Certification Report

EAL 3 Evaluation of

NATEK Bilişim Bilgisayar Eğitim Danışmanlık Yazılım Ticaret Sanayi A.Ş.
SIEM GUI v2.0.2 with SIEM SERVER v6.2.0 and SIEM RECORDER v9.2.2 and SIEM AGENT v6.1.0

issued by

Turkish Standards Institution
Common Criteria Certification Scheme

Certificate Number: 21.0.03/TSE-CCCS-36

TABLE OF CONTENTS

Document Information

Date of Issue	01.09.2016
Approval Date	01.09.2016
Certification Report Number	21.0.03/16-005
Sponsor and Developer	NATEK Bilişim Bilgisayar Eğitim Danışmanlık Yazılım Ticaret Sanayi A.Ş.
Evaluation Facility	TÜBİTAK BİLGEM OKTEM
TOE	SIEM GUI v2.0.2 with SIEM SERVER v6.2.0 and SIEM RECORDER v9.2.2 and SIEM AGENT v6.1.0
Pages	17

Prepared by	Cem ERDİVAN
Reviewed by	İbrahim Halil KIRMIZI

This report has been prepared by the Certification Expert and reviewed by the Technical Responsible of which signatures are above.
Document Change Log

Release	**Date**	**Pages Affected**	**Remarks/Change Reference**
1.0	01.09.2016	All	First Release

DISCLAIMER

This certification report and the IT product defined in the associated Common Criteria document has been evaluated at an accredited and licensed evaluation facility conformance to Common Criteria for IT Security Evaluation, version 3.1, revision 4, using Common Methodology for IT Products Evaluation, version 3.1, revision 4. This certification report and the associated Common Criteria document apply only to the identified version and release of the product in its evaluated configuration. Evaluation has been conducted in accordance with the provisions of the CCCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report and its associated Common Criteria document are not an endorsement of the product by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document, and no warranty is given for the product by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document.

FOREWORD

The Certification Report is drawn up to submit the Certification Commission the results and evaluation information upon the completion of a Common Criteria evaluation service performed under the Common Criteria Certification Scheme. Certification Report covers all non-confidential security and technical information related with a Common Criteria evaluation which is made under the ITCD Common Criteria Certification Scheme. This report is issued publicly to and made available to all relevant parties for reference and use.

The Common Criteria Certification Scheme (CCSS) provides an evaluation and certification service to ensure the reliability of Information Security (IS) products. Evaluation and tests are conducted by a public or commercial Common Criteria Evaluation Facility (CCTL = Common Criteria Testing Laboratory) under CCCS' supervision.

CCEF is a facility, licensed as a result of inspections carried out by CCCS for performing tests and evaluations which will be the basis for Common Criteria certification. As a prerequisite for such certification, the CCEF has to fulfill the requirements of the standard ISO/IEC 17025 and should be accredited by accreditation bodies. The evaluation and tests related with the concerned product have been performed by TÜBİTAK BİLGEM OKTEM, which is a public CCTL.

A Common Criteria Certificate given to a product means that such product meets the security requirements defined in its security target document that has been approved by the CCCS. The Security Target document is where requirements defining the scope of evaluation and test activities are set forth. Along with this certification report, the user of the IT product should also review the security target document in order to understand any assumptions made in the course of evaluations, the environment where the IT product will run, security requirements of the IT product and the level of assurance provided by the product.

This certification report is associated with the Common Criteria Certificate issued by the CCCS for SIEM GUI v2.0.2 with SIEM SERVER v6.2.0 and SIEM RECORDER v9.2.2 and SIEM AGENT v6.1.0 whose evaluation was completed on 29.08.2016 and whose evaluation technical report was drawn up by TÜBİTAK BİLGEM OKTEM (as CCTL), and with the Security Target document with version no 1.12 of the relevant product.

The certification report, certificate of product evaluation and security target document are posted on the ITCD Certified Products List at bilisim.tse.org.tr portal and the Common Criteria Portal (the official web site of the Common Criteria Project).

RECOGNITION OF THE CERTIFICATE

The Common Criteria Recognition Arrangement logo is printed on the certificate to indicate that this certificate is issued in accordance with the provisions of the CCRA.

The CCRA has been signed by the Turkey in 2003 and provides mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL4. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

1 - EXECUTIVE SUMMARY

Natek SIEM (Security Information and Event Management) is a systemassociating 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 is 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.

1.1 TOE Overview

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 system 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.

1.2 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

1.3 Required non-TOE Hardware, Software or Firmware

The TOE is software product that runs on a host computer. The host computer must run the operating system platform on which the TOE can execute. 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;

❖ *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 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.

2 CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

Certificate Number	21.0.03/TSE-CCCS-36
TOE name and Version	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 Title	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
Security Target Version	1.12
Security Target Date	29.08.2016
Assurance Level	EAL 3
Criteria	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012 Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1 Revision 4, September 2012 Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2012-09-003, Version 3.1 Revision 4, September 2012
Methodology	Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012
Protection Profile Conformance	N/A
Common Criteria Conformance	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 4, September 2012 Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 4, September 2012, conformant Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1, Revision 4, September 2012, conformant
Sponsor and Developer	NATEK Bilişim Bilgisayar Eğitim Danışmanlık Yazılım Ticaret Sanayi A.Ş.
Evaluation Facility	TÜBİTAK BİLGEM OKTEM
Certification Scheme	TSE CCCS

2.2 Security Policy

The security policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

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.

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

2.3 Assumptions and Clarification of Scope

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.

There are two main OSPs defined for this TOE:

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 connection is also applied for communication between SIEM GUI and NASCMDB.

2.4 Architectural Information

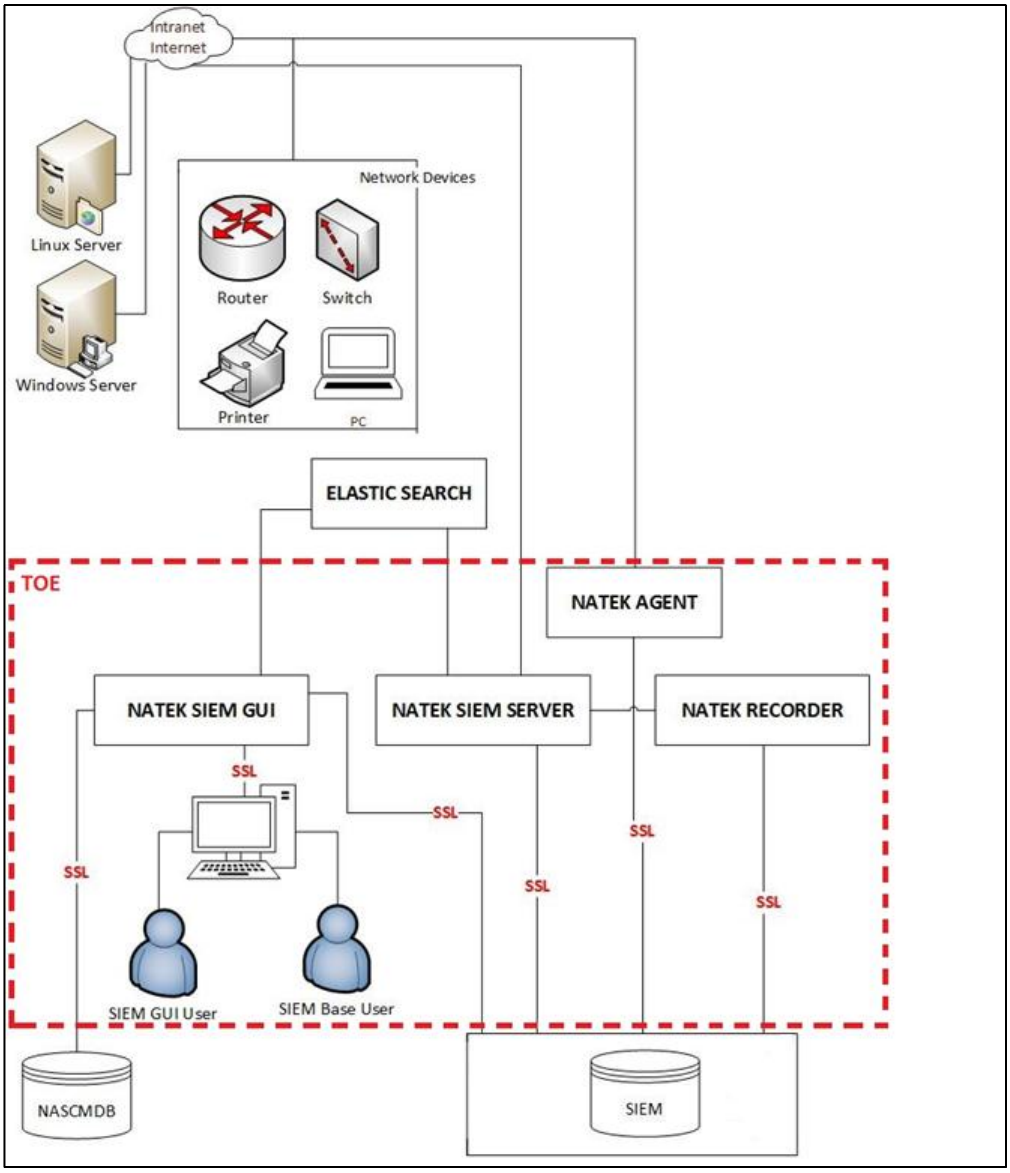

Figure 1 – Physical Scope of TOE

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 are 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 statistical 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 Correlation 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. Composite Count Correlation is similar to Count Correlation. Different from the Count Correlation in the Composite 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 occurrence average of these events. When the calculated value excesses th e 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 information 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.

2.5 Documentation

These documents listed below are provided to customer by the developer alongside the TOE:

Document Name	Version	Release Date
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	1.12	29.08.2016
SIEM User Manual	1.7	27.05.2016
SIEM Secure Installation and Delivery Manual	1.2	27.05.2016

2.6 IT Product Testing

During the evaluation, all evaluation evidences of TOE were delivered and transferred completely to CCTL by the developers. A ll the delivered evaluation evidences which include software, documents, etc. are mapped to the assurance families Common Criteria and Common Methodology; so the connections between the assurance families and the evaluation evidences has been established. The evaluation results are available in the final Evaluation Technical Report v2.0 of SIEM GUI v2.0.2 with SIEM SERVER v6.2.0 and SIEM RECORDER v9.2.2 and SIEM AGENT v6.1.0. It is concluded that the TOE supports EAL 3.

IT Product Testing is mainly realized in two parts:

1-Developer Testing: (7 Tests)

- TOE Test Coverage: Developer has prepared TOE Test Document according to the TOE Functional Specification documentation.
- TOE Test Depth: Developer has prepared TOE Test Document according to the TOE Design documentation which includes TSF subsystems and its interactions.
- TOE Functional Testing: Developer has made functional tests according to the test documentation. Test plans, test scenarios, expected test results and actual test results are in the test documentation.

2- Evaluator Testing:

- Independent Testing: The evaluator conducted 9 independent tests. All of them are related to TOE security functions.

- Penetration Testing: Evaluator has done 9 penetration tests to find out if TOE`s vulnerabilities can be used for malicious purposes:

  - XSS -Cross Site Scripting Test
  - Session Fixation Test
  - SQL Injection Test
  - HTML Injection Test
  - Bypass of Authentication Test
  - Unauthorized Transaction Test
  - Unauthorized Privilege Escalation Test
  - Application Logic Flaw, Business Logic Flaw Test
  - CSRF - Cross Site Request Forgery Test

2.7 Evaluated Configuration

Please refer to section 1-4 “Operating Environment for evaluated configuration”.

2.8 Results of the Evaluation

The verdict for the CC Part 3 assurance components (according to EAL3) are all pass and the security target evaluation is summarized in the following table:

ASSURANCE CLASS	ASSURANCE COMPONENTS	DESCRIPTION
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.3	Functional specification with complete summary
	ADV_TDS.2	Architectural Design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life-cycle support	ALC_CMC.3	Authorization Control
	ALC_CMS.3	Implementation representation CM coverage

	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
ASE: Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended component definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security Objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specifications
ATE: Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: Basic Design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
AVA: Vulnerability assessment	AVA_VAN.2	Vulnerability analysis

2.9 Evaluator Comments / Recommendations

No recommendations or comments have been communicated to CCCS by the evaluators related to the evaluation process of “SIEM GUI v2.0.2 with SIEM SERVER v6.2.0 and SIEM RECORDER v9.2.2 and SIEM AGENT v6.1.0” product, result of the evaluation, or the ETR.

3 SECURITY TARGET

The security target associated with this Certification Report is identified by the following terminology:
Title: 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
Date of Document: 29.08.2016

This Security Target describes the TOE, intended IT environment, security objectives, security requirements (for the TOE and IT environment), TOE security functions and all necessary rationale.

4 GLOSSARY

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

5 BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012

[2] Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012

[3] BTBD-03-01-TL-01 Certification Report Preparation Instructions, Rel. Date: February 8, 2016

[4] ETR v2.0 of SIEM GUI v2.0.2 with SIEM SERVER v6.2.0 and SIEM RECORDER v9.2.2 and SIEM AGENT v6.1.0, Rel. Date: 29.08.2016

[5] 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 v1.12 [ST] 29.08.2016