Certification Report

EAL4+ (ALC_FLR.1) Evaluation of

HAVELSAN Inc.

HAVELSAN GÖZCÜ v1.0.3

issued by

Turkish Standards Institution

Common Criteria Certification Scheme

Certificate Number: 21.0.03/TSE-CCCS-76

TABLE OF CONTENTS

Document Information

Date of Issue	*11.08.2021*
Approval Date	*13.08.2021*
Certification Report Number	*21.0.03/21-008*
Sponsor and Developer	*HAVELSAN A.Ş*
Evaluation Facility	*TÜBİTAK OKTEM*
TOE	*HAVELSAN GÖZCÜ v1.0.3*
Pages	15

Prepared by	*Halime Eda BİTLİSLİ 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	*11.08.2021*	*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 conformant to Common Criteria for IT Security Evaluation, *version 3.1, revision 5*, using Common Methodology for IT Products Evaluation, *version 3.1, revision 5*. 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.

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

CCTL 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 CCTL 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 OKTEM which is a commercial 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 *HAVELSAN GÖZCÜ v1.0.3* whose evaluation was completed on *03.08.2021* and whose evaluation technical report was drawn up by *03.08.2021* (as CCTL), and with the Security Target document with version no 1.16 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 EAL2. The current list of signatory nations and approved certification schemes can be found on:

http://www.commoncriteriaportal.org

1. EXECUTIVE SUMMARY

This report constitutes the certification results by the certification body on the evaluation results applied with requirements of the Common Criteria for Information Security Evaluation.

Evaluated IT product name: HAVELSAN GÖZCÜ

IT Product version: 1.0.3

Developer's Name: Havelsan Inc.

Name of CCTL: TÜBİTAK OKTEM

Assurance Package: EAL4+ (ALC_FLR.1)

Completion date of evaluation: 03.08.2021

1.1. Brief Description

TOE is a web application that manages a system that collects security and event logs from applications, products appliances of organizations. The collected logs then get correlated, achieved and timestamped. Working on these logs, the system creates near real time alerts and flexible reports. TOE visualizes collected logs, alerts and reports. Authorized users can define custom alerts and reports. TOE is capable of managing authorization. Unauthorized actions will be denied and logged as well as user interactions. Additionally, TOE provides configuration management interface, network topology visualization, archiving and supports high level REST API integration with third party applications.

1.2. Major Security Features

The following features are the major security functionality of the TOE;

- **Audit:** TOE will generate audit logs in order to provide accountability for the administrators and users.

- **Cryptographic Support:** TOE should provide hashing mechanisms for securely storing user passwords. No keys are required for this action.

- **Identification, Authentication and Authorization**: TOE will successfully identify, authenticate and authorize its users.

- **Data Protection**: TOE provides confidentiality and integrity of user and TSF data during import/export of data to/from third parties.

- **Security Management:** TOE will manage the security attributes and user roles.

1.3. Threats

T.UNAUTHORIZED_ACCESS: A malicious user may gain unauthorized access to the TOE and change the TOE configuration.

T.EAVES_DROPPING: Malicious Users could gain the valuable information (passwords and enterprise data) of authorized administrator by sniffing the traffic between waf and web application.

T.NO_ROUTE : A malicious user may cause the TOE to lose connection on the network layer to the source of its enforcement policies, adversely affecting data collection.

2. CERTIFICATION RESULTS

2.1. Identification of Target of Evaluation

Certificate Number	*21.0.03/TSE-CCCS-76*
TOE Name and Version	*HAVELSAN GÖZCÜ v1.0.3*
Security Target Title	HAVELSAN GÖZCÜ v1.0.3 Security Target
Security Target Version	*1.16*
Security Target Date	*08.07.2021*
Assurance Level	*EAL4+ (ALC_FLR.1)*
Criteria	• *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017* • *Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017* • *Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017*
Methodology	*Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2017-04-004, Version 3.1, Revision 5, April 2017*
Protection Profile Conformance	*None*
Sponsor and Developer	*HAVELSAN A.Ş*
Evaluation Facility	*TÜBİTAK OKTEM*
Certification Scheme	*TSE CCCS*

2.2. Security Policy

There are no Organizational Security Policies for the application.

2.3. Assumptions and Clarification of Scope

Assumptions for the operational environment of the TOE are;

A.ADMIN It is assumed that authorized administrator who is responsible to install, configure and operate the TOE and the IT entities in the operational environment of the TOE are experi-enced, trained and meet the security conditions.

A.PROTECT It is assumed that all hardware within the environment, including network and pe-ripheral devices, has been approved for the transmitting of secure data. Each of these appliance configurations is securely managed by administrators to provide protection of secured data in terms of its confidentiality and integrity.

A.NO_GENERAL_PURPOSE It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.

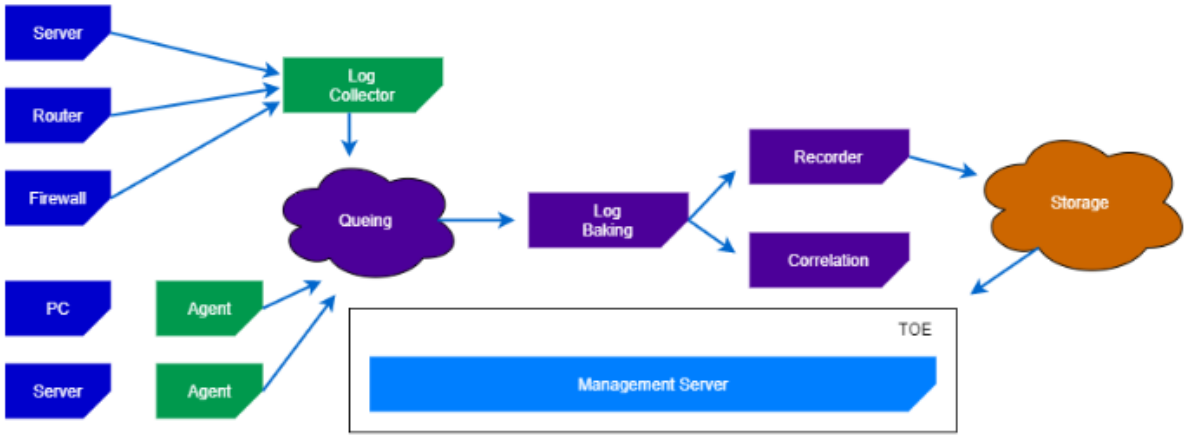
A.PHYSICAL Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.

A.TIME_SERVER It is assumed that trusted time server provides reliable time information.

2.4. Architectural Information

TOE consists of GUI (Graphical User Interface) and the back-end functionalities in a single application. TOE is supplied as a software product installed on Linux-based platforms. TOE will be evaluated PC platform under the following Linux operating systems: Ubuntu 14.04, Ubuntu 16.04, Ubuntu 18.04.

Additionally, TOE will be installed on client workstation and client will be required to connect log sources to TOE.



2.5. Documentation

Documents below are provided to the customer by the developer alongside the TOE;

Name of Document	Version Number	Date
HAVELSAN GÖZCÜ v1.0.3 OPE Operational User Manual	*1.12*	*02.02.2021*
HAVELSAN GÖZCÜ v1.0.3 Installation Procedure	*1.9*	*02.02.2021*
HAVELSAN GÖZCÜ v1.0.3 Security Target	*1.16*	*08.07.2021*

2.6. IT Product Testing

During the evaluation, all evaluation evidences of TOE were delivered and transferred completely to CCTL by the developer. All 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 (ETR) of Havelsan Gözcü v1.0.3.

It is concluded that TOE supports EAL4+ (ALC_FLR.1). IT Product Testing is composed of two parts:

2.6.1. Developer Testing

Developer has prepared TOE Test Document according to the TOE Functional Specification documentation, TOE Design documentation which includes TSF subsystems and its interactions. Developer has conducted 45 functional tests in total.

2.6.2. Evaluator Testing

- Independent Testing: Evaluator has conducted 5 tests of developer and also has prepared 13 independent tests. TOE has passed all functional tests to demonstrate that its security functions work as it is defined in the ST.

- Penetration Testing: Evaluator has conducted 11 penetration tests to find out TOE's vulnerabilities that can be used for malicious purposes.

2.7. Evaluated Configuration

TOE is a web application that is responsible for SIEM management. Toe is reached from web browser. In order to use the product, the following modules must be installed.

GÖZCÜ/agent

GÖZCÜ/management

GÖZCÜ/data-engine/log-collector-without-flink

GÖZCÜ/data-engine/log-formatter-without-flink

GÖZCÜ/data-engine/log-correlator

The evaluator has performed an installation and configuration of the TOE using the information provided in the preparation manual and the operational manual. Also evaluator satisfied the security objectives for the operational environment described in the security target.

The TOE configuration used to execute the independent tests is consistent with the evaluated configuration according to security target.

2.8. Results of the Evaluation

Table below provides a complete listing of the Security Assurance Requirements for the TOE. These requirements consist of the Evaluation Assurance Level 4 (EAL 4) components as specified in Part 3 of the Common Criteria, augmented with ALC_FLR.1.

Assurance Class	**Component**	**Component Title**
Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.4	Complete functional specificationw
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic Modular Design
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
Life-Cycle Support	ALC_CMC.4	Production Support, Acceptance Procedures and automation
	ALC_CMS.4	Problem Tracking CM Coverage
	ALC_DEL.1	Delivery Procedures
	ALC_DVS.1	Sufficiency of Security Measures
	ALC_LCD.1	Developer Defined Life-Cycle Model
	ALC_TAT.1	Well-Defined Development Tools
	ALC_FLR.1	Basic Flaw Remediation
Security Target Evaluation	ASE_CCL.1	Conformance Claims
	ASE_ECD.1	Extended Components Definition
	ASE_INT.1	ST Introduction
	ASE_OBJ.2	Security Objectives
	ASE_REQ.2	Derived Security Requirements

	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE Summary Specification
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing
Vulnerability Analysis	AVA_VAN.3	Focused vulnerability analysis

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 4+ (ALC_FLR.1) assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer about the issues requiring resolution or clarification within the evaluation evidence. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. So for TOE "Havelsan Gözcü V1.0.3", the results of the assessment of all evaluation tasks are "Pass".

2.9. Evaluator Comments / Recommendations

No recommendations have been communicated to CCCS by the evaluators related to the evaluation process of ""Havelsan Gözcü V1.0.3" 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: HAVELSAN GÖZCÜ v1.0.3 Security Target

Version: 1.16

Date of Document: 08.07.2021

4. GLOSSARY

ADV : Assurance of Development

AGD : Assurance of Guidance Documents

ALC : Assurance of Life Cycle

ASE : Assurance of Security Target Evaluation

ATE : Assurance of Tests Evaluation

AVA : Assurance of Vulnerability Analysis

CC : Common Criteria (Ortak Kriterler)

CCCS : Common Criteria Certification Scheme (TSE)

CCRA : Common Criteria Recognition Arrangement

CCTL : Common Criteria Test Laboratory

CEM :Common Evaluation Methodology

CMC : Configuration Management Capability

CMS : Configuration Management Scope

DEL : Delivery

DVS : Development Security

EAL : Evaluation Assurance Level

OPE : Opretaional User Guidance

OSP : Organisational Security Policy

PP : Protection Profile

SAR : Security Assurance Requirements

SF : Security Function

SFP : Security Function Policy

SFR : Security Functional Requirements

TOE : Target of Evaluation

TSF : TOE Secırity Functionality

TSFI : TSF Interface

5. BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017,

[2] Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 5, April 2017

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

6. ANNEXES

There is no additional information to this report.