Record Identifier: CCEVS-VR-VID10419-2011

CCEVS Approved Assurance Continuity Maintenance Report

Product:	Q1 Labs, Inc. QRadar 7.0, Maintenance Release 5
EAL:	Part 3 Conformant – EAL3 augmented with ALC_FLR.2
Date of Activity:	November 20, 2012
References:	CCIMB-2004-02-009 Assurance Continuity: CCRA Requirements, Version 1.0, February 2004. Q1 Labs Impact Analysis Report (IAR), Version 1.0, August 1, 2012, prepared by Booz Allen Hamilton Common Criteria Testing Laboratory
Documentation Updated:	Q1 Labs QRadar Release 7.0 Maintenance Release 5 Security Target v2.0; Release Notes; QRadar Administration Guide QRadar 7.0 Maintenance Release 5; QRadar Users Guide QRadar 7.0 Maintenance Release 5; QRadar Installation Guide QRadar 7.0 Maintenance Release 5; QRadar Hardware Guide QRadar 7.0; Log Sources User Guide QRadar 7.0 Maintenance Release 5; Evaluated Configuration for Q1 Labs QRadar 7.0 Maintenance Release 5.

I. Introduction

In August, 2012, Q1 Labs, Inc. submitted an Impact Analysis Report (IAR) to CCEVS for approval. The IAR is intended to satisfy requirements outlined in Common Criteria document CCIMB-2004-02-009, "Assurance Continuity: CCRA Requirements", version 1.0, February 2004. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence updated as a result of the changes and the security impact of the changes

II. Changes to the TOE

A list of the new features and enhancements to the TOE is provided in the Tables below, together with a description of the change.

Table 1 - New Features

New Feature	Description
Offenses Interface Enhancement	Previously events and flows were counted and displayed together in the Offenses interface. QRadar now counts and displays events and flows separately in the Offenses interface. This separation allows a user to now search offenses by event count, flow count, or total events and flows.
Template Enhancements	The following rule templates have been added to the QRadar based upon the splitting of events and flows in the Offenses interface: - when the number of events making up the offense is greater than this number - when the number of flows making up the offense is greater than this number - when the number of events and flows making up the offense is greater than this number
Support for Native LDAP without Kerberos	Previously QRadar only supported Lightweight Directory Access Protocol (LDAP) using Kerberos. QRadar now supports configuration options to use native LDAP as an authentication type.
Event and Flow Retention Buckets	Retention buckets define a retention storage policy for events or flows as defined by custom filters to match specific flow or event attributes. For example, a retention bucket might be defined by filtering on just a log source, or it could be defined by a log source and a set of event categories. This feature replaces the Flow Data Retention Period and Event Data Retention Period system settings. Retention buckets are configured in the Admin interface.
PCAP Integration	QRadar now has the ability to receive packet capture files (PCAP) from Juniper SRX that were captured based on event triggering. QRadar correlates the PCAP file with the event and allows a user to click on a PCAP icon associated with events that have packet capture files to view the packet capture, or download the packet capture to view with a packet analyzer application.
Improved Chart Functionality and Performance	QRadar chart display functionality has been updated for the following: - Charts legends have been improved to not truncate object names. - A new option in the Log Activity and Network Activity interfaces allows you to show or hide chart legends. - Chart legends now support the standard IP address and username right-click menu functions.
Improved Time Series Chart Behavior	QRadar chart functionality was updated to automatically display a time series chart if your search parameters match a previously

	saved search for column definition and grouping options.
Self-Signed Certificates	QRadar was updated to support self-signed certificates that can be provided by the organization.
Rule Searching	This allows users to quickly locate the rules they want to edit in the Rules interface.
Calculation-Based Custom Event Properties	This allows a user to create a calculation-based custom property which is based upon already collected event and flow numeric data which is placed through a user defined calculation.
Reports Interface	The following updates have been made to the Reports interface: - Business Hour Reporting - Using the updated features in the Reports Wizard, a user can select a time zone and indicate the time range in which they want data collected for weekly and monthly reports. - Support for 65,000 Records - The Reports Wizard now provides a user with additional options in the Graph drop-down list box for the number of rows that can be printed to include: 25000, 50000, and 65000.
Support for IF-MAP	QRadar now supports Interface For Metadata Access Points (IF-MAP) rule responses. In the System Settings window on the Admin tab, an admin can configure an IF-MAP server. Once the server is configured, a user can use the Rules Wizard to configure rule responses to publish alert and offense data derived from events, flows, and offense data on the configured IF-MAP server.
Quick Filtering	The Quick Filter feature enables a user to search event and flow payloads using a text search string.
Payload Indexing	Payload indexing will index the collected data when processed by QRadar. Payload indexing was added to improve Quick Filter search speeds.
Updated Kernel for Red Hat Enterprise Systems	QRadar appliances running Red Hat Enterprise Linux, now run kernel-2.6.18-238.19.1.el5 for the prebuilt Endace Network Monitoring Interface Card drivers.
Updated Browser Support	QRadar now supports the Internet Explorer 8.0 and 9.0, and Mozilla Firefox web browsers.
New Virtual Appliances	QRadar can now be purchased and used as a virtual appliance, which includes the following models: - QRadar 3199 - QRadar 1699 - QRadar 1799
Updated Event Forwarding Feature	The event forwarding feature on QRadar was updated to allow an administrator the ability to configure routing rules, custom rules, or both to determine what log data they want to forward and what routing options apply to the log data.

Custom Email Notifications	QRadar now allows a user to customize the subject and body of email notifications that are generated as rule responses.
USB Flash Drive Upgrade	QRadar now supports the ability to re-install certain QRadar appliances using a bootable USB flash drive.
Pending Deployment Changes Viewer	Allows an admin to view pending deployment changes that have not been deployed to the remainder of the deployment. Each time and admin accesses the Admin tab and each time they close a window on the Admin tab, a banner at the top of the page displays the following message: Checking for undeployed changes. If undeployed changes are found, the banner updates to provide information about the undeployed changes
Improvements to the Backup and Restore Feature	The Backup and Restore feature was updated to enable a user to backup and restore offense and asset data.
Improvements to the Automatic Update Feature	The Automatic Update window provides more information about the available updates, more detailed error messaging, and better tools to manage your updates. If configured, an admin can now include automatically applying the Device Support Module (DSM) updates as part of the automatic update process.
Improved Handling of Inactive Offenses	The Offenses tab was updated to enable a user to view and search for inactive offenses. Inactive offenses now display an icon in the Flag column to indicate their inactive status.
Improved Navigation in Log Activity and Network Activity Tabs	QRadar was updated to provide Next and Previous icons on the detail pages for events and flows. These icons allow you to easily navigate backward and forward through your events or flows rather than requiring you return to the event or flow list to make another selection.
HMAC Integrity Support	An HMAC Encryption setting is now available on the System Settings window of the Admin UI. When this setting is enabled, integrity hashes on stored event and flow log files are encrypted.
Improved Workflow for Closing Offenses	When offenses are closed, they can now be associated with a pre-defined reason for closure. Closed offenses can then be searched by the closing user or the reason for closure.
Internet Threat Information Center Dashboard Item	The Internet Threat Information Center item is now available on the Dashboard window of the Admin UI. This item is an embedded RSS reader that queries an IBM security website for news that may be of interest to security administrators.

Table 2 - Bug Fixes

Bug Fix	Description
UI Display and Reporting	A number of UI display and reporting bugs were fixed that were preventing or impeding the ability to display data to the user or allow the user to perform management functions.

System Performance	There were several improvements made to increase the performance of QRadar's systems.
High Availability	A number of high availability bugs were fixed that impacted the product's failover function when deployed in a high availability (HA) configuration.
Backup/Restore, Patching, and Updating	A number of bugs were fixed that relate to performing the backup/restore function, installing a new patch, and updating to a new version of the product.
Error Handling	A number of bugs were fixed that relate to incorrect errors displayed, additional logging of errors, and improper functioning of a system due to an error.
Vulnerability	There were several updates made to fix newly discovered potential vulnerabilities within QRadar.
Expected Functionality	A number of bugs were fixed that addressed an issue with QRadar operating as claimed. These bugs were discovered through real-world purposing of the product in a variety of scenarios.
Outside Previous TOE Boundary	A number of bugs were fixed that addressed an issue with functionality that was outside the TOE boundary during the previous evaluation.
Miscellaneous	A number of miscellaneous bugs were fixed.

Note: The details of the bug fixes are contained in the maintenance releases, MR1 through MR5, inclusive.

III. Analysis and Testing

The development team assessed the impacts of each of the changes to determine whether they constituted major or minor changes, or no change. After completing the analysis for each new feature and bug fix, the development team was able to determine that no feature or fix adversely affected the functionality of the TOE and none of the changes had other than a minor impact. For that reason, the overall impact for the release of Q1 Labs, Inc. QRadar Release 7.0 Maintenance Release 5 is of "minor impact."

IV. Conclusions

The changes to the TOE are confined to user interfaces, primarily to improve the usability of the product. No existing security functionality was removed and no new security functionality was added. The development team's analysis and conclusions are acceptable.