Security Information and Event Management

SIEM GUI v2.0.2 with SIEM SERVER v6.2.0 and SIEM RECORDER v9.2.2 and SIEM AGENT v6.1.0

Security Target Version 1.12

Release Date: 29.08.2016

AUTHOR:

NATEK BİLİŞİM BİLGİSAYAR EĞİTİM DANIŞMANLIK YAZILIM TİCARET SANAYİ ANONİM ŞİRKETİ

Revision History

Version No	Reason for Change	Release Date	Prepared By	Approved By
1.0	First Draft	25.06.2015	Ertuğrul BALABAN	Necati ERTUĞRUL
1.1	Release Version	13.07.2015	Ertuğrul BALABAN	Necati ERTUĞRUL
1.2	“Survey Report 1” Update (GR_1)	25.08.2015	Ertuğrul BALABAN	Necati ERTUĞRUL
1.3	“Survey Report 4” Update (GR_4)	06.10.2015	Ertuğrul BALABAN	Necati ERTUĞRUL
1.4	“Survey Report 6” Update (GR_6)	15.10.2015	Ertuğrul BALABAN	Necati ERTUĞRUL
1.5	“ST Survey Report”	06.11.2015	Ertuğrul BALABAN	Necati ERTUĞRUL
1.6	“ST Survey Report”	10.11.2015	Ertuğrul BALABAN	Necati ERTUĞRUL
1.7	“ST Survey Report”	18.01.2016	Ertuğrul BALABAN	Necati ERTUĞRUL
1.8	“ST Survey Report”	21.01.2016	Ertuğrul BALABAN	Necati ERTUĞRUL
1.9	“ST Survey Report 16” Update (GR_16)	11.02.2016	Ertuğrul BALABAN	Necati ERTUĞRUL
1.10	Release Version	27.05.2016	Ertuğrul BALABAN	Necati ERTUĞRUL
1.11	Release Version OKTEM Quality Update	07.06.2016	Ertuğrul BALABAN	Necati ERTUĞRUL
1.12	“ST Survey Report 26” Update (GR_26)	29.08.2016	Ertuğrul BALABAN	Necati ERTUĞRUL

TABLE OF CONTENTS

1. Introduction

Information and event security have become an important requirement for the companies. These requirements increase the dependency to more effective security management, systematic real time analysis and reports, apprehending the patterns and activities that cannot be detected by human eye, correlation of incidents and logs.

Natek SIEM (Security Information and Event Management) is a system associating security information and security event management of software products and services. Natek SIEM aims to meet the requirements mentioned above by providing security intelligence, punctual event response, flawless log management, renewable compliance reporting. In this regard, Natek SIEM also enables the information relevant to enterprise's security to be revised from a single point of view to assess the trends and patterns.

Structural Features

In the core of NATEK SIEM is a Lucene Based big data platform for audit data analysis. By using an agentless log collection infrastructure collected data is filtered and centralized. Advanced correlation features enable real-time visibility for security risks.

The solution offers correlation analysis based on frequency analysis, long term trend analysis, linking distinct events and linking data for an expected order of occurrence.

For end-point tracking agents are deployed on Windows based devices. The system polls the computer information from Active Directory or uses IP Range Scans for deployment. The deployments can be performed manually or continuously. In case continuous deployment is used, the system will deploy the agents automatically without any user effort.

After the agents are installed, the status of the agents are monitored centrally. In case a problem occurs or an agent is uninstalled in the system, an alert is raised to security administrators. This enables system administrators to identify any problems occurring within the agents. NATEK Agent offers distinctive features for tracking any possible security risks.

Through inventory analysis module software installations/removals, processes running on computers and many similar events can be tracked. Any inventory information needed can be collected using WMI protocol.

NATEK SIEM also tracks USB and printers. The tracking can be based on the activity record or content. In case content tracking is chosen all data copied to USB or printed is duplicated on a central server for analysis. USB authorization can also be performed permitting only defined USB devices for use within the company network. Other features of NATEK SIEM are process authorization, RDP session tracking and local user account password management.

Within NATEK SIEM all rules are configured centrally. The rules define what to collect, which data to correlate, and generate alarms for the tracked events. The alert generation is handled centrally, making it possible to make customizations with ease.

This Security Target is for evaluation of Natek Security Information and Event Management (SIEM) 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:	NATEK Security Information and Event Management (SIEM)
Version:	1.12
Publication Date:	29.08.2016
ST Author:	Natek Bilişim Bilgisayar, Eğitim, Danışmanlık, Yazılım Ticaret Sanayi Anonim Şirketi.
Assurance Level:	The ST is EAL 3 conformant.

1.2. TOE Reference

TOE Identification:	NATEK Security Information and Event Management (SIEM)
Version:	SIEM GUI 2.0.2 with SIEM Server 6.2.0, SIEM Recorder 9.2.2 and SIEM Agent 6.1.0
Publication Date:	29.08.2016
Vendor:	Natek Corporation
Assurance Level:	The TOE is EAL 3 conformant.

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 NATEK Security Information and Event Management (SIEM) SIEM GUI Version 2.0.2 with SIEM Server v6.2.0, SIEM Recorder v.9.2.2 and SIEM Agent v6.1.0 will hereafter be referred to as the TOE through this document. The TOE is a security information and event manager that collects, stores, and normalizes log and event data from a variety of sources, and displays that data in a web interface for monitoring, searching, and analysis. Data is also available for scheduled and reporting.

1.4. TOE Major Security Features for Operational Use

Natek SIEM is software-only product for the administration of enterprise IT Environments and consists of 4 main modules; SIEM GUI, SIEM Server, SIEM Recorder and SIEM Agent. It also provides platform-independent control over the combined IT infrastructure and the applications they support. Its architecture and design provides users a single management approach to monitor resources.

- **SIEM GUI:** SIEM GUI Functions provides graphical user interface for SIEM operations like SIEM Log Settings, Dashboard Management and fast data fetch for log in Elastic Search.
- **SIEM Server:** SIEM Server Functions provides server operations to show how to collects the event data logs for the devices.
- **SIEM Recorder:** SIEM Recorder Functions provides special recorder properties for each network devices to collect log data.
- **SIEM Agent:** SIEM Agent Functions provides to collect the log data according to customer needs. Agent structure can be selected for log collection if customer wants to use agent for each client.

TOE of the Natek SIEM System should contain 5 main Security Functions which are;

- Security Audit,
- User Data Protection,
- Identification and Authentication,
- Security Management,
- Cryptographic Support

All of these security functions will be examined in a detailed on Chapter 1.4.2.

1.4.1. TOE Type

TOE Type is ***software*** based Security Information and Event Management (Log Management).

1.4.2. 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. Natek SIEM has 4 main modules; ***SIEM GUI, SIEM Server, SIEM Recorder and SIEM Agent.***

- *The minimum operating system (O/S) and hardware requirements for the* ***SIEM GUI*** *host computer are;*

O/S	: Windows 7 or higher, preferably Windows Server 2008 64-bit, or higher
CPU	: Intel Pentium Core 2 Duo 2.0 GHz, or faster
RAM	: At least 1GB, preferably 2GB
Connectivity	: TCP/IP network interfaces
Disk space for TOE	: At least 4 GB
Hard Drive Space	: 100 GB

- *The minimum operating system (O/S) and hardware requirements for the* ***SIEM Server*** *host computer are;*

O/S	: VMware, preferably Windows Server 2008 64-bit, or higher
CPU	: Intel Pentium Core 2 Duo 2.4 GHz, or faster
RAM	: At least 4GB, preferably 8GB
Connectivity	: TCP/IP network interfaces
Disk space for TOE and logs	: At least 2 GB / Subject to Log details
Hard Drive Space	: 50 GB

- *The minimum operating system (O/S) and hardware requirements for the* ***SIEM Recorder*** *host computer are;*

O/S	: VMware, preferably Windows Server 2008 64-bit, or higher
CPU	: Intel Pentium Core 2 Duo 2.4 GHz, or faster
RAM	: At least 4GB, preferably 8GB
Connectivity	: TCP/IP network interfaces
Disk space for TOE and logs	: At least 2 GB / Subject to Log details
Hard Drive Space	: 50 GB

- *The minimum operating system (O/S) and hardware requirements for the* ***SIEM Agent*** *host computer are;*

O/S	: VMware, preferably Windows Server 2008 64-bit, or higher
CPU	: Intel Pentium Core 2 Duo 2.4 GHz, or faster
RAM	: At least 1GB, preferably 2GB
Connectivity	: TCP/IP network interfaces
Disk space for TOE and logs	: At least 2 GB / Subject to Log details
Hard Drive Space	: 50 GB

1.4.3. 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. In addition to this:

For SIEM GUI;

- The operational environment must include 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 authorized administrators of the TOE as a medium of communication with the TOE's web GUI.
- The operational environment must include .NET Framework 4.0 and IIS 7.5 or higher
- The operational environment must include the database MSSQL 2008 R2 or higher
- The operational environment must include either Windows 2008 or Windows 2012

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.

For SIEM Server;

- The operational environment must include minimum .NET Framework 4.0
- The operational environment must include the database MSSQL 2008 R2 or higher
- The operational environment must include either Windows 2008 or Windows 2012

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.

For SIEM Recorder;

- The operational environment must include minimum .NET Framework 4.0
- The operational environment must include the database MSSQL 2008 R2 or higher
- The operational environment must include either Windows 2008 or Windows 2012

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.

For SIEM Agent;

- The operational environment must include .NET Framework 3.5
- The operational environment must include the database MSSQL 2008 R2 or higher
- The operational environment must include either Windows 2008 or Windows 2012

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.

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 Natek SIEM components.

1.5. TOE Description

This section provides the detailed information and description of TOE included physical and Logical boundaries of the system.

NATEK SIEM is a solution, which centrally monitors and manages the security information and security event infrastructure.

SIEM acts as a monitoring and management tool for use by network managers. It collects logs and events from multiple remote third-party systems, and alerts the network managers to specified conditions. It operates based on below scenario.

There are four main components which are SIEM GUI, SIEM Server, SIEM Recorder and SIEM Agent.

SIEM Server responsibilities and services;

- Natek SIEM Action,
- Natek SIEM Agent Check
- Natek SIEM Intelligence
- Natek SIEM Maintenance
- Natek SIEM Monitor
- Natek SIEM Schedule
- Natek SIEM Control

In Natek SIEM, there **two roles** for SIEM GUI that are **SIEM GUI User** (Administrator) and **SIEM Base User**. These roles have specified and defined authorization according to needs. Later on, more roles can be added through GUI.

Moreover, there are **three database** to store information which are **NASCMDB** , **SIEM DB and Elastic Search DB.** They provide to store user and network device information and configurations.

- **NASCMDB** stores user and user related information like username, password, roles, tickets, etc...
- **SIEM DB** stores all SIEM system operation information like devices data, recorders, agents, alerts, correlations, etc…
- **Elastic Search DB** store real-time device logs

All these items included in the **physical boundary** of the system.

The TOE of Natek SIEM System also provides **logical boundary** of the system. It depends on security audits, cryptographic security functions, identification and authentication information, user data protection and security management.

- User accesses GUI through **http://ServerIPAdress/siem** address.
- Via User Settings >> Authentication Management, users are created and their roles are determined for GUI.
- Through Server Settings;
  - ✓ Credential Management, required log processes are operated for Recorders to register the logs.
  - ✓ Data Management Settings, table creation is operated.
  - ✓ Group Management, groups required for tables and Recorders are created.
  - ✓ Remote Log Collection Settings>>Log Collection Rules, Recorder definitions are made for tracking status.
  - ✓ Remote Log Collection Settings>>Remote Log Collection Management, policy and groups are activated according to the created Filter Hosts.
- Through Policy Management >> Audit Policy, policies are determined for relevant tables.
- Through Correlation Settings >> Count Correlation, correlation settings are managed.
- Through Reporting >> Report Editor, new reports are created and report outputs are received.
- On Dashboard, search operations are executed based on pars structure from Fields field on the right bottom part.
- During this process when the confirmed field is clicked, the statical data of the top 10 data through 5000 lines is displayed.
- Through Dashboard, filtering is operated for different index are implemented from the “Action” in the default Document Types.
- The time period of the logs registered in “Time Filter” through Dashboard, can be specified and ordered.
- On Dashboard, the elements set as default can be managed and saved from “Configure Dashboard”.
- Through Query Panel in Dashboard, Full-Text search can be executed.
- Through Data Analysis >> Big Data Query Builder tab, queries can be created for retrieving required data.

According to scenarios above, as a summary with the concept of the TOE, SIEM GUI, SIEM Recorder, SIEM Agent and SIEM Server' s components and databases have the following functions.

SIEM Server

- **SIEM Agent Check;** checks the Agent status and control it's works.
- **SIEM Action;** named as Alert Engine which creates alarm according to alert values.
- **SIEM Control;** Update Central State. It pings the down machines and according to response updates the status of it.
- **SIEM Schedule;** installs the agent on remote according to selected IP ranges in provided and defined schedule.
- **SIEM Monitor;** check the system status and system health. Checks and controls the SIEM Component's status (SIEM Server, SIEM Agent and SIEM Recorder), if one of them down, it is restarted.
- **SIEM Correlation;** Mapper Correlation, Count Correlation and Composite Count Correlation. Mapper Correllation Configuration provides flow relationship between two different log types. For instance, the user who enters the impact field is expected to register first in the entry system. If the first register logs out then it can be found that another user utilizes this account. Count Correlation enables action production via SNMP or email when a specific event occurs in specified amount. Composit Count Correlation is similar to Count Correlation. Different from the Count Correlation in the Composit Count Correlation, it is considered how much other correlations occur instead of considering a specific event occurrence in specific amount. If the defined threshold is excessed then alert production is enabled.
- **SIEM Intelligence;** Trend Analysis and Correlation Calculation. Intelligence Analysis Configuration calculates the occurence amount of specific events in the specified time periods. The calculated values are kept in the tables the names of which start with 'I_'. The system calculates the occurence average of these events. When the calculated value excesses the average, the action production is enabled via SNMP or email.
- **SIEM Maintenance;** Delete Logs

SIEM Recorder

- **SIEM Recorder Engine;** activate the new recorder to collect data and refresh the local recorders.
- **SIEM Refresh Remote Recorder;** provides the remote working recorders which defined on database before.
- **SIEM Filter;** scans the to do lists and processes then, filter them according to defined rules.

SIEM Agent

- **SIEM Access;** checks the permitted ip list access, according to results limit the access.
- **SIEM Distributer;** makes distribution rules, does registry and policy configurations and makes remote connection to agent for distribution configurations.
- **SIEM Inventory;** collects machines asset informations and send the related data for WMI configuration.
- **SIEM Printer;** checks the system printer events and collect event logs.
- **SIEM Recorder;** catches the events from the agent installed machine’s logs and send them remote.
- **SIEM Sender;** sends the applied command to the remote after applying the filter for remote recorders.

Databases

- **NASCMDB;** stores user’s information for controlling access to GUI.
- **SIEM DB;** stores all system operation information of the SIEM system.
- **Elastic Search DB** stores real-time device logs.

1.5.1. 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”). For a graphical representation of the scope and the points of interaction between the various components of the TOE also refer to the Figure 1.

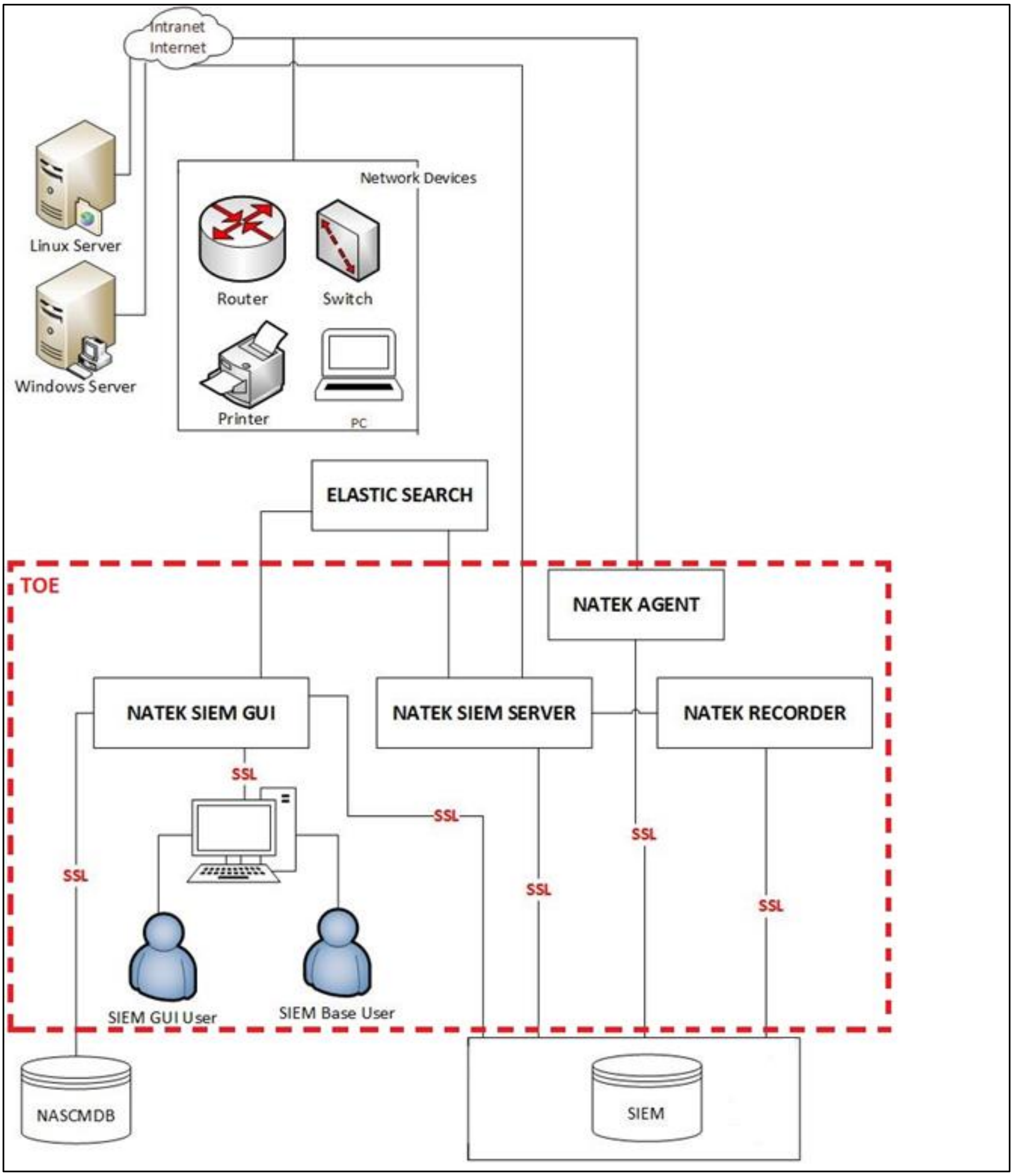


Figure 1: Physical Boundary of TOE

1.5.2. 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.

Table 1: Logical Boundary

Security Functions	Description
Security Audit	The TOE generates audit records for security events. Only the admin role is allowed to view the audit trail.
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. Administrator can configure the TOE, manage users and audit among other routine maintenance activities.
Cryptographic Support	The TOE support cryptographic security functions for storing crucial informations for user like User Password.

1.5.2.1. Security Audit

The TOE 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.

The audit data can be viewed only by administrators.

1.5.2.2. User Data Protection

The information below which are identified in TOE scope, is protected against access by unauthorized users. This information is used by Natek SIEM components.

- User Information (SIEM GUI User and Baseuser)
- Authorization and Authentication Information (Roles, Menu, Ticket etc...)

- Configuration and Configuration Items Information (Network and Credentials etc…)
- System Logs (GUI, functions and database etc…)
- Audit Logs (Real-time device logs which stores in Elastic Search)
- Device and Inventory Information (Scanned Device, OS, Installed Applications etc…)

1.5.2.3. Identification and Authentication

The TOE 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 a forward redirection to the login page.

1.5.2.4. Security Management

TOE provides Security Management functions like configuration of TOE; manage the users, audit, maintenance activities etc…

In the Security Management activities of the TOE uses the list below;

- Users and passwords
- Roles, Tickets, Menus
- Authentication and Authorization Mechanism
- Audit Logs

The TOE allows for the management of sessions (SIEM GUI) connection. Authorized administrators are granted the ability to set the idle timeout threshold after which an authorized user would be automatically logged out of his active session. Idle timeout is defined as a period of inactivity from the user on database (Default value is an hour).

1.5.2.5. Cryptographic Support

In Natek SIEM System, authentication and identification is performed via a username password combination that will not only identify a specific user to the system but also define the level of access permitted to that particular user account. On top of it, the password will be encapsulated by system automatically using Microsoft Library SHA_1 Managed Algorithm when saved into the database (NASCMDB). Besides, audit operations on SIEM, related user data are stored by the System Administrator and these information will also be hashed. Hashed data stored to control if any modification on log data.

1.6. Document Conventions

The notation formatting and conventions used in this Security Target are consistent with those used in Version 3.1 Revision 4 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, FAU_GEN.1(A), FAU_GEN.1(B)

1.7. Document Terminology

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

CC	: Common Criteria
CPU	: Central Processing Unit
DAU	: Data Authentication
EAL	: Evaluation Assurance Level
GUI	: Graphical User Interface
IT	: Information Technology
MAC	: Media Access Control
MIB	: Management Information Base
MSA	: Management of Security Attribute
NASCMDB	: Natek Application Suit Central Management Database
OS	: Operating System
OSP	: Organization Security Policy
PP	: Protection Profile
RPC	: Remote Procedure Call
SAR	: Security Assurance Requirement
SFR	: Security Functional Requirement
SIEM	: Security Information and Event Management
SMF	: Specification of Management Functions
ST	: Security Target
TOE	: Target of Evaluation
TSF	: TOE Security Function

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 (September 2012) 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 4 (September 2012). 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 4, September 2012.

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

There are no Protection Profile claims for this Security Target.

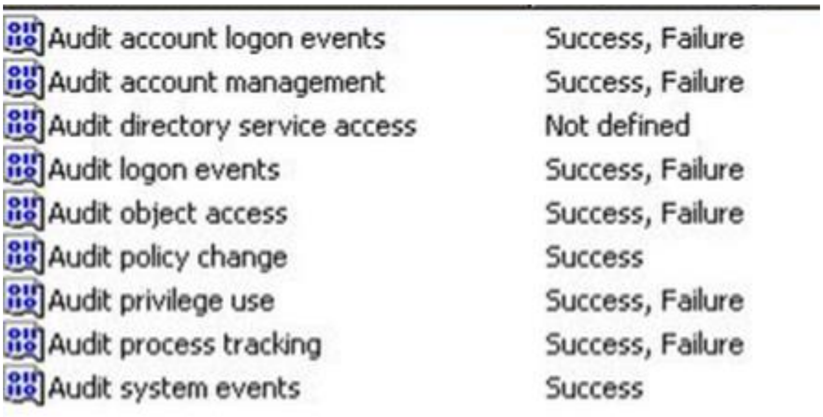
3. Security Problem Definition

3.1. Roles

- **SIEM GUI User (Admin/Administrator):** During the user description, the user is required to have a role with the purpose of displaying the menus. This role arranges the role authorizations, it has administrative authority.
- **SIEM Base User:** Monitor the systems in a limited screen.

3.2. Assets

- **Configuration and device data** are stored in the SIEM 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. In the example group policy:



Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Not defined
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit policy change	Success
Audit privilege use	Success, Failure
Audit process tracking	Success, Failure
Audit system events	Success

Figure 2: Group Policy Example

If the relevant policy is not arranged, then log will not be created. SIEM is basically required to meet the 5651 law thus the system logs in the law must be received. The user logon/logoff actions will be created by activation of "Audit logon events","Audit account logon events" policies explained above.

- **System log data** related with the SIEM Components logs which helps System Admin to understand the any error in the SIEM System.
- **User information data** such as role, ticket data related to GUI. This data is stored in the NASCMDB.

3.3. 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 SIEM Database Table and NASCMDB.

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**

A user or process 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

3.4. 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.

- ✓ **OSP.SECURE TRANSFER:**

There are two main OSPs defined for this Security Target.

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

Second policy is same as first policy, SSL communication is used for communication between SIEM Components (SIEM GUI, SIEM Server, SIEM Recorder and SIEM Agent) to SIEM Databases. NASCMDB database has only connection with SIEM GUI. That’s why SSL secure connnection is also applied for communication between SIEM GUI and NASCMDB.

3.5. 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. The specific conditions listed in the following subsections are assumed to exist in the TOE environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

- ✓ **A.ACCESS DATA-A.ACCDATA:** The TOE has access to all the IT System data it needs to perform its functions.
- ✓ **A.EDUCATED USER-A.EDUCUSER:** Authorized administrator and end users are educated so as to use the Natek SIEM system suitably and correctly. The Administrator will install and configure the TOE according to the management guide.
- ✓ **A.NO EVIL USER-A.NOEVIL:** Authorized administrator, who manage the TOE are non-hostile use, configure and maintain the TOE and follow all guidance.
- ✓ **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. Secure environment should include server data collection is only related with the intranet, there is no internet connection.
- ✓ **A.TRUSTED PERSON-A.TRUST:** The designer, programmer (coder) and administrator who are responsible for creation of architecture, coding and administrative functions done by trusted persons.

4. Security Objectives

4.1. Security Objectives for the TOE

The IT security objectives for the TOE are addressed below:

- ✓ **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.AUDIT REVIEW-O.AUDREV:** The TOE will provide the capability to view audit and system data information in a human readable form.
- ✓ **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 Natek SIEM Server component.
- ✓ **O.DATA STORAGE-O.DATASTOR:** The TOE will provide audit data storage in a secure manner. When it will be out of memory, user will be warned, if not or user ignore the warning the audit data will be deleted according to Administrator decision, transferred suitable data storage or continue to store in a ".bat" format.
- ✓ **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 authorized administrators (SIEM GUI User) to specify which resources may be accessed by which users.
- ✓ **O.SECURITY FUNCTIONS-O.SECFUN:** The TOE will provide functionality that enables an authorized administrator to use the TOE security functions and will ensure that only authorized administrator 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:** Authorized administrators 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.TRUSTED PERSON-OE.PERTRST:** Authorized administrators, coder, designer and also service personnel will be trusted person and they will not generate any threat for the TOE.
- ✓ **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.

Table 2 Security Objective Rationale

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	A.TRUST	OSP.SECURE TRANSFER
O.AUDREC				X	X							
O.AUDREV				X	X							
O.CORRDATA	X											
O.DATASTOR			X									
O.IDAUTH				X	X							
O.RESACC		X		X	X							
O.SECFUN					X							
OE.TIMESTAMP	X											
OE.ADMTRA							X					
OE.COMM									X			X
OE.ENVSEC		X							X	X		
OE.GUIDAN						X		X				
OE.PERTRST											X	
OE.ELASTRUCTURE	X					X						

4.3.1. Rationale for Security Threats to the TOE

Table 3 Justification about Threats

THREAT	RATIONALE
T.DATAUPDATE	This threat is completely countered by • O.CORRDATA which ensures user access corrects 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 authorized administrators 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 in a secure manner. When it will be out of memory, the audit data will be deleted according to Administrator decision or stored or transferred suitable data storage.
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.AUDREV which ensures the TOE will provide the capability to view audit and system data information in a human readable form. • 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 authorized administrators 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.AUDREV which ensures the TOE will provide the capability to view audit and system data information in a human readable form. • O.RESACC which must control access to resources based on the identity of users. The TSF must allow authorized administrators 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 Security Objectives

Table 4 Justification about Objectives

OBJECTIVES	RATIONALE
O.AUDREC	This security objective is necessary to counter the threat: T.MASQ and T.NOAUTH by requiring that the TOE provides a means to record a readable audit trail of security related events. 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 audit records.
O.AUDREV	This security objective is necessary to counter the threat: T.MASQ and T.NOAUTH by requiring that administrator may not have the ability to notice potential security violations such as attempts by users to gain unauthorized access to the TOE, thus limiting the administrator's ability to identify and take action against a possible security breach.
O.CORRDATA	This security objective is necessary to counter the threat: T.DATAUPDATE mitigates this threat by controlling the logical access to the TOE and its resources. By constraining how and when authorized users can access the TOE this objective helps mitigate the possibility of a user attempting to login and masquerade as an authorized user.
O.DATASTOR	This security objective is necessary to counter the threat: T.FUL_AUD by requiring that the TOE provides functionality that ensures that only authorized users have access to the TOE security functions.
O.IDAUTH	This security objective is necessary to counter the threat: T.NOAUTH because it requires that user be uniquely identified before accessing the TOE and strong password policy for user authentication. Then, T.MASQ by requiring that administrator may not have the ability to notice potential security violations

O.RESACC	This security objective is necessary to counter the threats: T.MASQ by requiring that administrator may not have the ability to notice potential security violations such as attempts by users to gain unauthorized access to the TOE, thus limiting the administrator's ability to identify and take action against a possible security breach and T.DATALOSS which consists of unauthorized access to data and resources. Then, T.NOAUTH because it requires that user be uniquely identified before accessing the TOE and strong password policy for user authentication
O.SECFUN	This security objective is necessary to counter the threat: T.NOAUTH because it requires that user be uniquely identified before accessing the TOE and strong password policy for user authentication.
OE.TIMESTAMP	This security objective is necessary to counter the threat: T.DATAUPDATE by requiring a readable audit trail. This threat ability to identify and take action against a possible security breach.
OE.ADMTRA	This non-IT security objective is necessary to counter the assumption: A.EDUCUSER which ensures that it is delivered, installed, administrated and operated in a secure manner and usage.
OE.COMM	This non-IT security objective is necessary for the providing environment security of the product that the TOE ensure that it should be physical protection for secure channel for administrator authentication procedure. (A.PYHPROT)
OE.ENVSEC	This non-IT security objective is necessary to counter the threat: T.DATALOSS which consists of unauthorized access to data and resources and, providing environment security of the product that the TOE ensure that it is protected and it has secure environment which also provides secure channel for administrator authentication procedure. (A.SECENV and A.PYHPROT)

OE.GUIDAN	This non-IT security objective is necessary for the providing TOE has access to all the IT System resources necessary to perform its functions (A.ACCDATA). Administrators are non-hostile and follow the administrator guidance when using the TOE. Administration is competent and on-going (A.NOEVIL).
OE.PERTRST	This non-IT security objective provides reliability about personality related with the TOE security. All personnel are faithful, trained and not permit offensive attack about product. (A.TRUST)
OE.ELASTURCTURE	This non-IT security objective is necessary to counter the threat: T.DATAUPDATE mitigates this threat by controlling the logical access to the TOE and its resources. By constraining how and when authorized users can access the TOE this objective helps mitigate the possibility of a user attempting to login and masquerade as an authorized user. Then, The TOE has access to all the IT System resources necessary to perform its functions. (A.ACCDATA).

5. Extended Components Definition

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

5.1. Extended TOE Security Functional Components

There is no Extended TOE Security Functional Components Definition in the Security Target.

5.2. Extended TOE Security Assurance Components

There is no Extended TOE Security Assurance Components Definition in the Security Target.

5.3. Rationale for Extended Security Functional Components

There is no extended Security Functional Components and Security Assurance Components that have been defined for this Security Target.

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 list of included Security Functional Requirements Components.

Table 5 Suitability of the SFRs

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.4	Prevention of audit data loss
	FAU_ARP.1	Security Alarms
User Data Protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Simple 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
	FDP_ETC.1	Export of user data without security attributes
Identification and Authentication	FIA_ATD.1	User Attribute Definition
	FIA_UAU.2	User Authentication before any action
	FIA_UID.2	User Identification before any action
	FIA_AFL.1	Authentication failure handling
	FIA_SOS.1	Verification of Secrets
Security Management	FMT_MSA.1 (A)	Management of security attributes
	FMT_MSA.1 (B)	Management of security attributes
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specifications of Management Functions
	FMT_MSA.3 (A)	Static Attribute Initialization
	FMT_MSA.3 (B)	Static Attribute Initialization
	FMT_MOF.1	Management of Security Functions
	FMT_SMR.1	Security Roles
TOE Access	FTA_SSL.3	TSF Initiated termination
Cryptographic Support	FCS_COP.1 (A)	Hash operation/Password Protection
	FCS_COP.1 (B)	Hash operation/Log Protection

Table 6 Security Functional Requirements Dependencies

SFR	Dependency	Applied
FAU_GEN.1	FPT_STM.1 Reliable Time Stamp	*FAU_GEN.1 requires that FPT_STM.1 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 is not included.*
FAU_GEN.2	FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification	YES
FAU_SAA.1	FAU_GEN.1 Audit data generation	YES
FAU_SAR.1	FAU_GEN.1 Audit data generation	YES
FAU_SAR.2	FAU_SAR.1 Audit Review	YES
FAU_STG.4	FAU_STG.1 Protected audit trail storage	YES
FAU_ARP.1	FAU_SAA.1 Potential Violation Analysis	YES
FDP_ACC.1	FDP_ACF.1 Security attribute based access control	YES
FDP_ACF.1	FDP_ACC.1 Subset Access Control FMT_MSA.3 (A)Static Attribute Initialization	YES
FDP_IFC.1	FDP_IFF.1 Simple Security Attributes	YES
FDP_IFF.1	FDP_IFC.1 Subset Information Flow Control FMT_MSA.3(B)Static Attribute Initialisation	YES
FDP_ITC.1	[FDP_ACC.1 Subset Access Control or FDP_IFC.1 Subset Information Flow Control] FMT_MSA.3 (B) Static Attribute Initialisation	YES (FDP_IFC.1)

FDP_ETC.1	[FDP_ACC.1 Subset Access Control or FDP_IFC.1 Subset Information Flow Control]	YES (FDP_IFC.1)
FIA_ATD.1	No dependencies	-
FIA_UAU.2	FIA_UID.1 Timing of identification.	YES
FIA_UID.2	No dependencies	-
FIA_AFL.1	FIA_UAU.1 Timing of Authentication dependencies.	YES FIA_UAU.2 hierarchical to FIA_UAU.1 included
FIA_SOS.1	No dependencies	-
FMT_MSA.1(A)	[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.	YES (FDP_ACC.1)
FMT_MSA.1(B)	[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.	YES (FDP_IFC.1)
FMT_MSA.3 (A)	FMT_MSA.1 Management of Security Attributes, FMT_SMR.1 Security roles	YES (FMT_MSA.1 (A))
FMT_MSA.3 (B)	FMT_MSA.1 Management of Security Attributes, FMT_SMR.1 Security roles	YES (FMT_MSA.1 (B))
FMT_MTD.1	FMT_SMR.1 Security roles FMT_SMF.1 Specifications of Management Functions	YES
FMT_SMF.1	No dependencies	-
FMT_MOF.1	FMT_SMR.1 Security Roles and FMT_SMF.1 Specification of Management Functions	YES
FMT_SMR.1	FIA_UID.1 Timing of identification	YES FIA_UID.2 hierarchical to FIA_UID.1 is included
FTA_SSL.3	No dependencies	-

FCS_COP.1 (A)- Hash Operation/Password Protection	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	*Hash algorithms don't require cryptographic keys, hence no restriction has been made on assignments. FCS_CKM.4 component has not been added, since it is not definite that there will be a need for cryptographic keys. Using FDP_ITC.1 and FDP_ITC.2 not related with FCS_COP.1*
FCS_COP.1 (B)- Hash Operation/Log Protection	[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	*Hash algorithms don't require cryptographic keys, hence no restriction has been made on assignments. FCS_CKM.4 component has not been added, since it is not definite that there will be a need for cryptographic keys. Using FDP_ITC.1 and FDP_ITC.2 not related with FCS_COP.1*

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 PP/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_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 [SIEM GUI User] with the capability to read [all recorded 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.

6.1.1.4. 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.

6.1.1.5. 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 user about storage capacity and delete old logs manually] if the audit trail is full.

6.1.1.6. FAU_ARP.1 – Security Alarms

Description: Security alarms, the TSF shall take actions in case a potential security violation is detected.

Hierarchical to: No other components.

Dependencies: FAU_SAA.1 Potential Violation Analysis

FAU_ARP.1.1 The TSF shall take [sending alarms] upon detection of a potential security violation.

6.1.1.7. 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
5. Recorder Stopped]

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 [Administrative Access Control SFP] on

[Subjects: users attempting to establish and interactive session with the TOE,

Objects: user interface items, SIEM 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 [Administrative access control SFP] to objects based on the following:
Subject: users attempting to establish and interactive session with the TOE,

Object: user interface items, SIEM authentication and authorization configurations,

[Subject attribute:

1. User Role,
2. User ID,
3. User's Tickets.

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:

[If the subject is the TOE Administrator, then access is granted,

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 Attribute

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: [

<u>SIEM Server connection establishment is allowed, if</u>

- 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(s)] 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.

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(s)] 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].

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_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.

6.1.3.4. FIA_AFL.1 – Authentication Failure Handling

Description: Authentication failure handling requires that the TSF be able to terminate the session establishment process after a specified number of unsuccessful user authentication attempts. It also requires that, after termination of the session establishment process, the TSF be able to disable the user account or the point of entry (e.g. workstation) from which the attempts were made until an administrator-defined condition occurs.

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of Authentication dependencies.

FIA_AFL.1.1 The TSF shall detect when *an administrator configurable positive integer within* [3] unsuccessful authentication attempts occur related to [user logon].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [*met*], the TSF shall [Captcha Validation].

6.1.3.5 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_MSA.1 (A)– Management of Security Attribute

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 The TSF shall enforce the [Administrative Access Control SFP] to restrict the ability to *[query, modify, delete]* the security attributes [user role, user ID, user tickets, and permissions assigned objects] to [SIEM GUI User].

6.1.4.2. FMT_MSA.1 (B)– Management of Security Attribute

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 The TSF shall enforce the [Information flow control SFP] to restrict the ability to *[start and stop]* the security attributes [query and responses] to [SIEM GUI User].

6.1.4.3. 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 The TSF shall enforce the [Administrative Access Control SFP] to provide *[permissive]* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [SIEM GUI User] to specify alternative initial values to override the default values when an object or information is created.

6.1.4.4. 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 The TSF shall enforce the [Information flow control SFP] to provide *[permissive]* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [SIEM GUI User] to specify alternative initial values to override the default values when an object or information is created.

6.1.4.5. FMT_MOF.1 – Management of Security Functions Behaviour

Description: Management of security functions behaviour allows the authorised users (roles) to manage the behaviour 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 [admin and authorized by admin].

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

6.1.4.6. 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].

6.1.4.7. 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 [SIEM GUI User and SIEM Base User].

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

6.1.4.8. 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 [SIEM GUI User].

6.1.5. Class TOE Access (FTA)

6.1.5.1. 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 logout or a specified time interval of user inactivity set by an authorized administrator. The default cookie session timeout value is 1 hour and it can be updated by user but, default session timeout value which is 20 minute can not updated].

6.1.6. Class Cryptographic Support (FCS)

6.1.6.1. 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. User's password data stored in encrypted form in the databse using 160 bit SHA_1 algorithms for the security reasons. Secure hash algoritm is performed using SHA_1 Managed algorithms in the Microsoft.System.Security.Cryptology library.

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 The TSF shall perform [Hash Operations] in accordance with a specified cryptographic algorithm [SHA_1] and cryptographic key sizes [none] that meet the following: [FIPS 180-2].

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

Description: Hash algorithms don't require cryptographic keys, hence no restriction has been made on assignments. FCS_CKM.4 component has not been added, since it is not definite that there will be a need for cryptographic keys. For the log protection in SIEM, log data stored in encrypted mode using SHA_1 Algorithm.

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_COP.1.1 The TSF shall perform [Hash Operations] in accordance with a specified cryptographic algorithm [SHA-1] and cryptographic key sizes [none] that meet the following: [FIPS 180-2].

6.2. 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 4 September 2012. These assurance requirements compose an Evaluation Assurance Level 3 (EAL 3). The assurance components are summarized in the following table:

Table 7: Assurance Components

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

6.3. Security Functional Requirements Rationale

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

Table 8 Coverage of Security Objectives by SFRs for TOE

Objective SFR	O.AUDREC	O.AUDREV	O.CORRDATA	O.DATASTOR	O.IDAUTH	O.RESACC	O.SECFUN
FAU_GEN.1	X						
FAU_GEN.2	X			X			
FAU_SAA.1				X			
FAU_SAR.1		X					
FAU_SAR.2	X		X	X			
FAU_STG.4				X			X
FAU_ARP.1	X					X	X
FDP_ACC.1						X	
FDP_ACF.1					X	X	
FDP_IFC.1			X	X			
FDP_IFF.1			X	X			
FDP_ITC.1			X	X		X	X
FDP_ETC.1			X			X	
FIA_ATD.1					X	X	
FIA_UAU.2					X	X	X
FIA_UID.2					X	X	
FIA_AFL.1					X		
FIA_SOS.1					X		
FMT_MSA.1(A)				X		X	X
FMT_MSA.3(A)						X	X
FMT_MSA.1(B)				X		X	X
FMT_MSA.3(B)						X	X
FMT_MOF.1							X
FMT_SMF.1							X
FMT_SMR.1						X	X
FMT_MTD.1						X	
FTA_SSL.3							X
FCS_COP.1 (A)				X	X	X	
FCS_COP.1 (B)			X	X			

Table 9: Justification about SFRs

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.AUDREC.
FAU_GEN.2	This component addresses the requirement of accountability of auditable events at the level of individual user identity. This component should be used in addition to FAU_GEN.1 Audit Data Generation. This component traces back to and aids in meeting the following objectives: O.AUDREC and O.DATASTOR.
FAU_SAA.1	This component 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 and traces back to and aids in meeting 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.AUDREV.
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.AUDREC, O.CORRDATA and O.DATASTOR.
FAU_STG.4	This requirement specifies actions in case the audit trail is full and prevents the audit data loss. The requirement also states that no matter how the requirement is instantiated, the authorised user with specific rights to this effect, can continue to generate audited events. This component traces back to and aids in meeting the following objectives: O.DATASTOR and O.SECFUN.
FAU_ARP.1	This requirement defines the response to be taken in case of detected events indicative of a potential security violation. An action should be taken for follow up action in the event of an alarm. This action can be to inform the authorised user, to present the authorised user with a set of possible containment actions, or to take corrective actions. This component traces back to and aids in meeting the following objectives: O.AUDREC, O.RESACC and O.SECFUN.
FDP_ACC.1	This requirement defines subjects, objects and operations controlled by the Natek Access Control Policy. 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.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 Administrative 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 allow authorized administrators (Super Admin) to specify which resources may be accessed by which users. This component traces back to and aids in meeting the following objectives: O.IDAUTH
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.CORRDATA and O.DATASTOR.
FDP_IFF.1	This component describes the rules for the specific functions that can implement the information flow control SFPs named in Information flow control policy. This component traces back to and aids in meeting the following objectives: O.CORRDATA and O.DATASTOR.
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.IDAUTH This component also identifies control access to resources based on the subject attribute of users. This component traces back to and aids in meeting the following objectives: O.RESACC
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 control 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.SECFUN
FIA_UID.2	This component requires successful identification of a role before having access to the TSF and such aids in meeting O.IDAUTH 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

FIA_AFL.1	This component contains requirements for defining values for some number of unsuccessful authentication attempts and TSF actions in cases of authentication attempt failures. This component traces back to and aids in meeting the following objectives: 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 objectives: O.IDAUTH
FMT_MSA.1(A)	This component restricts the ability to modify, delete, or query object and subject security attributes for the Administrative Access Control SFP to super admin. It also assists in effective management and such as aids in meeting O.DATASTOR and 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.
FMT_MSA.1(B)	This component restricts the ability to modify, delete, or query object and subject security attributes for the Administrative Access Control SFP to super admin. It also assists in effective management and such as aids in meeting O.DATASTOR and 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.
FMT_MSA.3(A)	This requirement allows authorised users control over the management of security attributes. This management might include capabilities for viewing and modifying of security attributes. This component traces back to and aids in meeting the following objectives: O.RESACC and O.SECFUN.
FMT_MSA.3(B)	This requirement allows authorised users control over the management of security attributes. This management might include capabilities for viewing and modifying of security attributes. This component traces back to and aids in meeting the following objectives: O.RESACC and O.SECFUN.
FMT_MOF.1	This component ensures that the TOE provides a default restrictive value for security attributes, yet allows a super admin to override the default values. This component traces back to and aids in meeting the following objectives: O.SECFUN.
FMT_SMF.1	This component was chosen to consolidate all TOE management, administration and security functions. This component traces back to and aids in meeting the following objectives: O.SECFUN
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 an authorized administrator. 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

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.
FTA_SSL.3	This component ensures that TOE terminates interactive session after specified time interval of user inactivity set by an authorized administrator. This component traces back to and aids in meeting the following objectives: O.SECFUN
FCS_COP.1 (A)	This requirement includes secure hash (message digest). This component traces back to and aids in meeting the following objectives O.IDAUTH, O.RESACC and O.DATASTOR.
FCS_COP.1 (B)	This requirement includes secure hash (message digest). This component traces back to and aids in meeting the following objectives: O.DATASTOR and O.CORRDATA.

6.2. Security Assurance Requirements Evidence

This section identifies the measures applied to satisfy CC assurance requirements.

Table 10 CC assurance requirements

ASSURANCE REQUIREMENTS	EVIDENCE
ASE_INT.1 Security Target Introduction	Security Target: Natek Security Information and Event Management SIEM GUI 2.0.2 with SIEM Server 6.2.0, SIEM Recorder 9.2.2 and SIEM Agent 6.1.0
ASE_CCL.1 Conformance Claim	Security Target: Natek Security Information and Event Management SIEM GUI 2.0.2 with SIEM Server 6.2.0, SIEM Recorder 9.2.2 and SIEM Agent 6.1.0
ASE_SPD.1 Security Problem Definition	Security Target: Natek Security Information and Event Management SIEM GUI 2.0.2 with SIEM Server 6.2.0, SIEM Recorder 9.2.2 and SIEM Agent 6.1.0
ASE_OBJ.1 Security Objectives	Security Target: Natek Security Information and Event Management SIEM GUI 2.0.2 with SIEM Server 6.2.0, SIEM Recorder 9.2.2 and SIEM Agent 6.1.0
ASE_REQ.2 Security Requirements	Security Target: Natek Security Information and Event Management SIEM GUI 2.0.2 with SIEM Server 6.2.0, SIEM Recorder 9.2.2 and SIEM Agent 6.1.0
ADV_ARC.1 Security architecture description	Security and Design Architecture: Natek Security Information and Event Management SIEM GUI 2.0.2 with SIEM Server 6.2.0, SIEM Recorder 9.2.2 and SIEM Agent 6.1.0
ADV_FSP.3 Functional specification with complete summary	Functional Specification: Natek Security Information and Event Management SIEM GUI 2.0.2 with SIEM Server 6.2.0, SIEM Recorder 9.2.2 and SIEM Agent 6.1.0
ADV_TDS.2 Architectural Design	Security and Design Architecture: Natek Security Information and Event Management SIEM GUI 2.0.2 with SIEM Server 6.2.0, SIEM Recorder 9.2.2 and SIEM Agent 6.1.0
AGD_OPE.1 Operational user guidance	Operational User Guide: Natek Security Information and Event Management SIEM GUI 2.0.2 with SIEM Server 6.2.0, SIEM Recorder 9.2.2 and SIEM Agent 6.1.0
AGD_PRE.1 Preparative procedures	Installation and Delivery: Natek Security Information and Event Management SIEM GUI 2.0.2 with SIEM Server 6.2.0, SIEM Recorder 9.2.2 and SIEM Agent 6.1.0

ALC_CMC.3 Authorization Control	Configuration Management: Natek Security Information and Event Management SIEM GUI 2.0.2 with SIEM Server 6.2.0, SIEM Recorder 9.2.2 and SIEM Agent 6.1.0
ALC_CMS.3 Implementation Representation CM coverage	Configuration Management: Natek Security Information and Event Management SIEM GUI 2.0.2 with SIEM Server 6.2.0, SIEM Recorder 9.2.2 and SIEM Agent 6.1.0
ALC_DEL.1 Delivery procedures	Installation and Delivery: Natek Security Information and Event Management SIEM GUI 2.0.2 with SIEM Server 6.2.0, SIEM Recorder 9.2.2 and SIEM Agent 6.1.0
ALC_DVS.1Identification of Security Measures	Development Environment Security: Natek Security Information and Event Management SIEM GUI 2.0.2 with SIEM Server 6.2.0, SIEM Recorder 9.2.2 and SIEM Agent 6.1.0
ALC_LCD.1 Developer defined life-Cycle model	Software Life-Cycle: Natek Security Information and Event Management SIEM GUI 2.0.2 with SIEM Server 6.2.0, SIEM Recorder 9.2.2 and SIEM Agent 6.1.0
ATE_COV.2 Analysis of Coverage	Testing Plan and Analysis: Natek Security Information and Event Management SIEM GUI 2.0.2 with SIEM Server 6.2.0, SIEM Recorder 9.2.2 and SIEM Agent 6.1.0
ATE_DPT.1 Testing: Basic Design	Testing Plan and Analysis: Natek Security Information and Event Management SIEM GUI 2.0.2 with SIEM Server 6.2.0, SIEM Recorder 9.2.2 and SIEM Agent 6.1.0
ATE_FUN.1 Functional Testing	Testing Plan and Analysis: Natek Security Information and Event Management SIEM GUI 2.0.2 with SIEM Server 6.2.0, SIEM Recorder 9.2.2 and SIEM Agent 6.1.0
AVA_VAN.1 Vulnerability Analysis	Vulnerability Tests: Natek Security Information and Event Management SIEM GUI 2.0.2 with SIEM Server 6.2.0, SIEM Recorder 9.2.2 and SIEM Agent 6.1.0

6.4. 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

7.1.1. Security Audit

The TOE generates a set of audit logs. These logs are stored on the database and administrator (SIEM GUI User) can also view them to a local machine.

The TOE generates Local Logs for the following list of events:

- All user of user identification and authentication mechanism, which includes the user identities provided to the TOE in each related log;
- All user database interactions logs like Create, Update, Delete Operations;
- All system Exception logs within any failure

The logs are only accessible through the Web-Based Administrative interface, which only authorized operators (SIEM GUI User) can access. When logs are saved from the TOE, they are transferred to the PC connected to the Web-Based Administrative interface.

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

- FAU_GEN.1: The TOE generates all the audit events identified in this requirement. Within each event is the information listed above which addresses all required details. The log which is generated by this security function also includes Time Stamp value.
- FAU_SAA.1: TOE defines requirements for automated means that analyse system activity and audit data looking for possible or real security violations.
- FAU_SAR.1: TOE provides ability to review logs.
- FAU_SAR.2: The TOE is required to restrict the review of audit data to those granted with explicit read-access.
- FAU_STG.4: TOE provides logs storage management capability.
- FAU_ARP.1: TOE provides ability to generate security alarms for the configured alerts on monitored devices.

7.1.2. User Data Protection

Natek SIEM determines access to the management functions for users identifying and authenticating to the TOE through the Natek SIEM GUI. Administrators are given access to functions based on their User ID, User Role, Group ID, Ticket ID, User's configured permissions, and Group's configured permissions. If the administrator's permissions match the permissions assigned to the object to which the administrator is attempting access, then that access is granted. Otherwise, it is denied. (Administrative Control SFP)

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

- FDP_ACC.1: This component ensures that the access control policies are enforced on all operations among subjects and objects in the Administrative Access Control SFP. Users are first authenticated via SSO component and after authentication every access to management operations are checked via this user. When an authenticated user tries to interact with a web GUI component, server side GUI component checks if the user has the privileges to view or edit the component. If the user has appropriate rights the action is accepted, if not an error is returned to the user. Either way after this interaction audit log is generated to record the event.
- FDP_ACF.1: This component ensures that permissions and privileges can be granted to specific subjects and objects for different accesses according to Administrative Access Control SFP. User permissions are defined in roles and attached to the users. Permissions is checked via looking to assigned role definitions to users.
- FDP_IFC.1: Information to be collected are defined by log collection policies and settings. Via log collection settings log collector component gets its running parameters including the destination and required credentials to gather the logs. With the running parameters taken from log collection settings log are collected accordingly. Collected logs are normalized, enriched and stored in the big data platform as defined in Log collection policies. Stored logs are gathered from the big data platform by server side GUI component to be shown to user that is requested. Record level Access control is applied when stored information is gathered from big data platform.

- FDP_IFF.1: For log collection there are functions to DROP, ALERT or STORE the collected log record. Drop is used to exclude records that matches a certain condition to be stored on the big data platform. Alert is used to trigger alarms when a certain type of log is collected. Store is used to define where the collected log is stored.
- FDP_ITC.1: This component is used to specify the import of user data that does not have reliable security attributes associated with it. Collected logs that contains user data is collected with related log collection settings and policies. According to settings and policies logs are normalized, enriched and stored as defined in FDP_IFF and FDP_IFC.
- FDP_ETC.1: Stored logs are gathered from the big data platform for viewing and exporting. Record level permissions are applied by serve side GUI component to satisfy user permissions. Gathered information does not contain security related attributes of users.

7.1.3. Identification and Authentication

The TOE performs identification and authentication of all users and administrators accessing the TOE. The TOE has the ability to authenticated users locally using a password or can integrate with a remote authentication server. Users enter a username and password, which is validated by the TOE against the user information stored by the database. If the authentication succeeds, the user receives a session token that is used for identification of subsequent requests during that session.

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

- FIA_ATD.1: For each registered user, the TOE stores the following information:
  - User Identity
  - User Name
  - User Roles
  - Password
- FIA_UAU.2: The TOE requires a valid password associated with a username before providing access to the TOE.
- FIA_UID.2: The TOE requires a username during the identification and authentication Process. The username is entered, then a password. If the password is valid, the user will be associated with a role and set of privileges based on the username.
- FIA_AFL.1: The session establishment process is the interaction with the user to perform the session establishment independent of the actual implementation. If the number of unsuccessful authentication attempts exceeds the indicated threshold (3 times), either the captcha will be shown.
- FIA_SOS.1: The TOE requires a strong password policy for user authentication and it should contain at least 8 characters long and include at least three of uppercase, lowercase, number and symbol.

7.1.4. Security Management

The TOE provides security management functions via browser interface. The Administrator logs on to the TOE perform all management functions through the browser interface. The administrator has the ability to control all aspects of the TOE configuration including:

- User Management
- Audit Management

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

- FMT_MSA.1(A): This component restricts the ability to modify, delete or query the subject and object security attributes for the Administrative Access Control SFP to the super admin role (SIEM GUI User).
- FMT_MSA.3 (A): TOE provides restrictive default values for security attributes specified in FDP_ACF.1.
- FMT_MSA.1 (B): This component restricts the ability to modify, delete or query the subject and object security attributes for the Information flow control SFP to the super admin role (SIEM GUI User).
- FMT_MSA.3 (B): TOE provides restrictive default values for security attributes specified in FDP_IFC.1.
- FMT_SMF.1: The TOE supports the following security management functions:
  - System and Service Start-up and Shutdown
  - Create, Delete, Modify and View user attribute values, which include a user's identity, association and authentication credentials.
  - Enable and Disable External IT entities from communicating to the TOE.
  - Review the Audit Records
  - Configure authorization rules
- FMT_SMR.1: The TOE supports the roles SIEM GUI User and SIEM Base User for limited administrator role user.
  - The SIEM GUI User role can perform all management functionalities. The administrator dynamically sets up user roles and access rules associated with the roles.
  - The SIEM Base User role can perform limited functionalities according to permitted authorization.

- FMT_MTD.1: This component allows users with a certain role to manage values of TSF data. The users are assigned to a role within the component FMT_SMR.1 Security roles.
- FMT_MOF.1: This component allows identified roles to manage the security functions of the TSF. This might entail obtaining the current status of a security function, disabling or enabling the security function, or modifying the behaviour of the security function.
- FTA_SSL.3: TOE terminates interactive session after specified time interval of user inactivity set by an authorized administrator. Default value is 1 hour.

7.1.5. Cryptographic Support

- 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 password protection in SIEM System.
- 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 log protection in SIEM System.