Maintenance Report

NetIQ® Sentinel™ 7.2.1

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-7-116 MR
Version: 1.0
Date: January 9th, 2015
Pagination: 1 to 2

1 Introduction

EWA-Canada has submitted the Impact Analysis Report (IAR) for NetIQ® Sentinel™ 7.2.1 (hereafter referred to as Sentinel 7.2.1), satisfying the requirements outlined in Assurance Continuity: CCRA Requirements, v2.1, June 2012. In accordance with those requirements, the IAR describes the changes implemented in Sentinel 7.2.1, (the maintained Target of Evaluation), the evidence updated as a result of the changes and the security impact of the changes.

2 Description of changes in the Maintained Target of Evaluation

The following characterizes the changes implemented in Sentinel 7.2.1. For each change, it was verified that there were no required changes to the security functional requirements in the ST, and thorough functional and regression testing was conducted by the developer to ensure that the assurance in the Target of Evaluation (TOE) was maintained. The changes in Sentinel 7.2.1 comprise:

- Features and enhancements outside of the claimed functionality, such as integrations with ISO formatting standards, the addition of high availability configuration features, improved grouping of event options, saving of favorite reports, support for new Plug ins, a hardware appliance version, and support for optional Microsoft SQL 2008 R2 and Microsoft SQL 2012 databases;
- Cosmetic and usability improvements, such as new templates and report options, new search, correlation, and filter options, improvements to error messages (for functionality not included in the evaluated configuration);
- Upgrades to embedded components such as the underlying PostgreSQL database, and Java version; and
- Bug fixes, including those related to the use of special characters, remote caching of events, Sentinel uninstallation errors, XML file handling, correlated event message field (which now displays events that triggered the correlation), LDAP authentication fixes (not part of evaluated configuration), improved handing of export of search results with more than 50,000 events, correction to 'view triggers' which now displays only the events that triggered the correlation event, database connection fixes, raw data handling fixes (large volumes of raw data no longer trigger out of memory errors), report fixes (reports no longer fail if there are more than 10,000 unique groups - limit changed to 20,000), security intelligence data migration issues fixed, corrections to custom mapping issues, distributed search display errors fixed, limits to simultaneous non-user initiated searches to prevent out of memory errors fixed, the database password is no longer stored in clear text in the .pgpass file, improved handing of use of an unavailable port number in the web interface, fixes to correlation displays (correlated events now display the correlation rule name and description), data file fixes (raw data files now have the correct extension (.gz)), and the link to Sentinel Plug ins in the console is now labelled 'Sentinel Plug-ins".

3 Description of Changes to the IT Environment

The following changes were made to the underlying IT environment;

- The Sentinel component is now supported on both SUSE Linux Enterprise Server (SLES) 11 SP3 and Red Hat Enterprise Linux (RHEL) 6.4; and
- The log manager component is now supported on SUSE Linux Enterprise Server (SLES) 11 SP3.

4 Description of Changes to the Development environment

The following changes were made to the development environment;

- The development and storage sites have been consolidated for the changed TOE, with development no longer being performed in Hyderabad, India, and software no longer being held at the Verizon Data Center. Development and storage has been consolidated to NetIQ facilities and servers in Vienna, Virginia; Provo, Utah; and Bangalore, India. All these facilities/servers were included in the original evaluation.

5 Affected developer evidence

Modifications to the product necessitated changes to a subset of the developer evidence that was previously submitted for the TOE. The set of affected developer evidence was identified in the IAR.

Modifications to the security target were made to reflect the new product versions.

6 Conclusions

Through functional and regression testing of Sentinel 7.2.1, assurance gained in the original TOE certification was maintained. As all of the changes to the maintained TOE have been classified as minor, it is the conclusion of the CB that the maintained TOE is appropriate for assurance continuity and re-evaluation is not required.

7 References

- Assurance Continuity: CCRA Requirements, v2.1, June 2012;
- CCS Guide #6, Technical Oversight for Assurance Continuity of a Certified TOE, v1.6, May 2011;
- Certification Report EAL 3+ Evaluation of NetIQ® Sentinel Version 7.0.1, v1.0, 20 December 2012;
- NetIQ® Sentinel™ 7.2.1 Security Target, v0.3, 14 November 2014