Annex D

Test Plan/Results:

Vulnerability Compliance Management Service RFP

Table of Contents

1. Background 3
2. Introduction 4
   - 2.1. VCMS RFP Test Plan 4
   - 2.2. Document scope 4
   - 2.3. Assumptions 5
   - 2.4. Test environment 5
   - 2.5. Terminology and abbreviations 5
3. Test plan 6
   - 3.1. Description 6
   - 3.2. Test Cases 6

1. Background

The Vulnerability & Compliance Management Service (VCMS) is a collection of processes, procedures, and tools that are collectively used to cost-effectively manage information system IT security exposures, and reduce the attackable surface that is available to both a deliberate and non-deliberate threat actor within enterprise computer networks, systems, applications, and the important information they contain.

The VCMS improves the GC's capacity to

- determine the owners, and the mission criticality of network-attached IT assets;
- discover, inventory, and track these assets;
- maintain a current and effective database, and detect and identify code-based and configuration-based (i.e., design and specification, implementation, and operation and configuration) IT security vulnerabilities within these assets,
- assign severity ratings to these findings that, in conjunction with the mission criticality of the affected assets, enable risk prioritization based on business context, and drive timelines and thresholds of remediation activities;
- consolidate these findings; and
- propose remediation advice, options, and sequencing to mitigate the IT security risk associated with these findings.

The VCMS also paves the way for integrated and automated vulnerability detection and remediation across the SSC/Partner environments.

Design principles of the solution set include: least privilege, separation of duties, least common mechanism, consolidation, interoperability, scalability, accuracy, coverage, and timelines.

2. Introduction

The primary purpose of the VCMS Request for Proposal (RFP) is to establish a vehicle to replace end-of-life and end-of-support VCMS solutions currently deployed at Shared Services Canada (SSC) partners, as well as meet future SSC/partner procurement requirements for equipment, software and professional services necessary to acquire, develop, implement, and maintain a GC wide VCMS for data centres, legacy data centres, Internet facing infrastructure and up to 2,000,000 network-attached IT assets.

2.1. VCMS RFP Test Plan

The primary purpose of the VCMS Test Plan is to verify the functional and security assurance requirements, validate the design of the VCMS solution, and to evaluate risk and product and process capabilities. Effectively, this test plan will be used to verify a subset of the VCMS solution mandatory requirements. Only the winning bid will be subjected to this test plan; if bidder fails to demonstrate the requirements to the satisfaction of SSC, the bidder will automatically be disqualified and the next eligible bid will be evaluated.

2.2. Document scope

This test document is written to detail which Mandatory RFP requirements will be tested, and how they will be tested.

The mandatory requirements that will be tested are:

- M1: The solution must fully support implementation, administration, configuration and scanning for both IPv4 and IPv6 networks.
- M2: The solution must be capable of performing asset discovery, inventory, tracking, and vulnerability scans of 2,000,000 network-attached IT assets. A discovery scan must record 10,000 IP addresses in one day. A full non-credential based scan of 10,000 IP addresses must complete over a 2 day period, staggered over non-production hours to limited impact to daily operations. A full credential based scan of 10,000 IP addresses must complete over a 3 day period, staggered over non-production hours to limited impact to daily operations.
- M4: The solution must be capable of risk prioritization customization based on business context.
- M6: The solution must have the ability to ingest vulnerability scan results from other vendors in various formats.
- M7: The solution must have the ability to consume and execute industry or custom SCAP 1.2 or later content.
- M9: The solution must maintain and store secure audit logs in accordance with GC policies. (See http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12742)
- M11: The solution must be capable of processing, communicating, and storing data using a GC approved encryption method where deemed necessary (i.e. data sensitivity), use cryptographic algorithms, cryptographic key sizes and crypto periods that have been approved by CSE, validated by the Cryptographic Algorithm Validation Program (http://csrc.nist.gov/groups/STM/cavp/), and are specified in ITSB-111 (https://www.cse-cst.gc.ca/en/node/1428/html/25015) or subsequent version;

- M13: The solution must uniquely identify and authenticate organizational users through the use of Microsoft Active Directory Services.
- M18: The solution must have the ability to back up its entirety which includes but not limited to scan data configuration.
- M27: The solution must provide asset discovery, grouping, classification, and management capabilities.

2.3. Assumptions

This document assumes the following:

- A representative of the OEM will be executing the test plan, which will be witnessed and scored by the Crown's testing resources.
- The OEM representative testers have expert knowledge with all the hardware and software components of the solution.
- The OEM representative will provide the solution testing equipment. The equipment must match what is being bid.
- All data used for the testing will be provided by and gathered from the lab environment of the bidder.

2.4. Test environment

The Bidder will provide the test environment, including all hardware and software required for the testing.

2.5. Terminology and abbreviations

See RFP SOW.

3. Test plan

3.1. Description

The following section is intended to verify a subset of the RFP mandatory requirements and document the test results. The test cases that have been created are non-solution specific. The environment can be set up dynamically based on the execution needs of each test case. In addition, the Crown has the flexibility to update the test execution to suit the design of the OEM default architecture.

3.2. Test Cases

Case #	Description	Test Execution	PASS / FAIL
M1	The solution must fully support implementation, administration, configuration and scanning for both IPv4 and IPv6 networks.	The bidder will demonstrate that the solution fully supports IPv4 and IPv6 coexistence (dual-stack), and that it does not require IPv4 for proper and complete function. The bidder will demonstrate that IPv6 support is equivalent or better in quality and functionality when compared to IPv4 support. These tests will demonstrate that all subsystems of the solution function properly and completely over a dual-stack implementation, and without IPv4, including: • client network access to the management, scan engine, repository/database, reporting, Command-line Interface (CLI), and Graphical User Interface (GUI); • the network access between the scan engine and the network-attached IT assets (e.g., network-oriented asset discovery, network and port scanning, port scanning, enumeration of network resources and shares, and vulnerability and compliancy checks); • the network access between the repository/database and the vendor update sites; and • the intercommunication between the scan engine, repository/database, management, and reporting	

Case #	Description	Test Execution	PASS / FAIL
		components.	
M2	The solution must be capable of performing asset discovery, inventory, tracking, and vulnerability scans of 2,000,000 network-attached IT assets. A discovery scan must record 10,000 IP addresses in one day. A full non-credential based scan of 10,000 IP addresses must complete over a 2 day period, staggered over non-production hours to limited impact to daily operations. A full credential based scan of 10,000 IP addresses must complete over a 3 day period, staggered over non-production hours to limited impact to daily operations.	The bidder will demonstrate that the solution can scale IT asset discovery and identification, inventory, tracking, scanning and reporting on 2,000,000 network-attached IT assets. The bidder will demonstrate this requirement using 3 separate multi-zone networks consisting of several IT zones per multi-zone network. These tests will demonstrate • scalability via an architecture of multiple hierarchies of distributed, centrally coordinated management and reporting VCMS subsystems and components; • ability to execute multiple scheduled, and on-demand scans concurrently from multiple user classes, from multiple client organizations, and across multiple echelons of hierarchy; • a method of excluding hosts or host groups from being scanned (IP range, dynamic asset groups, etc.); • ability to identify and track changes in vulnerability states; and • ability to view real-time status of all running scans. The above must be at a scanning frequency of one week or less, with no loss in detection or accuracy.	
M4	The solution must be capable of risk prioritization customization based on business context.	The bidder will demonstrate that risk prioritization can be customized and configured using a console demonstration. The tests will demonstrate that network-attached IT assets can be categorized into groups and assignment of business value based on the criticality of the business processes they support.	

Case #	Description	Test Execution	PASS / FAIL
M6	The solution must have the ability to ingest vulnerability scan results from other vendors in various formats.	The bidder will demonstrate that the solution supports the ability to consume vulnerability scan reports from other vendors. These tests will demonstrate that the solution imports asset discovery and vulnerability scan reports from other vendors within the VA market with no loss in the quality of information being imported.	
M7	The solution must have the ability to consume and execute industry or custom SCAP 1.2 or later content.	The bidder will demonstrate that the solution support's a method for using a standards-based approach to automate vulnerability management. Including describing publicly known information security vulnerabilities and exposures, determining the relative severity of software flaw vulnerabilities and providing a standardized format for communicating vulnerability characteristics, and representing security checklists, benchmarks, and related documents in a machine-readable form. These tests will demonstrate: • the solution supports a standard-based approach for describing, communicating and consuming publicly known information security vulnerabilities and exposures; • determining the relative severity of software flaw vulnerabilities and providing a standardized format for communicating or consuming vulnerability characteristics; and • representing, communicating and consuming security checklists, benchmarks, and related documents in a machine-readable form.	
M9	The solution must maintain and store secure audit logs in accordance with GC policies. (See http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12742)	The bidder will demonstrate that the solution maintains and stores secure audit logs in accordance with GC policies. The tests will demonstrate that the solution: • is NTP synchronized,	

Case #	Description	Test Execution	PASS / FAIL
		• produces audit logs, including network traces associated with any scanning activity and associated administrator accounts to ensure that this activity is limited to the time frames of legitimate scan.	
M11	The solution must be capable of processing, communicating, and storing data using a GC approved encryption method where deemed necessary (i.e., data sensitivity), use cryptographic algorithms, cryptographic key sizes and crypto periods that have been approved by CSE, validated by the Cryptographic Algorithm Validation Program (http://csrc.nist.gov/groups/STM/cavp/), and are specified in ITSB-111 (https://www.cse-cst.gc.ca/en/node/1428/html/25015) or subsequent version.	The bidder will demonstrate that the solution supports GC approved encryption algorithms for securing the communication channels between all subsystems of the solution. These tests will demonstrate that the solution uses GC approved encryption algorithms for securing the communication channels, including: • client network access to the management, scan engine, repository/database, reporting, Command-line Interface (CLI), and Graphical User Interface (GUI); • the network access between the repository/database and the vendor update sites; and • the intercommunication between the scan engine, repository/database, management, and reporting components.	
M13	The solution must uniquely identify and authenticate organizational users through the use of Microsoft Active Directory Services.	The bidder will be required to provision an AD server, and demonstrate that AD can be used for authentication to the solution. The tests will demonstrate that RBAC can be used to provide different right and functionality, enforcing the separation of duties from multiple user classes, from multiple client organizations, and across multiple echelons of hierarchy.	
M18	The solution must have the ability to back up its entirety which includes but is not limited to scan data configuration.	The bidder will demonstrate that the solution can be backed up in its entirety. The test will demonstrate that: • the database subsystem and components are backed up, including configuration, credentials, templates, and	

Case #	Description	Test Execution	PASS / FAIL
		data; and • configurations can be re-used as configuration templates. A replacement manager that is identical to the original (appliance, server or virtual machine) will then be configured by the bidder to the state required to allow the restore.	
M27	The solution must provide asset discovery, grouping, classification, and management capabilities.	The bidder will demonstrate the ability to uniquely identify, group, classify, and manage network-attached IT assets based on these or other known identifiers and/or known information. These tests will demonstrate: • ability to discover and identify classes of applications, operating systems, and hardware devices present among the discovered network-attached IT assets; • that these IT assets can be: – grouped by client organization, and by timeline, – classified based on the mission criticality of the IT assets, – classified based on the severity of the findings, • that the asset discovery does not pollute or cross-contaminate inventories of network-attached IT assets discovered within other clients or SSC/Partner environments. • that the reporting subsystem can be reported upon by rolling up from multiple user classes, from multiple client organizations, and across multiple echelons of hierarchy, including: – client organizations – management system node	

Case #	Description	Test Execution	PASS / FAIL
		– all organizations/Partners, – multiple management subsystem nodes • that references to the same assets can be detected and removed.	