



DEFEND Guardian XDR for Enterprise

Managed Security Operations

The success of a security operations service depends on the ability of the service partner to understand organisational context, what assets are important to the organisation, the resultant threats and likelihood of those threats eventuating.

This is really where most operational outsources fail – the contract starts in the wrong place, with unclear expectations and the team never quite gains the level of business context needed to be effective. Security operations are best blended – combining specialist technical skillsets and know how (external), with organisation knowledge and context (internal).

With that in mind we propose our “Guardian XDR for Enterprise” service.

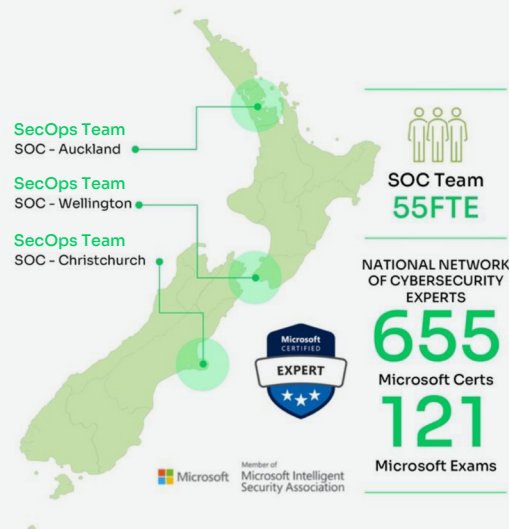
DEFEND works in partnership with its customers, essentially becoming an extension of your existing security team. DEFEND’s customers find this approach delivers better outcomes as this not only improves the cybersecurity posture within you but achieves shared knowledge via security operations manual that we work on together.

As we embed into your team, we will quickly demonstrate our value and how we collectively identify and respond to incidents through proactively tuning your environment in alignment to the enablement of existing operating policies and frameworks. DEFEND provide best of breed Security Operations to New Zealand government entities and organisations of national significance.

Our service offering comprises of three core functions – Incident Management, Handling & Response, Advanced Incident Response and SHERLOCK Threat Protection. At its core we utilise the Microsoft Unified Security Operations platform which integrates both Defender XDR for and Microsoft Sentinel.

DEFEND Guardian XDR for Enterprise Managed Security Operations

- > Fully remote working enabled = 24 x 7 x 365 Support
- > Award winning, globally recognised
- > Current portfolio of 55+ leading/ nationally significant NZ organisations across public & private sector
- > Track Record – All clients are referenceable



DEFEND Guardian XDR for Enterprise Service Modules

DEFEND Guardian XDR for Enterprise modular services that embed, complement and strengthen your existing capability. It delivers real time monitoring, correlation and expert analysis of activity.

DEFEND Guardian XDR for Enterprise provides the flexibility you require in delivering successful security operations.

- > **Incident Management, Handling & Response**
24x7x365 proactive tuning, monitoring, and responding to alerts and incidents.
- > **Advanced Incident Response**
Escalation of any major incidents to our skilled response team to manage and coordinate response activities end to end for you.
- > **SHERLOCK Threat Management**
Provided by our SHERLOCK Threat Management platform, this module protects you from threats targeting New Zealand organisations by utilising the NCSC's Malware Free Networks® (MFN®) and Phishing Disruption Service (PDS) threat intelligence feeds.



Detect

Flexible

Works with your existing technology landscape to maximise your return on investment and operational effectiveness.

Available

24x7x365 monitoring of security alerts. We triage these alerts to determine if response or tuning is required.

Proactive

We perform threat hunting and are armed with Sherlock Threat management to identify abnormal behaviours, indicators of compromise, and potential threats beyond standard alerts.



Protect

Visible

Weekly health check reports provide activity insights and progress via seamless and constant communication.

Optimise

Our analysts fine tune logging, alerting and incident identification continually optimising your environment.

Improve

We provide status updates on continuous improvement actions, adoption of new capability, and work with you to ensure that you receive the best possible service that adapts with your business.



Respond

Escalate

24x7 senior response provided for any incident escalations. Giving you a safe pair of hands to rely upon.

Investigate

Rapid investigation, analysis and containment is provided by our senior responders ensuring eradication is achieved.

Remediate

We support ongoing recovery steps and perform remediation to improve control effectiveness and posture hardening, reducing risk.

Services Overview

Incident Management, Handling & Response

The key features of Incident Management, Handling and Response are:

Feature	Description
Security Event Monitoring	We will monitor all incoming security alerts to Sentinel that are generated by Defender or other log sources according to the specified incident response SLA.
Security Event Triage and Analysis	We triage events received via incoming security alerts and those logged by the customer in the DEFEND service management portal, or directly via our 0800 2 DEFEND phone number. The events will be reviewed, contextualising them within the system and determining if they are an incident requiring response and remediation activities or an event which we can look to tune out where appropriate.
Security Incident Response and Remediation	We will respond to security alerts based on their priority and provide updates when incidents are closed. Where an incident is deemed a high priority, additional incident communications and escalation will be provided. Our engineers will manage the incident response process and engage with you to prioritise implementation and remediation.
Threat Hunting	We will perform proactive threat hunting activities within the Defender Portal which would allow for the identification of 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 following any verified incidents.
Microsoft Defender Threat Detection Optimisation and Alert Tuning	Microsoft Defender Threat detection policies and alert tuning configuration are used to fine tune logging, alerting and incident identification against the agreed threat scenarios that are aligned and relevant to your business. Alert tuning covers the analysis and investigation, including event correlation to ensure that security alerts which are tuned out are done so in a structured manner to ensure no loss of visibility. Further improvements may be related to automating incident response where defined repeatable actions need to be undertaken.
Continuous Improvement	Improvements that are identified through activities such as tuning and optimisation or through incident response will be assessed based on complexity and effort to implement. Where these activities fall under the scope of alert tuning or threat detection policy configuration, these will be implemented as part of the service. Improvements not meeting these criteria will be surfaced to you for review and approval through our regular engagement meetings. These can be implemented as Standard Service Requests, or under T&M or a Statement of Work depending on effort required.
Reporting	Reporting will be created and provided by our cybersecurity engineers on both a weekly and monthly basis. Weekly health check reports will provide a summary of items like BAU coverage and ticket handling numbers, as well as any outstanding items awaiting attention. Monthly Dashboard reports will provide a summary of items like 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 for advanced incident response to highlight a timeline, summary of activities, remediation activities and recommendations, and any lessons learnt.
Meetings	A regular cadence (fortnightly initially, can be reassessed once processes, familiarity, and rapport are well established and practiced) security operations meeting will be scheduled between our team and your operations representatives, with an agenda 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.

Service Scope

We are responsible for the ongoing operational management of your Azure subscription and Sentinel instance (where the subscription being used is provisioned solely for the purposes of hosting the managed Sentinel instance), and certain configuration within Defender XDR related to threat detection and alert tuning. This includes:

- > Configuration and management of workbooks, runbooks, analytics rules and logic apps for in-scope source systems
- > Configuration of the underlying Log Analytics workspace, including retention parameters.
- > Configuration and management of Sentinel connectors to source systems.
- > Detection and alerting policies of in-scope Microsoft Defender workloads.

All other configuration of source systems is the responsibility of the customer.

Operational ownership and management of source systems remain your responsibility and are not included in scope. Additional connectors and log or event ingestion, which are not specified above, such as events forwarded via Syslog can be considered for support but are subject to additional cost or price variation based on support and onboarding requirements. We can of course help to guide and advise your team, and our Security Capability Management module is designed to offer this support should you wish additional ongoing support.

Service Management – Incident Notification & Response

Incidents within Microsoft Sentinel will be sent to our service management system to allow for notification to our team. Representatives specified by you will be provided access to our service management portal, allowing for direct creation of incidents in the system if required. The mechanism, process, and conditions for this will be developed as part of service establishment.

Specified representatives can also raise incidents directly with our team by calling 0800 2 DEFEND (0800 233 3363). We recommend that in the event of a suspected major breach or incident that you notify us directly by calling 0800 2 DEFEND.

Response Hours: We will respond to incidents according to the below table:

Task	Coverage
Incident Response – Sentinel High & Medium severity	24x7x365
Incident Response – Customer initiated Severity 1-3 incidents	24x7x365
Incident Response – Sentinel Low & Informational severity	Business Hours
Incident Response – Customer initiated Severity 4+ incidents	Business Hours

*Standard business hours are defined as 08:30-17:00, Monday to Friday in local New Zealand time zone, taking into consideration adjustments for daylight savings. Business hours also exclude recognised NZ national public holidays.

Included Response Allowance:

Type	Incident Retainer	Support cap
Incidents	2 hours per incident*	While this is uncapped, a fair use condition does apply. We will work with you to identify the cause for high alert volumes and ensure additional tuning is performed at source to reduce alert volumes in the first instance, followed by development/improvement of Sentinel Analytics.
Major Incidents	Time & Materials	This is uncapped and once the two hours are consumed and when a major incident is declared we will seek your approval to support and if required manage the major incident for you.

*2 hours per incident includes triage time and is the total cumulative effort spent of the team in responding to the incident.

Service Requests

Your nominated contacts can engage our team via agreed methods to log service requests in relation to the service provided to you. Service requests are categorised according to the below table:

Priority	Response Time	Support Hours	Definition
Standard Request	8 Hours	Business Hours	Standard configuration tasks taking less than 2 hours to complete. Can be pre-approved
Urgent Request	2 Hours	24/7/365	High priority standard changes that are not part of an active incident. Fair use policy applies. Time spent responding to urgent requests will incur a fee.
Major Request	2 Days	Business Hours	Complex configuration tasks requiring specific approval. Can often result in an independent project, SoW (Statement of Work) or Work Order.

Service Requests may arise at the suggestion of configuration changes from our team for the supporting services or platforms providing data to Sentinel. These requests will be submitted to you, to be implemented following your change management process. We can of course assist you and provide skilled specialists to help make changes in your environment.

Our team will continually look to improve the service through tuning and optimisation activities within Sentinel. Generally, minor tuning is performed, and we will advise you either in the next weekly report, or the next fortnightly meeting.

Standard Service Requests are included in the service and are subject to a fair use condition. Additional work will be performed on a T&M basis once approved by you.

We recommend that anything which requires the immediate attention of our team is raised by calling the 0800 2 DEFEND number.

Grey Area Support

We recognise that the root cause of technology problems or issues cannot always be immediately identified. It may be hard to identify if an issue is security or technology related. We will work in good faith with you and your other support partners to help triage and investigate issues until they can be identified as either being security related or outside of our area. Fair use policy applies to this, and we will reach out and advise you if the effort is putting our ability to deliver the wider service at risk.

Fair Use

Fair use is defined as a reasonable volume of incidents or requests based on industry benchmarks and DEFEND's experience with organisations of comparable size and digital footprint. Accordingly, the service is designed to accommodate volumes within these ranges.

Should the number of incidents or requests consistently exceed this benchmark, despite reasonable attempts in consultation with you to identify and resolve the root cause of the excessive volume, DEFEND reserve the right to review the terms and pricing of the service and may, after providing you with 60 days written notice, adjust the terms and pricing to provide for the additional resourcing required.

Service Level Target

We aim to respond to incidents generated in Sentinel within agreed SLA targets, 100% of the time, however our ability to respond is limited by availability of the services used to provide this overall service.

Specifically, we operate two separate notification systems to enable us to continue to direct alerts to responders when they occur in your environment, however Microsoft Log Analytics and Microsoft Sentinel are provided by Microsoft with a 99.9% Uptime SLA. Any outage or incident affecting availability of these services will impact our ability to meet this target.

For the avoidance of doubt, the timestamp of when an alert or incident is generated in Sentinel will be used as T=0 when calculating response time for an incident.

Incident Response Targets

The following table specifies incident severity mapping, response times and support hours:

DEFEND ITSM Severity	Sentinel Severity	Response Time	Support Hours	Definition
1	N/A – raised only after triage and validation	Based on originating Sentinel Incident Severity	24/7/365	Escalation within 30 minutes of triaged and validated security alert or notification indicating an uncontained and active threat within the environment, or a major 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	24/7/365	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	24/7/365	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 which could highlight anomalous behaviour for further investigation but does not pose any immediate threat.

As part of service onboarding, and the process of formalising our service processes, we will ensure alignment between our incident severity and your internal incident severity or priority classifications.

Security Operations Meetings

A regular (usually fortnightly) security operations meeting will be scheduled with DEFEND cybersecurity engineers and your key security stakeholders, and consist of the following items:

- > Status update on continuous improvement actions
- > Review and update of any operational processes if required
- > Roadmap around other log sources for ingestion and expansion of security coverage

Reporting

Reporting will be created and provided by DEFEND cybersecurity engineers to the customer on both a weekly and monthly basis. This reporting will take the form of both a written management overview report and implementation of our Security Operations Monthly Report Workbook dashboard in Sentinel for near-real time oversight reporting, for relevant/agreed management stakeholders.

- > Monthly Reports will be provided to the customer within 5 business days from the 1st of the month.
- > Weekly health checks will provide a summary of items like BAU check coverage, and ticket handling numbers.
- > Monthly dashboards will provide a summary of items including alert, incident, and near miss handling numbers, status of continuous improvement actions, and any other relevant content.
- > Post Incident reports will provide a summary of activities that occurred during a high priority incident, remediations activities, and lessons learnt.



Figure 1: Example Reporting(s) [customisable]

Advanced Incident Response

This service integrates into your existing operational environment and Major Incident Management (MIM) processes and provides a seamless escalation and transition point from daily Incident Management as provided by 24/7 Managed Extended Detection & Response, to dealing with major cybersecurity incidents. This is achieved through direct integration of DEFEND's resources into your incident and major incident management (MIM) processes, providing responsive support for major security incidents, as required.

The service supports the following key activities:

Description	Benefit
24/7 Response	Senior Responders available for any incident escalations. We have skilled responders across New Zealand and while most organisations are now geared for remote response, it is sometimes still valuable and necessary to go onsite. Our service target is that within 30 minutes of calling, our customers are engaged by a senior responder that will provide direction and leadership. We achieve this through rapid triage and escalation through our 24x7 team.
Management & Coordination	Support of your existing process including rapid investigation and containment, as required.
Communications & Updates	Supporting establishment of incident communications (e.g. war rooms) and providing regular updates to technical and senior stakeholders as required.
Detailed Investigation & Analysis	Leveraging existing customer technologies for investigation or deploying specialist technologies as required.
Stakeholder Coordination	Liaising with internal technical and senior stakeholders to ensure a coordinated and managed response.
Expert Technical Leadership & Surveillance	Support ongoing MIM investigation and recovery activities including the deployment of additional monitoring tools and providing ongoing surveillance to ensure eradication is achieved.
Recovery & Reporting	Supporting ongoing recovery steps including providing detailed reports and analysis for review and improvement.

SHERLOCK Threat Management

To provide Threat Protection to customers, we utilise two functions from our SHERLOCK Advanced Threat Management¹ product offering. These are Critical Threat Protection and Enhanced Threat Protection. These functions enable the integration of NCSC NZ Malware Free Networks[®] (MFN[®]) and Phishing Disruption Service (PDS) threat intelligence into your Microsoft Sentinel instance, Defender for Endpoint and other security controls such as firewalls and DNS allowing you to ingest highly curated threat intelligence relevant to New Zealand's most critical organisations and proactively disrupt threats within your environment.

Function	Description
SHERLOCK Critical Threat Protection	Critical Threat Protection leverages your Microsoft Sentinel and/or Microsoft Defender for Endpoint deployment(s) to provide visibility, alerting and disruption of indicators from the MFN [®] and PDS threat intelligence feeds.
SHERLOCK Enhanced Threat Protection	Enhanced Threat Protection extends this disruption capability to the following capabilities you may have in your environment: Palo Alto Networks Firewalls & Prisma Access, Fortinet Firewalls, Zscaler, and DNS. In addition, you get the benefit of quarterly threat intelligence reports tailored to your organisation, based on DEFEND's own threat intelligence research supported by both public and closed threat intelligence sources.

¹ Comprehensive threat management capabilities and managed services to manage the lifecycle of external and internal threats end-to-end are available to customers of SHERLOCK Advanced Threat Management. This includes Threat Landscape Monitoring, Exposure Management and Threat & Attack Simulation.