

**IBM Managed Security Services (Cloud Computing) -  
Hosted Security Event and Log Management - Select**

# Table of Contents

<a href="#">.1 Scope of Services.....</a>	<a href="#">4</a>
<a href="#">.2 Definitions.....</a>	<a href="#">4</a>
<a href="#">.3 Services.....</a>	<a href="#">4</a>
<a href="#">.3.1 Security Operations Centers.....</a>	<a href="#">5</a>
<a href="#">.3.2 Portal.....</a>	<a href="#">5</a>
<a href="#">.1.1.1 IBM Portal Responsibilities.....</a>	<a href="#">5</a>
<a href="#">.1.1.2 Your Portal Responsibilities.....</a>	<a href="#">5</a>
<a href="#">.3.3 Services Contacts.....</a>	<a href="#">6</a>
<a href="#">.1.1.3 IBM Services Contacts Responsibilities.....</a>	<a href="#">6</a>
<a href="#">.1.1.4 Your Services Contacts Responsibilities.....</a>	<a href="#">7</a>
<a href="#">.3.4 Security Intelligence.....</a>	<a href="#">8</a>
<a href="#">.1.1.5 IBM Security Intelligence Responsibilities.....</a>	<a href="#">8</a>
<a href="#">.1.1.6 Your Security Intelligence Responsibilities.....</a>	<a href="#">8</a>
<a href="#">.3.5 Deployment and Activation.....</a>	<a href="#">9</a>
<a href="#">.1.1.7 IBM Deployment and Activation Responsibilities.....</a>	<a href="#">9</a>
<a href="#">.1.1.8 Your Deployment and Activation Responsibilities.....</a>	<a href="#">12</a>
<a href="#">.3.6 Collection and Archival.....</a>	<a href="#">14</a>
<a href="#">.1.1.9 IBM Collection and Archival Responsibilities.....</a>	<a href="#">14</a>
<a href="#">.1.1.10 Your Collection and Archival Responsibilities.....</a>	<a href="#">15</a>
<a href="#">.3.7 Automated Analysis.....</a>	<a href="#">15</a>
<a href="#">.1.1.11 IBM Automated Analysis Responsibilities.....</a>	<a href="#">16</a>
<a href="#">.1.1.12 Your Automated Analysis Responsibilities.....</a>	<a href="#">16</a>
<a href="#">.3.8 OA Health and Availability Monitoring.....</a>	<a href="#">16</a>
<a href="#">.1.1.13 IBM OA Health and Availability Monitoring Responsibilities.....</a>	<a href="#">16</a>
<a href="#">.1.1.14 Your OA Health and Availability Monitoring Responsibilities.....</a>	<a href="#">17</a>
<a href="#">.3.9 OA Management.....</a>	<a href="#">17</a>
<a href="#">.1.1.15 IBM OA Management Responsibilities.....</a>	<a href="#">17</a>
<a href="#">.1.1.16 Your OA Management Responsibilities.....</a>	<a href="#">18</a>
<a href="#">.3.10 Security Reporting.....</a>	<a href="#">18</a>
<a href="#">.1.1.17 IBM Security Reporting Responsibilities.....</a>	<a href="#">18</a>
<a href="#">.1.1.18 Your Security Reporting Responsibilities.....</a>	<a href="#">18</a>
<a href="#">.4 Optional Services.....</a>	<a href="#">19</a>
<a href="#">.4.1 Event Monitoring and Notification.....</a>	<a href="#">19</a>
<a href="#">.1.1.19 IBM Event Monitoring and Notification Responsibilities.....</a>	<a href="#">19</a>
<a href="#">.1.1.20 Your Event Monitoring and Notification Responsibilities.....</a>	<a href="#">19</a>
<a href="#">.4.2 Out-of-Band Access.....</a>	<a href="#">20</a>
<a href="#">.1.1.21 IBM Out-of-Band Access Responsibilities.....</a>	<a href="#">20</a>
<a href="#">.1.1.22 Your Out-of-Band Access Responsibilities.....</a>	<a href="#">20</a>
<a href="#">.4.3 Ticket System Integration.....</a>	<a href="#">21</a>
<a href="#">.1.1.23 IBM Ticket System Integration Responsibilities.....</a>	<a href="#">21</a>
<a href="#">.1.1.24 Your Ticket System Integration Responsibilities.....</a>	<a href="#">21</a>
<a href="#">.4.4 Security Event and Log Delivery.....</a>	<a href="#">21</a>
<a href="#">.1.1.25 IBM Security Event and Log Delivery Responsibilities.....</a>	<a href="#">21</a>
<a href="#">.1.1.26 Your Security Event and Log Delivery Responsibilities.....</a>	<a href="#">21</a>
<a href="#">.5 Service Level Agreements.....</a>	<a href="#">22</a>

[.5.1 SLA Availability.....22](#)  
[.5.2 SLA Remedies.....22](#)  
[.5.3 Intellectual Property Services Components.....23](#)

---

## Services Description

### IBM Managed Security Services (Cloud Computing) - Hosted Security Event and Log Management – Select

In addition to the terms and conditions specified below, this services description includes the “ibm managed security services general provisions” (“general provisions”) located at <http://www.ibm.com/services/iss/wwcontracts/us/mssgp> and incorporated herein by reference.

#### .1 Scope of Services

IBM Managed Security Services (Cloud Computing) - Hosted Security Event and Log Management - Select (called “Hosted SELM - Select” or “Services”) is designed to provide a security-enhanced Web-based solution for the collection, consolidation, analysis, correlation, alerting, trending 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 and product features being utilized. Even in the case of supported products, not all product features may be supported. Information on supported features is available from IBM upon request. This includes both IBM-provided and non-IBM-provided hardware, software, and firmware.

#### .2 Definitions

**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, the 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 Managed Security Services (“IBM MSS”) portal (called “Portal”).

**Education Materials** – include, but are not limited to, lab manuals, instructor notes, literature, methodologies, electronic course and case study images, policies and procedures, and all other training-related property created by or on behalf of IBM. Where applicable, Education Materials may include participant manuals, exercise documents, lab documents and presentation slides provided by IBM.

**intrusion prevention system (“IPS”)** – a network security device or software application 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.

#### .3 Services

The following table highlights the measurable Services features. The subsequent sections provide narrative descriptions of each Services feature.

##### Services Feature Summary

Services Feature	Metric or Qty	Service Level Agreements
<a href="#">Services availability</a>	100%	<a href="#">Services availability SLA</a>
<a href="#">IBM MSS Portal availability</a>	99.9%	<a href="#">IBM MSS Portal availability SLA</a>
<a href="#">Authorized Security Contacts</a>	3 users	N/A
<a href="#">Log/event archival</a>	5 Gb of compressed data per year for each year of the contract (up to 7 years)	N/A
<a href="#">Security incident identification</a>	100%	<a href="#">Security incident identification SLA</a>
<a href="#">Security incident alert notification</a>	60 minutes	<a href="#">Security incident alert SLA</a>
<a href="#">OA health alerting</a>	15 minutes	<a href="#">System monitoring SLA</a>
<a href="#">Security incident notification</a>	15 minutes	<a href="#">Security incident notification SLA</a>

<a href="#">(optional Services add-on)</a>		
--	--	--

### .3.1 Security Operations Centers

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

### .3.2 Portal

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

The Portal may also be used to deliver Education Materials. All such Education Materials are licensed not sold and remain the exclusive property of IBM. IBM grants you a license in accordance with the terms provided in the Portal. EDUCATION MATERIALS ARE PROVIDED “AS IS” AND WITHOUT WARRANTY OR INDEMNITY OF ANY KIND BY IBM, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF PROPRIETARY AND INTELLECTUAL PROPERTY RIGHTS.

#### .1.1.1 IBM Portal Responsibilities

IBM will:

- .a provide access to the Portal 24 hours/day, 7 days/week. The Portal will provide:
  - (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) the ability to parse and normalize unknown, text-based system activity logs;
  - (8) granular security event and log query capabilities;
  - (9) authorization to download log data;
  - (10) access to Education Materials in accordance with the terms provided in the Portal; and
  - (11) the ability to create user-defined correlation rules.
- .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](#)”;

Note: You may contract separately with IBM to parse and normalize unknown system activity logs. Such services are not included as part of this offering.

#### .1.1.2 Your Portal Responsibilities

You agree:

- .a to utilize the Portal to perform daily operational Services activities;
- .b to ensure your employees accessing the Portal on your behalf comply with the Terms of Use provided therein including, but not limited to, the terms associated with Educational Materials;
- .c to appropriately safeguard your login credentials to the Portal (including not disclosing such credentials to any unauthorized individuals.);
- .d to promptly notify IBM if a compromise of your login credentials is suspected;
- .e to indemnify and hold IBM harmless for any losses incurred by you or other parties resulting from
  - (1) your failure to safeguard your login credentials;
  - (2) your incorrect use of regular expressions when parsing and normalizing event and log data; and
  - (3) your incorrect use of user-defined correlation rules.
- .f to be responsible for parsing and normalizing unknown log formats in the Portal;

- .g to be solely responsible for testing and verifying the performance of log parsers and user-defined correlation rules;
- .h to enable and disable log parsers and user-defined correlation rules utilizing the Portal; and
- .i and acknowledge that:
  - (1) OA performance and the timely delivery of log data can be negatively affected by incorrectly written or inefficient log parsers;
  - (2) IBM is not responsible for the log parsers or user-defined correlation rules that are configured and saved in the Portal; and
  - (3) configuration assistance for parsing unknown log formats is not included in the Services.

### **.3.3 Services Contacts**

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

#### **Authorized Security Contacts**

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

#### **Designated Services Contacts**

A Designated Services Contact is defined as a decision-maker on a subset of operational issues pertaining to IBM Managed Security Services, an Agent, or a group of Agents. IBM will only interface with a Designated Services 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 a public-key encryption technology you provide (for example, RSA SecureID token) based on your requirements.

### **.1.1.3 IBM Services Contacts Responsibilities**

#### **Authorized Security Contacts**

IBM will:

- .a allow you to create up to three Authorized Security Contacts;
- .b provide each Authorized Security Contact with:
  - (1) administrative Portal permissions to your Agents;
  - (2) the authorization to create unlimited Designated Services Contacts and Portal users;
  - (3) the authorization to delegate responsibility to Designated Services 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 Services Contacts**

IBM will:

- .a verify the identity of Designated Services Contacts using an authentication method that utilizes a pre-shared challenge pass phrase; and
- .b interface only with Designated Services 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:

- (j) creating and editing vulnerability watch lists;
  - (k) performing live event monitoring;
  - (l) querying security event and log data;
  - (m) enabling/disabling automated intelligence (“AI”) analysis alert policy rules;
  - (n) creating custom user-defined correlation rules;
  - (o) scheduling downloads of security event and log data; and
  - (p) 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 you 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 public-key encryption technology you provide (for example, RSA SecureID token) based on your requirements.

#### **.1.1.4 Your Services Contacts Responsibilities**

##### **Authorized Security Contacts**

You agree:

- .a to provide IBM with contact information for each Authorized Security Contact. Such Authorized Security Contacts will be responsible for:
  - (1) creating Designated Services 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 your 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 your contact information changes; and
- .d and acknowledge that you are permitted to have no more than three Authorized Security Contacts regardless of the number of IBM services or Agent subscriptions for which you have contracted.

##### **Designated Services Contacts**

You agree:

- .a to provide IBM with contact information and role responsibility for each Designated Services Contact. Such Designated Services Contacts will be responsible for authenticating with the SOCs using a pass phrase; and
- .b and acknowledge that a Designated Services 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**

You agree:

- .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 acknowledge the SOCs will only interface with Authorized Security Contacts and Designated Services 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 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 you with real-time access into IBM's global situation briefing. As a user of the Portal, you have access to the X-Force Hosted Threat Analysis Service. The X-Force Hosted Threat Analysis Service includes access to the IBM X-Force Threat Insight Quarterly ("Threat IQ").

Utilizing the Portal, you can create a vulnerability watch list with customized threat information. In addition, each Portal user can request to receive an Internet assessment e-mail 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.

NOTE: Your access and use of the security intelligence provided via the Portal (including the Threat IQ and the daily Internet assessment e-mail) is subject to the Terms of Use provided therein. Where such Terms of Use conflict with the terms of this Agreement, the Portal Terms of Use shall prevail over this Agreement. In addition to the Terms of Use provided in the Portal, your use of any information on any links or non-IBM Web sites and resources are subject to the terms of use posted on such links, non-IBM Web sites, and resources.

### **.1.1.5 IBM Security Intelligence Responsibilities**

IBM will:

- .a provide you with access to the X-Force Hosted Threat Analysis Service;
- .b provide you 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 you, provide security intelligence specific to your defined vulnerability watch list, via the Portal;
- .e if configured by you, provide an Internet security assessment e-mail 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 you with real time access into IBM's global situation briefing;
- .h provide Portal feature functionality for you 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 access to the Threat IQ via the Portal.

### **.1.1.6 Your Security Intelligence Responsibilities**

You agree to use the Portal to:

- .a subscribe to the daily Internet security assessment e-mail, if desired;
- .b create a vulnerability watch list, if desired;

- .c access the Threat IQ; and
- .d agree to adhere to the licensing agreement and not forward Services information to individuals who do not have a proper license.

### **.3.5 Deployment and Activation**

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

Note: Deployment and Activation activities are performed one time during the performance of the services. If you choose to replace, or move your Agent during the Services contract, IBM may require that such Agent be redeployed and reactivated (called "Redeployment"). Such Redeployments will be provided at an additional charge as specified in the Schedule. Redeployment charges apply only to hardware replacements, upgrades, or moves that you initiate. Such charges do not apply to Agent failures resulting in Agent Return Material Authorization ("RMA") activities.

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

#### **.1.1.7 IBM Deployment and Activation Responsibilities**

##### **Activity - 1Project Kickoff**

The purpose of this activity is to conduct a project kickoff call. IBM will send you a welcome e-mail and conduct a kickoff call, for up to one hour for up to three of your personnel, to:

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

##### ***Completion Criteria:***

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

##### ***Deliverable Materials:***

- None

##### **Activity - 2Network Access Requirements**

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

IBM will:

- .a provide you with a document called "Network Access Requirements", detailing:
  - (1) how IBM will connect remotely to your 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 your 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 your network. Such VPN may be provided by IBM for an additional charge as specified in the Schedule.

##### ***Completion Criteria:***

This activity will be complete when IBM has provided your Point of Contact with the Network Access Requirements document.

##### ***Deliverable Materials:***

- Network Access Requirements document

##### **Activity - 3Assessment**

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

##### ***Task -1 Gather Data***

IBM will:

- .a provide your Point of Contact with a data gathering form on which you will be asked to document:

- (1) team member names, contact information, roles and responsibilities;
- (2) unique country and site requirements;
- (3) your 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 Log 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 your environment (as applicable).

**Deliverable Materials:**

- None

**Activity - 4On-site Aggregator Implementation**

The purpose of this activity is to configure the on-site aggregator (“OA”).

The OA is a required device that you provide. Such device is deployed at your location and managed and monitored by IBM MSS for an additional charge, as specified in the Schedule.

The basic functions of the OA are to:

- .a compile or otherwise combine the security events and log data;
- .b parse and normalize unknown, text-based system activity log formats for submission to the IBM MSS infrastructure;
- .c compress and encrypt the security events and log data; and
- .d transmit the security events and log data to the IBM MSS infrastructure.

Core features of the OA are to:

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

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 e-mail, and will assist you 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 you with hardware specifications for the OA platform;
- .c provide you with OA software and configuration settings;
- .d provide you with telephone and e-mail support to assist with the installation of the IBM-provided OA software on the hardware platform you provide. Such support must be scheduled in advance to ensure availability of an IBM deployment specialist;

- .e at your request, and for an additional charge specified in the Schedule, provide software installation services;
- .f for existing platforms:
  - ()1 assess existing hardware configurations to ensure they meet IBM's specification; and
  - ()2 identify required hardware upgrades to be provided and installed by you.

**Task -2 Install the OA**

IBM will:

- .a provide live support, via phone and e-mail, and will assist you with location of applicable 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;
- .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 - 5Universal Log Agent Implementation**

The ULA is a light-weight log collection application that runs on an Agent subscribing to the Services. The ULA gathers text-based logs locally from the Agent and securely forwards them to the OA. The OA then securely forwards the logs to the IBM MSS infrastructure for collection, long term storage, and display in the Portal.

The basic functions of the ULA are to:

- .a collect events/logs locally from the Agent;
- .b compress the events/log data;
- .c encrypt the events/log data; and
- .d 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 unidirectional 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 you in the Portal.

**Task -1 Prepare Your Agent**

IBM will provide you with a list of Agents that require ULA installation.

### **Task -2 Install the ULA**

IBM will:

- .a provide the ULA for download via the Portal; and
- .b provide you with access to the SELM ULA Installation Guide via the Portal.

### **Task -3 Configure the ULA**

IBM will provide you with instructions on how to login to the Portal and configure the Agent.

#### **Completion Criteria:**

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

#### **Deliverable Materials:**

- None

### **Activity - 6Non-ULA Log Collection Implementation**

The purpose of this activity is to facilitate log collection via SYSLOG streams when it is not technically feasible or appropriate to install the ULA on an Agent.

IBM will:

- .a provide you with a list of Agents that require SYSLOG collection;
- .b provide the IP address of the OA to which the SYSLOG stream must be forwarded.

#### **Completion Criteria:**

This activity will be complete when IBM has provided your Point of Contact with the IP address of the OA to which the SYSLOG stream must be forwarded.

#### **Deliverable Materials:**

- None

### **Activity - 7Testing and Verification**

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

IBM will:

- .a verify connectivity of the OA 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; and
- .e remotely demonstrate the primary features of the Portal for up to ten of your 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 - 8Services Activation**

The purpose of this activity is to activate the Services.

IBM will:

- .a assume support of the Services; and
- .b transition the Services to the SOCs for ongoing support.

#### **Completion Criteria:**

This activity will be complete when the SOC has assumed support of the Services.

#### **Deliverable Materials:**

- None

## **.1.1.8 Your Deployment and Activation Responsibilities**

### **Activity - 1 Project Kickoff**

You agree to:

- .a attend the project kickoff call; and
- .b review each party's respective responsibilities.

### **Activity - 2 Network Access Requirements**

You agree 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 your network.

### **Activity - 3 Assessment**

#### ***Task -1 Gather Data***

You agree to:

- .a complete and return any questionnaires and/or data gathering forms to IBM within five days of your 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 your network environment;
- .d provide contacts within your organization, and specify a notification path through your organization in the event IBM must contact you; and
- .e update IBM within three calendar days when your contact information changes.

#### ***Task -2 Assess Environment***

No additional responsibilities are required by you for this activity.

### **Activity - 4 On-site Aggregator Implementation**

#### ***Task -1 Configure the OA***

You agree:

- .a to provide IBM with an external IP address for the OA;
- .b to provide the hardware for the OA platform, based on IBM's recommendations and requirements;
- .c to maintain current licensing, and support and maintenance contracts for the hardware the OA is installed upon;
- .d to install the IBM-provided OA software on your 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 procure and install IBM-requested hardware upgrades.

#### ***Task -2 Install the OA***

You agree to:

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

### **Activity - 5 Universal Log Agent Implementation**

#### ***Task -1 Prepare Your Agent***

You agree to:

- .a enable your organizations desired system, security and application-level auditing of the operating systems, or applications that will be monitored; and
- .b verify connectivity between the Agent and the OA.

### **Task -2 Install the ULA**

You agree:

- .a to download the ULA software from the Portal;
- .b to install the ULA on Agent(s) subscribing to the Services; and
- .c and acknowledge you are solely responsible for all ULA installation tasks.

### **Task -3 Configure the ULA**

You agree:

- .a to login to the Portal and confirm the Agent is available and is receiving logs within three business days of ULA installation and configuration;
- .b to configure the ULA with appropriate configuration settings (including: service level, site, platform, operating system and time zone);
- .c to update the ULA configuration settings (including service level, site, platform, operating system and time zone), within three days of any future device modification;
- .d to modify the ULA policy (if desired); and
- .e and acknowledge that you are solely responsible for all ULA configuration tasks.

### **Activity - 6Non-ULA Log Collection Implementation**

You agree:

- .a to configure the Agent to point SYSLOG streams to the OA under the guidance of IBM;
- .b to login to the Portal and confirm the Agent is available and is receiving logs within three business days; and
- .c and acknowledge you are solely responsible for all SYSLOG installation tasks.

### **Activity - 7Testing and Verification**

You agree:

- .a to be responsible for development of all of your specific acceptance testing plans;
- .b to be responsible for performing acceptance testing of your applications and network connectivity;
- .c to verify that the logs of each Agent are available in the Portal;
- .d to update the ULA configuration settings (including service level, site, platform, operating system and time zone), within three days of any future device modification; and
- .e and acknowledge that additional acceptance testing performed by you, or lack thereof, does not preclude IBM from setting the Agent to "active" in the SOCs for ongoing support and management.

### **Activity - 8Services Activation**

No additional responsibilities are required by you 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 you 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 compressed 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 Schedule.

### **.1.1.9 IBM Collection and Archival Responsibilities**

IBM will:

- .a collect log and event data generated by the managed Agent as such data reaches the IBM MSS infrastructure;
- .b utilize enabled parsers to normalize inbound log traffic for display and archival; and

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

Note: Notwithstanding any retention periods defined by you, IBM will not retain log and event data for more than seven years. If you exceed your 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.

#### **.1.1.10 Your Collection and Archival Responsibilities**

You agree:

- .a to provide IBM with security event and log retention periods not to exceed five Gb of compressed 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 - Select 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 your security event and log data.

- .e and acknowledge that:
  - (1) all log and event data will be transmitted to the SOCs via the Internet;
  - (2) IBM can only collect and archive log and event data that successfully reaches the IBM MSS infrastructure;
  - (3) 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 your ability to prove proper data handling and chain of custody for each set of data presented;
  - (4) IBM has the right to throttle event streams generated by the Agent that exceed 100 EPS (if required);
  - (5) IBM will begin purging data using a FIFO method when collected log and event data exceeds allocated storage space;
  - (6) IBM will not store log and event data for more than seven years;
  - (7) your 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 your specified retention periods; and
  - (8) IBM may collect, gather and compile the log parsers and data utilized by the Services for the purposes of: 1) sanitizing and publishing parsers for general use, and 2) identifying trends, and real or potential threats. IBM may compile or otherwise combine this information with that of other Services Recipients 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 you.

#### **.3.7 Automated Analysis**

Agents are capable of generating a high volume of alarms in response to the security conditions they are configured to detect. The actual security risk corresponding to a particular condition detected is not

always clear, and it is not practical to block all data that may be harmful as the default behavior. Additional monitoring and analysis of these alarms is important to a sound security program.

IBM has developed and maintains a proprietary automated intelligence (“AI”) analysis engine as part of the X-Force Protection System. Events from Agents are submitted to the AI analysis engine for correlation and identification, as they are collected.

The AI analysis engine performs the following basic functions:

- correlates both real-time and historical alarms;
- utilizes statistical and rules-based analysis techniques;
- leverages raw, normalized and consolidated data; and
- operates on application and operating system alarms.

X-Force Protection System AI alerts are made available to you via the Portal. IBM will send you an hourly X-Force Protection System alert notification e-mail, summarizing the AI alerts, if you select this option in the Portal.

Automated analysis and the subsequent AI alerts generated by the X-Force Protection System are available on IBM-specified platforms or the system activity log sources you normalize utilizing the custom log parser.

#### **.1.1.11 IBM Automated Analysis Responsibilities**

IBM will:

- .a submit collected event data to the X-Force Protection System AI analysis engine for correlation and identification;
- .b utilize user-defined correlation rules that are enabled for analysis and alerting.
- .c display alerts generated by the X-Force Protection System AI analysis engine in the Portal, as such alerts become available; and
- .d if configured by you, deliver X-Force Protection System alert notification within the timeframes established in the section of this Services Description entitled “[Service Level Agreements](#)”, “[Security incident alert notification](#)”.

#### **.1.1.12 Your Automated Analysis Responsibilities**

You agree:

- .a to be responsible for enabling/disabling AI engine rules, using the Portal;
- .b to be responsible for creating user-defined correlation rules, using the Portal;
- .c to be responsible for scheduling X-Force Protection System alert notification, using the Portal; and
- .d and acknowledge;
  - ()1 the Portal can be used to monitor and review alerts generated by the X-Force Protection System AI analysis engine; and
  - ()2 that automated analysis is available on IBM-specified platforms or the log sources you normalize utilizing the custom log parser.

### **.3.8 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.

#### **.1.1.13 IBM OA Health and Availability Monitoring Responsibilities**

##### **Activity - 1Agent-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 - 2Troubleshooting**

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 - 3Notification**

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

IBM will:

- .a notify you 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.

### **.1.1.14 Your OA Health and Availability Monitoring Responsibilities**

#### **Activity - 1Agent-Based Monitoring**

No additional responsibilities are required by you for this activity.

#### **Activity - 2Troubleshooting**

You agree:

- .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 acknowledge that if the OA is eliminated as the source of a given problem, no further troubleshooting will be performed by IBM.

#### **Activity - 3Notification**

You agree to:

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

### **.3.9 OA Management**

IBM will apply application and security updates to the OA.

#### **.1.1.15 IBM OA Management 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 your assistance to complete; and
- .f clearly state, within the maintenance window notification, the expected impacts of a scheduled maintenance on the OA and your specific requirements.

#### **.1.1.16 Your OA Management Responsibilities**

You agree:

- .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 to ensure appropriate consents are in place with your vendors to allow IBM to leverage existing support and maintenance contracts on your behalf. If such agreements are not in place, IBM will not be able to contact the vendor directly to resolve support issues; and
- .f and acknowledge:
  - (1) all updates are transmitted and applied via the Internet;
  - (2) if vendor consents are not obtained or are revoked at any point during the contract period, Services and/or SLAs may be suspended by IBM;
  - (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.

### **.3.10 Security Reporting**

Utilizing the Portal, you 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 you with the ability to schedule customized reporting.

#### **.1.1.17 IBM Security Reporting Responsibilities**

IBM will provide you 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);
- .g firewall reports that include summary, traffic analysis, protocol usage, targeted IP and rule utilization (as applicable); and
- .h Payment Card Industry ("PCI") Audit Readiness Reports that tie system activity events on designated devices to specific PCI requirements.

#### **.1.1.18 Your Security Reporting Responsibilities**

You agree:

- .a to generate Services-related reports using the Portal;
- .b to be responsible for scheduling reports (as applicable); and
- .c and acknowledge that assistance from a PCI qualified security assessor ("QSA") is not provided as part of the Services, but you may contract separately with IBM to address this need.

## **.4 Optional Services**

Optional services selected by you, and any additional charges for such services, will be specified in the Schedule.

### **.4.1 Event Monitoring and Notification**

IBM MSS security analysts will perform event monitoring and analysis of intrusion event AI alerts generated by the X-Force Protection System which result from automated analysis performed on supported network IDS/IPS events. Whether or not a security event is considered a security incident is determined solely by IBM. Identified events will be classified, prioritized, and escalated as IBM deems appropriate. Alerts that are not eliminated as benign triggers are classified as a security incident ("SI").

Security incidents ("SI") are classified into one of the three priorities described below:

- SI – Priority 1  
Investigations that result in a high priority classification (i.e., Priority 1) require immediate defensive action.
- SI – Priority 2  
Investigations that result in a medium priority classification (i.e., Priority 2) require action within 12 - 24 hours of notification.
- SI – Priority 3  
Investigations that result in a low priority classification (i.e., Priority 3) require action within 1 - 7 days of notification.

#### **.1.1.19 IBM Event Monitoring and Notification Responsibilities**

During any period in which you have subscribed to Event Monitoring and Notification, and for an additional charge specified in a Schedule, IBM will:

- .a notify you via email at the start and finish of the event monitoring and notification window notifying you that monitoring has commenced/completed;
- .b monitor X-Force Protection System AI alerts that result from real-time AI analysis on network IDS/IPS event data;
- .c perform investigation and analysis of AI alerts;
- .d request modification to the Agent IDS/IPS configuration, to be implemented by you, if the current policy prevents the SOC from processing event data satisfactorily;
- .e when possible, eliminate false positives and benign triggers and classify them as commented security incidents ("CSI");
- .f identify alerts that are not eliminated as benign triggers and classify such alerts security incidents ("SIs")
  - (1) start the SLA timers; and
  - (2) prioritize the SI as either high, medium or low;
- .g using the standard notification path that you provide, escalate SIs to an Authorized Security Contact or Designated Services Contact based on IBM security notification "best practices" within the time frame and using the medium (for example e-mail or telephone) established in the section of this Services Description entitled "[Service Level Agreements](#)", "[Security Incident Notification](#)";
- .h provide remediation/countermeasure recommendations, if applicable;
- .i document details of CSIs and SIs in the IBM ticketing system; and
- .j list CSIs and SIs in the Portal.

#### **.1.1.20 Your Event Monitoring and Notification Responsibilities**

You agree:

- .a to utilize the Portal to schedule event monitoring and notification;
- .b to implement MSS request policy changes to the Agent prior to the next monitoring period;
- .c to utilize the Portal for investigation of audit events or ongoing events that are not considered to be immediate threats;

- .d to provide IBM with current in-depth documentation of your environment;
- .e to update IBM within three calendar days of changes within your environment;
- .f to provide IBM with the following information, and keep such information current via the Portal;
  - (1) information about critical servers (for example, name, platform, operating system ("OS"), Internet protocol ("IP") address and network segment type);
  - (2) information about monitored networks;
  - (3) information about devices utilizing network address translation ("NAT"); (for example, name, platform, OS, and network segment type);
  - (4) proxy servers; and
  - (5) authorized scanners;
- .g to provide and keep current a linear contact notification path, including telephone numbers and e-mail addresses;
- .h to update IBM, via the Portal, within three calendar days of a change in your contact information;
- .i to provide e-mail aliases, as necessary to facilitate notification;
- .j to ensure an Authorized Security Contact or Designated Services Contact listed in the notification path is available 24 hours /day, 7 days / week;
- .k to view details of CSIs and SIs via the Portal;
- .l to work with IBM to optimize the monitoring service;
- .m to provide feedback on CSIs and SIs via the Portal;
- .n and acknowledge that:
  - (1) once IBM has escalated an SI, you are solely responsible for all SI incident responses and remediation activities;
  - (2) not all investigations of suspicious activity will result in the declaration of an SI;
  - (3) Event Monitoring and Notification applies only to AI alerts resulting from automated analysis performed on network IDS/IPS events;
  - (4) lack of feedback can result in a lower prioritization of persistent or recurring activity; and
  - (5) if you do not make the requested policy modifications prior to the next monitoring period, the Security Incident Notification SLA established in the section of this Services Description entitled "Service Level Agreements" will be null and void;

## **.4.2 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 you.

### **.1.1.21 IBM Out-of-Band Access Responsibilities**

At your request, for no additional charge, IBM will:

- .a provide live support, via phone and e-mail, to assist you 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 you to utilize an IBM-approved existing OOB solution.

### **.1.1.22 Your Out-of-Band Access Responsibilities**

You agree:

- .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 acknowledge 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 you elect not to implement an OOB solution or if the OOB solution is unavailable for any reason.

### **.4.3 Ticket System Integration**

If you wish 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.

#### **.1.1.23 IBM Ticket System Integration Responsibilities**

At your request, and for an additional charge specified in the Schedule, IBM will provide an API to allow for customized integration with external ticketing systems.

#### **.1.1.24 Your Ticket System Integration Responsibilities**

You agree:

- .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 acknowledge that IBM will not provide assistance or consulting for your ticketing system integration.

### **.4.4 Security Event and Log Delivery**

At your 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 deemed by IBM to be too excessive to make available via download, IBM will store the data on encrypted media and ship it to a location you specify. The feasibility of delivery via download will be assessed on a case-by-case basis.

#### **.1.1.25 IBM Security Event and Log Delivery Responsibilities**

At your request, and for an additional charge specified in the Schedule, IBM will:

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

#### **.1.1.26 Your Security Event and Log Delivery Responsibilities**

You agree:

- .a to request security event log delivery via the Portal;
- .b to download requested data from a secured IBM server;
- .c and acknowledge that requests for retrieval of excessively large amounts of data may require data be stored on encrypted media and shipped to a location you specify; 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 specific events 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 you meet your obligations as defined in this Services Description and all associated contract documents.

### **.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 Security incident identification – IBM will identify all events it deems to be Priority 1, 2, and 3 level security incidents based on Agent IDS/IPS event data received by the SOCs.
  - (1) Priority 1 incidents: high-risk events that have the potential to cause severe damage to your systems or environments and require immediate defensive action. Priority 1 incident examples include system or data compromises, worm infections/propagation, and massive denial of service (“DOS”) attacks.
  - (2) Priority 2 incidents: lower-risk events that have the potential to impact your systems or environments and require action within 12-24 hours of notification. Priority 2 incident examples include unauthorized local scanning activity and attacks targeted at specific servers or workstations.
  - (3) Priority 3 incidents: low-risk or low confidence events that have the potential to impact your systems or environments. This category of investigation encompasses activity on a network or server that should be further investigated within 1-7 days but may not be directly actionable. Discovery scanning, information gathering scripts, and other reconnaissance probes are grouped into this category.

Note: Whether or not a security event is considered a security incident is determined solely by IBM.

- .b Security incident alert notification (not available during any period in which you have subscribed to event monitoring and notification) – If X-Force Protection System alert notification has been configured by you in the Portal and an alert has been generated, IBM will send an hourly e-mail notification to the Designated Services Contact, summarizing the X-Force Protection System AI alerts. This SLA only applies to the initial sending of the X-Force Protection System alert notification; not the confirmed delivery to the end recipient(s).

For purpose of clarification, an e-mail notification will be sent only if an alert has been generated during the preceding hour.
- .c Security incident notification (available during any period in which you have subscribed to event monitoring and notification) - During the SOC monitoring period, IBM will initiate notification for all identified security incidents within 15 minutes of such identification. Your Authorized Security Contact or Designated Services Contact will be notified by telephone for Priority 1 security incidents and via email for Priority 2 and 3 security incidents. During a Priority 1 security incident notification, IBM will continue attempting to contact the Authorized Security Contact or Designated Services Contact until such contact is reached or all notification contacts have been exhausted.

Operational activities related to security incidents and responses will be documented and time-stamped within the IBM trouble ticketing system. Such documentation and time-stamp shall be used as the sole authoritative information source for purposes of this SLA.
- .d Proactive system monitoring – IBM will notify you within 15 minutes after IBM determines your OA is unreachable via standard in-band connectivity.
- .e Services availability – IBM will provide 100% service availability for the SOCs.
- .f 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**

- .a Security incident identification remedy – If IBM fails to meet this SLA in a given calendar month, a credit will be issued as specified below;

- (1) Priority 1 incidents: Failure to identify the security event(s) as a security incident will result in a one month credit for the initial Agent that reported the event(s).
  - (2) Priority 2 incidents: Failure to identify the security event(s) as a security incident will result in a one week credit for the initial Agent that reported the event(s).
  - (3) Priority 3 incidents: Failure to identify the security event(s) as a security incident will result in a one day credit for the initial Agent that reported the event(s).
- .b Security incident alert notification, security incident notification, 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 for which the respective SLA was not met.

**SLAs and Remedies Summary**

Service Level Agreements	Availability Remedies
Security incident identification	Credit for 1 month, 1 week, or 1 day for the initial Agent that reported the event, as indicated above
Proactive system monitoring	Credit of 1 day of the monthly monitoring charge for the affected OA
Security incident alert notification	Credit of 1 day of the monthly monitoring charge for the affected Agent
Security incident notification	
Services availability	
Portal availability	

**.5.3 Intellectual Property Services Components**

**IPSC Definition**

Intellectual Property Services Components ("IPSCs") are pre-existing IBM or third party proprietary literary works or other works of authorship (such as programs, program listings, programming tools, documentation, reports, drawings and similar works) that IBM may license to you or that IBM may use when providing Services. IPSCs are not Products or Materials, as such terms are defined in the IBM Customer Agreement (called "ICA"). The terms of the ICA shall otherwise apply to IPSCs, except that the section entitled "Limitation of Liability," shall apply to IPSCs as if an IPSC was a "Product" for purposes of that section without reference to any other section. IBM or third parties have all right, title, and interest (including ownership of copyright) in IPSCs and IPSCs are licensed, not sold. Except as provided by mandatory law, without the possibility of contractual waiver or limitation, IBM provides IPSCs WITHOUT INDEMNITIES OR WARRANTIES OF ANY KIND.

**IPSC License Grant**

Subject to the IPSC Special Terms below, IBM grants you a revocable, nonexclusive, paid-up license to use, within your Enterprise only, the following IPSC:

- Universal Log Agent

**IPSC Special Terms**

- .g IBM may terminate this license if you do not comply with any of the terms of this SOW.
- .h Upon termination of this license, you agree to destroy all copies of, and make no further use of, Universal Log Agent, and certify such destruction to IBM.

By accepting receipt of the Universal Log Agent, you agree to the following Terms of Use: During the term of your IBM Managed Security Services, IBM grants you a limited nonexclusive, nontransferable license solely to internally use the Universal Log Agent. Except as otherwise provided herein, the terms of your agreement for the Managed Security Services with IBM shall apply to IBM's provision, and your use, of any Universal Log Agent. No title to or ownership in the Universal Log Agent is transferred to you. Your rights will at all times be subject to IBM's copyrights and other intellectual property rights, and IBM will retain all right, title and interest in the Universal Log Agent and any derivative works thereof.

UNIVERSAL LOG AGENT IS PROVIDED "AS IS" AND WITHOUT WARRANTY OR INDEMNITY OF ANY KIND BY IBM, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF PROPRIETARY AND INTELLECTUAL PROPERTY RIGHTS. Universal Log Agent may not be: 1) used, copied, modified, or distributed except as expressly provided herein; 2) reverse assembled, reverse compiled, or otherwise translated, except as specifically permitted by law without the possibility of contractual waiver; 3) sublicensed, rented, or leased; or 4) used for commercial purposes, including commercial research, consulting or running a business. You may not create derivative works based on the Universal Log Agent and shall not remove any notices included in the Universal Log Agent. You may not use the Universal Log Agent to design, develop or test software applications for any commercial purposes. You may not allow others to use your passwords to gain access to IBM's restricted Web sites or use the Universal Log Agent for any purposes. The Universal Log Agent is considered confidential to IBM and you shall hold such confidential information ("Information") in trust and confidence for IBM. You will use the same care and discretion to avoid disclosure of the Information as you use with your own similar information which you do not wish to disclose. During such period, you may only disclose the Information to (1) your employees who have a need to know, and (2) any other party with IBM's prior written consent. Prior to any such disclosure, you must have a written and appropriate agreement with your employees and any other party authorized to receive such Information sufficient to require the party to treat the Information in accordance with these Terms of Use. You may use such Information only for the purpose for which it was disclosed or otherwise for the benefit of IBM. These Terms of Use impose no obligation upon you regarding the Universal Log Agent or any information contained in it where such items: (1) are or become publicly available through no fault of yours; or (2) are developed independently by you.