MASTER SERVICES AGREEMENT

SERVICE DESCRIPTION

SERVICE DESCRIPTION: DEFEND ICE – SHERLOCK THREAT MANAGEMENT

PART A – DESCRIPTION

SHERLOCK Threat Management, a module of DEFEND iCE (intelligent Cybersecurity Ecosystem), provides an integration of the New Zealand National Cyber Security Centre's (NCSC's) Malware Free Networks (MFN) and CERT NZ's Phishing Disruption Service (PDS) threat intelligence feeds with your supported security technologies allowing you to receive and make use of highly curated threat intelligence, relevant to New Zealand's most critical organisations.

The SHERLOCK Threat Management platform is deployed for you to manage the threat feeds from external partners such as the NCSC and CERT NZ to task the Indications of Compromise (IoC's) into your security technologies and to collect the telemetry associated with the sightings.

SHERLOCK is provided to you by DEFEND Limited, as subcontractor for One New Zealand, and is a monthly subscription-based service.

PART B – OPTIONS & INCLUSIONS

INCLUSIONS	
IoC tasking into Security Platforms	DEFEND will deploy specific capability to enable IoCs to be tasked into identified security platforms, allowing the platform to utilise them to enhance the overall cybersecurity posture of your organisation.
Security Platform Configuration	DEFEND will configure, or assist with configuring (depending on the security platform) rules, analytics, or policies to ensure the security platform can take advantage of the IoCs provided by SHERLOCK Threat Management.
IoC Telemetry Return	Enablement of basic or expanded telemetry return (see options) to the NCSC to further enhance the overall MFN service.
OPTIONS	
Critical Threat Protection	Critical Threat Protection enables the MFN and PDS threat feeds to be used in conjunction with Microsoft Sentinel playbooks with automation rules, to identify if any IoCs are accessed in your environment and create alerts as required, and task the IoC's into Defender for Endpoint (where available), blocking access to the URL based IoC's in the Microsoft Edge browser for proactive protection.
Enhanced Threat Protection	Enhanced Threat Protection extends the ability to task IoCs into the following technologies to proactively disrupt threats across your environment: • Palo Alto Networks Firewalls • Palo Alto Networks Prisma Access • Fortinet Firewalls • Zscaler Internet Access • Domain Name Servers
Quarterly Threat Intelligence Report (Enhanced Threat Protection only)	Threat Intelligence report presenting an analysis of the cyber threats against your industry and region, based on DEFEND's own threat intelligence research supported by both public and closed threat intelligence sources.

MFN Consenting Customer Agreement	If you sign the Malware Free Networks Consenting Customer Agreement with NCSC, you will be authorising the collecting and passing of telemetry information to NCSC which identifies your organisation
MFN Expanded Telemetry (Consenting customers only)	The MFN Expanded telemetry integrates a customer identifier, which may be an IP address, with the IoC block, date and time. Depending on the service integration, this may include source and destination ports and protocols.

PART C – SERVICE CONDITIONS

1. 1 The iCE – SHERLOCK Threat Management Service is based on a minimum 12-month term

1. 2 Fixed monthly recurring charges will commence no later than 45 calendar days after the start of implementation.

1. 3 There may be a one-off charge for implementation.

1. 4 Early termination charges apply.

1. 5 We make no guarantees or warranties that the Service will correctly respond and remediate:

1. 6 Security Events or Incidents:

(a) Instances of unauthorised access to your network

(b) Malware

(c) Exploits or

(d) Other types of attacks or issues.

1. 7 Access to your physical offices will be provided as required

1. 8 The engagement will commence at a mutually convenient time

1. 9 You will provide the access required to establish and maintain the Service

1. 10 You will provide remote access to information and communication capabilities

1. 11 You will make available any required system or information

1. 12 You will provide resources to support implementation of and ongoing improvement of the Service

1. 13 You will provide access to the relevant resources and materials to enable completion of the deliverables of the Service

1. 14 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. 15 Travel and disbursements will be agreed prior and charged at cost if required.