Pensando Systems, Inc.

Distributed Services Platform

v1.28.0-E-96

Security Target

Evaluation Assurance Level (EAL): 2+
Document Version: 0.6

Prepared for:

PENSANDO

Pensando Systems, Inc.

570 Alder Drive
Milpitas, CA 95035
United States of America

Phone: +1 408 451 9026
www.pensando.io

Prepared by:

Corsec

Corsec Security, Inc.

13921 Park Center Road Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050
www.corsec.com

Table of Contents

©2022 Pensando Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

List of Figures

List of Tables

©2022 Pensando Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

1. Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The TOE is the Pensando Systems, Inc.'s (Pensando's) Distributed Services Platform (DSP) and will hereafter be referred to as the TOE throughout this document. The TOE is a network traffic security solution that provides observability and orchestration of internal network traffic through its components that include the Distributed Services Card (DSC) firmware v1.28.0-E-96 and Policy and Services Manager (PSM) software v1.28.0-E-96. It provides secure connections between components, customizable observability and metrics charts about the DSC's network traffic, NetFlow/IPFIX [1] streaming, high availability of the PSM cluster, cluster health monitoring/alerting, and a centralized location for managing polices related to the TOE's functionality.

1.1 Purpose

This ST is divided into nine sections, as follows:

- Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functionality and describes the physical and logical scope for the TOE as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), Protection Profile (PP), and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (Section 3) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Extended Components (Section 5) – Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3.
- Security Requirements (Section 6) – Presents the SFRs and SARs to which the TOE adheres.
- TOE Summary Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the SFRs and objectives.
- Rationale (Section 8) – Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms (Section 9) – Defines the acronyms used within this ST.

1.2 Security Target and TOE References

Table 1 below shows the ST and TOE references.

Table 1 – ST and TOE References

ST Title	*Pensando Systems, Inc. Distributed Services Platform v1.28.0-E-96 Security Target*
ST Version	Version 0.6

[1] IPFIX - Internet Protocol Flow Information Export

©2022 Pensando Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

ST Author	Corsec Security, Inc.
ST Publication Date	2022-01-26
TOE Reference	Distributed Services Platform v1.28.0-E-96

1.3 Product Overview

The Product Overview provides a high-level description of the product that is the subject of the evaluation. The following section, TOE Overview, will provide the introduction to the parts of the overall product offering that are specifically being evaluated.

Pensando DSP provides network services at an interface level for servers in an enterprise datacenter. The platform consists of DSCs that are installed on each server and a PSM cluster that manages the DSCs from a single point within the datacenter. DSP provides telemetry and analytics, automated updates for DCS policies, host interface security policies, IPFIX exports, and mirror sessions to allow datacenter administrators to see and understand the network traffic at each server. Distributing these network services to each server relieves the bottlenecks at the top-of-rack (TOR) switches and specialized network appliances. DSP is available with the two service level agreements listed in Table 2 below.

Table 2 – DSP Service Level Agreement

Distributed Services Platform	Enterprise Package	Enterprise Pro Package
Platform Foundation		
Driver Performance Offloads (TSO/LSO/LRO Stateless & Checksum, RSS)	✓	✓
Driver Host Utility (penctl)	✓	✓
Server Platform Integration (HPE iLO, Smart Update Manager, Oneview)	✓	✓
Policy & Services Management & Automation		
Pensando Policy and Services Manager (PSM)	✓	✓
Highly available microservices-based management cluster	✓	✓
Declarative Model Based REST API	✓	✓
Authentication & RBAC with Radius, Active Directory, LDAP	✓	✓
Centralized Policy and Services Provisioning	✓	✓
Customized Observability & Metrics Charting	✓	✓
Third Party Orchestration Integration for VMware vCenter®	✓	✓
Flexible Deployment Profiles	✓	✓
Observability & Telemetry		
Bi-directional Mirror Sessions (Port & Flow Based ERSPAN)	✓	✓
Netflow/IPFIX Streaming	✓	✓
DSP Cluster Health Status Monitoring & Alerting	✓	✓
Traffic Flow Analysis (Flow-Aware Mode)	✓	✓
Network & Connection State Metrics (Bandwidth, Drops, Resets, CPS)	✓	✓

©2022 Pensando Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Distributed Services Platform	Enterprise Package	Enterprise Pro Package
Distributed Firewall Visibility & Connection Logging		✓
Security		
Distributed Firewall (Stateful)		✓
Application Layer Gateway (ALG)		✓
DDoS Protection for Workloads & DSC		✓
Micro-Segmentation for virtualized workloads		✓
Customizable DDoS Protection Firewall Profiles		✓
Connection Tracking and Logging To SIEM/Syslog & PSM		✓

1.4 TOE Overview

The TOE Overview summarizes the usage and major security features of the TOE. This section provides a context for the TOE evaluation by identifying the TOE type, describing the TOE, and defining the specific evaluated configuration.

The TOE is a combination of software and firmware that provides functionality related to the "Network and Network-Related Devices and Systems" product category in CC. It is comprised of 3 instances of the PSM node software and multiple instances of DSC firmware. The PSM node software and DSC firmware run on virtual machines (VMs) and DSC hardware in the operating environment (OE), respectively. Both set of these components run on separate server hosts. See Figure 1 below for a depiction of the TOE deployment.

The TOE has the ability to generate audits for events pertaining to management of alert policies, alert destinations, TOE user accounts, authentication methods, roles, mirror sessions, and DSC hosts. It can also generate audits for non-management activities including authentication, password changes, and node failures. All audits contain the identity of the TOE user that performed the operation that caused an audit if it is applicable. Based on the generated audit events, the TOE can setup rules that will monitor for administrator-defined criteria to send alerts to the syslog server in the OE. These alerts can be used to notify TOE users of potential security violations. The TOE also provides two area for reviewing the audit events generated by the TOE, which are restricted to TOE users with the role of AdminRole or with the All[2] permission. The TOE also utilizes the host's time source to provide reliable timestamps for audit events.

The TOE maintains local account attributes for TOE users that login using the local authentication method. When setting a local password in the TOE, it must meet the TOE's complexity requirements before the TOE will allow it to be saved. The TOE requires TOE users to be authenticated and identified before allowing any actions besides viewing the internal REST[3] API[4] documentation. When authenticating, TOE users may use local or directory-based authentication methods. Passwords being entered into the Web UI[5] are obscured by using bullets to hide the characters. The TOE also allows TOE users to terminate their own session from the Web UI.

[2] The All permission is when a role is created with the permissions and actions are set to All in each checkbox.
[3] REST – Representational State Transfer
[4] API – Application Programming Interface
[5] UI – User Interface

©2022 Pensando Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

The TOE provides multiple areas of management within its interfaces including alert policies, alert destinations, accounts, roles, authentication methods, DSC hosts, and mirrored sessions. The TOE has one predefined role, AdminRole, and can maintain any number of administrator-defined roles. It can also preserve its secure state and will be fully functional in the event of a PSM node fails.

The TOE uses TLS[6] connections between itself, the workstation, and Active Directory (AD) server or OpenLDAP server. All of these connections are setup to protect the transmitted data from modification or disclosure. When communicating to the AD/OpenLDAP server in the operating environment, only the TOE can initiate communication via the trusted channel. When TOE users communicate with the TOE, they must initiate the secure path to the TOE.

1.4.1 TOE Components

The TOE consists of multiple copies of DSC firmware and a three-node cluster of the PSM software. The same DSC firmware runs on multiple DSCs that differ in interface type and form factor but can be deployed in any datacenter server. The cards are managed by the PSM cluster via the DSC firmware.

1.4.1.1 Pensando Policy and Services Manager Cluster

The PSM cluster allows for configuration and delivery of network data and observability policies to Pensando DSCs from a central location. The PSM cluster is delivered as three VMs (duplicates of the same VM) that can be used either in VMware ESXi or KVM[7] to make the high-availability cluster for the TOE. Each node in the PSM cluster runs on a VM. A leader node is elected during the initial configuration and the nodes work in quorum when making decisions. The architecture of the nodes consists of Docker containers and microservices that are controller by Kubernetes.

Accessible to PSM is through either a Web UI or a REST API. Both of these connections are secured using HTTP[8] over TLS. These interfaces provide management of the DSCs and the TOE data. Authentication can be through local or AD/OpenLDAP accounts.

A PSM cluster can manage thousands of DSCs and their firmware. The PSM cluster operates completely out of band and is not in-line with the data path operations for the datacenter. DSCs must be associated with the PSM cluster and the cluster must admit each DSC card.

1.4.1.2 Pensando Distributed Services Card Firmware

The DSC firmware is installed on a Pensando Capri chip that is available on the Pensando DSC-25 and Pensando DSC-100 cards. The cards are installed in a PCIe[9] slot of a server to provide network services to its host and visibility features to the TOE. The DSC firmware provides telemetry and analytics, mirroring, and IPFIX exports from the server on which they are installed. Each card has a dedicated RJ45 [10] management port that allows for communications with the PSM cluster. The DSC firmware communicates with the PSM cluster through a TLS channel with mutual authentication.

[6] TLS – Transport Layer Security
[7] KVM – Kernel-based Virtual Machine
[8] HTTP – Hypertext Transport Protocol
[9] PCIe – Peripheral Component Interconnect Express
[10] RJ45 – Registered Jack 45

©2022 Pensando Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

1.5 TOE Environment

The TOE relies on the OE to properly function. Table 3 specifies the minimum system requirements for the TOE's OE. To host the PSM node cluster, the OE contains the PMS Host Server running a hypervisor that the three PMS node VMs are loaded onto. To run the DSC Firmware, the OE contains the DSC-25 and DSC-100, which are installed into separate DSC Host Servers.

The TOE also relies on external servers to execute functionality including an NTP[11] server for time synchronization, an AD or OpenLDAP server for directory-based authentication and resolving expanded group, and a syslog server for receiving alerts.

TOE users will also be able to manage the TOE from a workstation in the OE that connects to the PSM cluster.

Table 3 – OE Requirements

Category	Requirement

PMS Host Server	• CPU[12] – 2x 8-core (minimum configuration)
	  ○ Required to provide a minimum of 16 virtual CPU
	• Memory – 64 GB[13] (minimum configuration)
	• Disk – 250 GB (minimum configuration)
	  ○ This should be provided by an SSD[14] for performance
	  ○ 400 GB can be allocated for the max configuration
	• Network – 2x 1 Gbps[15] ports (for redundancy)
	• Hypervisor – One of the following:
	  ○ VMware ESXi v6.7
	  ○ VMware ESXi v6.5
	  ○ KVM on CentOS 7.6 with QEMU emulator version 2.11.1
	  ○ KVM on Red Hat Enterprise Linux 7.6 with QEMU emulator version 2.11.1
	  ○ KVM on Ubuntu 18.04 with QEMU emulator version 2.11.1

DSC Host Server	For DSC-25 cards:
	• Any server with a PCIe x8 Gen3 slot
	
	For DSC-100 cards:
	• Any server with a PCIe x16 Gen4 slot
	
	For both:
	• One of the following systems:
	  ○ VMware ESXi 6.5.0 through 7.0
	  ○ Red Hat Enterprise Linux 7.3 through 8.1
	  ○ CentOS 7.3 through 8.1
	  ○ Ubuntu Server 20.04 or 18.04.03
	  ○ Microsoft Windows Server 2019 or 2016
	  ○ SUSE Linux Enterprise Server SLES15 (SP 0/1) or SLES12 (SP 4/5)
	• The server's hardware must be able to support the installed OS[16].
	• The DSC driver comes on most of the operating systems but must be installed if it is not present.

Workstation	A general-purpose computer with a REST API client and a web browser.

[11] NTP – Network Time Protocol
[12] CPU – Central Processing Unit
[13] GB – Gigabyte
[14] SSD – Solid State Drive
[15] Gbps – Gigabits per second
[16] OS – Operating System

©2022 Pensando Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Category	Requirement
Authentication Server	One of the following servers: • A Microsoft Windows Server running Active Directory services. • A server capable of running Docker, which will be used to run a containerized version of OpenLDAP.
NTP Server	A server running NTPv3 (RFC[17] 1305) or any trusted NTP server like the AD server.
Syslog Server	A server running a syslog collector (RFC 5424) to receive alerts.

1.6 TOE Description

This section primarily addresses the physical and logical components of the TOE that are included in the evaluation.

1.6.1 Physical Scope

The TOE is a combination of software and firmware that run on VMs and DSCs respectively, which are compliant to the minimum software and hardware requirements as listed in Table 3. The software component running on the VMs is the PSM node software and runs in a three-node cluster. The firmware component is the DSC firmware and runs on each DSC in the OE.

The TOE is installed on server hardware as depicted in Figure 1 below. The essential components for the proper operation of the TOE in the evaluated configuration are:

- Pensando Distributed Services Card Firmware v1.28.0-E-96 running on the Capri chip that is attached to the DSC-25 and DSC-100 in the OE on separate servers.
    - The DSC firmware is packaged in a .tgz file and available for download from the Pensando Support Portal. The DSC firmware is also pre-installed on the DSCs and shipped to customers through third-party delivery services.
- Pensando Policy and Services Manager v1.28.0-E-96 running in a three-node cluster on VMs in the OE.
    - The PSM software is pre-installed inside on VMs and are packaged in .tgz files, which are available for download from the Pensando Support Portal.

Figure 1 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE.

[17] RFC – Request for Comments

©2022 Pensando Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

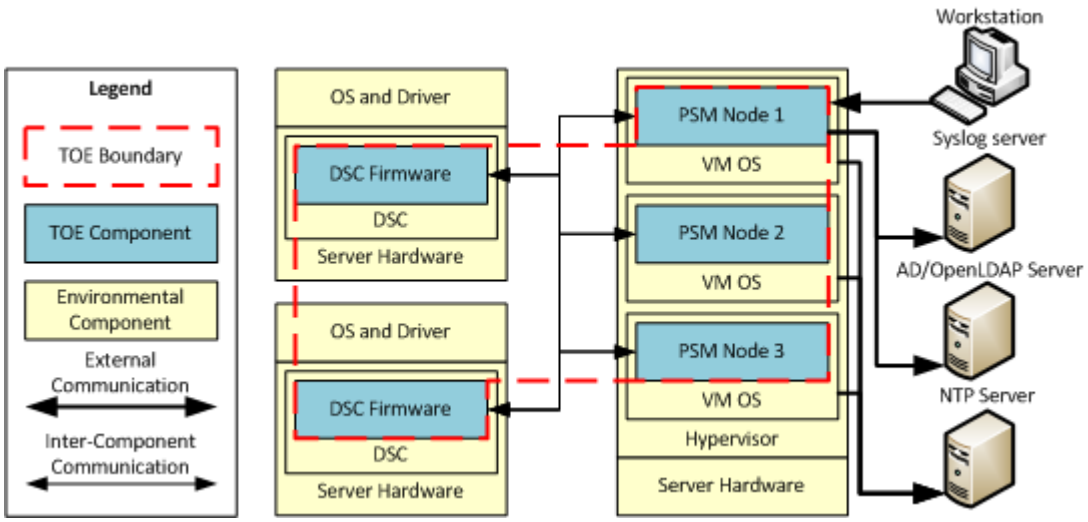

Figure 1 – Physical TOE Boundary

1.6.1.1 Guidance Documentation

The following PDF[18] formatted guides, that are available for download through the Pensando Support Portal, are required reading and part of the TOE:

- *Pensando Distributed Services Platform, Enterprise Edition Release Notes* Version 1.28.0-E-96 August 2021
- *Pensando Policy and Services Manager, Enterprise Edition User Guide* July 2021
- *Pensando Policy and Services Manager LDAP[19] Server Configuration Guide* September 2020
- *Pensando Distributed Services Platform, Enterprise Edition Troubleshooting Guide* August 2021
- *Pensando Policy and Services Manager, Enterprise Edition Design Best Practice* October 2020
- *Pensando Distributed Services Card DSC-25 User Guide for Enterprise Edition* August 2021
- *Pensando Distributed Services Card DSC-100 User Guide for Enterprise Edition* August 2021
- *Pensando Systems, Inc.; Distributed Services Platform v1.28.0-E-96; Guidance Documentation Supplement*; Evaluation Assurance Level (EAL): EAL2+; Document Version: 0.4

1.6.2 Logical Scope

The logical boundary of the TOE will be broken down into the following security classes which are further described in sections 6 and 7 of this ST. The logical scope also provides the description of the security features of the TOE. The SFRs implemented by the TOE are usefully grouped under the following Security Function Classes:

- Security Audit
- Identification and Authentication
- Security Management
- Protection of the TOE Security Functionality (TSF)
- Resource Utilization
- TOE Access

[18] PDF – Portable Document Format
[19] LDAP – Lightweight Directory Access Protocol

©2022 Pensando Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

- Trusted Path/Channel

1.6.2.1 Security Audit

The TOE generates audit records for startup and shutdown of audit functions, authentication, password changes, node failures, and management operations. It is able to associate audit records with the TOE user that caused the audited event. Audit records are presented in a human-readable manner and are only viewable if the account has the AdminRole assigned to it or a role with the All permission assigned to it. While viewing the audit records, the TOE user can order the rows by the values in the Time column.

The TOE will also monitor audit events for administrator-defined criteria and send an alert to a syslog server once the criteria is met.

1.6.2.2 Identification and Authentication

The TOE maintains the following security attributes for each local account: full name, email, roles, login name, password, and authentication type. When setting a password, the TOE will also enforce its password complexity rules. When typing a password, the TOE obfuscates the characters using the bullet character.

The TOE requires authentication and identification before any action can be taken within the TOE except for viewing the internal REST API documentation. When authenticating to the TOE, TOE users can use one of the following authentication methods: local and directory-based authentication.

1.6.2.3 Security Management

The TOE provides management functions for security-related functionality including the management of alert policies, alert destinations, accounts, roles, authentication methods, mirror sessions, and DSC hosts. The TOE had the default AdminRole when first setup but is capable of maintaining any administrator-defined role created by the TOE users.

1.6.2.4 Protection of the TSF

The TOE preserves a secure state when a PSM node fails. While a node is down, the TOE still provides all of its functionality. The TOE provides reliable timestamps by utilizes the system's time, which is synchronized to an NTP server.

1.6.2.5 Resource Utilization

The TOE ensures that it provides all of its functionality while a PSM node has failed.

1.6.2.6 TOE Access

While using the TOE's Web UI, TOE users have an option to terminate their own session by clicking on the sign out link.

1.6.2.7 Trusted Path/Channel

The TOE provides trusted channels between itself and the AD/OpenLDAP server in the OE using TLS connections. The TOE also provides trusted paths between itself and remote TOE users using TLS connections to secure authentication and all TSF-related activities.

©2022 Pensando Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

1.6.3 Product Physical/Logical Features and Functionality not included in the TOE

Features and/or Functionality that are not part of the evaluated configuration of the TOE are:

- Functionality provided by the DSC driver on the host's OS
- Functionality that is covered by only the Enterprise Pro service level agreement
- RADIUS[20] authentication

[20] RADIUS – Remote Authentication Dial-In User Service

©2022 Pensando Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

2. Conformance Claims

This section and Table 4 provide the identification for any CC, PP, and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 4 – CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017; CC Part 2 conformant; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the CEM[21] as of 2020-12-04 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2+ augmented with Flaw Remediation (ALC_FLR.2)

[21] CEM – Common Evaluation Methodology

©2022 Pensando Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

3. Security Problem

This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains all:

- Known and presumed threats countered by either the TOE or by the security environment
- Organizational security policies to which the TOE must comply
- Assumptions about the secure usage of the TOE, including physical, personnel, and connectivity aspects

3.1 Threats to Security

This section identifies the threats to the IT[22] assets against which protection is required by the TOE or by the security environment. The threat agents are divided into two categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings or parameters, and no physical access to the TOE.
- TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings or parameters, and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE.)

Both are assumed to have a low level of motivation. The IT assets requiring protection are the TSF and user data saved on or transitioning through the TOE and the hosts on the protected network. Removal, diminution, and mitigation of the threats are through the objectives identified in Section 4 Security Objectives. Table 5 below lists the applicable threats.

Table 5 – Threats

Name	Description
T.CONFIG	A TOE user or attacker could improperly gain access to TSF data if the product is misconfigured or does not enforce proper roles and permissions.
T.CRITICAL_FAILURE	A TOE user or attacker could corrupt the TOE to cause a critical failure that prevents TOE users from being able to access TOE functionality.
T.INTERCEPT	A TOE user or attacker may be able to view or modify data that is transmitted between the TOE and a remote authorized external entity.
T.MASQUERADE	A TOE user or attacker may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
T.NO_AUDIT	A TOE user or attacker may perform security-relevant operations on the TOE without being held accountable for them.
T.TAMPERING	A TOE user or attacker may be able to bypass the TOE's security mechanisms without being detected by tampering with the TOE or TOE environment.

[22] IT – Information Technology

©2022 Pensando Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Name	Description
T.UNAUTHORIZED	A TOE user or attacker may gain access to security data stored on the TOE, even though the user is not authorized in accordance with the TOE security policy.

3.2 Organizational Security Policies

An Organizational Security Policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE. There are no OSPs defined for this Security Target.

3.3 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. Table 6 lists the specific conditions that are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 6 – Assumptions

Name	Description
A.INSTALL	The TOE is installed on the appropriate, dedicated hardware and operating system.
A.NETCON	The TOE environment provides the network connectivity required to allow the TOE to provide secure network connections.
A.TIMESTAMP	The TOE's OE must provide a connection to an NTP server so the TOE can create reliable timestamps.
A.PROTECT	The TOE will be protected from unauthorized modification. The TOE and OE components are located within a controlled access facility.
A.NOEVIL	There are one or more competent TOE users assigned to manage the TOE, its OE, and the security of the information it contains. The TOE users are non-hostile, appropriately trained, and follow all guidance.

©2022 Pensando Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

4. Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 3). The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment.

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are listed in Table 7 below.

Table 7 – Security Objectives for the TOE

Name	Description
O.AUDIT_GEN	The TOE must record events of security relevance at the "not specified level" of audit and associate TOE users to audit records when applicable. The TOE must record the resulting actions for security-related management, authentication, password changes, and node failures. When recording audit events, the TOE must use a reliable timestamp.
O.AUDIT_REVIEW	The TOE must provide the authorized TOE users with the ability to review the audit trail in a human-legible format. The TOE must also allow TOE users to order the records based on date and time.
O.AUDIT_ALERT	The TOE must provide functionality to manage rules for monitoring audit events and sending an alert based on those rules.
O.AUTH_ATTRIBUTES	The TOE must be able to maintain security attributes related to TOE users and their accounts. Passwords saved by the TOE must also pass a complexity check before being saved.
O.LOGIN	The TOE must be able to identify and authenticate users prior to allowing access to TOE and its data except for noted areas. When authenticating, the TOE must be able to accept local or AD/OpenLDAP accounts. The TOE must also obscure passwords that are entered into its graphical interfaces. After logging in, the TOE must provide the TOE user with a method of terminating their session.
O.MANAGEMENT	The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate roles and only those TOE users, may exercise such control.
O.FAIL_SECURE	The TOE must preserve a secure state and provide all of its functions in the event of a node failure without loss of data or functionality.
O.SECURE_COMMS	The TOE must provide protected communications for TOE users and AD/OpenLDAP server for access to and from the TOE.

4.2 Security Objectives for the Operational Environment

This section describes the environmental objectives.

4.2.1 IT Security Objectives

Table 8 below lists the IT security objectives that are to be satisfied by the environment.

©2022 Pensando Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Table 8 – IT Security Objectives

Name	Description
OE.TIME	The TOE environment must provide a connection to the NTP server so the TOE can provide a reliable timestamp.
OE.PROTECT	The TOE environment must protect itself and the TOE from external interference or tampering.
OE.PLATFORM	The DSC host hardware and PSM OS must support all required TOE functions.
OE.TRAFFIC	The TOE environment must be implemented such that the TOE is appropriately located within the network to perform its intended function.

4.2.2 Non-IT Security Objectives

Table 9 below lists the non-IT environment security objectives that are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 9 – Non-IT Security Objectives

Name	Description
NOE.MANAGE	Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.
NOE.PHYSICAL	The TOE and its required OE components must be located in a physically secured room or data center with the appropriate level of physical access control and physical protections (e.g., badge access, fire control, locks, alarms, etc.). The physical environment must be suitable for supporting a computing device in a secure setting.

©2022 Pensando Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

5. Extended Components

There are no extended SFRs and extended SARs for this TOE.

©2022 Pensando Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

6. Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

6.1 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the Security Target reader.

The CC allows for assignment, refinement, selection and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Part 2 of the CC and are shown as follows:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [underlined text within brackets].
- Completed assignment statements within a selection statement are identified using [*underlined and italicized text within brackets*].

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 10 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement. Note that the following column names are abbreviations: S=Selection, A=Assignment, R=Refinement, and I=Iteration.

Table 10 – TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_ARP.1	Security alarms		✓		
FAU_GEN.1	Audit Data Generation	✓	✓		
FAU_GEN.2	User Identity Association				
FAU_SAA.1	Potential violation analysis		✓		
FAU_SAR.1	Audit review		✓		
FAU_SAR.3	Selectable audit review		✓		
FIA_ATD.1	User attribute definition		✓		
FIA_SOS.1	Verification of secrets		✓		
FIA_UAU.1	Timing of authentication		✓		
FIA_UAU.5	Multiple authentication mechanisms		✓		
FIA_UAU.7	Protected authentication feedback		✓		
FIA_UID.1	Timing of identification		✓		
FMT_SMF.1	Specification of Management Functions		✓		

©2022 Pensando Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Name	Description	S	A	R	I
FMT_SMR.1	Security roles		✓		
FPT_FLS.1	Failure with preservation of secure state		✓		
FPT_STM.1	Reliable time stamps				
FRU_FLT.2	Limited fault tolerance		✓		
FTA_SSL.4	User-initiated termination				
FTP_ITC.1	Inter-TSF trusted channel	✓	✓		
FTP_TRP.1	Trusted path	✓	✓		

6.2.1 Class FAU: Security Audit

FAU_ARP.1 Security alarms

Hierarchical to: No other components.
Dependencies: FAU_SAA.1 Potential violation analysis

FAU_ARP.1.1

The TSF shall take [*display the alert entry in the Alerts table and send a syslog alert to the administrator-defined destination*] upon detection of a potential security violation.

Application Note: The PSM component of the TOE, which sends alerts, contains a deduplication feature that will count duplicate events that are triggered within a short amount of time instead of making a new audit log or sending a new alert for the duplicate entry.

FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.
Dependencies: FPT_STM.1 Reliable time stamps

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
c. [*The following auditable events related to the TSF:*
   - *Managing alert policies*
   - *Managing alert destinations*
   - *Managing TOE user accounts*
   - *Managing roles*
   - *Managing authentication methods*
   - *Managing mirror sessions*
   - *Managing DSC hosts*
   - *Authentication*
   - *Password changes*
   - *Failure of a PSM node*

   ].

FAU_GEN.1.2

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

©2022 Pensando Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

a. Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b. For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [
   - *The following columns are displayed on the Events page: Severity, Type, Message, Object Ref, Count, Source Node & Component, and Time*
   - *The following columns are displayed on the Audit Event page: Who, Time, Action, Act On (kind), Act On (name), Outcome, Client, Service Node, and Service Name*

   ].

FAU_GEN.2 User identity association

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_GEN.2.1

For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_SAA.1 Potential violation analysis

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation

FAU_SAA.1.1

The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2.

The TSF shall enforce the following rules for monitoring audited events:

a. Accumulation or combination of [*administrator-defined criteria against audit event fields*] known to indicate a potential security violation;
b. [*The TSF shall also set the alert's severity to either info, warn, or critical based on the administrator's choice when defining the alert policy*].

FAU_SAR.1 Audit review

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1

The TSF shall provide [*TOE users that have the role of AdminRole or a role with the All permission*] 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.

FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.
Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1

The TSF shall provide the ability to apply [*ordering*] of audit data based on [*the values in the Time column*].

©2022 Pensando Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

6.2.2 Class FIA: Identification and Authentication

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.
Dependencies: No dependencies
FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual users: [*full name, email, roles, login name, password, and authentication type*].

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.
Dependencies: No dependencies
FIA_SOS.1.1

The TSF shall provide a mechanism to verify that secrets meet [

- *At least 9 characters in length*
- *Contains at least 1 digit*
- *Contains at least 1 uppercase letter*
- *Contains at least 1 special character from the following: ~!@#$%^&*()_+'-={}|[]\:"<>?,./*

].

FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification
FIA_UAU.1.1

The TSF shall allow [*the viewing of the REST API documentation*] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.
Dependencies: No dependencies
FIA_UAU.5.1

The TSF shall provide [*local and directory-based authentication*] to support user authentication.

FIA_UAU.5.2

The TSF shall authenticate any user's claimed identity according to the [*administrator-defined order for the authentication methods within the TOE and following the below rules for each method:*

- *Local authentication – The TOE user navigates to the TOE and enters their local account's credentials either in the Web UI or through a REST API Client. The TOE searches for the entered username in the local accounts database. If it is found, the entered password is compared to the stored password for that account. If the passwords match, the TOE user is bound to the appropriate roles and allowed access to the TOE.*
- *Directory-based authentication – The TOE user navigates to the TOE and enters their domain account's credentials either in the Web UI or through a REST API Client. The TOE forwards the credentials to the AD/OpenLDAP server. The AD/OpenLDAP server evaluates the credentials, and if the username corresponds to a valid domain user and the password matches the stored*

©2022 Pensando Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

password, the AD/OpenLDAP server sends a successful message back to the TOE. The account's AD/OpenLDAP groups are queried to bind the account to the correct roles in the TOE, and the TOE user is allowed access to the TOE.].

FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1

The TSF shall provide only [*bullets characters*] to the user while the authentication is in progress.

FIA_UID.1 Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies

FIA_UID.1.1

The TSF shall allow [*the viewing of the REST API documentation*] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2

The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.2.3 Class FMT: Security Management

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No Dependencies

FMT_SMF.1.1

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

- *Managing alert policies*
- *Managing alert destinations*
- *Managing TOE user accounts*
- *Managing roles*
- *Managing authentication methods*
- *Manage mirror sessions*
- *Manage DSC hosts*

].

FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1

The TSF shall maintain the roles [*AdminRole and any administrator-defined roles created by the TOE users*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

©2022 Pensando Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

6.2.4 Class FPT: Protection of the TSF

FPT_FLS.1 Failure with preservation of secure state
Hierarchical to: No other components.
Dependencies: No dependencies.
FPT_FLS.1.1
The TSF shall preserve a secure state when the following types of failures occur: [*failure of a PSM node*].

FPT_STM.1 Reliable time stamps
Hierarchical to: No other components.
Dependencies: No dependencies
FPT_STM.1.1
The TSF shall be able to provide reliable time stamps.

6.2.5 Class FRU: Resource Utilization

FRU_FLT.2 Limited fault tolerance
Hierarchical to: FRU_FLT.1 Degraded fault tolerance
Dependencies: FPT_FLS.1 Failure with preservation of secure state
FRU_FLT.2.1
The TSF shall ensure the operation of all the TOE's capabilities when the following failures occur: [*failure of a PSM node*].

6.2.6 Class FTA: TOE Access

FTA_SSL.4 User-initiated termination
Hierarchical to: No other components.
Dependencies: No dependencies
FTA_SSL.4.1
The TSF shall allow user-initiated termination of the user's own interactive session.

6.2.7 Class FTP: Trusted Path/Channels

FTP_ITC.1 Inter-TSF trusted channel
Hierarchical to: No other components.
Dependencies: No dependencies
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] to initiate communication via the trusted channel.
FTP_ITC.1.3
The TSF shall initiate communication via the trusted channel for [*user authentication to the AD/OpenLDAP server*].

©2022 Pensando Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

FTP_TRP.1 Trusted path

Hierarchical to: No other components.

Dependencies: No dependencies

FTP_TRP.1.1

The TSF shall provide a communication path between itself and [remote] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification, disclosure].

FTP_TRP.1.2

The TSF shall permit [remote users] to initiate communication via the trusted path.

FTP_TRP.1.3

The TSF shall require the use of the trusted path for [initial user authentication, [*all other TSF-related functionality*]].

6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are 2+ augmented with ALC_FLR.2. Table 11 summarizes these requirements.

Table 11 – Assurance Requirements

Assurance Requirements	
Class 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
Class ALC: Life Cycle Support	ALC_CMC.2 Use of a CM[23] system
	ALC_CMS.2 Parts of the TOE CM Coverage
	ALC_DEL.1 Delivery Procedures
	ALC_FLR.2 Flaw Reporting Procedures
Class ADV: Development	ADV_ARC.1 Security Architecture Description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing

[23] CM – Configuration Management

©2022 Pensando Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Assurance Requirements	
	ATE_IND.2 Independent testing – Sample
Class AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

©2022 Pensando Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

7. TOE Summary Specification

This section presents information to detail how the TOE meets the functional requirements described in previous sections of this ST.

7.1 TOE Security Functionality

Each of the security requirements and the associated descriptions correspond to a security functionality. Hence, each security functionality is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functionality and rationalize that the security functionality satisfies the necessary requirements. Table 12 lists the security functionality and their associated SFRs.

Table 12 – Mapping of TOE Security Functionality to Security Functional Requirements

TOE Security Functionality	SFR ID[24]	Description
Security Audit	FAU_ARP.1	Security alarms
	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_SAA.1	Potential violation analysis
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
Identification and Authentication	FIA_ATD.1	User attribute definition
	FIA_SOS.1	Verification of secrets
	FIA_UAU.1	Timing of authentication
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.1	Timing of identification
Security Management	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
Protection of the TSF	FPT_FLS.1	Failure with preservation of secure state
	FPT_STM.1	Reliable time stamps
Resource Utilization	FRU_FLT.2	Limited fault tolerance
TOE Access	FTA_SSL.4	User-initiated termination
Trusted Path/Channel	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1	Trusted path

[24] ID – Identification

©2022 Pensando Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

7.1.1 Security Audit

To ensure the audit functionality is active, the TOE generates audit records for startup and shutdown of audit functions. While the TOE is active, it will generate audit records for authentication, password changes, node failures, and management of the following areas: alert policies, alert destinations, accounts, roles, and authentication methods. If applicable, the audit records will indicate the TOE user account that caused the audited event. Audit records are presented in a human-readable manner and are only viewable if the account has the AdminRole assigned to it or a role with the All permission assigned to it. While viewing the audit records, the TOE user can order the rows by the values in the Time column.

Table 13 describes the columns that are displayed on the Events page:

Table 13 – Events Page

Column Name	Description
Severity	The severity of an alert that was set by its rules. Valid options include info, warn, and critical.
Type	The category of the event.
Message	The description of the event that will be sent to the destination.
Object Ref	The specific object in the setup that produces this event.
Count	The amount of times the event was seen over 10 seconds.
Source Node & Component	The IP[25] address of the cluster's node the event processed from and the PSM service that was used.
Time	The timestamp of the event.

Table 14 describes the columns that are displayed on the Audit Events page:

Table 14 – Audit Events Page

Column Name	Description
Who	The TOE user caused the action.
Time	The timestamp of the event.
Action	The type of action was executed. Examples are read, login, create, etc.
Act On (kind)	The kind of object the action was executed on. Examples are workload, host, network security policy, etc.
Act On (name)	The name of the object that the action was executed on.
Outcome	The result of the event.
Client	The source IP where the action was executed from.
Service Node	The cluster's node the event processed from.
Service Name	The PSM service that was used.

The TOE also follows administrator-defined rules called alert policies to monitor audit events for criteria that could indicate potential security violations. The rules are defined based on the text of the audit events and the count of how many have been seen. The alert policies will also set the alerts severity for use in the receiving system. Once the policy's criteria are met, the TOE will send an alert to the alert destination (the syslog server) for further actions.

[25] IP – Internet Protocol

©2022 Pensando Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

TOE Security Functional Requirements Satisfied: FAU_ARP.1, FAU_GEN.1, FAU_GEN.2, FAU_SAA.1, FAU_SAR.1, FAU_SAR.3.

7.1.2 Identification and Authentication

When managing local accounts, the TOE maintains the following security attributes that are associated to each of them: full name, email, roles, login name, password, and authentication type. The full name and email attributes are optional. The TOE will enforce the following password complexity rules on any password that a TOE user tries to save to an account's security attributes:

- At least 9 characters in length
- Contains at least 1 digit
- Contains at least 1 uppercase letter
- Contains at least 1 special character from the following: ~!@#$%^&*()_+'-={}|[]\:"<>?,./

The TOE requires authentication and identification before any action can be taken within the TOE except for viewing the internal REST API documentation. When typing a password during authentication, the TOE obfuscates the characters using the bullet character. When authenticating to the TOE, TOE users can use one of the following authentication methods: local and directory-based authentication. The order that the TOE authentications TOE users is administrator-defined to allow for efficient authentication. The TOE will follow the below rules for each authentication method:

- Local authentication – The TOE user navigates to the TOE and enters their local account's credentials either in the Web UI or through a REST API Client. The TOE searches for the entered username in the local accounts database. If it is found, the entered password is compared to the stored password for that account. If the passwords match, the TOE user is bound to the appropriate roles and allowed access to the TOE.
- Directory-based authentication – The TOE user navigates to the TOE and enters their domain account's credentials either in the Web UI or through a REST API Client. The TOE forwards the credentials to the AD/OpenLDAP server. The AD/OpenLDAP server evaluates the credentials, and if the username corresponds to a valid domain user and the password matches the stored password, the AD/OpenLDAP server sends a successful message back to the TOE. The account's AD/OpenLDAP groups are queried to bind the account to the correct roles in the TOE, and the TOE user is allowed access to the TOE.

TOE Security Functional Requirements Satisfied: FIA_ATD.1, FIA_SOS.1, FIA_UAU.1, FIA_UAU.5, FIA_UAU.7, FIA_UID.1.

7.1.3 Security Management

The TOE capable of performing the following management functions:

- Managing alert policies – A TOE user can create, edit, or delete policies that will monitor the audit records for sending alerts to different destinations.
- Managing alert destinations – A TOE user can create, edit, or delete the destinations used by the alert policies for sending their alerts to.

©2022 Pensando Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

- Managing accounts – A TOE user can create, edit, or delete TOE user accounts or their security attributes that are saved within the TOE. The admin account cannot be deleted.
- Managing roles – A TOE user can create, edit, or delete role bindings, roles, and the permissions that make-up the roles. When deleting roles, at least one must be kept for binding to user accounts.
- Managing authentication methods – A TOE user can create, edit, or delete connections to the authentication servers in the OE. They can also setup the priority order for the different authentication methods.
- Managing mirror sessions – A TOE user can create, edit, or delete a mirror session, which allows PSM to send mirrored traffic from the DSC to an external destination collector.
- Managing DSC hosts – A TOE user can add, edit, and remove DSC hosts in the TOE that are managed by the PSM cluster.

The TOE maintains the default role named AdminRole that is setup during installation. It is also capable of maintaining any administrator-defined role created by the TOE users. The created roles are comprised of different permissions that give access to the various functions within the TOE's boundary.

TOE Security Functional Requirements Satisfied: FMT_SMF.1, FMT_SMR.1.

7.1.4 Protection of the TSF

When a PSM node fails, the TOE provides a secure state that protects the TOE users and TSF data. This is possible because while a node is down, there will always be a leader node provides all of the PSM functionality within the TOE.

The TOE provides reliable timestamps by utilizes the system's time, which is synchronized to an NTP server.

TOE Security Functional Requirements Satisfied: FPT_FLS.1, FPT_STM.1.

7.1.5 Resource Utilization

The TOE ensures that it provides all of its functionality while a PSM node has failed. It does this with the 3-node high availability setup. If the leader node fails, one of the other nodes becomes the new leader and provides all the needed PSM functionality that is within the TOE boundary.

TOE Security Functional Requirements Satisfied: FRU_FLT.2.

7.1.6 TOE Access

TOE users can log out of their account to terminate their session by clicking on the user icon in the top right and choosing the sign out link.

TOE Security Functional Requirements Satisfied: FTA_SSL.4.

©2022 Pensando Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

7.1.7 Trusted Path/Channels

The TOE uses TLS to provides trusted channels between itself and the AD/OpenLDAP server in the OE. The connection to the AD/OpenLDAP server is made using LDAP over TLS, which is known as LDAPS, for the directory-based authentication method.

The TOE also uses TLS to provide trusted paths between itself and remote TOE users. The browser on a workstation initiates the remote connection to the TOE with HTTP over TLS, which is known as HTTPS, for TOE user authentication and TSF-related activities. The REST client on a workstation initiates the remote connection to the TOE over HTTPS for programmatic authentication and TSF-related activities.

TOE Security Functional Requirements Satisfied: FTP_ITC.1, FTP_TRP.1.

©2022 Pensando Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

8. Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 and Part 3 of the *Common Criteria for Information Technology Security Evaluation*, Version 3.1 Revision 5.

8.2 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target. Sections 8.2.1, 8.2.2, and 8.2.3 demonstrate the mappings between the threats, policies, and assumptions to the security objectives are complete. The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

8.2.1 Security Objectives Rationale Relating to Threats

Table 15 below provides a mapping of the objectives to the threats they counter.

Table 15 – Threats: Objectives Mapping

Threats	Objectives	Rationale
T.CONFIG A TOE user or attacker could improperly gain access to TSF data if the product is misconfigured or does not enforce proper roles and permissions.	O.MANAGEMENT The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate roles and only those TOE users, may exercise such control.	O.MANAGEMENT supports the mitigation of this threat by ensuring that only authorized users may configure the TOE security mechanisms and enforces the proper role permissions on accounts.
	OE.PLATFORM The DSC host hardware and PSM OS must support all required TOE functions.	OE.PLATFORM ensures that the TOE is installed on the appropriate OE components to properly support the TOE.
T.CRITICAL_FAILURE A TOE user or attacker could corrupt the TOE to cause a critical failure that prevents TOE users from being able to access TOE functionality.	O.FAIL_SECURE The TOE must preserve a secure state and provide all of its functions in the event of a node failure without loss of data or functionality.	O.FAIL_SECURE mitigates this threat by ensuring that the TOE is capable of maintaining a secure state and offering its full set of security functionalities in the event of a node failure.
T.INTERCEPT A TOE user or attacker may be able to view or modify data that is transmitted between the TOE and a remote authorized external entity.	O.SECURE_COMMS The TOE must provide protected communications for TOE users and AD/OpenLDAP server for access to and from the TOE.	O.SECURE_COMMS mitigates this threat by ensuring that communications between the TOE, workstation, and AD/OpenLDAP server are not tampered with.
	OE.PROTECT The TOE environment must protect itself and the TOE from external interference or tampering.	OE.PROTECT ensures that the TOE is installed in an environment that would protect it from interference or tampering.

©2022 Pensando Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Threats	Objectives	Rationale
T.MASQUERADE A TOE user or attacker may masquerade as another entity in order to gain unauthorized access to data or TOE resources.	O.LOGIN The TOE must be able to identify and authenticate users prior to allowing access to TOE and its data except for noted areas. When authenticating, the TOE must be able to accept local or AD/OpenLDAP accounts. The TOE must also obscure passwords that are entered into its graphical interfaces. After logging in, the TOE must provide the TOE user with a method of terminating their session.	By ensuring that The TOE is able to identify and authenticate TOE users prior to allowing access to TOE administrative functions and data, O.LOGIN mitigates this threat.
	O.MANAGEMENT The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate roles and only those TOE users, may exercise such control.	O.MANAGEMENT mitigates this threat by ensuring that only authorized users may configure the TOE security mechanisms and enforces the proper role permissions on accounts.
T.NO_AUDIT A TOE user or attacker may perform security-relevant operations on the TOE without being held accountable for them.	O.AUDIT_GEN The TOE must record events of security relevance at the “not specified level” of audit and associate TOE users to audit records when applicable. The TOE must record the resulting actions for security-related management, authentication, password changes, and node failures. When recording audit events, the TOE must use a reliable timestamp.	O.AUDIT_GEN mitigates this threat by ensuring that security relevant events are recorded and include the TOE user that initiated the task (if applicable).
	O.AUDIT_REVIEW The TOE must provide the authorized TOE users with the ability to review the audit trail in a human-legible format. The TOE must also allow TOE users to order the records based on date and time.	O.AUDIT_REVIEW mitigates this threat by allowing TOE users to review audited activities in a human-legible manor.
	OE.TIME The TOE environment must provide a connection to the NTP server so the TOE can provide a reliable timestamp.	OE.TIME supports the mitigation of this threat by ensuring the TOE has a time source that it can use for its audit logging.
T.TAMPERING A TOE user or attacker may be able to bypass the TOE’s security mechanisms without being detected by tampering with the TOE or TOE environment.	O.AUDIT_ALERT The TOE must provide functionality to manage rules for monitoring audit events and sending an alert based on those rules.	O.AUDIT_ALERT mitigates this threat by allowing TOE users to define alert policies that can identify tampering attempts and notify the TOE users.
	O.AUDIT_GEN The TOE must record events of security relevance at the “not specified level” of audit and associate TOE users to audit records when applicable. The TOE must record the resulting actions for security-related management, authentication, password changes, and node failures. When recording audit events, the TOE must use a reliable timestamp.	O.AUDIT_GEN ensures that security relevant events that may indicate attempts to tamper with the TOE are recorded.

©2022 Pensando Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Threats	Objectives	Rationale
	O.LOGIN The TOE must be able to identify and authenticate users prior to allowing access to TOE and its data except for noted areas. When authenticating, the TOE must be able to accept local or AD/OpenLDAP accounts. The TOE must also obscure passwords that are entered into its graphical interfaces. After logging in, the TOE must provide the TOE user with a method of terminating their session.	O.LOGIN supports the mitigation of this threat by ensuring that only TOE users with valid credentials are able to modify the TOE and its data.
	O.MANAGEMENT The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate roles and only those TOE users, may exercise such control.	O.MANAGEMENT supports the mitigation of this threat by ensuring that only authorized users may configure the TOE security mechanisms.
	OE.PROTECT The TOE environment must protect itself and the TOE from external interference or tampering.	OE.PROTECT ensures that the TOE is protected from external interference or tampering.
T.UNAUTHORIZED A TOE user or attacker may gain access to security data stored on the TOE, even though the user is not authorized in accordance with the TOE security policy.	O.AUDIT_GEN The TOE must record events of security relevance at the “not specified level” of audit and associate TOE users to audit records when applicable. The TOE must record the resulting actions for security-related management, authentication, password changes, and node failures. When recording audit events, the TOE must use a reliable timestamp.	O.AUDIT_GEN ensures that unauthorized attempts to access the TOE are recorded.
	O.AUTH_ATTRIBUTES The TOE must be able to maintain security attributes related to TOE users and their accounts. Passwords saved by the TOE must also pass a complexity check before being saved.	O.AUTH_ATTRIBUTES mitigates this threat by ensuring that the TOE maintains associated roles with the TOE user accounts so they can only access TOE functionality they have permission to.
	O.LOGIN The TOE must be able to identify and authenticate users prior to allowing access to TOE and its data except for noted areas. When authenticating, the TOE must be able to accept local or AD/OpenLDAP accounts. The TOE must also obscure passwords that are entered into its graphical interfaces. After logging in, the TOE must provide the TOE user with a method of terminating their session.	O.LOGIN mitigates this threat by ensuring that TOE users are identified and authenticated prior to gaining access to TOE security data.

©2022 Pensando Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Threats	Objectives	Rationale
	O.MANAGEMENT The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate roles and only those TOE users, may exercise such control.	O.MANAGEMENT supports the mitigation of this threat by ensuring that only roles and permissions are applied to TOE users to control their access within the TOE.

Every threat is mapped to one or more objectives in the table above. This complete mapping demonstrates that the defined security objectives counter all defined threats.

8.2.2 Security Objectives Rationale Relating to Policies

There are no Organizational Security Policies defined for this Security Target.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 16 below gives a mapping of assumptions and the environmental objectives that uphold them.

Table 16 – Assumptions: Objectives Mapping

Assumptions	Objectives	Rationale
A.INSTALL The TOE is installed on the appropriate, dedicated hardware and operating system.	OE.PLATFORM The DSC host hardware and PSM OS must support all required TOE functions.	OE.PLATFORM satisfies the assumption that the TOE hardware and OS supports the TOE functions.
	NOE.MANAGE Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.	NOE.MANAGE satisfies the assumption that those responsible for the TOE will provide competent TOE users to perform management of the security of the environment and restrict these functions and facilities from unauthorized use.
	NOE.PHYSICAL The TOE and its required OE components must be located in a physically secured room or data center with the appropriate level of physical access control and physical protections (e.g., badge access, fire control, locks, alarms, etc.). The physical environment must be suitable for supporting a computing device in a secure setting.	NOE.PHYSICAL satisfies the assumption that there will be physical security for the TOE and OE to appropriately protection all components of this setup.
A.NETCON The TOE environment provides the network connectivity required to allow the TOE to provide secure network connections.	OE.TRAFFIC The TOE environment must be implemented such that the TOE is appropriately located within the network to perform its intended function.	OE.TRAFFIC satisfies the assumption that the TOE environment will provide the appropriate connectivity to allow the TOE to perform its function.
A.TIMESTAMP The TOE's OE must provide a connection to an NTP server so the TOE can create reliable timestamps.	OE.TIME The TOE environment must provide a connection to the NTP server so the TOE can provide a reliable timestamp.	OE.TIME satisfies the assumption that the OE provides a connection to an NTP server so the TOE can create reliable timestamps.

©2022 Pensando Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Assumptions	Objectives	Rationale
A.PROTECT The TOE will be protected from unauthorized modification. The TOE and OE components are located within a controlled access facility.	OE.PROTECT The TOE environment must protect itself and the TOE from external interference or tampering.	OE.PROTECT satisfies the assumption that the TOE environment provides protection from external interference or tampering.
	NOE.PHYSICAL The TOE and its required OE components must be located in a physically secured room or data center with the appropriate level of physical access control and physical protections (e.g., badge access, fire control, locks, alarms, etc.). The physical environment must be suitable for supporting a computing device in a secure setting.	NOE.PHYSICAL satisfies the assumption that the TOE will be located in an access-controlled facility and all components of this setup are protected from unauthorized modification.
A.NOEVIL There are one or more competent TOE users assigned to manage the TOE, its OE, and the security of the information it contains. The TOE users are non-hostile, appropriately trained, and follow all guidance.	NOE.MANAGE Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.	NOE.MANAGE satisfies the assumption that the TOE users who manage the TOE are non-hostile, appropriately trained and follow all guidance.

Every assumption is mapped to one or more objectives in the table above. This complete mapping demonstrates that the defined security objectives uphold all defined assumptions.

8.3 Rationale for Extended Security Functional Requirements

There are no extended functional requirements defined for this TOE.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended functional requirements defined for this TOE.

8.5 Security Requirements Rationale

The following discussion provides detailed evidence of coverage for each security objective.

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 17 below shows a mapping of the objectives and the SFRs that support them.

©2022 Pensando Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Table 17 – Objectives: SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.AUDIT_GEN The TOE must record events of security relevance at the "not specified level" of audit and associate TOE users to audit records when applicable. The TOE must record the resulting actions for security-related management, authentication, password changes, and node failures. When recording audit events, the TOE must use a reliable timestamp.	FAU_GEN.1 Audit Data Generation	The requirement meets this objective by ensuring that the TOE maintains a record of defined security related events, including relevant details about the event.
	FAU_GEN.2 User Identity Association	The requirement meets this objective by ensuring that the TOE associates TOE users to applicable audit events.
O.AUDIT_REVIEW The TOE must provide the authorized TOE users with the ability to review the audit trail in a human-legible format. The TOE must also allow TOE users to order the records based on date and time.	FAU_SAR.1 Audit review	The requirement meets the objective by ensure that the TOE provides the ability to review logs.
	FAU_SAR.3 Selectable audit review	The requirement meets this objective by ensuring that the TOE provides a method for ordering audit records by date and time.
	FPT_STM.1 Reliable time stamps	The requirement meets this objective by ensuring that the TOE provides a reliable timestamp for audit records.
O.AUDIT_ALERT The TOE must provide functionality to manage rules for monitoring audit events and sending an alert based on those rules.	FAU_ARP.1 Security alarms	The requirement meets this objective by ensuring that the TOE sends alerts based on rules that monitor audit events.
	FAU_SAA.1 Potential violation analysis	The requirement meets this objective by ensuring that the TOE provides functionality to create and manage rules for monitoring audit events.
O.AUTH_ATTRIBUTES The TOE must be able to maintain security attributes related to TOE users and their accounts. Passwords saved by the TOE must also pass a complexity check before being saved.	FIA_ATD.1 User attribute definition	The requirement meets this objective by ensuring that the TOE maintains security attributes for each local account that belongs to a TOE user.
	FIA_SOS.1 Verification of secrets	The requirement meets this objective by ensuring that the TOE enforces a minimum password complexity for local accounts.
O.LOGIN The TOE must be able to identify and authenticate users prior to allowing access to TOE and its data except for noted areas. When authenticating, the TOE must be able to accept local or AD/OpenLDAP accounts. The TOE must also obscure passwords that are entered into its graphical interfaces. After logging in, the TOE must provide the TOE user with a method of terminating their session.	FIA_UAU.1 Timing of authentication	The requirement meets this objective by ensuring that the TOE authenticates TOE users before they can gain access to TOE administrative functions with the exception of opening the REST API documentation.
	FIA_UAU.5 Multiple authentication mechanisms	The requirement meets this objective by ensuring that the TOE provides local and AD/OpenLDAP methods of authentication to TOE users.
	FIA_UAU.7 Protected authentication feedback	The requirement meets this objective by ensuring that the TOE obscures passwords that are entered into the Web UI.

©2022 Pensando Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Objective	Requirements Addressing the Objective	Rationale
	FIA_UID.1 Timing of identification	The requirement meets this objective by ensuring that the TOE identifies TOE users before they can gain access to TOE administrative functions with the exception of opening the REST API documentation.
	FTA_SSL.4 User-initiated termination	The requirement meets this objective by ensuring that the TOE provides functionality that allows TOE users to terminate their own Web UI session.
O.MANAGEMENT The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate roles and only those TOE users, may exercise such control.	FMT_SMF.1 Specification of management functions	The requirement meets this objective by ensuring that the TOE includes administrative functions to facilitate the management of the TSF.
	FMT_SMR.1 Security roles	The requirement meets this objective by ensuring that the TOE associates TOE users with roles and permissions to provide access to TSF management functions and data.
O.FAIL_SECURE The TOE must preserve a secure state and provide all of its functions in the event of a node failure without loss of data or functionality.	FPT_FLS.1 Failure with preservation of secure state	The requirement meets this objective by ensuring that the TOE preserves a secure state when a node fails.
	FRU_FLT.2 Limited fault tolerance	The requirement meets this objective by ensuring that the TOE provides all of its functionality when a node fails.
O.SECURE_COMMS The TOE must provide protected communications for TOE users and AD/OpenLDAP server for access to and from the TOE.	FTP_ITC.1 Inter-TSF trusted channel	The requirement meets this objective by ensuring that the TOE protects communications from the TOE to the AD/OpenLDAP server.
	FTP_TRP.1 Trusted path	The requirement meets this objective by ensuring that the TOE protects communications from the remote TOE user's workstation to the TOE.

8.5.2 Security Assurance Requirements Rationale

EAL2+ was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the System may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL2+, the system will have incurred a search for obvious flaws to support its introduction into the non-hostile environment. The augmentation of ALC_FLR.2 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

©2022 Pensando Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

8.5.3 Dependency Rationale

The SFRs in this ST satisfy all of the required dependencies listed in the Common Criteria, applicable PPs, and SFRs explicitly stated in this ST. Table 18 lists each requirement to which the TOE claims conformance and indicates whether the dependent requirements are included. As the table indicates, all dependencies have been met.

Table 18 – Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_ARP.1	FAU_SAA.1	✓	
FAU_GEN.1	FPT_STM.1	✓	
FAU_GEN.2	FAU_GEN.1	✓	
	FIA_UID.1	✓	
FAU_SAA.1	FAU_GEN.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	
FAU_SAR.3	FAU_GEN.1	✓	
FIA_ATD.1	No dependencies	✓	
FIA_SOS.1	No dependencies	✓	
FIA_UAU.1	FIA_UID.1	✓	
FIA_UAU.5	No dependencies	✓	
FIA_UAU.7	FIA_UAU.1	✓	
FIA_UID.1	No dependencies	✓	
FMT_SMF.1	No dependencies	✓	
FMT_SMR.1	FIA_UID.1	✓	
FPT_FLS.1	No dependencies	✓	
FPT_STM.1	No dependencies	✓	
FRU_FLT.2	FPT_FLS.1	✓	
FTA_SSL.4	No dependencies	✓	
FTP_ITC.1	No dependencies	✓	
FTP_TRP.1	No dependencies	✓	

©2022 Pensando Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

9. Acronyms

Table 19 defines the acronyms used throughout this document.

Table 19 – Acronyms

Acronym	Definition
AD	Active Directory
API	Application Programming Interface
CC	Common Criteria
CEM	Common Evaluation Methodology
CM	Configuration Management
CPU	Central Processing Unit
DSC	Distributed Services Card
DSP	Distributed Services Platform
EAL	Evaluation Assurance Level
GB	Gigabyte
Gbps	Gigabits per second
HTTP	Hypertext Transport Protocol
ID	Identification
IP	Internet Protocol
IPFIX	Internet Protocol Flow Information Export
IT	Information Technology
KVM	Kernel-based Virtual Machine
LDAP	Lightweight Directory Access Protocol
NTP	Network Time Protocol
OE	Operating Environment
OS	Operating System
OSP	Organizational Security Policy
PCIe	Peripheral Component Interconnect Express
PDF	Portable Document Format
PP	Protection Profile
PSM	Policy and Services Manager
RADIUS	Remote Authentication Dial-In User Service
REST	Representational State Transfer
RFC	Request for Comments

©2022 Pensando Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Acronym	Definition
RJ45	Registered Jack 45
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SSD	Solid State Drive
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TOR	Top-of-Rack
TSF	TOE Security Functionality
UI	User Interface
VM	Virtual Machine

©2022 Pensando Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Prepared by:

Corsec Security, Inc.

13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
https://www.corsec.com/