

## Service Description

---

### IBM Vulnerability Management Service

#### 1. Service Overview

IBM Vulnerability Management Service (called "VMS" or "Service") is designed to provide a comprehensive, Web-driven vulnerability management program that provides visibility into potential exposure areas within a distributed network environment.

The details of Customer's order (for example, the services requested, contract period, and charges) will be specified in an Order.

Definitions of Service-specific terminology can be found at [www.ibm.com/services/iss/wwcontracts](http://www.ibm.com/services/iss/wwcontracts)

VMS is designed to help provide Customers with the tools required to implement an effective vulnerability management program. The Service may be delivered as either an external or an internal solution. If delivered as an external solution, scanning will be provided which originates from scanning agents hosted at the Security Operations Center ("SOC") via the Internet. If delivered as an internal solution, a scanning agent (called "Agent") will be deployed into Customer's internal network to provide vulnerability management of internal Hosts which may not be directly accessible by Hosts outside of Customer's network.

The following features and capabilities are provided as part of the Service.

- a. Web-driven interface for scan scheduling, and reporting;
- b. internal and external scanning;
- c. accurate and detailed vulnerability results;
- d. on-line access to vulnerability data;
- e. ability to track individual assets, device criticality, and assignment of owners;
- f. comprehensive tool-set for workflow management and remediation tracking;
- g. productivity tracking of those responsible for vulnerability remediation; and
- h. access to research needed to quickly identify effective remediation steps.

The IBM approach to vulnerability management includes six key components.

- a. vulnerability discovery - provides a Web-driven interface that allows Customer to schedule and launch either internal or external scans of assets within its individual environments;
- b. asset clarification - catalogs each scanned device (i.e., asset) and allows Customers to assign business criticality ratings and match system owners to specific assets. Asset owners are notified using the Virtual Security Operations Center (called "Virtual-SOC") when vulnerabilities are discovered, and are provided with a personalized view into overall program impacts on their security posture;
- c. remediation – helps Customer identify vulnerabilities and assigns them to designated asset owners for review and remediation. Individual asset owners can use the Virtual-SOC to learn about a specific vulnerability and track its remediation within the enterprise. The Service provides a detailed workflow;
- d. dynamic protection – integrates VMS with Customer's existing IBM Managed Security Services (as applicable) to update server and network Intrusion Prevention policies with appropriate blocking responses. This capability enhances vulnerability management to provide vulnerability protection;
- e. verification – permit the vulnerability to remain active until VMS verifies the patch has been effectively implemented and all attack vectors for the vulnerability have been successfully eliminated; and
- f. detailed reporting - provides a results-oriented view of Service performance and security posture.

The following table provides an overview of VMS service features.

## **Service Features**

<b>Service Features</b>	<b>External Scanning</b>	<b>Internal Scanning</b>
Ideal for:	Identifying vulnerabilities within the network perimeter	Identifying vulnerabilities across the enterprise
Organization size	Any	Any
Number of available scans	Based on number of Internet protocols ("IPs") and frequency purchased	Unlimited scans of a specified number of IPs – within the constraints of the platform
Hardware platform required	No	Yes
Available policies	15	15
Scans external IPs	Yes	Yes, depending on network configuration
Scans internal IPs	No	Yes
Ranking of discovered assets		Yes
Assignment of administrators to discovered assets		Yes
Assign vulnerabilities for remediation		Yes
Dynamic IBM Virtual Patch® technology	Yes, requires purchase of a compatible managed service	
Full vulnerability remediation workflow		Yes
Industry and vertical comparisons		Yes
Verification of resolved vulnerabilities		Yes
Integration with IBM Managed Security Services and IBM Managed Protection Services		Yes

## **2. IBM Responsibilities**

### **2.1 Deployment and Initiation**

During deployment and initiation of internal VMS, IBM will work with Customer to either deploy a new internal scanning Agent or begin management of an existing Agent.

For external VMS, IBM will work with Customer to enable scanning of Customer's externally facing Hosts.

#### **2.1.1 Project Kickoff**

IBM will send Customer a welcome e-mail and conduct a kickoff call to:

- introduce Customer contacts to the assigned IBM deployment specialist;
- review IBM and Customer responsibilities; and
- begin to assess Customer requirements and environment, if an internal scanning Agent will be deployed.

To enable deployment of internal VMS, IBM will provide a document called "Network Access Requirements", detailing how IBM will connect remotely to Customer's network, and any specific technical requirements to enable such access. Typically, IBM will connect via standard access methods through the Internet; however, a site-to-site VPN may be used, if appropriate.

External VMS requires only a short deployment session between Customer and the IBM deployment specialist.

## **2.1.2 Assessment**

### **Data Gathering**

IBM will work with Customer to help configure Customer's profile within the Virtual-SOC. This configuration may include setup of accounts and valid IP addresses that may be scanned.

### **Environment Assessment**

This section applies only to Customers who have purchased the internal scanning option of VMS.

Using the provided information, IBM will work with Customer to understand the existing Customer environment, and build a configuration for the Agent. During this assessment, IBM may make recommendations to adjust the layout of the network to improve scanning capability or otherwise enhance security.

### **Existing Agent Assessment**

This section applies only to Customers who have purchased the internal scanning option of VMS.

If IBM will be taking over management of an existing Agent, IBM must assess the Agent to be sure it meets certain specifications. IBM may require the Agent software or Security Content to be reinstalled, or upgraded to the most current versions in order to provide the Service. Other required criteria may include the addition or removal of applications and user accounts.

## **2.1.3 Implementation**

This section applies only to Customers who have purchased the internal scanning option of VMS.

### **Configuration at IBM**

For Agents purchased through IBM at the time of deployment, much of the configuration and policy setting will take place at IBM facilities. For existing Agents already in use, Customer will have the option to ship the Agent to IBM for configuration at IBM facilities.

### **Installation**

While physical installation and cabling are a Customer responsibility, IBM will provide live support, via phone and e-mail, and will assist Customer with location of vendor documents detailing the installation procedure for the Agent. Such support must be scheduled in advance to ensure availability of an IBM deployment specialist.

At Customer's request and for an additional fee, IBM will provide physical installation services.

### **Remote Configuration**

When taking over management of an existing Agent, IBM will typically perform the configuration remotely. Customer may be required to physically load media.

All managed Agents will require some remote configuration, which may include registration of the Agent with IBM Managed Security Services infrastructure.

## **2.1.4 Transition to SOC**

Once the Agent is configured, physically installed and implemented, and connected to the IBM Managed Security Services infrastructure, IBM will provide Customer with the option of having a demonstration of the Virtual-SOC capabilities and performance of common tasks.

The final step of Service deployment is when the SOC takes over management and support of the Agent and the relationship with Customer. At this time, the ongoing management and support phase of the Service officially begins. Typically, IBM will introduce the Customer via phone to the SOC personnel.

## **2.2 Ongoing Management and Support**

### **2.2.1 Vulnerability Management**

VMS is an electronic service that automatically scans Customer devices for known vulnerabilities. Each scan results in comprehensive reports that are designed to identify potential weaknesses, assess relative network risk, and provide recommendations to manage identified vulnerabilities.

External VMS consists of remotely delivered scans which originate from IBM facilities. IBM will require Customer to validate it is the owner of the IP address range to be scanned, prior to the initial scan of such IP address range being performed. IBM can only scan publicly routable IP addresses belonging to Customer.

Internal VMS provides all the benefits of vulnerability management but is delivered by an Agent that is deployed inside Customer's internal network. IBM will provide a licensed copy of IBM Internet Scanner® software for the duration of the internal VMS contract.

### **2.2.2 Virtual-SOC**

The Virtual-SOC is a Web-based interface designed to deliver key Service features and on-demand protection solutions. The Virtual-SOC is structured to deliver a consolidated view of Customer's overall security posture. The portal is capable of merging data from multiple geographies or technologies into a common interface, allowing for comprehensive analysis, alerting, remediation, and reporting.

The Virtual-SOC provides real-time access for communications including ticket creation, security event handling, incident response, data presentation, report generation, and trend analysis.

#### **Reporting**

VMS is designed to provide reports that focus on the status of vulnerabilities within Customer's enterprise, protection measures employed, security activities, subordinate activities and Service summaries. Many of the available reports can be generated using customizable data sets and user-defined reporting periods with varying views.

#### **Users of the System**

The Service is designed to help organizations manage vulnerability exposures across the enterprise by providing multiple individuals, from different levels within the organization, with varying levels of access to the system.

##### **a. Authorized Security Contacts**

Users classified as Customer security contacts will be the primary users of VMS and will have full access to the system including the ability to implement scans, generate reports, assign vulnerabilities for remediation, and apply virtual patches. IBM SOC analysts will only accept phone calls from authorized Customer security contacts. Customers may identify up to three authorized security contacts for VMS.

##### **b. Subordinates/System Administrators**

Users classified at this level will receive limited access to the VMS system. Subordinates/system administrators are identified by authorized Customer security contacts, and are then assigned specific devices for which they may have access. Vulnerabilities can then be assigned to these individuals for remediation once identified during the discovery process. Subsequently, subordinates/system administrators may login to the system, review and research assigned vulnerabilities, and document any remediation efforts. Users at this level do not have the authority to review data or make changes outside of devices assigned directly to them. Customers may identify an unlimited number of subordinates/system administrators for the VMS service (within the constraints of the platform).

#### **Dashboard**

In addition to vulnerabilities, VMS provides an overview "at a glance" (called "Dashboard") to deliver a snapshot of Customer's state of security as it relates to vulnerabilities. The Dashboard provides administrators with a comprehensive overview of the vulnerabilities within the Customer network, broken down by severity and ticket assignment, current scan results, top vulnerable Hosts (i.e., assets) and remediation status of the subordinate users.

Authorized Customer security contacts will have access to the entire Dashboard and all Service features and functionality. Subordinate users will receive a more focused view that outlines vulnerabilities or assets to which they have been assigned.

### **2.2.3 Scanning**

VMS identifies network assets (for example, servers and network devices), cataloging each item, and building an association between assets and their respective vulnerabilities. VMS provides a Web-driven

interface that controls scan initiation, identification of assets to be scanned, and types of scans to be conducted. After a scan is completed, electronic notifications will be delivered to the authorized Customer security contacts informing them that results are pending review.

VMS provides Customer with two distinct types of scanning which can be employed together or separately:

### **External Scanning**

External scanning provides the Customer with a potential hacker's view of the network perimeter and is designed to highlight those risk exposures open to the general Internet community. External scans will identify and assess only devices with routable IP addresses. Non-routable IP addresses behind closed firewalls will not be scanned. Scans are scheduled by the Customer through the Virtual-SOC and launched from the IBM secure data center environment. External scans do not require CPE, setup, or hardware/software investment. External scanning is delivered based on the number of IPs and the frequency of scanning.

External scanning is purchased based on the number of IPs to be scanned over a given period of time. Customer may purchase any number of IPs to be scanned on a weekly, monthly or quarterly basis. Each scan will subtract from the available pool of IPs regardless of whether the same or unique systems are being assessed during each scan. Available IPs will automatically refresh, based on the purchased frequency. At the close of the allotted time period, unused IPs will be forfeited.

### **Internal Scanning**

Internal scanning is designed to allow the Customer to assess the state of vulnerabilities within their enterprise. This type of assessment is important as a large percentage of network-based attacks (for example, mass-propagating worms) often originate unknowingly from inside a protected or private network. Internal scans are launched from a scanning Agent located at Customer's premises and require Customer to provide the appropriate hardware and operating system. An unlimited number of scans may be launched from the internal scanning Agent, based on the number of IPs purchased. Internal scanning Agents can process up to 10,000 unique IPs per device.

When both scanning types are used together, they help Customer delineate which vulnerabilities are identifiable only from the outside, only from the inside, or from both locations. This information can help Customer prioritize the vulnerabilities to be addressed.

## **2.2.4 Scan Policies**

To provide flexibility for each scheduled scan, a total of 15 different policies are available for both internal and external scanning. These 15 policies allow Customer to assess vulnerabilities and exposures that exist across a variety of device types with varying degrees of intrusiveness. An example of such a policy is one tailored specifically for conducting assessment scans, to identify vulnerabilities on assets such as servers, desktops, routers, and switches.

## **2.2.5 Scheduling of Scans**

Customers can schedule scans 24 hours/day by 7 days/week through the Virtual-SOC. Customer may schedule a scan by providing the following parameters:

- scan name – a brief alias for the scan;
- description – purpose of the scan;
- scan type – external or internal;
- scan time and recurrence – scans can be scheduled on one-time or recurring basis;
- scan retry interval – number of hours before a failed scan starts again;
- policy – any of the outlined policies can be selected; and
- scan target – a predefined target range of IPs or a user-specific range.

## **2.2.6 Scan Results**

Scan results are available immediately following the successful completion of a scheduled scan. Results of each separate scan can be viewed independently through the "Scan History" option of the Dashboard.

This distributed manner of archiving and storing scan data allows authorized Customer security contacts to quickly review the results of a single scan, while also reviewing the overall state of assets and their

respective vulnerabilities across the enterprise. Scan results typically include some or all of the following information:

- discovered assets (IPs);
- available services;
- operating systems identified; and
- vulnerabilities with associated severity.

## **2.3 Prioritization and Vulnerability Assignment**

One of the challenges of vulnerability management is properly prioritizing which vulnerabilities should be remediated first, and tracking and recording the prioritization. VMS displays vulnerable systems with the severity of identified vulnerabilities and the business criticality of the impacted assets. The available information makes prioritizing vulnerabilities more manageable. Vulnerabilities can be assigned electronically to the appropriate subordinate/system administrator for remediation.

### **2.3.1 Asset Criticality**

VMS provides authorized Customer security contacts with the ability to assign a numeric business criticality ranking to each discovered asset. Rankings can be assigned to single or multiple assets at one time. Assigning a criticality ranking to each discovered asset allows prioritization for which vulnerabilities should be remediated first. Business criticality ratings will be stored in the VMS system and can be modified by authorized Customer security contacts at any time.

### **2.3.2 Assigning Vulnerabilities for Remediation**

VMS allows Customer to track and distribute workload by assigning vulnerabilities directly to those responsible for fixing them. Authorized Customer security contacts can define subordinate/system administrators in the system. Defining these individuals will automatically create the appropriate logins and electronically notify the user they have been added to the system. This provides subordinate/system administrators the ability to log directly into the system to receive assigned workload (vulnerabilities). If user maintenance is required, an authorized Customer security contact will have the authority to modify login credentials, and add or delete accounts.

After the appropriate users have been entered into the system, they can be assigned directly to discovered assets for which they hold remediation responsibility. As vulnerabilities are discovered, having system administrators associated with specific assets will help to speed the vulnerability assignment process.

### **2.3.3 Tracking Assigned Vulnerabilities**

Using the Dashboard, authorized Customer security contacts can review a summary of system administrators and their assigned vulnerabilities. A variety of reporting options is available to allow authorized Customer security contacts to generate reports on subordinate/system administrator activity. These reports can help identify which individuals have been most productive and where additional effort may be required.

## **2.4 Dynamic Virtual Patching**

By combining VMS with the IBM Proventia® Network Intrusion Prevention System ("IPS") under the umbrella of Managed Security Services, VMS can provide Customer with dynamic virtual patching capabilities. Authorized Customer security contacts can configure their Service implementation to automatically or selectively request the SOC deploy virtual patches to other managed devices. Virtual patching helps protect vulnerable systems from attack while system administrators are applying vendor-supplied patches.

Virtual patching capabilities are supported on Proventia IPS Appliances and RealSecure® Server software. For virtual patching to occur, the Intrusion Prevention devices must be under full management by IBM Managed Security Services which are available for an additional fee. Virtual patching of unmanaged or third party Intrusion Prevention technology is not supported.

## **2.5 Vulnerability Remediation**

When subordinate/system administrators have been electronically notified of vulnerability assignments, these individuals will be prompted to log directly into the Virtual-SOC to review their assigned workload. Following review, users may begin researching and documenting efforts as they work towards a

resolution. As progress is made, authorized Customer security contacts can follow along using the real-time review capabilities provided through the Virtual-SOC.

### **2.5.1 Reviewing/Researching Vulnerabilities**

As subordinate/system administrators login to the Virtual-SOC, they will be provided with a detailed list of vulnerabilities pending review. The vulnerabilities can be reviewed in detail, including asset properties, vulnerability severity, description, impacts and recommended remediation steps.

VMS provides the user with reference information to understand specific vulnerabilities and appropriate remediation steps. Extensive reading and outside research is not required to formulate a plan for resolving a specific issue.

### **2.5.2 Remediation Workflow**

VMS provides Customer with a workflow designed to guide Customer through the remediation process. Using this tool, a subordinate/system administrator will be provided with the next step to resolve a specific vulnerability.

The workflow is primarily driven by the status of the vulnerability. For example, the following status may be used during the remediation process:

- open – initial status, set automatically following discovery of a vulnerability;
- ignored – indicates a given vulnerability should be ignored for the time being. This status is set manually and is not recommended;
- notified – indicates a vulnerability has been assigned for remediation. This status is set automatically;
- reviewed – indicates the system administrator has reviewed the vulnerability. This status is set automatically;
- in progress – indicates the vulnerability has been reviewed and the remediation is in progress. This item is set manually;
- resolved pending confirmation – indicates the vulnerability is believed to be resolved and a follow-up scan is necessary to confirm. This status is set manually.

The above status indicators are provided for example purposes only. Actual status indicators in the Service may be modified based on Customer's feedback or technical necessity.

Vulnerability remediation typically requires disabling vulnerable services or applying software patches. Because it may be difficult to determine if a patch was applied successfully, or if a given vulnerability was resolved, VMS does not allow users to set a vulnerability status to "resolved". Rather, VMS allows users to set status to "resolved pending confirmation". Vulnerabilities will remain in this status until a follow-up scan is launched and the vulnerability is confirmed to no longer exist.

### **2.5.3 Managed Security and Protection Services Integration**

VMS provides additional capability when used in conjunction with other IBM Managed Security Services. This combination helps blend the gathered data to provide a comprehensive view of vulnerabilities as they relate to Security Incidents and escalations under the IBM Managed Security Services and IBM Managed Protection Services.

### **2.5.4 Management of Scanning Agents**

If Agent licenses are provided as part internal scanning of the VMS implementation, IBM will provide full management of the Agents. Management of the Agents will be facilitated through the use of Windows Terminal Services with encryption enabled. Under this configuration, IBM will retain sole administrator level access to the device. Any and all changes to the scanning application or underlying operating system will be the sole responsibility of IBM security operations analysts.

The Customer may perform management of internal scanning Agents provided Customer owns or purchases an applicable license for the Agent. Customer must receive approval from IBM prior to making any changes to the Agent or the operating system. If approval is not received, IBM will not be held responsible for service failures related to improper scanning Agent functionality.

### **Health and Availability Monitoring**

The health and performance of VMS is monitored by using a Host-based monitoring Agent (when possible) or Simple Network Management Protocol ("SNMP"). The Agent keeps IBM security analysts informed of some potential problems as they develop. Key metrics analyzed by the monitoring Agent include:

- hard disk capacity;
- CPU utilization;
- memory utilization; and
- process availability.

In addition to system health metrics, IBM will monitor device availability. If contact with a managed device is lost, additional time-based checks will be initiated to verify a valid outage has been identified.

In the event system health problems or an outage has been confirmed, a trouble ticket will be created and an IBM security analyst will be notified to begin research and investigation. The status of all system health tickets is available through the Virtual-SOC.

### **Outage Notification**

If the Agent is not reachable through standard in-band means, Customer will be notified via telephone using a predetermined escalation procedure. Following telephone escalation, IBM will begin investigating problems related to the configuration or functionality of the managed device.

### **Application Updates**

Periodically, it will be necessary for IBM to install patches and software updates to improve device performance, enable additional functionality, and resolve potential application problems. The application of such patches and updates may require platform downtime or Customer assistance to complete. If required, IBM will declare a maintenance window in advance of any such updates, and the notification will clearly state the impacts of the scheduled maintenance and any Customer-specific requirements.

### **Security Content Updates**

To help ensure that the most current threats are properly identified, IBM will update the Agent with the most current Security Content. Such Security Content, delivered in the form of new checks or signatures for the vulnerability scanner, enhances the Agent's detection capabilities.

At the discretion of IBM, Security Content updates may be downloaded and installed onto the security platform at any time. Such an operation is transparent to users.

### **Scanning Agent Troubleshooting**

If a scanning Agent does not perform as expected, or is identified as the potential source of a network or server-related problem, IBM will examine the Agent configuration and functionality for potential issues. Troubleshooting may consist of an offline analysis by IBM, or an active troubleshooting session between IBM and Customer. IBM will attempt to resolve any technical issues as expediently as feasible. If the Agent is eliminated as the source of a given problem, no further troubleshooting will be performed by IBM.

### **Data Retention and Restoration**

During the course of Service delivery, the scanning Agent will generate a large amount of data related to discovered vulnerabilities within the Customer environment. This data will be stored within the Virtual-SOC and will remain accessible online for a period of one year from the time the data enters the system.

At Customer's request, IBM will submit a request for media location and retrieval. Hourly consulting fees will apply for all time spent restoring and preparing data in Customer's requested format.

All specified retention times assume an active VMS contract has been maintained for each unique event / log source. Cancellation of the Service for a given event/log source, or cancellation of VMS will require IBM to delete all collected data from the affected event/log sources.

## **3. Customer Responsibilities**

While IBM will work with internal scanning Customers to deploy and implement the Agent, and IBM will manage the Agent, Customer will be required to work with IBM in good faith and assist IBM in certain situations as requested by IBM.

### **3.1 Deployment and Initiation**

With remote IBM assistance, the Customer will deploy a new Agent or begin management of an existing Agent, as applicable.

At IBM's request, Customer will provide documentation showing its ownership of any IP address ranges to be scanned and will work with IBM in good faith to accurately assess Customer's network and environment. Customer must provide contacts within the organization, and specify an escalation path through the organization in the event that IBM must contact Customer.

Customer must ensure that any existing Agent meets IBM specifications, and must work to meet recommendations concerning Customer's network and network access requirements, if changes are required to ensure workable protection strategies.

If IBM will be taking over management of an existing Agent, IBM may require the Agent software or Security Content to be reinstalled or upgraded to the most current versions in order to provide the Service. Other required criteria may include the addition or removal of applications and user accounts. Such upgrades, additions, or removals will be the sole responsibility of the Customer.

Customer will work with IBM in good faith to bring internal scanning Agents "live" within committed timeframes.

Customer is responsible for assisting IBM in gaining remote access to the internal scanning Agent by configuring terminal services, as requested by the IBM deployment specialist.

### **3.2 Ongoing Management and Support**

#### **3.2.1 Configuration / Change Management**

Customer acknowledges that IBM is the sole party authorized to make direct system changes to the Agent when such Agent is managed by IBM.

Customer agrees to work in good faith to allow IBM to upgrade internal scanning Agents as new releases of the Internet scanner application become available.

Customer is required to provide advance notice of any scheduled system reboots, maintenance, or power tests that may result in temporary inaccessibility of the internal scanning Agent.

In the case of hardware or operating system failure of the internal scanning Agent, Customer is responsible for all activities associated with resolution of the failure.

Customer may be required to assist in patching or upgrading of the internal scanning Agent application.

#### **3.2.2 Server Environment / Requirements**

Servers with the internal scanning Agent installed must meet the most current application minimum system requirements as outlined in the vendor's product documentation.

Customer is responsible for taking appropriate measures to ensure the network in which the internal scanning Agent is installed is secure, using firewall configurations and following appropriate security practices.

Customer must provide a secure, physically controlled environment for servers on which the internal scanning Agent resides.

Customer will ensure that access control points within its respective networks allow scanning Agents to pass traffic through them in order to properly assess for vulnerabilities.

Customer will ensure the internal scanning Agent is Internet-accessible via a static IP address.

#### **3.2.3 Software Maintenance**

Customer is responsible for ensuring that valid support and maintenance are maintained for any Customer-provided instances of Internet scanner and for any hardware platforms on which the application resides.

#### **3.2.4 Data Compilation**

Customer consents to IBM gathering and compiling security event log data to look at trends, and real or potential threats. IBM may compile or otherwise combine this security event log data with similar data of other customers so long as such data is compiled or combined in a manner that will not in any way reveal the data as being attributable to Customer.

## 4. Service Level Agreements

IBM service level agreements (“SLAs”) establish response time objectives and countermeasures for Security Incidents resulting from the Service. The SLAs become effective when the deployment process has been completed, the device has been set to “live”, and support and management of the device have been successfully transitioned to the SOC.

The SLA remedies are available provided the Customer meets its obligations as defined in this Service Description.

### 4.1 SLA Guarantees

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

- a. Vulnerability scanning implementation guarantee – IBM will begin implementation of a scheduled vulnerability assessment within one hour (plus or minus) of the time scheduled by Customer (or by IBM on behalf of Customer) and all scans will be completed without failure. This guarantee applies only to correctly configured scan requests, for devices and networks covered by a current subscription to VMS.
- b. Virtual patch application guarantee – IBM will implement virtual patch requests, received through the Virtual-SOC, within two hours of the request being entered into the system. This guarantee is based on actual time of implementation; not on the time Customer was notified that the request was completed. This guarantee is only applicable when the requested implementation applies to a valid managed Intrusion Prevention technology under a current subscription for IBM Managed Security Services.
- c. Proactive system monitoring guarantee - Customer will be notified within 15 minutes after IBM determines Customer’s managed internal scanning Agent is unreachable via standard in-band connectivity.
- d. Proactive Security Content update guarantee – IBM will apply all new Security Content updates to Customer’s managed security platform within 72 hours from the time the Security Content update was published for general availability by the vendor.

#### SLA Guarantees Summary

SLA	External Scanning	Internal Scanning
Vulnerability scanning implementation guarantee	Available	Available
Virtual patch application guarantee	Available	Available
Proactive system monitoring guarantee	Not available	Available
Proactive Security Content update guarantee	Not available	Available

### 4.2 SLA Remedies

IBM will issue a credit as the sole remedy for failure to meet any of the guarantees described in the section entitled “SLA Guarantees”, during any given calendar month. The Customer may obtain no more than one credit for each SLA per day, not to exceed a total for all SLAs of €25.000 (euro), or the equivalent in local currency, in a given calendar month.

- a. Vulnerability scanning implementation remedy – if IBM fails to meet this guarantee, a credit will be issued as follows:
  - (1) External scans – one additional (i.e., in addition to the original) scheduled scan of equal or lesser value, at no charge; or
  - (2) Internal scans – one day of the total invoiced VMS monthly fee;
- b. Virtual patch application remedy – if IBM fails to meet this guarantee, a credit will be issued for one day of the total VMS monthly fee;

- c. Proactive system monitoring and proactive Security Content update remedies - if IBM fails to meet either of these guarantees, a credit will be issued for one day of the total VMS monthly fee.

**SLAs and Remedies Summary**

Service Level Agreements	Remedies for VMS	
	External Scans	Internal Scans
Vulnerability scanning implementation guarantee	Credit of 1 additional scan	Credit of 1 day of the monthly fee for VMS
Virtual patch application guarantee	Credit of 1 day of the monthly fee for VMS	
Proactive system monitoring guarantee	Not available	
Proactive Security Content update guarantee	Not available	

**5. SLA Exclusions and Stipulations**

**5.1 Customer Contact Information**

Multiple SLAs require IBM to provide notification to the designated Customer contact after certain events occur. In the case of such an event, Customer is solely responsible for providing IBM with accurate and current contact information for the designated contact(s). The current contact information on record is available to authorized contacts. IBM will be relieved of its obligations under these SLAs if IBM contact information is out of date or inaccurate due to Customer action or omission.

**5.2 Customer Network/Server Change Notifications**

Customer is responsible for providing IBM advance notice regarding any network or server changes to the firewall environment. If the event advance notice cannot be provided, Customer is required to provide IBM with notification of changes within seven calendar days of said network or server changes. If Customer fails to notify IBM as stated above, all SLA remedies are considered null and void.

**5.3 SLA Compliance and Reporting**

SLA compliance and the associated remedies are based on fully functional network environments, Internet and circuit connectivity, firewalls, and properly configured servers. If SLA compliance failure is caused by CPE hardware or software (including any and all Agents), all SLA remedies are considered null and void. IBM will provide SLA compliance reporting through the Virtual-SOC.

**5.4 Testing of Monitoring and Response Capabilities**

Customer may test IBM monitoring and response capabilities by staging simulated or actual reconnaissance activity, system or network attacks, and/or system compromises. These activities may be initiated directly by Customer or by a contracted third party with no advance notice to IBM. SLAs will not apply during the period of such staged activities, and remedies will not be payable if the associated guarantee(s) are not met.

**6. Service Level Objectives**

IBM service level objectives (called "SLOs") establish nonbinding objectives for the provision of certain features of the Service. The SLOs become effective when the deployment process has been completed, the device has been set to "live", and support and management of the device have been successfully transitioned to the SOC. IBM reserves the right to modify these SLOs with 30 days prior written notice.

- a. Virtual-SOC – IBM will provide a 99.9% accessibility objective for the Virtual-SOC outside of the times detailed in the section entitled "Scheduled and Emergency Portal Maintenance".
- b. Internet Emergency – In the event IBM declares an Internet emergency, it is IBM's objective to notify Customer's specified points of contact via e-mail within 15 minutes of emergency declaration. This notification will include an incident tracking number, telephone bridge number, and the time that IBM will conduct a situation briefing.

During declared Internet emergencies, IBM will provide a live telephone-conference situation briefing and summarized e-mail designed to provide information that Customer can use to protect its organization. Situation briefings following the onset of an Internet emergency will supersede any requirement for IBM to provide Customer-specific escalations for events directly related to the declared Internet emergency. IBM will communicate all other priority level incidents, during an Internet emergency, via automated systems such as e-mail, pager and voice mail.

Standard escalation practices will resume upon conclusion of the stated Internet emergency. Termination of an emergency state is marked by a decrease in the AlertCon level to AlertCon 2, or an e-mail notification delivered to an authorized Customer security contact.

## **7. Scheduled and Emergency Portal Maintenance**

Scheduled maintenance shall mean any maintenance:

- a. of which Customer is notified at least five days in advance; or
- b. that is performed during the standard monthly maintenance window on the second Saturday of every month from 8:00 a.m. – 4:00 p.m. United States Eastern Time. Notice of scheduled maintenance will be provided to the designated Customer contact.

No statement in the section entitled "Service Level Agreements" shall prevent IBM from conducting emergency maintenance on an "as needed" basis. During such emergency maintenance, the affected Customer's primary point of contact will receive notification within 30 minutes of initialization of the emergency maintenance and within 30 minutes of the completion of any emergency maintenance.

## **8. Other Terms and Conditions**

IBM reserves the right to modify the terms of this Service Description at any time. Should such modification reduce the scope or level of the Service being delivered (for example, eliminating a previously provided Service or lengthening the Security Incident response time), IBM will provide a minimum of 30 days prior notice via the ISS Web portal or other electronic means.