CYBER SECURITY – SERVICE DESCRIPTION

Vulnerability Management as a Service

This document ("**VMaaS Service Description**") contains the terms governing the provision of the Vulnerability Management as a Service by Interactive Pty Ltd (ABN:17 088 952 023) of 461 Williamstown Road, Port Melbourne Vic 3207 ("**Interactive**") to the customer named in the CMS SOW that applies to this VMaaS Service Description ("**Customer**").

This VMaaS Service Description forms part of the Agreement, also containing the Cyber Security Service Terms (found at https://www.interactive.com.au/terms-and-conditions) and the Master Services Agreement.

1 Vulnerability Management Service

1.1 The Vulnerability Management Service identifies security vulnerabilities exposed on the Assets. The vulnerability scanning function is implemented using a network of vulnerability scanners and/or agents using the Cloud Platform.

1.2 Interactive will perform Vulnerability Scans of IP addresses to identify and rank vulnerabilities in network infrastructure and web applications in accordance with the schedule agreed between the parties during the Preparation Phase. This is a proactive check of the network and web applications to reduce the cyber security risks due to vulnerabilities.

1.3 Interactive will provide notification of vulnerabilities to the Assets by business criticality and severity, with recommendations to mitigate the vulnerability. This may include recommendations to patch systems or change rules on perimeter devices.

1.4 The Customer may request Vulnerability Scans be performed ad-hoc outside the agreed scan schedule by making a Service Request. An amount of ad-hoc Vulnerability Scans is included in the Service Fee, as set out in the CMS SOW. If the Customer requests additional ad-hoc Vulnerability Scans, they will be deemed Out of Scope Work.

2 Customer Onboarding

2.1 Interactive will perform following activities as part of onboarding for the Vulnerability Management Service:

(a) Interactive will schedule a Customer kick-off meeting within 2 weeks after the Service Start Date to obtain an understanding of the environment, such as the number of sites, virtual or physical Assets, bandwidth utilisation, internet connectivity and connectivity between different sites.

(b) Interactive will provide the Cloud Platform scanner appliance to the Customer. The Customer must download and install the agent for the Cloud Platform to the appliance. Interactive will remotely apply updates to the appliance as they are made available.

3 Asset Discovery

3.1 Interactive will undertake an Asset discovery activity to ensure a complete register of Assets is created. During this activity:

(a) the Customer will provide information on IP ranges and specific Assets;

(b) Interactive will perform a network discovery scan at a time agreed between Interactive and the Customer during the Preparation Phase; and

(c) the CMS SOW will be deemed to be updated to include any Assets discovered during the network discovery scan above the quantities specified in the CMS SOW, with additional Assets charged accordingly.

3.2 The Customer acknowledges Interactive is not liable for impact or outages caused as a result of performing the network discovery scan.

4 Asset Classification

4.1 Assets will be classified by the Customer into groups based on criticality to the Customer's business.

4.2 Assets will be classified by the Customer during the Preparation Phase as being one of:

(a) External IP (public addresses);

(b) Critical devices with an internal IP address, including devices such as servers, routers and core switches; or

(c) Other devices with an internal IP address, including desktops and laptops.

5 Vulnerability Scan

5.1 Interactive will perform the following Vulnerability Scans:

(a) External scans;

(b) Internal scans including authenticated scans;

(c) Critical Internal IP's scanned (via agents when required); and

(d) Other Internal IP's scanned (via agents when required).

5.2 Interactive will perform automated scanning of Assets according to the frequency set out in the CMS SOW.

5.3 The Customer must raise a Service Request to change any agreed date/time for Vulnerability Scans.

6 Reporting

6.1 Interactive will produce, validate, and review a report on a monthly basis that will be presented to the Customer ("the VM Report"). The VM Report will include the following:

(a) Executive summary - a high-level summary that provides a snapshot of vulnerabilities by:

(i) Severity set by the scanning technology; and

(ii) Top vulnerabilities ranked by severity and showing affected Assets.

(b) Vulnerabilities identified and an assessment on each vulnerability:

(i) Title of the vulnerability;

(ii) CVE-ID and Cloud Platform Vendor assigned ID;

(iii) Base CVSS and Cloud Platform Vendor assigned severity;

(iv) Threat (observation);

(v) Impact on the Customer's services;

(vi) Recommendations to mitigate the vulnerability; and

(vii) Next steps.

(c) Remediation recommendations and implementation:

(i) Recommendations to remediate in accordance with the remediation timeframe as detailed in Table 1, with each Asset in this part of the report highlighting detected vulnerabilities and the criticality of remediation.

(ii) Interactive will raise a Service Request in Interactives ITSM tool to notify the person responsible for remediation about the identified vulnerabilities and track remediation based on rules agreed with the Customer during the Preparation Phase.

(iii) Interactive will notify the Customer via email about vulnerable Assets containing affected software and enabled features.

(iv) Interactive will raise a Service Request to notify the person responsible for remediation about vulnerabilities based on the grouping of the Asset. The Service Request will contain the following information:

A. Asset criticality;

B. Vulnerability;

C. Reported date;

D. Severity of vulnerability; and

E. Assignee.

(d) If the vulnerabilities are identified in managed components provided by Interactive to the Customer under a separate agreement for the provision of cloud IaaS services (for example, the operating system of Interactive managed virtual machines), Interactive will co-ordinate the remediation of the vulnerability until it is remediated and detail current progress within the VM Report. The Customer remains ultimately responsible to remediate.

6.2 The Customer must approve the format and content of the template VM Report before Interactive will provide the first VM Report to the Customer.

6.3 The Customer must raise a Service Request for any system generated reports available under the Cloud Platform through the Vulnerability Management Service. Bespoke or non-system generated reports are not in scope but may be requested as Out of Scope Work.

6.4 Interactive recommends that the Customer adheres to the recommended remediation timeframes detailed in Table 1.

Table 1.	**Remediation Timeframes**	
Vulnerability	**Description**	**Suggested Remediation Timeframe (from notification)**
Critical	Intruders can easily gain control of the Asset, which can lead to the compromise of the Customer's entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.	Within 48 Hours
High	Intruders can possibly gain control of the Asset, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the Asset.	Within 1 week
Medium	Intruders may be able to gain access to specific information stored on the Asset, including security settings. This could result in potential misuse of the Asset by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the Asset, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorised use of services, such as mail-relaying.	Within the next patch cycle (either monthly or quarterly)
Low	Intruders may be able to collect sensitive information from the Asset, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.	Remediation should be considered in relation to other vulnerabilities present on the system. These vulnerabilities are unlikely to be exploited however could be used in reconnaissance by an attacker to formulate an attack plan.
Info	Intruders can collect information about the Asset (open ports, services, etc.) and may be able to use this information to find other vulnerabilities	

7 Re-scan

7.1 The process of re-scanning is the verification of any remediation. The re-scan will be undertaken on the same Assets with the same scan profile at the end of remediation to verify whether the remediation was successful.

8 Vulnerability Management Pricing

8.1 The Service Fees for the Vulnerability Management Service are based on the quantity of Assets specified in the CMS SOW.

8.2 The Customer may request to add Assets by making a Service Request and providing relevant details. Interactive will add the Assets and the Customer will be charged for the addition pro-rata from the date it is added.

9 Customer Responsibilities and Acknowledgements

9.1 The Customer must:

(a) provision user accounts for Interactive that permit authenticated Vulnerability Scans; and

(b) open all ports from the Scanner to all internal Assets, to ensure proper functionality of the Scanner.

9.2 The Customer authorises Interactive to deploy an agent on the Assets and acknowledges the agent to be deployed on the Assets can impact performance.

9.3 The Customer acknowledges that any software provided as part of the Vulnerability Management Service is licensed, not sold, to the Customer on a Subscription basis and only for the limited use as permitted by, and in accordance with, this VMaaS Service Description. The Customer acknowledges that not all Vulnerability Management Service Subscriptions include software.

9.4 The Vulnerability Management Service utilises the Cloud Platform Vendor’s service. The Customer’s use of the Vulnerability Management Service is subject to, and the Customer must comply with, the Cloud Platform Vendor Terms. The Customer must monitor the relevant URL (as may be changed from time to time) for updates to the Cloud Platform Vendor’s Terms and comply with the Cloud Platform Vendor’s Terms as they are updated. Interactive is an authorised reseller of the Cloud Platform Vendor and has the right to resell the Vulnerability Management Service.

9.5 The Customer acknowledges the Cloud Platform may change.

9.6 The Customer agrees and acknowledges that Interactive is not liable for any failure of the Cloud Platform (including if the Cloud Platform is unavailable), or for any failure to provide Vulnerability Management Services, to the extent the failure is caused or contributed to by the Cloud Platform or Cloud Platform Vendor.

9.7 Except to the extent permitted by applicable law, the Customer must not:

(a) modify, prepare derivative works or, reverse engineer, reverse assemble, disassemble, decompile or otherwise attempt to decipher any code used in connection with the Cloud Platform and/or any aspect of Cloud Platform Vendor’s technology;

(b) knowingly or negligently access and/or engage in any use of the Vulnerability Management Service in a manner that abuses or materially disrupts the networks or security systems of any third party;

(c) market, distribute, sublicence, offer to sell, sell, and/or resell the Vulnerability Management Service to any third party; or

(d) use the Vulnerability Management Service, VM Reports, API or any data or information contained in any of the foregoing, except for the limited purpose of monitoring its own security (e.g. vulnerability management or malware detection) in accordance with this VMaaS Service Description.

10 Network requirements

10.1 For single network/multiple network scanning, the Customer must ensure that the destination network for LAN is configured to allow all ports (IP) from the Cloud Platform Vendor's scanner (the "Scanner"), which will be deployed virtually or physically at the Customer Location, as agreed during the Preparation Phase.

10.2 The Customer must enable the Scanner to have access to the Internet over TCP port 443 and provide a connection to the Cloud Platform with a minimum bandwidth of 3Mbps.

10.3 The Scanner must be able to resolve DNS for the hostnames to be scanned. For the purpose of clarity, the Customer may choose to enable the Scanner to utilise a DNS server provided by the Customer or utilise an internet accessible DNS server. The Customer acknowledges that if the Scanner cannot resolve DNS, scan performance will be affected.

10.4 Virtual deployment

If the Customer elects to proceed with a virtual Scanner deployed, this item 10.4 applies.

(a) The Customer must provide a virtual environment for the Scanner and deploy the Scanner on that environment.

(b) The Customer must provision the following configurable resources for virtual Scanner:

(i) Minimum resource configuration:

1 x vCPU | 1.5 GB RAM | 1 x 56GB virtual HDD (40GB for versions prior to qVSA 2.4.26-x).

(ii) Maximum resource configuration:

16 x vCPU (recommended maximum of 8) | 16GB RAM.

(iii) Interactive will advise the Customer on recommended resources based on the number of Assets to be scanned. If the Customer does not provision the recommended resources, scan performance will be affected.

(c) The Customer must configure its network to support the virtual Scanner (up to 2 x virtual network interfaces):

(i) If one interface is in use:

A. Interface 1: "LAN/WAN" interface - used for both scanning of targets and outbound connection to the Cloud Platform.

(ii) If two interfaces are in use:

A. Interface 1: "LAN" interface - used for scanning of Assets.

B. Interface 2: "WAN" interface - used for outbound connection to the Cloud Platform.

(iii) IPv4 address assignment: static, DHCP.

(iv) Proxy server - outbound to Cloud Platform:

A. Username/password authentication supported;

B. VLAN tagging; and

C. Static routing.

10.5 Physical deployment

If the Customer elects to proceed with a physical Scanner deployed, this item 10.5 will apply.

(a) The Customer must pay additional costs for:

(i) the physical Scanner;

(ii) deployment and configuration onsite; and

(iii) ongoing management and maintenance of the Scanner.

(b) The Customer must configure its network to support the physical Scanner (up to 2 x virtual network interfaces):

(i) IPv4 address assignment: static, DHCP; and

(ii) Proxy server - outbound to Cloud Platform

A. Username/password authentication supported;

B. VLAN tagging; and

C. Static routing.

(c) The Customer is responsible for:

(i) providing rack space, cooling and power requirements for the physical Scanner;

(ii) all physical networking requirements (cables, switches, routing etc); and

(iii) courier and logistical costs associated with the initial shipping of the physical Scanner and any subsequent back-to-base requirements for repair.

11 Definitions

11.1 The following definitions apply to this VMaaS Service Description:

Asset is a single piece of hardware or software that has an IP address that is being scanned by the Vulnerability Management Service.

Cloud Platform refers to the distributed platform used by the Vulnerability Management Service to conduct scanning, vulnerability testing and reporting.

Cloud Platform Vendor means the person or entity providing the Cloud Platform, which may be Interactive or a third party engaged by Interactive.

Cloud Platform Vendor Terms mean the following documents, which may be updated or replaced from time to time without notice:

(a) Platform SLA https://www.qualys.com/docs/service-level-agreement.pdf

(b) Master Cloud Services Agreement (MCSA), also called EULA referenced as the click through document https://www.qualys.com/docs/master-cloud-service-agreement.pdf

External means a Vulnerability Scan that is conducted from outside the Customer's Network.

Internal means a Vulnerability Scan that is conducted from inside the Customer's Network, which may involve installing Tools on the Customer's Network or integration into Interactive's network.

Network means a network that is part of or connected in some way to the IT Environment.

Preparation Phase means the Asset Discovery phase (item 3) and Classification of Assets phase (item 4).

Service Request means a request from the Customer for information, advice or change.

Subscription means a non-exclusive, non-transferable right to use the Vulnerability Management Service in accordance with this VMaaS Service Description.

Tools means the commercial, open source or in-house developed tools and scripts Interactive will use to perform the Vulnerability Management Services, which may be chosen by Interactive. Interactive may use certain scripts, which may be manual or automatic, such as JavaScript, Python or PowerShell, to perform the Vulnerability Management Services.

Vulnerability Scan means the scans set out in item 5 to identify and quantify known vulnerabilities in the IT Environment (which may include misconfigurations, lack of controls, bugs and other security weaknesses), the possibilities of reducing those vulnerabilities and improving the capacity to manage future Cyber Security Threats.

Vulnerability Management Service means the services described in this VMaaS Service Description.