Certification Report

EAL 3 Evaluation of

May Siber Teknoloji Bilişim Bilgisayar Eğitim Danışmanlık Yazilim Ticaret Sanayi Anonim Şirketi

scopSOC v2

issued by

Turkish Standards Institution

Common Criteria Certification Scheme

Certificate Number: 21.0.03/TSE-CCCS-70

TABLE OF CONTENTS

Document Information

Date of Issue	*19.02.2021*
Approval Date	*23.02.2021*
Certification Report Number	*21.0.03/21-002*
Sponsor and Developer	*May Siber Teknoloji Bilişim Bilgisayar Eğitim Danışmanlık Yazilim Ticaret Sanayi Anonim Şirketi*
Evaluation Facility	*STM ITSEF*
TOE	*scopSOC v2*
Pages	*18*

Prepared by	*İbrahim Halil KIRMIZI*	
Reviewed by	*Halime Eda BİTLİSLİ ERDİVAN*	

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	*19.02.2021*	*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 *STM ITSEF*, which is a public/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 *scopSOC v2* whose evaluation was completed on *02.02.2021* and with the Security Target document with version no *1.8* 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: *scopSOC*

IT Product version: *v2*

Developer's Name: *May Siber Teknoloji Bilişim Bilgisayar Eğitim Danışmanlık Yazilim Ticaret Sanayi Anonim Şirketi*

Name of CCTL: *STM ITSEF*

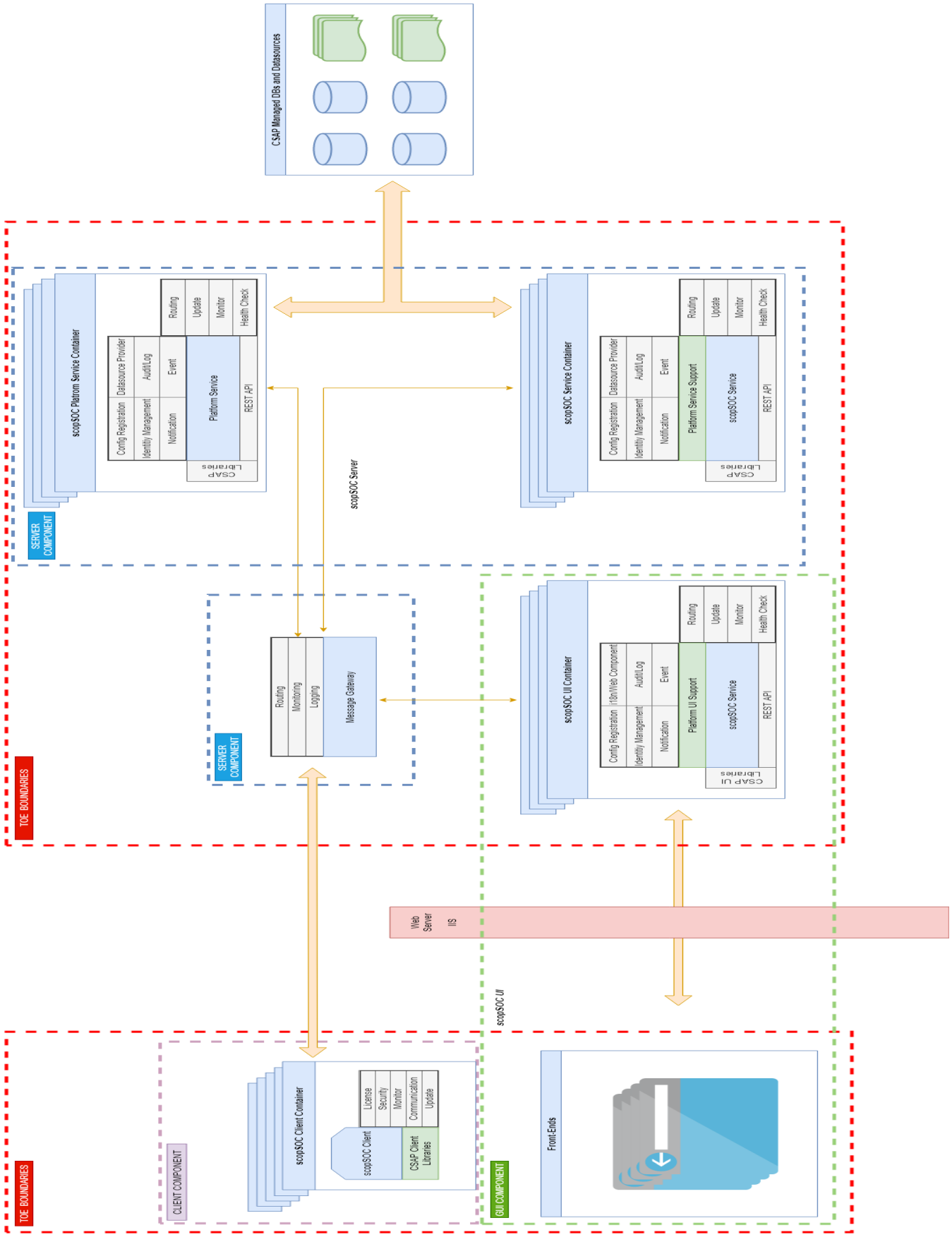
Assurance Package: *EAL 3*

Completion date of evaluation: *02.02.2021*

1.1. Brief Description

The TOE is a platform that integrate SIEM solution (scopVISION), endpoint security, incident management (scopDESK), monitoring (scopMON), asset discovery, vulnerability scanning and threat analysis. TOE provide centralized management for organizations wishing to implement a comprehensive Security Operation Center by including these components.

The TOE boundaries are illustrated with the red dotted lines at the image figure below.


CSAP Managed DBs and Datasources
scopSOC Platrom Service Container
Routing
Update
Monitor
Health Check
Config Registration
Datasource Provider
AuditLog
Event
Identity Management
Notification
Platform Service
REST API
CSAP Libraries
scopSOC Server
scopSOC Service Container
Platform Service Support
scopSOC Service
SERVER COMPONENT
Routing
Monitoring
Logging
Message Gateway
scopSOC UI Container
I18n/Web Component
Platform UI Support
CSAP UI Libraries
TOE BOUNDARIES
Web Server
IIS
scopSOC UI
scopSOC Client Container
License
Security
Monitor
Communication
Update
scopSOC Client
CSAP Client Libraries
CLIENT COMPONENT
GUI COMPONENT
Front-Ends

1.2. Major Security Features

The TOE provides the following security services;

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

1.3. Threats

The threats are;

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

- **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

- **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

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

2. CERTIFICATION RESULTS

2.1. Identification of Target of Evaluation

Certificate Number	*21.0.03/TSE-CCCS-70*
TOE Name and Version	*scopSOC v2*
Security Target Title	*scopSOC v2 Security Target*
Security Target Version	*1.8*
Security Target Date	*14.01.2021*
Assurance Level	*EAL 3*
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	*May Siber Teknoloji Bilişim Bilgisayar Eğitim Danışmanlık Yazilim Ticaret Sanayi Anonim Şirketi*
Evaluation Facility	*STM ITSEF*
Certification Scheme	*TSE CCCS*

2.2. Security Policy

There is one Organisational Security Policy presented at the Security Target;

- **OSP.Secure Transfer:** Operational environment will provide a secure channel so that credentials are protected between the scopSOC Server and scopSOC GUI application. SSL (Secure Socket Layer) which are cryptographic protocols designed to provide communications security over a computer network, is used for communication between scopSOC Users and scopSOC GUI. It provides “HTTPS” connection. As well as, SSL communication is used for communication between scopSOC Server and scopSOC Client

2.3. Assumptions and Clarification of Scope

Assumptions for the operational environment of the TOE are;

- **A.ACCESS DATA – A.ACCDATA:** The TOE has access to all the IT System data it needs to perform its functions
- **A.NO EVIL USER – A.NOEVIL:** Super User and user authorized by Super User, who manage the TOE are non-hostile use, configure and maintain the TOE and follow all guidance
- **A.EDUCATED USER – A.EDUCUSER:** Super User and user authorized by Super User and end users are educated so as to use the scopSOC system suitably and correctly. The Administrator will install and configure the TOE according to the management guide
- **A.PHYSICAL ACCESS AND PROTECTION – A.PYHPROT:** The TOE resides in a physically controlled access facility that prevents unauthorized physical Access. Therefore, the physical hardware and software in which the TOE is deployed will be protected from unauthorized physical modification
- **A.SECURE ENVIRONMENT – A.SECENV:** The Operating Systems, Database, Application and Web Server, on which the TOE is running are, fixed against all security bugs and protected against all threats

2.4. Architectural Information

TOE consists of three main components; scopSOC GUI, scopSOC Server and scopSOC Client.

2.5. Documentation

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

Name of Document	Version Number	Date
scopSOC v2 Security Target	*V1.8*	*14.01.2021*
scopSOC Administration Guide	*V1.0*	*10.12.2019*

scopSOC Install and Upgrade Guide	*V1.1*	*16.12.2019*

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 scopSOC v2.

It is concluded that the TOE supports EAL 3. There are 22 assurance families which are all evaluated with the methods detailed in the ETR.

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. All SFR-Enforcing TSFIs have been tested by developer. Developer has conducted 141 functional tests in total.

2.6.2. Evaluator Testing

- Independent Testing: Evaluator has chosen 15 developer tests to conduct by itself. Additionally, evaluator has prepared 5 independent tests. TOE has passed all 20 functional tests to demonstrate that its security functions work as it is defined in the ST.

- Penetration Testing: TOE has been tested against common threats and other threats surfaced by vulnerability analysis. As a result, 10 penetration tests have been conducted.

2.7. Evaluated Configuration

The evaluated TOE configuration is composed of;

- scopSOC v2,
- Guidance Documents

Also as consistent with the minimum Hardware/Software/OS requirements for the TOE, the test environment presented at the ETR is composed of;

- scopSOC GUI;

  .NET Framework 4.8

  MSSQL Server 2008 R2

  Windows 2012 R2

- scopSOC Server;

  .NET Framework 4.8

  MSSQL Server 2008 R2

  Windows 2012 R2

  Elasticsearch 7.5

- scopSOC Client

  .NET Framework 3.5

  MSSQL Server 2008 R2

  Windows 2012 R2

2.8. Results of the Evaluation

The table below provides a complete listing of the Security Assurance Requirements for the TOE. These requirements consists of the Evaluation Assurance Level 3 (EAL 3) components as specified in Part 3 of the Common Criteria.

Assurance Class	**Component**	**Component Title**
Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.3	Functional Specification with Complete Summary
	ADV_TDS.2	Architectural Design
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
Life-Cycle Support	ALC_CMC.3	Authorisation controls
	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
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 - sample
Vulnerability Analysis	AVA_VAN.2	Vulnerability analysis

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 3 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 “scopSOC v2”, the results of the assessment of all evaluation tasks are “Pass”.

2.9. Comments / Recommendations

It is recommended that all guidance outlined in the Guidance Documents be followed and all assumptions are fulfilled in order to the secure usage of the TOE.

3. SECURITY TARGET

The Security Target associated with this Certification Report is identified by the following terminology:

Title: *scopSOC v2 Security Target*

Version: *1.8*

Date of Document: *14.01.2021*

A public version has been created and verified according to ST-Santizing:

Title: scopSOC V2 Security Target Lite

Version: 1.1

Date of Document: 17.02.2021

4. GLOSSARY

CCCS: Common Criteria Certification Scheme

CCMB: Common Criteria Management Board

ITCD: Information Technologies Test and Certification Department

EAL : Evaluation Assurance Level

OSP : Organisational Security Policy

SAR : Security Assurance Requirements

SFR : Security Functional Requirements

SOC: Security Operation Center

ST : Security Target

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] Evaluation Technical Report for scopSOC v1.0, February 2nd 2021

6. ANNEXES

There is no additional information which is inappropriate for reference in other sections