PROACT

G-Cloud 15

Security Incident and Event Management SIEM (Microsoft Sentinel)

PROACT

Document control

Document type	Public - Freely Distributable		
Company	Proact IT UK		
Address	Proact IT UK Grayson House, Venture Way, Chesterfield, Derbyshire, S41 8NE		
Telephone	01246 266 300		
Primary contact	bids@proact.oc.uk	Role	N/A

Revision history

Issue date	Author	Version	Revision description
08/12/2025	Colin Abram	V1	Document Upload

PROACT

Security Incident and Event Management SIEM (Microsoft Sentinel)

Description

Built on Microsoft Sentinel and Defender our MDR service provides comprehensive protection against cyber-attacks that threaten the enterprise by delivering 24/7 detection and response capability.

- **Proactive Threat Detection and Response**: Your organisation will be protected against a wide range of security threats in real-time as we continuously monitor your network for any suspicious activity, using our team of security analysts and experts to detect and respond to cyber-attacks on behalf of your organisation.

- **24/7 SOC Services**: Your organization will have access to Proact's UK based 24/7 SOC services, meaning that you can rest assured that your network and systems are being monitored around the clock. This ensures that any security incidents are detected and responded to quickly, minimising the impact of any potential security breaches in and outside of business hours.

- **Expert Analysis**: Our specialist team of security professionals will continuously monitor your systems and networks, providing a security extension to your own IT operations with access to highly trained security professionals who can quickly identify and respond to any potential threats.

- **Threat Intelligence**: With the threat landscape changing in cyber security on a daily basis our security teams ingest and process threat intelligence data into our daily operations to stay up to date with the latest trends and techniques being used by adversaries.

- **Cost-Effective Risk Reduction**: By outsourcing your security operations to our MDR service, your organisation can avoid the high costs of hiring, training and retaining an in-house security team. Our service provides a cost-effective solution for organisations of all sizes, allowing you to focus on your core business activities while we handle your security needs.

- **Maximising Your Investment in Microsoft**: Our MDR service is based on Microsoft Sentinel and Defender, which means that we can leverage the full capabilities of these powerful security tools, ensuring that you are getting the most out of your security investment in Microsoft. This approach may also align more closely with wider business strategies around consolidation, cloud adoption and data governance.

- **Scalability**: Our MDR service is scalable, which means that it can grow and adapt to meet the changing needs of your organisation. Whether you are expanding your operations, adding new systems, or facing new security threats, our service can be tailored to meet your specific requirements with bespoke playbooks and escalation processes for each client.

- **Comprehensive Reporting**: The service provides comprehensive reporting, including detailed insights into security incidents and trends, which can help your organization make informed decisions about security policies and procedures.

This document contains the following appendix detailing the service definitions for Proact Managed Detection and Response (MDR):

- Appendix 1 - Managed Detection and Response (MDR) Service Definition

PROACT

Appendix 1 - Managed Detection and Response (MDR) Service Definition

1.1 - Service Overview

Proact's Managed Detection and Response (MDR) Security Operations is a service designed to improve the Customer's: protection, detection, and response capabilities by analyzing and triaging data from their infrastructure, operating systems, application logs, end point devices using Cloud Security Platforms and Cloud SIEM Services. This service will monitor, manage and build upon the functionality licensed to the Customer through their Microsoft security subscriptions.

See the glossary for the definition of acronyms used.

General Service Deliverables
Proact shall: • Provide a service desk and customer support portal to report and update incidents, change requests and escalations. • Provide service delivery management. • Maintain documentation of the service configuration. • Maintain a CMDB listing for all CIs. • Coordinate any product vendor involvement necessary. • Respond to reasonable service requests for relevant information and advice. • Provide a change advisory board to review normal, standard, and emergency change requests. • Subject to agreement, join the Customer's change advisory board, for relevant changes. • Implement agreed changes to CIs. • Provide reasonable problem management. • Provide incident trend analysis.
The Customer shall: • Maintain compatibility with Proact-managed systems/applications at the hardware, OS, and application level. • Log incidents via the portal, telephone, or email. Priority one incidents must be logged by telephone. • Assist with any systems or applications not under Proact's management. • Respond to requests for information/actions within five working days. Inactive incidents may be closed. • Resolve health issues on customer-managed systems. • Nominate named individuals to engage with Proact on the approval and timing of changes.

MDR Security Operations
Proact shall: • Manage the Customer's CSP/CSS and receive telemetry and log data from CIs. • Interact with the Customer's CSP/CSS via the provided portals and APIs. • Provide near real time monitoring of the CIs in scope through the CSP. • Utilise provided data connectors for CSS log collection, where required. • Use reasonable endeavours to define common log patterns for the CSS where a data connector is not available. • Keep a short-term audit log of administration actions undertaken on the CSP/CSS. • Apply standard configuration settings to the CSP portals and apply to the CIs. • Make recommendations regarding the tuning of log and telemetry collection to optimise data collection. • Validate the CSPs 'in-scope' during quarterly service reviews and adjust under a Contract change. • Work with the Customer to agree pre-defined 'playbook' actions to apply during common security incidents. • Respond to and investigate alerts/incidents issued by the CSP/CSS to triage risk exposure. • Where appropriate, the SOC will raise a security incident and provide guidance on resolution and future prevention. • Respond to security incidents with pre-defined 'playbook' responses. • Issue a P1 security incident where there is an immediate and uncontained threat. Assign an Incident Manager to direct activity and communicate with key Customer stake holders.

• Issue a P2 security incident where there is a severe threat to business data. Proact's security team will contact the Customer's security contact(s) with incident details and advice on resolution. • Issue a P3 security incident where access to business data is potentially at risk. Proact's security team will contact the Customer's security contact(s) with incident details and advice on resolution. • Work with the Customer to tune alerts and settings to minimise false positives. • Schedule a report detailing Customer users that are considered 'at risk'. • Provide a service review report. • Assist the Customer, upon request, with the creation of security dashboards within the CSP/CSS portals.
The Customer shall: • Maintain a valid subscription and provide credentials/access for the CSP/CSS in scope. • Open internal firewall ports to allow CIs to access CSP/CSS in scope. • Inform Proact where the CSPs in scope should be added or removed and adjust under a Contract change. • Utilise the storage areas provided by the CSP/CSS to store log and telemetry data. • Define the granularity and retention age of log and telemetry data. • Provide and manage servers/cloud instances required to host agent software. • Provide sufficient compute, network, and storage resource to allow for efficient data collection. • Deploy agent software at Proact's request. • Be billed directly by the cloud provider for any charges related to their CSP/CSS subscriptions. • Define the endpoint devices as 'in-scope' or 'excluded' and deploy endpoint agents on 'in-scope' endpoints. • Provide sufficient network bandwidth between the CIs and the CSP/CSS. • Apply any logging and telemetry tuning recommendations provided by Proact. • Work with Proact to agree pre-defined 'playbook' actions to apply during common security incidents. • Work with Proact to tune alerts and settings to minimise false positives. • Nominate security contact(s) and contact details to be informed when handling incidents. • Act upon Proact's advice/guidance regarding alert/incident prevention.

1.2 - Service Level Agreement

1.2.1 - Response Time Service Levels

Response	Proact is deemed to have 'responded' when a case is created in Proact's customer support portal and a case number is allocated.
Initiation	A change is initiated at the point at which (as recorded in the support system) Proact commences implementation of the change.
Response Time SLA - P1 Incident	Proact will use its reasonable endeavours to respond to priority 1 (P1) incidents **within 30 minutes**. A P1 incident is: a reasonable request by the Customer, which will be logged by phone (not email), for support or information in connection with the services, in circumstances in which the service(s) are completely unavailable or are imminently expected to be completely unavailable; or an alert received by Proact directly from its monitoring platform in connection with the services, that the service(s) are completely unavailable or are imminently expected to be completely unavailable; or have breached defined critical monitoring thresholds; or an incident logged by Proact in relation to an imminent and serious threat to the service(s). If Proact fails to respond to a P1 incident within 30 minutes the Customer will be entitled to a Service Credit of **15%** of the monthly minimum service Charges.
Response Time SLA - P2 Incident	Proact will use its reasonable endeavours to respond to priority 2 (P2) incidents **within 1 working hour.**

	A P2 incident is a reasonable request by the Customer for support or information, or an alert received by Proact directly from its monitoring platform, in connection with the services, in circumstances in which the service(s) are malfunctioning such that the service is significantly impacted but remains operational or have breached defined major monitoring thresholds. If Proact fails to respond to a P2 incident within 1 working hour the Customer will be entitled to a Service Credit of **5%** of the monthly minimum service Charges.
Response Time SLO - P3 Incident	Proact will use its reasonable endeavours to respond to priority 3 (P3) incidents **within 4 working hours.** A P3 incident is a reasonable request by the Customer for support or information, or an alert received by Proact directly from its monitoring platform, in connection with the services, in circumstances in which the service(s) are malfunctioning but with no significant impact on service or have breached defined minor monitoring thresholds.
Response Time SLO - P4 Incident	Proact will use its reasonable endeavours to respond to priority 4 (P4) incidents **within 8 working hours.** A P4 incident is a reasonable request by the Customer for support or information, in connection with the services, in circumstances in which there is no specific malfunction.
Service Credit Limits	A Service Credit is not a refund, cannot be exchanged into a cash amount and is capped at a maximum of 50% of the monthly minimum charges for the relevant service. A Service Credit is the sole and exclusive remedy for any failure by Proact to meet its obligations under the SLA.
Response Time SLO – Standard Change Request	Proact will use its reasonable endeavours to initiate standard changes within **8 working hours** from when authorised**.** A 'Standard' change is any pre-authorised change that is low risk, relatively common and follows a predefined procedure or work instruction. Proact's change advisory board (CAB) is not required to approve 'Standard' changes prior to implementation.
Response Time SLO – Normal Change Request	Proact will use its reasonable endeavours to initiate normal changes within **8 working hours** from when authorised**.** A 'Normal' change is any change that is not a 'Standard' change according to the above definition and is not an emergency. An agreed ad-hoc change to the configuration of the services. The CAB must authorise 'Normal' changes and approve an implementation plan.
Response Time SLA – Emergency Change Request	Proact will use its reasonable endeavours to initiate required emergency changes within **4 hours** from when authorised. An 'Emergency' change is any 'Normal' change that requires an expedited timeframe to resolve a P1 incident causing significant impact to the services in scope, and which cannot wait for review and approval from the CAB. Where there is not an active P1 incident, the change shall not be classified as 'Emergency'. Proact's Emergency Change Advisory Board (E-CAB) must authorise 'Emergency' changes and approve an implementation plan. If Proact fails to respond to an Emergency Change Request within 4 hours, then the Customer will be entitled to a Service Credit of **15%** of the monthly minimum service Charges.
Response Time SLO – Service Request	Proact will use its reasonable endeavours to initiate service requests **within 8 working hours.** A 'Service request' is a reasonable request by the Customer for activity or information, in connection with the services, that is neither an incident nor a

	change and follows a predefined procedure or work instruction. A common example of a Service Request is a password reset.
Working Hours for Changes	All Standard changes and Normal changes shall be scheduled by Proact and will be carried out during local business hours except where a change is requested by Proact and is expected by Proact (upon evaluation by the Proact CAB) to have a significant impact on availability or performance of the services in scope. The Customer may request that any particular change is implemented at a specific time, including outside local business hours, but, if such request is accepted by Proact, additional charges shall apply as agreed in advance between Proact and the Customer. 'Emergency' changes are implemented 24/7 and are not subject to additional charges.

1.3 - Glossary

Glossary Term	Definition
Configuration Item (CI)	A term used for a component which is within the scope of the Contract and stored within the Configuration Management Database (CMDB). The CIs will be security platform user accounts monitored and managed by Proact, as set out in the Contract.
Cloud Security Platforms (CSP)	CSP are a suite of platforms available to the Customer through their Microsoft subscription offering multiple area of security protection, including: Identity protection, endpoint protection, vulnerability management and Office 365 protection. These platforms can be utilised individually allowing the Customer to customize their level of protection.
Cloud SIEM Service (CSS)	The CSS is a Security Information and Event Management (SIEM) platform available to the Customer through their Microsoft subscription. The SIEM service is a repository for the Customer's log data, generated by their business systems, servers and hardware. This log data is analyzed by the SIEM service to detect anomalies and threats and raise security alerts.