scopSOC

v2

Common Criteria Evaluation

Security Target

Document Name	**:**	scopSOC V2 Security Target Lite
Document ID	**:**	scopSOC_V2_Security Target Lite_(v.1.1)
Dissemination Level	**:**	Public
Status	**:**	Final Version
Document Version	**:**	1.1
Version Date	**:**	17.02.2021
Author	**:**	Volkan NERGİZ

Revision History

Version No	Reason for Change	Release Date	Prepared By	Approved By
1.0	Initial Version	18.06.2019	Volkan NERGİZ	Berivan ARSLAN KAVGAOĞLU
1.1	Final Version	17.02.2021	Volkan NERGİZ	Berivan ARSLAN KAVGAOĞLU

TABLE OF CONTENTS

1. Introduction

The importance of cyber security is constantly increasing as organizations are becoming more dependent to information technologies. Implementation of Security Operation Center (SOC) is increasing as centralized management and advanced analytics offer new possibilities in identifying security threats.

scopSOC is an integrated platform for organizations wishing to implement a comprehensive Security Operation Center. scopSOC is easy to implement, easy to operate solution with a low cost of ownership.

This Security Target is for evaluation of scopSOC at Evaluation Assurance Level 3. This section presents Security Target Identification, TOE Overview and Description. It also includes Document Conventions and Document Terminology.

1.1. Security Target Reference

ST Title: scopSOC Security Target Lite

Version: v.1.1

1.2. TOE Reference

Target of Evaluation **:** scopSOC

Version **:** V2

Vendor **:** MAY Cyber Technology, Inc.

1.3. TOE Overview

The TOE Description summarizes the usage and major security features. It also provides a context for the TOE Evaluation by identifying the TOE type, describing the product and defining the specific evaluated configuration.

The Target of Evaluation (TOE) is the scopSOC Version 2 and will hereafter be referred to as the TOE through this document. scopSOC V2 includes all the security functions which the TOE has.

The TOE is a security operations center management system that provides an integrated platform for the effective management of an organization’s cyber security infrastructure.

1.3.1. Usage and Main Security Features

The TOE is a software-only product and consists of the Security Operation Center (SOC) software components namely; scopSOC GUI, scopSOC Server and scopSOC Client. scopSOC and its components have the following functions;

- **scopSOC GUI:** Provides a web interface for the users to interact with system and its settings
- **scopSOC Server:** Manages and maintains system operations such as collecting the logs using the collector, finding and detecting assets, sending notifications, evaluating the correlations, managing events, providing the data storage information to submodules and organizing incidents.
- **scopSOC Client:** Collects data which are event logs, system logs, processes and their status, running service information, hardware data and status, from the endpoints. An endpoint is a remote computing device that communicates back and forth with a network to which is it connected.

Roles:

Role	Access Level	Permissions
Super User	Settings, scopMON, scopDESK, scopVISION, Event Engine, Dashboard, Asset Management, Command Execution and Reporting	User role which has all privileges on the platform
Platform Manager	Settings	Configure platform level configurations
Monitoring Manager	scopMON	Monitor system and network resources
Incident and Request Manager	scopDESK	Manage and track security incident
SIEM Manager	scopVISION	Collect logs and create analytics rules
Event Manager	Event Engine	Manage security events and take centralized actions
Dashbord Manager	Dashboards	Analyze and visualize security data
Asset Manager	Asset Management	Discover assets and manage vulnerabilities
Command Execution Manager	Command Execution	Manage and create external commands
Reporting Manager	Reporting	Create and distribute reports

scopSOC should contain 8 main Security Functions which are described in the following table. All of these security functions will be examined in detail on Chapter 6.

Security Functions	DESCRIPTION
Security Audit	The TOE generates audit records for security events. Only the Super User and user authorized by Super User role is allowed to view the audit trail.
Cryptographic Support	The TOE supports cryptographic security functions for storing crucial information for user like User Password.
User Data Protection	The TOE provides specifying requirements for TOE security functions and TOE security function policies related to protecting user data.
Identification and Authentication	All users are required to perform identification and authentication before any information flows are permitted.
Security Management	The TOE provides a wide range of security management functions. Super User can configure the TOE, manage users and audit among other routine maintenance activities.
TOE Access	An interactive user session is terminated after a period of user inactivity. The user is also allowed to terminate his/her own interactive session.
Trusted Path/Channels	The TOE uses trusted path/channels to provide confidence that a user is communicating directly with the TSF whenever it is invoked. A user's response via the trusted path guarantees that untrusted applications cannot intercept or modify the user's response.
Protection of the TSF	The TOE protects the TSF data from modification when it is transmitted between separate parts of the TOE.

1.3.2. TOE Type

The TOE belongs to the "Detection Devices and Systems" category. TOE Type is software-based Security Operations Center Management System.

1.3.3. Required non-TOE Hardware, Software or Firmware

The TOE is software product that runs on a host computer. The host computer must run the operating system platform on which the TOE can execute. scopSOC has 3 main modules; scopSOC GUI, scopSOC Server and scopSOC Client. The table below shows the system requirements which enable scopSOC components to run properly. Before scopSOC components are installed, it should be checked that the required software is found on the system.

scopSOC Component	.NET Framework	IIS	MSSQL	ElacticSearch
scopSCOC GUI	✓	✓	✓	
scopSOC Server	✓		✓	✓
scopSOC Client	✓			

The minimum operating system (O/S) and hardware requirements for the scopSOC GUI host computer are:

O/S	Windows Server 2008 64-bit, or higher
CPU	4 Core 2.4 GHz, or faster
RAM	At least 16GB, preferably 32GB
Connectivity	TCP/IP network interfaces
Disk space for TOE and logs	At least 160 GB / Subject to Log details

The minimum operating system (O/S) and hardware requirements for the scopSOC Server host computer are:

O/S	Windows Server 2008 64-bit, or higher
CPU	4 Core 2.4 GHz, or faster
RAM	At least 16GB, preferably 32GB
Connectivity	TCP/IP network interfaces
Disk space for TOE and logs	At least 160 GB / Subject to Log details
Hard Drive Space	200GB

The minimum operating system (O/S) and hardware requirements for the scopSOC Client host computer are:

O/S	Windows 7 64-bit, or higher
CPU	Intel Pentium Core 2 Duo 2.4 GHz, or faster
RAM	At least 8GB, preferably 16GB
Connectivity	TCP/IP network interfaces
Disk space for TOE and logs	At least 10GB / Subject to Log details
Hard Drive Space	150GB

1.3.4. Operating Environment

This section describes the general environment in which the TOE is expected to perform. The environment of operation for the TOE is expected to be a facility that is physically secure from unauthorized intrusion. Personnel with explicit physical access to the hardware storing log data and application execution files must be authorized, trained and competent. At a minimum, a monitor, keyboard and mouse must be locally collected to the server machine in which the TOE is deployed or operated on. In addition to this the operational environment must include:

For scopSOC GUI;

• A web browser (offered Internet Explorer 10 or higher, or Mozilla Firefox 33.0 or higher, Google Chrome 40.0 or higher) to be used by Super User and user authorized by Super User of the TOE as a medium of communication with the TOE's web GUI.

•.NET Framework 4.8 and IIS 7.5 or higher

• The database MSSQL 2008 R2 or higher

• Either Windows 2012R2+ or higher

For scopSOC Server;

•. NET Framework 4.8

• The database MSSQL 2008 R2 or higher

• Either Windows 2012R2+ or higher

• Elasticsearch 7.5.x or higher

For scopSOC Client;

•.NET Framework 3.5

• The database MSSQL 2008 R2 or higher

• Either Windows 2012R2+ or higher

The TOE is intended to be used in cases where there is a low level of risk. The TOE is intended to protect itself against attackers assumed to be unsophisticated with access to only standard equipment and public information about the product.

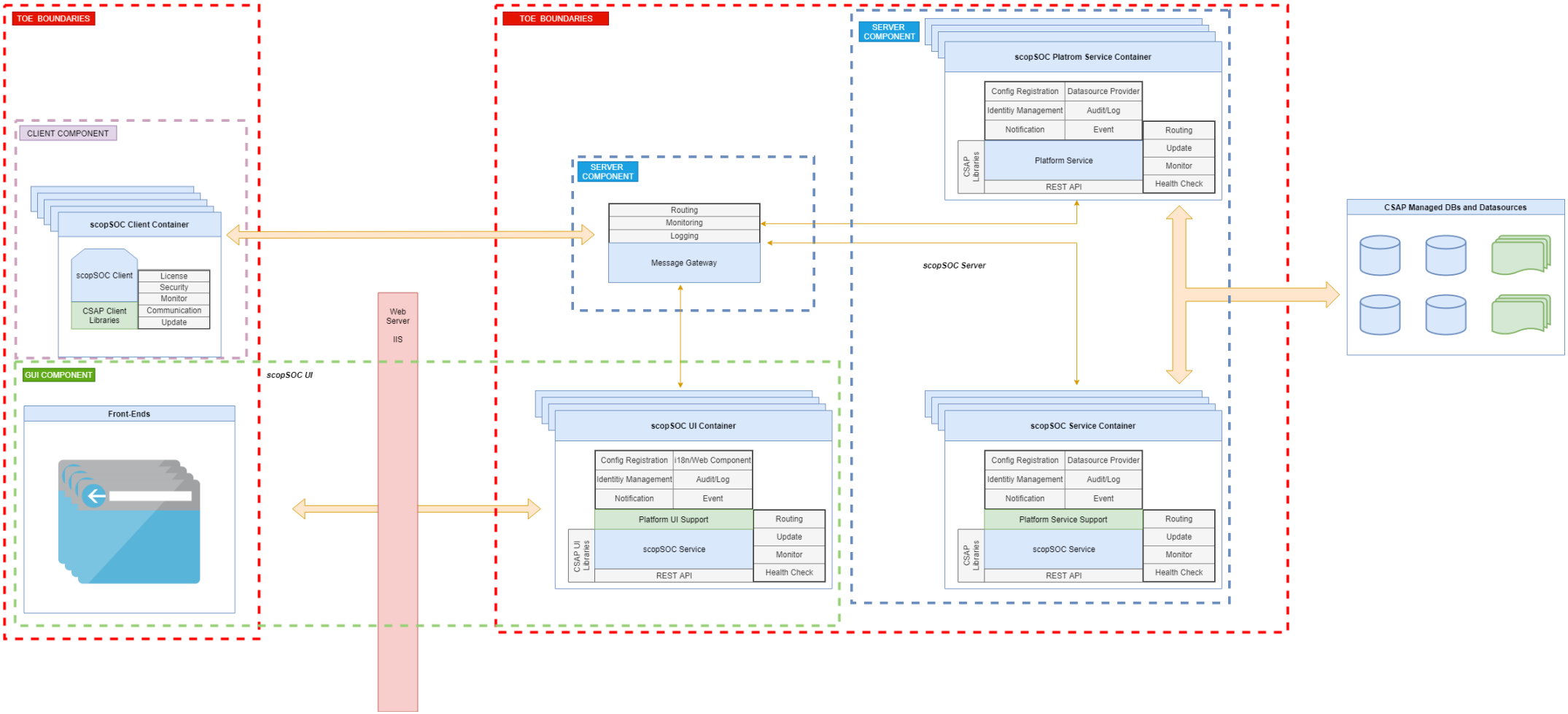
The EAL 3 Assurance Requirements are consistent with such an environment. There should also physical protection of TOE component host platforms that are critical to the security policy enforcement. No untrusted users or software are allowed on the host platforms of the scopSOC components.

1.4. TOE Description

This section provides the detailed information and description of TOE including physical and logical boundaries of the system. The TOE boundary is represented with the red dotted lines in the following figure.

Color-Code	Description
TOE BOUNDARIES	Represented with the red dotted lines
GUI COMPONENT	Represented with the green dotted lines
SERVER COMPONENT	Represented with the blue dotted lines
CLIENT COMPONENT	Represented with the purple dotted lines

TOE Boundary



1.4.1. Physical Boundary

The TOE composed of multiple software modules that run as complete IT products on required host computers. The host computers must run with an operating system platform on which the TOE executes (Please refer to the "Operating Environment).

scopSOC consists of the following components:

- **scopSOC GUI :** Graphical User Interface of scopSOC provides management and configuration functions of all scopSOC System (Configurations, Logs, Reports).
- **scopSOC Server:** This component manages the system. It is responsible for operating the system, collecting the log data and managing the events which was triggered by system.
- **scopSOC Client:** This component collects the log data and the related system information from the end points.

For a graphical representation of the scope and the points of interaction between the various components of the TOE also refer to figure in section 1.4 TOE Description.

A brief description of required settings of TOE is provided in this section. A more detailed description of the setting configurations is provided in scopSOC Guidance documents.

- Account with local administrative privileges in personal computers for log collection is required.
- SSH Credentials are required for collecting log data and executing the commands on active devices.
- Server for scopSOC Server Windows 2012R2+ or higher Supported with MS- SQL Server should be installed.
- Server for scopSOC GUI Windows 2012R2+ or higher Supported with MS- SQL Server should be installed.
- Active directory credentials are required.

TOE Refence and product version number are identical. Thus, monitoring of development activities within the scope of TOE is handled. MAY Cyber R&D Manager checks the versions of scopSOC product and each scopSOC component against the TOE version for compatibility before delivery. After this verification it is handled to MAY Cyber Service Team Product Responsible. Delivery and installation of the TOE is done by MAY Cyber Service Team Product Responsible and technical team. Right after the installation and customer's verification setup files and guidance documentation are delivered to the customer.

The physical boundary also includes the following guidance documentation:

- scopSOC Installation Guide
- scopSOC Administration Guide

1.4.2. Logical Boundary

This section outlines the boundaries of the security functions of the TOE. The Logical Boundary of the TOE includes the security functionality described here.

1.4.2.1. Security Audit

scopSOC provides for a comprehensive auditing layer, which will monitor activities and executions occurring with the system. Activities in this context are defined as operations occurring within the system that might or might not be initiated by a user. Each auditable event marks the exact time the event occurs, the account associated with that action as well as parametric details that are specific to that activity.

1.4.2.2. User Data Protection

In scopSOC system there are two SFPs for user data protection One of them is MAY Cyber Access Control SFP which is enforced by TOE on scopSOC users (Super User and user authorized by Super User) and user interface items, scopSOC authentication and authorization configurations are covered by this SFP based on user role, user ID and user permission.

scopSOC also enforces Information Flow Control SFP on Network Devices that receive information through the TOE and received information and sent query based on IP address, source IP address, destination IP address, protocol type, port number and port types or subtypes, using the methods like RPC, WMI, SNMP, SSH and Telnet Protocols. Moreover, TOE enforces the Information Flow Control SFP when importing and exporting device log data, controlled under the SFP, from outside of the TOE.

1.4.2.3. Identification and Authentication

scopSOC provides an identification and authentication layer independent from that of the Operating System it executes on. This security feature acts to protect and prevent access by unauthorized users to the system. In addition, it will also require each user to be identified and authorized before any access to security functions and data is granted. In the case of an authentication or identification failure, the TOE will disregard any request made an issue and forward redirection to the login page. scopSOC system enforces users to have a strong password policy and protects the authentication feedback by providing only dots as digits of the password to the user during authentication.

1.4.2.4. Security Management

scopSOC maintains ten security roles by default; Super User, Platform Manager, Monitoring Manager, Incident and Request Manager, SIEM Manager, Event Manager, Dashboard Manager, Asset Manager, Command Execution Manager, Reporting Manager for the management and monitoring of TOE. Super User is the user role which has all privileges on the platform. The TOE restricts the ability to query, modify and delete security attributes like event information, asset information, collected log data, incident information to Super User and user authorized by Super User. Additionally, scopSOC allows Super User and user authorized by Super User to specify alternative initial values to override the default values when an object or information is created.

1.4.2.5. Cryptographic Support

In scopSOC System, timestamp value of audit logs and collected logs in TOE is hashed using MD5 algorithm with 128-bit cryptographic key sizes that meets the criteria defined in RFC 6151 when saved into the database. User account passwords of Super User and users defined by Super User are hashed using SHA-256 algorithm with 256-bit salt sizethat meets the criteria defined in (FIPS) PUB 180-4 when saved into the database. SNMP, SMTP, SSH, WMI, SMB, SFTP, API passwords are encrypted (and decrypted) using AES algorithm with 256 bit cryptographic key sizes that meets the criteria defined in (FIPS) 140-2 and Annex A, NIST FIPS 197, RFC 2315, PKCS 7, RFC 4648 when saved into the database.

1.4.2.6. TOE Access

After the logout or a specified time interval of user inactivity, scopSOC terminates interactive session. The session timeout value is by default 1 (one) hour.

1.4.2.7. Trusted Path/Channels

A trusted path provides a means for users to perform functions through an assured direct interaction with the TSF. It is usually desired for user actions such as initial identification and/or authentication, but may also be desired at other times during a user's session. In scopSOC system, credentials are protected between the scopSOC and scopSOC GUI application. SSL (Secure Socket Layer), cryptographic protocols designed to provide communications security over a computer network, is used for communication between scopSOC Users and scopSOC GUI. It provides “HTTPS” connection.

1.4.2.8. Protection of the TSF

The TOE protects the TSF data from modification when it is transmitted between separate parts of the TOE. TOE provides 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.

1.5. Document Conventions

The notation formatting and conventions used in this Security Target are consistent with those used in Version 3.1 Revision 5 of the Common Criteria. Selected section choices are discussed here to aid the Security Target reader. The Common Criteria allows several operations to be performed on functional requirements: The allowable operations defined in part 2 of the Common Criteria are selection and assignment.

- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by *[italicized text]*.
- The assignment operation is used to assign a specific value to an unspecified parameter to a component element. Assignments are denoted by [Blue-Colored Text]
- The iteration operation is used to denote using SFR’s more than one. Iteration is denoted by SFR component title (letter). For example, FDP_ACC.1(A)

1.6. Document Terminology

The table below defines the acronyms used in this Security Target document of scopSOC.

ABBREVIATION	MEANING
CC	Common Criteria
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
IT	Information Technology
MOF	Management of Security
MSA	Management of Security Attribute
OS	Operating System
OSP	Organization Security Policy
PP	Protection Profile
RPC	Remote Procedure Call
SAR	Security Assurance Requirement
SFP	Security Functional Policy
SFR	Security Functional Requirement
SMF	Specification of Management Functions
SNMP	Simple Network Management Protocol
SOC	Security Operations Center
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
USB	User Subject Binding
WMI	Windows Management Instrumentation

2. Conformance Claims

This section provides the identification for any CC, Protection Profile (PP) and EAL Package Conformance Claims.

2.1. CC Conformance Claim

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

2.2. PP Claim

The ST does not claim Conformance to any registered Protection Profile.

2.3. Package Claim

The TOE claims conformance to the EAL 3 assurance Package defined in Part 3 of the Common Criteria Version 3.1 Revision 5 (April 2017). The TOE does not claim conformance to any Functional Package.

2.4. Conformance Rationale

This Security Target conforms to Parts 2 and 3 of the Common Criteria Standard for Information Technology

Security Evaluations, Version 3.1, Revision 5, April 2017.

There are no extended SFRs or SARs contained within this ST.

There are no Protection Profile claims for this Security Target.

3. Security Problem Definition

Assets:

- **Configuration and device data** are stored in the scopSOC Database. These data are directly stored to the database.
- **Audit data** (Elastic Search DB). It includes real-time device's log data which stores in Elastic Search. The policies required for creating audit logs.
- **System log data** related with the scopSOC Components logs which helps System Admin to understand the any error in the scopSOC System.
- **User information data** such as role, ticket data related to scopSOC GUI. This data is stored in the Database 1.

Threat Agents:

- Attacker from the internal network: A company user that is a domain member and has authorization but tries to attack.
- Attacker from the outside network: An evil user that is not a domain member but tries to be authorized.

3.1. Threats

✓ **T.DATAUPDATE:** An attacker from the internal network could try to modify ***audit data***. If the audits are not controlled regularly or the audit control could be bypassed, this action may not be noticed. Thus, the attacker succeeds without being detected.
Asset: Audit data

✓ **T.DATALOSS/MODIFY:** An attacker from the outside or internal network may attempt to remove, destroy or modify configuration, device and user information data store in the scopSOC Database Table and Database 1.
Asset: User information data, Configuration and device data

✓ **T.FUL_AUD:** An attacker from the internal network could take actions resulting in low importance audits so as to exhaust audit storage capacity. If the audit storage capacity is exhausted, future audits are lost since no further audit could be recorded.
Asset: System Log Data

✓ **T.MASQ:** An attacker may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
Asset: User information data

- ✓ **T.NOAUTH:** An attacker from internal network may attempt to bypass the security services of the TOE so as to access and use resources on the internal network. Attempts by user to gain unauthorized access to the TOE, thus limiting the administrator's ability to identify and take action against a possible security breach.
  Asset: User information data

3.2. Organizational Security Policy

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 two main OSPs defined for this Security Target.

- ✓ **OSP.SECURE TRANSFER:**

First policy is about operational environment will provide a secure channel so that credentials are protected between the scopSOC Server and scopSOC GUI application. SSL (Secure Socket Layer) which are cryptographic protocols designed to provide communications security over a computer network, is used for communication between scopSOC Users and scopSOC GUI. It provides "HTTPS" connection.

Second policy is same as first policy, SSL communication is used for communication between scopSOC Server and scopSOC Client.

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. The following specific conditions are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

- ✓ **A.ACCESS DATA - A.ACCDATA:** The TOE has access to all the IT System data it needs to perform its functions.

- ✓ **A.NO EVIL USER - A.NOEVIL:** Super User and user authorized by Super User, who manage the TOE are non-hostile use, configure and maintain the TOE and follow all guidance.

- ✓ **A.EDUCATED USER - A.EDUCUSER:** Super User and user authorized by Super User and end users are educated so as to use the scopSOC system suitably and correctly. The Administrator will install and configure the TOE according to the management guide.

- ✓ **A.PHYSICAL ACCESS AND PROTECTION - A.PYHPROT:** The TOE resides in a physically controlled access facility that prevents unauthorized physical Access. Therefore, the physical hardware and software in which the TOE is deployed will be protected from unauthorized physical modification.

- ✓ **A.SECURE ENVIRONMENT - A.SECENV:** The Operating Systems, Database, Application and Web Server, on which the TOE is running are, fixed against all security bugs and protected against all threats.

4. Security Objectives

4.1. Security Objectives for the TOE

The IT security objectives for the TOE are addressed below:

- ✓ **O.ADMINISTRATION - O.ADMIN:** The TOE will include a set of functions that allow efficient management of TSF and TSF data, ensuring that TOE users with appropriate privileges exist.

- ✓ **O.AUDIT RECORD - O.AUDREC:** The TOE will provide a means to record a readable audit trail of security related events, with accurate dates and times and means to the search the audit trail based on relevant attributes.

- ✓ **O.ACCOUNTABILITY - O.ACCOUN:** The TOE will provide user accountability for information flows through the TSF and TSF data.

- ✓ **O.CORRECT DATA - O.CORRDATA:** The TOE will provide data security each data hashed line by line with real server time. This operation is provided by scopSOC Server component.

- ✓ **O.DATA STORAGE - O.DATASTOR:** The TOE will provide audit data storage including user account passwords and audit timestamp value in a secure manner. When it will be out of memory, user will be warned, if not or user ignore the warning, system will continue to store the audit data to a designated storage area.

- ✓ **O.IDENTIFY AND AUTHENTICATE - O.IDAUTH:** The TOE will uniquely identify and authenticate the claimed identity of all users before granting a user access to TOE functions. Besides, the TOE shall define the rules for user authentication that forces users to have strong password policy.

- ✓ **O.RESOURCE ACCESS - O.RESACC:** The TOE will control access to resources based on the identity of users. The TSF must allow Super User to specify which resources may be accessed by which users.

- ✓ **O.SECURITY FUNCTIONS - O.SECFUN:** The TOE will provide functionality that enables Super User and user authorized by Super User to use the TOE security functions and will ensure that only Super User and user authorized by Super User are able to access such functionality.

4.2. Security Objectives for the Operational Environment

The security objectives for the Operational Environment are addressed below:

- ✓ **OE.ADMINISTRATOR TRAINING - OE.ADMTRA:** Super User and user authorized by Super User will be trained to appropriately install, configure and maintain the TOE within its evaluated configuration according to the installation and guidance documents for the TOE.

- ✓ **OE.COMMUNICATION - OE.COMM:** communication will be protect between the TOE and system outside the TOE boundary from disclosure.

- ✓ **OE.ENVIRONMENT SECURITY - OE.ENVSEC:** The company has responsibility for the TOE will ensure that those parts of TOE should be running in a secure and protected environment.

- ✓ **OE.GUIDAN - OE.GUIDAN:** The TOE will be delivered, installed, administrated and operated in a manner that maintains security and correctly.

- ✓ **OE.TIMESTAMP - OE.TIMESTAMP:** For the sign operation, time of the server in the company will be accepted for trusted time.

- ✓ **OE.ELASTIC STRUCTURE - OE.ELASTRUCTURE:** Elastic Search Structure do not provide data modification (delete, update) in Log data. Log data are signed and hashed for preventing the data modification. Log data and hashed log data will be compared. According to comparison user understand that log data were modified or not. Hash structure provide security of data validation.

4.3. Security Objectives Rationale

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions, threats and Organizational Security Policies.

Assumption & Threats / Objectives	T.DATAUPDATE	T.DATALOSS/MODIFY	T.FUL_AUD	T.MASQ	T.NOAUTH	A.ACCDATA	A.EDUCUSER	A.NOEVIL	A.PYHPROT	A.SECENV	OSP.SECURE TRANSFER
O.AUDREC				✓	✓						
O.CORRDATA	✓										
O.DATASTOR			✓								
O.IDAUTH				✓	✓						
O.RESACC		✓		✓	✓						
O.SECFUN					✓						
OE.TIMESTAMP	✓										
OE.ADMTRA							✓				
OE.COMM									✓		✓
OE.ENVSEC		✓							✓	✓	
OE.GUIDAN						✓		✓			
OE.ELASTRUCTURE	✓					✓					

4.3.1. Rationale for Security Threats to the TOE

THREAT	RATIONALE
T.DATAUPDATE	This threat is completely countered by • **O.CORRDATA** which ensures user access correct log data information. • **OE.TIMESTAMP** which ensures the IT Environment will provide reliable timestamps for the TOE in the company server time. • **OE.ELASTRUCTURE** which ensures the modification of audit data is not possible because of **elastic search data structure security.**
T.DATALOSS/MODIFY	This threat is completely countered by • **O.RESACC** which must control access to resources based on the identity of users. The TSF must allow Super User and user authorized by Super User to specify which resources may be accessed by which users. • **OE.ENVSEC** which provides the security zone at the TOE environment to reach audit data.
T.FUL_AUD	This threat is completely countered by • **O.DATASTOR** which provides audit data storage including user account passwords and audit timestamp value in a secure manner. When it will be out of memory, user will be warned, if not or user ignore the warning, system will continue to store the audit data to a designated storage area.
T.MASQ	This threat is completely countered by • **O.AUDREC** which ensures the TOE provide a means to record a readable audit trail of security related events, with accurate dates and times and means to the search the audit trail based on relevant attributes. • **O.IDAUTH** which ensures the unique identification and authenticates the claimed identity of all users before granting a user access to TOE functions. • **O.RESACC** which must control access to resources based on the identity of users. The TSF must allow Super User and user authorized by Super User to specify which resources may be accessed by which users.

T.NOAUTH	This threat is completely countered by • **O.IDAUTH** which ensures the unique identification and authenticates the claimed identity of all users before granting a user access to TOE functions. • **O.AUDREC** which ensures the TOE provide a means to record a readable audit trail of security related events, with accurate dates and times and means to the search the audit trail based on relevant attributes. • **O.RESACC** which must control access to resources based on the identity of users. The TSF must allow Super User and user authorized by Super User to specify which resources may be accessed by which users. • **O.SECFUN** which ensures the TOE provides functionality that enables an administrator to use the TOE Security Functions and also ensures that only administrator are able to access such functionality. Admin also examines the log and takes the necessary actions.

4.3.2. Rationale for Assumptions of the TOE

ASSUMPTION	RATIONALE
A.ACCDATA	This assumption is completely countered by • **OE.GUIDAN** provides The TOE to be delivered, installed, administrated and operated in a manner that maintains security and correctness. • **OE.TIMESTAMP** ensures that the IT environment provides reliable time stamps. Time stamp value, which shows the accurate dates and times of audit logs.
A.NOEVIL	This assumption is completely countered by • **OE.ADMTRA** which ensures the identification and authentication for Super User and user authorized by Super User prior to allowing access to TOE administrative functions and data.
A.EDUCUSER	This assumption is completely countered by • **OE.GUIDAN** provides The TOE to be delivered, installed, administrated and operated in a manner that maintains security and correctness. • **OE.ADMTRA** which ensures the identification and authentication for provides Super User and user authorized by Super User prior to allowing access to TOE administrative functions and data.

A.PYHPROT	This assumption is completely countered by • **OE.ENVSEC** provides to ensure that those parts of TOE should be running in a secure and protected environment. • **OE.COMM** which protects the communication between the TOE and system outside the TOE boundary from disclosure.
A.SECENV	This assumption is completely countered by • **OE.ENVSEC** provides to ensure that those parts of TOE should be running in a secure and protected environment. • **OE.COMM** which protects the communication between the TOE and system outside the TOE boundary from disclosure.

4.3.3. Rationale for Organizational Security Policy of the TOE

OBJECTIVES	RATIONALE
OSP.SECURE TRANSFER	This organizational security policy is countered by; • **OE.COMM** which protects the communication between the TOE and system outside the TOE boundary from disclosure.

5. Extended Components Definition

No extended components are defined.

6. Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) met by the TOE.

6.1. Security Functional Requirements

This section specifies the SFRs for the TOE and also organizes the SFRs by CC Class.

CLASS	CLASS FAMILY	DESCRIPTION
Security Audit	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.2	Restricted Audit Review
	FAU_STG.1	Protected Audit Trail Storage
	FAU_STG.4	Prevention of Audit Data Loss
User Data Protection	FDP_ACC.1	Subset Access Control
	FDP_ACF.1	Security Attribute Based Access Control
	FDP_ETC.1	Export of User Data Without Security Attributes
	FDP_IFC.1	Subset Information Flow Control
	FDP_IFF.1	Simple Security Attributes
	FDP_ITC.1	Import of User Data Without Security Attributes
Identification and Authentication	FIA_ATD.1	User Attribute Definition
	FIA_SOS.1	Verification of Secrets
	FIA_UAU.2	User Authentication Before Any Action
	FIA_UAU.7	Protected Authentication Feedback
	FIA_UID.2	User Identification Before Any Action
	FIA_USB.1	User-Subject Binding
Security Management	FMT_MOF.1	Management of Security Functions Behaviour
	FMT_MSA.1(A)	Management of Security Attributes - Administrative Access Control SFP
	FMT_MSA.1(B)	Management of Security Attributes - Information Flow Control SFP
	FMT_MSA.3(A)	Static Attribute Initialisation - Administrative Access Control SFP
	FMT_MSA.3(B)	Static Attribute Initialisation - Information Flow Control SFP
	FMT_MTD.1	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles
Cryptographic Support	FCS_COP.1(A)	Password Hashing
	FCS_COP.1(B)	Log Hashing
	FCS_COP.1(C)	Password Encryption & Decryption
TOE Access	FTA_SSL.3	TSF-Initiated Termination
	FTA_SSL.4	User-Initiated Termination
Trusted Path/Channels	FTP_TRP.1	Trusted Path
Protection of the TSF	FPT_ITT.1	Basic Internal TSF Data Transfer Protection

6.1.1. Class Security Audit (FAU)

6.1.1.1. FAU_GEN.1 – Audit Data Generation

Description: Audit Data Generation defines the level of auditable events and specifies the list of data that shall be recorded in each record.

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable Time Stamp

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)** [System logs, User access, database interaction events and software exceptions]

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

- **a)** Date and time of 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 ST, [event message according to event type].

6.1.1.2. FAU_GEN.2 – User Identity Association

Description: User identity association, the TSF shall associate auditable events to individual user identities.

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.

6.1.1.3. FAU_SAA.1 – Potential Violation Analysis

Description: Potential violation analysis, basic threshold detection on the basis of a fixed rule set is required.

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 [user and event log data according to defined rule] known to indicate a potential security violation.

b) [rules: when

1. Elastic HealthCheck Connection Down
2. Disk Space on Elasticsearch Node become critical
3. Elasticsearch File System Low at Node
4. Elastic Cluster Status is RED]

6.1.1.4. FAU_SAR.1 – Audit Review

Description: Audit review, provides the capability to read information from the audit records.

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit Data Generation

FAU_SAR.1.1 The TSF shall provide [Super User and user authorized by Super User] with the capability to read [all recorded audit information] from the audit records.

6.1.1.5. FAU_SAR.2 – Restricted Audit Review

Description: Restricted audit review, requires that there are no other users except those that have been identified in FAU_SAR.1 Audit review that can read the information.

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit Review

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

6.1.1.6. FAU_STG.1 – Protected Audit Trail Storage

Description: Protected audit trail requirements are placed on the audit trail. It will be protected from unauthorised deletion and/or modification.

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to [*prevent*] unauthorised modifications to the stored audit records in the audit trail.

6.1.1.7. FAU_STG.4 – Prevention of Audit Data Loss

Description: Prevention of audit data loss, specifies actions in case the audit trail is full.

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss.

Dependencies: FAU_STG.1 Protected Audit trail Storage

FAU_STG.4.1 The TSF shall [*ignore audit records*] and [warns Super User and user authorized by Super User about storage capacity and delete old logs manually] if the audit trail is full.

Application Note 5: *Audit log storage thresold value is identified depending on the storage capacity of the environment on which the TOE is installed. Warning is triggered when the storage is full. There is not an automatic mechanism for deleting old logs. Deleting operation of the old logs is executed manually by the Super User and user authorized by Super User depending on the organizational log policy of the institution where the TOE is installed. When the audit storage is full TOE neither ceases producing logs nor stops the action that causes producing logs. Instead of this TOE starts to record the logs to a designated storage area. Perchance this designated storage area is full then the system shuts itself down and stops the action that causes producing logs.*

6.1.2. Class User Data Protection (FDP)

6.1.2.1. FDP_ACC.1 – Subset Access Control

Description: Subset access control, requires that each identified access control SFP be in place for a subset of the possible operations on a subset of the objects in the TOE.

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute-based access control

FDP_ACC.1.1 The TSF shall enforce the [MAY Cyber Access Control SFP] on

[Subjects: Super User and user authorized by Super User attempting to establish an interactive session with the TOE,

Objects: user interface items, scopSOC authentication and authorization configurations,

Operations: all interactions between the subjects and objects identified above].

6.1.2.2 FDP_ACF.1 – Security Attribute Based Access Control

Description: Security attribute-based access control Security attribute-based access control allows the TSF to enforce access based upon security attributes and named groups of attributes. Furthermore, the TSF may have the ability to explicitly authorize or deny access to an object based upon security attributes.

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset Access Control, FMT_MSA.3 Static Attribute Initialization

FDP_ACF.1.1 The TSF shall enforce the [MAY Cyber Access Control SFP] to objects based on the following:
[Subject: Super User and user authorized by Super User attempting to establish and interactive session with the TOE,

Subject attribute:

1. User Role,
2. User ID,
3. User Permission.

Objects: user interface items, scopSOC authentication and authorization configurations,
Object attributes:

1. Permissions assigned objects

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

[1. If the subject request access to an object and subject has permission the object, then access is granted,

2. If none of the above rules apply, access is denied].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [no additional rules].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [no additional rules].

6.1.2.3 FDP_IFC.1 – Subset Information Flow Control

Description: Subset information flow control, requires that each identified information flow control SFPs be in place for a subset of the possible operations on a subset of information flows in the TOE.

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple Security Attributes

FDP_IFC.1.1 The TSF shall enforce the [information flow control SFP] on

[a) Subjects: Network Devices that receive information through the TOE,

b) Information: receive information and send query

c) Operations: allow or deny RPC, WMI, SNMP, SSH and Telnet Protocols].

6.1.2.4 FDP_IFF.1 – Simple Security Attributes

Description: Simple security attributes, requires security attributes on information, and on subjects that cause that information to flow and on subjects that act as recipients of that information. It specifies the rules that must be enforced by the function, and describes how security attributes are derived by the function.

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset Information Flow Control

FMT_MSA.3 Static Attribute Initialisation

FDP_IFF.1.1 The TSF shall enforce the [information flow control SFP] based on the following types of subject and information security attributes:

[Subject attributes:

1) IP Address

Information (traffic) attributes:

1) Source IP address,

2) Destination IP address,

3) Protocol type,

4) Port number, and

5) Port types or subtypes].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

[scopSOC Server connection establishment is allowed, if

- IP address = acceptable
- Protocol type = RPC, WMI, SNMP, SSH and Telnet Protocols].

FDP_IFF.1.3 The TSF shall enforce the [none].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [none].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [none].

6.1.2.5 FDP_ITC.1 – Import of User Data without Security Attributes

Description: Import of user data without security attributes, requires that the security attributes correctly represent the user data and are supplied separately from the object.

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset Access Control or FDP_IFC.1 Subset Information Flow Control]

FMT_MSA.3 Static Attribute Initialisation

FDP_ITC.1.1 The TSF shall enforce the [information flow control SFP] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [no additional importation control rules].

***Application Note 1*:** *User data is device log data*

6.1.2.6 FDP_ETC.1 – Export of User Data without Security Attributes

Description: Export of user data without security attributes, requires that the TSF enforce the appropriate SFPs when exporting user data outside the TSF. User data that is exported by this function is exported without its associated security attributes.

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset Access Control or FDP_IFC.1 Subset Information Flow Control]

FDP_ETC.1.1 The TSF shall enforce the [information flow control SFP and MAY Cyber Access Control SFP] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.1.2 The TSF shall export the user data without the user data's associated security attributes.

Application Note 2: *User data is device log data*

6.1.3. Class Identification and Authentication (FIA)

6.1.3.1. FIA_ATD.1 – User Attribute Definition

Description: User attribute definition, allows user security attributes for each user to be maintained individually.

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: [Authorization status as determined by the TOE, User role, User ID, IP Address].

6.1.3.2. FIA_UAU.2 – User Authentication Before any Action

Description: User authentication before any action, requires that users are authenticated before any other action will be allowed by the TSF.

Hierarchical to: FIA_UAU.1 Timing of authentication.

Dependencies: FIA_UID.1 Timing of identification.

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

6.1.3.3. FIA_UAU.7 - Protected authentication feedback

Description: Protected authentication feedback, requires that only limited feedback information is provided to the user during the authentication.

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication.

FIA_UAU.7.1 The TSF shall provide only [dots as digits of the password] to the user while the authentication is in progress.

6.1.3.4. FIA_UID.2 – User Identification Before any Action

Description: User identification before any action, requires that users identify themselves before any other action will be allowed by the TSF.

Hierarchical to: FIA_UID.1 Timing of authentication.

Dependencies: No dependencies.

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

6.1.3.5. FIA_USB.1 – User Subject Binding

Description: User-subject binding, requires the specification of any rules governing the association between user attributes and the subject attributes into which they are mapped.

Hierarchical to: No other components.

Dependencies: FIA_ATD.1 User attributes definition.

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [Authorization status as determined by the TOE, User role, User ID, IP Address].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [None].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [None].

6.1.3.6. FIA_SOS.1 – Verification of Secrets

Description: Secrets can be generated by the user. This component ensures that those user generated secrets can be verified to meet a certain quality metric. This component allows the TSF to generate secrets for specific functions such as authentication by means of user authentication passwords.

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet

[a) Should be at least 8 characters long,

b) Should contain at least three of following:

- uppercase letter,
- lowercase letter,
- number,
- symbol].

6.1.4. Class Security Management (FMT)

6.1.4.1. FMT_MOF.1 – Management of Security Functions Behaviour

Description: Management of security functions behavior allows the authorized users (roles) to manage the behavior of functions in the TSF that use rules or have specified conditions that may be manageable.

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions.

FMT_MOF.1.1 The TSF shall restrict the ability to [*disable and enable*] the functions [password policy flag] to [Super User and user authorized by Super User].

Application Note 3: *The password policy is defined under the FIA_SOS.1 SFR.*

6.1.4.2. FMT_MSA.1(A) – Management of Security Attributes

Description: Management of security attributes allows authorized users (roles) to manage the specified security attributes.

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions.

FMT_MSA.1.1(A) The TSF shall enforce the [MAY Cyber Access Control SFP] to restrict the ability to *[query, modify, delete]* the security attributes [Event Information, Asset Information, Collected Log Data, Incident Information] to [Super User and user authorized by Super User].

6.1.4.3. FMT_MSA.1(B) – Management of Security Attributes

Description: Management of security attributes allows authorized users (roles) to manage the specified security attributes.

Hierarchical to: No other components.

Dependencies: **[**FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions.

FMT_MSA.1.1(B) The TSF shall enforce the [Information flow Control SFP] to restrict the ability to *[change_default]* the security attributes [query and responses] to [Super User and user authorized by Super User].

6.1.4.4. FMT_MSA.3(A) – Static Attribute Initialization

Description: Static attribute initialization ensures that the default values of security attributes are appropriately either permissive or restrictive in nature.

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of Security Attributes, FMT_SMR.1 Security roles

FMT_MSA.3.1(A) The TSF shall enforce the [MAY Cyber Access Control SFP] to provide *[permissive]* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(A) The TSF shall allow the [Super User and user authorized by Super User] to specify alternative initial values to override the default values when an object or information is created.

6.1.4.5. FMT_MSA.3(B) – Static Attribute Initialization

Description: Static attribute initialization ensures that the default values of security attributes are appropriately either permissive or restrictive in nature.

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of Security Attributes, FMT_SMR.1 Security roles

FMT_MSA.3.1(B) The TSF shall enforce the [Information flow control SFP] to provide *[restrictive]* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(B) The TSF shall allow the [Super User and user authorized by Super User] to specify alternative initial values to override the default values when an object or information is created.

6.1.4.6. FMT_MTD.1 – Management of TSF data

Description: Management of TSF data allows authorised users to manage TSF data.

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specifications of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to [*modify*] the [user information] to [Super User and user authorized by Super User].

6.1.4.7. FMT_SMF.1 – Specification of Management Functions

Description: Specification of Management Functions requires that the TSF provide specific 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: [Create, Delete, Modify and View security attribute values, enable and disable External IT entities from communicating to the TOE, review of audit trail].

6.1.4.8. FMT_SMR.1 – Security Roles

Description: Security roles specify the roles with respect to security that the TSF recognizes.

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [Super User, Platform Manager, Monitoring Manager, Incident and Request Manager, SIEM Manager, Event Manager, Dashboard Manager, Asset Manager, Command Execution Manager, Reporting Manager].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.1.5. Class Cryptographic Support (FCS)

6.1.5.1. FCS_COP.1(A) – Cryptographic Operation – Hash Operation/Password Protection

Description: Cryptographic operation requires a cryptographic operation to be performed in accordance with a specified algorithm and with a cryptographic key of specified sizes. The specified algorithm and cryptographic key sizes can be based on an assigned standard.

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1(A) The TSF shall perform [user accounts' password hashing of Super User and users defined by Super User] in accordance with a specified cryptographic algorithm [SHA_256] and cryptographic key sizes [256 bit] that meet the following: [(FIPS) PUB 180-4].

6.1.5.2. FCS_COP.1(B) – Cryptographic Operation – Hash Operation/Log Protection

Description: Cryptographic operation requires a cryptographic operation to be performed in accordance with a specified algorithm and with a cryptographic key of specified sizes. The specified algorithm and cryptographic key sizes can be based on an assigned standard.

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1(B) The TSF shall perform [timestamp value of audit log and collected log hashing] in accordance with a specified cryptographic algorithm [MD5] and cryptographic key sizes [128 bit] that meet the following: [RFC 6151].

Application Note 4: *Collected logs are the data gathered from various devices using the collector.*

6.1.5.3. FCS_COP.1(C) - Cryptographic Operation – Encryption & Decryption Operation/Password Protection

Description: Cryptographic operation requires a cryptographic operation to be performed in accordance with a specified algorithm and with a cryptographic key of specified sizes. The specified algorithm and cryptographic key sizes can be based on an assigned standard.

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1(C) The TSF shall perform [SNMP, SMTP, SSH, WMI, SMB, SFTP, API password encryption/decryption] in accordance with a specified cryptographic algorithm [AES] and cryptographic key sizes [256 bit] that meet the following: [FIPS 140-2 and Annex A, NIST FIPS 197, RFC 2315, PKCS 7, RFC 4648].

6.1.6. Class TOE Access (FTA)

6.1.6.1. FTA_SSL.3 – TSF Initiated Termination

Description: TSF-initiated termination, provides requirements for the TSF to terminate the session after a specified period of user inactivity.

Hierarchical to: No other components.

Dependencies: No dependencies

FTA_SSL.3.1 The TSF shall terminate an interactive session after [a specified time interval of user inactivity. The default cookie session timeout value is 1 hour].

6.1.6.2. FTA_SSL.4 – User Initiated Termination

Description: User-initiated termination, provides capabilities for the user to terminate the user's own interactive sessions.

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.

6.1.7. Class Trusted Path/Channels (FTP)

6.1.7.1. FTP_TRP.1 – Trusted Path

Description: Trusted path, requires that a trusted path between the TSF and a user be provided for a set of events. The user and/or the TSF may have the ability to initiate the 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*].

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*].

6.1.8. Class Protection of the TSF (FPT)

6.1.8.1. FPT_ITT.1 – Basic Internal TSF Data Transfer Protection

Description: Basic internal TSF data transfer protection, requires that TSF data be protected when transmitted between separate parts of the TOE.

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_ITT.1.1 The TSF shall protect TSF data from [*modification*] when it is transmitted between separate parts of the TOE.

6.2. Security Functional Requirements Dependencies

SFR	Dependency	Applied
FAU_GEN.1	FPT_STM.1	*FAU_GEN.1 Audit data generation requires that FPT_STM.1 Reliable Time Stamp is included as a component. However, the TOE is not capable of providing this functionality. This functionality will be provided by a TOE environment. Hence, FPT_STM.1 Reliable Time Stamp is not included.*
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	*FAU_GEN.1 Audit data generation is included. FIA_UID.2 User identification before any action, which is hierarchical to FIA_UID.1 Timing of identification is included.*
FAU_SAA.1	FAU_GEN.1	*FAU_GEN.1 Audit data generation is included.*
FAU_SAR.1	FAU_GEN.1	*FAU_GEN.1 Audit data generation is included.*
FAU_SAR.2	FAU_SAR.1	*FAU_SAR.1 Audit review is included.*
FAU_STG.1	FAU_GEN.1	*FAU_GEN.1 Audit data generation is included.*
FAU_STG.4	FAU_STG.1	*FAU_STG.1 Protected audit trail storage is included.*
FDP_ACC.1	FDP_ACF.1	*FDP_ACF.1 Security attribute-based access control is included.*
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3(A)	*FDP_ACC.1 Subset access control and FMT_MSA.3 Static attribute initialization are included.*
FDP_ETC.1	FDP_ACC.1 or FDP_IFC.1	*FDP_ACC.1 Subset access control is included.*
FDP_IFC.1	FDP_IFF.1	*FDP_IFF.1 Simple security attributes is included.*
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3(B)	*FDP_IFC.1 Subset information flow control and FMT_MSA.3 Static attribute initialization are included.*
FDP_ITC.1	FDP_ACC.1 or FDP_IFC.1 FMT_MSA.3(B)	*FDP_ACC.1 Subset access control, FDP_IFC.1 Subset information flow control and FMT_MSA.3 Static attribute initialization are included.*

FIA_ATD.1	No Dependencies	-
FIA_SOS.1	No Dependencies	-
FIA_UAU.2	FIA_UID.1	*FIA_UID.2 User identification before any action, which is hierarchical to FIA_UID.1 Timing of identification is included.*
FIA_UAU.7	FIA_UAU.1	*FIA_UAU.2 User authentication before any action, which is hierarchical to FIA_UAU.1 Timing of authentication is included.*
FIA_UID.2	No Dependencies	-
FIA_USB.1	FIA_ATD.1	*FIA_ATD.1 User attribute definition is included.*
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	*FMT_SMR.1 Security roles* *and FMT_SMF.1 Specification of Management Functions are included.*
FMT_MSA.1(A)	FDP_ACC.1 or FDP_IFC.1 and FMT_SMR.1 FMT_SMF.1	*FDP_ACC.1 Subset access control, , FMT_SMR.1 Security roles and FMT_SMF.1 Specification of Management Functions are included.*
FMT_MSA.1(B)	FDP_ACC.1 or FDP_IFC.1 and FMT_SMR.1 FMT_SMF.1	*FDP_IFC.1 Subset information flow control, FMT_SMR.1 Security roles and FMT_SMF.1 Specification of Management Functions are included.*
FMT_MSA.3(A)	FMT_MSA.1 FMT_SMR.1	*FMT_MSA.1(A) Management of security attributes and FMT_SMR.1 Security roles are included.*
FMT_MSA.3(B)	FMT_MSA.1 FMT_SMR.1	*FMT_MSA.1(B) Management of security attributes and FMT_SMR.1 Security roles are included.*
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	*FMT_SMR.1 Security roles* *And FMT_SMF.1 Specification of Management Functions are included.*

FMT_SMF.1	No Dependencies	-
FMT_SMR.1	FIA_UID.1	*FIA_UID.2 User identification before any action, which is hierarchical to FIA_UID.1 Timing of identification is included.*
FCS_COP.1(A)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 and FCS_CKM.4	*FDP_ITC.1 Import of user data without security attributes is included.* *FCS_CKM.1Cryptographic key generation is not included because hash algorithms don't require cryptographic keys.* *FCS_CKM.4 Cryptographic key destruction is not included because passwords are being encapsulated by the hash algorithm thus, keys are not being destructed.*
FCS_COP.1(B)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 and FCS_CKM.4	*FDP_ITC.1 Import of user data without security attributes is included.* *FCS_CKM.1Cryptographic key generation is not included because hash algorithms don't require cryptographic keys.* *FCS_CKM.4 Cryptographic key destruction is not included because passwords are being encapsulated by the hash algorithm thus, keys are not being destructed.*
FCS_COP.1(C)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 and FCS_CKM.4	*FDP_ITC.1 Import of user data without security attributes is included.* *FCS_CKM.1 Cryptographic key generation and FCS_CKM.4 Cryptographic key destruction are not included since cryptographic keys are kept embedded in code, key generation, key import or key destruction is not required.*
FTA_SSL.3	No Dependencies	-
FTA_SSL.4	No Dependencies	-
FTP_TRP.1	No Dependencies	-
FPT_ITT.1	No Dependencies	-

6.3. Security Assurance Requirements

EAL3 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and interface specification, guidance documentation, and an architectural description of the design of the TOE, to understand the security behavior.

The assurance security Requirements for the Security Target are taken from Part 3 of the CC v.3.1 Revision 5 (April 2017). These assurance requirements compose an Evaluation Assurance Level 3 (EAL 3). The assurance components are summarized in the following table:

ASSURANCE CLASS	ASSURANCE COMPONENTS	DESCRIPTION
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.3	Functional specification with complete summary
	ADV_TDS.2	Architectural Design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life-cycle support	ALC_CMC.3	Authorization Control
	ALC_CMS.3	Implementation representation CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
ASE: Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended component 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 specifications
ATE: Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: Basic Design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
AVA: Vulnerability assessment	AVA_VAN.2	Vulnerability analysis

6.4. Security Functional Requirements Rationale

The following table provides the correspondence mapping between security objectives for the TOE and the requirements that satisfy them.

SFR \ Objective	O.ACCOUN	O.ADMIN	O.AUDREC	O.DATASTOR	O.CORRDATA	O.IDAUTH	O.RESACC	O.SECFUN
FAU_GEN.1	✓		✓					
FAU_GEN.2	✓		✓					
FAU_SAA.1				✓				
FAU_SAR.1	✓		✓					
FAU_SAR.2	✓		✓					
FAU_STG.1	✓		✓	✓			✓	
FAU_STG.4			✓	✓			✓	
FDP_ACC.1	✓	✓					✓	
FDP_ACF.1	✓	✓					✓	
FDP_IFC.1	✓	✓					✓	
FDP_IFF.1	✓	✓					✓	
FDP_ITC.1				✓	✓		✓	✓
FDP_ETC.1					✓		✓	
FIA_ATD.1		✓				✓		
FIA_UAU.2	✓					✓	✓	
FIA_UAU.7	✓					✓		
FIA_UID.2	✓					✓	✓	
FIA_USB.1						✓		
FIA_SOS.1						✓		
FMT_MOF.1	✓	✓					✓	✓
FMT_MSA.1(A)	✓	✓					✓	✓
FMT_MSA.1(B)	✓	✓					✓	✓
FMT_MSA.3(A)	✓	✓					✓	✓
FMT_MSA.3(B)	✓	✓					✓	✓
FMT_MTD.1							✓	
FMT_SMF.1	✓	✓						✓
FMT_SMR.1	✓	✓					✓	✓
FCS_COP.1(A)				✓				
FCS_COP.1(B)				✓				
FCS_COP.1(C)				✓				
FTA_SSL.3								✓
FTA_SSL.4								✓
FTP_TRP.1	✓							
FPT_ITT.1					✓			

SFR	RATIONALE
FAU_GEN.1	This component outlines what data must be included in audit records and what events must be audited. This component traces back to and aids in meeting the following objectives: **O.ACCOUN** and **O.AUDREC**.
FAU_GEN.2	This component provides association of each auditable event with the identity of the user that caused the event. This component traces back to and aids in meeting the following objectives: **O.ACCOUN** and **O.AUDREC**.
FAU_SAA.1	This requirement defines requirements for automated means that analyse system activity and audit data looking for possible or real security violations. This analysis may work in support of intrusion detection, or automatic response to a potential security violation. It meets the following objectives: **O.DATASTOR**.
FAU_SAR.1	This requirement provides the ability to review logs. This component traces back to and aids in meeting the following objectives: **O.ACCOUN** and **O.AUDREC**.
FAU_SAR.2	This requirement provides the restricted audit review, requires that there are no other users except those that have been identified in FAU_SAR.1 Audit review that can read the information and aids in meeting the following objectives**:** **O.ACCOUN** and **O.AUDREC**.
FAU_STG.1	This requirement is placed on the audit trail. It will be protected from unauthorised deletion and/or modification. Unauthorised modifications to the stored audit records in the audit trail are preventented. This component traces back to and aids in meeting the following objectives: **O.ACCOUN**, **O.AUDREC**, **O.DATASTOR** and **O.RESACC**.
FAU_STG.4	This requirement specifies actions in case the audit trail is full and prevents the audit data loss. When the audit storage is out of memory the user is warned about storage capacity if not or user ignore the warning, system will continue to store the audit data to a designated storage area. This component traces back to and aids in meeting the following objectives: **O.AUDREC**, **O.DATASTOR** and **O.RESACC**.
FDP_ACC.1	This requirement defines subjects, objects and operations controlled by the MAY Cyber Access Control SFP. This component specifies that the policy cover some well-defined set of operations on some subset of the objects. It places no constraints on any operations outside the set - including operations on objects for which other operations are controlled. This component traces back to and aids in meeting the following objectives: **O.ACCOUN**, **O.ADMIN** and **O.RESACC**.

FDP_ACF.1	The requirement meets the objective by defining the subject and object attributes, and the rules by which subjects can operate on objects under the MAY Cyber Access Control SFP. This component traces back to and aids in meeting the following objectives: **O.RESACC**. This component also identifies control access to resources based on the subject attributes of users. The TSF must Super User to specify which resources may be accessed by which users. This component traces back to and aids in meeting the following objectives: **O.ADMIN** and **O.ACCOUN**.
FDP_IFC.1	This component identifies the information flow control SFPs and defines the scope of control for each named information flow control SFP. Each identified information flow control SFPs be in place for a subset of the possible operations on a subset of information flows in the TOE. This component traces back to and aids in meeting the following objectives: **O.ACCOUN**, **O.ADMIN** and **O.RESACC**.
FDP_IFF.1	The requirement meets the objective by defining the subject attributes on information and on subjects that cause that information to flow and on subjects that act as recipients of that information and the rules under the information flow control SFP. This component traces back to and aids in meeting the following objectives: **O.ACCOUN**, **O.ADMIN** and **O.RESACC**.
FDP_ITC.1	This requirement defines the mechanisms for TSF-mediated importing of user data (without security attribute) into the TOE such that it has appropriate security attributes and is appropriately protected. This component traces back to and aids in meeting the following objectives: **O.DATASTOR**, **O.CORRDATA**, **O.RESACC** and **O.SECFUN**.
FDP_ETC.1	This requirement defines functions for TSF-mediated exporting of user data (without security attribute) from the TOE such that its security attributes and protection either can be explicitly preserved or can be ignored once it has been exported. This component traces back to and aids in meeting the following objectives: **O.CORRDATA** and **O.RESACC**.
FIA_ATD.1	This component exists to provide users with attributes to distinguish one user from another for accountability purposes and to associate the role chosen in FMT_SMR.1 with a user. This component traces back to and aids in meeting the following objectives: **O.ADMIN** and **O.IDAUTH**.
FIA_UAU.2	This component requires successful authentication of a role before having access to the TSF and such aids in meeting **O.IDAUTH**. This component also identifies controlled access to resources based on the identity of users. This component traces back to and aids in meeting the following objectives: **O.RESACC** and **O.ACCOUN**.
FIA_UAU.7	TOE requires protection of authentication for the cases when the users trying to authenticate to access their private keys. This component traces back to and aids in meeting the following objectives: **O.ACCOUN** and **O.IDAUTH**.

FIA_UID.2	This component requires successful identification of a role before having access to the TSF and such aids in meeting **O.IDAUTH** and **O.ACCOUN**. This component also identifies controlled access to resources based on the identity of users. This component traces back to and aids in meeting the following objectives: **O.RESACC**.
FIA_USB.1	This component requires the specification of any rules governing the association between user attributes and subject attributes into which they are mapped. This component traces back to and aids in meeting the following objective: **O.IDAUTH**.
FIA_SOS.1	This component can be used to ensure that the external generated secret adheres to certain standards, for example user authentication strong password policy. This component traces back to and aids in meeting the following objective: **O.IDAUTH**.
FMT_MOF.1	This component has been chosen to determine all TOE management, administration and security functions behaviour. This component traces back to and aids in meeting the following objectives: **O.SECFUN**, **O.RESACC**, **O.ADMIN** and **O.ACCOUN**.
FMT_MSA.1(A)	This component restricts the ability to modify, delete, or query object and subject security attributes for the MAY Cyber Access Control SFP to Super User and user authorized by Super User. It also assists in effective management and such as aids in meeting **O.SECFUN**. This component also identifies control access to resources based on the identity of users. This component traces back to and aids in meeting the following objectives: **O.RESACC**, **O.ACCOUN** and **O.ADMIN**.
FMT_MSA.1(B)	This component restricts the ability to modify, delete, or query object and subject security attributes for the Information Flow Control SFP to Super User and user authorized by Super User. It also assists in effective management, and such as aids in meeting **O.SECFUN**. This component also identifies control access to resources based on the identity of users. This component traces back to and aids in meeting the following objectives: **O.RESACC**, **O.ACCOUN** and **O.ADMIN**.
FMT_MSA.3(A)	This component ensures that the TOE provides a default restrictive value for security attributes yet allows a Super User and user authorized by Super User to override the default values. This component traces back to and aids in meeting the following objective: **O.SECFUN**. This component also identifies control access to resources based on the identity of users. This component traces back to and aids in meeting the following objectives: **O.RESACC**, **O.ADMIN** and **O.ACCOUN**.
FMT_MSA.3(B)	This component ensures that the TOE provides a default restrictive value for security attributes yet allows a Super User to override the default values. This component traces back to and aids in meeting the following objective: **O.SECFUN**. This component also identifies control access to resources based on the identity of users. This component traces back to and aids in meeting the following objectives: **O.RESACC**, **O.ADMIN** and **O.ACCOUN**.

FMT_MTD.1	This component allows authorised users (roles) control over the management of TSF data, for example change password operation. This component traces back to and aids in meeting the following objectives: **O.RESACC**.
FMT_SMF.1	This component has been chosen to consolidate all TOE management, administration and security functions. This component traces back to and aids in meeting the following objectives: **O.SECFUN**, **O.ADMIN** and **O.ACCOUN**.
FMT_SMR.1	This component ensures that roles are available to allow for varying levels of administration capabilities and restricts access to perform TSF relevant functionality depending on the role assigned to a user. This component traces back to and aids in meeting the following objectives: **O.SECFUN**. This component also identifies control access to resources based on the identity of users. This component traces back to and aids in meeting the following objectives: **O.RESACC**, **O.ADMIN** and **O.ACCOUN**.
FCS_COP.1(A)	This component requires the hash operation which can be based on an assigned standard. This cryptographic support item is used for Super User and user authorized by Super User accounts' password protection in scopSOC System. This component traces back to and aids in meeting the following objective **O.DATASTOR**.
FCS_COP.1(B)	This component requires the hash operation which can be based on an assigned standard. This cryptographic support item is used for timestamp value of audit log protection in scopSOC System. This component traces back to and aids in meeting the following objective **O.DATASTOR**.
FCS_COP.1(C)	This component requires the encryption/decryption operation which can be based on the assigned standards. This cryptographic support item is used for SNMP, SMTP, SSH, WMI, SMB, SFTP, API passwords protection in scopSOC System This component traces back to and aids in meeting the following objective **O.DATASTOR**.
FTA_SSL.3	This component ensures that TOE terminates interactive session after 1 hour. This component traces back to and aids in meeting the following objectives: **O.SECFUN**.
FTA_SSL.4	This component ensures that TOE provides capabilities for the user to terminate his/her own interactive sessions. This component traces back to and aids in meeting the following objectives: **O.SECFUN**.
FTP_TRP.1	This component is required for trusted path, which requires a trusted path between the TSF and a user be provided for a set of events. This component traces back to and aids in meeting the following objective: **O.ACCOUN**.
FPT_ITT.1	This component ensures the protection of TSF data from modification when it is transmitted between separate parts of the TOE. This component traces back to and aids in meeting the following objective: **O.CORRDATA**.

6.5. Security Assurance Requirements Rationale

The general level of assurance for the TOE consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market. Besides, TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL3 from part 3 of the Common Criteria. Therefore EAL 3 was chosen to provide a moderate level of assurance that is consistent with good commercial practices.

7. TOE Summary Specifications

This section presents the Security Functions implemented by the TOE.

7.1. TOE Security Functions

The Security functions performed by the TOE are as follows:

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

7.1.1. Security Audit

The TOE generates a set of audit logs. The TOE generates logs for the following list of events:

- Start-up and Shutdown of the audit Functions
- System logs,
- User access,
- database interaction events,
- software exceptions

Date and time of event, type of event, type of event and the success or failure status of the event is recorded. For audit events resulting from actions of identified users, the TOE associates each auditable event with the identity of the user that caused the event.

For monitoring audited events TOE enforces accumulation or combination of user and event log data according to defined rule known to indicate a potential security violation;

- Elastic HealthCheck Connection Down
- Disk Space on Elasticsearch Node become critical
- Elasticsearch File System Low at Node
- Elastic Cluster Status is RED

TOE provides Super User and user authorized by Super User with the capability to read all recorded audit information from the audit records and prohibits all users read access to the audit records, except those users that have been granted explicit read-access.

Recorded audit information is prevented and protected against unauthorized modifications, deletion or audit data loss. If the audit trail is full, Super User and user authorized by Super

User is warned about storage capacity, if not or users ignore the warning, system will continue to store the audit data to a designated storage area.

Generated logs should include Time Stamp value. Time Stamp value is hashed with MD5 algorithm and kept in a separate colon of the database table.

The Security Audit functions are designed to satisfy the following security functional requirements:

- **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.2** – Restricted Audit Review
- **FAU_STG.1** – Protected Audit Trail Storage
- **FAU_STG.4** – Prevention of Audit Data Loss

7.1.2. User Data Protection

scopSOC determines access to the management functions for users identifying and authenticating to the TOE through the scopSOC GUI.

For subset access control TOE enforces MAY Cyber Access Control SFP on Super User and user authorized by Super User attempting to establish and interactive session with the TOE, and user interface items, scopSOC authentication and authorization configurations based on user role, user ID and user permission. If the subject request access to an object and subject has permission the object, then access is granted otherwise the access is denied.

For subset information flow control, TOE enforces Information Flow Control SFP on Network Devices that receive information through the TOE and received information and sent query based on IP address, source IP address, destination IP address, protocol type, port number and port types or subtypes, using the methods like RPC, WMI, SNMP, SSH and Telnet Protocols.

TOE enforces the Information Flow Control SFP when importing and exporting device log data, controlled under the SFP, from outside of the TOE.

The User Data Protection functions are designed to satisfy the following security functional requirements:

- **FDP_ACC.1** – Subset Access Control
- **FDP_ACF.1** – Security Attribute Based Access Control
- **FDP_IFC.1** – Subset Information Flow Control
- **FDP_IFF.1** – Simple Security Attributes
- **FDP_ITC.1** – Import of User Data without Security Attributes
- **FDP_ETC.1** – Export of User Data without Security Attributes

7.1.3. Identification and Authentication

The TOE performs identification and authentication of all users accessing the TOE. Security attributes belonging to individual users like; Authorization status as determined by the TOE, user role, user ID and IP address is maintained. Additionally, these security attributes with subjects acting on the behalf of that user is associated.

A mechanism is provided by the TOE to verify the rules for user authentication that forces users to have a strong password policy, which should be at least 8 characters long and should contain at least three of the following;

- Uppercase letter,
- Lowercase letter,
- Number,
- Symbol

The TOE protects the authentication feedback by providing only dots as digits of the password to the user while the authentication is in progress.

The Identification and Authentication function is designed to satisfy the following security functional requirements:

- **FIA_ATD.1** – User Attribute Definition
- **FIA_UAU.2** – User Authentication Before any Action
- **FIA_UAU.7** - Protected authentication feedback
- **FIA_UID.2** – User Identification Before Any Action
- **FIA_USB.1** – User Subject Binding
- **FIA_SOS.1** – Verification of Secrets

7.1.4. Security Management

The TOE maintains ten security roles by default for the management and monitoring of TOE.

- Super User; is the user role which has all privileges on the platform.
- Platform Manager; is the user role who configures platform level configurations and has access to Settings.
- Monitoring Manager; is the user role who monitors system and network resources and has access to scopMON.
- Incident and Request Manager; is the user role who manages and tracks security incident and has access to scopDESK.
- SIEM Manager; is the user role who collects logs and creates analytics rules and has access to scopVISION.
- Event Manager; is the user role who manages security events and takes centralized actions and has access to Event Engine.
- Dashboard Manager; is the user role who analyzes and visualizes security data and has access to Dashboards.
- Asset Manager; is the user role who discovers assets and manages vulnerabilities and has access to Asset Management.
- Command Execution Manager; is the user role who manages and creates external commands and has access to Command Execution.
- Reporting Manager; is the user role who creates and distributes reports and has access to Reporting

The TOE is capable of performing the management functions such as Create, Delete, Modify and View security attribute values, enable and disable External IT entities from communicating to the TOE, review of audit trail.

The TOE restricts the ability to disable and enable the password policy flag function and modify the user information to Super User and user authorized by Super User.

The TOE enforces the MAY Cyber Access Control SFP to restrict the ability to query, modify and delete the following security attributes to Super User and user authorized by Super User;

- Event Information,
- Asset Information,
- Collected Log Data,
- Incident Information

The TOE enforces Information Flow Control SFP to restrict the ability to change default the security attributes query and responses to Super User and user authorized by Super User.

While MAY Cyber Access Control SFP provides permissive default values for security attributes that are used to enforce the SFP, Information Flow Control SFP on the other hand provides restrictive default values for security attributes that are used to enforce the SFP.

Additionally, TOE allows the Super User and user authorized by Super User to specify alternative initial values to override the default values when an object or information is created.

The Security Management function is designed to satisfy the following security functional requirements:

- **FMT_MOF.1** – Management of Security Functions Behaviour
- **FMT_MSA.1(A)** – Management of Security Attributes
- **FMT_MSA.1(B)** – Management of Security Attributes
- **FMT_MSA.3(A)** – Static Attribute Initialization
- **FMT_MSA.3(B)** – Static Attribute Initialization
- **FMT_MTD.1** – Management of TSF data
- **FMT_SMF.1** – Specification of Management Functions
- **FMT_SMR.1** – Security Roles

7.1.5. Cryptographic Support

In scopSOC System, timestamp value of audit logs and collected logs in TOE is hashed using MD5 algorithm with 128 bit cryptographic key sizes that meets the criteria defined in RFC 6151 when saved into the database. User account passwords of Super User and users defined by Super User are hashed using SHA-256 algorithm with 256 bit cryptographic key sizes that meets the criteria defined in (FIPS) PUB 180-4 when saved into the database. SNMP, SMTP, SSH, WMI, SMB, SFTP, API passwords are encrypted (and decrypted) using AES algorithm with 256 bit cryptographic key sizes that meets the criteria defined in (FIPS) 140-2 and Annex A, NIST FIPS 197, RFC 2315, PKCS 7, RFC 4648 when saved into the database.

The Cryptographic Support functions are designed to satisfy the following security functional requirement

- **FCS_COP.1(A)** – Cryptographic Operation – Hash Operation/Password Protection
- **FCS_COP.1(B)** – Cryptographic Operation – Hash Operation/Log Protection
- **FCS_COP.1(C)** – Cryptographic Operation – Encryption & Decryption Operation/Password Protection

7.1.6. TOE Access

After the logout or a specified time interval of user inactivity, TOE terminates interactive session. The session timeout value is by default 1 (one) hour.

The TOE Access function is designed to satisfy the following security functional requirements:

- **FTA_SSL.3** – TSF Initiated Termination
- **FTA_SSL.4** – User Initiated Termination

7.1.7. Trusted Path/Channels

TOE provides 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. In scopSOC System, credentials are protected between the scopSOC and scopSOC GUI application. SSL (Secure Socket Layer), cryptographic protocols designed to provide communications security over a computer network, is used for communication between scopSOC Users and scopSOC GUI. It provides "HTTPS" connection.

The Trusted Path/Channels function is designed to satisfy the following security functional requirement:

- **FTP_TRP.1** – Trusted Path

7.1.8. Protection of the TSF

The TOE protects the TSF data from modification when it is transmitted between separate parts of the TOE.

The Protection of the TSF function is designed to satisfy the following security functional requirement:

- **FPT_ITT.1** – Basic Internal TSF Data Transfer Protection