National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

QRadar™ V5.1.2

Report Number: CCEVS-VR-07-0003
Dated: January 26, 2007
Version: 1.1

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 6740
Fort George G. Meade, MD 20755-6740

Table of Contents

Table of figures

1. Executive Summary

This Validation Report (VR) documents the evaluation and validation of QRadar V5.1.2.

This VR is not an endorsement of the Information Technology (IT) product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

The Q1 Labs QRadar v5.1.2 product is an administrator configurable network intrusion detection and response system. QRadar collects and processes data both from network taps and from event collectors installed on network devices. The product produces security events by real-time event matching and by comparing the collected data to historical flow-based behavior patterns. The security events are then correlated by the product to produce weighted alerts which are sent to the product users.

The Target of Evaluation (TOE), which is software-only, includes the QRadar v5.1.2 server software and user interface components, the product modules Offence Resolution v1.0 and Offence Manager Software and user interface components, the product's collectors that access network taps, and the interface to the External Event Collector and the Device Support Module.

Aspects of the following security functions are controlled / provided by the TOE in conjunction with the IT environment:

- Security Audit
- Identification and Authentication
- Security Management
- Partial TSF Self-Protection
- Intrusion Detection

The following are explicitly excluded from the TOE configuration, but are included in its IT environment:

- Hardware platform(s) for all product components
- Operating System platform(s) for all product components
- Cryptographic module(s): OpenSSL implementation on all platforms
- SFP domain separation
- Non-bypassability of the TSP
- Reliable time-stamp.
- Software used for event and vulnerability data collection on the customer network
- Network or other connectivity: (Ethernet network)

The evaluation was performed by the CygnaCom Common Criteria Testing Laboratory (CCTL), and was completed during January 2007. The information in this report is derived from the Security Target (written by CygnaCom Solutions), the Evaluation Technical Report (ETR) and associated test reports, all written by the CygnaCom CCTL. The evaluation team determined that the product is Common Criteria version 2.2 [CC] Part 2 and Part 3 conformant, and meets the assurance requirements of EAL2 from the Common Methodology for Information Technology Security Evaluation, Version 2.2, Part 2: Evaluation Methodology [CEM]. The product is not conformant with any published Protection Profiles, but rather is targeted to satisfying specific security objectives.

The evaluation and validation were consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) best practices as described within CCEVS Publication #3 [CCEVS3] and Publication #4 [CCEVS4]. The Security Target (ST) is contained within the document Security Target for QRadar V5.1.2 [ST]. The ST has been shown to be compliant with the Specification of Security Targets requirements found within Annex A of Part 1 of CC.

2. Identification

Target of Evaluation:	QRadar V5.1.2
Evaluated Software:	QRadar V5.1.2, with modules Offence Resolution v1.0 and Offence Manager
Developer:	Q1 Labs Inc. New Brunswick, Canada
CCTL:	CygnaCom Solutions Suite 100 West 7925 Jones Branch Drive McLean, VA 22102-3305
Validation Body:	NIAP Common Criteria Evaluation and Validation Scheme
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 2.2, January 2004
CEM Identification:	Common Methodology for Information Technology Security Evaluation, Version 2.2, January 2004

3. Security Policy

The TOE's security policy is expressed in the security functional requirements identified in section 5.2 of the ST. A summary of the SFRs for the TOE and IT environment are included in the tables below.

TOE Security Functional Requirements

No.	Component	Component Name
1.	FAU_LOG_EXP.1	Audit log generation
2.	FAU_GEN.2	User identity association
3.	FAU_SAR.1	Audit review
4.	FAU_SAR.2	Restricted audit review
5.	FIA_ATD.1*	User attribute definition
6.	FIA_SOS.1	Verification of secrets
7.	FIA_UAU.2	User authentication before any action
8.	FIA_UID.2	User identification before any action
9.	FMT_MTD.1*	Management of TSF data
10.	FMT_SMF.1	Specification of management functions
11.	FMT_SMR.1	Security roles
12.	FPT_RVM_EXP.1-1	Non-bypassability of the TSP
13.	IDS_DPD_EXP.1	Defense perspective data collection
14.	IDS_ANL_EXP.1	Analyzer analysis
15.	IDS_SA_EXP.1	Security alarms
16.	IDS_SR_EXP.1	Security response
17.	IDS_RDR_EXP.1	Restricted data review
18.	IDS_STG_EXP.1-1	Guarantee of defense perspective data availability
19.	IDS_DRS_EXP.1	Data reporting

IT Environment Security Functional Requirements

No.	Component	Component Name
20.	FAU_STG_EXP.2	Guarantees of audit data availability
21.	FPT_RVM_EXP.1-2	Non-bypassability of the TSP
22.	FPT_SEP_EXP.1	TSF domain separation
23.	FPT_STM.1	Reliable time stamps
24.	FTP_ITC.1	Trusted path/channels
25.	IDS_STG_EXP.1-2	Prevention of Defense Perspective data loss
26.	IDS_EVD_EXP.1	Event and vulnerability data collection

4. Assumptions and Clarification of Scope

4.1 Usage Assumptions

For secure usage, the operational environment must be managed in accordance with the documentation associated with the following EAL2 assurance requirements.

ADO_DEL.1 Delivery procedures
ADO_IGS.1 Installation, generation, and start-up procedures
AGD_ADM.1 Administrator guidance
AGD_USR.1 User guidance

4.2 Environmental Assumptions

- The TOE has access to all the IT security management data and defense perspective data it needs to perform its functions.
- The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
- There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
- The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
- Authorized users will follow the guidance provided by the TOE documentation for choosing good passwords.
- The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
- Those responsible for the TOE will ensure the communications between the TOE components are secure via a SSL secure channel.
- The TOE is appropriately scalable to the IT System the TOE monitors.
- There will be no untrusted users of the TOE and no untrusted software loaded on the TOE host platforms.

4.3 Clarification of Scope

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

1. This evaluation does not verify all claims made in the product's end-user documentation. The verification of the security claims is limited to those claims made in the TOE SFRs and TOE Summary Specification (see ST sections 5 and 6 respectively).
2. This evaluation only covers the evaluated configuration of the specific version identified in this document, and not any later versions released or in process.
3. As with all EAL2 evaluations, this evaluation did not specifically search for, nor seriously attempt to counter, 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.

4. QRadar V5.1.2 depends on the IT environment to provide a trusted communication channel between the TOE and a remote trusted IT product.

The ST provides additional information on the assumptions made and the threats countered.

5. Architectural Information

The TOE is defined as Q1 Lab's QRadar v5.1.2 software components QRadar Engine and Console and the QFlow Collector. The exact version of the software components is version 5.1.2. All product components of the TOE are software. QRadar v5.1.2 includes the following product components and subcomponents:

- QFlow Collector(s)
- QRadar Engine and Console
    - Flow Processor
    - Classification Engine
    - Internal Event Collector
    - External Event Processor
    - QRadar Console
    - Magistrate Processing Core

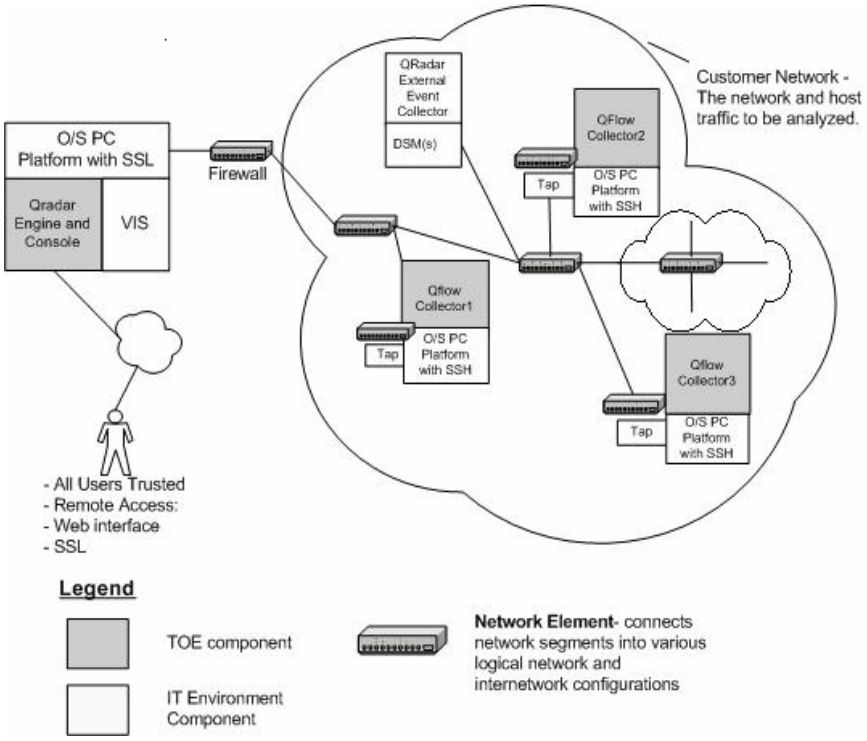

Figure 1. TOE Physical Boundary.

6. Documentation

The following is a list of the end-user documentation that was used to support this evaluation:

QRadar 3.0 Administrator Guide Document release v5.1.1 July, 2006
QRadar 3.0 User Guide Document release v5.1 May, 2006
QRadar Installation Guide, release v5.1 May, 2006
QRadar Hardware Installation Guide, release v5.1 May, 2006
Getting Started Guide, release v5.1 May, 2006

7. IT Product Testing

At EAL2, the overall purpose of the testing activity is "to determine, by independently testing a subset of the TSF, whether the TSF behaves as specified in the design documentation and in accordance with the TOE security functional requirements specified in the ST" (6.8 [CEM]).

At EAL 2, the developer's test evidence must only "demonstrate a correspondence between the tests and the functional specification" (ATE_COV.1, Evidence of Coverage [CC]) and does not include a test coverage analysis that shows that the "TSF has been tested against its functional specification in a systematic manner" (ATE_COV.2, Analysis of coverage [CC]). As a result, the developer's test evidence "need not demonstrate that all security functions have been tested, or that all external interfaces to the TOE Security Function (TSF) have been tested. Such shortcomings are considered by the evaluator during the independent testing sub-activity." (6.8.2.2 [CEM]).

The objective of the evaluator's independent testing sub-activity is "to demonstrate that the security functions perform as specified. Evaluator testing includes selecting and repeating a sample of the developer tests" (ATE_IND.2, Independent testing – sample [CC]). The [CEM] provides the general guidance on the various factors that should be considered by the evaluators in devising their test subset and states that the "evaluators should exercise most of the security functional requirements identified in the ST using at least one test" (6.8.4.4 [CEM]). While, the evaluators build on the developer's testing and use the developer's correspondence evidence to identify shortcomings in the developer's test coverage, the evaluators do not perform a test coverage analysis that would demonstrates that all of the security functions as described in the functional specification were tested. As a result, the testing at EAL 2 may not be systematic and the end-users should not assume that all claims in the ST have been explicitly verified by either the developer or the evaluators.

QRadar V5.1.2 was tested running on the Trustix 2.2 operating system. However, an architectural equivalency argument was provided that documented why both the Trustix 2.2 and Linux Red Hat Enterprise v.4 platforms are functionally equivalent. The product runs on the same Java Virtual Machine using the same set of libraries, the underlying Linux kernel is the same for both the Trustix and Red Hat operating systems, and the

application interface to all services provided by the operating system is identical in all respects. This is assured by the CVS build tree which does not include any operating system specific branches. Therefore, the evaluators determined that QRadar v5.1.2 is architecturally the same product, whether running on the Trustix 2.2 or Red Hat Enterprise 4 operating systems which negated the need for testing on both platforms.

7.1 Developer Testing

The vendor testing covered the security functions identified in Section 6.1 of the ST. These security functions were: Security Audit, Identification and Authentication, Security Management, Partial Protection of TSF and Intrusion Detection System (IDS).

The testing was focused on demonstrating that the SFRs worked as claimed in the ST. The test procedures consisted primarily of manually invoking functions described in the product's user and administrative guides and verifying the function's behavior. In general, only those user interface functions that were directly related to SFRs were explicitly verified.

The evaluator determined that the vendor tested (at a high level) most of the security-relevant aspects of the product that were claimed in the ST. The evaluator determined that the developer's tests were sound in their approach. The test document provided the configuration of the test hardware and software, the objective for each of the tests, and test procedures. The information provided was adequate to be able to reproduce the tests. The evaluators determined that the developer's approach to testing the TSFs was appropriate for this EAL2 evaluation.

7.2 Evaluator Independent Testing

The evaluation team's strategy testing the TOE was to supplement the tests provided by Q1 Labs. The tests provided by Q1 Labs demonstrated almost all aspects of the security functional requirements for QRadar Version 5.1.2 as described in the ST. The team-defined functional tests were developed to cover any areas of functionality that were not included in the developer tests.

Each test was intended to explicitly exercise the Security Audit – Rules or Security Audit - Reporting functionality of the TOE. However, all of the tests also implicitly exercised the Security Audit collection and management functions.

Test results, which are contained in proprietary reports, were satisfactory to both the Evaluation Team and the Validation Team.

7.3 Strength of Function

QRadar is a distributed, software-only product and provides user identification and authentication independent of that provided by the operating system through the use of user identifiers and passwords.

The TOE depends on the strength of the passwords used to authenticate access by administrative users. For authentication mechanisms a qualification of the security behavior can be made using the results of a quantitative or statistical analysis of the effort required to overcome the mechanism. The overall minimum strength of function (SOF) requirements claim for the TOE is SOF-Basic, which effectively requires resistance to password guessing attacks of greater than one day.

The QRadar SOF analysis assumes passwords length to be greater than 4 characters. The character set available for passwords included upper and lower case alphanumeric characters and special characters. Users are trained to pick passwords that include upper and lower case characters as well as at least one numeric and special character.

7.4 Vulnerability Analysis

The developer searched for publicly known vulnerabilities specifically related to the TOE. No publicly-known vulnerabilities specific to the evaluated version of QRadar V5.1.2 were found. The following sources were used to identify and search for relevant vulnerabilities:

- Common Vulnerabilities and Exposures database (http://cve.mitre.org/cve)
- Vendor Advisories, studies, white papers, and vulnerability related documentation
- TOE functions, assumptions, and threats described in the Security Target
- IT Environment Dependencies

Known vulnerabilities in the IT environment could also be exploited to bypass the TOE's security policies. While these vulnerabilities are outside the scope of the evaluation, it is expected that the customer will install the latest security critical patches to the operating system and database software. Under unusual circumstances a patch to TOE may also be required to address compatibility issues with a specific operating system or database patch. The customer is advised to check the QRadar support web site for any restrictions on specific patches to components of the IT environment.

The assumed level of expertise of an attacker is unsophisticated, with access to only standard equipment and public information about the product. The specific threats that the TOE is designed to counter are listed in section 3.2 of the ST.

8. Evaluated Configuration

The evaluated configuration version of QRadar is version 5.1.2 with software modules QRadar Console, Event Processor, Offense Manager, Internal Event Collector, Flow Processor, Classification Engine, and Qflow Collector installed on Linux Red Hat Enterprise v.4 or Trustix 2.2 for all product components. QRadar v5.1.2 running on Linux Red Hat Enterprise v.4 was not formally tested, however, it is considered architecturally equivalent to QRadar v5.1.2 running on the Trustix 2.2 operating system. The product runs on the same Java Virtual Machine using the same set of libraries, the underlying Linux kernel is the same for both the Trustix and Red Hat operating systems, and the application interface to all services provided by the operating system is identical in all respects. This is assured by the CVS build tree which does not include any operating system specific branches.

9. Results of Evaluation

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 version 2.2 of the CC and the CEM.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL2 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of 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.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by CygnaCom CCTL. The security assurance requirements are displayed in the following table.

TOE Security Assurance Requirements

Item	Component	Component Title
1	ACM_CAP.2	Configuration items
2	ADO_DEL.1	Delivery procedures
3	ADO_IGS.1	Installation, generation, and start-up procedures
4	ADV_FSP.1	Informal functional specification
5	ADV_HLD.1	Descriptive high-level design
6	ADV_RCR.1	Informal correspondence demonstration
7	AGD_ADM.1	Administrator guidance
8	AGD_USR.1	User guidance
9	ATE_COV.1	Evidence of coverage
10	ATE_FUN.1	Functional testing
11	ATE_IND.2	Independent testing – sample
12	AVA_SOF.1	Strength of TOE security function evaluation

Item	Component	Component Title
13	AVA_VLA.1	Developer vulnerability analysis

10. Validator Comments/Recommendations

The QRadar Version 5.1.2 TOE is software consisting of modular components and subcomponents. The software can support product configurations where product components are installed on independent platforms. However, in the evaluated configuration, the QFlow Collectors are installed on one platform and all other TOE components are installed on a single server. Therefore, it is possible that some problems remain in configurations that were not tested.

The TOE includes only a portion of the software required to operate and support its security functions. The TOE excludes the hardware, operating system, and third party software. Consequently, much of the burden for maintaining security falls to the environment, and many of the security functional requirements were put on the environment rather than the TOE, where they are subjected to much less scrutiny than the TOE components. Specifically, timestamp for audit, cryptographic functionality (necessary to protect data in transit between the TOE components), and domain separation are levied upon the environment.

The Validation Team agreed with the conclusion of the CygnaCom CCTL Evaluation Team, and issued an EAL2 certificate rating for the QRadar V5.1.2.

11. Security Target

The Security Target for QRadar V5.1.2 is contained within the document QRadar V5.1.2 Security Target V 2.0.4 [ST]. The ST is compliant with the Specification of Security Targets requirements found within Annex A of Part 1 of the CC.

12. Glossary

The following table is a glossary of terms used within this validation report.

Acronym	Expansion
CC	Common Criteria [CC]
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CEM	Common Criteria Evaluation Methodology [CEM]

EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
PP	Protection Profile
SFR	Security Functional Requirement
SOF	Strength of Function
SSL	Secure Socket Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

13. Bibliography

URLs

- Common Criteria Evaluation and Validation Scheme (CCEVS): (http://www.nsa.gov/ia/industry/niap.cfm).
- CygnaCom Solutions CCTL (http://www.cygnacom.com).

CCEVS Documents

- [CC] Common Criteria for Information Technology Security Evaluation, Version 2.2, January 2004.
- [CEM] Common Methodology for Information Technology Security Evaluation, Version 2.2 Part 2: Evaluation Methodology, January 2004.
- [CCEVS3] Guidance to Validators of IT Security Evaluations, Version 1.0, February 2000.

Other Documents

- [ST] Security Target for QRadar V5.1.2, Version 2.0.4, dated 30 January 2007.