National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

IBM QRadar Security Intelligence Platform

Report Number:	**CCEVS-VR-11027-2019**
Dated:	**01/21/2020**
Version:	**0.3**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Common Criteria Testing Laboratory

Chris Keenan
Gossamer Security Solutions, Inc.
Catonsville, MD

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of IBM QRadar Security Intelligence Platform solution provided by IBM, Corporation. It presents the evaluation results, their justifications and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Catonsville, MD, United States of America, and was completed in January 2020. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements of the collaborative Protection Profile for Network Devices, Version 2.1, 11 March 2019.

The Target of Evaluation (TOE) is the IBM QRadar Security Intelligence Platform.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the IBM QRadar Security Intelligence Platform (NDcPP21) Security Target, Version 0.7, 01/15/2020 and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common

Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	IBM QRadar Security Intelligence Platform (Specific models identified in Section 8)
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.1, 11 March 2019
ST	IBM QRadar Security Intelligence Platform (NDcPP21) Security Target, Version 0.7, 01/15/2020
Evaluation Technical Report	Evaluation Technical Report for IBM QRadar Security Intelligence Platform, version 0.3, 01/21/2020
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	IBM, Corporation
Developer	IBM, Corporation
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Catonsville, MD
CCEVS Validators	

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

IBM QRadar SIEM consolidates log source event data from device endpoints and applications that are distributed throughout a network. QRadar performs intermediate normalization and correlation activities on this raw data and can forward data to another network server when so configured. Communication with network peers for outbound log/event data is accomplished using TLS protected communication channels. QRadar is capable of providing an X.509v3 certificate to authenticate itself as part of an outbound TLS connection.

The QRadar SIEM utilizes multiple cryptographic security kernel libraries internally, IBMFIPSJCE, OpenSSL and GPG. The related CAVP algorithm certs are shown in Table 6 1 CAVP Certificates for OpenSSL library.

QRadar provides its cryptographic features through a Java implementation (IBMFIPSJCE) which is developed by IBM independently from QRadar. The OpenSSL library included in the TOE is OpenSSL 1.0.2k-fips as provided by RedHat Enterprise Linux. Thus, all cryptographic functions except those associated with a TOE update validation are provided by IBMFIPSJCE or OpenSSL.

The TOE includes support for GNU Privacy Guard (GPG), which is a public key software package. GPG is used to verify signatures on product updates.

3.1 TOE Evaluated Configuration

The evaluated product is a single All-in-one device running QRadar SIEM 7.3.2 w/ QFlow enabled. The All-in-One device is a self-contained appliance running the QRadar SIEM in a Red Hat RHEL 7.5 environment. The appliance makes only those interfaces offered by QRadar available.

The IBM All-In-One: Dell 3128C, model utilizes an x86 64-bit CPU architecture, with 4 network interface cards, and varying amounts of memory

3.2 TOE Architecture

The evaluated product is a single All-in-one device running QRadar SIEM w/ QFlow enabled. A QRadar QFlow collectors collect network traffic passively through network taps and span ports. A QFlow collector can detect and collect information from networked applications. The All-in-One device is a self-contained appliance running the QRadar SIEM in a Red Hat RHEL 7.5 environment. The appliance makes only those interfaces offered by QRadar available.

The IBM All-In-One: Dell 3128C, model utilizes an x86 64-bit CPU architecture, with 4 network interface cards, and varying amounts of memory.

The All-In-One device can connect to an external audit server allowing QRadar to transmit audit and event data to an external server. All outbound audit data is transferred using TLS protected communication channels.

An IBM QRadar All-In-One device provides a trusted path to remote administrators using an HTTPS protected web GUI or SSH protected Command Line Interface (CLI). The QRadar system offers a CLI at the local console and remotely via SSH as an administrative interface. QRadar also offers a web interface for additional administrative functionality. A single device will have four (4) network connections which can be used either for remote management, receipt of event/syslog data, transmission of audit data, or other network support traffic (e.g.,DNS). A REST API interface is offered by QRadar and can be protected by HTTPS/TLS.

3.3 Physical Boundaries

The TOE is composed of one physical component that is accessed and managed by administrators from computers in the environment.

The TOE can be configured to forward its audit records to an external syslog server in the environment. All audit records sent to the external syslog server are protected using a TLS channel

4 Security Policy

This section summaries the security functionality of the TOE:

1. Security audit
2. Cryptographic support
3. Identification and authentication
4. Security management
5. Protection of the TSF
6. TOE access
7. Trusted path/channels

4.1 Security audit

The TOE generates logs for a wide range of security relevant events. The TOE can be configured to store the logs locally so they can be accessed by an administrator and also to send the logs to a designated network peer using TLS to protect data while in transit. The TOE is also capable of acting as a log storage device and receiving TLS protected communication from network peers sending audit/event data.

4.2 Cryptographic support

The TOE utilizes NIST validated cryptographic algorithms to support key management, random bit generation, encryption/decryption, digital signature and secure hashing and key-hashing features in support of higher level cryptographic protocols including SSH and TLS.

4.3 Identification and authentication

The TOE requires users to be identified and authenticated before they can use functions mediated by the TOE, with the exception of reading the login banner. The TOE authenticates administrative users. In order for an administrative user to access the TOE, a user account including a user name and password must be created for the user.

4.4 Security management

The TOE provides Command Line Interface (CLI) commands and an HTTP over TLS (HTTPS) Graphical User Interface (GUI) to access the wide range of security management functions to manage its security policies. The TOE also offers HTTP over TLS protection for RESTAPI interfaces that can be used for administration. All administrative activity and functions including security management commands are limited to authorized users (i.e., administrators) only after they have provided acceptable user identification and authentication data to the TOE. The security management functions are controlled through the use of privileges associated with roles that can be assigned to TOE users.

4.5 Protection of the TSF

The TOE implements a number of features designed to protect itself to ensure the reliability and integrity of its security features.

It protects particularly sensitive data such as stored passwords and cryptographic keys so that they are not accessible even by an administrator. It also provides its own timing mechanism to ensure that reliable time information is available (e.g., for log accountability).

Note that the TOE is a single appliance, and as such, no intra-TOE communication is subject to any risks that may require special protection (e.g., cryptographic mechanisms).

The TOE includes functions to perform self-tests so that it might detect when it is failing. It also includes support for GNU Privacy Guard (GPG) is a public key software package. GPG is used to verify signatures on product updates. The GPG signature of an update is verified against a published GPG key for IBM which is installed in the TOE.

4.6 TOE access

The TOE can be configured to display a logon banner before a user session is established. The TOE also enforces inactivity timeouts for local and remote sessions.

4.7 Trusted path/channels

The TOE protects communication channels between itself and remote administrators using HTTPS/TLS and SSH. The SSH protocol is used to protect administrative connections utilizing the TOE’s command line interface (CLI). Additionally, web-based GUI and RESTAPI interfaces are available for remote administration which are protected using HTTP over TLS (HTTPS/TLS).

The TOE also protects communication with network peers using TLS. Protected communication includes the TOE’s outbound connection to an external audit server.

5 Assumptions & Clarification of Scope

Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- collaborative Protection Profile for Network Devices, Version 2.1, 11 March 2019

That information has not been reproduced here and the NDcPP20E should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP20E as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

Clarification of scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in the Protection Profile for Network Devices and performed by the evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the NDcPP20E and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6 Documentation

The following documents were available with the TOE for evaluation:

- IBM QRadar Common Criteria for NIAP, Version 7.3.2, Revision 1.4
- IBM QRadar Security Intelligence Platform (NDcPP21) Security Target, Version 0.7, 01/15/2020

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Assurance Activity Report (NDcPP20E) for IBM QRadar Security Intelligence Platform, version 0.3, 01/21/2020 (AAR).

7.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according a Common Criteria Certification document and ran the tests specified in the NDcPP20E including the tests associated with optional requirements.

8 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all assurance activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 5 and CEM version 3.1 rev 5. The evaluation determined the IBM QRadar Security Intelligence Platform TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP20E.

8.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the the IBM QRadar Security Intelligence Platform products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

8.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security target and Guidance documents. Additionally, the evaluator performed the assurance activities specified in the NDcPP20E related to the examination of the information contained in the TSS.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

8.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

8.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

8.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the NDcPP20E and recorded the results in a Test Report, summarized in the AAR.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

8.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities and fuzz testing. Neither the public search for vulnerabilities nor the fuzz testing uncovered any residual vulnerability.

The evaluation team performed a public search for vulnerabilities in order to ensure there are no publicly known and exploitable vulnerabilities in the TOE from the following sources:

- National Vulnerability Database (https://web.nvd.nist.gov/vuln/search)
- Vulnerability Notes Database (http://www.kb.cert.org/vuls/)
- Rapid7 Vulnerability Database (https://www.rapid7.com/db/vulnerabilities)
- Tipping Point Zero Day Initiative (http://www.zerodayinitiative.com/advisories)
- Exploit / Vulnerability Search Engin (http://www.exploitsearch.net)
- SecurITeam Exploit Search (http://www.securiteam.com)
- Tenable Network Security (http://nessus.org/plugins/index.php?view=search)
- Offensive Security Exploit Database (https://www.exploit-db.com/)

The search was performed on 01/07/2020 with the following search terms: "QRadar", "OpenSSL", "openssl", "OpenSSH", "openssh", "SEIM", "IBMFIPSJCE", "libgcrypt".

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

8.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's testing also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

9 Validator Comments/Recommendations

10 Annexes

Not applicable

11 Security Target

The Security Target is identified as: *IBM QRadar Security Intelligence Platform (NDcPP21) Security Target, Version 0.7, 01/15/2020.*

12 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

13 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.

[4] collaborative Protection Profile for Network Devices, Version 2.1, 11 March 2019.

[5] IBM QRadar Security Intelligence Platform (NDcPP21) Security Target, Version 0.7, 01/15/2020 (ST).

[6] Assurance Activity Report (NDcPP20E) for IBM QRadar Security Intelligence Platform, version 0.3, 01/21/2020 (AAR).

[7] Detailed Test Report (NDcPP20E) for IBM QRadar Security Intelligence Platform, version 0.2, 01/08/2020 (DTR).

[8] Evaluation Technical Report (NDcPP20E) for IBM QRadar Security Intelligence Platform, version 0.3, 01/21/2020 (ETR)