Government of Canada Managed Security Service (GCMSS)

Annex A-7: Statement of Work - Security Information and Event Management (SIEM)

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 SECURITY INFORMATION AND EVENT MANAGEMENT SERVICE (SIEM)

(1) The Security Information and Event Management is one of the GCMSS Threat Management Services. When ordered by Canada, by issuing a Task Authorization, the SIEM, 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 Data Collection

(2) The SIEM must collect events, security logs and operational logs (CPU and RAM utilization, etc.) simultaneously from a wide range of sources including:

a) routers;

b) switches;

c) firewalls;

d) IDS/IPS;

e) databases;

f) web servers;

g) Antivirus/Antispam agents;

h) Syslog servers;

i) Internet Proxy Server;

j) Mail Gateways and MTA;

k) vulnerability scanners;

l) asset scanners;

m) Security Incidents scanners;

n) GCMSS Threat Management Services;

o) VPN and remote access devices;

p) wireless access points and sensors;

q) Windows Server 2003 and above;

r) Solaris;

s) IBM-AIX;

t) HP-UX;

u) Unix;

v) Linux (Redhat); and

w) all other sources agreed to between the Contractor and Canada.

(3) The SIEM must collect data using one or more of the following methods:

a) agent collector on the source device;

b) direct connection to the source device;

c) log file collection; and

d) all other methods agreed to between the Contractor and Canada.

(4) The SIEM must support NAT Traversal to enable collection of events beyond NAT boundaries.

(5) The SIEM must normalize the collected raw data into a common data structure in a common Client Organization specific repository.

(6) The SIEM must keep a copy of the collected raw data.

(7) The SIEM must keep a link between the normalized data and the collected raw data.

(8) The SIEM must not drop incoming raw data.

(9) The SIEM must store the data on a storage area network specified by Canada for the Client Organization.

1.2 Detection and Response

(10) The SIEM must correlate the normalized data based on rules specified by Canada.

(11) The SIEM must analyze incoming data and compare it against normal behaviours rules/policies and alert of any deviations.

(12) The SIEM must analyze incoming data and compare it against customized normal behaviours rules/policies specified by Canada and alert of any deviations.

(13) The SIEM must analyze incoming data and automatically build normal behaviours policies/rules based on observed events.

(14) The SIEM must correlate the operations alerts with the security alerts originating from a common source.

1.3 Configuration

(15) The SIEM must allow for the configuration of custom normal behaviours rules/policies.

(16) The SIEM must have configurable data retention and archival periods.

1.4 Automatic Security Updates

(17) The SIEM must support automatic security updates of rules/policies directly over the public Internet (i.e. no dependency of any intermediate device) at maximum every hour.

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

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

1.5 Events and Logs Collection Protocols

(20) The SIEM must support events and logs collection protocols including:

a) Syslog;

b) Microsoft RPC;

c) Cisco RDEP;

d) OPSEC LEA;

e) SNMP Traps;

f) HTTP; and

g) HTTPS;

h) Microsoft WMI;

i) SDEE;

j) NetFlow v9 and above;

k) IPFIX;

l) Windows event log; and

m) all other events and logs collection protocols agreed to between the Contractor and Canada.

1.6 Security

(21) The SIEM must protect the confidentiality and the integrity of the collected raw data and the normalized data at all time.

(22) The SIEM must store the collected raw data and the normalized data on Client Organization premises.

1.7 Reporting

(23) The SIEM must provide pre-built compliance reports (HIPPA, Sarbanes Oxley, etc).

1.7.1 Monthly Reports

(24) The Contractor must provide a monthly SIEM 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 Daily Reports

(25) The Contractor must provide a daily SIEM report by source device 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 devices;

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

ii) source device name on the y axis;

b) a top 50 event summary in tabular format;

i) source device;

ii) event detail;

iii) event severity; and

iv) number of events.

(26) The Contractor must provide a daily SIEM 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;

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.

(27) The Contractor must provide a daily SIEM 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.

(28) The Contractor must provide a daily SIEM 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 Management Services

1.8.1 Change Management

(29) The Contractor must configure the data retention and archival periods, as requested by Canada, in accordance with priority levels as specified by Canada.

(30) The Contractor must enable and disable policies/rules, as requested by Canada, in accordance with priority levels as specified by Canada.

1.8.2 Incident Management

(31) The Contractor must log alerts from the SIEM as Security Incidents.