ANNEX D

TEST PLAN

Table of Contents

1. Introduction 3
   - 1.1 About 3
   - 1.2 Document scope 3
   - 1.3 Assumptions 3
   - 1.4 Test environment 3
   - 1.5 What is not tested 5
   - 1.6 Terminology and acronyms 5
2. Test plan 6
   - 2.1 Description 6
   - 2.2 Prerequisites 6
   - 2.3 Test Cases 8

1. Introduction

1.1 About

The primary purpose of the Full Packet Capture and Security Analysis Tool Request for Proposal (RFP) is to replace an end-of-life and end-of-support (as of March 31, 2016) full packet capture and security analysis solution. The second objective of the RFP is to establish a method to expand the solution within the Government of Canada (GC) over time. In order to meet both objectives, several mandatory and rated requirements have been established to evaluate bids. This Test Plan will be used to verify a subset of the mandatory requirements as part of the RFP process. Only the winning bid will be subjected to this Test Plan; if the Test Plan fails, the bidder will automatically be disqualified and the next eligible bid will be evaluated.

1.2 Document scope

This test document was written with the intent of validating the following requirements:

- Mandatory requirements from the RFP: C2M7, C2M8, C2M10, C2M11, C2M12, C2M13, C2M15, C2M16, C2M33, C2M35, C2M38, C2M39, C2M41, and C2M42
- The test cases will be based on a medium sized solution

1.3 Assumptions

This document assumes the following:

- A representative of the OEM will be present during the testing, and will work with the Crown's testing resources to execute the test plan.
- 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 suitable to be placed in the test lab. The equipment must match what is being bid for the medium solution.
- Testing will occur within 1 to 2 business days.
- The Crown will provide the test lab. Crown testers will be fully familiar with this lab.
- The testing will occur at 101 Goldenrod Driveway, Ottawa, Ontario. Both OEM and Crown resources will conduct the testing onsite.
- All data used for the testing will be unclassified.

1.4 Test environment

A unclassified test and development center will be used. The test environment is comprised of the following components:

1. Workstation(s). Will be provided by the Crown and be used to generate network traffic. A Windows 7 workstation will be used. A secondary Windows 7 workstation will be used to stage files and to send test emails.
2. SOC Operators Server. Will be provided by the Crown and will be a Windows 2012 Server. If required, the software required to access the solution will be installed on the solution. The Server will be on same LAN as the management interface of the Solution.
3. Solution. Will be provided by OEM. A 1G copper cable will be wired from solution to F5 span port. A minimum amount of storage to meet the test cases is required, at the discretion of the OEM. Equipment will be returned to OEM on completion of the testing.
4. F5. Will be provided by the Crown. Positioned between the Test and Development center and workstation. Traffic to and from the workstation will be replicated to the solution using traffic mirroring.
5. Application Server. Will be provided by the Crown. A Windows 2012 Server. Used to host server applications.
6. TDC. Will be provided by the Crown. A GC National Test and Development Center (TDC).
7. TDC Firewall. Will be provided by the Crown. An Intel based Firewall used to provide Internet access to the TDC.
8. Internet. Public sites will be accessed to perform several of the tests.

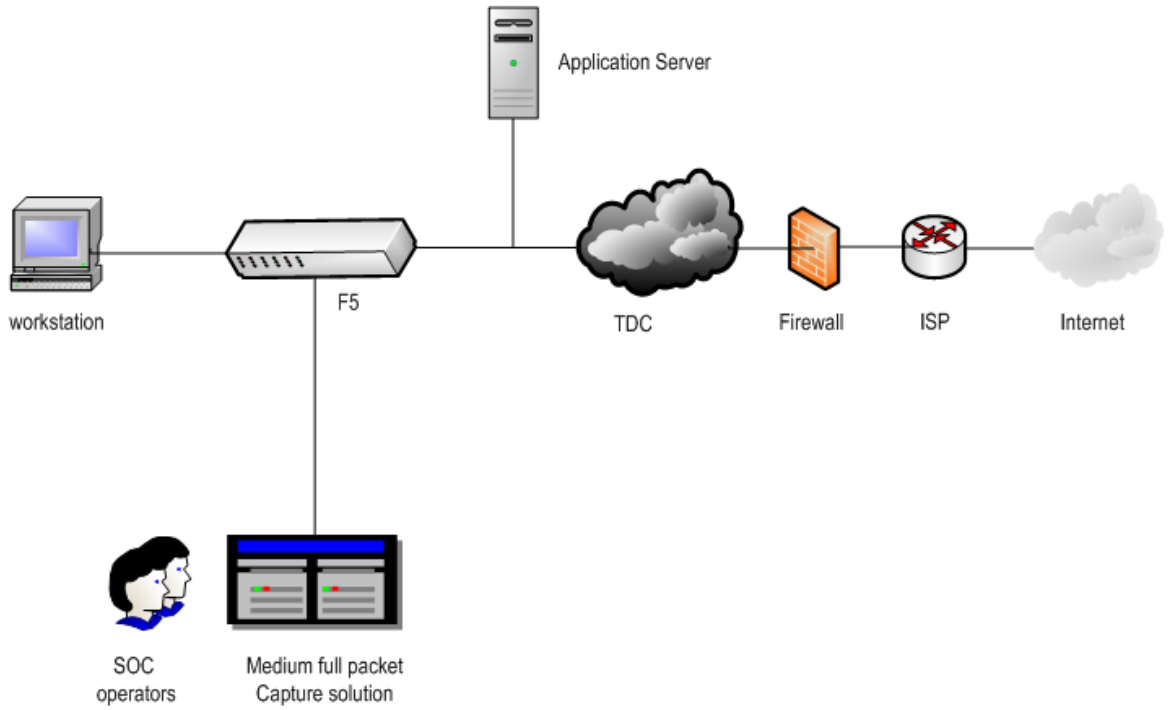

Figure 1

1.5 What is not tested

This document will not test the following infrastructure:

- The central management system.
- Requirements that are not explicitly listed in section 1.2.
- The execution of known malware will not be performed in the environment.
- Known malicious sites will not be accessed in the environment.

1.6 Terminology and acronyms

See RFP SOW.

2. Test plan

2.1 Description

The following section is intended to document the test results and verify a subset of the RFP mandatory requirements. The test cases that have been created are non-solution specific. The environment can be setup 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.

2.2 Prerequisites

The following prerequisite configurations for the components listed in section 1.4 are to be completed prior to executing the test cases:

- Staging Workstation
  - ☐ Install the following applications: Microsoft Outlook 2010, Microsoft Office 2010, Wireshark, Notepad, Internet Explorer, Google Chrome Web Browser, RDP client, and FTP client.
  - ☐ Install the Adobe Reader PDF plug-in on Internet Explorer and Google Chrome Web Browser
  - ☐ Internet Explorer and Google Chrome Web Browser are configured to use a web proxy: 172.16.16.80:8080
  - ☐ Assign a Static IP of 172.16.16.12 with subnet mask of /24 default gateway of 172.16.16.250
  - ☐ Create a Microsoft Word file and type into the body: "*The quick brown fox jumps over the lazy dog*" and save as "*test.docx*" to the Desktop.
  - ☐ Login as "testuser2", open Microsoft Outlook and send an email message with the following criteria:
    - Sender: testuser2@foo.local

      Recipient: testuser@foo.local

      Subject Line: "Test"

      Body: "Testing 1 2 3"

      Attachment: "test.docx"
- Workstation:
  - ☐ Install the following applications: Microsoft Outlook 2010, Microsoft Office 2010, Wireshark, Notepad, Internet Explorer, Google Chrome Web Browser, RDP client, and FTP client.
  - ☐ Install the Adobe Reader PDF plug-in on Internet Explorer and Google Chrome Web Browser

- ☐ Internet Explorer and Google Chrome Web Browser are configured to use a web proxy: 172.16.16.80:8080
- ☐ Assign a Static IP of 172.16.16.10 with subnet mask of /24 and default gateway of 172.16.16.250
- ☐ Create a Microsoft Word file and type into the body: "*The following is my proposal for consolidating IT services.*" and save as "*test2proposal.docx*" to the Desktop.
- ☐ Create a text file and type into the contents: "*The quick brown fox jumps over the lazy dog*" and save as "*test.txt*" to the Desktop.

- Solution:
  - ☐ Create the following test accounts:
    i. User-Admin (Administrator)
    ii. User-SOC (SOC Operator)
    iii. User-Guest (Guest)
- SOC Operator Server:
  - ☐ Install the Solution operator console (if applicable)
  - ☐ Internet Explorer will have Adobe Reader PDF plug-in
  - ☐ Create a 1 GB file prepopulated with PCAP traffic and save as "import.pcap" to the Desktop
- Application Server:
  - ☐ Windows DNS configured with foo.local domain
  - ☐ FTP site with at least one folder in the root directory
  - ☐ Create a subpage of foo.local: http://www.foo.local/bigpage.html
    i. Configure with GZIP compression using level 6 (http://www.iis.net/configreference/system.webserver/httpcompression/scheme)
  - ☐ Microsoft Exchange configured as an SMTP server with the following test email accounts:
    i. testuser@foo.local
    ii. testuser2@foo.local
    iii. testuser3@foo.local

Notes:

1. The SOC Operator account ("User-SOC") will always be used to validate test cases on the solution console, unless otherwise noted.
2. The "testuser" account will always be used to login to Workstation to execute test cases, unless otherwise noted.

2.3 Test Cases

Case #	Description	Test Execution	Desired Outcome	Actual Result	PASS / FAIL
1.	C2M7. Solution must be able to work in an out-of-band deployment consisting of a network tap or packet flow switch that duplicates network traffic to the solution.	1. Login to Workstation and launch Wireshark 2. Start live capture with capture filter on HTTP traffic 3. Open IE browser and navigate to http://www.canada.ca/en/index.html 4. Once page has completely loaded, stop the live capture on Wireshark 5. Login to SOC Operator Server 6. In solution, navigate to raw data view and filter on HTTP traffic	SOC Operator selects a random sample of 10 packets. The sample should match the data from Wireshark in the solution.		
2.	C2M8. Solution must support role based access control. At a minimum, the following roles are mandatory: • Administrator • Operator • Guest	1. Login to SOC Operator Server 2. Login to solution as User-Admin 3. Verify account privileges 4. Logout of User-Admin account 5. Login as User-SOC account 6. Verify account privileges 7. Logout of User-SOC account 8. Login as User-Guest account	• User-Admin should be able to create, read, update, and delete all aspects of the solution. • User-SOC should be able to query packets and generate reports • User-Guest		

Case #	Description	Test Execution	Desired Outcome	Actual Result	PASS / FAIL
		9. Verify account privileges 10. Logout of User-Guest account	should only be able to view specific aspects of the solution		
3.	C2M10. The solution must be able to support Layer 4 to 7 Application parsing/decoding and reconstructing of the following protocols: • (3a) DNS to Internal server; and • (3b) FTP to Internal server.	**3a:** 1. Login to Workstation 2. Launch a command prompt and perform the following commands: a. nslookup www.foo.local (Server ip) b. nslookup –type=mx foo.local (Server IP) c. nslookup –type=ns foo.local (Server IP) 3. Note the results from the commands 4. Login to SOC Operator Server 5. In solution, reconstruct the DNS traffic **3b:** 6. Login to Workstation 7. Launch an FTP session to the Application server 8. Once FTP session has been initiated, enter the following commands:	• 3a: In solution, verify that the DNS commands are correctly reconstructed. • 3b: In solution, the reconstructed session should be correctly displayed; including the ability to view the “dir” and “cd switch folder” commands.		

Case #	Description	Test Execution	Desired Outcome	Actual Result	PASS / FAIL
		a. dir b. cd switch folder 9. Logout of FTP session 10. Login to SOC Operator Server 11. In solution, reconstruct the FTP traffic			
4.	C2M11. The solution must have the ability to apply Berkeley Packet Filters (BPF) on what traffic is captured or ignored.	1. Login to SOC Operator Server 2. Activate Berkeley Packet Filter (BFP) in the solution and apply the following filters: a. Allow HTTP packets b. Ignore source port 443 3. Login to the Workstation, open IE browser, and navigate to the following websites: a. https://www1.bmo.com/onlinebanking/cgi-bin/netbnx/NBmain?product=5; and b. http://www.canada.ca 1. Login to SOC Operator Server 2. In solution, verify the traffic captured	The solution should only capture HTTP outbound packets. HTTPS packets are not present.		
5.	C2M12, C2M33. The solution can provide data search capabilities in	1. Login to workstation, open IE browser, and navigate to the	Within the solution GUI:		

Case #	Description	Test Execution	Desired Outcome	Actual Result	PASS / FAIL
	support of network forensics and incident handling. All data searches/queries and/or meta-indexing must be achievable within 120 seconds based on a search across all data collected for the past one (1) day from time of search. Note: Testing requirement updated based on one (1) day of retention. The RFP mandatory requirement for retention period is not feasible due to testing being conducted over 1-2 days.	following websites: a. http://www.canada.ca/en.html; b. http://www.canada.ca/en/contact.html; c. http://www.canada.ca/en/government/system.html; and d. http://open.canada.ca/en?_ga=1.161942908.1908648822.1449089745 2. Open Chrome browser, and navigate to the following websites: a. http://www.canada.ca/en.html; b. http://www.canada.ca/en/contact.html; c. http://www.canada.ca/en/government/system.html; and d. http://open.canada.ca/en?_ga=1.161942908.1908648822.1449089745 3. Open Windows Outlook, and create/send the following emails: a. Email 1: *Recipient: testuser2@foo.local* *Subject: "Hello World"*	• 10a: Results should only contain IE with "canada" in the body • 10b: Results contain both IE and Chrome user agents with "canada.ca" in the URL • 10c: Results should only return Chrome traffic • 10d: One (1) result from Email 1 • 10e: One (1) result from Email 1 • 10f: One (1) result from Email 3 • 10g: At least 3 results from Email 1, Email 2, and Email 3. May also include results from		

Case #	Description	Test Execution	Desired Outcome	Actual Result	PASS / FAIL
		Body: "Did you get my project proposal? It's due next week." *Attachment: "test.docx"* b. Email 2: *Recipient: testuser3@foo.local* *Subject: "Monday Morning!"* *Body: "Let's work on our project proposal. We need to get it done this week."* *Attachment: "test2proposal.docx"* c. Email 3: *Time: To be sent a half hour after Email 1 and Email 2* *Recipient(s): testuser1@foo.local; testuser2@foo.local* *Subject: "Strategic Planning."* *Body: "Attachment is completed. Please review. I had help from Jake. His email is*	previous test cases. • 10h: Results only contain traffic from source IP "172.16.16.x" • 10i: Results only contain traffic from source ports 443 and 7016		

Case #	Description	Test Execution	Desired Outcome	Actual Result	PASS / FAIL
		Jake@foo.local" *Attachment: "test2proposal.docx"* 4. Login to SOC Operator Server. 5. In solution, conduct the following searches: a. (10a) Webpage body contains "*canada*" AND user agent equals to IE b. (10b) URL contains "*canada.ca"* c. (10c) Any traffic not using IE as the user agent d. (10d) Subject line equals "*Hello World"* e. (10e) Recipient equals testuser2@foo.local AND Body contains "*proposal"* f. (10f) Timeframe is within the last half hour AND attachment title contains "*tes*.doc"* g. (10g) Wildcard search for "**@foo.local"* h. (10h) Source IP contains *"172.16.16.x"*			

Case #	Description	Test Execution	Desired Outcome	Actual Result	PASS / FAIL
		i. (10i) Source ports contains 443, 7016			
6.	C2M13. The solution must provide data export and import capabilities using PCAP format.	1. Login to Workstation, open IE browser and navigate to bandwidth heavy webpages 2. Login to SOC Operator Server 3. In solution, export last 10 GB of raw capture traffic in PCAP format and save to Desktop as "export.pcap" 4. Import data from "import.pcap" in the solution	• The solution can successfully import "import.pcap" • The solution can successfully export 10 GB of raw traffic • The "export.pcap" can be imported and read by Wireshark		
7.	C2M15. Solution must be able to decode compressed traffic at web traffic level HTTP content coding (application layer) from the following compression scheme including GZIP based on the DEFLATE algorithm. For example: Web server compressing HTML code to web browser	1. Login to Workstation, open IE browser, and navigate to http://www.foo.local/bigpage.html 2. Login to SOC Operator Server 3. In solution, test the reconstruction of the compressed webpage	The solution GUI should be able to reconstruct the compressed webpage and display in human readable format.		
8.	C2M16. Solution must provide a Network Threat Intelligence service that is updated by the vendor at	1. Ensure proxy configuration has been disabled 2. Login to Workstation, open IE	The solution GUI should automatically flag the destination		

Case #	Description	Test Execution	Desired Outcome	Actual Result	PASS / FAIL
	least once per week (see SOW for details). Intelligence service must provide at a minimum: • Ability to flag traffic to or from suspected infected web servers (based on either URL or IP). • Ability to flag traffic to or from TOR exit points. • Ability to flag traffic generated from known malware applications.	browser and navigate to a known TOR exit point via https. Valid as of testing date and agreed between OEM and Crown testers. 3. Login to SOC Operator Server 4. In the solution, verify the traffic	as TOR.		
9.	C2M35. For network session reconstruction that contains text data, the reconstruction process must be compatible with displaying Unicode character sets and displaying them. The solution must be compatible with both alphabetic and logogram languages, and be able to display the reconstructed text in the associated	1. Login to Workstation, open IE browser and navigate to http://chinese.korea.net/index.jsp. 2. Once page has completely loaded, login to SOC Operator Server 3. In solution, reconstruct the traffic	In the solution GUI, the reconstructed traffic should be similar to the site that is directly viewed on a browser. The language and layout should be correctly displayed.		

Case #	Description	Test Execution	Desired Outcome	Actual Result	PASS / FAIL
	language. At a minimum network sessions containing the following languages must be decoded by the solution: • English • Mandarin				
10.	C2M38. The solution is able to associate all Source IP and Destination IP addresses to a geographic country location.	1. Login to the Workstation, open IE browser, and navigate to the following four (4) websites: a. http://www.apnic.net (Asia); b. http://www.enisa.europa.eu (Europe); c. http://www.afrinic.net (Africa); and d. http://www.google.com (North America) 2. Once all websites have fully loaded, login to SOC Operator Server 3. In solution, locate the traffic and identify the geographic locations of each IP address	The solution GUI should correctly show geographic information of the websites.		
11.	C2M39. The solution must be able to add a custom	3. Login to SOC Operator Server. In solution, assign tag “Lab Box” to IP	The solution GUI should show the tag		

Case #	Description	Test Execution	Desired Outcome	Actual Result	PASS / FAIL
	descriptive tag to private internal IP addresses.	address of the Workstation 4. Login to the Workstation, open IE browser, and navigate to www.google.com 5. Login to SOC Operator Server 6. In solution, locate the Internal traffic and verify tag	of the Workstation IP as “Lab Box”.		
12.	C2M41. The solution must be able to reconstruct and display the entire web page as part of the session recreation (excluding encrypted content).	1. Login to Workstation, open IE browser and navigate to the following websites: a. http://www.cra-arc.gc.ca/E/pbg/tf/rc66/README.html ; and b. http://www.cra-arc.gc.ca/E/pbg/tf/rc66/rc66-15e.pdf 2. Once both pages have completely loaded, login to SOC Operator Server 3. In solution, reconstruct the sessions and display the web pages Note: if the URLs are no longer active at the time of testing, they can be replaced with comparable alternatives.	• SOC Operator should be able to view the reconstructed webpages in *.HTML* format from the solution console. • The SOC Operator should be able to view the reconstructed *.PDF* file from the solution console. The contents should match the webpages displayed on the workstation.		
13.	C2M42. Ability to reconstruct files from captured traffic and	**5a:** 1. Login to Workstation	• 5a: In solution, SOC Operator should be able to		

Case #	Description	Test Execution	Desired Outcome	Actual Result	PASS / FAIL
	provides the ability to download the reconstructed files. At a minimum, the following files must be able to be reconstructed: • (5a) Files attached to SMTP emails; and • (5b) Files transferred using FTP.	2. Launch Microsoft Mail, and ensure the Inbox is up to date by clicking the "Send/Receive" button 3. Confirm that the email from testuser2@foo.local has been received with attachment 4. Login to SOC Operator Server 5. In solution, reconstruct the SMTP session and download the email message **5b:** 1. Login to Workstation 2. Launch an FTP session to the Application server 3. Once FTP session has been initiated, transfer the "test.txt" file into a directory on the Application server using the "put" command 4. Logout of FTP session 5. Login to SOC Operator Server 6. In solution, reconstruct the FTP session and download the "test.txt" file	reconstruct the SMTP session and view the email contents including opening the word document. The contents must match the test scenario. • 5b: In solution, SOC Operator should be able to reconstruct the FTP session and open the text file. The contents must match the test scenario.		