SERVICE DESCRIPTION: DEFEND ICE - INCIDENT MANAGEMENT HANDLING AND RESPONSE (IMHR)

PART A – DESCRIPTION

DEFEND iCE (Intelligent Cybersecurity Ecosystem) Incident Management Handling and Response (IMHR) provides a specialised Cybersecurity Operations team, with 24x7x365 security event monitoring and response, with proactive tuning, optimisation, and threat hunting. This enables your organisation to respond to and mitigate cybersecurity incidents. IMHR is a monthly subscription-based service. DEFEND iCE IMHR is provided to you by DEFEND Limited, as subcontractor for One New Zealand.

As part of IMHR, Microsoft Sentinel is deployed into your environment and configured with appropriate service options and connectors, ensuring that your data stays within your Azure environment. Incidents are sent to DEFEND's ITSM system, allowing for an immediate investigation by DEFEND's cybersecurity operations team.

PART B – OPTIONS & INCLUSIONS

<table>
<tr><th colspan="2">OPTIONS</th></tr>
<tr><td rowspan="4">Initial Connectors will connect to your data sources, and can be deployed, configured, and verified prior to service go-live.
DEFEND will ingest data based from the Connectors selected, to gain an understanding of threats, risks, and controls giving visibility of actions.
You may have one or a variety of these Connectors (as selected as part of the implementation.)</td><td>Microsoft Native Connector – Microsoft Sentinel comes with many out of the box connectors for Microsoft services, which you can integrate in real time</td></tr>
<tr><td>Syslog – stream events from Linux-based, Syslog-supporting devices into Microsoft Sentinel using the Log Analytics agent for Linux</td></tr>
<tr><td>Standard MS Cloud Connectors - No license required
Azure Active Directory
Azure Activity
Office 365</td></tr>
<tr><td>Premium MS Defender Connectors – License required. Available from One New Zealand or from your existing MS Licencing Partner (charges apply)
Azure Active Directory Identity Protection
Microsoft Defender for Cloud
Microsoft Defender for Cloud Apps
Microsoft Defender for Endpoint
Microsoft Defender for Identity
Microsoft Defender for Office 365</td></tr>
<tr><th colspan="2">INCLUSIONS</th></tr>
<tr><td>Security Event Monitoring</td><td>Monitors all incoming security alerts generated in your Microsoft Sentinel instance 24/7</td></tr>
<tr><td>Security Event Triage and Analysis</td><td>Triages events received via incoming security alerts and those logged by you. Reviews events determining if they are an incident requiring response and remediation activities or an event which DEFEND can look to tune out where appropriate</td></tr>
<tr><td>Security Incident Response and Remediation</td><td>Responds to security alerts based on priority and provides closure updates. For high priority incidents, additional communications and escalation will be provided. DEFEND's engineers will manage the incident response process and engage with you to prioritise implementation and remediation.</td></tr>
</table>

Threat Hunting	Proactive threat hunting activities within Sentinel to identify anomalous behaviour, threat indicators, and entities that would be outside the scope of generating alerts. Threat Hunting capability may also be leveraged as a reactive activity off the back of any verified incidents.
Tuning and Optimisation	Threat playbooks are used to fine-tune logging, alerting and incident identification rules against the agreed threat scenarios relevant to your business. Includes analysis, investigation and event correlation meaning that tuned-out security alerts are still visible if required. Further improvements may be related to automating incident response where defined repeatable actions need to be undertaken.
Configuration Assistance	Daily health checks of the Microsoft Sentinel service and data connectors. Quarterly configuration review and new feature implementations will be performed
Reporting	Weekly health check, reporting on BAU coverage and ticket handling numbers, as well as any outstanding items awaiting attention. Monthly Dashboard reports summarise security alert, incident and near miss volumes and details, continuous improvements action statuses, and SLA response time coverage. Post Incident reports will also be provided as appropriate
Meetings	Operations meetings are scheduled fortnightly covering a high-level review of the Sentinel environment, any outstanding tuning and continuous improvement propositions and actions, any changes to operational processes, and discussion around any upcoming work or roadmap items.
Advanced Incident Response	Integrates into existing operational environment & provides seamless escalation and transition point from daily IMHR to dealing with major cybersecurity incidents (T&M basis). Please refer to AIR Service Description

INCIDENT RESPONSE TARGETS

ITSM Severity	Sentinel Severity	Response Time	Support Hours	Definition
1	N/A – raised only after triage and validation	Based on originating Sentinel Incident Severity	24/7	Response within 30 minutes of triaged and validated security alert or notification indicating an uncontained and active threat within the environment, or a breach of confidentiality, integrity, and/or availability of/to monitored critical systems, and/or priority accounts leading to a critical security incident
2	High	30 Minutes	24/7	Response within 30 minutes of received Security Alerts or notifications indicating a probable policy breach or major impact to confidentiality, integrity, and/or availability of monitored systems and accounts.
3	Medium	2 Hours	24/7	Response within 2 hours of receiving Security Alerts or notifications indicating a suspected policy breach or significant impact to confidentiality, integrity, and/or availability of monitored systems and accounts.

4	Low	4 Hours	Standard Business Hours	Response within 4 hours of receiving Security Alerts or notifications indicating a potential policy breach or minor impact to confidentiality, integrity, and/or availability of monitored systems and accounts.
5	Informational	8 Hours	Standard Business Hours	Response within 8 hours of receiving Security Alerts or notifications indicating a noteworthy event that could highlight anomalous behaviour for further investigation but does not pose any immediate threat.

PART C – SERVICE CONDITIONS

1. 1 The iCE – Incident Management Handling and Response is based on a minimum 12-month term

1. 2 Threat workshop is a prerequisite for scoping and determining which log sources will be ingested

1. 3 A one-off implementation charge applies for the discovery and onboarding phase.

1. 4 Fixed monthly recurring charges will commence no later than 45 calendar days after the start of the discovery and onboarding phase.

1. 5 We make no guarantees or warranties that the service will correctly detect and identify all:

   (a) Security Events or Incidents

   (b) Instances of unauthorised access to your network

   (c) Malware

   (d) Exploits or

   (e) Other types of attacks or issues.

1. 6 Incident response that takes over 2 hours of dedicated resource activity is chargeable on a T&M base. Time is based on work activity Early termination charges apply

1. 7 All necessary access controls will be provided

1. 8 Access to your physical offices will be provided as required

1. 9 The engagement will commence at a mutually convenient time

1. 10 You will provide the access required to establish and maintain the service

1. 11 You will provide remote access to information and communication capabilities

1. 12 You will make available any required system or information

1. 13 You will inform (or authorise us to inform) all relevant parties of the activities being carried out by DEFEND under your authorisation, including any key third parties

1. 14 You will provide resources to support the discovery and onboarding phase and on-going improvement of the service

1. 15 You will provide the necessary business context and confirmation of activities outside the scope of our level of visibility and privileges

1. 16 You will provide access to the relevant resources and materials to enable completion of the deliverables of the service

1. 17 You will take responsibility for raising support requests with Microsoft for any issues with deployed resources within the subscription being used, including Sentinel and Log Analytics

1. 18 Travel and disbursements will be agreed prior and charged at cost if required.