IBM Cloud Security Services -
Managed Distributed Denial of Service Protection
Service Description
Table of Contents

IBM Cloud Security Services ..............................................................................................................................1
Managed Distributed Denial of Service Protection ..............................................................................................1
Service Description ..............................................................................................................................................1

1. Managed Distributed Denial of Service Protection Services .....................................................................3
2. Definitions ....................................................................................................................................................4

3. Managed DDoS Protection Services ñ Foundational Features ....................................................................5
   3.1 Mss Portal ...........................................................................................................................................5
   3.2 Luna Portal .......................................................................................................................................5
   3.3 MDDoS Contacts ...............................................................................................................................6
   3.4 IBM X-Force Threat Analysis .........................................................................................................8
   3.5 Deployment and Activation ..............................................................................................................10

4. Managed DDoS Protection Services ñ Common Features ......................................................................11
   4.1 Threat Analyst Monitoring and Notification ....................................................................................11
   4.2 Policy Management ........................................................................................................................12
   4.3 Preparation Consulting ....................................................................................................................13
   4.4 Response Consulting .......................................................................................................................15

5. Managed DDoS Protection ñ Optional Features .....................................................................................17
   5.1 Mitigation Technology - Kona Site Defender ..................................................................................17
   5.2 Your Mitigation Technology Responsibilities ................................................................................18
6. Additional DDoS Fee Protection Terms ................................................................. 19
   6.1 SSL Certificates ............................................................................................... 19
      6.1.1 IBM’s SSL Certificate Responsibilities .................................................... 19
      6.1.2 Your SSL Certificate Responsibilities ...................................................... 20
   6.2 Enhanced DNS .................................................................................................. 20
   6.3 User Validation Module .................................................................................... 21
   6.4 Ticket System Integration ................................................................................ 21
      6.4.1 IBM Ticket System Integration Responsibilities ....................................... 21
      6.4.2 Your Ticket System Integration Responsibilities ....................................... 21

7. Service Level Objectives and Agreements .......................................................... 21
   7.1 Service Level Objectives .................................................................................. 21
   7.2 Kona Site Defender Service Level Availability .............................................. 22
      7.2.1 Service Levels for Kona Site Defender ..................................................... 22
      7.2.2 SLA Monitoring Methodology for Kona Site Defender ............................. 22
      7.2.3 Performance Metric .................................................................................. 23
      7.2.4 Outages ...................................................................................................... 23
      7.2.5 SLA Activation ........................................................................................... 23
      7.2.6 Governing SLA .......................................................................................... 23
   7.3 Simulation Mode SLA Modification ................................................................. 23

8. Limitation of Services ........................................................................................... 23

9. Permission to Perform Testing ............................................................................. 24

10. Systems Owned by a Third Party ....................................................................... 24

11. Acceptable Use Policy ......................................................................................... 25

12. Suspected Violations ............................................................................................ 25

13. Bandwidth Overage Policy ................................................................................ 25


15. Other Disclaimers ............................................................................................... 25

16. Indemnification ................................................................................................... 26

17. General ................................................................................................................ 26
Services Description

IBM Cloud Security Services - Managed Distributed Denial of Service Protection

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-935.ibm.com/services/be/iss/pdf/BEL_INTC-8484-02.pdf AND INCORPORATED HEREIN BY REFERENCE.

1. Managed Distributed Denial of Service Protection Services

IBM Cloud Security Services – Managed Distributed Denial of Service Protection Services (called "MDDoS" or "Services") is designed to provide monitoring, alerting and support of denial of service security technologies across a variety of platforms and technologies. Such Services must not be used for any other purpose while under management by IBM.

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.

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

MDDoS includes preparation, mitigation, monitoring, response and security intelligence.

DDoS Preparation - IBM will provide resources to assist you in DDoS protection preparation including assessing incident readiness and preparing response protocols.

DDoS Mitigation - IBM will provide a multi-layered defense architecture that caches host data in the cloud and extends visibility and control to the edge of the internet. MDDoS is designed to provide the DDoS cloud mitigation technology specified in Optional Features in this service description. The DDoS mitigation technology platform (also called "Kona Site Defender") includes thousands of servers worldwide and provides local and global load balancing of network traffic using proprietary algorithms and continuous performance monitoring. The platform also provides network and rate controls, a web application layer firewall, IP white/blacklisting, geo access controls, and site cloaking. All legitimate, non-cached internet traffic will source from a limited range of servers, allowing perimeter firewalls the ability to filter traffic sources. IBM will provide access to the Luna Portal that you can access and use to monitor real time events.

DDoS Monitoring and Management - IBM will provide steady state support for the DDoS mitigation technology which includes 24x7 monitoring of web application firewall alerts.

DDoS Response - IBM will provide resources to assist you with computer security incidents, covering enterprise wide emergency incidents in addition to DDoS attacks. IBM will provide resources to assist you in responding to computer security incidents, including steps for data collection and analysis, intelligence gathering, containment, eradication, recovery, and prevention. IBM will use existing, commercially available tools, as well as IBM proprietary tools, to perform the services. Such tools and their associated documentation remain the property of IBM or third parties.

Security Intelligence - IBM X-Force Hosted Threat Analysis Service (XFTAS) is a security intelligence service that is designed to deliver customized information about a variety of threats that could affect your network security.

Each of the above mentioned services provide features that are categorized as Foundational, Common and Optional features.
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 “MSS Portal”).

Antispam – is designed to minimize the volume of spam e-mail to user mail boxes.

Antivirus – is designed to scan many kinds of file transfers (such as Web pages, e-mail traffic, and file transfer protocol (“FTP”) exchanges) for worms, viruses, and other forms of malware.

Application or “App” – means any discrete instance of computer software that performs a particular function for you or your end user and can be accelerated by any acceleration Service. For billing purposes, each instance of any such software is considered an independent “Internet Application” or “App”. For example, each Application running on a particular platform (e.g., Force.com, Amazon AWS, Microsoft Azure, SAP, .NET, etc.) is considered a discrete App, while the platform itself would not be considered an App. Also, a portal consisting of many Applications will be counted as more than one application.

Authorized Security Contact -- a decision-maker on all operational issues pertaining to the DDoS Protection feature(s).

CSIRP – Computer Security Incident Response Plan.

CSIRT – Computer Security Incident Response Team.

Content – information, software, and data that you provide, including, without limitation, any hypertext markup language files, scripts, programs, recordings, sound, music, graphics, images, applets or servlets that you or your subcontractors or services recipients create, install, upload or transfer to or through the Edge Platform.

DDoS – (distributed denial-of-service) or DoS (denial-of-service) attack.

Digital Property – a Site requiring separately configured and distinct application services deployed on the Edge Platform, reporting feeds or invoicing. A Digital Property may consist of at most one domain name and five hostnames.

Designated Services Contact -- a decision-maker on a subset of operational issues pertaining to each IBM DDoS Protection feature, the feature’s Service(s), or a group of Service(s).

Edge Platform – a cloud-based network platform providing distributed denial-of-service protection.

EdgeServer – one or many servers within the Edge Platform.

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.

Emergency Incident Declaration (EIR) – a request for assistance responding to a computer security incident.

ERS – emergency response service(s).

Firewall – 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 the Services Recipient’s security policy.

IBM Managed Security Services (“IBM MSS”) Portal (called “MSS Portal”) -- The MSS Portal provides access to an environment (and associated tools) designed to monitor and manage security posture by merging technology and service data from multiple vendors and geographies into a common, Web-based interface.

Luna Portal Users – are users of the Luna Portal with different levels of authorization to the Luna Portal.
MSS Portal Users – are users of the MSS Portal with different levels of authorization to the MSS Portal. MSS Portal Users can have restricted, regular, or administrative MSS Portal access to all MSS Service(s), or just a subset of MSS Service(s). The MSS Portal views and permissions available to the MSS Portal Users are dictated by the Authorized Security Contact.

NetStorage – on demand storage capacity.

Purchased Subscription Hours – Number of Emergency Incident Support or consulting hours included annually for the contract term.

Request – a request to an Edge Platform server to retrieve an item of anonymous non-personally identifiable user data from an Edge Platform proprietary database or to perform a certain function specified by you.

Site – means a set of URLs used to deliver content and Applications for a discrete and individual corporate unit (e.g., legal entity, company business unit, publishing group, product brand or Application) that may consist of at most one (1) domain and up to ten (10) hostnames. For example, in the case of www.customer.com and images.customer.com “customer.com” is the domain and “www” and “images” are hostnames.

SSL – secure sockets layer.

SSL Network Access – a network resource allocated to you for the purpose of accelerating SSL sessions with a X.509 digital certificate. You purchase the type of digital certificate to be included with the SSL Network Access, such as Standard (Single-Hostname), Wildcard, SAN, Extended Validation (EV), Extended Validation SAN or Third Party.

WAF – Web Application Firewall.

3. Managed DDoS Protection Services – Foundational Features

Foundational features are provided with MDDoS and are not optional. There may be different levels of the feature that can be provided, however these features are included with MDDoS.

3.1 MSS Portal

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

The MSS 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 MSS 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.

3.2 Luna Portal

The Luna Portal provides access to an environment (and associated tools) designed to look at real-time metrics of available cloud data.

3.2.1 IBM MSS Portal & Luna Portal Responsibilities

IBM will:

a. provide access to the MSS Portal & Luna Portal 24 hours/day, 7 days/week;

b. as part of IBM's MSS Portal Responsibilities, provide:

   (1) multiple levels of access for MSS Portal users which may be applied to an IBM Managed Security Service, an MSS Service, or a group of Service(s);

   (2) security intelligence awareness and alerting;

   (3) security incident and/or service ticket information;
(4) ticketing and workflow initiation and updates;
(5) interaction with SOC analysts;
(6) access to Education Materials in accordance with the terms provided in the MSS Portal; and
(7) where applicable, the MSS Portal will include:
   (a) the ability to parse and normalize unknown, text-based system activity logs; and
   (b) the ability to create user-defined correlation rules.

c. maintain availability of the MSS Portal in accordance with the metrics provided in the section of this
   Services Description entitled “Service Level Objectives and Agreements”;

d. provide a username, password, URL and appropriate permissions to access the MSS Portal and
   Luna Portal; and

e. as part of IBM's Luna Portal Responsibilities, provide:
   (1) access to view DDoS Services configuration and policy details where applicable;
   (2) access to DDoS Services logs and events where applicable;
   (3) authorization to download DDoS log data when applicable; and
   (4) access to perform live event monitoring, where applicable.

3.2.2 Your MSS Portal & Luna Portal Responsibilities
You agree to:

a. ensure your employees accessing either Portal on your behalf comply with the Terms of Use
   provided therein;

b. appropriately safeguard your login credentials to either Portal (including not disclosing such
   credentials to any unauthorized individuals);

c. promptly notify IBM if a compromise of your login credentials is suspected;

d. indemnify and hold IBM harmless for any losses incurred by you or other parties resulting from your
   failure to safeguard your login credentials;

e. utilize the MSS Portal to perform daily operational Services activities; and

f. not adjust any MDDoS specific configuration and/or policy settings within the Luna Portal.

3.3 MDDoS Contacts
You may choose from multiple levels of access to the SOC and the MSS Portal to accommodate varying
roles within your organization: Authorized Security Contacts, Designated Services Contacts, and MSS
Portal Users.

3.3.1 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 MSS Portal permissions to your MSS Service(s) as applicable;
   (2) the authorization to create Designated Services Contacts and MSS 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 MSS Features; and

d. verify the identity of Authorized Security Contacts using an authentication method that utilizes a pre-
   shared challenge pass phrase.

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

3.3.2 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;
b. interface only with Designated Services Contacts regarding the subset of operational issues for which such contact is responsible.

You will:

a. provide IBM with contact information including roles and responsibilities for each Designated Services Contact. Such Designated Services Contacts will be responsible for authenticating with the SOCs using a pass phrase; and
b. 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 (e.g., FW Service(s) outage).

3.3.3 MSS Portal Users

IBM will:

a. provide multiple levels of access to the MSS Portal, as follows:
   (1) administrative user capabilities which will include:
       (a) creating MSS users;
       (b) submitting policy change requests to the SOCs;
       (c) submitting other (non-policy-based) MDDoS requests to the SOCs;
       (d) "live chat" communicating with SOC analysts regarding specific incidents or tickets, generated as part of MDDoS;
       (e) creating internal MDDoS-related tickets and assigning such tickets to MSS Portal users;
       (f) querying, viewing, and updating MDDoS-related tickets; and
       (g) viewing MDDoS policies, where applicable;
   (2) regular user capabilities which will include all of the capabilities of an administrative user, for services to which they have been assigned, with the exception of creating MSS Portal users;
   (3) restricted user capabilities which will include all of the capabilities of a regular user, for the services to which they have been assigned, with the exception of:
       (a) creating and submitting policy change requests; and
       (b) updating tickets.
b. provide you with authorization to apply levels of access to MDDoS or groups of MDDoS services;
c. authenticate MSS Portal Users using static password; and
d. authenticate MSS Portal Users using two-factor authentication tokens you provide (RSA SecureID).

You agree:

a. that Portal users will use the Portal to perform daily operational MDDoS 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 IBM X-Force Threat Analysis

Security intelligence is provided by the IBM X-Force Threat Analysis Center. The X-Force Threat Analysis Center publishes an Internet threat-level. The Internet threat-level describes progressive alert postures of current Internet security threat conditions. In the event Internet threat-level 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. Utilizing the MSS Portal, you can create a vulnerability watch list with customized threat information. In addition, each MSS 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 MSS Portal (including 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 MSS Portal Terms of Use shall prevail over this Agreement. In addition to the Terms of Use provided in the MSS 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.

3.4.1 IBM Security Intelligence Responsibilities

IBM will:

a. provide access, via the MSS Portal, to the X-Force Hosted Threat Analysis Service;
b. display security information on the MSS Portal as it becomes available;
c. if configured by you, provide security intelligence specific to your defined vulnerability watch list, via the MSS Portal;
d. if configured by you, provide an Internet security assessment e-mail based on your subscription, each business day;
e. publish an Internet threat-level via the MSS Portal;
f. declare an Internet emergency if the daily Internet threat level reaches threat-level 3;
g. provide MSS Portal feature functionality to create and maintain a vulnerability watch list;
h. provide additional information about an alert, advisory, or other significant security issue as IBM deems necessary; and
i. provide access to regularly produced IBM X-Force Threat Reports via the MSS Portal.

3.4.2 Your Security Intelligence Responsibilities

You will use the MSS Portal to:

a. subscribe to the daily Internet security assessment e-mail, at your option;
b. create a vulnerability watch list, if desired;
c. access the IBM X-Force Threat Reports; and
d. agree to adhere to the licensing agreement and not forward 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 MDDoS or begin management of an existing MDDoS.  

Note: Deployment and Activation activities are performed one time during the performance of the MDDoS. If you choose to replace, upgrade, or move your MDDoS during the contract, IBM may require that such MDDoS be redeployed and reactivated (called "Redeployment").  Such Redeployments will be provided at an additional charge.  Redeployment charges apply only to MDDoS changes that you initiate.

3.5.1 **IBM Deployment and Activation Responsibilities**

**Activity 1 - Project 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 2 - Assessment**

The purpose of this activity is to perform an assessment of your current environment, business and technology goals. In addition, this assessment will be used to help develop the required security strategy for all applicable MDDoS services.

**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 MDDoS delivery or timelines.

**Task 2 - Assess Environment**

IBM will:

a. use the information provided in the data gathering form to assess your existing environment;
b. determine an optimal MDDoS configuration; and
c. if applicable, provide:
   - recommendations to adjust the policy of the MDDoS configuration.

**Completion Criteria:**

This activity will be complete when IBM has assessed your environment.

- None
Activity 3 - Implementation
The purpose of this activity is to implement MDDoS and IBM will provide the following services where applicable.

Task 1 - Configure MDDoS
IBM will:
- remotely assess MDDoS to verify it meets IBM specifications;
- remotely configure MDDoS, including setting the policy;
- tune the MDDoS policy to reduce the number of erroneous alarms (if applicable); and
- at your request, exercise the configuration and policy on the existing MDDoS.

Completion Criteria:
This activity will be complete when MDDoS is configured.

Deliverable Materials:
- None

Activity 4 - Testing and Verification
The purpose of this activity is to perform testing and verification of MDDoS.

IBM will:
- perform MDDoS acceptance testing;
- verify availability and functionality of MDDoS in the MSS Portal;
- perform quality assurance testing of MDDoS; and
- remotely demonstrate the primary features of MDDoS 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 MDDoS.

Deliverable Materials:
- None

Activity 5 - Activation
The purpose of this activity is to activate MDDoS.

IBM will:
- assume management and support of MDDoS;
- set MDDoS to “active” (where applicable); and
- transition MDDoS to the SOCs for ongoing management and support.

Completion Criteria:
This activity will be complete when MDDoS is set to “active”.

Deliverable Materials:
- None

3.5.2 Your Deployment and Activation Responsibilities

Activity 1 - Project Kickoff
You agree to:
- attend the project kickoff call; and
- review each party’s respective responsibilities.
Activity 2 - 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 MDDoS 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.

Activity 3 - Implementation
This activity will need to be performed by you for MDDoS (where applicable).

Task 1 - Configure MDDoS
You agree to:

a. assist IBM in exercising the existing MDDoS configuration and policy (if applicable).

Activity 4 - Testing 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; and

c. and acknowledge that additional acceptance testing performed by you, or lack thereof, does not preclude IBM from setting MDDoS to “active” in the SOCs for ongoing support and management.

Activity 5 - Activation
No additional responsibilities are required by you for this activity.

4. Managed DDoS Protection Services – Common Features
Common features allow you to define (where applicable) the necessary response, escalation, implementation or update timeframe associated with the service.

4.1 Threat Analyst Monitoring and Notification
Threat Analyst Monitoring and Notification will be provided as part of MDDoS. IBM MSS security analysts will perform monitoring and analysis of alerts. Whether or not an alert is considered a security incident is determined solely by IBM. Alerts will be classified, prioritized, and escalated as IBM deems appropriate. Alerts that are not eliminated as benign 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 defensive action within 1 hour of occurrence.

- 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.
4.1.1 IBM Threat Analyst Monitoring and Notification Responsibilities

IBM will:

a. perform investigation and analysis of alerts;
b. when possible, eliminate false positives and benign triggers and classify them as commented security incidents (“CSI”);
c. identify alerts that are not eliminated as benign triggers and classify such alerts as security incidents (“SI’s”):
   (1) start the SLA timers; and
   (2) prioritize the SI as either high, medium or low;
d. using the standard notification path that you provide, escalate SIs to an Authorized Security Contact or Designated 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 Objectives and Agreements”, “Security Incident Notification”;
e. provide remediation/countermeasure recommendations, if applicable;
f. document details of CSIs and SIs in the IBM ticketing system; and
g. list CSIs and SIs in the MSS Portal.

4.1.2 Your Threat Analyst Monitoring and Notification Responsibilities

You agree:

f. to utilize the MSS and Luna Portals for investigation of logs and events that are not considered to be immediate threats;
g. to provide IBM with current in-depth documentation of your environment;
h. to update IBM within three calendar days of changes within your environment;
i. to provide IBM with the following information, and keep such information current via the MSS Portal:
   (1) information about monitored networks;
   (2) authorized scanners; and
   (3) Trusted IP addresses that are exempt from monitoring.
j. to provide and keep current a linear contact notification path, including telephone numbers and e-mail addresses;
k. to update IBM, via the MSS Portal, within three calendar days of a change in your contact information;
l. to provide e-mail aliases, as necessary, to facilitate notification;
m. to ensure an Authorized Security Contact or Designated Services Contact listed in the notification path is available 24 hours /day, 7 days / week;
n. to view details of CSIs and SIs via the MSS Portal;
o. to work with IBM to optimize the monitoring service;
p. to provide feedback on CSIs and SIs via the MSS Portal;
q. and acknowledge that:
   (1) once IBM has escalated an SI, you are solely responsible for all SI incident responses, and remediation activities; and
   (2) not all investigations of alerts will result in the declaration of an SI;
   (3) Alert Monitoring and Notification applies only to alerts resulting from analysis performed against applicable MDDoS services;
   (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 Objectives and Agreements” will be null and void.

4.2 Policy Management
Policy Management will be provided as part of MDDoS. IBM will provide the following services where applicable.

4.2.1 IBM Policy Management Responsibilities
IBM will:

a. accept policy change requests up to the designated number of changes selected by you per month from Authorized Security Contacts or Designated Services Contacts, via the MSS Portal;

b. acknowledge policy change requests via the MSS Portal within the timeframes established in the section of this Services Description entitled “Service Level Objectives and Agreements”, "Policy change request acknowledgement";

c. review submitted policy change requests to verify you have provided all required information in such requests;

d. if necessary, notify the submitter that additional information is needed. During this time, service level objective (“SLO”) timers will be placed on hold;

e. prepare and review the policy change configuration as requested by you;

f. implement policy change requests within the time specified in the Schedule as the Time to Implement which is selected by you when initiating your change request through the MSS Portal. Time to Implement options are established in the section of this Services Description entitled “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 MSS Portal;

i. rollover any unused policy change requests from the current month to the next month; rollover policy change requests will be available for use until the last day of the following month, at which point, if unused, these rollover policy change requests will expire;

j. at your request, and for an additional charge (and subject to availability of IBM resource), provide up to the number of policy changes as specified in the Schedule;

k. upon your written request, provide up to the number of policy reviews as specified in the Schedule;

(1) audit your policy settings to verify accuracy; and

(2) work with you to review MDDoS under management and provide recommended changes to DDoS protection strategy.

4.2.2 Your Policy Management Responsibilities
You agree:

a. to ensure all policy change requests are submitted by an Authorized Security Contact or a Designated Services Contact, using the MSS 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 you wish IBM to perform a policy review;

d. to be solely responsible for your own security strategy, including security incident response procedures; and

e. and acknowledge:

(1) all policy changes will be completed by IBM and not by you;
implementation of policy changes that IBM has deemed as having an adverse impact on the MDDoS ability to protect the network environment will result in the suspension of applicable SLAs;

following closure of a calendar month, unused changes will be used upon request by you for an extended period of 30 days. After this 30 day period, these changes will no longer be available. Unused policy changes that have rolled over to the following month will be used first before using the new month’s policy changes;

to clearly identify a policy change that requires an emergency implementation when submitting such a request in the MSS Portal; and

to contact the SOC via telephone, following submission of an emergency policy change request using the MSS Portal, to escalate such policy change request to an emergency status.

4.3 Preparation Consulting

Note: Preparation Consulting is for year 1 only or your contract period, as specified in the Schedule. Year 2 and beyond, any un-used hours (of the 120 hour cap per year) can be used for proactive work such as proactive penetration test—where proactive scope is jointly determined and agreed to by both you and IBM on a per request basis.

4.3.1 IBM Preparation Consulting Responsibilities

Activity 1 - Project Initiation

IBM will facilitate a remote project initiation workshop, for up to one hour, on a mutually agreed date and time.

IBM agrees to:

a. introduce the personnel to be providing MDDoS consulting;
b. confirm your locations to be included in the MDDoS response;
c. review MDDoS setup and service offering features;
d. define the process for making an Emergency Incident Declaration, including establishing the designated telephone number(s) and e-mail address(es);
e. review processes for responding to an Emergency Incident Declaration and for exchanging security incident data in a secure manner; and
f. develop a service calendar outlining regular checkpoint schedules, and selected preemptive incident preparation tasks.

Completion Criteria:

This activity will be considered complete when the project kickoff workshop has been conducted and the service calendar delivered.

Deliverable Materials:

• service calendar

Activity 2 - DDoS Protection and Preemptive Incident Preparation

IBM will facilitate remote (or on-site if requested by you) workshop, for up to one week (five days), on a mutually agreed date and time.

IBM agrees to:

a. review current network architecture and logical application architecture in accordance to planned DDoS deployment;
b. identify and document potential risks and recommendations from existing architecture as applicable;
c. review the current computer security incident response plan for your enterprise, if available, make recommendations for incorporating MDDoS and incident response into the plan and identify potential issues;
d. conduct interviews, via conference call (or on-site if requested by you), for up to one day, with key
CSIRP participants such as I/T system administration, I/T network administration, I/T security,
corporate security, business continuity, legal, human resources, and public relations;

e. document findings and recommendations;

f. discuss findings, for up to two hours, via conference call with your computer security incident
response team; and


g. conduct a workshop for up to four hours to provide first responder training and discuss DDoS
incident scenarios, for up to 12 attendees.

Completion Criteria:
This activity will be considered complete when IBM has provided the number of hours mutually agreed
upon or provides the deliverable material for the task(s) performed, or when the contract end date has
passed.

Deliverable Materials:

- DDoS Protection and Preemptive Incident Preparation Report
  The DDoS Protection and Preemptive Incident Preparation Report consists of the following, as
appropriate:
  (1) Summary of the review and exercises;
  (2) Current network and application architecture;
  (3) Findings and recommendations;
  (4) Industry best practices for incident response plan as appropriate;
  (5) Gaps and recommended updates to the existing incident response policy and process;
  (6) Description of incident scenario; and
  (7) Any observations and recommendations resulting from the mock incident scenario.

IBM will deliver one copy of the applicable deliverable(s) electronically to your Point of Contact within five
business days following the closing of the activity.

Activity 3 - Quarterly Incident Related Support and Status Update
The purpose of this activity is to provide you with ongoing incident related support, up-to-date threat
trends, and status updates.

IBM agrees to:

a. provide up to 8 hours telephone support each quarter with access to advice and assistance from
ERS during normal business hours (currently 8 a.m. to 5 p.m., Eastern Time) on topics in the areas
of security incident assessment, preparedness, management, response, and basic triage;

b. provide a checkup via remote teleconference for up to 2 hours to review quarterly status, relevant
events, service hours utilized and remaining, update service schedule, provide update on threat
trends, ensure your incident response readiness, and provide recommendations if appropriate;

c. document result of each telephone support and discussion of the checkup teleconference in a
quarterly status report; and

This activity will be considered complete when IBM has provided the following deliverable at the end of
each quarter according to the service calendar.

Deliverable Materials:

- Quarterly Status Report
  The Quarterly Status Report consists of the following, as appropriate:
  (1) Status of activities and tasks performed or in progress in the reporting quarter;
  (2) Documentation of remote support provided in the reporting quarter;
Relevant trends and industry updates on incident management; and
Documentation of any issues or risks.

IBM will deliver one copy of the applicable deliverable(s) electronically to your Point of Contact within five business days following the closing of the activity.

4.3.2 Your Preparation Consulting Responsibilities
No additional responsibilities are required by you for Preparation Consulting.

4.4 Response Consulting

4.4.1 IBM Response Consulting Responsibilities
IBM agrees to:

a. Provide emergency response 24 hours/day, 7 days/week for Emergency Incident Declarations per the term of this Services Description and the Schedule. Such response will utilize included subscription hours for on-site and/or remote support for the designated physical locations as specified in the Schedule. If additional physical location coverage is required in response to an incident, additional charges may apply;

b. within approximately one hour after receiving your call or e-mail for an Emergency Incident Declaration, host a conference call with your designated personnel to discuss the symptoms you are observing, actions taken and similar items;

c. provide assistance and advice if possible for handling the Emergency Incident Declaration including:
   (1) analysis of computer security incident data to determine the source of the incident, its cause, and its effects;
   (2) preventing the effects of the computer security incident from spreading to other computer systems and networks;
   (3) stopping the computer security incident at its source and/or protecting your computer systems and networks from the effects of the computer security incident;
   (4) recommendations for restoration of the affected computer systems and networks to normal operation; and
   (5) suggesting protection methods for your computer systems and networks from future occurrences of the computer security incident;

d. prepare and provide an After-Incident Report to your Point of Contact describing the computer security incident, causes and effects, actions taken by IBM, and recommended future actions to mitigate risk; and

e. provide additional emergency incident hourly support, in response to your written request. Such support will be provided based on the Usage charge specified as “Additional emergency incident hourly support” in the “Charges” section of the Schedule.

Note: The tasks outlined in this section, if performed, will consume included incident response hours. (40) hours are included and additional hours may be purchased at the Usage charge rate listed in the Schedule.

Completion Criteria:
This activity will be considered complete when the contract end date has passed.

Deliverable Materials:

- Incident Analysis Report, as applicable.

The Incident Analysis Report consists of the following, as appropriate:

(1) Executive Summary – a high level overview of the background and findings related to the incident;

(2) Data Collection and Preservation – specific actions and steps performed to collect and preserve incident data;
(3) Data Analysis – detailed results of the incident analysis; and
(4) Conclusions and Recommendations – summary of the incident and specific actions or considerations to help mitigate the risk of future occurrences.

IBM will deliver one copy of the applicable deliverable(s) electronically to your Point of Contact within five business days following the closing of the activity.

### 4.4.2 Your Response Consulting Responsibilities

You agree:

a. and acknowledge:

   (1) that you may not make an Emergency Incident Declaration until after the project kickoff session has been conducted;
   (2) your additional locations, or locations not specified in the Schedule, must be contracted for separately;
   (3) one IBM consultant will be assigned for remote and/or on-site Emergency Incident Declaration response to the declared physical location. Additional IBM consultants must be contracted for separately and are subject to availability; and
   (4) that if IBM discovers what it considers, in its sole discretion, to be inappropriate content during the performance of MDDoS, IBM has the authority to report such information to law enforcement. Examples of what IBM would consider inappropriate content includes, but is not limited to, content or activity that involves obscene, pornographic or violent material;

b. to provide the IBM specialist with the names and telephone numbers (including after hours telephone or pager numbers) of your lead investigator, technical and management contact personnel (including backup personnel) who have the authority to make Emergency Incident Declarations and act upon suggestions and recommendations made by IBM;

c. to make appropriate personnel available during IBM’s response to an Emergency Incident Declaration to answer questions, obtain requested data, perform suggested actions, and similar items;

d. to provide copies of all configuration information, log files, intrusion detection events, and other data related to an Emergency Incident Declaration and its analysis;

e. to manage the collection and dissemination of information regarding an Emergency Incident Declaration with your technical and managerial personnel, legal and public relations departments, others within your organization, and other companies as applicable;

f. to be responsible for and facilitate all communications between IBM and any third party vendors, including Internet service providers and content-hosting firms used by you to implement your Internet presence;

g. to provide supervised access to your computer systems and computer networks during the agreed upon times and days;

h. to provide IBM with an editable copy of you computer security incident response plan for review, if available;

i. and acknowledge, that during the Computer Security Incident Response Assessment Report review cycle only three opportunities will be allowed to provide input;

j. to provide your proposed changes, comments and feedback during the Computer Security Incident Response Assessment Report review cycle within 5 business days of the receipt of the report, at no additional charge to IBM;

k. and acknowledge, that during an emergency incident and upon your request to IBM, additional emergency incident support hours will be provided based on Usage charge specified in the Schedule;

l. to provide an executive sponsor for the services to communicate management commitment to the project; and
m. to be responsible for all charges associated with any additional Emergency Incident Declarations you make during the term of this Services Description.

5. Managed DDoS Protection – Optional Features

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

5.1 Mitigation Technology - Kona Site Defender

Kona Site Defender is designed to improve the security posture of your Sites and reduce the likelihood and impact of security events by mitigating attacks at the within the Edge Platform.

5.1.1 IBM Mitigation Technology Responsibilities

IBM will provide Kona Site Defender which consists of the following features and modules:

a. **Access Control**: Allows you to move access control and authentication functionality to the Edge Platform rather than requiring these decisions to be made through interaction with the origin, or to improve interaction with the origin where access is centrally managed.

b. **DDoS Fee Protection**: Provides you with adjusted overage fees incurred due to a DDoS Attack.
   
   (1) DDoS (distributed denial-of-service) or DoS (denial-of-service) Attack Definition: An ongoing traffic increase where Site traffic is four (4) or more times higher than the average Site traffic, per unit, over the immediately preceding two (2) month period,
   
   (2) You and IBM mutually agree that the traffic spike is malicious, and/or unwanted, and you requests IBM to declare the traffic as a DDoS attack, and
   
   (3) You informs IBM that they are willing to NOT serve the unexpected traffic and are willing to allow IBM to determine the approach for mitigating potential negative impacts of the DDoS traffic (e.g., blocking the traffic, redirecting the traffic, serving the traffic, etc.).

c. **Log Delivery**: Provides access to website and application logs for manipulation, analysis, and audit purposes

d. **Origin Cloaking**: shields an origin website from direct access from the public Internet.

e. **Security Monitor**: Luna Portal dashboard which displays real-time metrics of security events.

f. **Site and Visitor Intelligence**: Site and Visitor Intelligence provides you with additional reporting insight and consist of:
   
   (1) URL reporting on Luna Portal that allows you to obtain detailed reporting information on each configured URL. For each URL, you have access to traffic volume (MB delivered) and number of hits. You can also run reports on the top URLs by traffic volume and number of hits. URL reports can be run for HTTP Content, downloads (HTTP & FTP), and streaming services; and
   
   (2) visitor reporting on Luna Portal that provides powerful reporting insight into number of unique visitors as well as top visitors. Visitor demographics can be broken down by operating system, browser, top countries, and top US states.

g. **Site Failover consists of**:
   
   (1) Origin server monitoring – monitoring the availability of the origin server and re-routing origin server requests when the origin server is not available;
   
   (2) Failover to EdgeServer – You may specify Content to be served out of cache on the EdgeServer in the event of an origin failure;
   
   (3) Failover to NetStorage – If subscribed, you may upload a static Site to NetStorage to be served in the event of an origin failure;
   
   (4) Failover to alternate data center – if you have more than one origin server, the Service can detect the failure of one origin and direct requests to an alternate data center; and
   
   (5) Site Snapshot Tool – periodically copies site content to NetStorage.
h. Web Application Firewall (WAF): Provides a highly scalable layer of protection against application-level attacks from the Edge Platform and helps detect and deflect threats in HTTP and HTTPS traffic, thereby issuing alerts or blocking attack traffic near the source. The WAF module consists of:
   (1) Network layer controls including IP Blacklist, IP Whitelist and Strict IP Whitelist;
   (2) Network layer rules activity report;
   (3) Application layer controls – firewall rules;
   (4) Application layer rules activity report;
   (5) Real time reporting log functionality;
   (6) IP Rate Limitation – Enables monitoring and control of the rate of delivery by the Edge Platform and your origin for defined categories of requests; and
   (7) Custom Rules - Enables creation and management of create metadata-based rules that are enforced either before or after the execution of the application layer rules.

5.1.2 Your Mitigation Technology Responsibilities
You agree:

a. and acknowledge that Kona Site Defender does not prevent or eliminate all attacks;

b. IBM does not warrant or guarantee that Kona Site Defender will detect and mitigate all possible attacks and/or threats;

c. as set forth in the Schedule, Kona Site Defender shall be configured and enabled only for the associated Managed DDoS Protection Services features selected and specified or referenced in the Schedule;

d. to provide the URL(s) and/or domain(s) for the number of sites, as specified in the Schedule, to be covered by the Kona Site Defender Services;

e. to provide an escalation matrix including a minimum of three (3) contacts with name, email address and mobile phone information that IBM may need to reach during suspected attacks;

f. to ensure your provided contacts will be authorized individuals with origin access and authority to implement system changes recommended to manage an attack;

g. and acknowledge, indirect access to your appropriate resources may result in delays in the diagnosis and resolution of the attack;

h. and acknowledge that IBM will capture relevant proprietary service specific session information for purposes of identifying the source of DDoS traffic;

i. and acknowledge that IBM is not responsible for your action or non-action that might result in a service disruption, availability issues or performance degradation;

j. and acknowledge, traffic bursts or increased usage resulting from your actions that exceed your monthly bandwidth allocation for Kona Site Defender may incur usage fees, as specified in the Schedule; and

k. any requests that are not directly related to your use of the Edge Platform or extended use thereof, and are not related to the preparation or mitigation of malicious security events, shall be considered outside the scope of Kona Site Defender.

6. Additional DDoS Fee Protection Terms
For eligible requests, your overage fees for the month in which the DDoS Attack occurred are reversed and replaced with the “Capped Burst Fee” value set forth in the Schedule (unless actual overage fees are less than the Capped Burst Fee amount in which case the actual overage fees will apply).

a. By electing to purchase the DDoS Fee Protection module, you:
authorize IBM to impose technical measures available in the Edge Delivery Services that control and/or mitigate a DDoS Attack, even if such measures result in degraded application and/or site performance, and

acknowledge that Service Level Agreements do not apply during the period of a DDoS Attack.

b. To be eligible for a credit:

(1) the DDoS Attack must result in overage charges in excess of twice the average monthly overage fee measured in the preceding six (6) months, and excluding months in which a mutually agreed DDoS Attack occurred;

(2) You must notify IBM of a DDoS Attack;

(3) IBM must verify reported DDoS Attack is a legitimate Attack eligible for credit; and

(4) the credit requests must be submitted no later than thirty (30) days following a disputed invoice. When issuing a credit IBM shall have sole authority in determining whether the reported Service incident qualifies for credit. If your average monthly Service fee exceeds their selected tier or if more than two credits are requested in any given calendar year, then IBM shall have the right to require you to pay a higher Capped Burst Fee. A single credit shall be applied on a monthly basis, even when multiple Attacks occur in the month. WAF Module limitations consists of:

(a) provides protection for only digital properties associated with the applicable Service contractually associated with WAF Module;

(b) Real-Time Reporting (RTR) restricted to logging to servers that are digital properties specified in the Schedule that contain the WAF Module; and

(c) availability only as specified in the Schedule.

IBM DOES NOT WARRANT OR GUARANTEE THE WAF MODULE WILL DETECT ALL POSSIBLE ATTACKS AND/OR THREATS. IBM RECOMMENDS ALL CUSTOMERS MAINTAIN APPROPRIATE SECURITY CONTROLS ON THEIR ORIGIN SERVER(S). YOU ASSUME ALL RISK OF USE WITH CUSTOM RULES, INCLUDING POTENTIAL SERVICE OUTAGES DUE TO MISCONFIGURED RULES. THE SERVICE LEVEL AGREEMENT DOES NOT APPLY WHEN CUSTOM RULES ARE USED BY YOU.

6.1 SSL Certificates

SSL Certificates can be added to the Kona Site Defender installation for additional charge.

6.1.1 IBM's SSL Certificate Responsibilities

IBM can provide the following types of SSL certificates:

   ● A X.509 digital certificate identifying a single hostname that is issued by either Edge Platform or an Edge Platform-chosen certificate authority.

b. Wildcard Digital Certificate SSL Network Access
   ● A X.509 digital certificate that signs multiple hostnames within a specified domain. For example, the wildcard ".example.com" specifies the domain "example.com" and can sign hostnames such as "www.example.com" and "images.example.com". Wildcard Digital Certificates are is-sued by either Edge Platform or an Edge Platform-chosen certificate authority. In cases where Edge Platform issues the wildcard certificate there is a ten (10) hostname limit under the primary domain. Otherwise, Wildcard Digital Certificates can sign an unlimited quantity of hostnames in the specified domain.

c. Subject Alternative Name (SAN) SSL Network Access
   ● A SAN certificate allows multiple disjointed hostnames to be combined into a single certificate. e.g. www.example.com, www.example.co.uk, www.example.fr SAN certificates require a
minimum of 3 hostnames and allow a maximum of forty (40) hostnames including the common name.

d. Extended Validation Subject Alternative Name (EV SAN) SSL Network Access

Combines the flexibility and additional security of two (2) certificate types:

1. Extended Validation (EV) certificates are single hostname certificate signing one hostname (site) where address bar is rendered green, e.g. https://www.example.com.
   a. EV certificates require organizations submit to a rigorous validation process that meets the Extended Validation guidelines established by the Certification Authority Browser Forum (CA/Browser Forum).
   b. You must sign the Certificate Authority Subscriber Agreement, a separate agreement between you and the Certificate Authority, as a condition to the effectiveness of this Services Description.
   c. IBM is not a party to the Subscriber Agreement Terms and Conditions and is not liable for any violations of it by you.
   d. EV certificates cannot be renewed automatically, and require a subsequent re-validation.
2. A SAN certificates allow multiple disjointed hostnames to be combined into a single certificate. e.g. www.example.com, www.example.co.uk, www.example.fr SAN certificates require a minimum of three (3) hostnames and allow a maximum of forty (40) hostnames including the common name.

e. Extended Validation SSL Network Access

1. Extended Validation (EV) certificates are single hostname certificate signing one hostname (site) where address bar is rendered green, e.g. https://www.example.com.
   a. EV certificates require organizations submit to a rigorous validation process that meets the Extended Validation guidelines established by the Certification Authority Browser Forum (CA/Browser Forum).
   b. You must sign the Certificate Authority Subscriber Agreement, a separate agreement between you and the Certificate Authority, as a condition to the effectiveness of this Services Description.
   c. IBM is not a party to the Subscriber Agreement Terms and Conditions and is not liable for any violations of it by you.
   d. EV certificates cannot be renewed automatically, and require a subsequent re-validation.

f. Third Party Digital Certificate SSL Network Access

- A X.509 digital certificate furnished by you to Edge Platform for use with the purchased Service(s).

6.1.2 Your SSL Certificate Responsibilities

You hereby grant IBM and its subcontractor permission to reproduce and host the applicable 3rd Party SSL Certificate on its network for the purpose of providing Secure Content Delivery Service. You represent and warrant that it has the right to authorize IBM and its subcontractor to reproduce and host such 3rd Party SSL Certificate across the network and such actions are not in violation of any third party con-tract or rights. You agree to indemnify and hold harmless IBM and its directors, officers and employees and subcontractor’s from any losses that you may incur arising out of the use of the applicable 3rd Party SSL Certificate.”

6.2 Enhanced DNS

Enhanced DNS service provides an outsourced secondary DNS service via a distributed network of DNS servers deployed across multiple networks to improve DNS performance, security and scalability.
6.3 **User Validation Module**
User Validation provides understanding of whom or what is generating traffic targeting a web site. Browser traffic identified as potentially malicious will be redirected to a JavaScript confirmation page for verification. If the verification is accepted, the client request is accepted.

6.4 **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.

6.4.1 **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.

6.4.2 **Your Ticket System Integration Responsibilities**
You agree:
- a. to be responsible for all additional charges associated with API ticket integration;
- b. to utilize the 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.

7. **Service Level Objectives and Agreements**
IBM Service Level Agreements (SLAs) and Service Level Objectives (SLOs) establish response time objectives and countermeasures for specific events resulting from MDDoS. The SLAs and SLOs become effective when the deployment process has been completed, and support and management of MDDoS 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.

7.1 **Service Level Objectives**
The SLO defaults described below comprise the measured metrics for delivery of MDDoS. Unless explicitly stated below, no warranties of any kind shall apply to MDDoS delivered under this Services Description.
- a. Security incident identification – IBM will identify all events it deems to be Priority 1, 2, and 3 level security incidents based on Agent event data received by the SOCs (where applicable).
  - (1) Priority 1 incidents: high-risk events that have the potential to cause severe damage to your systems or environments and require defensive action. Priority 1 incident examples include 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.
  - (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.

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

- b. Security incident notification - IBM will initiate notification for all identified security incidents within the selected Incident Response SLA. Your Authorized Security Contact or Designated Services Contact will be notified by telephone for Priority 1 security incidents and via e-mail 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.

The incident response SLA that applies is based on the following options and is specified in the Schedule.

c. Policy change request acknowledgement – when applicable, IBM will acknowledge receipt of your policy change request by IBM within the Policy change request acknowledgement response time specified in the Schedule. This SLO is only available for policy change requests submitted by an Authorized Security Contact or a Designated Services Contact in accordance with the established procedures documented in the MSS Portal.

d. Policy change request implementation – when applicable, IBM will implement your policy change requests within the selected Time to Implement number of hours specified in the Schedule. The Time to Implement hours will be met 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 SLO is only available for policy change requests submitted by an Authorized Security Contact or a Designated Services Contact in accordance with the established procedures documented in the MSS Portal, and does not apply to policy change requests that exceed the monthly entitlements – commonly referred to as “overages”.

The policy change request implementation SLO that applies is based on the following Time to Implement options and is specified in the Schedule.

e. MDDoS availability – IBM will provide 100% service availability for the SOCs.

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

7.2 Kona Site Defender Service Level Availability

The SLA defaults described below comprise the measured metrics for delivery of Kona Site Defender. Unless explicitly stated below, no warranties of any kind shall apply to MDDoS delivered under this Services Description.

7.2.1 Service Levels for Kona Site Defender

IBM agrees to provide a level of service demonstrating:

a. 100% Uptime: The Service will serve content 100% of the time.

b. Measurable Performance Enhancement: Kona Site Defender will deliver content measurably faster than your web site.

7.2.2 SLA Monitoring Methodology for Kona Site Defender

The following methodology will be employed to measure the Kona Site Defender availability and performance enhancement: Agents and Polling Frequency

a. From at least six (6) geographically and network-diverse locations in major metropolitan areas, Akamai will simultaneously poll a test file residing on the your production servers and on Akamai’s network

b. The polling mechanism will perform two (2) simultaneous http GET operations:

c. A test file will be placed on your origin server (i.e., origin.customer.com).

d. One GET operation will be performed to retrieve the file directly from the origin server (i.e., http://origin.customer.com/testobject), or via an Akamai Site Shield region if the customer is using the Site Shield feature.

e. The other GET operation will be performed to retrieve the file through the Service, by requesting the object from your appropriate hostname CNAMEd to Akamai (i.e., http://www.customer.com/testobject, where www.customer.com is CNAMEd to Akamai and configured to pull content from origin.customer.com)
f. The test content must use a TTL of 2 hours or greater.
g. The test content will be a file of approximately 10 KB in size.
h. Polling will occur at approximately 6-minute intervals.
i. Based on the http GET operations described in II(b) above, the response times received from the two sources, (a) your server (directly, or via a Site Shield region if applicable), and (b) the Akamai network, will be compared for the purpose of measuring performance metrics and outages.

7.2.3 Performance Metric
The performance metric will be based on a daily average of performance for Kona Site Defender and your production web server (measured directly, or via a Site Shield region if applicable), computed from data captured across all regions and hits.

7.2.4 Outages
An outage is defined as a period of at least two consecutive failed attempts six minutes apart by a single agent to GET your test file from the Service while succeeding to GET the test file from your Origin Server (directly, or via a Site Shield region if applicable).

7.2.5 SLA Activation
In order to activate the Kona Site Defender Service Level Agreement, you must enter and indicate the location of two valid test files for the same object (as described in II(c) and (d) above) into the SLA Activation Tool located in the Provisioning Center on https://control.akamai.com (Luna Portal). Detailed instructions are provided with the SLA Activation Tool on https://control.akamai.com. Customers using Remote Site Shield must ensure that their firewall configurations are updated to reflect changes made by Akamai to the Site Shield access control list no later than 60 days following notification by Akamai, via email or the https://control.akamai.com Luna portal, of such a change. Failure to timely update such firewall configurations will invalidate the performance portion of this SLA. The SLA will go into effect within five business days after you enter valid test files into the SLA Activation Tool.

7.2.6 Governing SLA
This SLA shall apply solely to delivery configurations using the Kona Site Defender service. For delivery configurations using other services, the SLA for those services shall apply and supersede this SLA.

7.3 Simulation Mode SLA Modification
The Managed DDoS Protection service allows WAF policies to be tested in simulation mode. Any simulation mode testing will be performed by you, and will require DNS changes on the testing machine. You may enable and disable simulation mode at any time by one of the following methods:

a. pre-deployment - you must provide a written or e-mail policy change request to the assigned IBM deployment specialist.
b. post-deployment – you must submit requests to begin or end simulation mode via a service ticket or policy change request within the MSS Portal.

During simulation mode, all active blocking functionality will be disabled, thereby preventing active blocking in the cloud, and IBM will cease to provide you with the security incident prevention SLA as described in the section of this Services Description entitled “SLA Availability”.

8. Limitation of Services
You acknowledge and agree that the following are not included as part of MDDoS described herein:

a. services involving incidents of violence, injury to persons, or damage to or theft of tangible personal property;
b. services to identify a perpetrator; however, determining the source of network traffic or specific digital activity may be included in the services;
c. investigatory interrogation;
d. testifying in judicial or administrative proceedings;
e. communication on your behalf with any entity, such as law enforcement, the news media, or its customers;
f. any services requiring professional licensing of the service provider;
g. evidentiary chain of custody control or management, but IBM may adhere to your chain of custody procedures in performing its obligations hereunder, provided these are reviewed and agreed to by IBM prior to starting work;
h. legal counsel of any kind;
i. opinions as to the credibility of any person; or
j. any other related services which IBM, at its reasonable discretion, may at any time decline.

9. Permission to Perform Testing
If Purchased Subscription hours are utilized to perform any type of security testing, you acknowledge and agree that:

Certain laws prohibit any unauthorized attempt to penetrate or access computer systems. You authorize IBM to perform the Services as described herein and acknowledge that the Services constitute authorized access to your computer systems. IBM may disclose this grant of authority to a third party if deemed necessary to perform the Services.

The Services that IBM performs entail certain risks and you agree to accept all risks associated with such Services; provided, however, that this does not limit IBM’s obligation to perform the Services in accordance with the terms of this services description. You acknowledge and agree to the following:

a. excessive amounts of log messages may be generated, resulting in excessive log file disk space consumption;
b. the performance and throughput of your systems, as well as the performance and throughput of associated routers and firewalls, may be temporarily degraded;
c. some data may be changed temporarily as a result of probing vulnerabilities;
d. your computer systems may hang or crash, resulting in system failure or temporary system unavailability;
e. any service level agreement rights or remedies will be waived during any testing activity;
f. a scan may trigger alarms by intrusion detection systems;
g. some aspects of the Services may involve intercepting the traffic of the monitored network for the purpose of looking for events; and
h. new security threats are constantly evolving and no service designed to provide protection from security threats will be able to make network resources invulnerable from such security threats or ensure that such service has identified all risks, exposures and vulnerabilities.

10. Systems Owned by a Third Party
If Purchased Subscription hours are utilized to perform any type of security testing, you acknowledge and agree that:

For systems (which for purposes of this provision includes but is not limited to applications and IP addresses) owned by a third party that will be the subject of testing hereunder, you agree:

a. that prior to IBM initiating testing on a third party system, you will obtain a signed letter from the owner of each system authorizing IBM to provide the Services on that system, and indicating the owner's acceptance of the conditions set forth in the section entitled “Permission to Perform Testing” and to provide IBM with a copy of such authorization;
b. to be solely responsible for communicating any risks, exposures, and vulnerabilities identified on these systems by IBM’s remote testing to the system owner, and

c. to arrange for and facilitate the exchange of information between the system owner and IBM as deemed necessary by IBM.
You agree:

d. to inform IBM immediately whenever there is a change in ownership of any system that is the subject of the testing hereunder;

e. not to disclose the deliverable Materials, or the fact that IBM performed the Services, outside your Enterprise without IBM’s prior written consent; and

f. to indemnify IBM in full for any losses or liability IBM incurs due to third party claims arising out of the your failure to comply with the requirements of this section entitled, "Systems Owned by a Third Party" and for any third party subpoenas or claims brought against IBM or IBM’s subcontractors or agents arising out of (a) testing the security risks, exposures or vulnerabilities of the systems that are the subject of testing hereunder, (b) providing the results of such testing to you, or (c) your use or disclosure of such results.

11. Acceptable Use Policy

You represent and warrant that your use of the Services and all Content will comply with the acceptable Internet use policy for IBM services (“Acceptable Use Policy”) located on the Internet at www.ibm.com/services/e-business/aup.html, as of the Effective Date, and any subsequent modification. IBM, in its reasonable discretion, may modify the Acceptable Use Policy upon thirty (30) days’ prior notice to you. If such modification has a material adverse effect on your use of the Services and provided such modification is not required by law, regulation, or similar governmental action, or a ruling by a court of competent jurisdiction, your sole remedy is to terminate this Services Description pursuant to terms listed in the Schedule.

12. Suspected Violations

IBM reserves the right to investigate potential violations of the Acceptable Use Policy. If IBM reasonably determines that a breach of any such Acceptable Use Policy has occurred, then IBM may, in its sole discretion:

a. restrict your access to the Services or any offending Content;

b. terminate this Services Description pursuant to the Schedule; and

c. exercise other rights and remedies, at law or in equity.

Except in an emergency or as may otherwise be required by law, before undertaking the activities in this Section, Suspected Violations, IBM will attempt to notify you by any reasonably practical means under the circumstances, such as, without limitation, by telephone or e-mail.

You will promptly notify IBM of any event or circumstance related to this Services Description, your use of MDDoS, or Content of which you become aware that could lead to a claim or demand against IBM and you will provide all relevant information relating to such event or circumstance to IBM at IBM’s request.

13. Bandwidth Overage Policy

The pricing provided to you for the Managed DDoS Protection Services being purchased under this Order is limited to specific bandwidth capacity. You acknowledges and agrees that (i) such Service as delivered is capable of excess of the bandwidth capacity and such overages (not resulting from a DDoS attack) will result in Usage Overage Fees as defined in the Schedule, and (ii) use of the Services to process data in excess of the bandwidth capacity will require payment of an upgrade fee for the associated Managed Security Services should you exceed the bandwidth capacity for two consecutive months.

14. Security Disclaimer and Acknowledgment

You understand and agree that new technology, configuration changes, software upgrades and routine maintenance, among other items, can create new and unknown security exposures. Moreover, computer "hackers" and other third parties continue to employ increasingly sophisticated techniques and tools, resulting in ever-growing challenges to individual computer system security. IBM’s performance of Services as described in this Services Description does not constitute any representation or warranty by IBM about the security of your Content while loaded on or being transmitted through the Edge Platform including, but not limited to, any representation or warranty that your Content is safe from intrusions,
viruses, virus threats, or any other security exposures. IBM’s performance of the Services does not constitute any representation or warranty by IBM about the security of your computer systems including, but not limited to, any representation that your computer systems are safe from intrusions, viruses, or any other security exposures. IBM does not make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information provided as part of the Services.

15. Other Disclaimers
a. IBM does not warrant uninterrupted or error-free operation of any Service or that IBM will correct all defects.

b. IBM provides Materials, non-IBM products, and non-IBM services on an “AS-IS” BASIS WITHOUT WARRANTIES OR INDEMNITIES OF ANY KIND. However, non-IBM manufacturers, suppliers, or publishers may provide their own warranties or indemnities to you.

You understand and agree:

c. that it is solely within your discretion to use or not use any of the information provided pursuant to the Services hereunder. Accordingly, IBM will not be liable for any actions that you take or choose not to take based on the Services performed and/or deliverables provided hereunder;

d. that it is your sole responsibility to provide appropriate and adequate security for the company, its assets, systems and employees;

e. that it is your responsibility to add the IP addresses associated with the testers to any filtering devices, thereby permitting unfiltered network access to the target systems; and

f. not to modify the configurations of any in-scope systems and infrastructure devices during the period of testing.

16. Indemnification
You will defend IBM, its Affiliates, and its suppliers and their employees, officers, and directors, at your expense, and pay all costs, damages, and reasonable attorneys’ fees that a court finally awards (or which you agree in any final settlement) for any third party claim:

a. that Content or your use of the Services violates your obligation in section entitled Acceptable Use Policy;

b. that Content infringes that party’s patent or copyright; or

c. that is brought by a Services recipient and is related, directly or indirectly, to the Services.

For indemnification under this section entitled Indemnification IBM will:

d. promptly notify you in writing of the claim; and

e. allow you to control, and will cooperate with you in, the defense and any related settlement negotiations.

17. General
a. You acknowledge that IBM may use global resources and personnel located in various countries for the delivery of MDDoS.

b. Notwithstanding any provision of this Services Description and subject to applicable law and without waiver of any defenses that may be available to a party, a party may initiate proceedings for a preliminary injunction if necessary to protect such party’s confidential information or intellectual property rights at any time.

c. Except as may be required by law or as may be required for financing purposes or by IBM to perform MDDoS, neither party may disclose to any third party the terms and conditions of this Services Description, without prior written consent.

d. Any notices required or permitted hereunder will be effective upon receipt and will be: 1) personally delivered; 2) mailed; 3) sent by reliable overnight courier; or 4) transmitted by confirmed facsimile. All notices will be in writing and addressed to the applicable party’s designated representative.
Except as to notices permitted or required for a claim under “Patent and Copyrights”, “Limitation of Liability”, or for a termination for material breach, each of us may communicate with the other by electronic means and such communication is acceptable as a signed writing. In addition, IBM may provide notice under section entitled Acceptable Use Policy by a posting to the Web site identified in section entitled Acceptable Use Policy.

e. The failure of one party to insist upon strict adherence to any term of this Services Description on any occasion shall not be considered a waiver of such term, nor shall it deprive that party of the right to insist later on adherence thereto. Any such waiver must be in writing and signed by an authorized representative of the waiving party.