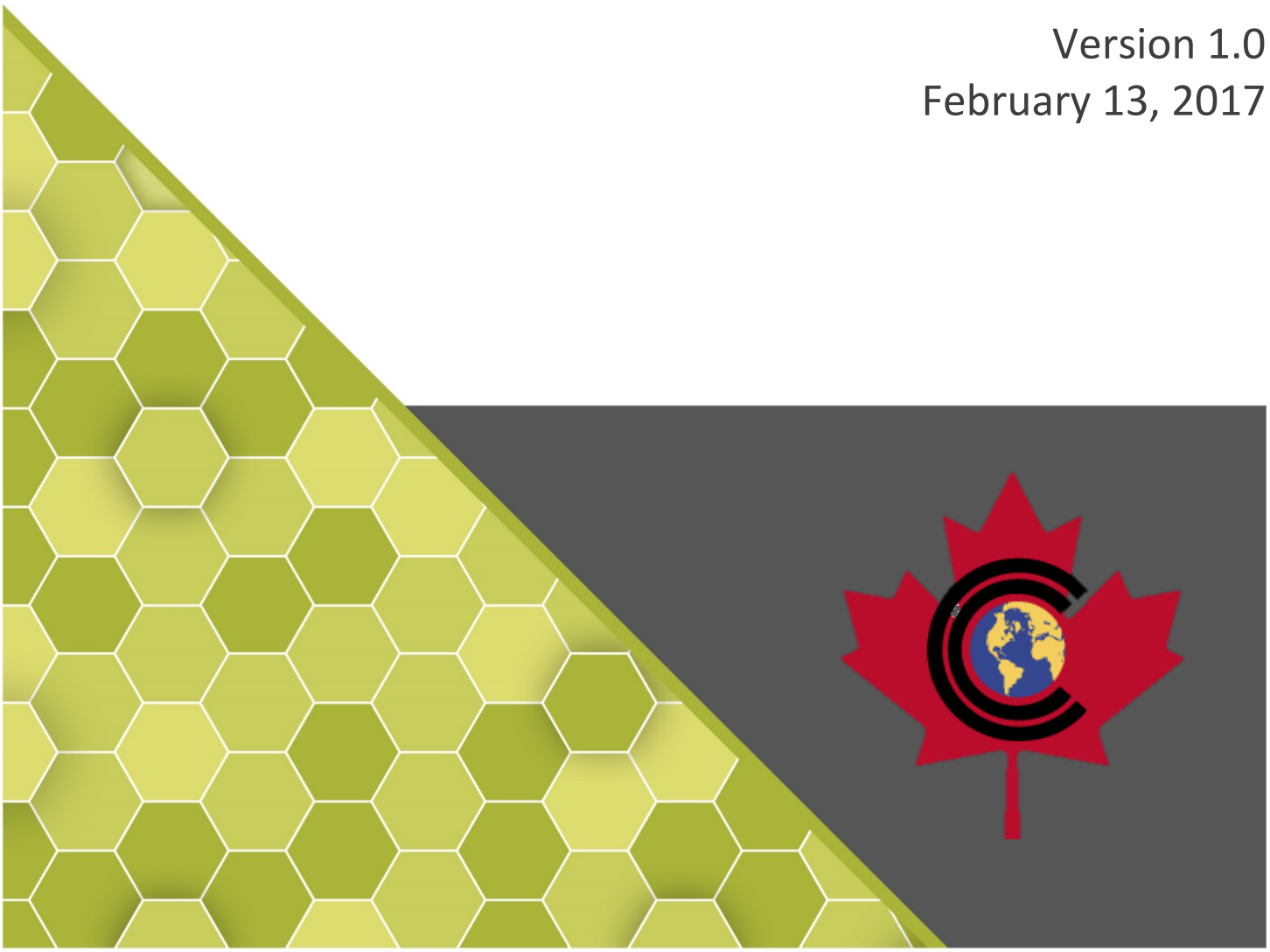
COMMON CRITERIA MAINTENANCE REPORT

Trustwave AppDetectivePRO Version 8.7

Version 1.0
February 13, 2017



Canada

FOREWORD

The Maintenance Report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE). Suggestions for amendments should be forwarded through departmental communications security channels to your Client Services Representative at CSE.

If your department has identified a requirement for report based on business needs and would like more detailed information, please contact:

ITS Client Services
Telephone: (613) 991-7654
E-mail: itsclientservices@cse-cst.gc.ca

OVERVIEW

Trustwave Holdings, Inc. has submitted the Impact Analysis Report (IAR) for Trustwave AppDetectivePRO Version 8.7 (hereafter referred to the TOE), 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 the TOE, (the maintained Target of Evaluation), the evidence updated as a result of the changes and the security impact of the changes.

TABLE OF CONTENTS

1 CHANGES

The following characterizes the changes implemented in the TOE and/or the environment. 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.

1.1 DESCRIPTION OF CHANGES IN THE MAINTAINED TARGET OF EVALUATION

The changes in the TOE comprise;

- Session Management: Sessions can be locked with a password and multiple sessions can be deleted at a time.
- Policy Results: Enhanced view of occurrences, showing all the occurrence types.
- Report Enhancement: Check Results Report can now be generated in XCCDF format (Extensible Configuration Checklist Description Format). Added SHATTER KB version used to run scans on reports. Added a section to reports to indicate if results were filtered. Added an option to exclude exceptions being displayed for vulnerability details report.
- License Expiration Notification: Popup warning of license expiration will display starting 60 days for expiration.
- Policy Editor Enhancements: Clone and customize policies belonging to CIS or DISA STIG frameworks. Modify risk level of checks in any custom policies.
- System Settings Enhancements: User Configuration: Option to view and delete any added users configured to run the product. Password Configuration: Option to unmask passwords found during scans if needed. This must be disabled prior to running any new scans.
- License Management: Only current licenses will be displayed. There is an option to view any expired licenses still installed.
- Results Filtering: Updated search filter to be global rather than specific for check or object name in Policy and User Rights results.
- Named Pipe Connection Support: Run audits via named pipe connection for your SQL Servers.
- Discovery Detection Options:- New options provide different levels of database detection during discovery.
- Asset Inventory Report: Generates a list of all the assets in your session.
- Scan Later: New option to run a scan at a later time within a 24 hour period.
- Enhanced Experience for Credentials Input: Credentials are input once for an audit and choose to apply them to more than one asset.
- Added the CHECK_ID information to the Check Results report.
- Fixed a critical application crash when scanning an Oracle 11g for the first time.

- User Rights Review reports are filtered per filtered data in the UI.
- Control Review and DISA-STIG Review reports now show occurrence level notes.

1.2 DESCRIPTION OF CHANGES TO THE IT ENVIRONMENT

No changes have been made to the IT environment.

1.3 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.

2 CONCLUSIONS

Through functional and regression testing of the TOE, 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.

The IT product identified in this report has been evaluated at an approved evaluation facility established under the Canadian Common Criteria Evaluation and Certification Scheme using the Common Methodology for IT Security Evaluation, Version 3.1 Revision 4, for conformance to the Common Criteria for IT Security Evaluation, Version 3.1 Revision 4. These evaluation results apply only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report.

The evaluation has been conducted in accordance with the provisions of the Canadian Common Criteria Evaluation and Certification Scheme and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This is not an endorsement of the IT product by CSE or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by CSE or by any other organization that recognizes or gives effect to this certificate, is expressed or implied.

2.1 REFERENCES

Reference
Assurance Continuity: CCRA Requirements, v2.1, June 2012
Certification Report, Trustwave AppDetectivePRO Version 8.3.1, 17 July 2015
Trustwave AppDetectivePRO Version 8.7 Security Target, Version 1.10, 13 February 2017