Managed Security Services - Managed Detection and Response

The services described herein are governed by the terms and conditions of the agreement specified in the Order Document for IBM Security Services (“Order Document”). If there is a conflict between the terms in the documents, the terms of the Order Document prevail over those of this document, and the terms of this document prevail over those of the agreement specified in the Order Document ("the Agreement"). Capitalized terms not otherwise defined in this document are defined in the Agreement or any other referenced document, and have the same meaning in this document as ascribed to them therein.

This document describes the Services and incorporates by reference the following contract document(s). The terms and conditions contained in the incorporated document(s) are in addition to the terms and conditions contained herein.

Contract Document(s)	Document #
Managed Security Services General Provisions	I126-8484
Standard Services Deployment and Activation	I126-7794

The document(s) identified above are located at: http://www.ibm.com/services/iss/wwcontracts. From this security services contract documents portal, Client selects the applicable country to access the above documents. If any documents are not accessible, please request a copy from Client's IBM sales contact.

1.1 Services

IBM will provide Managed Detection and Response (“Services”), which includes threat intelligence, advanced malware analysis, threat monitoring, threat hunting, and response services. These services utilize endpoint detection and response technology across a variety of endpoint/host platforms such as laptops, desktops, servers, and fixed function devices (e.g., point-of-sale terminals, kiosks, etc.) This document describes the Services IBM provides to Client. Services may include the following core service offering as selected in the Order document, and Client may purchase add-on(s) to the core offering as described in this document.

This service provides the following capabilities:

- Deployment, configuration and SOC onboarding (i.e., establishing SOC contacts, device records, etc.);
- Connection to a system information and event management (“SIEM”), if applicable;
- Agent app and device support module (“DSM”) enablement and configuration (if applicable);
- Endpoint telemetry (threat feed and watch list configuration, tuning);
- Automated threat monitoring and threat detection;
- Proactive threat hunting with complete threat investigations, threat assessment reports, and response recommendations;
- Threat intelligence and analytics;
- IBM portal for Client access and communication with IBM analysts;
- Remediation actions;
- Quarterly checkpoints; and
- Ongoing configuration and endpoint telemetry tuning.

Unused investigation entitlement as specified in the Order Document will rollover one time for the following month.

If additional proactive hunting investigations are indicated and the monthly allotment including rollovers have been exceeded, IBM will, as a one-time courtesy during the life of the contract, provide up to three (3) investigations.

Operational Hours for this service

Configuration / telemetry tuning, and threat hunting investigation requests will be met during the following hours (subject to change).

Monday to Friday: 06:00 am to 21:00 GMT

1.1.1 Services Activities – Incident Assessment Workshop

IBM Responsibilities

IBM will:

a. provide a remote (usually via conference call) 2-hour workshop including:
   (1) information gathering around Client's environment;
   (2) introduce personnel providing service(s), confirm location(s);
   (3) review current incident management and workflow procedures and processes; and
   (4) pre-emptive incident preparation – best practices;
b. discuss current threat and risk levels, threat intelligence feeds and telemetry policy tuning.

Client Responsibilities

Client will:

a. agree to identify relevant subject matter experts and/or Client contact to participate in the workshop and provide required information; and
b. within one month of any expiration or termination of Services, unless agreed in writing by IBM at the time, return all products or assets (including without limitation all whole or partial copies thereof) and destroy and certify as such in writing to IBM all documentation and all IBM Confidential Information.

1.1.2 Services Activities – Tuning, Threat Hunting and Steady State

There will be an initial tuning phase for telemetry tuning, learning, and contextual awareness. During this phase, IBM will provide threat hunting and steady state activities listed below for a specific set of end-points and/or for a duration (not to exceed eight (8) weeks) mutually agreed upon by Client and IBM dur-ing the Ser-vice kickoff. Following the completion of the tuning phase, the Service is considered to be in Steady State.

IBM Responsibilities

IBM will:

a. provide automated detection and threat monitoring based on the intelligence feed, watchlist configu-ration, and other telemetry obtained from a SIEM, if applicable;
b. categorize security events/incidents into critical, high, medium, and low priority events, based on the National Institute of Standards and Technology's security incident categorization, modified as fol-lows:
   (1) critical event: critical business impact, unauthorized access, brand damage, data theft, com-promised asset;
   (2) high event: significant business impact, potential loss of data, denial of service;
   (3) medium event: malware or malicious code, potential loss of service, data, business impact;
   (4) low event: reconnaissance or scans or probes, policy violations or improper usage, others and uncategorized event;
c. provide proactive threat hunting on the critical and high events using knowledge of Client's envi-ronment, current threat landscape and global threat intelligence;
d. provide in the event the outcome of the proactive threat hunting warrants a security incident notifica-tion, deep dive malware analysis, response recommendations, perform and complete investigations and reports for up to any and all remaining number of investigations specified in the Order Docu-ment;

e. notify Client Contact regarding security events using one or more of the following means: electronically via the SOC portal or via telephone;

f. make recommendations to Client as to any remediation actions to be performed on endpoints in response to an identified threat;

g. make any additional remediation actions in the event additional containment procedures may be required or warranted in response to an identified threat;

h. take additional action in the case malware detected warrants further remediation, which may include but not limited to:

   (1) endpoint isolation (isolate a computer from the rest of the network, leaving only connections needed for access to its sensor by the management server; and

   (2) banning process hashes (ban a process hash so that the process cannot be run again on hosts reporting to this management server and any running version of it is terminated);

i. provide a digital threat/incident summary report and remediation recommendations/actions taken;

j. make telemetry/configuration changes as appropriate and required;

k. respond to Client's requests for investigations, for up to any remaining number of investigations specified in the Order Document;

l. provide quarterly briefing checkpoints (up to two (2) hours via conference call) to review incident reports, any changes to incident reporting procedures, telemetry, processes, workflows, and technologies;

m. monitor the Services infrastructure and remediate issues as necessary;

n. perform patches and upgrades of the management system;

o. notify Client if sensors require updating; and

a. notify Client if parts of the IBM solution become unreachable.

Client Responsibilities

Client will:

a. review incident tickets, alerts, reports, and events provided on the customer SOC portal or via other electronic and/or telephone means;

b. implement recommended remediation techniques if available and applicable;

c. if applicable, request threat hunting / additional analysis for up to any remaining number of investigations specified in the Order Document;

d. provide written approval for any and all remediation and recommended actions as required by IBM;

e. give IBM prior written notice of any software or hardware alterations or attachments which may affect Services;

f. ensure appropriate Client entities are available for quarterly briefings; and

g. install sensors as recommended by IBM.