://www.openssl.org/docs/man1.1.1/man3/TLS_method.html
X509_digest	https://www.openssl.org/docs/man1.1.1/man3/X509_digest.html
X509_free	https://www.openssl.org/docs/man1.1.1/man3/X509_free.html
X509_get_ex_data	https://www.openssl.org/docs/man1.1.1/man3/X509_get_ex_data.html
X509_set_ex_data	https://www.openssl.org/docs/man1.1.1/man3/X509_set_ex_data.html

When the TOE is establishing outgoing connections to a non-TOE entity, the TOE is using standard Python *ssl* module (https://docs.python.org/3/library/ssl.html?highlight=ssl#module-ssl) to establish a TLS connection. The Python library then places a call to the platform-provided OpenSSL library to establish an encrypted connection socket. All low-level cryptographic operations (including calls to the DRBG) are performed by that module transparently for the TOE.

When establishing outgoing TLS connections, the TOE will not present x.509 certificates to non-TOE entities. The server's certificate validation is being performed by the platform-provided OpenSSL according to the certificate validation requirements as described above.

When the TOE performs a connection to the Kafka server it is using Kafka Confluent client that calls an API for the platform-provided OpenSSL library to establish an encrypted connection to the Kafka service with the provided parameters. All required low-level cryptographic operations (including calls to the DRBG) are performed by that module transparently for the TOE.

Table 8: Confluent Kafka API Calls for channel encryption

API	Description
SSL_CTX_new	https://www.openssl.org/docs/man1.1.1/man3/SSL_CTX_new.html
SSL_CTX_set_options	TLS version is defined
SSL_CTX_set_cipher_list	Ciphersuites to be used are defined.
SSL_CTX_set1_curves_list	EC Curves to be used are defined
SSL_CTX_set1_sigalgs_list	Signature algorithms are defined.
SSL_CTX_load_verify_locations	CA certificates location is defined.
SSL_CTX_set_default_verify_paths	CA certificates location is defined.
X509_STORE_set_flags	CRL check is requested to be performed by platform.
SSL_CTX_use_certificate_chain_file	Provide Certificate file and key files for the connection.
SSL_CTX_use_PrivateKey_file	Provide Certificate file and key files for the connection.
d2i_PKCS12_fp	https://www.openssl.org/docs/man1.1.0/man3/d2i_PKCS12_fp.html
PKCS12_parse	https://www.openssl.org/docs/manmaster/man3/PKCS12_parse.html
SSL_CTX_use_certificate	https://www.openssl.org/docs/man1.1.1/man3/SSL_CTX_use_certificate.html
SSL_CTX_use_PrivateKey	https://www.openssl.org/docs/man1.1.1/man3/SSL_CTX_use_PrivateKey_file.html
SSL_CTX_set_mode	https://www.openssl.org/docs/man1.1.1/man3/SSL_CTX_set_mode.html

SSL_write	https://www.openssl.org/docs/man1.1.1/man3/SSL_write.html
SSL_read	https://www.openssl.org/docs/man1.1.1/man3/SSL_read.html
SSL_do_handshake	https://www.openssl.org/docs/man1.1.1/man3/SSL_do_handshake.html
SSL_get_peer_certificate	https://www.openssl.org/docs/man1.1.1/man3/SSL_get_peer_certificate.html
SSL_get_verify_result	https://www.openssl.org/docs/man1.1.1/man3/SSL_get_verify_result.html
SSL_shutdown	https://www.openssl.org/docs/man1.1.1/man3/SSL_shutdown.html
SSL_new	https://www.openssl.org/docs/man1.1.1/man3/SSL_new.html
SSL_set_fd	https://www.openssl.org/docs/man1.1.1/man3/SSL_set_fd.html
SSL_set_tlsext_host_name	https://www.openssl.org/docs/man1.1.1/man3/SSL_set_tlsext_host_name.html
SSL_connect	https://www.openssl.org/docs/man1.1.1/man3/SSL_connect.html

The TOE instructs the underlying platform to establish connections using TLS 1.2 protocol and the following ciphersuites:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 and RFC 8422
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289

FTP_DIT_EXT.1

8. Terms and Definitions

Table 9: TOE Abbreviations and Acronyms	
Abbreviations/ Acronyms	Description
AES	Advanced Encryption Standard
ADFS	Active Directory Federation Service
ASLR	Address Space Layout Randomization
CN	Common Names
CRL	Certificate Revocation List
DHE	Diffie-Hellman Ephemeral
DNS	Domain Name System
DRBG	Deterministic Random Bit Generator
DTLS	Datagram Transport Layer Security
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
FIPS	Federal Information Processing Standards
FQDN	Fully Qualified Domain Name
HMAC	Hash-based Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MIME	Multi-purpose Internet Mail Extensions
NFC	Near Field Communication
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OIDC	OpenID Connect
OS	Operating System
PDF	Portable Document Format
PE	Portable Executable
PID	Process Identifier
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
IT	Information Technology
RBG	Random Bit Generator
RFC	Request for Comment
RNG	Random Number Generator
SAN	Subject Alternative Name
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SP	Special Publication
SSH	Secure Shell
SWID	Software Identification
TLS	Transport Layer Security
UI	User Interface
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

Table 10: CC Abbreviations and Acronyms	
Abbreviations/ Acronyms	Description
CC	Common Criteria
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards
OSP	Organizational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
TSS	TOE Summary Specification

9. References

Table 11: TOE Guidance			
Reference	Description	Version	Date
[G1]	Bastille Enterprise Fusion Center Administrative Guidance for Common Criteria	3.6	2025

Table 12: Common Criteria v3.1 References			
Reference	Description	Version	Date
[C1]	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model CCMB-2017-04-001	V3.1 R5	April 2017
[C2]	Common Criteria for Information Technology Security Evaluation Part 2: Security functional components CCMB-2017-04-002	V3.1 R5	April 2017
[C3]	Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components CCMB-2017-04-003	V3.1 R5	April 2017
[C4]	Common Criteria for Information Technology Security Evaluation Evaluation Methodology CCMB-2017-04-004	V3.1 R5	April 2017
[C5]	CC and CEM addenda - Exact Conformance, Selection-Based SFRs, Optional SFRs CCDB-2017-05-xxx	V0.5	May 2017

Table 13: Supporting Documentation			
Reference	Description	Version	Date
[PP]	Protection Profile for Application Software	1.4	2021-10-07

Appendix A

Table 14: Platform API Usage	
Library	**API call**
Expat	XML_ErrorString
Expat	XML_ExpatVersionInfo
Expat	XML_ExpatVersion
Expat	XML_ExternalEntityParserCreate
Expat	XML_FreeContentModel
Expat	XML_GetBase
Expat	XML_GetBuffer
Expat	XML_GetCurrentByteIndex
Expat	XML_GetCurrentColumnNumber
Expat	XML_GetCurrentLineNumber
Expat	XML_GetErrorCode
Expat	XML_GetFeatureList
Expat	XML_GetInputContext
Expat	XML_GetSpecifiedAttributeCount
Expat	XML_ParseBuffer
Expat	XML_ParserCreate_MM
Expat	XML_ParserFree
Expat	XML_Parse
Expat	XML_SetAttlistDeclHandler
Expat	XML_SetBase
Expat	XML_SetCharacterDataHandler
Expat	XML_SetCommentHandler
Expat	XML_SetDefaultHandlerExpand
Expat	XML_SetDefaultHandler
Expat	XML_SetElementDeclHandler
Expat	XML_SetElementHandler
Expat	XML_SetEncoding
Expat	XML_SetEndCdataSectionHandler
Expat	XML_SetEndDoctypeDeclHandler
Expat	XML_SetEndElementHandler
Expat	XML_SetEndNamespaceDeclHandler
Expat	XML_SetEntityDeclHandler
Expat	XML_SetExternalEntityRefHandler
Expat	XML_SetHashSalt

Expat	XML_SetNamespaceDeclHandler
Expat	XML_SetNotationDeclHandler
Expat	XML_SetNotStandaloneHandler
Expat	XML_SetParamEntityParsing
Expat	XML_SetProcessingInstructionHandler
Expat	XML_SetReturnNSTriplet
Expat	XML_SetSkippedEntityHandler
Expat	XML_SetStartCdataSectionHandler
Expat	XML_SetStartDoctypeDeclHandler
Expat	XML_SetStartElementHandler
Expat	XML_SetStartNamespaceDeclHandler
Expat	XML_SetUnknownEncodingHandler
Expat	XML_SetUnparsedEntityDeclHandler
Expat	XML_SetUserData
Expat	XML_SetXmlDeclHandler
Expat	XML_StopParser
Expat	XML_UseForeignDTD
OpenSSL	ASN1_d2i_bio
OpenSSL	ASN1_GENERALIZEDTIME_print
OpenSSL	ASN1_TIME_print
OpenSSL	BIO_ctrl
OpenSSL	BIO_free
OpenSSL	BIO_int_ctrl
OpenSSL	BIO_new_file
OpenSSL	BIO_new
OpenSSL	BIO_read
OpenSSL	BIO_s_mem
OpenSSL	BIO_write
OpenSSL	CRYPTO_free
OpenSSL	CRYPTO_get_ex_new_index
OpenSSL	CRYPTO_malloc
OpenSSL	d2i_OCSP_RESPONSE
OpenSSL	d2i_SSL_SESSION
OpenSSL	DH_free
OpenSSL	ENGINE_by_id
OpenSSL	ENGINE_free
OpenSSL	ENGINE_load_private_key
OpenSSL	ENGINE_set_default
OpenSSL	ERR_clear_error

OpenSSL	ERR_error_string_n
OpenSSL	ERR_get_error
OpenSSL	ERR_peek_error_line_data
OpenSSL	ERR_peek_error
OpenSSL	ERR_peek_last_error
OpenSSL	EVP_aes_128_cbc
OpenSSL	EVP_aes_256_cbc
OpenSSL	EVP_CIPHER_iv_length
OpenSSL	EVP_DecryptInit_ex
OpenSSL	EVP_DigestFinal_ex
OpenSSL	EVP_DigestInit_ex
OpenSSL	EVP_DigestUpdate
OpenSSL	EVP_EncryptInit_ex
OpenSSL	EVP_MD_CTX_free
OpenSSL	EVP_MD_CTX_new
OpenSSL	EVP_PKEY_free
OpenSSL	EVP_sha1
OpenSSL	EVP_sha256
OpenSSL	HMAC_Init_ex
OpenSSL	i2a_ASN1_INTEGER
OpenSSL	i2d_OCSP_REQUEST
OpenSSL	i2d_OCSP_RESPONSE
OpenSSL	i2d_SSL_SESSION
OpenSSL	OBJ_nid2sn
OpenSSL	OCSP_BASICRESP_free
OpenSSL	OCSP_basic_verify
OpenSSL	OCSP_CERTID_free
OpenSSL	OCSP_cert_to_id
OpenSSL	OCSP_check_validity
OpenSSL	OCSP_request_add0_id
OpenSSL	OCSP_REQUEST_free
OpenSSL	OCSP_REQUEST_new
OpenSSL	OCSP_resp_find_status
OpenSSL	OCSP_RESPONSE_free
OpenSSL	OCSP_response_get1_basic
OpenSSL	OCSP_RESPONSE_new
OpenSSL	OCSP_response_status
OpenSSL	OPENSSL_init_ssl

OpenSSL	OPENSSL_sk_num
OpenSSL	OPENSSL_sk_value
OpenSSL	OpenSSL_version
OpenSSL	PEM_read_bio_DHparams
OpenSSL	PEM_read_bio_X509_AUX
OpenSSL	PEM_read_bio_X509
OpenSSL	PEM_write_bio_X509
OpenSSL	SSL_CIPHER_description
OpenSSL	SSL_CIPHER_find
OpenSSL	SSL_CIPHER_get_name
OpenSSL	SSL_ctrl
OpenSSL	SSL_CTX_callback_ctrl
OpenSSL	SSL_CTX_clear_options
OpenSSL	SSL_CTX_ctrl
OpenSSL	SSL_CTX_free
OpenSSL	SSL_CTX_get_cert_store
OpenSSL	SSL_CTX_get_client_CA_list
OpenSSL	SSL_CTX_get_ex_data
OpenSSL	SSL_CTX_get_options
OpenSSL	SSL_CTX_get_timeout
OpenSSL	SSL_CTX_get_verify_callback
OpenSSL	SSL_CTX_get_verify_depth
OpenSSL	SSL_CTX_get_verify_mode
OpenSSL	SSL_CTX_load_verify_locations
OpenSSL	SSL_CTX_new
OpenSSL	SSL_CTX_remove_session
OpenSSL	SSL_CTX_sess_set_get_cb
OpenSSL	SSL_CTX_sess_set_new_cb
OpenSSL	SSL_CTX_sess_set_remove_cb
OpenSSL	SSL_CTX_set_alpn_protos
OpenSSL	SSL_CTX_set_alpn_select_cb
OpenSSL	SSL_CTX_set_cipher_list
OpenSSL	SSL_CTX_set_client_CA_list
OpenSSL	SSL_CTX_set_default_passwd_cb
OpenSSL	SSL_CTX_set_default_passwd_cb_userdata
OpenSSL	SSL_CTX_set_ex_data
OpenSSL	SSL_CTX_set_info_callback
OpenSSL	SSL_CTX_set_next_protos_advertised_cb
OpenSSL	SSL_CTX_set_options

OpenSSL	SSL_CTX_set_session_id_context
OpenSSL	SSL_CTX_set_timeout
OpenSSL	SSL_CTX_set_verify_depth
OpenSSL	SSL_CTX_set_verify
OpenSSL	SSL_CTX_use_certificate
OpenSSL	SSL_CTX_use_PrivateKey_file
OpenSSL	SSL_CTX_use_PrivateKey
OpenSSL	SSL_do_handshake
OpenSSL	SSL_free
OpenSSL	SSL_get0_alpn_selected
OpenSSL	SSL_get0_next_proto_negotiated
OpenSSL	SSL_get1_session
OpenSSL	SSL_get_certificate
OpenSSL	SSL_get_current_cipher
OpenSSL	SSL_get_error
OpenSSL	SSL_get_ex_data
OpenSSL	SSL_get_ex_data_X509_STORE_CTX_idx
OpenSSL	SSL_get_peer_certificate
OpenSSL	SSL_get_rbio
OpenSSL	SSL_get_servername
OpenSSL	SSL_get_session
OpenSSL	SSL_get_shutdown
OpenSSL	SSL_get_verify_result
OpenSSL	SSL_get_version
OpenSSL	SSL_get_wbio
OpenSSL	SSL_in_init
OpenSSL	SSL_is_server
OpenSSL	SSL_load_client_CA_file
OpenSSL	SSL_new
OpenSSL	SSL_read
OpenSSL	SSL_select_next_proto
OpenSSL	SSL_SESSION_free
OpenSSL	SSL_SESSION_get_id
OpenSSL	SSL_session_reused
OpenSSL	SSL_set_accept_state
OpenSSL	SSL_set_connect_state
OpenSSL	SSL_set_ex_data
OpenSSL	SSL_set_fd
OpenSSL	SSL_set_options

OpenSSL	SSL_set_quiet_shutdown
OpenSSL	SSL_set_session
OpenSSL	SSL_set_shutdown
OpenSSL	SSL_set_SSL_CTX
OpenSSL	SSL_set_verify_depth
OpenSSL	SSL_set_verify
OpenSSL	SSL_shutdown
OpenSSL	SSL_write
OpenSSL	TLS_method
OpenSSL	X509_check_host
OpenSSL	X509_check_issued
OpenSSL	X509_digest
OpenSSL	X509_free
OpenSSL	X509_get0_notAfter
OpenSSL	X509_get0_notBefore
OpenSSL	X509_get_ex_data
OpenSSL	X509_get_issuer_name
OpenSSL	X509_get_serialNumber
OpenSSL	X509_get_subject_name
OpenSSL	X509_LOOKUP_ctrl
OpenSSL	X509_LOOKUP_file
OpenSSL	X509_NAME_digest
OpenSSL	X509_NAME_oneline
OpenSSL	X509_NAME_print_ex
OpenSSL	X509_set_ex_data
OpenSSL	X509_STORE_add_lookup
OpenSSL	X509_STORE_CTX_free
OpenSSL	X509_STORE_CTX_get1_issuer
OpenSSL	X509_STORE_CTX_get_current_cert
OpenSSL	X509_STORE_CTX_get_error_depth
OpenSSL	X509_STORE_CTX_get_error
OpenSSL	X509_STORE_CTX_get_ex_data
OpenSSL	X509_STORE_CTX_init
OpenSSL	X509_STORE_CTX_new
OpenSSL	X509_STORE_set_flags
OpenSSL	X509_up_ref
OpenSSL	X509_verify_cert_error_string

PCRE	pcre_compile
PCRE	pcre_config
PCRE	pcre_exec
PCRE	pcre_free_study
PCRE	pcre_fullinfo
PCRE	pcre_study
Zlib	adler32
Zlib	crc32
Zlib	deflateCopy
Zlib	deflateEnd
Zlib	deflateInit2_
Zlib	deflateInit_
Zlib	deflateSetDictionary
Zlib	deflate
Zlib	inflateEnd
Zlib	inflateInit2_
Zlib	inflateReset
Zlib	inflateSetDictionary
Zlib	inflate
Zlib	zlibVersion
Zlib	inflateCopy
Linux Sys	chmod
Linux Sys	close
Linux Sys	epoll_ctl
Linux Sys	epoll_pwait
Linux Sys	epoll_wait
Linux Sys	exit
Linux Sys	flistxattr
Linux Sys	fstat
Linux Sys	ftime
Linux Sys	futex
Linux Sys	getdents64
Linux Sys	getegid32
Linux Sys	getuid
Linux Sys	llistxattr
Linux Sys	madvise1
Linux Sys	mkdir
Linux Sys	nanosleep
Linux Sys	newfstatat

Linux Sys	open
Linux Sys	openat
Linux Sys	pivot_root
Linux Sys	profil
Linux Sys	read
Linux Sys	readlinkat
Linux Sys	remap_file_pages
Linux Sys	restart_syscall
Linux Sys	rt_sigreturn
Linux Sys	sigsuspend
Linux Sys	write
Linux Sys	getrandom

Python language is being used as per the official language specification published at https://docs.python.org/3.11/.

Listed libraries are part of Ubuntu 18.04 platform:

- Expat version 2.2.5-3ubuntu0.9
- Openssl version 1.1.1-1ubuntu2.fips.2.1~18.04.15.2
- Zlib version 1:1.2.11.dfsg-0ubuntu2.2
- PCRE3 version 2:8.39-9ubuntu0.1

Listed libraries are part of Ubuntu 22.04 platform:

- Expat version 2.4.7-1ubuntu0.6
- Openssl version 3.0.2-0ubuntu1.12+Fips1
- Zlib version 1:1.2.11.dfsg-2ubuntu9.2
- PCRE3 version 2:8.39-13ubuntu0.22.04.1

Appendix B

This Appendix describes 3rd-party libraries that the TOE is packaged with.

Platform:

The TOE is delivered to the customer with the OS (TOE platform), which is the Ubuntu 18.04 LTS or 22.04 LTS distribution.

TOE:

The following third party tools and libraries are included in the TOE:

NGINX, Elastic FileBeat, Confluent Kafka Python Client.

Javascript libraries:

@appbaseio/reactivesearch, @appbaseio/reactivesearch, aws4, axios, change-case, chart.js, classnames, date-fns, dateformat, @date-io/date-fns, @date-io/moment, dom-to-image-more downloadjs, elastic-builder, @elastic/datemath, elasticsearch, emotion, history, js-file-download, jsonexport, leaflet, leaflet-draw, lodash, lodash.clonedeep, lodash.drop, lodash.get, lodash.groupby, lodash.isequal, lodash.uniq, @material-ui/core, @material-ui/icons @material-ui/lab @material-ui/pickers, @material-ui/pickers, mobx-react, moment, multidict, ngeohash, numeral, object-hash, papaparse, pluralize, printable-characters, qs, ra-core, rc-slider, react, react-admin, react-chartjs-2, react-color, react-dom, react-emotion, react-final-form, react-icons, react-json-view react-leaflet, react-leaflet-control, react-leaflet-draw, react-leaflet-heatmap-layer, @react-pdf/layout @react-pdf/renderer, react-redux, react-resize-detector, react-router, react-router-dom, react, router-dom, react-select, react-select, react-sizeme, react-spinkit, react-spinners-kit, react-to-print, react-use, react-use, react-vis, react-vis, js-timeline, shorted, uppy, @uppy/react, url-search-params, vis

Python 3.11.3 with the following python libraries:

Aiofiles, aiohttp, aiokafka, backoff, cachetools, charset normalizer, cffi, greenlit, scipy, sql alchemy, shortuuid, skops, starlette, streamz, torch, tornado, ujson, uvicorn, uvloop, redis, requests, scikit-learn, shapely, psutil, pydantic, pydash, PyJWT, pyOpenSSL, pypager, PyYAML, optuna, polars-lts-cpu, ntplib, cmd2, configclasses, configclasses confluent-kafka, cryptography, dictdiffer, querystring-parser, MarkupSafe, lightning, validators, fastapi, fastavro, frozenlist, httptools jinja2, numpy, websockets, yarl