

**IBM Managed Security Services
for
Security Event and Log Management - Standard**

Table of Contents

| | | |
|-----------|---|-----------|
| 1. | Scope of Services | 4 |
| 2. | Definitions..... | 4 |
| 3. | MSS for Security Event and Log Management – Standard Features..... | 4 |
| 3.1 | Security Operations Centers | 5 |
| 3.2 | Portal..... | 5 |
| 3.2.1 | IBM Responsibilities | 5 |
| 3.2.2 | Customer Responsibilities | 5 |
| 3.3 | Customer Contacts..... | 5 |
| 3.3.1 | IBM Responsibilities | 5 |
| 3.3.2 | Customer Responsibilities | 6 |
| 3.4 | Security Intelligence | 7 |
| 3.4.1 | IBM Responsibilities | 7 |
| 3.4.2 | Customer Responsibilities | 8 |
| 3.5 | Deployment and Activation..... | 8 |
| 3.5.1 | IBM Responsibilities | 8 |
| 3.5.2 | Customer Responsibilities | 12 |
| 3.6 | Collection and Archival..... | 13 |
| 3.6.1 | IBM Responsibilities | 14 |
| 3.6.2 | Customer Responsibilities | 14 |
| 3.7 | OA Health and Availability Monitoring | 15 |
| 3.7.1 | IBM Responsibilities | 15 |
| 3.7.2 | Customer Responsibilities | 15 |
| 3.8 | OA Management..... | 16 |
| 3.8.1 | IBM Responsibilities | 16 |
| 3.8.2 | Customer Responsibilities | 16 |
| 3.9 | Security Reporting..... | 16 |
| 3.9.1 | IBM Responsibilities | 16 |
| 3.9.2 | Customer Responsibilities | 17 |
| 4. | Optional Services | 17 |
| 4.1 | Out-of-Band Access | 17 |
| 4.1.1 | IBM Responsibilities | 17 |
| 4.1.2 | Customer Responsibilities | 17 |
| 4.2 | Customer Ticket System Integration | 18 |
| 4.2.1 | IBM Responsibilities | 18 |
| 4.2.2 | Customer Responsibilities | 18 |
| 4.3 | Security Event and Log Delivery | 18 |
| 4.3.1 | IBM Responsibilities | 18 |
| 4.3.2 | Customer Responsibilities | 18 |
| 5. | Service Level Agreements..... | 18 |
| 5.1 | SLA Availability | 18 |
| 5.2 | SLA Remedies | 19 |
| 5.3 | SLA Exclusions and Stipulations | 19 |
| 5.3.1 | SLA Compliance and Reporting | 19 |
| 5.3.2 | Scheduled and Emergency Portal Maintenance | 19 |
| 5.3.3 | Customer Contact Information | 19 |
| 5.3.4 | Customer Network/Server Change Notifications | 19 |

| | | |
|-----------|---|-----------|
| 5.3.5 | Network Traffic Applicable to SLAs | 20 |
| 5.3.6 | Policy Change Request Overages | 20 |
| 5.3.7 | Services Decommission or Turn-Down | 20 |
| 5.3.8 | Testing of Monitoring and Response Capabilities | 20 |
| 6. | Other Terms and Conditions..... | 20 |
| 6.1 | Modification of Services | 20 |
| 6.2 | Data Compilation..... | 20 |
| 6.3 | Customer General Responsibilities | 21 |
| 6.4 | Mutual Responsibilities..... | 21 |

Services Description

IBM Managed Security Services for Security Event and Log Management - Standard

1. Scope of Services

IBM Managed Security Services for Security Event and Log Management - Standard (called “MSS for Security Event and Log Management - Standard” or “Services”) is designed to provide a security-enhanced Web-based solution for the collection, consolidation, analysis and archiving of security event and log data from supported devices (called “Agents”).

The Services features described herein are dependent upon the availability and supportability of products being utilized. This includes both IBM-provided and Customer-provided hardware, software, and firmware.

The details of Customer’s order (for example, the contract period and charges) will be specified in an Order.

2. Definitions

- a. network intrusion detection and intrusion prevention system (“IDS/IPS”)

IDS/IPS is a network security device that employs detection and prevention techniques to monitor network activities for malicious or unwanted behavior. Such monitoring may identify and, in some cases, block possible security breaches in real-time.

- b. firewall (“FW”)

FW is a network security device that is designed to block unauthorized access and allow authorized communications based on a configuration of allow, deny, encrypt, decrypt, or proxy rules aligned with Customer’s security policy.

- c. Alert Condition (“AlertCon”) – a global risk metric developed by IBM, using proprietary methods.

The AlertCon is based on a variety of factors, including quantity and severity of known vulnerabilities, exploits for such vulnerabilities, availability of such exploits to the public, mass-propagating worm activity, and global threat activity. The four levels of AlertCon are described in the IBM MSS Customer portal (called “Portal”).

3. MSS for Security Event and Log Management – Standard Features

The following table highlights the measurable Services features of MSS for Security Event and Log Management - Standard. The subsequent sections provide narrative descriptions of each Services feature.

Services Feature Summary

| Services Feature | Metric or Qty | Service Level Agreements |
|--|---|---|
| Services availability | 100% | Services availability SLA |
| IBM MSS Portal availability | 99.9% | IBM MSS Portal availability SLA |
| Internet emergency | N/A | N/A |
| Authorized Security Contacts | 3 users | N/A |
| Log/event archival | 5 Gb/year for each year of the contract (up to 7 years) | N/A |
| OA health alerting | 30 minutes | System monitoring SLA |

3.1 Security Operations Centers

IBM Managed Security Services (“MSS”) are delivered from a network of IBM Security Operations Centers (“SOCs”). IBM will provide Customer with access to the SOCs 24 hours/day, 7 days/week.

3.2 Portal

The Portal provides Customer with access to an environment (and associated tools) designed to monitor and manage its security posture by merging technology and service data from multiple vendors and geographies into a common, Web-based interface.

3.2.1 IBM Responsibilities

IBM will:

- a. provide access to the Portal 24 hours/day, 7 days/week. The Portal will provide Customer with:
 - (1) security intelligence awareness and alerting;
 - (2) security incident and service ticket information;
 - (3) ticketing and workflow initiation and updates;
 - (4) live chat and collaboration with SOC analysts;
 - (5) a template-driven reporting dashboard;
 - (6) access to real-time and archived Agent logs and events;
 - (7) authorization to download log data; and
 - (8) granular security event and log query capabilities; and
- b. maintain availability of the Portal in accordance with the metrics provided in the section of this Services Description entitled “Service Level Agreements”, “Portal Availability”.

3.2.2 Customer Responsibilities

Customer agrees to:

- a. utilize the Portal to perform daily operational Services activities;
- b. appropriately safeguard its login credentials to the Portal (including not disclosing such credentials to any unauthorized individuals.);
- c. promptly notify IBM if a compromise of its login credentials is suspected; and
- d. indemnify and hold IBM harmless for any losses incurred by Customer or other parties resulting from Customer’s failure to safeguard its login credentials.

3.3 Customer Contacts

Customer may choose from multiple levels of access to the SOC and the Portal to accommodate varying roles within its organization.

Authorized Security Contacts

An Authorized Security Contact is defined as a decision-maker on all operational issues pertaining to MSS.

Designated Customer Contacts

A Designated Customer Contact is defined as a decision-maker on a subset of operational issues pertaining to an IBM Managed Security Service, an Agent, or a group of Agents. IBM will only interface with a Designated Customer Contact regarding operational activities that fall within the subset for which such contact is responsible (for example, designated Agent outage contact).

Portal Users

IBM provides multiple levels of access for Portal users. These levels of access can be applied to an IBM Managed Security Service, an Agent, or a group of Agents. Portal users will be authenticated via static password or Customer-provided public-key encryption technology (for example, RSA SecureID token) based on Customer requirements.

3.3.1 IBM Responsibilities

Authorized Security Contacts

IBM will:

- a. allow Customer to create up to three Authorized Security Contacts;
- b. provide each Authorized Security Contact with:
 - (1) administrative Portal permissions to Customer Agents;
 - (2) the authorization to create unlimited Designated Customer Contacts and Portal users;
 - (3) the authorization to delegate responsibility to Designated Customer Contacts;
- c. interface with Authorized Security Contacts regarding support and notification issues pertaining to the Services; and
- d. verify the identity of Authorized Security Contacts using an authentication method that utilizes a pre-shared challenge pass phrase.

Designated Customer Contacts

IBM will:

- a. verify the identity of Designated Customer Contacts using an authentication method that utilizes a pre-shared challenge pass phrase; and
- b. interface only with Designated Customer Contacts regarding the subset of operational issues for which such contact is responsible.

Portal Users

IBM will:

- a. provide multiple levels of access to the Portal:
 - (1) administrative user capabilities which will include:
 - (a) creating Portal users;
 - (b) creating and editing custom Agent groups;
 - (c) submitting Services requests to the SOCs;
 - (d) “live chat” communicating with SOC analysts regarding specific incidents or tickets, generated as part of the Services;
 - (e) creating internal Services-related tickets and assigning such tickets to Portal users;
 - (f) querying, viewing, and updating Services-related tickets;
 - (g) viewing and editing Agent details;
 - (h) viewing Agent policies (if applicable);
 - (i) creating and editing vulnerability watch lists;
 - (j) performing live event monitoring;
 - (k) querying security event and log data;
 - (l) scheduling downloads of security event and log data;
 - (m) scheduling and running reports;
 - (2) regular user capabilities which will include all of the capabilities of an administrative user, for the Agents to which they have been assigned, with the exception of creating Portal users;
 - (3) restricted user capabilities which will include all of the capabilities of a regular user, for the Agents to which they have been assigned, with the exception of:
 - (a) creating and submitting policy change requests;
 - (b) updating tickets; and
 - (c) editing Agent details;
- b. provide Customer with authorization to apply levels of access to an Agent or groups of Agents;
- c. authenticate Portal users using static password; and
- d. authenticate Portal users using a Customer-provided public-key encryption technology (for example, RSA SecureID token) based on Customer requirements.

3.3.2 Customer Responsibilities

Authorized Security Contacts

Customer agrees:

- a. to provide IBM with contact information for each Authorized Security Contact. Such Authorized Security Contacts will be responsible for:
 - (1) creating Designated Customer Contacts and delegating responsibilities and permissions to such contacts, as appropriate;
 - (2) creating Portal users;
 - (3) authenticating with the SOCs using a pre-shared challenge pass phrase; and
 - (4) maintaining notification paths and Customer contact information, and providing such information to IBM;
- b. to ensure at least one Authorized Security Contact is available 24 hours/day, 7 days/week;
- c. to update IBM within three calendar days when Customer contact information changes; and
- d. and acknowledges that it is permitted to have no more than three Authorized Security Contacts regardless of the number of IBM services or Agent subscriptions for which Customer has contracted.

Designated Customer Contacts

Customer agrees:

- a. to provide IBM with contact information and role responsibility for each Designated Customer Contact. Such Designated Customer Contacts will be responsible for authenticating with the SOCs using a pass phrase; and
- b. and acknowledges that a Designated Customer Contact may be required to be available 24 hours/day, 7 days/week based on the subset of responsibilities for which it is responsible (i.e., Agent outage).

Portal Users

Customer agrees:

- a. that Portal users will use the Portal to perform daily operational Services activities;
- b. to be responsible for providing IBM-supported RSA SecureID tokens (as applicable); and
- c. and acknowledges the SOCs will only interface with Authorized Security Contacts and Designated Customer Contacts.

3.4 Security Intelligence

Security intelligence is provided by the IBM X-Force® Threat Analysis Center. The X-Force Threat Analysis Center publishes an Internet alert condition (called “AlertCon”) threat level. The AlertCon describes progressive alert postures of current Internet security threat conditions. In the event Internet security threat conditions are elevated to AlertCon 3, indicating focused attacks that require immediate defensive action, IBM will provide Customer with real-time access into IBM’s global situation briefing. As a user of the Portal, Customer has access to the X-Force Threat Analysis Service. The X-Force Threat Analysis Service includes access to the IBM X-Force Threat Insight Quarterly (“Threat IQ”).

Utilizing the Portal, Customer can create a vulnerability watch list with customized threat information. In addition, each Portal user can request to receive an Internet assessment email each business day. This assessment provides an analysis of the current known Internet threat conditions, real-time Internet port metrics data, and individualized alerts, advisories and security news.

3.4.1 IBM Responsibilities

IBM will:

- a. provide Customer with access to the X-Force Threat Analysis Service;
- b. provide Customer with a username, password, URL and appropriate permissions to access the Portal;
- c. display security information on the Portal as it becomes available;
- d. if configured by Customer, provide security intelligence specific to a Customer-defined vulnerability watch list, via the Portal;

- e. if configured by Customer, provide an Internet security assessment email each business day;
- f. publish an Internet AlertCon via the Portal;
- g. declare an Internet emergency if the daily AlertCon level reaches AlertCon 3. In such event, IBM will provide Customer with real time access into IBM's global situation briefing;
- h. provide Portal feature functionality for Customer to create and maintain a vulnerability watch list;
- i. provide additional information about an alert, advisory, or other significant security issue as IBM deems necessary; and
- j. provide the Threat IQ via the Portal.

3.4.2 Customer Responsibilities

Customer agrees to use the Portal to:

- a. subscribe to the daily Internet Security Assessment email, if desired;
- b. create a vulnerability watch list, if desired; and
- c. access the Threat IQ.

3.5 Deployment and Activation

During deployment and activation, IBM will work with Customer to deploy a new Agent.

3.5.1 IBM Responsibilities

Activity 1 - Project Kickoff

The purpose of this activity is to conduct a project kickoff call. IBM will send Customer a welcome email and conduct a kickoff call, for up to one hour for up to three Customer participants, to:

- a. identify Customer Point of Contact;
- b. introduce Customer Point of Contact to the assigned IBM deployment specialist;
- c. review IBM and Customer responsibilities;
- d. set schedule expectations; and
- e. begin to assess Customer's requirements and environment.

Completion Criteria:

This activity will be complete when IBM has conducted the kickoff call.

Deliverable Materials:

- None

Activity 2 - Network Access Requirements

The purpose of this activity is to establish network access requirements.

IBM will:

- a. provide Customer with a document called "Network Access Requirements", detailing:
 - (1) how IBM will connect remotely to Customer's network;
 - (2) specific technical requirements to enable such remote connectivity;
 Note: IBM may make changes to the "Network Access Requirements" document, as it deems appropriate, throughout the performance of the Services;
- b. connect to Customer's network through the Internet, using IBM standard access methods; and
- c. if appropriate, utilize a site-to-site virtual private network ("VPN") to connect to Customer's network. Such VPN will be provided by IBM for an additional charge as specified in an Order.

Completion Criteria:

This activity will be complete when IBM has provided Customer with the Network Access Requirements document.

Deliverable Materials:

- Network Access Requirements document

Activity 3 - Assessment

The purpose of this activity is to perform an assessment of Customer's current environment, and business and technology goals.

Task 1 - Gather Data

IBM will:

- a. provide Customer Point of Contact with a data gathering form on which Customer will be asked to document:
 - (1) team member names, contact information, roles and responsibilities;
 - (2) unique country and site requirements;
 - (3) Customer's existing network infrastructure;
 - (4) critical servers;
 - (5) number and type of end users; and
 - (6) key business drivers and/or dependencies that could influence Services delivery or timelines.

Task 2 - Assess Environment

IBM will:

- a. determine if Agent data collection will be implemented using the Universal Logging Agent ("ULA") or via SYSLOG; and
- b. if applicable, provide recommendations to adjust the policy of an Agent.

Completion Criteria:

This activity will be complete when IBM has assessed Customer's environment and existing Agent (as applicable).

Deliverable Materials:

- None

Activity 4 - Universal Logging Agent Implementation

The ULA is a software-based Agent that runs on an Agent subscribing to the Services, and collects text-based logs. The ULA gathers such logs locally from the Agent and forwards them to the onsite aggregator ("OA"). The OA then forwards the logs to the IBM infrastructure for collection, long term storage, and display in the Portal.

The basic functions of the ULA are to:

- Collect events/logs locally from the Agent;
- Compress the events/log data;
- Encrypt the events/log data; and
- Securely transmit the events/logs to the OA.

Core features of the ULA are to:

- a. perform generic text file data collection;
- b. perform event log collection;
- c. perform system information collection, which may include:
 - (1) operating system ("OS") version;
 - (2) memory;
 - (3) CPU;
 - (4) local user accounts;
 - (5) network interface details;
 - (6) running processes; and
 - (7) open network sockets;
- d. perform uni-directional log transmission. ULA communication is performed via outbound SSL/TCP-443 connections;

- e. perform message throttling, if configured. This limits the bandwidth from the ULA to the OA, in messages per second, to preserve bandwidth; and
- f. provide transmit windows, if configured. The transmit windows enable/disable event transmission to the IBM MSS infrastructure during the timeframe specified by Customer in the Portal.

Task 1 - Install the ULA

IBM will:

- a. provide Customer with a list of Agents that require ULA installation;
- b. provide Customer with instructions for downloading the ULA onto the Agent using the Web server that has been configured on the OA;
- c. provide Customer with instructions for specific auditing/system logging that must be enabled for the Agent to produce useful data feeds; and
- d. at Customer's request, and for an additional charge, provide physical installation services of the ULA.

Task 2 - Configure ULA

IBM will provide Customer with instructions on how to login to the Portal and confirm the Agent.

Completion Criteria:

This activity will be complete when IBM has provided Customer with a list of Agents requiring ULA installation.

Deliverable Materials:

- ULA installation instructions

Activity 5 - Agentless Collection Implementation

The purpose of this activity is to facilitate log collection in an Agentless fashion when it is not technically feasible to install the ULA on an Agent.

IBM will provide Customer with instructions for directing SYSLOG streams from the Agent to the OA.

Completion Criteria:

This activity will be complete when IBM has provided Customer with instructions for directing SYSLOG streams from the Agent to the OA.

Deliverable Materials:

- SYSLOG configuration instructions

Activity 6 - Onsite Aggregator Implementation

The purpose of this activity is to configure the OA.

The OA is a required Customer-provided device that is deployed at Customer's location and managed and monitored by IBM MSS for an additional charge, as specified in the Order.

The basic functions of the OA are to:

- compile or otherwise combine the security events and log data;
- compress the security events and log data; and
- encrypt the security events and log data and transmit to the IBM MSS Infrastructure.

Core features of the OA are to:

- perform local spooling by queuing the events locally when a connection to the IBM MSS infrastructure is not available;
- perform uni-directional log transmission. OA communication is performed via outbound SSL/TCP-443 connections;
- perform message throttling, if configured. This limits the bandwidth from the OA to the IBM MSS infrastructure, in messages per second, to preserve bandwidth; and
- provide transmit windows, if configured. The transmit windows enable/disable event transmission to the IBM MSS infrastructure during the timeframe specified by Customer in the Portal.

IBM strongly encourages Out-of-Band (“OOB”) access to the OA, as described in the section of this Services Description entitled “Out-of-Band Access”.

Task 1 - Configure the OA

IBM will:

- a. provide live support, via phone and email, and will assist Customer with the location of applicable vendor documents detailing the installation and configuration procedures for the OA operating system and IBM provided OA software. Such support must be scheduled in advance to ensure availability of an IBM deployment specialist;
- b. provide Customer with hardware specifications for the OA platform;
- c. provide Customer with OA software and configuration settings;
- d. provide Customer with telephone and email support to assist in the installation of the IBM-provided OA software on the Customer-provided hardware platform. Such support must be scheduled in advance to ensure availability of a deployment specialist;
- e. at Customer’s request, and for an additional charge, provide software installation services;
- f. for existing platforms:
 - (1) assess existing hardware configurations to ensure they meet IBM specification; and
 - (2) provide hardware upgrade specifications (as applicable).

Task 2 - Install the OA

IBM will:

- a. provide live support, via phone and email, assisting Customer with location of vendor documents detailing physical installation procedures and cabling of the OA. Such support must be scheduled in advance to ensure availability of an IBM deployment specialist;

Note: Customer may contract separately for IBM to provide physical cabling and installation services.

- b. remotely configure the OA to include registration of the OA with the IBM MSS infrastructure and begin the deployment and management takeover process of the OA; and
- c. confirm the IBM MSS infrastructure is receiving communication from the OA.

Completion Criteria:

This activity will be complete when the OA is installed and configured and IBM has confirmed the IBM MSS infrastructure is receiving communications from the OA.

Deliverable Materials:

- None

Activity 7 - Testing and Verification

The purpose of this activity is to perform testing and verification of the Services.

IBM will:

- a. verify connectivity of the Agent to the IBM MSS infrastructure;
- b. perform Services acceptance testing;
- c. verify delivery of log data from the Agent to the IBM MSS infrastructure;
- d. verify availability and functionality of the Agent in the Portal;
- e. perform quality assurance testing of the Agent; and
- f. remotely demonstrate the primary features of the Portal for up to ten Customer personnel, for up to one hour.

Completion Criteria:

This activity will be complete when IBM has verified availability and functionality of the Agent in the Portal.

Deliverable Materials:

- None

Activity 8 - Services Activation

The purpose of this activity is to activate the Services.

IBM will:

- a. assume support of the Agent;
- b. set the Agent to “active”;
- c. transition the Agent to the SOCs for ongoing support; and
- d. provide the Services 24 hours/day, 7 days/week.

Completion Criteria:

This activity will be complete when the Agent is set to “active”.

Deliverable Materials:

- None

3.5.2 Customer Responsibilities

Activity 1 - Project Kickoff

Customer agrees to:

- a. designate a Customer Point of Contact to whom all communications relative to the Services deployment will be addressed and who will have the authority to act on Customer’s behalf in all matters regarding the Services. The Customer Point of Contact will:
 - (1) attend the project kickoff call;
 - (2) serve as the interface between IBM’s deployment team and all Customer departments participating in the Services deployment;
 - (3) help resolve Services deployment issues, and escalate issues within Customer’s organization, as necessary; and
- b. review IBM and Customer responsibilities.

Activity 2 - Network Access Requirements

Customer agrees to:

- a. review and comply with the IBM “Network Access Requirements” document during deployment and throughout the term of the contract; and
- b. be solely responsible for any charges incurred as a result of IBM utilizing a site-to-site VPN to connect to Customer’s network.

Activity 3 - Assessment

Task 1 - Gather Data

Customer agrees to:

- a. complete and return any questionnaires and/or data gathering forms to IBM within five days of Customer’s receipt;
- b. obtain and provide applicable information, data, consents, decisions and approvals as required by IBM to perform the Services deployment, within two business days of IBM’s request;
- c. work in good faith with IBM to accurately assess Customer’s network environment;
- d. provide contacts within its organization, and specify a notification path through its organization in the event IBM must contact Customer; and
- e. update IBM within three calendar days when Customer contact information changes.

Task 2 - Assess Environment

No additional Customer responsibilities are required for this activity.

Activity 4 - Universal Logging Agent Implementation

Task 1 - Install the ULA

Customer agrees:

- a. to download the ULA software from the Web server that is hosted on the OA;
- b. to install the ULA on Agent(s) subscribing to the Service; and
- c. and acknowledges it is solely responsible for all ULA installation tasks.

Task 2 - Configure the ULA

Customer agrees:

- a. to configure the ULA with appropriate configuration settings and an IP address configured on OA,
- b. to configure the Agent with IBM-recommended auditing/system logging specifications (as needed);
- c. to login to the Portal and confirm the Agent within three business days of ULA installation and configuration; and
- d. and acknowledges it is solely responsible for all ULA configuration tasks.

Note: Customer may contract separately for IBM to provide physical installation and configuration services.

Activity 5 - Agentless Collection Implementation

Customer agrees to:

- a. configure the Agent to point SYSLOG streams to the OA under the guidance of IBM; and
- b. login to the Portal and confirm the Agent within three business days.

Activity 6 - Onsite Aggregator Implementation

Task 1 - Configure the OA

Customer agrees:

- a. to provide IBM with an external IP address for the OA;
- b. to provide hardware for the OA platform, based on IBM's recommendations and requirements;
- c. to maintain current licensing, and support and maintenance contracts for the OA;
- d. to install the IBM-provided OA software on the Customer-provided hardware, under the guidance of IBM;
- e. to configure an external IP address and associated settings on the OA;
- f. to provide IBM with the OA IP address, hostname, machine platform, application version, and Agent time zone; and
- g. for existing platforms, to make IBM-requested hardware upgrades.

Task 2 - Install the OA

Customer agrees to:

- a. be responsible for physical installation and cabling of the OA; and
- b. schedule live support with an IBM deployment specialist.

Note: Customer may contract separately for IBM to provide physical cabling and installation services.

Activity 7 - Testing and Verification

Customer agrees:

- a. to be responsible for development of all "Customer-specific" acceptance testing plans;
- b. to be responsible for performing acceptance testing of Customer applications and network connectivity; and
- c. and acknowledges that additional acceptance testing performed by Customer, or lack thereof, does not preclude IBM from setting the Agent to "active" in the SOCs for ongoing support.

Activity 8 - Services Activation

No additional Customer responsibilities are required for this activity.

3.6 Collection and Archival

IBM utilizes the X-Force Protection System for collecting, organizing, archiving and retrieving security event and log data. The Portal provides Customer with a 24 hours/day, 7 days/week view into the

Services, including online access to raw logs collected and stored within the X-Force Protection System infrastructure. Security event and log data will be viewable online in the Portal for one year. At the end of the one year period, the data will be transitioned to offline storage (if applicable).

The Services provide up to five Gb of storage space for each year of the contract term. On day one of the contract, IBM will make available the total storage space based on the contract term (5 Gb x n where "n" equals contract term). Additional storage space may be purchased for an additional charge, as specified in the Order.

3.6.1 IBM Responsibilities

IBM will:

- a. collect log and event data generated by the managed Agent as such data reaches the IBM MSS infrastructure;
- b. throttle log and event data streams generated by the managed Agent when such data streams exceed 100 events per second ("EPS");
- c. uniquely identify collected log and event data;
- d. archive collected data in its native format in the X-Force Protection System;
- e. provide storage for up to five Gb of collected log and event data for each year of the contract term;
- f. display collected log and event data in the Portal for one year;
- g. where supported, normalize the log and event data for enhanced presentation in the Portal;
- h. begin purging collected log and event data using a first in, first out ("FIFO") method:
 - (1) based on Customer-defined retention periods;
 - (2) when Customer storage space has been exceeded; or
 - (3) when the log and event data age has exceeded seven years.

Note: Notwithstanding any Customer-defined retention periods, IBM will not retain log and event data for more than seven years. If Customer exceeds its total storage space or its seven year retention period at any time during the contract period, IBM will begin purging the collected log and event data using the FIFO method.

3.6.2 Customer Responsibilities

Customer agrees:

- a. to provide IBM with security event and log retention periods not to exceed five Gb of storage space for each year of the contract term;
- b. to use the Portal to review and query security event and log data;
- c. to use the Portal to maintain available log and event storage space awareness;
- d. to ensure an active MSS for Security Event and Log Management - Standard contract is being maintained for each unique security event and log source;

Note: If the Services are terminated for any reason whatsoever, IBM will be relieved of its obligation to store Customer's security event and log data.

- e. and acknowledges that:
 - (1) all log and event data will be transmitted to the SOCs via the Internet;
 - (2) data traveling across the Internet is encrypted using industry-standard strong encryption algorithms whenever possible;
 - (3) IBM can only collect and archive log and event data that successfully reaches the IBM MSS infrastructure;
 - (4) IBM does not guarantee the legal submission of any security event or log data into any domestic or international legal system. Admissibility of evidence is based on the technologies involved and Customer's ability to prove proper data handling and chain of custody for each set of data presented;
 - (5) IBM has the right to throttle event streams generated by the Agent that exceed 100 EPS (if required);

- (6) IBM will begin purging data using a FIFO method when collected log and event data exceeds allocated storage space;
- (7) IBM will not store log and event data for more than seven years; and
- (8) Customer-defined retention periods may not exceed seven years. IBM will begin purging data using the FIFO method when collected log and event data exceeds seven years, regardless of Customer-specified retention periods.

3.7 OA Health and Availability Monitoring

IBM will monitor the health status and availability of the OA. Such monitoring is designed to assist in increasing availability and uptime of the OA.

3.7.1 IBM Responsibilities

Activity 1 - Agent-Based Monitoring

The purpose of this activity is to monitor the health and performance of the OA.

IBM will:

- a. install monitoring software on the OA;
- b. analyze and respond to key metrics, which may include:
 - (1) hard disk capacity;
 - (2) CPU utilization;
 - (3) memory utilization; and
 - (4) process availability; and
- c. respond to alerts generated by the monitoring software.

Activity 2 - Troubleshooting

The purpose of this activity is to perform research and investigation if the OA does not perform as expected or a potential OA health issue is identified.

IBM will:

- a. create a trouble ticket in the event of an OA performance problem or potential OA health issue;
- b. begin research and investigation of the documented issue;
- c. if the OA is identified as the potential source of a network-related problem, examine the OA configuration and functionality for potential issues; and
- d. display the OA health and outage ticket in the Portal.

Activity 3 - Notification

The purpose of this activity is to notify Customer if the OA becomes unreachable through standard in-band means.

IBM will:

- a. notify Customer if the OA becomes unreachable through standard in-band means. Such notification will be via telephone using a predetermined notification procedure within the timeframe established in the section of this Services Description entitled "Service Level Agreements", "Proactive system monitoring";
- b. begin investigation of problems related to the configuration or functionality of the OA, following initiation of telephone notification; and
- c. display OA health and outage tickets in the Portal.

3.7.2 Customer Responsibilities

Activity 1 - Agent-Based Monitoring

No additional Customer responsibilities are required for this activity.

Activity 2 - Troubleshooting

Customer agrees:

- a. to participate in troubleshooting sessions with IBM (as required);
- b. to be responsible for providing all remote configuration and troubleshooting, if it has elected not to implement an OOB solution, or if the OOB solution is unavailable for any reason; and
- c. and acknowledges that if the OA is eliminated as the source of a given problem, no further troubleshooting will be performed by IBM.

Activity 3 - Notification

Customer agrees to:

- a. provide Customer notification paths and contact information;
- b. update IBM within three calendar days when Customer contact information changes; and
- c. ensure an Authorized Security Contact or Agent outage Designated Customer Contact is available 24 hours/day, 7 days/week.

3.8 OA Management

IBM will apply application and security updates to the OA.

3.8.1 IBM Responsibilities

IBM will:

- a. be the sole provider of software-level management for the OA;
- b. maintain system status awareness;
- c. install new application and security content updates on the OA, as they become available;
- d. install patches and software updates in order to improve performance, enable additional functionality, or resolve an application problem;
- e. declare a maintenance window in advance of OA updates that may require platform downtime or Customer assistance to complete; and
- f. clearly state, within the maintenance window notification, the impacts of a scheduled maintenance on the OA and identify Customer-specific requirements.

3.8.2 Customer Responsibilities

Customer agrees:

- a. to perform IBM-specified hardware upgrades to support the current software and firmware;
- b. to work with IBM to perform OA updates (as required);
- c. to be responsible for all charges associated with hardware upgrades;
- d. to maintain current licensing, and support and maintenance contracts;
- e. and acknowledges:
 - (1) all updates are transmitted and applied via the Internet;
 - (2) data traveling across the Internet is encrypted using industry-standard strong encryption algorithms whenever possible;
 - (3) noncompliance with IBM-required software upgrades may result in suspension of Services delivery and/or SLAs; and
 - (4) noncompliance with IBM-required hardware upgrades may result in suspension of Services delivery and/or SLAs.

3.9 Security Reporting

Utilizing the Portal, Customer will have access to Services information and reporting with customizable views of activity at the enterprise, work group and Agent levels. The Portal also provides Customer with the ability to schedule customized reporting.

3.9.1 IBM Responsibilities

IBM will provide Customer with access to reporting capabilities in the Portal which include:

- a. number of SLAs invoked and met;
- b. number, types, and summary of Services requests/tickets;

- c. number of security incidents detected, priority and status;
- d. list and summary of security incidents;
- e. IDS/IPS sensor reports that include attack metrics, prevented attacks, vulnerability impact, event counts/trending;
- f. event correlation and analysis (as applicable); and
- g. firewall reports that include summary, traffic analysis, protocol usage, targeted IP and rule utilization (as applicable).

3.9.2 Customer Responsibilities

Customer agrees to:

- a. generate Services-related reports using the Portal; and
- b. be responsible for scheduling reports (as applicable).

4. Optional Services

Optional services selected by Customer, and any additional charges for such services, will be specified in an Order.

4.1 Out-of-Band Access

OOB access is a highly recommended feature that assists the SOCs if connectivity to the OA is lost. If such connectivity problems occur, the SOC analysts can dial into the modem to verify the OA is functioning properly and assist in determining the source of the outage before escalating to Customer.

4.1.1 IBM Responsibilities

At Customer's request, for no additional charge, IBM will:

- a. provide live support, via phone and email, to assist Customer in locating applicable vendor documents which detail physical installation procedures and cabling;
- b. configure the OOB device to access the OA; or
- c. work in good faith with Customer to utilize an IBM-approved existing OOB solution.

4.1.2 Customer Responsibilities

Customer agrees:

- a. for new OOB solutions:
 - (1) to purchase an IBM-supported OOB device;
 - (2) to physically install and connect the OOB device to the OA;
 - (3) to provide a dedicated analog telephone line for access;
 - (4) to physically connect the OOB device to the dedicated telephone line and maintain the connection;
 - (5) to be responsible for all charges associated with the OOB device and telephone line; and
 - (6) to be responsible for all charges associated with the ongoing management of the OOB solution;
- b. for existing OOB solutions:
 - (1) to ensure the solution does not allow IBM to access non-managed devices;
 - (2) to ensure the solution does not require installation of specialized software;
 - (3) to provide IBM with detailed instructions for accessing managed OA; and
 - (4) to be responsible for all aspects of managing the OOB solution;
- c. and acknowledges that existing OOB solutions must be approved by IBM;
- d. to maintain current support and maintenance contracts for the OOB (as required); and
- e. to be responsible for providing all remote configuration and troubleshooting, if it elects not to implement an OOB solution or if the OOB solution is unavailable for any reason.

4.2 Customer Ticket System Integration

If Customer wishes to leverage existing trouble ticketing and case management investments, IBM will provide an application program interface (“API”) which allows for customized integration with external ticketing systems.

4.2.1 IBM Responsibilities

At Customer’s request, and for an additional charge specified in an Order, IBM will provide an API to allow for customized integration with external ticketing systems.

4.2.2 Customer Responsibilities

Customer agrees:

- a. to be responsible for all additional charges associated with API ticket integration;
- b. to utilize the Portal API package to facilitate ticket integration;
- c. to be responsible for all engineering and development issues associated with ticket integration; and
- d. and acknowledges that IBM will not provide assistance or consulting for Customer’s ticketing system integration.

4.3 Security Event and Log Delivery

At Customer’s request, IBM will retrieve log and event data from the IBM MSS Infrastructure and make it available for download from a secured IBM server. In cases where the amount of log and event data is warranted by IBM as too excessive to make available via download, IBM will store the data on encrypted media and ship it to a Customer-specified location. The feasibility of delivery via download will be assessed on a case-by-case basis.

4.3.1 IBM Responsibilities

At Customer’s request, and for an additional charge specified in an Order, IBM will:

- a. upon Customer’s request (via the Portal), retrieve specified data from the IBM MSS infrastructure and make it available to Customer for download on a secured IBM server; and
- b. advise Customer of additional charges for all time and materials utilized to retrieve and prepare the data.

4.3.2 Customer Responsibilities

Customer agrees:

- a. to request security event log delivery via the Portal;
- b. to download requested data from a secured IBM server;
- c. and acknowledges that requests for retrieval of excessively large amounts of data may require data be stored on encrypted media and shipped to a Customer-specified location; and
- d. to be responsible for all time and material charges, and shipping charges (as applicable) associated with log delivery.

5. Service Level Agreements

IBM SLAs establish response time objectives and countermeasures for security incidents resulting from the Services. The SLAs become effective when the deployment process has been completed, the Agent has been set to “active”, and support and management of the Agent have been successfully transitioned to “active” in the SOCs.

The SLA remedies are available provided the Customer meets its obligations as defined in this Services Description.

5.1 SLA Availability

The SLA defaults described below comprise the measured metrics for delivery of the Services. Unless explicitly stated below, no warranties of any kind shall apply to Services delivered under this Services Description. The sole remedies for failure to meet the SLA defaults are specified in the section of this Services Description entitled “SLA Remedies”.

- a. Proactive system monitoring – IBM will notify Customer within 30 minutes after IBM determines Customer’s OA is unreachable via standard in-band connectivity.
- b. Services availability – IBM will provide 100% service availability for the SOCs.

- c. Portal availability – IBM will provide 99.9% accessibility for the Portal outside of the times specified in the section of this Services Description entitled “Scheduled and Emergency Portal Maintenance”.

5.2 SLA Remedies

For all SLAs, Customer may obtain no more than one credit for each SLA per day, not to exceed a total of \$25,000 (U.S.) in a given calendar month. Such credit is the sole remedy for failure to meet any of the SLAs described in the section of this Services Description entitled “SLA Availability” during any given calendar month.

- a. Proactive system monitoring, services availability and Portal availability credits – If IBM fails to meet any of these SLAs, a credit will be issued for the applicable charges for one day of the monthly monitoring charge for the affected Agent and, if applicable, the specific managed security platform for which the respective SLA was not met.

SLAs and Remedies Summary

| Service Level Agreements | Availability Remedies |
|-----------------------------|---|
| Proactive system monitoring | Credit of 1 day of the monthly monitoring charge for the affected OA |
| Services availability | Credit of 1 day of the monthly monitoring charge for the affected Agent |
| Portal availability | |

5.3 SLA Exclusions and Stipulations

5.3.1 SLA Compliance and Reporting

SLA compliance and the associated remedies are based on fully functional network environments, Internet and circuit connectivity, Agents, and properly configured servers. SLA compliance reporting will be provided through the Portal. If SLA compliance failure is caused by customer premise equipment hardware or software (including any and all Agents), all SLAs will be considered null and void and remedies will not be paid.

5.3.2 Scheduled and Emergency Portal Maintenance

Scheduled maintenance shall mean any maintenance:

- a. that is performed during the standard monthly maintenance window on the first Saturday of every month from 8:00 a.m. – 4:00 p.m. United States Eastern Time; or
- b. of which Customer is notified at least five days in advance. Notice of scheduled maintenance will be provided to the Designated Customer Contact.

Emergency maintenance shall mean any non-scheduled, non-standard maintenance required by IBM.

No statement in the section of this Services Description entitled “Service Level Agreements” shall prevent IBM from conducting emergency maintenance on an “as needed” basis. During such emergency maintenance, Customer’s primary point of contact will receive notification within 30 minutes of initialization of the emergency maintenance and within 30 minutes of the completion of any emergency maintenance. IBM will be relieved of its obligations under these SLAs during scheduled and emergency maintenance.

5.3.3 Customer Contact Information

Certain SLAs require IBM to provide notification to the Authorized Security Contact or a Designated Customer Contact after certain events occur. In the case of such an event, Customer is solely responsible for providing IBM with accurate and current contact information for Authorized Security Contact(s) and/or Designated Customer Contact(s). The current contact information on record is available to authorized Customer contacts through the Portal. IBM will be relieved of its obligations under these SLAs if contact information is out of date or inaccurate due to Customer action or omission.

5.3.4 Customer Network/Server Change Notifications

Customer is responsible for providing IBM advance notice regarding any network or server changes or outages to the Agent environment. In the event advance notice cannot be provided, Customer is required to provide IBM with notification of changes within seven calendar days of such network or server changes. Notification is completed by the submission or update of a Customer inquiry ticket through the Portal for changes that will be implemented by Customer. For changes that must be implemented by

IBM, Customer must submit a policy change request ticket. If Customer fails to notify IBM as stated above, all SLA remedies are considered null and void.

5.3.5 Network Traffic Applicable to SLAs

Certain SLAs focus on the prevention, identification and notification of security incidents. Such SLAs assume that traffic has successfully reached the Agent and therefore the Agent has the ability to process the traffic against the installed policy and generate a logged event. Traffic that does not logically or electronically pass through an Agent, or that does not generate a logged event, is not covered under these SLAs.

5.3.6 Policy Change Request Overages

The Services include support for a specified number of policy change requests as defined in the section of this Services Description entitled "Policy Management". Policy change requests in excess of the specified amount will not be addressed as a priority and will not be bound by the SLAs provided in the section of this Services Description entitled "Service Level Agreements".

If Customer exceeds its specified number of policy change requests for two or more months during the contract term, IBM may modify Customer's contracted Services level as applicable and invoice Customer for such modified Services level for the remainder of the contract period. SLAs will be re-set for the new Services level.

As an example, Customer contracts for the Standard level of Services and is allowed two policy changes per month. For two months during the contract term, Customer requests (and IBM provides) more than two policy changes. IBM may move Customer to the Select or Premium level of Services (as applicable) and invoice Customer at the then-current rate.

5.3.7 Services Decommission or Turn-Down

If the Services are terminated or the contract is not renewed, Customer will have either 90 days from the date of termination or 90 days from the date of contract expiration, whichever first occurs, to request the receipt of archived data. Such request may be submitted through the Portal or via telephone if access to the Portal is no longer available. IBM will charge Customer for all time and materials, and shipping charges if applicable, utilized to restore and make the data available via download from a secured IBM server. In cases where the amount of archived data is warranted by IBM as too excessive to make available via download, IBM will store the data on encrypted media and ship it to a Customer-specified location.

If a request is not received within the 90 day period described above, IBM will permanently destroy all archived data pertaining to security Agents no longer under a valid Services contract.

5.3.8 Testing of Monitoring and Response Capabilities

Customer may test IBM monitoring and response capabilities by staging simulated or actual reconnaissance activity, system or network attacks, and/or system compromises. Such activities may be initiated directly by Customer or by a contracted third party with advance notice to IBM. SLAs will not apply during the period of such staged activities, and remedies will not be payable if the associated SLA(s) are not met.

6. Other Terms and Conditions

6.1 Modification of Services

IBM reserves the right to modify the terms of this Services Description at any time. Should such modification reduce the scope or level of the Services being delivered (for example, eliminating previously provided Services or lengthening the security incident response time), IBM will provide a minimum of 30 days prior notice via the Portal or other electronic means. Customer may request that IBM defer the change effective date until the end of the then-current contract period for the Services by notifying IBM in writing within the 30 calendar days immediately following IBM's notice of such modification. The modification will then become effective when the Services are renewed. If the modification is the result of circumstances outside of IBM's control (such as technology changes or vendor service changes), IBM reserves the right to reject Customer's request for deferment.

6.2 Data Compilation

Customer consents to IBM collecting, gathering and compiling security event log data to look at trends, and real or potential threats. IBM may compile or otherwise combine this security event log data with

similar data of other customers so long as such data is compiled or combined in a manner that will not in any way reveal the data as being attributable to Customer.

6.3 Customer General Responsibilities

Customer agrees to:

- a. obtain any necessary consents and take any other actions required by applicable laws, including but not limited to data privacy laws, prior to disclosing any of its employee information or other personal information or data to IBM. Customer also agrees that with respect to data that is transferred or hosted outside of the United States, Customer is responsible for ensuring that all such data transmitted outside of the United States adheres to the laws and regulations governing such data;
- b. be responsible for the identification and interpretation of any applicable laws, regulations, and statutes that affect Customer's existing systems, programs, or data to which IBM will have access during the Services. It is Customer's responsibility to ensure the systems, programs, and data meet the requirements of those laws, regulations and statutes; and
- c. be responsible as sole Data Controller for complying with all applicable data protection or similar laws regulating the processing of any Personal Data (as such terms are defined in Directive 95/46/EC) provided by or through Customer to IBM. IBM will only process such Personal Data in a manner which is reasonably necessary to provide the Services and only for that purpose. IBM will follow Customer's reasonable processing instructions with respect to the Personal Data and IBM will use its reasonable endeavors to apply the security measures as set forth in this SOW and the Agreement or as notified to IBM in writing in advance. Customer is responsible for determining that these measures provide an appropriate level of protection. IBM, in providing the Services, may transfer Customer data, including Personal Data, across a country border, including outside the European Economic Area ("EEA"), if IBM reasonably considers such transfer appropriate or useful for IBM's performance of the Services and reasonably cooperates with Customer to meet legal requirements. Customer is solely responsible for determining that any transfer by IBM or Customer of Customer Data, including Personal Data, across a country border under the SOW and the Agreement complies with the applicable data protection laws.

Customer understands and acknowledges that IBM is permitted to use global resources (non-permanent residents used locally and personnel in locations worldwide) for the delivery of the Services.

6.4 Mutual Responsibilities

IBM and Customer will each comply with applicable export and import laws and regulations, including those of the United States that prohibit or limit export for certain uses or to certain end users, and each of us will cooperate with the other by providing all necessary information to the other, as needed for compliance. Each of us shall provide the other with advance written notice prior to providing the other party with access to data requiring an export license.