

**IBM Managed Security Services  
for  
Unified Threat Management - Standard**

# Table of Contents

<b>1.</b>	<b>Scope of Services .....</b>	<b>4</b>
<b>2.</b>	<b>Definitions.....</b>	<b>4</b>
<b>3.</b>	<b>MSS for UTM - Standard Features .....</b>	<b>4</b>
3.1	Security Operations Centers .....	5
3.2	Portal.....	5
3.2.1	IBM Responsibilities .....	5
3.2.2	Customer Responsibilities .....	6
3.3	Customer Contacts.....	6
3.3.1	IBM Responsibilities .....	6
3.3.2	Customer Responsibilities .....	7
3.4	Security Intelligence .....	8
3.4.1	IBM Responsibilities .....	8
3.4.2	Customer Responsibilities .....	9
3.5	Deployment and Activation.....	9
3.5.1	IBM Responsibilities .....	9
3.5.2	Customer Responsibilities .....	11
3.6	Collection and Archival.....	13
3.6.1	IBM Responsibilities .....	13
3.6.2	Customer Responsibilities .....	13
3.7	Automated Analysis.....	14
3.7.1	IBM Responsibilities .....	14
3.7.2	Customer Responsibilities .....	14
3.8	Policy Management.....	14
3.8.1	IBM Responsibilities .....	15
3.8.2	Customer Responsibilities .....	15
3.9	Virtual Private Network Support .....	15
3.9.1	IBM Responsibilities .....	16
3.9.2	Customer Responsibilities .....	16
3.10	Managed Agent Health and Availability Monitoring .....	16
3.10.1	IBM Responsibilities .....	16
3.10.2	Customer Responsibilities .....	17
3.11	Agent Management .....	18
3.11.1	IBM Responsibilities .....	18
3.11.2	Customer Responsibilities .....	18
3.12	Security Reporting.....	18
3.12.1	IBM Responsibilities .....	18
3.12.2	Customer Responsibilities .....	19
<b>4.</b>	<b>Optional Services .....</b>	<b>19</b>
4.1	Content Security.....	19
4.1.1	IBM Responsibilities .....	19
4.1.2	Customer Responsibilities .....	19
4.2	Out-of-Band Access .....	20
4.2.1	IBM Responsibilities .....	20
4.2.2	Customer Responsibilities .....	20
4.3	Cold Standby.....	20
4.3.1	IBM Responsibilities .....	20

4.3.2	Customer Responsibilities .....	20
4.4	Warm Standby .....	21
4.4.1	IBM Responsibilities .....	21
4.4.2	Customer Responsibilities .....	21
4.5	High Availability .....	21
4.5.1	IBM Responsibilities .....	22
4.5.2	Customer Responsibilities .....	22
4.6	Onsite Aggregator .....	22
4.6.1	IBM Responsibilities .....	23
4.6.2	Customer Responsibilities .....	24
4.7	Customer Ticket System Integration .....	24
4.7.1	IBM Responsibilities .....	24
4.7.2	Customer Responsibilities .....	24
4.8	Security Event and Log Delivery .....	24
4.8.1	IBM Responsibilities .....	25
4.8.2	Customer Responsibilities .....	25
<b>5.</b>	<b>Service Level Agreements.....</b>	<b>25</b>
5.1	SLA Availability .....	25
5.2	SLA Remedies .....	26
5.3	SLA Exclusions and Stipulations .....	27
5.3.1	SLA Compliance and Reporting .....	27
5.3.2	Scheduled and Emergency Portal Maintenance .....	27
5.3.3	Customer Contact Information .....	27
5.3.4	Customer Network/Server Change Notifications .....	27
5.3.5	Network Traffic Applicable to SLAs .....	27
5.3.6	Policy Change Request Overages .....	27
5.3.7	Services Decommission or Turn-Down .....	28
5.3.8	Testing of Monitoring and Response Capabilities .....	28
<b>6.</b>	<b>Other Terms and Conditions.....</b>	<b>28</b>
6.1	Modification of Services .....	28
6.2	Data Compilation.....	28
6.3	Customer General Responsibilities .....	28
6.4	Mutual Responsibilities.....	29

## Services Description

---

### IBM Managed Security Services for Unified Threat Management - Standard

#### 1. Scope of Services

IBM Managed Security Services for Unified Threat Management – Standard (called “MSS for UTM - Standard” or “Services”) is designed to provide monitoring and support of unified threat management devices (called “Agents”) across a variety of platforms and technologies. Such Agents must not be used for any other purpose while under management by IBM.

MSS for UTM - Standard is provided in two distinct packages:

- Protection Package - includes Intrusion Prevention System (“IPS”) and firewall support; and
- Content Package – an optional add-on package that includes management of, and support for, Web filtering, antispam, and antivirus modules.

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. 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”).
- c. 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.
- d. virtual private network (“VPN”)  
VPN utilizes public telecommunications networks to conduct private data communications, using encryption. Most implementations use the Internet as the public infrastructure, and a variety of specialized protocols to support private communications.
- e. antispam  
Antispam technology is designed to minimize the volume of spam email to user mail boxes.
- f. Web filtering  
Web filtering helps Customer block objectionable content, mitigate Web-borne threats, and govern Web viewing behavior of personnel behind the managed Agent.
- g. antivirus  
Antivirus systems scan many kinds of file transfers (such as Web pages, email traffic, and file transfer protocol (“FTP”) exchanges) for worms, viruses, and other forms of malware.

#### 3. MSS for UTM - Standard Features

The following table highlights the measurable Services features of MSS for UTM - Standard. 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="#">Internet emergency</a>	N/A	N/A
<a href="#">Authorized Security Contacts</a>	3 users	N/A
<a href="#">Log/event archival</a>	up to 7 years (1 year default)	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="#">Policy change request</a>	2 per month	N/A
<a href="#">Policy change request acknowledgement</a>	2 hours	<a href="#">Policy change request acknowledgement SLA</a>
<a href="#">Policy change request implementation</a>	24 hours	<a href="#">Policy change request implementation SLA</a>
<a href="#">Agent health alerting</a>	30 minutes	<a href="#">System monitoring SLA</a>
<a href="#">Content updates</a>	72 hours	<a href="#">Content update SLA</a>

### 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) Agent configuration and policy details;

- (3) security incident and service ticket information;
  - (4) ticketing and workflow initiation and updates;
  - (5) live chat and collaboration with SOC analysts;
  - (6) a template-driven reporting dashboard;
  - (7) access to real-time and archived Agent logs and events;
  - (8) authorization to download log data; and
  - (9) 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 policy change requests to the SOCs for a managed Agent or a group of Agents;
    - (d) submitting Services requests to the SOCs;
    - (e) "live chat" communicating with SOC analysts regarding specific incidents or tickets, generated as part of the Services;
    - (f) creating internal Services-related tickets and assigning such tickets to Portal users;
    - (g) querying, viewing, and updating Services-related tickets;
    - (h) viewing and editing Agent details;
    - (i) viewing Agent policies;
    - (j) creating and editing vulnerability watch lists;
    - (k) performing live event monitoring;
    - (l) querying security event and log data;
    - (m) scheduling downloads of security event and log data;
    - (n) 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 or begin management of an existing 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, to help develop the required security strategy for the Agent.

##### ***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. use the information provided in the data gathering form to assess Customer's existing environment;
- b. determine an optimal Agent configuration; and
- c. if applicable, provide recommendations to adjust the policy of an Agent or layout of the network to enhance security.

**Task 3 - Assess Existing Agent**

IBM will:

- a. remotely assess the Agent to verify it meets IBM specifications;
- b. identify application and user accounts to be removed or added, as applicable;
- c. for Agents not meeting IBM's specifications:
  - (1) identify Agent software requiring upgrading, and/or
  - (2) identify Agent hardware requiring upgrading to meet applicable vendor compatibility lists.

**Completion Criteria:**

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

**Deliverable Materials:**

- None

**Activity 4 - Implementation**

The purpose of this activity is to implement the Agent.

**Task 1 - Configure the Agent**

IBM will:

- a. remotely assess the Agent to verify it meets IBM specifications;
- b. identify Agent software, hardware, and/or content that does not meet current IBM-supported levels ;
- c. as appropriate, identify required hardware upgrades to support applicable vendor hardware compatibility lists;
- d. remotely configure the Agent, including setting the policy, hardening the operating system, and registering the Agent with the MSS infrastructure;
- e. provide live phone support and location of vendor documents to assist Customer in configuring the Agent with a public IP address and associated settings. Such support must be scheduled in advance to ensure availability of an IBM deployment specialist;
- f. tune the Agent policy to reduce the number of erroneous alarms (if applicable); and
- g. at Customer's request, exercise the configuration and policy on the existing Agent.

**Task 2 - Install the Agent**

IBM will:

- a. provide live support, via phone and/or email, to assist Customer in locating applicable vendor documents that detail physical installation procedures and cabling. Such support must be scheduled in advance to ensure availability of a deployment specialist;
- b. provide recommendations to adjust the layout of the network to enhance security (as applicable);
- c. remotely configure the Agent, including registering the Agent with the IBM MSS infrastructure; and
- d. tune the Agent policy to reduce the number of erroneous alarms (if applicable).

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

**Completion Criteria:**

This activity will be complete when the Agent is registered with the IBM MSS infrastructure.

**Deliverable Materials:**

- None

**Activity 5 - Testing and Verification**

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

IBM will:

- verify connectivity of the Agent to the IBM MSS infrastructure;
- perform Services acceptance testing;
- verify delivery of log data from the Agent to the IBM MSS infrastructure;
- verify availability and functionality of the Agent in the Portal;
- perform quality assurance testing of the Agent; and
- 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 6 - Services Activation**

The purpose of this activity is to activate the Services.

IBM will:

- assume management and support of the Agent;
- set the Agent to “active”;
- transition the Agent to the SOCs for ongoing management and support; and
- 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:

- 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:
  - attend the project kickoff call;
  - serve as the interface between IBM’s deployment team and all Customer departments participating in the Services deployment;
  - help resolve Services deployment issues, and escalate issues within Customer’s organization, as necessary; and
- 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***

Customer agrees to:

- a. maintain current licensing, and support and maintenance for the Agents; and
- b. perform all IBM-requested changes to Customer's network layout to enhance security.

#### ***Task 3 - Assess Existing Agent***

Customer agrees to:

- a. to ensure the existing Agent meets IBM's specifications;
- b. to remove or add IBM-specified applications and user accounts;
- c. if requested by IBM:
  - (1) to upgrade IBM-specified Agent software; and
  - (2) to upgrade IBM-specified Agent hardware.

### **Activity 4 - Implementation**

#### ***Task 1 - Configure the Agent***

Customer agrees to:

- a. update Agent software or content to the most current IBM-supported version (i.e., physically load media as applicable);
- b. update hardware to support applicable vendor hardware compatibility lists (if applicable);
- c. adjust the Agent policy as requested by IBM;
- d. configure the Agent with a public IP address and associated settings; and
- e. assist IBM in exercising the existing Agent configuration and policy (if applicable).

#### ***Task 2 - Install the Agent***

Customer agrees to:

- a. work with IBM in locating vendor documents that detail physical installation procedures and cabling. Customer will schedule such support in advance to ensure availability of an IBM deployment specialist;
- b. be responsible for the physical cabling and installation of the Agent(s); and
- c. perform any IBM-specified adjustments to the layout of the network to enhance security.

### **Activity 5 - Testing and Verification**

Customer agrees to:

- 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 and management.

**Activity 6 - 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).

**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 one year of log and event data storage unless otherwise specified by Customer;
- 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 the default (one year) retention period or the Customer-defined retention periods (if applicable); or
  - (2) 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 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 seven years;
- 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 UTM - 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) unless otherwise specified in writing by Customer, IBM will maintain the logs for one calendar year;
  - (2) all log and event data will be transmitted to the SOCs via the Internet;
  - (3) data traveling across the Internet is encrypted using industry-standard strong encryption algorithms whenever possible;

- (4) IBM can only collect and archive log and event data that successfully reaches the IBM MSS infrastructure;
- (5) 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;
- (6) IBM has the right to throttle event streams generated by the Agent that exceed 100 EPS (if required);
- (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 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. 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 Customer via the Portal.

Automated analysis and the subsequent AI alerts generated by the X-Force Protection System are available only on IBM-specified platforms.

#### 3.7.1 IBM Responsibilities

IBM will:

- a. submit collected event data to the X-Force Protection System AI analysis engine for correlation and identification;
- b. display alerts generated by the X-Force Protection System AI analysis engine in the Portal, as such alerts become available; and
- c. if configured by Customer, 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](#)".

#### 3.7.2 Customer Responsibilities

Customer agrees:

- a. to be responsible for enabling/disabling AI engine rules, using the Portal;
- b. to be responsible for scheduling X-Force Protection System alert notification, using the Portal;
- c. and acknowledges:
  - (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 only on IBM-specified platforms.

### 3.8 Policy Management

IBM defines a single rule-based Agent policy/configuration change as any authorized request for the addition or modification of one rule on one context with five or fewer objects in a single request. A change request requiring the addition of six or more objects or the manipulation of two or more rules will

be counted as two or more requests. If the request applies to changes outside of the rule-based Agent policy, each submitted request will be considered a single change.

Customer may configure the managed Agent with a single global policy that applies to all ports.

### 3.8.1 IBM Responsibilities

IBM will:

- a. accept up to two policy change requests per month from Authorized Security Contacts or Designated Customer Contacts, via the Portal;
- b. acknowledge policy change requests via the Portal within the timeframes established in the section of this Services Description entitled "Service Level Agreements", "[Policy change request acknowledgement](#)";
- c. review submitted policy change requests to verify Customer has provided all required information in such requests;
- d. if necessary, notify the submitter that additional information is needed. During this time, service level agreement ("SLA") timers will be placed on hold;
- e. prepare and review the policy change configuration as requested by Customer;
- f. implement policy change requests within the timeframes established in the section of this Services Description entitled "Service Level Agreements", "[Policy change request implementation](#)";
- g. document details of the policy change request in the IBM MSS ticketing system;
- h. display policy change request tickets in the Portal;
- i. at Customer's request, and for an additional charge (and subject to availability of IBM resource), provide additional policy changes;
- j. perform daily configuration backup of the managed Agent;
- k. maintain 14 configuration backups;
- l. display the current configuration of the Agent in the Portal;
- m. on a quarterly basis upon Customer's written request:
  - (1) audit Customer's policy settings to verify accuracy; and
  - (2) work with Customer to review Agents under management and provide recommended changes to the network protection strategy.

### 3.8.2 Customer Responsibilities

Customer agrees:

- a. to ensure all policy change requests are submitted by an Authorized Security Contact or a Designated Customer Contact, using the Portal, in accordance with the established procedures identified above;
- b. to be responsible for providing sufficient information for each requested policy change to allow IBM to successfully perform such change;
- c. to be responsible for notifying IBM if it wishes IBM to perform a quarterly policy review;
- d. to be solely responsible for its own security strategy, including security incident response procedures;
- e. and acknowledges:
  - (1) all policy changes will be completed by IBM and not by Customer;
  - (2) implementation of policy changes that IBM has deemed as having an adverse impact on the Agents' ability to protect the network environment will result in the suspension of applicable SLAs; and
  - (3) following closure of a calendar month, unused changes are considered void and may not be rolled over to the following month.

## 3.9 Virtual Private Network Support

Using one of the following methods, IBM will enable the Customer-requested VPN features of the managed Agent:

- a. site-to-site VPNs between two IBM-managed VPN capable Agents, or one IBM-managed Agent and a non-IBM-managed VPN capable device;
- b. client-to-site VPNs through a model where IBM establishes the configuration and enables Customer to administer client-to-site VPN users;
- c. Secure Sockets Layer (“SSL”) VPNs through a model where IBM establishes the configuration and enables Customer to administer SSL VPN users.

Support for client-to-site and SSL VPNs are available only on IBM-specified platforms.

### 3.9.1 IBM Responsibilities

IBM will:

- a. configure up to two site-to-site VPNs during the deployment and activation of each Agent;
- b. provide support for static and dynamic authentication methods of the VPN configuration;
- c. configure client-to-site VPNs, and create and authorize up to five client-to-site VPN users;
- d. configure SSL VPNs, and create and authorize up to five SSL VPN users;
- e. provide Customer with appropriate access permissions to administer its client-to-site or SSL VPN users; and
- f. provide Customer with a demonstration of client-to-site or SSL VPN user administration (if applicable).

### 3.9.2 Customer Responsibilities

Customer agrees:

- a. to provide IBM with all required information to enable the Customer-requested VPN features;
- b. to be solely responsible for creating and administering all client-to-site and SSL VPN users after the initial enablement by IBM;
- c. and acknowledges:
  - (1) any site-to-site VPNs it requests after deployment and activation of the Agent will be counted against the current month’s policy change allocation;
  - (2) it is solely responsible for the procurement and all associated charges for any required client-to-site or SSL VPN administration applications from the Agent manufacturer;
  - (3) it is solely responsible for the support and maintenance, and all associated charges, for any required client-to-site or SSL VPN administration applications assigned to the Agent manufacturer;
  - (4) that client-to site VPN solutions must be approved by IBM; and
  - (5) certificate-based authentication is not currently supported as part of the VPN configuration.

## 3.10 Managed Agent Health and Availability Monitoring

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

### 3.10.1 IBM Responsibilities

#### Activity 1 - Monitoring

The purpose of this activity is to monitor the health and performance of the Agents. IBM MSS will perform this task using either Agent-based monitoring or Agentless monitoring.

#### Agent-Based Monitoring

When technically feasible, IBM will install software on eligible Agents to monitor system health and performance, and report metrics back to the SOCs.

IBM will:

- a. for eligible platforms, install monitoring software on the Agents;
- 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.

#### **Agentless Monitoring**

When it is not technically feasible to install monitoring software, IBM will monitor the data stream coming from the Agents and/or poll administrative interfaces on the Agents.

IBM will:

- a. monitor the administrative interfaces of the Agents; and/or
- b. monitor the event stream generated by the Agents; and
- c. initiate additional time-based checks if contact with a managed Agent is lost.

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

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

IBM will:

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

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

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

IBM will:

- a. notify Customer if the Agent 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 Agent, following initiation of telephone notification; and
- c. display Agent health and outage tickets in the Portal.

### **3.10.2 Customer Responsibilities**

#### **Activity 1 - Monitoring**

Customer agrees to:

- a. allow IBM to install monitoring software on all managed Agents, where such installation is deemed by IBM to be technically feasible; or
- b. allow IBM to monitor the administrative interfaces and event stream of the managed Agents when it is not technically feasible to install monitoring software on such Agents.

#### **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 Out-of-Band ("OOB") solution, or if the OOB solution is unavailable for any reason; and
- c. and acknowledges that if the managed Agent 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.

### **3.11 Agent Management**

Agent application and security updates are critical components of an enterprise. IBM uses a vendor agnostic approach to Agent management.

#### **3.11.1 IBM Responsibilities**

IBM will:

- a. be the sole provider of software-level management for the Agents;
- b. maintain system status awareness;
- c. install new security content updates on the Agents, as they become available, within the timeframe established in the section of this Services Description entitled "Service Level Agreements", "[Proactive security content update](#)";
- 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 Agent 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 and Customer-specific requirements.

#### **3.11.2 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 Agent 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.

### **3.12 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.

#### **3.12.1 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 Agent reports that include attack metrics, prevented attacks, vulnerability impact, event counts/trending;
- f. event correlation and analysis; and
- g. firewall reports that include summary, traffic analysis, protocol usage, targeted IP and rule utilization.

### **3.12.2 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 Content Security**

The Agent can be configured to enable a content security solution on certain IBM-specified platforms. MSS for UTM - Standard does not support external content security solutions.

If requested by Customer, IBM can provide support for the following content features of the managed Agent:

- Web filtering;
- antispam; and
- antivirus.

#### **4.1.1 IBM Responsibilities**

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

- a. configure the Agent to support an internal content security solution on an IBM-specified platform;
- b. configure a Customer-specific Web filtering content security policy during deployment and activation of the Agent that includes:
  - (1) category lists – a selection of content categories to block;
  - (2) destination white lists – specific sites that should be blocked even if they exist within a denied content category;
  - (3) destination black lists – specific sites that should be blocked even if they exist within an allowed content category; and
  - (4) source white list – specific IP addresses that should be excluded from content filtering;
- c. configure a Customer-specific antispam policy during deployment and activation of the Agent that includes:
  - (1) white lists – specific email addresses and/or domains to always pass; and
  - (2) black lists – specific email addresses and/or domains that should be blocked.
- d. enable antivirus support during deployment and activation of the Agent;
- e. apply content security updates as described in the section of this Services Description entitled "Agent Management"; and
- f. accept and apply content security policy changes as described in the section of this Services Description entitled "Policy Management".

#### **4.1.2 Customer Responsibilities**

Customer agrees:

- a. to be responsible for providing sufficient information for each requested policy change to allow IBM to successfully perform such change;
- b. to be responsible for all charges associated with ongoing management of the content security solution;
- c. and acknowledges:

- (1) it is responsible for the procurement, support, licensing, maintenance, and other associated charges for the content security solution; and
- (2) all changes to the content security policy requested after deployment and activation of the Agent will be counted against the current month's policy change allocation.

## **4.2 Out-of-Band Access**

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

### **4.2.1 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 managed Agents; or
- c. work in good faith with Customer to utilize an IBM-approved existing OOB solution.

### **4.2.2 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 Agent;
  - (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 Agents; 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.

## **4.3 Cold Standby**

Cold standby is a method of disaster recovery whereby a spare Agent is available as a substitute in the event the primary Agent has a hardware and/or software failure. Cold standby Agents are not powered or ready for use, and do not contain active configuration, policy, or content updates.

### **4.3.1 IBM Responsibilities**

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

- a. work with Customer to transition the cold standby Agent to production and set such Agent to "active" in the event the primary Agent fails;
- b. apply required content updates to the cold standby Agent in the event the primary Agent fails; and
- c. apply the active current configuration to the Agent in the event the primary Agent fails.

### **4.3.2 Customer Responsibilities**

Customer agrees:

- a. to provide a secondary Agent to act as a cold standby Agent;

- b. to maintain current licensing, and support and maintenance contracts, for the cold standby Agent;
- c. to work with IBM to transition the cold standby Agent to production and set such Agent to “active” in the event the primary Agent fails;
- d. and acknowledges that:
  - (1) cold standby Agents are not managed and maintained by IBM unless they are transitioned to “active”;
  - (2) cold standby Agents require configuration changes in order to transition to “active”; and
  - (3) cold standby Agents may not generate traffic for the SOCs unless the primary Agent has failed and the cold standby Agent has been placed into production and transitioned to “active”.

#### **4.4 Warm Standby**

Warm standby is a method of redundancy that can reduce downtime due to Agent hardware and/or software failures. Warm standby management is designed to provide Customer with the option of having IBM manage and keep up to date a single spare Agent. In the event Customer's primary Agent fails, the spare or “warm” Agent will be on-hand to restore Services more quickly. A standby Agent may not generate any traffic for the SOCs unless it is placed into production and set to “active”.

IBM strongly encourages OOB access to the warm standby Agent as described in the section of this Services Description entitled “Out-of-Band Access”.

##### **4.4.1 IBM Responsibilities**

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

- a. maintain health and availability status of the warm standby Agent as described in the section of this Services Description entitled “Managed Agent Health and Availability Monitoring”;
- b. apply content updates to the warm standby Agents as described in the section of this Services Description entitled “Agent Management”; and
- c. transition the warm standby Agent to “active” in the event the primary Agent fails.

##### **4.4.2 Customer Responsibilities**

Customer agrees:

- a. to maintain current licensing, and support and maintenance contracts, for all warm standby platforms;
- b. to be responsible for all charges associated with ongoing management of the warm standby Agent;
- c. to provide secondary IP addressing;
- d. to comply with and perform Customer Responsibilities as described in the section of this Services Description entitled “Managed Agent Health and Availability Monitoring”;
- e. to comply with and perform Customer Responsibilities as defined in the section of this Services Description entitled “Agent Management”;
- f. and acknowledges that:
  - (1) policy changes made to the primary Agent will not be reflected on the warm standby Agent;
  - (2) standby Agents may not generate traffic for the SOCs unless they have been placed into production and set to “active”; and
- g. 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.

#### **4.5 High Availability**

To help protect against hardware and/or software failure and provide high availability (“HA”), two managed protection Agents may be configured and deployed; one fully operational and the other waiting as a backup to take over should the first Agent fail. Some Agents can also be deployed as clusters, such that multiple Agents operate and share network load.

##### **Active/Passive Implementations**

In this configuration, a second Agent is configured, ready to begin serving the network if the primary Agent experiences a critical hardware or software failure. In such a scenario, failover is automatic and immediate.

### **Active/Active Implementations**

Active/active clusters use two or more Agents to handle the network traffic simultaneously. In this configuration, each Agent handles a share of the network packets, determined by a load-balancing algorithm. If one Agent fails, the other Agent(s) is/are designed to automatically handle all of the traffic until the failed Agent has been restored.

IBM strongly encourages OOB access to all Agents in the high availability configuration, as described in the section of this Services Description entitled "Out-of-Band Access".

#### **4.5.1 IBM Responsibilities**

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

- a. configure a secondary Agent in either an active/passive or active/active configuration, as specified by Customer;
- b. configure active/active configurations utilizing three or more Agents ("cluster") in unicast mode (i.e., communication between a single sender and a single receiver over a network);  
Note: IBM does not support active/active configurations in multicast mode.
- c. manage and monitor the HA solution;
- d. maintain health and availability status of the secondary Agent as described in the section of this Services Description entitled "Managed Agent Health and Availability Monitoring";
- e. apply content updates to the secondary Agent(s) as described in the section of this Services Description entitled "Agent Management"; and
- f. update the policy of the secondary Agent as described in the section of this Services Description entitled "Policy Management".

#### **4.5.2 Customer Responsibilities**

Customer agrees:

- a. to provide a secondary Agent;
- b. to make any required changes to software licensing;
- c. to provide secondary IP addressing;
- d. to be responsible for all charges associated with ongoing management for the secondary Agent;
- e. to comply with and perform Customer Responsibilities as defined in the section of this Services Description entitled "Managed Agent Health and Availability Monitoring";
- f. to comply with and perform Customer Responsibilities as defined in the section of this Services Description entitled "Agent Management";
- g. to comply with and perform Customer Responsibilities as defined in the section of this Services Description entitled "Policy Management";
- h. to be responsible for providing all remote configuration and troubleshooting, if Customer elects not to implement an OOB solution on both the primary and secondary Agents or if the OOB solution is unavailable for any reason; and
- i. and acknowledges that:
  - (1) the Services do not support non-integrated HA solutions;
  - (2) IBM supports active/active configurations utilizing three or more Agents in unicast mode only.

#### **4.6 Onsite Aggregator**

The Onsite Aggregator ("OA") is a Customer-provided device that is deployed at Customer's location. The purpose of the OA is to centralize the collection of log and security event data when Customer has multiple Agents subscribing to MSS, and securely transmit this data to IBM MSS for further processing and long-term storage.

The basic functions of the OA are to:

- a. compile or otherwise combine the security events and log data;
- b. compress the security events and log data;
- c. 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:

- 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; and
- d. 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 OOB access to the OA, as described in the section of this Services Description entitled "Out-of-Band Access".

#### **4.6.1 IBM Responsibilities**

At Customer's request, and for an additional charge specified in an Order, IBM will provide the following services.

##### **Activity 1 - Configuration**

The purpose of this activity is to 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 with 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 an IBM deployment specialist;
- e. at Customer's request, and for an additional charge specified in an Order, 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 Customer.

##### **Activity 2 - Installation**

The purpose of this activity is to install the OA.

IBM will:

- a. provide live support, via phone and email, and will assist Customer 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;

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.

##### **Activity 3 - Ongoing Management and Support**

The purpose of this activity is to provide ongoing management and support of the OA.

IBM will:

- a. set the OA to "active" in the SOCs for ongoing support and management;

- b. maintain health and availability status of the OA as described in the section of this Services Description entitled “Managed Agent Health and Availability Monitoring”;
- c. apply software updates to the OA as described in the section of this Services Description entitled “Agent Management”; and
- d. be responsible for the management and monitoring of the OA for the term of the contract and during any renewal period.

#### **4.6.2 Customer Responsibilities**

##### **Activity 1 - Configuration**

Customer agrees:

- 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 install the IBM-provided OA software on the Customer-provided hardware, under the guidance of IBM;
- d. to configure an external IP address and associated setting on OA;
- e. to provide IBM with the OA IP address, hostname, machine platform, application version, and Agent time zone; and
- f. for existing platforms, to procure and install IBM-requested hardware upgrades.

##### **Activity 2 - Installation**

Customer agrees to:

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

##### **Activity 3 - Ongoing Management and Support**

Customer agrees to:

- a. be responsible for procuring and installing required hardware upgrades to the OA platform for the term of the contract;
- b. comply with and perform Customer Responsibilities as described in the section of this Services Description entitled “Managed Agent Health and Availability Monitoring”; and
- c. comply with and perform Customer Responsibilities as described in the section of this Services Description entitled “Agent Management”.

#### **4.7 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.

##### **4.7.1 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.

##### **4.7.2 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.

#### **4.8 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.

#### **4.8.1 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.

#### **4.8.2 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. Security incident identification – IBM will identify all 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 Customer's 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 Customer's 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 Customer's 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.
- b. Security incident alert notification – If X-Force Protection System alert notification has been configured by Customer in the Portal, IBM will send an hourly email notification to the Designated Customer Contact, summarizing any 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).
- c. Policy change request acknowledgement – IBM will acknowledge receipt of Customer's policy change request within two hours of receipt by IBM. This SLA is only available for policy change

- d. Policy change request implementation – IBM will implement Customer policy change requests within 24 hours of receipt by IBM unless the request has been placed in a “hold” status due to insufficient information required to implement the submitted policy change request. This SLA is only available for policy change requests submitted by an Authorized Security Contact or a Designated Customer Contact in accordance with the established procedures documented in the Portal.
- e. Proactive system monitoring – IBM will notify Customer within 30 minutes after IBM determines Customer’s Agent is unreachable via standard in-band connectivity.
- f. Proactive security content update – IBM will begin application of new security content updates within 72 hours after such update is published as generally available by the applicable vendor.
- g. Services availability – IBM will provide 100% service availability for the SOCs.
- h. 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. 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, policy change request acknowledgement, policy change request implementation, proactive system monitoring, proactive security content update, 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
Security incident identification	Credit for 1 month, 1 week, or 1 day for the initial Agent that reported the event, as indicated above
Security incident alert notification	Credit of 1 day of the monthly monitoring charge for the affected Agent
Policy change request acknowledgement	
Policy change request implementation	
Proactive system monitoring	
Proactive security content update	
Services availability	
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

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.