Service Definition – Managed Sentinel SOC

Date of Issue: 08/09/2025

Managed Sentinel SOC

Overview

SIEM platform.

The Active Response service is designed for customers who have a small Security team but want the assurance provided by an experienced team of SOC analysts monitoring their SIEM who have the knowledge and tooling to understand the current and evolving threat landscape and how this could impact their organisation's business systems.

The Phoenix Protect - Active Response Managed Security Service is 24x7x365 support coverage.

Service Onboarding

Service onboarding includes setting up and provisioning access to the service portals, scheduling of reports and service kick off call, including walk through of the tools and service. Onboarding activities can typically take up to 4 weeks.

Activity	Description	Service Hours
Design workshop	will establish in detail where key Microsoft Sentinel components will reside within the organisation's network and the logging levels that can be achieved. This will include what it will ingest and how this will be achieved, for example Data Connectors, additional log servers, customer ingestions or parsers. A service design document will be created to capture this information, with acceptance criteria which is then shared for customer review and signoff. This will form part of the Requirements Document.	Normal Business Hours
Deployment of Sentinel	The SOC will deploy Sentinel in the customer's Azure subscription and configure it in accordance with the design created during the design workshop. The SOC will also deploy all agreed connectors for log ingestion and test their functionality.	Normal Business Hours
Onboarding to Microsoft Azure Lighthouse	The SOC will work with the customer to enrol their Sentinel deployment into the Lighthouse deployment. This is the tool used to create the multi-tenant monitoring and investigation capabilities required to deliver the Managed Service.	Normal Business Hours
Data Connector Onboarding	A Data Connector is the native method for Microsoft Sentinel to receive logs from security solutions and devices. These are direct RESTful APIs that can instantly ingest logs and output results within Analytical Rules, Workbooks, Hunting Queries, and Playbooks. Connectors available in the Microsoft Sentinel Content Hub or under Data Connectors are defined as Standard Connectors with respect to the Managed Service. Customers can have an unlimited number of Data Connectors categorised as Standard Connectors installed and configured in their Sentinel instance during the onboarding of their service, and up to three Standard Connectors added per year during the service contract term as described in the Service Tiers matrix.	Normal Business Hours
Transition into service	On completion of the deployment phase, the Sentinel implementation will be transitioned to a live Managed Service. At this stage alert data is being captured from the customer's environment and is monitored and triaged by the SOC.	Normal Business Hours
Baseline and Tuning	Once alert data is being captured, the SOC will deploy the current standard "base line" analytics rule set. Working in collaboration with the customer, the SOC will perform a period of tuning where alerts are captured and discussed to understand the reasons the alerts triggered, and which alerts	24 x 7

	should be categorised as false positives or genuine alerts that are potential threats. The tuning phase will typically be completed over a period of one to two weeks and on completion the Managed Service will be in BAU support.	

Tasks and Responsibilities

Activity	Bytes	Customer
Design workshop	X	X
Deployment of Sentinel	X	X
Onboarding to Microsoft Azure Lighthouse	X	X
Data Connector Onboarding	X	X
Transition into service	X	X
Baseline and Tuning	X	X

Data Connectors

Activity	Description	Service Hours
Standard Data Connector Ingestion Source Onboarding	Additional data sources can be added to the customers Sentinel configuration at their request at any point during the service contract where a Standard Data Connector exists in the sentinel library for example a new firewall or security product. Customers are entitled to three additional Standard Data Connector ingestion sources per contract year once their service has transitioned into BAU support	Normal Business Hours
Custom Data Connector Ingestion Source Onboarding	Data sources for which a Standard Data Connector does not exist in Sentinel may have a Custom Data Connector developed subject to a scoping exercise to establish if it is technically possible and to determine the effort required. In the event of a Custom Data Connector being required, a SoW will be generated for the delivery of the requirement. The Custom Data Connector is subject to an additional cost.	Normal Business Hours

Tasks and Responsibilities

Activity	Bytes	Customer
Standard Data Connector Ingestion Source Onboarding	X	
Custom Data Connector Ingestion Source Onboarding	X	

Sentinel Platform

Activity	Description	Service Hours
Sentinel Proactive Platform Management	Proactive management of the customers Microsoft Sentinel SIEM instance, including any maintenance of its core components are part of the Managed Service.	24 x 7
Sentinel Health Checks	A detailed health check is conducted every 6 months.	Normal Business Hours

Tasks and Responsibilities

Activity	Bytes	Customer
Sentinel Proactive Platform Management	X	
Sentinel Health Checks	X	

Security Monitoring

Activity	Description	Service Hours
Security Monitoring and Alerting	The SOC will continuously monitor the customers environment using the Microsoft Sentinel instance, which will be enhanced with regular updated to Threat Indicators using rich Threat Intelligence sources to rapidly reflect latest threats promptly after such threats have been identified	24 x 7
Security Advice and Guidance	When a security incident is discovered by the SOC team or triggered by the Sentinel instances capabilities, the SOC team will alert in accordance with Service Levels, to provide context and advice to enable a resolution.	24 x 7
Security Bulletins	The SOC will provide security bulletins to all Managed Service customers as appropriate to promptly update customers on the latest threats and vulnerabilities. Bulletins will contain information about new threats & vulnerabilities being reported	Normal Business Hours

Tasks and Responsibilities

Activity	Bytes	Customer
Security Monitoring and Alerting	X	
Security Advice and Guidance	X	
Security Bulletins	X	

Rule Management

Activity	Description	Service Hours
Rule Management	Analytical rules within the Sentinel SIEM platform require regular management and maintenance. The SOC will proactively make amendments to tune existing rules and create new automated rules using the SOCs extensive use case library to ensure that the new and emerging threats are being constantly monitored and alerted on.	24 x 7
Custom Rules per Quarter	Custom rules can be required where existing data sources are altered for any reason, and the rule is needed to detect the change and to continue alerting for new security threats. When the SOC receives a new data feed into the SIEM, it is strongly recommended that Custom Rules are created to make the most effective use of the information provided by this ingested data. The SOC will provide advice and make recommendations for the creation of Customer Rules to customers, who can then discuss the requirements with the SOC and agree the rule creation as appropriate.	Normal Business Hours
Custom Workbooks per Quarter	Workbooks are a form of customisable dashboard used in Microsoft Sentinel to monitor and visualise SIEM output data. The SOC can create Custom Workbooks to address any specific needs and any requirements for each customer that are not met by the Workbooks available natively.	Normal Business Hours

Tasks and Responsibilities

Activity	Bytes	Customer
Rule Management	X	
Custom Rules per Quarter	X	
Custom Workbooks per Quarter	X	

Service Governance

Activity	Description	Service Hours
Escalation to Microsoft for platform issues	Escalation to Microsoft for Azure platform or Sentinel related issues are included with the service. Customers can request escalation, and the SOC will escalate to Microsoft on a customer's behalf to resolve incidents or where escalations are otherwise reasonably required.	24 x 7
Regular Technical Reviews	For customers taking on the service, the SOC will arrange regular technical review meetings that will be scheduled and conducted using Microsoft Teams and will include representatives from the customers technical team, and representatives from the SOC that are actively involved in	Normal Business Hours

	deliver of the service to said customer. The purpose of these meetings is to discuss service performance with the technical audience, and they will be scheduled separately to regular service reviews that are led by the assigned Customer Success Manager.	
Root Cause Analysis	Root Cause Analysis can be undertaken by but a successful outcome is not a guarantee of this Service. Sometimes there is simply not enough information available to explain why an incident occurred. SOC analysts will provide guidance based on their experience and other information at hand, but a full Root Cause Analysis will not be possible without supporting evidence.	24 x 7
Authorised Named Contacts	To enhance customer security, the SOC maintain a list of customer Authorised Named Contacts. This is a list of customer employees and their contact details who are authorised to use the Managed Service by raising support tickets, incidents and change requests on behalf of the customer organisation. It is the customer's responsibility to ensure this list is kept up to date, for example when a member of staff leaves the organisation. Changes to the Authorised Named Contacts list can be made by customers as required by logging a change request with the IT Service Desk. A copy of the current list can be requested at any time. Only Authorised Named Contacts from a customer organisation can log tickets against the Managed Service.	24 x 7
Customer Success manager	All Managed Service customers are assigned a Customer Success Manager to help ensure they get the maximum value from their Managed Service.	Normal Business Hours
Service Management Reviews	Regular service reviews are delivered by the assigned Customer Success Manager. Regular reviews are scheduled during the onboarding period to ensure the SOC assist with embedding the service within customers organisations at 30-, 60- and 90-days post onboarding commencement. Following this, service reviews will be conducted on a quarterly basis, enabling customers to review the service performance.	Normal Business Hours
Service Reporting Dashboard	Access is provided to the Managed Services Dashboard to monitor the contract details, lifecycle. Customers will have access to the Reporting Dashboard. This Executive Summary dashboard gives customers a high-level view of contract details and service performance including SLA achievement, usage, and performance trends. The Reporting Dashboard can be accessed from the Portal, for which customers are provided with access details during the onboarding of their Managed Service. Protect Managed Security Service customers can also access the reports and dashboards available within their Sentinel instance.	24 x 7

Activity	Bytes	Customer
Escalation to Microsoft for platform issues	X	
Regular Technical Reviews	X	
Root Cause Analysis	X	
Authorised Named Contacts	X	X
Customer Success manager	X	
Service Management Reviews	X	X
Service Reporting Dashboard	X	

Incident Management SLAs

Service Level Agreements are in place for incident, change and request management and are only applicable within the contracted support hours.

Service Performance is available for the customer to monitor through access to the Service Reporting Dashboard. Performance will also be reviewed at Managed Service Customer Reviews.

SLA response times relate to the time it will take for a member of the SOC to respond to a customer support ticket or to notify the Customer of any incident identified. Response times apply to Support Hours only.

The SOC cannot commit to resolution time SLAs in respect of Security Incidents as there may be components beyond their control including, but not limited to, access to customer personnel and systems or issues relating to a cloud platform. The SLA KPI clock will be paused when a response is required from the customer to progress the ticket.

Any tickets from the customer which are not logged through the correct channels will be exempt from all SLAs until it is logged correctly through the Portal, via email or by using the SOC telephone number.

If the SOC becomes aware that a ticket has been logged incorrectly, it shall inform the customer as soon as reasonably practicable.

The SOC will manage all escalations to Microsoft with incidents that require escalation to Microsoft being exempt from SLAs and KPIs and shall ensure that escalations are followed up with Microsoft at appropriate intervals to ensure a timely resolution.

The SOC will update the customer as frequently as necessary and at least as frequently as outlined in the SLA table below.

Major Incidents will be subject to regular communication between SOC and the customer until the issue is resolved or impact mitigated to a point where the severity can be downgraded.

In the case of a Major incident, for example a current active attack, the SOC will promptly advise and respond to questions from the customer until the issue is resolved or the impact mitigated to a point where the severity can be downgraded (within contracted Support Hours).

The Inform service is an automated information service only with alerts delivered immediately without further triage, and as such SLAs are not included for customers taking the Inform service.

In respect of Service Incidents:

(i) The SOC shall use all reasonable endeavours to resolve P1 and P2 incidents as soon as reasonably practicable respectively of the earlier of becoming aware of the Service Incident by its Staff or the logging of the Service Incident by the customer;

(ii) The SOC shall use reasonable endeavours to resolve P3 incidents in a timely manner and in accordance with any reasonable requests and timeframes of the customer, taking account of the nature and urgency of the request; and

(iii) The SOC shall use reasonable endeavours to resolve P4 incidents in a timely manner and in accordance with any reasonable timeframes requested by the customer, taking account of the nature and urgency of the request.

Support Incidents

Priority Level	Priority Definition	Bytes Target Response Time
1	**Urgent/Major Incident** Severe business impact, whole business affected. Major Incident management invocation.	30 Minutes
2	**High** High probability that a resource is compromised, there is a high confidence in both the malicious intent and in the findings used to issue the alert. For example, an alert that detects the execution of a malicious tool.	30 Minutes
3	**Normal** Suspicious activity that may indicate a resource is compromised. Confidence in the analytic or finding is a medium, and the confidence of the malicious intent is medium to high. These would usually be machine learning or anomaly-based detections. For example, a sign-in attempt from an anomalous location.	4 Hours
4	**Low** This might be a benign positive or a blocked attack. Not enough evidence to suggest the intent is malicious and the activity might be innocent. For example, log clear is an action that might happen when an attacker tries to hide their tracks, but in many cases is a routine operation performed by admins	24 Hours

Service Requests

The following table provides guidance on how Service Incidents (Requests) including questions and requests by the customer, are categorised. Change requests are categorised differently and are set out further below. The severity category is associated with an appropriate Response Sla as described.

Priority Level	Priority Definition	Response Time SLA
1	**Urgent** The Service or a substantial part of it (including any systems or software used to provide the service has stopped working such that there is a severe business impact, the whole business is affected or there is a material impact to the Services, or a substantial part of the Service can no longer be provided. Major Incident management invocation will occur as a result of a P1 incident.	30 Minutes
2	**High** The Service, or a material part of it (including any systems or software used to provide the Services) has stopped working, such that a whole or material business, team or function (whether in the SOC or with the customer) is affected or there is an adverse impact to the provision or receipt of the Services (or any part of it) which is material in any respect.	30 Minutes
3	**Normal** Something is not working, one person or team is affected (whether in the SOC or with the customer), a workaround is available. No material impact to any business, team or function of the Service.	2 Hours
4	**Low** A question or basic request about how to do something.	24 Hours

Escalation Contacts

Escalation Level	Name	Contact Details	Available Hours
1	Security Operations Centre Manager	Assigned Support Engineer on Active Support Ticket	Support Hours

2	Customer Success Manager	Assigned Support Team Lead on Active Support Ticket	Support Hours
3	Head of Service Delivery	Assigned Service Delivery Manager via email	Core Business Hours
4	Director of Managed Services	Contact details provided during onboarding	Core Business Hours

Hours of Support Service

Support Cycle	Service Desk Available	Operating Times
Core Business Hours	Yes	Weekdays, excluding bank holidays, 0800 to 1800
After Hours (Weekdays)	Yes	Weekdays, excluding bank holidays, 1801 to 0759
Out of Hours (Weekends & Bank Holidays)	Yes	Anytime Weekends & Bank Holidays

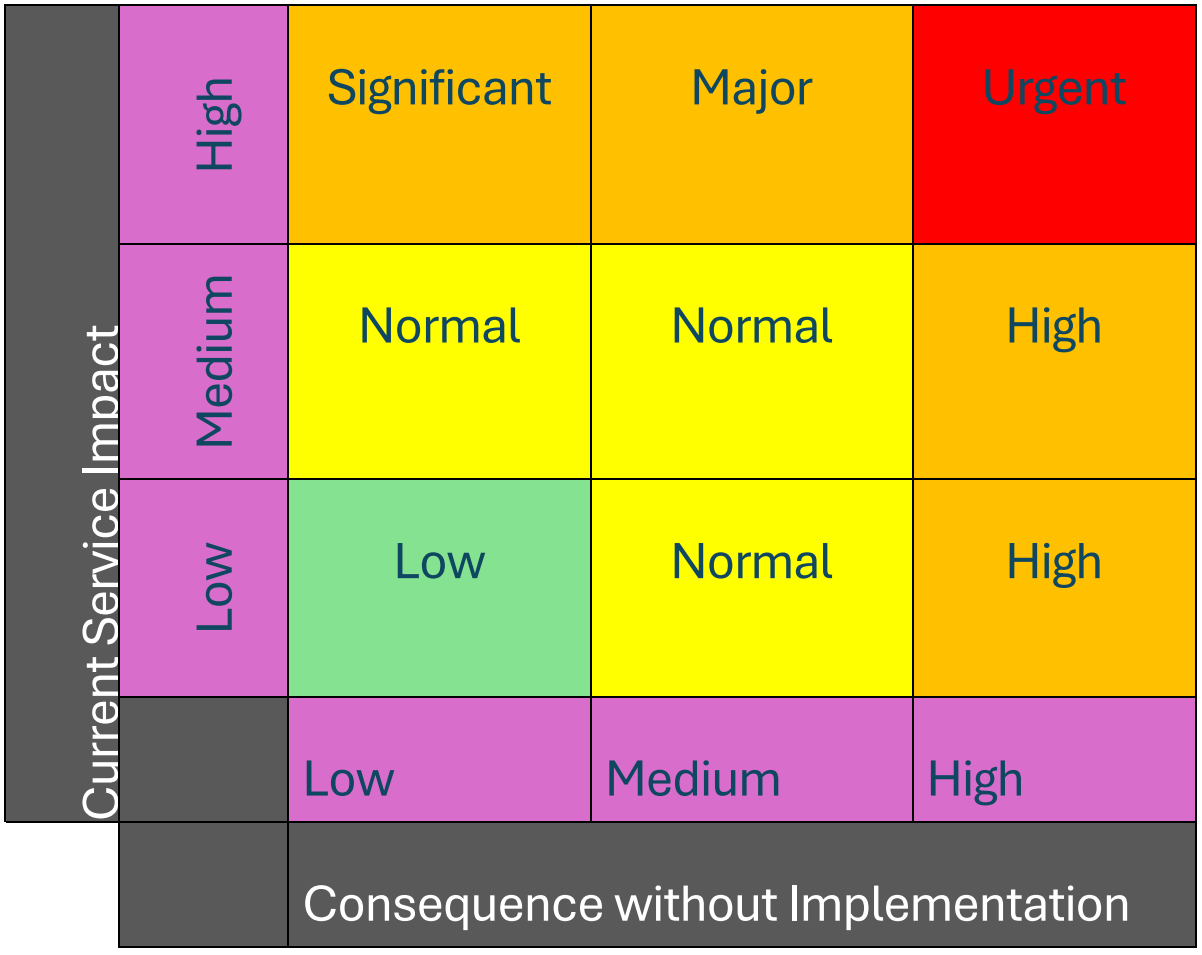
Change Management SLAs

Change management seeks to minimise the risk associated with Changes. A change is defined as “the addition, modification or removal of anything that could have an effect on the functionality or availability of the customers Sentinel platform or managed service”.
Change requests can only be logged or approved by Authorised Named Contacts from the customer organisation. Change requests tickets raised on behalf of the customer are sent to the Authorised Named Contact for change approval. The customer contact is responsible for seeking approval from the relevant change authority within the customer organisation before changes are implemented. If a customer has a Change Advisory Board (or equivalent) a representation from the SOC can be provided when enough notice is given, and the request is able to be accommodated.
Requests for change will be categorised by severity to prioritise tickets based on impact or potential impact if the change is not to be implemented. The following table provides guidance on how requests for change are categorised. Requests logged will be given a default priority of “normal”, these will then be assessed and categorised based on the information available in the ticket. As much detail should be provided on the requests for change including current service impact and consequence of the change not being implemented. Change request tickets that are not responded to will be closed after three consecutive attempts to contact the customer. Attempts to make contact will take place at least once within a 24-hour period but will not occur more than once per calendar day. Tickets can be “paused” for a finite period if the customer provides guidance on when they will be able to respond.

Consequence without Implementation	Description
Low	No or limited impact to customer IT operations if change not implemented within 30 days
Normal	Will have a significant impact to customer IT operations which will affect the organisation, a

	department, business unit or function if not implemented within 30 days
High	Significant to customer IT operations could occur immediately which will affect the organisation, a department, business unit or function if change not implemented as soon as possible.

Current Service Impact	Description
Low	No impact or limited impact.
Normal	Something is not working and its slowing you down, more than one person or team affected.
High	A major service has stopped working, whole business, team or function affected,



Change Implementation Schedule

Severity	Standard Request Response Target (hours)	Implementation Target (days)
Low	24	10
Normal	4	5
High	2	2
Urgent	2	1

Exclusions

- Technical support for implementation or project work which has not been completed successfully. A professional services engagement would be advisable for this type of activity.
- Technical support relating to development or coding.
- Environment, objects, and subscriptions that the SOC do not have administrative access will be
- excluded from support activities.
- Significant environment changes - a professional services engagement would be advisable for this
- type of activity.
- Continual incidents arising from poor management or housekeeping of the associated environments by the customer organisation.
- 1st line end user support - all support incidents and requests must be logged by an Authorised Named Contact.
- Service level targets for activities which need vendor escalation.
- Service level targets for incidents relating to a hosted platform service outage.
- Onsite support - this can be provided on case-by-case basis at an additional cost.
- Technology or services not in a supported configuration Technology or services not in supported product lifecycle.
- Patching of customer systems not related to a support incident.
- Project work, remediation, upgrades, or implementation of new systems.
- Any reporting that is outside the agreed scope of service and that cannot be provided using Azure Workbooks.
- The Customer acknowledges that the Services are only a part of its wider business transformation, business security, business continuity and disaster recovery strategy, and that the SOC cannot and does not provide a general guarantee of business transformation, security, business continuity and disaster recovery. It is for the Customer to assess, and to keep under review, the suitability of the contracted Services according to its circumstances, needs, risk appetite and budget.