IBM United Kingdom Limited
Registered in England: 741598
Registered Office: PO Box 41,
North Harbour, Portsmouth,
PO6 3AU (hereinafter "IBM")

Services Description

IBM Hosted Application Security Services - Production Application Scanning

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/uk/gts/html/contracts_landing.html AND INCORPORATED HEREIN BY REFERENCE.

1. Scope of Services

IBM Hosted Application Security Services – Production Application Scanning Service (called "Services") is designed for IBM to provide the Services Recipient with the ability to initiate and perform application scans of production environments. The Service provides access to a hosted and managed IBM environment and includes training of your personnel to help them understand the features of the Service. Scans of customer environments are performed either by IBM or by the Services Recipient depending on the details of the customer order.

The Services are intended to be leveraged to assess the security posture of an application that is in a production environment and can be assessed using non-intrusive application checks.

The Services features described herein are dependent upon the availability and supportability of the 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 will be provided using IBM AppScan Enterprise Edition Software (the "Scanning Software").

2. Definitions

Alert Condition ("AlertCon") – a global risk metric, developed by IBM, using proprietary methods. The AlertCon is based on a variety of factors, including quantity and severity of known vulnerabilities, exploits for such vulnerabilities, the availability of such exploits to the public, mass-propagating worm activity, and global threat activity. The four levels of AlertCon are described in the IBM Managed Security Services ("IBM MSS") portal (called "Portal").

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

Content – All data that is specific to the Services Recipient which is scanned or created in connection with the Services Recipient's use of the Services.

Content Scan Job – A scan of selected Pages using the Services. As part of executing a Content Scan Job, all web pages scanned are retrieved for the purposes of analyzing the HTML code and subsequently discards these web pages upon completion of the analysis.

Content Scan Job Reports – A set of reports with respect to a specific Content Scan Job. The Content Scan Job stores information regarding this analysis in the form of Content Scan Job Reports and Report Packs (i.e., collections of Content Scan Job Reports). Information is stored in a relational database and is accessed via a web-based interface.

Only one set of Content Scan Job Report information is available at any one time (i.e., previous scan information is deleted when a Content Scan Job is re-executed). Summary and trend information is viewable online in the Scanning Platform for one year. At the end of the one year period, the data will be transitioned to offline storage (if applicable).

Pages – All web site pages identified as part of the Service, including without limitation, all HTML (static and dynamically rendered). The Modules Licenses information screen will identify all pages with the same URL as one (1) Page, irrespective of how many times they are scanned. However, where the same page exists in different web environments (i.e., two (2) pages with different URLs) the License Management tab will identify them as two (2) Pages.

Application - An application that executes a unique or self-containing piece of business functionality.

Scan Information – The detailed information and instruction provided by you to IBM and used by IBM to perform the Content Scan Jobs.

Server – Each separate operating system environment required to perform the Services.

User – An employee, independent contractor, consultant or agent identified and authorized by you to receive a unique, password protected, SSL (Secure Socket Layer) encrypted URL in order to use the Scanning Software and access the Content Scan Job Reports in accordance with the terms and conditions of this Services Description.

Scanning Platform – The hardware infrastructure and software which enables Content Scan Jobs to be executed.

Application Security Analyst (ASA) – An IBM security analyst that provides the application assessment services and acts as the clients' primary contact regarding the results of the service provided.

Security Test Policy – The specific set of tests as configured for the Service used to determine which security vulnerabilities a Content Scan Job will target.

3. Application Size

The size of an application directly affects the time required to properly assess the security posture of the application. For this reason, applications to be scanned under the IBM Hosted Application Security Services – Production Application Scanning are classified by application size:

Application Size	Page count	Forms	Login
Level 1 – Small	<1000	Form filling not supported	Login not supported
Level 2 – Large	>1000	Form filling not supported	Login not supported

The upper limit on the number of pages of a Level 2 application is 10,000. An application that exceeds that limit shall be considered 2 applications.

4. Services

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

Services Feature Summary

Services Feature	Metric or Qty	Service Level Agreements
IBM Scanning Platform availability	99.9%	Scanning Platform Availability SLA
IBM MSS Portal Availability	99.9%	Portal Availability SLA
Authorized Security Contacts	3 users	N/A
Scan Initiation Response	1 or 2 Business days	Scan Initiation Response SLA
Critical Priority Issue Alert Notification	60 Minutes	Critical Priority Issue Alert Notification SLA
Scan Review Initiation	1 Business day	Scan Review Initiation SLA
False Positive Rate	0%	False Positive rate SLA
Request To Re-scan - Execute	1 or 2 Business days	Request To Re-scan – Execute SLA
Response To Inquiry	4 Business hours	Response To Inquiry SLA

4.1 Security Operations Centers

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

4.2 Service Delivery

IBM Hosted Application Security Services are delivered by resources located in IBM facilities. The Scanning Platform is available 24 hours/day, 7 days/week; however, access to Application Security Analysts for Services is provided during normal business hours, 8:30 AM to 5:15 PM, Eastern Time (US & Canada GMT-05:00), Monday through Friday, except Canadian holidays.

4.3 Scanning Platform

The Scanning Platform provides you with a Web-based interface to the software which enables scans of your websites and/or web applications to be created and executed. The Scanning Platform enables you to view the results of scans and to view summarized reports of the scans.

4.3.1 IBM Scanning Platform Responsibilities

IBM will:

a. provide access to the Scanning Platform 24 hours/day, 7 days/week. The Scanning Platform will provide:

   (1) security intelligence awareness and alerting; and

   (2) access to Education Materials in accordance with the terms provided in the Scanning Platform.

b. maintain availability of the Scanning Platform in accordance with the metrics provided in the section of this Services Description entitled “Service Level Agreements”, “Scanning Platform”;

c. enable you to access the Service by providing you with a unique, password protected, SSL encrypted URL for each user you designate, subject to the limitation of number of users as set out in this Service Description;

d. perform system administration and maintenance of the scanning platform that ensures the platform is up to date with respect to the supported versions and security patches as designated by IBM; and

e. allow you to perform (i.e., create and execute) your own scans. The limitation on this capability is page-based and is derived from the Schedule of application scans that you have purchased and as described in the following table:

Product (SKU)	Scanning Multiplier	Page scanning limit per SKU
Production Scanning – L1 Small	1 times # of SKUs purchased	1,000
Production Scanning – L2 Large		5,000

4.3.2 Your Scanning Platform Responsibilities

You agree to:

a. ensure your employees accessing the Scanning Platform on your behalf comply with the Terms of Use provided therein including, but not limited to, the terms associated with Educational Materials;

b. safeguard your login credentials to the Scanning Platform (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, and

e. indemnify and hold IBM harmless for any losses incurred by you or other parties resulting from your use of the Scanning Platform.

4.4 Portal

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

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

FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF PROPRIETARY AND INTELLECTUAL PROPERTY RIGHTS.

4.4.1 IBM Portal Responsibilities

IBM will:

a. provide access to the Portal 24 hours/day, 7 days/week. The Portal will provide:
   (1) security intelligence awareness and alerting; and
   (2) access to Education Materials in accordance with the terms provided in the Portal.

b. maintain availability of the Portal in accordance with the metrics provided in the section of this Services Description entitled “Service Level Agreements”, “Portal Availability”.

4.4.2 Your Portal Responsibilities

You agree to:

a. ensure your employees accessing the Portal on your behalf comply with the Terms of Use provided therein including, but not limited to, the terms associated with Educational Materials;

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

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

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

4.5 Services Contacts

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

Authorized Security Contacts

An Authorized Security Contact is defined as a decision-maker on all operational issues pertaining to IBM Managed Security Services. These contacts will have access to all objects within the Scanning Platform and optionally have the ability to create and execute scans.

Designated Services Contacts

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

Scanning Platform Executor

A Scanning Platform Executor has full access to a subset of objects in the Scanning Platform and the ability to create and executes scans within that subset.

Report Consumer Users

IBM provides multiple levels of access for Scanning Platform users. Scanning Platform users will be authenticated via static password or a public-key encryption technology you provide (for example, RSA SecureID token) based on your requirements. A Report Consumer User has access to areas of the Scanning Platform with the exception of modifying configuration or executing scans.

Portal Users

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

4.5.1 IBM Services Contacts Responsibilities

Authorized Security Contacts

IBM will:

a. allow you to create up to three Authorized Security Contacts;

b. provide each Authorized Security Contact with:
   (1) administrative Portal permissions to your Agents;
   (2) the authorization to create unlimited Designated Services Contacts and Portal Users; and
   (3) the authorization to delegate responsibility to Designated Services Contacts;

c. enable your Authorized Security Contacts access to the Scanning Platform, and optionally provide ability to create and execute scan;

d. interface with Authorized Security Contacts regarding support and notification issues pertaining to the Services; and

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

Scanning Platform Executor

IBM will:

a. verify the identity of Scanning Platform Executor using an authentication method that utilizes a pre-shared challenge pass phrase;

b. enable access to the Scanning Platform Executor as determined by the Authorized Security Contacts, including the ability to create/execute scans as needed; and

c. enable the Scanning Platform Executor the ability to create and execute scans to the extent of pages allowed as specified above and in the Schedule.

Report Consumer Users

IBM will:

a. provide appropriate access to your Report Consumer Users to the Scanning Platform as determined through discussions with the Authorized Security Contact; and

b. authenticate your Report Consumer Users as Scanning Platform users using static password.

Designated Services Contacts

IBM will:

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

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

Portal Users

IBM will:

a. provide your Portal Users with multiple levels of access to the Portal:

   (1) administrative user capabilities which will include:

      (a) ability to create Portal Users; and

      (b) ability to create and edit vulnerability watch lists;

b. authenticate Portal Users using static password; and

c. authenticate Portal Users using a public-key encryption technology you provide (for example, RSA SecureID token) based on your requirements.

4.5.2 Your Services Contacts Responsibilities

Authorized Security Contacts

You agree to:

a. provide IBM with contact information for each Authorized Security Contact. Such Authorized Security Contacts will be responsible for:

   (1) creating Designated Services Contacts and delegating responsibilities and permissions to such contacts, as appropriate;

   (2) creating Scanning Platform users;

   (3) authenticating with the SOCs using a pre-shared challenge pass phrase; and

   (4) maintaining notification paths and your contact information, and providing such information to IBM.

b. ensure at least one Authorized Security Contact is available during the business hours as described in the Service Delivery, consistent with the availability of the ASA or as specified in the Deployment Roadmap Outline;

c. update IBM within three calendar days when your Authorized Security Contact information changes; and

d. and acknowledge that you are permitted to have no more than three Authorized Security Contacts regardless of the number of IBM services or Agent subscriptions for which you have contracted.

Designated Services Contacts

You agree to:

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

b. and acknowledge that a Designated Services Contact may be required to be available 24 hours/day, 7 days/week based on the subset of responsibilities for which it is responsible (i.e., Agent outage).

Scanning Platform Executor

You acknowledge and agree:

a. that Scanning Platform users will use the Scanning Platform to perform daily operational Services activities;

b. that Scanning Platform users will be responsible for providing IBM-supported RSA SecureID tokens (as applicable);

c. that Scanning Platform users will not have direct contact with the SOCs and acknowledge the SOCs will only interface with Authorized Security Contacts and Designated Services Contacts; and

d. that, as it pertains to creating and executing your own scans, **YOU REPRESENT AND WARRANT THAT YOU SHALL NOT USE THE SOFTWARE TO SCAN ANY WEB SITES AND/OR APPLICATIONS OTHER THAN WEB SITES AND/OR APPLICATIONS OWNED BY YOU OR THOSE THAT YOU HAVE THE RIGHT AND AUTHORITY TO SCAN. YOU WILL INDEMNIFY IBM IN FULL FOR YOUR FAILURE TO COMPLY WITH THE TERMS OF THIS LICENSE OR APPLICABLE LAWS**.

Portal Users

You acknowledge and agree:

a. that Portal Users will use the Portal to perform daily operational Services activities;

b. that Portal Users will be responsible for providing IBM-supported RSA SecureID tokens (as applicable); and

c. that Portal Users will not have direct contact with the SOCs and acknowledge the SOCs will only interface with Authorized Security Contacts and Designated Services Contacts.

4.6 Security Intelligence

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

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

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

4.6.1 IBM Security Intelligence Responsibilities

IBM will:

a. provide you with access to the X-Force Hosted Threat Analysis Service;

b. provide you with a username, password, URL and appropriate permissions to access the Portal;

c. display security information on the Portal as it becomes available;

d. if configured by you, provide security intelligence specific to your defined vulnerability watch list, via the Portal;

e. if configured by you, provide an Internet security assessment e-mail each business day;

f. publish an Internet AlertCon via the Portal;

g. declare an Internet emergency if the daily AlertCon level reaches AlertCon 3. In such event, IBM will provide you with real time access into IBM's global situation briefing;

h. provide Portal feature functionality for you to create and maintain a vulnerability watch list;

i. provide additional information about an alert, advisory, or other significant security issue as IBM deems necessary; and

j. provide access to the Threat IQ via the Portal.

4.6.2 Your Security Intelligence Responsibilities

You agree to use the Portal to:

a. subscribe to the daily Internet security assessment e-mail, if desired;

b. create a vulnerability watch list, if desired;

c. access the Threat IQ; and

d. provide your agreement to adhere to the licensing agreement and not forward Services information to individuals who do not have a proper license.

4.7 Deployment and Activation

During deployment and activation, IBM will work with you to initialize the Service.

4.7.1 IBM Deployment and Activation Responsibilities

IBM will perform the following activities in order to activate your Service.

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 - Implementation for Scanning

Task 1 - Installation and Setup

IBM will:

a. install the Scanning Software on hosted infrastructure (the Scanning Platform) and confirm that it is operational; and

b. enable you to access the Scanning Platform by providing you with a unique, password protected, SSL encrypted URL for each user you designate, subject to the limitation of number of users as set out in your Service.

Completion Criteria:

This activity will be complete when IBM has provided you with one ID/password per the foregoing and you have confirmed that you have been able to access the Service.

Deliverable Materials:

- None

Task 2 - Conduct Solution Definition Interviews

IBM will:

a. conduct up to two interviews of 2 hour duration with key stakeholders in order to summarize and prioritize a mutually agreed upon direction for the implementation and deployment of the Scanning Software, as well as the agenda and specific activities to be performed during the Enablement Services. The key goals of these interviews are to determine:

   (1) Overall scoping of Solution Management Services activities, if applicable;

   (2) Organizational groups, administrative hierarchy, user roles and permissions;

   (3) Report definition;

   (4) Dashboard view definition;

   (5) Scheduling and notification configuration; and

   (6) Technical understanding of applications and sites to guide the scan configuration.

Completion Criteria:

This activity will be complete when IBM has completed the interviews.

Deliverable Materials:

- None

Task 3 - Provide Deployment Roadmap Outline

IBM will:

a. provide a Deployment Roadmap Outline to describe the deployment of the Scanning Software within your organization. The Deployment Roadmap Outline summarizes and prioritizes the following:

   (1) An overview of the deployment objectives and a sequence of activities for how they will be achieved;

   (2) An outline of processes that will be implemented or changed by the deployment;

   (3) An established scanning schedule that details the number of application assessments to occur throughout various periods that constitute the full contract period as specified in the Schedule for this Service. The scanning schedule will be developed based on the scope of services and must be approved by the Application Security Analyst;

   (4) Summary descriptions of user roles and responsibilities;

   (5) Define and document the definition of a critical issue for purposes of fulfilling the Critical Priority Issue Alert Notification;

   (6) Configuration or reporting definition captured during the interview phase; and

   (7) An organizational map that depicts accountability for compliance, as well as, content ownership.

b. upon receipt of a request from Services Recipient to revise the Deployment Roadmap Outline, which must occur within five days of initial delivery of Deployment Roadmap Outline, provide the Services Recipient with a revised Deployment Roadmap Outline within two business days after notification by the Services Recipient.

Note: The revised Deployment Roadmap Outline will be considered the final document, and no further revisions will be made to it by IBM.

Completion Criteria:

This activity will be complete when IBM has delivered the Deployment Roadmap Outline and you have accepted the contents thereof. IBM will accept one iteration of comments/revisions to the document before it will be deemed accepted.

Deliverable Materials:

- Deployment Roadmap Outline

  Purpose: This document, as mutually agreed upon during the solution definition interviews, summarizes and prioritizes the implementation and deployment direction for the Enablement Services and a sequence of activities for the solution implementation and deployment.

  Content: This document of up to five pages summarizes and prioritizes the software implementation definition and deployment activities.

Task 4 - Initial Configuration Creation

IBM will:

a. create the initial configuration of the Scanning Software which includes the following:

(1) the initial folder hierarchy;

(2) a trial scan (Content Scan Job) and report (Content Scan Job Reports) of one of your websites. Note: this task may be omitted if a full scan of an application is requested by you; and

(3) the configuration and Content Scan Job Reports.

Completion Criteria:

IBM will have met its responsibilities for this activity when IBM has completed the tasks as listed.

Deliverable Materials:

- None

Activity 3 - IBM Enablement Service Responsibilities

IBM will:

c. conduct two enablement sessions of 1 hour duration for up to 3 of your designated users. During the enablement sessions, provide your designated users with:

(1) Scanning Platform training; and

(2) assistance regarding activities to view and interpret reports.

Completion Criteria:

This activity will be complete when IBM has conducted the enablement sessions. IBM will not be required to reschedule the Enablement Services if designated users do not participate at the pre-determined date and time.

Deliverable Materials:

- None

4.7.2 Your Deployment and Activation Responsibilities

In order to provide for successful deployment and activation of your service, participation in the following will be necessary.

Activity 1 - Project Kickoff

You agree to:

a. attend the project kickoff call; and

b. review each party's respective responsibilities.

Activity 2 - Implementation for Scanning Requirements

Task 1 - Installation and Setup

You agree to:

a. verify your access to access the Scanning Platform; and

b. safeguard the password protected, SSL encrypted URL for each of your designated users.

Task 2 - Conduct Solution Definition Interviews

You agree to:

a. assign key stakeholders that will be required to participate in the Solution Definition Interviews; and

b. ensure the key stakeholders are available to participate in the Solution Definition Interviews.

Task 3 - Provide Deployment Roadmap Outline

You acknowledge and agree:

a. upon receipt, to review and notify IBM within five business days of any requested revisions to the Deployment Roadmap Outline;

b. that no further revisions will be made to the Deployment Roadmap Outline; and

c. that this Service provides the Services Recipient with the ability to perform up to the number of scans as specified in the Schedule and scans will be performed based on the established scanning schedule described in the Deployment Roadmap Outline. All unused scans for the given duration as per the established scanning schedule will be forfeited.

Task 4 - Initial Configuration Creation

You agree to:

a. review the configuration; and

b. review the trial scan report, if required.

Activity 3 - Your Enablement Service Responsibilities

You agree to:

a. provide the appropriate users that will participate in the enablement session; and

b. provide a scheduled date and time at which the authorized users will attend the enablement session.

4.8 Application Assessment

Application assessment services will be provided as part of the Service. These services include specific activities that encompass the initial configuration and scanning of an application, the rescanning of the application and the collaboration through business process activities.

4.8.1 IBM Application Initial Configuration and Scan Responsibilities

IBM will provide you with application assessment services based on the following activities specified.

Activity 1 - Application Initial Configuration and Scan

Initial configuration and scan services are performed to enable the configuration of the Scanning Software. These services must be completed in order to scan your websites and produce reports providing information about your websites and/or describing specific issues uncovered on your websites.

IBM will:

a. provide initial configuration and scan services which include:

   (1) creation and execution of initial scan;

   (2) validation of results for application coverage;

   (3) performing spot verification of security results;

   (4) configuration and execution of dashboards;

   (5) configuration and maintenance of folder hierarchy;

   (6) issuing alerts for high issues (where required and as mutually agreed); and

   (7) delivery of scan results in a document called Content Scan Job Report will be made available to the appropriate authorized contact via email and the reporting dashboards available in the scanning platform portal or through other methods as requested by the Services Recipient.

Notes: There are certain limitations when scanning production applications. These are noted here:

1. Content requiring authentication is not scanned. Scans will not be configured to execute login sequences in the web application (although the login page itself will be scanned).
2. Production websites and applications will be scanned using the automated web crawling capabilities of the Scanning Software. The manual explore capability (i.e., manually recording keystrokes and pages visit to “teach” the scanner how to navigate the site) will not be used. Thus, sequenced-based functionality may not be properly scanned (i.e., pages in correct order).
3. Automated form filling will be used for any forms encountered.

Completion Criteria:

IBM will have met its responsibilities for this activity when IBM has completed delivery to you of the Materials and completed the activities listed. Delivery will be made to the appropriate authorized contact via email and the reporting dashboards available in the scanning platform portal or through other methods as requested by the Services Recipient.

Deliverable Materials:

- Content Scan Job Report

4.8.2 Your Application Initial Configuration and Scan Responsibilities

The process of scanning web applications for security vulnerabilities requires cooperation between those creating and executing the scans and the application owner. The operations model for application scanning will be determined through discussions with your Authorized Security Contacts.

The Authorized Security Contact or other individuals as mandated by the Authorized Security Contact will typically be asked to provide the following information in order to enable application scanning:

You agree to:

a. provide name and URL/IP address of application;

b. provide date and time window in which to conduct the scan; and

c. participate in discussions regarding your desired Security Test Policy and provide final approval.

4.8.3 IBM Application Rescan Security Assessment Responsibilities

After the application has been initially assessed for security issues it is recommended that periodic rescanning takes place to ensure the continued security of the application through its final release to a production environment. The following rescan activities provide for the continued monitoring of the security posture of the application.

Activity 1 - Application Rescan Security Assessments

Application rescan security assessment activities consist of scans of the production application that take place after the initial scan and are intended to ensure continued application security after the initial assessment.

IBM will provide rescan security assessments which include the following actions:

a. Based on initial scan, verify changes to include in rescan;

b. Execute rescan;

c. Configure and execute dashboards;

d. Issue alerts for high priority issues (where required and as mutually agreed);

e. Provide extract of security issues to enable integration by client into existing problem tracking system; and

f. Delivery of scan results will be made to the appropriate authorized contact via email and the reporting dashboards available in the scanning platform portal or through other methods as requested by the Services Recipient.

Completion Criteria:

This activity will be complete when IBM has delivered to the Content Scan Job Report.

Deliverable Materials:

- Content Scan Job Report

4.8.4 Your Application Rescan Security Assessment Responsibilities

You agree to:

a. provide date and time window in which to conduct the scan;

b. participate in discussions regarding your desired Security Test Policy and provide final approval; and

c. provide application credentials (where applicable).

4.8.5 IBM Business Process Responsibilities

Activity 1 - Business Process Services

The purpose of this activity is to provide the on-going services to integrate the results of our application assessment services into your business processes. These services are provided during the course of initial and rescan activities during communications with you.

IBM will provide business process services which include:

a. working with your extended team members to advise solutions to issues discovered;

b. the development of processes to enable the integration (e.g., importation) of security issues into existing problem tracking system; and

c. integration of security scanning into software development life cycle.

Completion Criteria:

This is an on-going activity.

Deliverable Materials:

- None

4.8.6 Your Business Process Responsibilities

You agree to:

a. participate in discussion of issues discovered;

b. provide necessary information for integrating issues into existing ticketing system; and

c. provide information to the extended team members and stakeholders within your organization.

4.9 Security Test Policy Management

The application assessment service enables the creation of test policies which determine what the Scanning Software is testing for or analyzing on the web pages being scanned. IBM defines standard test policies which represent the initial scan configuration. These test policies can be modified during the execution of the services through discussions with you.

4.9.1 IBM Security Test Policy Management Responsibilities

IBM will:

a. modify the Security Test Policy as mutually agreed; and

b. test and verify the results of such changes.

4.9.2 Your Security Test Policy Management Responsibilities

You agree to:

a. participate in discussions regarding modifications to test policies; and

b. approve changes to test policies.

4.10 Security Reporting

The Scanning Platform provides you with a comprehensive reporting capability to be able to view the results of scans both at the detailed and summary level.

4.10.1 IBM Security Reporting Responsibilities

IBM will provide you with access to reporting capabilities in the Scanning Platform which include:

a. Summary level reports. IBM can configure dashboard reports which summarize the results of scans and provide trend analysis; and

b. Detail reports. The Scanning Software provides detailed results of application security scans which includes:

   (1) Pages (URLs) containing;

   (2) Title and description of the issue;

   (3) HTTP request used to create the issue; and

   (4) Remediation suggestions.

4.10.2 Your Security Reporting Responsibilities

You agree to:

a. participate in discussions to design the dashboard reports and approve the final design;

b. disseminate information from the reports as necessary or direct IBM to disclose to authorized parties;

c. participate in meetings to review results of the scans and accept (as necessary); and

d. assist with prioritising issues and liaise with remediation teams as necessary.

5. Optional Services

Optional services selected by you will be specified in the Schedule.

5.1 One-time Additional Rescan

This optional service provides for a one time rescan in addition to rescans that may be included in the IBM Hosted Application Security Services – Production Application Scanning Service. The One-time Additional Rescan is based on the size of the application (see Application Size description above) being scanned in the same way as the IBM Hosted Application Security Services – Production Application Scanning Service.

5.1.1 IBM One-time Additional Scan Responsibilities

One-time Additional Scan will include initial configuration and scan services are performed to enable the configuration of the Scanning Software. These services must be completed in order to scan your

websites and produce reports providing information about your websites and/or describing specific issues uncovered on your websites.

IBM will:

a. provide initial configuration and scan services which include:
   (1) creation and the execution of initial scan;
   (2) validation of results for application coverage;
   (3) performing spot verification of security results;
   (4) configuration and execution of dashboards;
   (5) configuration and maintenance of folder hierarchy;
   (6) issuing alerts for high issues (where required and as mutually agreed); and
   (7) delivery of scan results in a document called Content Scan Job Report will be made available to the appropriate authorized contact via email and the reporting dashboards available in the scanning platform portal or through other methods as requested by the Services Recipient.

Notes: There are certain limitations when scanning production applications. These are noted here:

1. Content requiring authentication is not scanned. Scans will not be configured to execute login sequences in the web application (although the login page itself will be scanned).
2. Production websites and applications will be scanned using the automated web crawling capabilities of the Scanning Software. The manual explore capability (i.e., manually recording keystrokes and pages visit to "teach" the scanner how to navigate the site) will not be used. Thus, sequenced-based functionality may not be properly scanned (i.e., pages in correct order).
3. Automated form filling will be used for any forms encountered.

Completion Criteria:

IBM will have met its responsibilities for this activity when IBM has completed delivery to you of the Materials, and completed the tasks as listed. Delivery will be made to the appropriate authorized contact via email and the reporting dashboards available in the scanning platform portal or through other methods as requested by the Services Recipient.

Deliverable Materials:

- Content Scan Job Report

5.1.2 Your One time additional scan responsibilities

The process of scanning web applications for security vulnerabilities requires cooperation between those creating and executing the scans and the application owners. The operations model for application scanning will be determined through discussions with your Authorized Security Contacts. The Authorized Security Contact or other individuals as mandated by the Authorized Security Contact will typically be asked to provide the following information in order to enable application scanning:

You agree to:

a. provide name and URL/IP address of application;

b. provide date and time window in which to conduct the scan; and

c. participate in discussions regarding your desired Security Test Policy and provide final approval.

6. Service Level Agreements

IBM SLAs establish response time objectives for specific events resulting from the Services. The SLAs become effective when the deployment process has been completed. The SLA remedies are available provided you meet your obligations as defined in this Services Description and all associated contract documents.

6.1 SLA Availability

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

a. Portal Availability – IBM will provide 99.9% accessibility for the Portal outside of the times specified in the section of this Services Description entitled "Scheduled and Emergency Portal Maintenance".

b. Scanning Platform Availability - IBM will provide 99.9% accessibility for the Scanning Platform outside of the times specified in the section of this Services Description entitled "Scheduled and Emergency Scanning Platform Maintenance".

c. Scan Initiation Response – Scan requests are limited to one new scan request per week for every 10 applications the client is scanning. Based on application size, IBM will respond to a new scan request within the timeframes listed below. The SLA starts once IBM has received all required information from the customer. The SLA is met when (1) the requested scan is initiated or (2) IBM has requested information or validation from the customer (e.g., scan coverage). Services Recipient and IBM can mutually agree to a different scanning schedule that does not increase the foregoing SLA.

   (1) Level 1 – Small Application – Scans will be initiated within 1 business day.

   (2) Level 2 – Large Application – Scans will be initiated within 2 business days.

d. Critical Priority Issue Alert Notification – IBM will notify you of any critical issues within 1 hour of IBM confirming the issue. The ASA will notify the listed authorized contact via the preferred method as designated by the Services Recipient. This SLA starts after the ASA has confirmed the legitimacy of the critical issue. The definition of a critical issue is determined through discussions and mutually agreed to in the Deployment Roadmap Outline.

e. Scan Review Initiation - IBM will begin reviewing a security scan within 1 business day of scan completion.

f. False Positive – For all security issues reviewed by an Application Security Analyst, IBM will provide a false positive rate of 0%. This SLA covers only those issues that the ASA has reviewed and confirmed. Reviewing of the issues may require collaboration with the Services Recipient before making a final decision regarding the legitimacy of the issue.

g. Request To Re-scan - Execute Rescan - IBM will execute the designated re-scan according to the desired time frame of the requested rescan as specified in the request. The time to execute the desired rescan can be effected by the complexity of the application.

   (1) Level 1 – Small Application – IBM will initiate a re-scan request within 1 business day.

   (2) Level 2 – Large Application – IBM will initiate a re-scan request within 2 business days.

h. Response To Inquiry - IBM will respond to your email/v-mail within 4 business hours of its receipt.

6.2 SLA Remedies

The following remedies are available if IBM fails to meet the SLA as designated in this service description.

a. Request To Re-scan - Execute Rescan and Scan Initiation Response Remedy– If IBM fails to meet these SLAs in a given calendar month, a credit will be issued for one week of the monthly service for the application that was being requested to be scanned.

b. False Positive, Response To Inquiry, Scan Review Initiation and Critical Priority Issue Alert Notification SLAs - If IBM fails to meet these SLAs in a given calendar month, a credit will be issued for one week of the monthly service for the application scan associated with the SLA not met.

c. Scanning Platform Availability and Portal Availability SLA - If IBM fails to meet any of these SLAs, a credit will be issued for one week of the monthly service for the affected application being scanned and, if applicable, the specific platform for which the respective SLA was not met.

6.2.2 SLAs and Remedies Summary

Scan Initiation Response	A credit will be issued for one week of the monthly service for the application that was being requested to be scanned
Request To Re-scan - Execute Rescan	
False Positive	A credit will be issued for one week of the monthly service for the application scan associated with the SLA not met.
Scan Review Initiation	
Response To Inquiry	
Critical Priority Issue Alert Notification	

Scanning Platform Availability	A credit will be issued for one week of the monthly service for the affected application being scanned and, if applicable, the specific platform for which the respective SLA was not met.
Portal Availability	

7. Other Terms and Conditions

7.1 General

You acknowledge and agree:

a. that all software provided by IBM as part of these Services is licensed, not sold. Except for the licenses specifically granted herein, all right, title, and interest in and to the software shall remain vested in IBM or its licensors;

b. that you will inform IBM in writing, at least 30 days prior to the cancellation or termination of the Services, or promptly if the license for the software is terminated by IBM for any reason, whether you choose to:

   (1) have IBM remove the IBM provided software either remotely or by assisting you to remove the IBM provided software; or

   (2) retain the IBM provided software.

   If you choose to have the software removed, you agree to cooperate with IBM by providing the remote access necessary for IBM to remove the software, or by assisting IBM in removing the software.

c. in addition to the terms and conditions listed above, specific licensing terms will be presented for your review and acceptance both when you download and when you install the software.

7.2 Permission to Perform Testing

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 Service 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.

7.3 Systems Owned by a Third Party

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 authorising 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:

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

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

c. to indemnify IBM in full for any losses or liability IBM incurs due to third party claims arising out of 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.

7.4 Disclaimer

You understand and agree that:

a. 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;

b. IBM does not provide legal services or represent or warrant that the services or products IBM provides or obtains on your behalf will ensure your compliance with any particular law, including but not limited to any law relating to safety, security or privacy; and

c. it is your responsibility to engage competent legal counsel to advise you as to the identification and interpretation of any relevant laws that may affect your business and any actions needed for compliance with such laws.