CYBER SECURITY – SERVICE DESCRIPTION

Managed Detection and Response

This document ("**MDR Service Description**") contains the terms governing the provision of managed or endpoint detection and response services 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 MDR Service Description ("**Customer**").

This MDR 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 Managed Detection and Response (MDR)

1.1 MDR Services are the combination of an anti-virus and end point detection and response agent, coupled with active monitoring and response services. The MDR Service will utilise Cloud Agents (which may be VMware Carbon Black, Microsoft Defender for Endpoint agent or CrowdStrike Falcon Enterprise, as set out in the CMS SOW) to analyse endpoint data to identify threats. MDR Services are intended to detect known malware, including viruses and unknown or zero-day malware, and attacker techniques based on behaviours.

1.2 Active monitoring services involves the triage of alerts generated by the Cloud Agent and utilises threat intelligence and other tools to manually assess the authenticity of the alert.

2 Managed Alerts and Triage

2.1 Interactive will, on a 24x7 basis:

(a) Manually review alerts generated by the Cloud Platform. The manual review may include a review of the following, depending on the alert received:

(i) File integrity.

(ii) Process execution tree.

(iii) Code execution in a sandbox.

(iv) Command line execution.

(v) Device history and status.

(vi) Software certificate status.

(vii) Network connectivity.

(b) Alert the Customer via telephone in the event of a genuine or suspected Security Incident.

3 Onboarding

3.1 Onboarding of Cloud Agents for Assets can be done via one of the following options (unless the parties agree to another onboarding method), which will be discussed and decided upon by Interactive and the Customer during the pre-engagement phase (being the phase after signing the CMS SOW and before on-boarding):

VMware Carbon Black

(a) Command-line installation (unattended) - Company registration code is required. Sensors are enrolled via the command-line or automated software deployment method. Unattended installation deployments use either SSCM (System Centre Configuration Manager) deployment or GPO (Group Policy Object) deployment.

(b) Direct end-user installation by email (attended) – Email activation code is required. The Customer's end users must enroll sensors manually via an email invitation from the console.

Microsoft Defender for Endpoint

(a) Local Script (for up to 10 Windows devices).

(b) Group Policy.

(c) Microsoft Endpoint Configuration Manager.

(d) Mobile Device Management / Microsoft Intune.

(e) VDI onboarding scripts for non-persistent devices.

CrowdStrike Falcon Enterprise

(a) Command-line installation (unattended) - Company registration code is required. Sensors are enrolled via the command-line or automated software deployment method. Unattended installation deployments use GPO (Group Policy Object) deployment.

3.2 As part of the on-boarding process, Interactive and the Customer will agree on certain pre-approved actions that Interactive can perform in the event of a Security Incident.

4 Requirements

4.1 The Customer must enable the Cloud Agent to have access to the internet over TCP port 443 and port 80 (this is for certificate revocation lists) and provide a connection to the Cloud Platform.

4.2 If the Customer has an existing anti-virus solution on the Assets, then:

(a) where the Customer already subscribes to the Interactive Trend Micro anti-virus solution Interactive will remove the Trend Micro solution after the Service Start Date; or

(b) where the Customer has its own anti-virus solution, the Customer is responsible for removing the anti- virus within a reasonable timeframe after the Service Start Date. If the Customer fails to do so, the Customer accepts any degradation to the MDR Service that may result.

4.3 The MDR Service relies on Cloud Agents and can therefore not be supported if the Cloud Platform Vendor has not certified the Cloud Agent on a specific platform. The Customer must ensure the Cloud Agent and/or MDR sensor is supported and may view the latest list of support platforms at the following URLs (or successor URLs):

(a) VMware Carbon Black: https://community.carbonblack.com/t5/Documentation-Downloads/Carbon- Black-Cloud-sensor-support/ta-p/66274

(b) Microsoft Defender for Endpoint: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/minimum-requirements?view=o365-worldwide.

(c) CrowdStrike Falcon Enterprise: https://www.crowdstrike.com/products/faq/

5 Rule Management

5.1 Interactive will apply the Standard Cloud Platform Policy as a baseline of the IT Environment to secure the Assets and determine applications in use.

5.2 In consultation with the Customer, Interactive will adjust the Standard Cloud Platform Policy. The Customer may select up to 5 separate policies, to apply to different parts of the IT Environment (for example, separate policies for end points, servers and test/dev environment). At the Customer's request by logging a ticket with Interactive's service desk, Interactive will provide up to 5 changes to policies or rules per month. Additional policy or rule changes will be deemed Out of Scope Work. Interactive will respond to requests for policy and rule changes within 48 hours but does not guarantee when the policy or rule change will be made effective, as this is contingent on the Customer's change process.

5.3 The Customer is responsible for ensuring changes to policies and rules are tested and accepted before implementation. After the Customer has tested and accepted the change to the policy or rule, Interactive will implement it.

6 Managing Allowlists / Denylists

6.1 The Customer must provide Interactive with a list of approved and prohibited software during the onboarding phase, which will be used to populate the allowlist and denylist. Allowlisted software is permitted to execute and will not alert in the Cloud Platform. Denylisted software is not permitted to execute and will also raise an alert on the Cloud Platform.

6.2 The Customer is responsible for ensuring the details of any approved software are communicated to Interactive to ensure allowlisting. Interactive will update the allowlist within 24 hours after being notified of a required change. The Customer acknowledges that delays may occur in updated policies being communicated to all Cloud Agents, notwithstanding the allowlist has been updated.

6.3 The Customer acknowledges that the MDR Service may prevent the execution of software that is not on the allowlist. The Customer must notify Interactive about any required changes to the allowlist and denylist via the change process defined during the onboarding phase.

6.4 Changes to the allowlist are unlimited and not deemed a change to policy. Changes to the denylist are deemed a change to policy and will be counted towards the 5 included changes referred to in item 5.2.

6.5 At Interactive's initiative and discretion, known malicious software may be added to the denylist, but will be done so only in consultation with the Customer.

6.6 The Customer must approve the allowlist and denylist in writing before Interactive implements the lists. After Interactive implements the allowlist and denylist, the Customer is responsible to test the lists to ensure they are accurate, and to advise Interactive if any changes to the lists are required.

7 User Compliance reporting

7.1 User compliance is measured through Asset readiness for response to active threats.

7.2 Assets are compliant when the Cloud Agents:

(a) are enabled on the Assets;

(b) are up to date with signature and virus definitions; and

(c) have the correct policy applied as defined during on-boarding.

7.3 As part of monthly reporting, the compliance check result identifies non-compliant Assets that require actions by the Customer. Actions will include one or a combination of:

(a) an Asset restart to ensure patch completion if not already completed;

(b) turning on an Asset that has not communicated for a period time defined in the policy; and

(c) troubleshooting connectivity issues between the Assets and the Cloud Platform.

8 Reporting

8.1 Interactive will provide a monthly report to the Customer, which will include the following:

(a) List of top detections.

(b) Top policy violations.

(c) Compliance check results.

(d) Suggested improvements to the Customer's security posture if any are identified through the MDR Service.

9 Response

9.1 The Cloud Platform categorises alerts as either a Threat or Observed Behaviour (as each are defined below) and assigns criticality ratings of between 1 and 10 according to the policy.

(a) **Threat**: A known or suspected malicious behaviour executing on an Asset. This includes threat intelligence events.

(b) **Observed Behaviour**: When an Asset exhibits malicious or anomalous behaviours that may indicate a threat to the Asset. Requires further investigation.

9.2 Interactive will triage any Threat alert or Observed Behaviour alert (as defined in item 9.1) within the following timeframes to determine if the alert is a Security Incident:

(a) Threat or Observed rating of 4, 5 and 6:

(i) Medium Priority Alert – 4 hours

(b) Threat and Observed rating of 7, 8, 9 and 10

(i) High Priority Alert – 1.5 hours

9.3 Interactive will respond to all Threat alerts and Observed Behaviour alerts with a criticality rating of 4 and above. Threat alerts and Observed Behaviour alerts rated 1-3 are considered informational. For informational alerts, Interactive will monitor the endpoint for any change in the Threat or Observed Behaviour alerts.

9.4 At the time of identification of Security Incident Interactive will classify and assign a priority rating of the Security Incident based on severity, magnitude and criticality of the systems affected by the Security Incident. The Customer will be notified.

9.5 If an Asset is actively compromised through malware:

(a) Interactive will respond by quarantining the device, such that the Asset may only communicate with the Cloud Platform and stop running any non-essential processes and services;

(b) Interactive may quarantine the Asset before notifying the Customer to stop a Threat before propagating to the wider network; and

(c) the Customer may be required to assist with containment or segregation of endpoints from the Network (physically).

9.6 Interactive may remove malicious software identified on Assets or hosted on the Network (via shared drives/folders) in consultation with the Customer.

10 MDR Services Pricing

10.1 The Service Fees for the MDR Service are based on the quantity of Assets specified in the CMS SOW and are payable from the Service Start Date.

10.2 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.

11 Licensing

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

11.2 This clause 11.2 applies if the Cloud Agents are CrowdStrike Falcon Enterprise.

(a) The Customer must agree and comply with CrowdStrike's terms applicable to CrowdStrike Falcon Enterprise, including those found at the following URLs (or successor URL):

(i) https://www.crowdstrike.com/terms-conditions/

(b) The Customer agrees that the use of CrowdStrike Falcon Enterprise is strictly for its own internal use.

(c) The Customer confirms that it holds valid licensing for the CrowdStrike Falcon Enterprise Cloud Platform.

(d) The Customer authorizes CrowdStrike to provide Interactive with the necessary rights and privileges to the Cloud Platform account, including but not limited to the ability to:

(i) download and install the CloudPlatform sensors on the Customer devices;

(ii) access and use the Cloud Platform and Customer data therein, as well as the Cloud Platform application programming interfaces, and

(iii) acquire and transmit Customer data from the Cloud Platform to Interactive or the Customer systems.

(e) The Customer acknowledges the CrowdStrike terms may vary at any time without notice.

11.3 This clause 11.3 applies if the Cloud Agents are Microsoft Defender for Endpoint.

(a) The Customer must comply with Microsoft's terms applicable to Microsoft Defender for Endpoint, including those found at the following URLs (or successor URL):

(i) https://docs.microsoft.com/en-us/legal/microsoft-365/mde-terms-windows

(ii) https://www.microsoft.com/licensing/terms/productoffering/MicrosoftDefenderforEndpoint/MCA

(b) The Customer acknowledges the Microsoft terms may vary at any time without notice.

11.4 This clause 11.4 applies if the Cloud Agents are VMware Carbon Black.

(a) **Acknowledgements:** Interactive and the Customer acknowledge that:

(i) The CMS SOW is concluded solely between Interactive and the Customer, and that Carbon Black Inc. ("Carbon Black") is not a party to the CMS SOW;

(ii) Interactive, not Carbon Black, is solely responsible to the Customer for the MDR Services, including the Cloud Platform;

(iii) Carbon Black has no liability directly to the Customer, and the Customer will seek any remedies to which it may be entitled under the CMS SOW or any other agreement against Interactive and not against Carbon Black, and any provisions of the Agreement regarding the limitation of Carbon Black's liability survive expiration or termination of the CMS SOW indefinitely;

(iv) the Customer may not, and may not help or assist others, to reverse engineer, reverse compile, modify or create derivative works of the Cloud Platform, sublicense the Cloud Platform or use the Cloud Platform other than as expressly permitted by this MDR Service Description;

(v) Interactive is solely responsible for providing any maintenance and support services to the Customer, and Interactive and the Customer acknowledge that Carbon Black has no obligation to furnish any maintenance and support services directly to the Customer; and

(vi) promptly upon expiration or termination of the CMS SOW, the Customer will delete all copies of the Cloud Platform and all related materials, and at Carbon Black's request (via Interactive), the Customer must agree to certify the destruction and return of the Cloud Platform and related materials.

(b) **Scope of Use:** The Customer is entitled to use the Cloud Platform solely as part of the MDR Service, in object code and cloud service form, for Customer's internal use only.

(c) **Warranty:** Interactive is solely responsible for any product warranties, whether express or implied by law, and for all liability from and to Customers arising out of Interactive's implementation and use of the MDR Service.

(d) **Export and Import Compliance; U.S. Government Rights:** Interactive and the Customer acknowledge and agree that:

(i) the Cloud Platform will not be used, and none of the underlying information, software, or technology may be transferred or otherwise exported or re-exported to countries as to which the United States and/or the European Union maintains an embargo (collectively, "Embargoed Countries"), or to or by a national or resident thereof, or any person or entity on the U.S. Department of Treasury's List of Specially Designated Nationals or the U.S. Department of Commerce's Table of Denial Orders (collectively, "Designated Nationals");

(ii) the Cloud Platform may use encryption technology that is subject to licensing requirements under the U.S. Export Administration Regulations, 15 C.F.R. Parts 730-774 and Council Regulation (EC) No. 1334/2000;

(iii) Interactive and the Customer acknowledge and agree that the Cloud Platform is "commercial computer software" or "commercial computer software documentation", and that absent a written agreement to the contrary, the U.S. Government's rights with respect to such Cloud Platform are limited by the terms of this MDR Service Description, pursuant to FAR§ 12.212(a) and/or DFARS § 227.7202-l(a), as applicable.

(e) **Third Party Beneficiary:** Interactive and the Customer acknowledge and agree that Carbon Black is a third party beneficiary of items 11.3(a) to (e) of this MDR Service Description with full power and authority to enforce those items against the Customer as a third party beneficiary thereof. For the avoidance of doubt, the parties acknowledge and agree that the Customer shall not be a third party beneficiary with respect to Carbon Black.

(f) On termination of the CMS SOW, the Customer must delete, or permit Interactive to delete, all copies of the Cloud Platform and any Carbon Black products that were installed at the Customer Location or other Customer site, and any related materials.

(g) Without limiting Interactive's rights to vary this MDR Service Description in accordance with the Cyber Security Terms, Interactive may amend this MDR Service Description without the Customer's written agreement to the amendment by giving the Customer at least 30 days' notice if Carbon Black amends the agreement between Interactive and Carbon Black. If Interactive believes, acting reasonably, that the amendment will impose additional obligations on Interactive or the Customer or materially affect their respective existing rights and obligations, except where the amendment is required by law or regulation, this MDR Service Description will remain unamended as to MDR Services and additional Assets ordered until the end of the current Individual Term, from when the amendment will take effect. If the amendment is required by law or regulation, Interactive will provide 30 days' notice of the amendment, unless the amendment is required by law or regulation to take immediate effect, in which case Interactive will provide as much notice as is possible in the circumstances.

11.5 The Customer acknowledges pricing for additional Assets added may change during the Individual Term.

11.6 The Customer will defend and indemnify Interactive and its, officers, directors and employees, against any and all damages, losses, liabilities and expenses (of whatever form or nature, including, without limitation, reasonable attorneys and expense fees and costs of litigation), that they or any of them may sustain, as a direct result of any claim by the Customer arising from or related to the Customer's use of the Cloud Platform or the Customer's breach of this clause 11, but excluding:

(a) claims arising from the Cloud Platform itself; or

(b) claims arising from the proper or intended use of the Cloud Platform.

11.7 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 MDR Services, to the extent the failure is caused or contributed to by the Cloud Platform or Cloud Platform Vendor.

11.8 Except for guarantees that cannot be excluded by law, Interactive expressly disclaims all guarantees and warranties, whether express, implied or otherwise, including without limitation, guarantees of merchantability, quality and fitness for a particular purpose in respect of the Cloud Platform. Interactive does not guarantee or warrant that the Cloud Platform will be available, uninterrupted or error free, meet the Customer's requirements, or operate with the combination of hardware and software the Customer intends to use, including Services provided by Interactive.

12 Definitions

12.1 The following definitions apply to this MDR Service Description:

Asset is a single piece of hardware or software that has an IP address that is being scanned by the Cloud Agents.

Cloud Agents means software agents that connect Assets to the Cloud Platform for purposes of event logging.

Cloud Platform refers to the distributed platform used by the MDR Service to conduct endpoint security event management.

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

MDR Services means the managed or endpoint detection and response services set out in this MDR Service Description. EDR Services (as may be specified in the CMS SOW) are also MDR Services.

Security Event means a condition or situation detected by the Cloud Platform, which is observed from one or more Cloud Agents.

Security Incident means one or more Security Events identified by the Customer or Interactive to be an adverse condition or situation in the IT Environment.

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

Standard Cloud Platform Policy means the standard policy as defined by the Cloud Platform Vendor.