G Cloud - Support

Service Definition Document

Managed Security Service



quorum

SERVICE DESCRIPTION

Quorum's Managed Security Service is designed to protect businesses against evolving cyber threats while simplifying security management. It combines proactive monitoring, detection, and response to deliver 24/7 monitoring, incident remediation, and escalation for security events detected by Microsoft Defender and Sentinel. The service emphasizes proactive threat detection, automation, and continuous improvement, aiming to reduce avoidable escalations to client teams, improve efficiency through advanced analytics and automation, and provide monthly KPI reporting and regular onsite reviews to ensure alignment with client needs and ongoing service enhancement.

Certified Specialists: Microsoft Solutions Partner for Security and member of the Microsoft Intelligent Security Association.

24/7 Threat Monitoring & Response: Continuous detection and alert triaging to minimise attacker dwell time and reduce false positives.

Endpoint & Identity Protection: Dedicated security software for endpoints, identity systems, M365, and SaaS applications to prevent phishing, malware, and identity compromise.

Security Hygiene & Compliance: Regular audits and configuration reviews to maintain best practices and meet compliance requirements.

Education & Awareness: Ongoing staff training to reduce human error and improve resilience against social engineering attacks.



Member of
Microsoft Intelligent Security Association

Microsoft Security



SERVICE FEATURES

Endpoint & Identity Protection: Dedicated security software for endpoints, identity systems, M365, and SaaS applications to prevent phishing, malware, and identity compromise.

Security Hygiene & Compliance: Regular audits and configuration reviews to maintain best practices and meet compliance requirements.

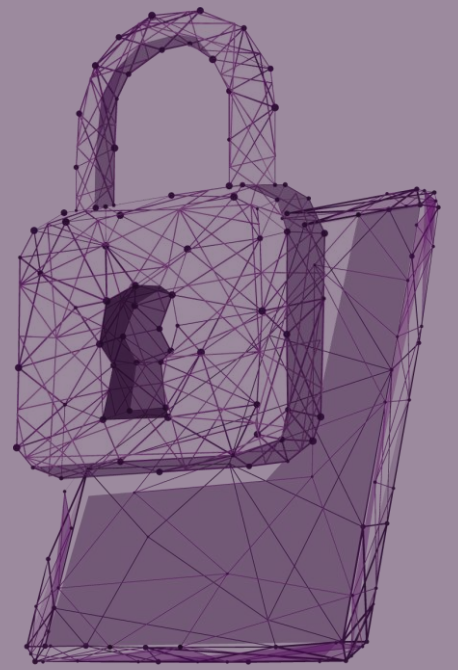
Education & Awareness: Ongoing staff training to reduce human error and improve resilience against social engineering attacks.

24/7/365 Monitoring and Incident Response: Continuous monitoring of security events using Microsoft Defender and Sentinel, with rapid investigation and remediation according to agreed SLAs.

Dedicated Security Team: Initial deployment of a dedicated team including security analysts and engineers, all based in the UK for data sovereignty.

Flexible Service Tiers: Flexible Service Tiers: Options ranging from design consultancy to fully managed MDR and incident response.

UK-Based Support: All SOC teams and support resources are located in Edinburgh, ensuring compliance with UK data residency requirements.



SERVICE FEATURES (Cont.)

Automation and Orchestration: Use of Microsoft Sentinel playbooks and Azure Logic Apps for automated enrichment, containment, notification, and escalation of incidents.

Data Ingestion & Cost Optimisation: Expertise in Optimising Sentinel data costs using Auxiliary Logs, Cribl, and Sentinel Data Lake.

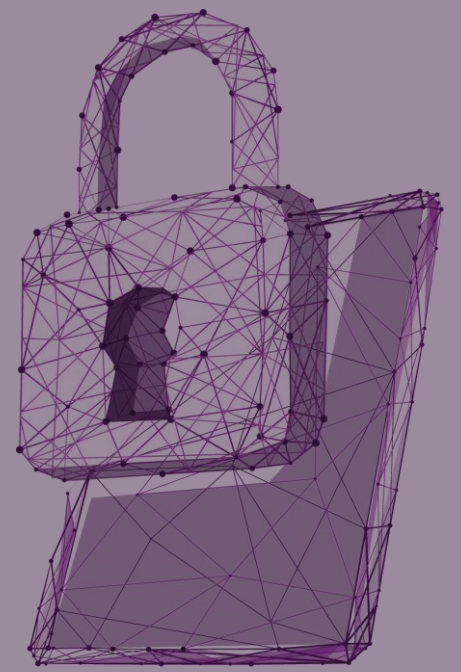
Advanced Analytics: Continuous improvement of detection rules, custom KQL queries, and integration of threat intelligence for proactive threat detection.

Compliance and Data Protection: Strong encryption, role-based access controls, and adherence to GDPR and UK/EU data protection regulations.

Scalability: Ability to flex resources in response to spikes in threat activity, leveraging a wider managed services pool.

Reporting and Dashboards: Monthly KPI reporting, tailored dashboards for different stakeholders, and regular onsite service reviews.

Continuous Improvement: Regular review of service quality, feedback incorporation, and alignment with client needs.



SERVICE BENEFITS

Proactive Threat Detection and Response:

The service is designed to continuously monitor, detect, and respond to security threats using Microsoft Defender and Sentinel. This proactive approach aims to reduce the number of incidents that require escalation to your internal team, especially out-of-hours, by handling less-complex events directly.

Continuous Improvement:

The service includes ongoing tuning and enhancement of detection rules within Sentinel, ensuring that threat detection capabilities evolve with the changing threat landscape and remain effective.

Expert Data Engineering:

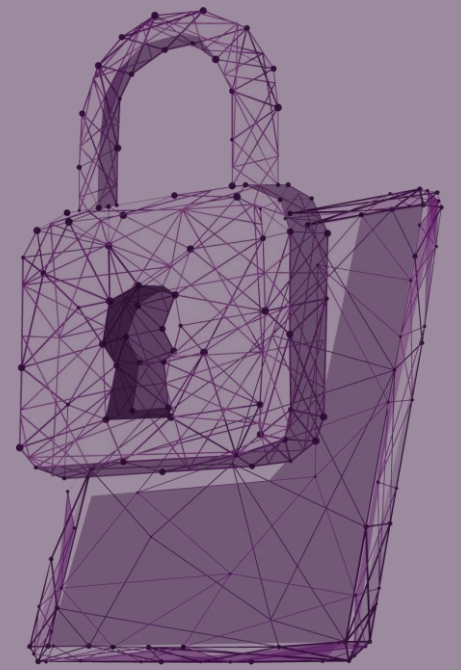
Certified data engineers are provided to onboard new data sources efficiently, create queries, and filter noise from data sent to Sentinel. This reduces onboarding time and frees up your internal engineering team for more strategic work.

Enhanced Use of Existing Tools:

Quorum's expertise with the Microsoft Defender product set helps you maximise the value of your existing licenses, potentially reducing costs on overlapping tools.

Comprehensive Reporting and KPIs:

The service includes monthly reporting of service KPIs, regular onsite reviews, and tailored dashboards to provide visibility into threats, incidents, and service performance.



SERVICE BENEFITS (Cont.)

Flexible, Dedicated Support:

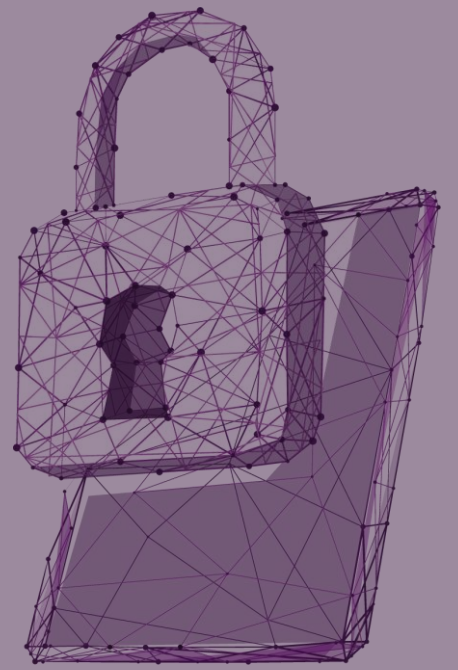
A dedicated team provides 24x7 monitoring, remediation, and escalation, with the ability to flex resources as needed to handle spikes in activity. The team is based in the UK, supporting data sovereignty requirements.

Reduced Total Cost of Ownership (TCO):

By reducing avoidable escalations, streamlining onboarding, and optimising use of existing security tools, the service aims to lower your overall security management costs.

Collaborative Partnership:

The approach emphasises working closely with your team, aligning with your business needs, and providing regular feedback and improvement workshops.



SERVICE PROVISION

1. Onboarding and Project Mobilisation: The process begins by establishing an onboarding framework, identifying key stakeholders, setting up communication plans, and defining access requirements to support initial discovery activities.

2. Discovery Phase: Quorum conducts a high-level discovery of the client's existing security environments (e.g., SIEM, XDR, data ingestion platforms) to ensure a smooth transition and gain visibility into core systems.

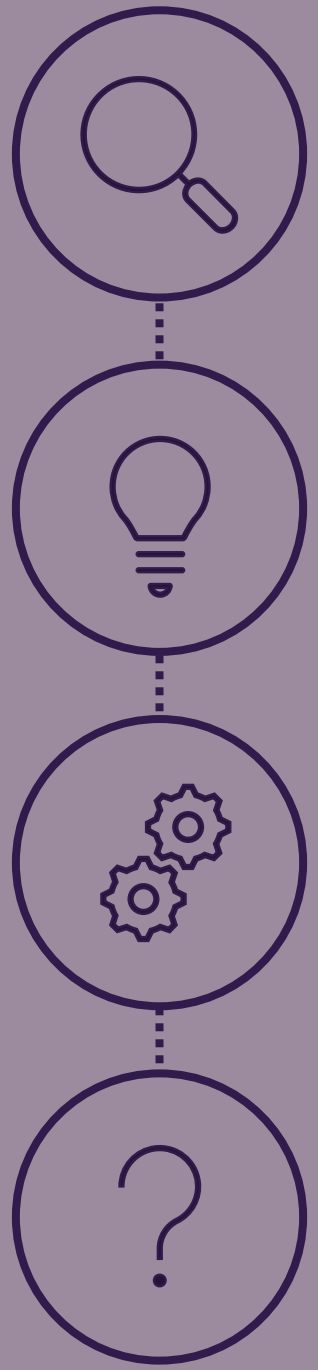
3. Service Design Workshops: Collaborative workshops are held to define roles, support requirements, escalation paths, reporting formats and frequency, support hours, and meeting structures. Additional workshops cover process design, such as change control, integration processes, and employee vetting.

4. Service Readiness: The provider ensures all required support documentation is available, sets up necessary integrations (e.g., access management, helpdesk systems), and completes a final operational readiness review with the client.

5. Go Live: The managed security service formally launches, transitioning operational responsibility to the dedicated service team.

6. Knowledge Transfer and Team Integration: We emphasise knowledge transfer by working alongside client personnel, ideally onsite during onboarding and the initial phase post-launch. This supports cultural immersion and informal communication, which are critical for effective service transition.

7. Continuous Improvement and Feedback: Regular reviews and monthly reporting ensure the service remains aligned with the client's needs and supports ongoing improvement.



SERVICE SUPPORT

Flexible Service Tiers: Support ranges from design consultancy to fully managed detection and response (MDR), including incident response and remediation.

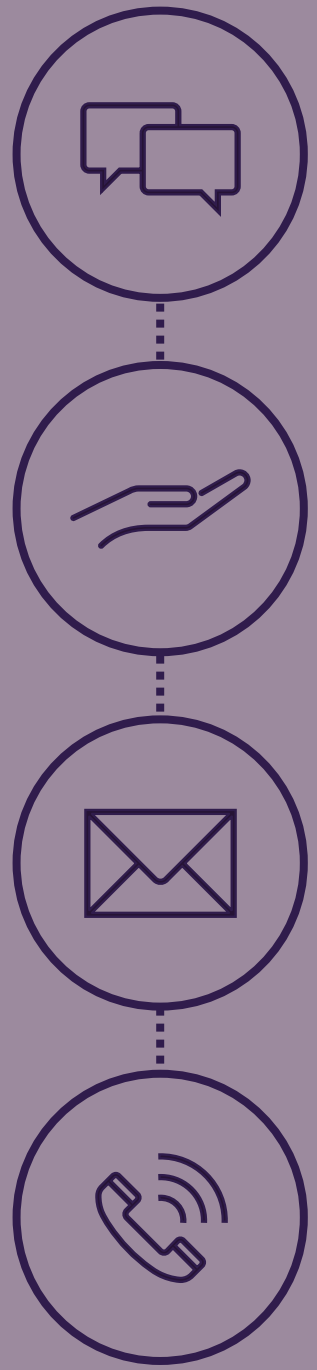
Incident Prioritisation and SLAs: Incidents are triaged using a structured matrix, with target response times agreed with each customer during service onboarding, tailored to individual requirements.

Scalable Resource Model: The team can flex resources to handle spikes in threat activity, drawing on a wider pool of managed services staff as needed.

Comprehensive Onboarding: A structured onboarding plan ensures rapid knowledge transfer, minimal disruption, and dedicated resources during the initial transition.

Continuous Improvement: Regular reviews, monthly reporting, and feedback mechanisms ensure the service evolves to meet changing needs and incorporates client input.

Clear Communication Channels: Support is accessible via Microsoft Teams, email, phone, and SMS, with a dedicated Service Delivery Manager as the main point of contact.





www.quorum.co.uk

Copyright © 2026 Quorum

0131 652 3954