Government of Canada Managed Security Service (GCMSS)

Annex A-2: Statement of Work - Intrusion Detection & Prevention (IDP)

Date: July 12, 2012

TABLE OF CONTENTS

REFERENCE

Please refer to Annex A - Appendix C: Definitions and Acronyms for a definition of terms and acronyms utilized throughout this annex.

1 INTRUSION DETECTION & PREVENTION (IDP)

(1) The Intrusion Detection & Prevention is one of the GCMSS Threat Managed Services. When ordered by Canada, by issuing a Task Authorization, the IDP, as managed and implemented by the Contractor, must meet or exceed all of the requirements listed in this annex, in the balance of the SOW and elsewhere in the Contract prior to acceptance by Canada and during the entire period of the Contract.

1.1 Detection and Response

(2) The IDP must scan incoming and outgoing packets.

(3) The IDP must scan inside encapsulated packets.

(4) The IDP must detect intrusion events in real time.

(5) The IDP must have a fuzzy hashing-based intrusion prevention system.

(6) The IDP must have a Signature-based intrusion prevention system.

(7) The IDP must have a Statistical Anomaly-based intrusion prevention system.

(8) The IDP must detect and mitigate Denial of Service (DoS) attacks.

(9) The IDP must be Common Vulnerabilities and Exposures (CVE) compatible.

(10) The IDP must support external profile-based Intrusion Detection & Prevention Sensors including:

a) seamless integration of the sensors;

b) enabling sensors;

c) configuring sensors;

d) accepting reports from sensors;

e) monitoring multiple sensors;

f) identifying events from sensor reports; and

g) transmitting commands to sensors to respond to events.

(11) The IDP must support a variety of prevention techniques including at minimum:

a) droppacket; and

b) tcp-reset.

(12) The IDP must support Stateful Operation (session aware) including:

a) TCP Reassembly;

b) IP Defragment;

c) Bi-directional Inspection;

d) Forensic Data Collection; and

e) Access Lists.

(13) The IDP must inspect web traffic consisting of HTML 5 and below.

(14) The IDP must block HTTP/HTTPS requests to a URL longer than a value specified by Canada.

(15) The IDP must have a configurable “Silent” mode where no message is issued when blocking requests.

(16) The IDP fail-safe state must be configurable to open or close as specified by Canada.

1.2 Configuration

(17) The IDP must support response configuration on a per signature basis.

(18) The IDP must support scanning exclusion configuration on a per host basis.

(19) The IDP must support scanning exclusion configuration on a per signature basis.

(20) The IDP must support definition of signatures with Regular Expressions.

(21) The IDP must support configuration of the maximum URL length.

(22) The IDP must support configuration of customized signatures.

(23) The IDP must support the following configurations:

a) Out of Band in IDS mode (traffic stream via network TAP);

b) In-band in IPS mode utilizing a bridge mode (acts as a Layer 2 device without any requirements of IP addresses); and

c) In-band in IPS mode in routed mode (traffic is routed through device at the TCP/IP layer).

(24) The IDP must support configuration of the IDP response for a signature.

1.3 Automatic Security Updates

(25) The IDP must support automatic security updates directly over the public Internet (i.e. no dependency of any intermediate device) at maximum every hour.

(26) The Contractor must provide automatic security updates within 15 minutes of availability from their supplier.

(27) The IDP must apply security updates without rebooting within 15 minutes of receiving the updates.

1.4 Network Protocols

(28) The IDP must monitor protocols including, but not limited to:

a) TCP/IP;

b) ICMP;

c) FTP;

d) UDP;

e) SMTP;

f) HTTP/HTTPS;

g) SNMP;

h) DNS;

i) RPC;

j) NetBIOS; and

k) Telnet.

(29) The IDP must monitor MPLS traffic.

(30) The IDP must monitor 802.1Q (trunked) traffic.

1.5 IDP Sensor

(31) The IDP Sensor must support the following platforms:

a) Microsoft Windows Server 2003 and above;

b) Solaris (SPARC);

c) SUSE Linux Server;

d) Red Hat Enterprise Linux;

e) HP-UX;

f) AIX;

g) other operating systems as agreed to between Canada and the Contractor; and

h) the OEM dedicated hardware appliance.

(32) The IDP Sensor must perform:

a) log analysis;

b) file integrity checking;

c) root kit detection;

d) time-based alerting;

e) detection of policy violations;

f) active response according to policies violated; and

g) reporting back to the IDP.

(33) The IDP Sensor on OEM dedicated hardware appliance must:

a) support the Wire Speed of the Threat Management Capacity; and

b) be fully managed by the Contractor.

1.6 Logging

(34) The IDP must log event packets with all the associated IDP metadata.

1.7 Reporting

1.7.1 Monthly Reports

(35) The Contractor must provide a monthly IDP management report to Canada per Client Organization that includes:

a) an executive summary comparing the number of events in the current month with the previous month, explaining in plain terms the differences and the drivers behind these statistics;

b) number of Incident Ticket of type “request for information” with pending status;

c) a problem management summary in tabular format;

i) Incident Ticket status (open, closed, pending); and

ii) number of Incident Ticket;

d) number of Change Requests processed;

e) a list of Incident Ticket of Incident type “request for information” in tabular format;

i) date closed;

ii) date created;

iii) Ticket number;

iv) Incident severity;

v) Incident description;

vi) comments;

vii) Incident status;

viii) time to respond (in seconds); and

ix) time to contain (in seconds);

f) a list of Change Request Tickets in tabular format;

i) Ticket number;

ii) change description;

iii) comments; and

iv) status.

1.7.2 Daiy Reports

(36) The Contractor must provide a daily IDP report by sensor to Canada in tabular and graphical format per Client Organization that includes:

a) an event summary in bar-chart format for the top 5 sensors;

i) total number of events for the sensor on the x axis; and

ii) sensor name on the y axis;

b) a top 50 event summary in tabular format;

i) sensor;

ii) event detail;

iii) event severity; and

iv) number of events.

(37) The Contractor must provide a daily IDP report by severity to Canada in tabular and graphical format per Client Organization that includes:

a) an event summary, for the previous 2 weeks, in stacked column-chart format;

i) event date on the x axis; and

ii) total number of events by event severity stacked on the y axis;

b) an event summary, for the previous 2 weeks, in tabular format;

i) event date;

ii) event severity; and

iii) number of events.

(38) The Contractor must provide a daily IDP report by source IP to Canada in tabular and graphical format per Client Organization that includes:

a) an event summary in bar-chart format for the top 5 source IPs;

i) total number of events for the source IP on the x axis; and

ii) source IP on the y axis;

b) a top 50 event summary in tabular format;

i) source IP;

ii) event detail;

iii) event severity; and

iv) number of events.

(39) The Contractor must provide a daily IDP report by target IP to Canada in tabular and graphical format per Client Organization that includes:

a) an event summary in bar-chart format for the top 5 target IPs;

i) total number of events for the target IP on the x axis; and

ii) target IP on the y axis;

b) a top 50 event summary in tabular format;

i) target IP;

ii) event detail;

iii) event severity; and

iv) number of events.

1.8 Implementation

(40) The Contractor must inventory, review, optimize and implement in GCMSS existing rules, policies, and any other configuration of the existing IDP solution of the Client Organization.

(41) The Contractor must document, review, optimize and implement in GCMSS configuration requirements of the Client Organization for the IDP.

(42) The Contractor must install hardware IDP Sensor as requested by Canada in a Task Authorization within the SL-TAR.

1.9 Change Management

(43) The Contractor must configure signature specific IDP responses, as requested by Canada, in accordance with priority levels as specified by Canada.

(44) The Contractor must configure scanning exclusions for hosts and signatures, as requested by Canada, in accordance with priority levels as specified by Canada.

(45) The Contractor must configure signature specific exceptions, as requested by Canada, in accordance with priority levels as specified by Canada.

(46) The Contractor must configure threat signatures, as requested by Canada, in accordance with priority levels as specified by Canada.

(47) The Contractor must configure IDP Sensors, as requested by Canada, in accordance with priority levels as specified by Canada.