الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

C003 Certification Report

[CB-4-RPT-QCCS]-C003

BREACH+ v2.0

Report

National Cyber Security Agency

06.08.2024

v1.1

Public

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

Document Authorization

This page detail may intentionally be removed or hidden when publicly published or shared

FOREWORD

The Qatar Common Criteria Scheme (QCCS) Certification Body (CB) has been established to increase Qatar's competitiveness in quality assurance of information security based on the Common Criteria (CC) standard and to build consumers' confidence towards Qatar information security products.

The QCCS is operated by National Cyber Security Agency (NCSA) and provides a model for licensed Evaluation Bodies (or Evaluation Security Facility) to conduct security evaluations of ICT products, systems and protection profiles against internationally recognized standards. The results of these evaluations are certified by Qatar Common Criteria Scheme Unit, a unit established within National Cyber Security Agency, NCSA.

By awarding a Common Criteria certificate, the QCCS CB asserts that the product complies with the security requirements specified in the associated Security Target. A Security Target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the Security Target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation; Certificate ID: QCCS-CERT-C003-001-2024, and the Security Target [Ref (5)]. The certification report, Certificate of product evaluation and security target are posted on the Scheme website and the Common Criteria Portal (the official website of the Common Criteria Recognition Arrangement).

DISCLAIMER / LEGAL RIGHTS

National Cyber Security Agency (NCSA) has designed and created this publication, titled "C003 Certification Report" - v1.1 - Public, product name Breach+, v2.0, as the outcome of evaluation and certification under the Qatar Common Criteria Scheme Certification Body.

QCCS CB is responsible for the review and maintenance of this document.

Any reproduction of the present document either in part or full and irrespective of the means of reproduction; shall acknowledge QCCS CB and NCSA as the source and owner of the "Certification Report".

Any reproduction concerning this document with intent of commercialization shall seek a written authorization from the QCCS CB and NCSA. QCCS CB and NCSA shall reserve the right to assess the functionality and applicability of all such reproductions developed for commercial intent.

The authorization from QCCS CB and NCSA shall not be construed as an endorsement of the developed reproduction and the developer shall in no way publicize or misinterpret this in any form of media or personal / social discussions.

The Information Technology (IT) product identified in this certification report and its associate certificate has been evaluated at an accredited and licensed evaluation facility established under the Qatar Common Criteria Scheme (QCCS) using the Common Methodology for IT Security Evaluation, version 3.1 revision 5 [Ref (3)], for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 5 [Ref(2)]

This certification report and its associated certificate apply only to the specific version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the Qatar Common Criteria Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certification report and its associated certificate is not an endorsement of the IT product by NCSA or by any other organization that recognizes or gives effect to this certification report and its associated certificate, and no warranty of the IT product by NCSA or by any other organization that recognizes or gives effect to this certificate, is either expressed or implied.

LEGAL MANDATE(S)

Article 18 of the Emiri Decree no (4) for the Year 2016 setting the mandate of Ministry of Transport and Communications (was referred as "MOTC") provided that MOTC had the authority to regulate and develop the sector of Information and Communications Technology in the State of Qatar in a manner consistent with the requirements of national development goals, with the objectives to create an environment suitable for fair competition, support the development and stimulate investment in these sectors; to secure and raise efficiency of information and technological infrastructure; to implement and supervise e-government programs; and to promote community awareness of the importance of ICT to improve individual's life and community and build knowledge-based society and digital economy.

Based on Cabinet decision (26) for the year 2018, the Compliance & Data Protection Department (was referred as CDP) was entrusted by the Ministry of Transport and Communications (MOTC) as the competent authority, responsible for determining, in the public interest, the technical competence and integrity of organizations such as those offering assessments, testing and compliance services and the Issuance of Certifications those seeking certificates of compliance within the State of Qatar. In 2021, the National Cyber Security Agency (NCSA) has taken over the role as the competent authority and assumed responsibility from MOTC since.

This Report has been prepared to take into consideration the current applicable laws of the State of Qatar. If a conflict arises between this document and the laws of Qatar, the latter shall take precedence. Any such term shall, to that extent be omitted from this Document, and the rest of the document shall stand without affecting the remaining provisions. Amendments, in that case, shall then be required to ensure compliance with the relevant applicable laws of the State of Qatar.

Executive Summary

BREACH+, v2.0 from Cytomate Solutions and Services is the Target of Evaluation (TOE). The TOE is defined as a system that includes both a website for user control and a special software agent that performs automatic security checks.

Breach+ is helpful for organizations wanting to make sure their defenses are strong. It checks how well security controls work by saving public exploits and executing new attack paths in a safe environment. It goes through the whole process of a cyberattack, mimicking a real attacker to check if security rules and protections hold up.

In addition to its primary functions, Breach+ provides detailed insights into potential vulnerabilities and strengths in security setups. By simulating real-world cyber threats, it helps users understand their system's weaknesses and where to strengthen them. With Breach+, users can stay one step ahead in the ongoing battle against cyber threats, ensuring their systems are well-protected and resilient against potential attacks.

The TOE provides the following main security functionality:

- Security audit
- Protection of Security Functionality
- User Data Protection
- Identification and Authentication
- Security Management
- TOE Access

The evaluation was performed by BEAM Teknoloji A.Ş. and completed by Evaluation Technical Report [Ref (6)] submission on 8th July 2024. The results documented in the evaluation technical report Evaluation Technical Report [Ref (6)] for this product provide sufficient evidence that the TOE meets the EAL1 assurance requirements for the evaluated security functionality.

This report confirms that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Qatar Common Criteria Scheme requirements [Ref (4)]. The Qatar Common Criteria Certification Body (QCCS CB) declares that the TOE evaluation meets all the Arrangements on the Recognition of Common Criteria certificates [Ref (1)].

The scope of the evaluation is defined by the Security Target [Ref (5)], which identifies assumptions made during the evaluation, the intended environment for the BREACH+, V.2.0, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements.

The Security Target [Ref (5)] includes Security Functional Requirements (SFR's), but does not claim conformance with any protection profile. It is the responsibility of user to ensure that the TOE meet their requirements. It is recommended that a potential user of the TOE to refer to the Security Target [Ref (5)] and this Certification Report prior to deciding whether to purchase the product. Note that the certification results apply only to the specific version of the product as evaluated.

Table of Contents

1 Introduction

1.1 TOE Description

The TOE is BREACH+, v2.0 detailed in section 1.2, Table 1 of this document.

The TOE is defined as a system that includes both a website for user control and a special software agent that performs automatic security checks. It checks how well security controls work by saving public exploits and executing new attack paths in a safe environment . It goes through the whole process of a cyberattack, mimicking a real attacker to check if security rules and protections hold up.

Breach+ is helpful for organizations (hereafter also referred as Consumer/User) wanting to make sure their defenses are strong. In addition to its primary functions, Breach+ provides detailed insights into potential vulnerabilities and strengths in security setups. By simulating real-world cyber threats, it helps users of the organization understand their system's weaknesses and where to strengthen them. With Breach+, users can stay one step ahead in the ongoing battle against cyber threats, ensuring their systems are well-protected and resilient against potential attacks.

The TOE provides the following main security functionality:

- Security audit
- Protection of Security Functionality
- User Data Protection
- Identification and Authentication
- Security Management
- TOE Access

Following are the non-TOE operational requirements:

- Endpoint Server
- Database
- All Kubernetes jobs

For more information on security functionality and the method of use of the TOE refer to the Security Target [Ref (5)], section 1.3.2.

The TOE comprises components as stated in the TOE Architecture section 1.4 of this document.

1.2 TOE Identification

The details of the TOE are identified in Table 1 below.

Table 1: TOE identification

Certification Scheme	Qatar Common Criteria Scheme
Project Identifier	C003
TOE Name	BREACH+ v2.0
TOE Version	v2.0
Security Target Title	Security-Target-(ST)-V.1.4-Breach+
Security Target Version	1.4
Security Target Date	16.07.2024
Assurance Level	Evaluation Assurance Level 1
Criteria	Common Criteria for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 [Ref (2)]
Methodology	Common Evaluation Methodology for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 [Ref (3)]
Protection Profile Conformance	none
Common Criteria Conformance	CC Part 1 CC Part 2 Conformant CC Part 3 Conformant
Sponsor and Developer	Cytomate Solutions and Services
Evaluation Facility	BEAM Teknoloji A.Ş. ODTÜ Teknokent Galyum Binası ZK-1 Çankaya/ANKARA

1.3 Security Policy

The Security Policy is expressed by the set of Security Functional Requirements (SFRs) and implemented by the TOE. It covers the following issues: Security Audit, Protection of Security Functionality, User Data Protection, Identification and authentication, Security Management, TOE access.

1.4 TOE Architecture

The TOE consists of two subsystems identified as follows:

- Web Portal
- Agent

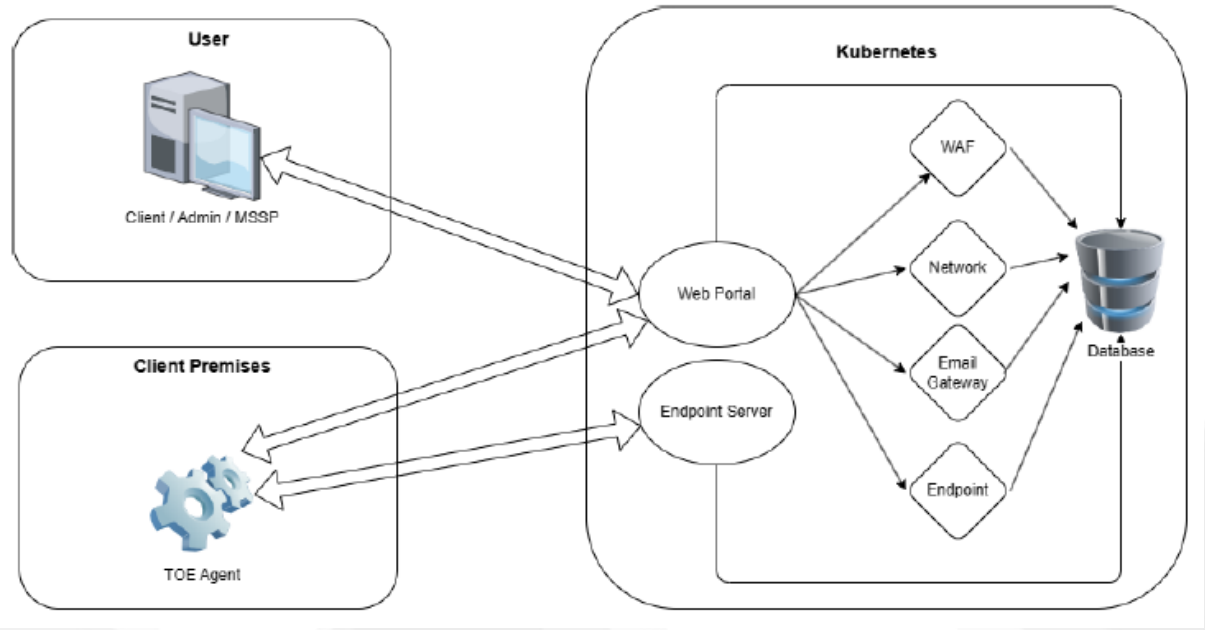

Figure 1: Architecture and boundaries of the TOE

1.4.1 Logical and Physical Boundaries

The logical and physical boundaries of the TOE can be defined by the functionality it provides and the sensor part of the TOE as stated in Security Target [Ref (5)] section 1.3.1 and 1.3.2.

1.5 Assumptions and Clarification of Scope

This section summarizes the security aspects of the environment and configuration in which IT product is intended to operate. Consumers should understand their own IT environments and that required for secure operation of the TOE which has defined in the Security Target [Ref (5)].

The Threats, Organizational Security Policy and Assumptions have not been defined in the Security Target since this is an EAL 1 evaluation.

For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 3.1 of the Security Target [Ref (5)].

1.6 Evaluated Configuration

The TOE is defined uniquely by its name and version number BREACH+, v2.0.

1.7 Delivery Procedures

Delivery method is described as “portal is accessible through TOE URL” and “Clients can download the agent directly from the website. There is no need to physically handover the TOE to clients.

1.8 Documentation

It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage of the product.

The following documentation is provided by the developer to the end user as guidance to ensure secure delivery, installation and operation of the product:

Type	Delivery Item	Version
Product Guidance (General)	Guidance Document	0.9

2 Evaluation

The evaluation was conducted in accordance with the requirements of the Common Criteria, version 3.1 Revision 5 [Ref (3)] and the Common Methodology for IT Security Evaluation (CEM), version 3.1 Revision 5 [Ref (3)]. The evaluation was conducted at Evaluation Assurance Level (EAL) stated in section 1.2 of this document. The Evaluation Body (EB) have performed the evaluation steps following to the scheme requirement [Ref (4)].

2.1 Evaluation Analysis Activities

The evaluation activities involved a structured evaluation of the TOE, including the following components:

2.1.1 Life-cycle support

An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the configuration items were clearly and uniquely

labelled, and access control measures as described in the configuration management documentation are effective in preventing unauthorized access to the configuration items. The developer's configuration management system was evaluated, and it was found to be consistent with the provided evidence.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the TOE during distribution to the consumer.

2.1.2 Development

The evaluators analyzed the TOE functional specification; they determined that the design completely and accurately describes the TOE security functionality interfaces (TSFIs), and how the TSF implements security functional requirements (SFRs).

The evaluators examined the TOE design specification; they determined that the structure of the entire TOE is described in terms of subsystems. They also determined that it provides a complete, accurate, and high-level description of the SFR-enforcing behavior of the SFR-enforcing subsystems.

The evaluators examined the TOE security architecture description; they determined that the information provided in the evidence is presented at a level of detail commensurate with the descriptions of the SFR-enforcing abstractions contained in the functional specification and TOE design.

2.1.3 Guidance documents

The evaluators examined the TOE preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously described how to securely transform the TOE into its evaluated configuration, and how to use and administer the product in order to fulfil the security objectives for the operational environment. The evaluators examined and tested the preparative and operational guidance and determined that they were complete and sufficiently detailed to result in a secure configuration.

2.1.4 IT Product Testing

All developer tests in the context of the evaluation were conducted using the final version of the TOE.

Overall, the developer tested the TOE systematically at the level of TSFI as given in the Functional Specification. The developer thereby followed the strategy to cover all TSFI.

All tests were passed successfully.

2.1.4.1 Independent Functional Testing

All evaluator tests in the context of the evaluation were conducted using the final version of the TOE. The evaluator examined the functions defined in the Security Target document and the interface behaviors and error messages defined in the FSP document. After, independent tests were added to test all aforementioned functionalities. There were 19 independent test scenarios written so that all interfaces defined in the FSP document and functions defined in the Security Target document are tested.

All tests were passed successfully.

2.1.4.2 Penetration Testing

The evaluators performed a vulnerability analysis of the TOE in order to identify potential vulnerabilities in the TOE. This vulnerability analysis considered public domain sources and an analysis of guidance documentation, functional specification, TOE design, and security architecture description.

From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE is resistant to attacks performed by an attacker possessing a basic attack potential. The following factors have been taken into consideration during penetration tests:

- Time taken to identify and exploit (elapsed time);
- Specialist technical expertise required (specialized expertise);
- Knowledge of the TOE design and operation (knowledge of the TOE);
- Window of opportunity; and
- IT hardware/software or other requirement for exploitation

The evaluators' search for vulnerabilities also considered public domain sources for published vulnerability data related to the TOE and the contents of all TOE deliverables. The following public domain sources were searched during the evaluation:

- OWASP TOP 10
- WASC

The penetration tests focused on:

- Bypassing
- Tampering
- Direct Attacks
- Monitoring
- Web Attacks

2.1.4.3 Testing Results

Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in its Security Target and its functional specification. The TOE passed all developer and EB tests.

3 Result of the Evaluation

After due consideration during the oversight of the execution of the evaluation and submission of the Evaluation Technical Report [Ref (6)], the Qatar Common Criteria Scheme Certification Body (QCCS CB) certifies the evaluation of Breach+, v2.0 performed by BEAM Teknoloji A.Ş.

The EB found that the TOE upholds the claims made in the Security Target [Ref (5)] and supporting documentations and has met the requirements of the Common Criteria (CC) assurance level as stated in Table 1, section 1.2 of this document.

Certification does not guarantee that a TOE is completely free of exploitable vulnerabilities. There will remain a small level of risk that exploitable vulnerabilities remain undiscovered in its claimed security functionality. The risk is reduced as the certified level of assurance or EAL increases for the TOE.

3.1 Assurance Level Information

The TOE claims to be conformant to an assurance package based on EAL 1. All of the SARs in Security Target [Ref (5)], section 5.2 has been found taken directly from [CC part 3] [Ref (2)].

The assurance level also provides assurance by a full security target and analysis of the SFRs in that Security Target, using a functional and interface specification, guidance documentation, and a basic description of the architecture of the TOE, to understand the security behavior.

The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.

The assurance level also provides assurance through the use of a configuration management system.

3.2 Recommendation

The consumer of the product shall consider the results of the certification within their system risk management process. In order for the evolution of attack methods and techniques to be

covered, the period of time until a re-assessment of the TOE is required should be defined and thus requested from the sponsor of the certificate.

If available, certified updates of the TOE should be used. If non-certified updates or patches are available, the user of the TOE should request the sponsor to provide a recertification. In the meantime, a risk management process of the system using the TOE should investigate and decide on the usage of not yet certified updates and patches or take additional measures in order to maintain system security. The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation.

4 References

All CB references are listed in [CB-2-LST-DocRefList] Documentation Control Reference List.

[1] Arrangement on the recognition of Common Criteria Certificates in the field of Information Technology Security, July 2, 2014 – Ratified September 8, 2014.

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

Part 1: Introduction and general model, Revision 5, April 2017

Part 2: Security functional components, Revision 5, April 2017

Part 3: Security assurance components, Revision 5, April 2017

[3] The Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.

[4] QCCS CB Scheme Certification Procedure [CB-4-PCD-QCCS], v2.0, March 2022.

[5] Security-Target-(ST)-V.1.4-Breach+.pdf

[6] Evaluation Technical Report, Version 4.2, 16 July 2024 - BTTM-CCE-075 DTR v.4.2.pdf

5 Terms and abbreviations

The current manual uses terms as defined in ISO/IEC17065 and CCRA [Ref (1)].

5.1 Terms

Table 3: Glossary of Terms

Term	Definition and Source
CC International Interpretation	An **interpretation** of the CC or CEM issued by the CCMB that is applicable to all CCRA participants.
Certificate	The official representation from the CB of the certification of a specific version of a product to the Common Criteria.
Certification Body	An organisation responsible for carrying out **certification** and for overseeing the day-today operation of an **Evaluation and Certification Scheme**. Source CCRA
Consumer	The organisation that uses the certified product within their infrastructure.
Developer	The organisation that develops the product submitted for CC evaluation and certification.
Evaluation	The assessment of an IT product, IT system, or any other valid target as defined by the scheme, proposed by an applicant against the standards covered by the scope defined in its application against the certification criteria specified in the rules of the scheme. Source CCRA and ISO/IEC 17065
Evaluation and Certification Scheme	The systematic organisation of the functions of **evaluation** and **certification** under the authority of a **certification body** in order to ensure that high standards of competence and impartiality are maintained, and that consistency is achieved. Source CCRA.
Interpretation	Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology. An interpretation may be either a **national interpretation** or a **CC international interpretation**.
Certifier	The certifier responsible for managing a specific certification task.
Evaluator	The evaluator responsible for managing the technical aspects of a specific evaluation task.

Term	Definition and Source
Maintenance Certificate	The update of a Common Criteria certificate to reflect a specific version of a product that has been maintained under the QCCS Scheme.
National Interpretation	An **interpretation** of the CC, CEM or QCCS Scheme rules that is applicable within the QCCS Scheme only.
Security Evaluation Facility	An organisation (or business unit of an organisation) that conducts ICT security evaluation of products and systems using the CC and CEM in accordance with Evaluation and Certification Scheme policy
Sponsor	The organisation that submits a product for evaluation and certification under the QCCS Scheme. The sponsor may also be the developer.
Protection Profile	A formal document defined in CC, expressing an implementation independent set of security requirements for a category of IT Products that meet specific consumer needs.
Security Target	An implementation-dependent statement of security needs for a specific identified TOE.
Target of Evaluation	An IT Product and its associated administrator and user guidance documentation that is the subject of an Evaluation.
TOE Security Functionality	Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

5.2 Abbreviations

Acronym	Expanded Term
API	Application Programming Interface
CB	Certification Body
CC	Common Criteria (ISO/IEC15408)
CEM	Common Evaluation Methodology (ISO/IEC 18045)
CCRA	Common Criteria Recognition Arrangement
EAL	Evaluation Assurance Level

Acronym	Expanded Term
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardization
QCCS	Qatar Common Criteria Scheme
ITSEF	Information Technology Security Evaluation Facility
EB	Evaluation Body (same function as ITSEF)
PP	Protection Profile
SAR	Security Assurance Requirement
SDK	Software Development Kit
SFR	Security Functional Requirement
ST	Security Target
OSP	Organizational Security Policy
TOE	Target of Evaluation
ETR	Evaluation Technical Report
TSF	TOE Security Functionality
TSFI	TSF Interface
ADV	Assurance Class – Development
FSP	Functional Specification
TDS	TOE Design

6 Template History

Version	Date	Comments	Author
1.0	2020/09/05	New - document template	MoTC
2.0	2022/04/03	Change logo, change org. details	NCSA

7 Document Change Log

Release	Date	Comments	Pages Affected
1.0	2022/04/12	Initial creation of certification report	All
1.1	2022/04/14	Minor change	2.1.4.2 – public domain searching

End of Document