oneAdvanced

Managed Security Operations Centre (SOC)

Detect. Investigate. Respond.
24×7 UK-Based Security Operations

With ransomware, phishing, insider risks and zero-day exploits growing in complexity and proliferation, organisations are increasingly at risk, especially when paired with a lack of around-the-clock expertise and tooling to detect and respond effectively. Disparate security products generate mountains of alerts, drowning small teams in false positives and leaving true threats undetected until it's too late.

OneAdvanced's Managed SOC delivers a comprehensive, always-on security operations centre as a service. Built on Microsoft Sentinel (SIEM/SOAR) and Qualys vulnerability management, our UK-based analysts centralise log collection, apply advanced analytics and machine learning to spot anomalies, and escalate true-positive incidents into structured containment, eradication and recovery workflows. With integrated incident response, compliance-ready reporting and automated playbooks, we turn security from a reactive burden into a strategic advantage.

What’s included in our Managed SOC Service?

24×7 Threat Monitoring & Alerting

Continuous collection and analysis of security events via Microsoft Sentinel - detecting known and emerging threats in real time.

Rapid Incident Response

Analyst intervention within 30 minutes for Critical/High alerts, with containment and eradication per NIST/SANS best practices.

Vulnerability Management

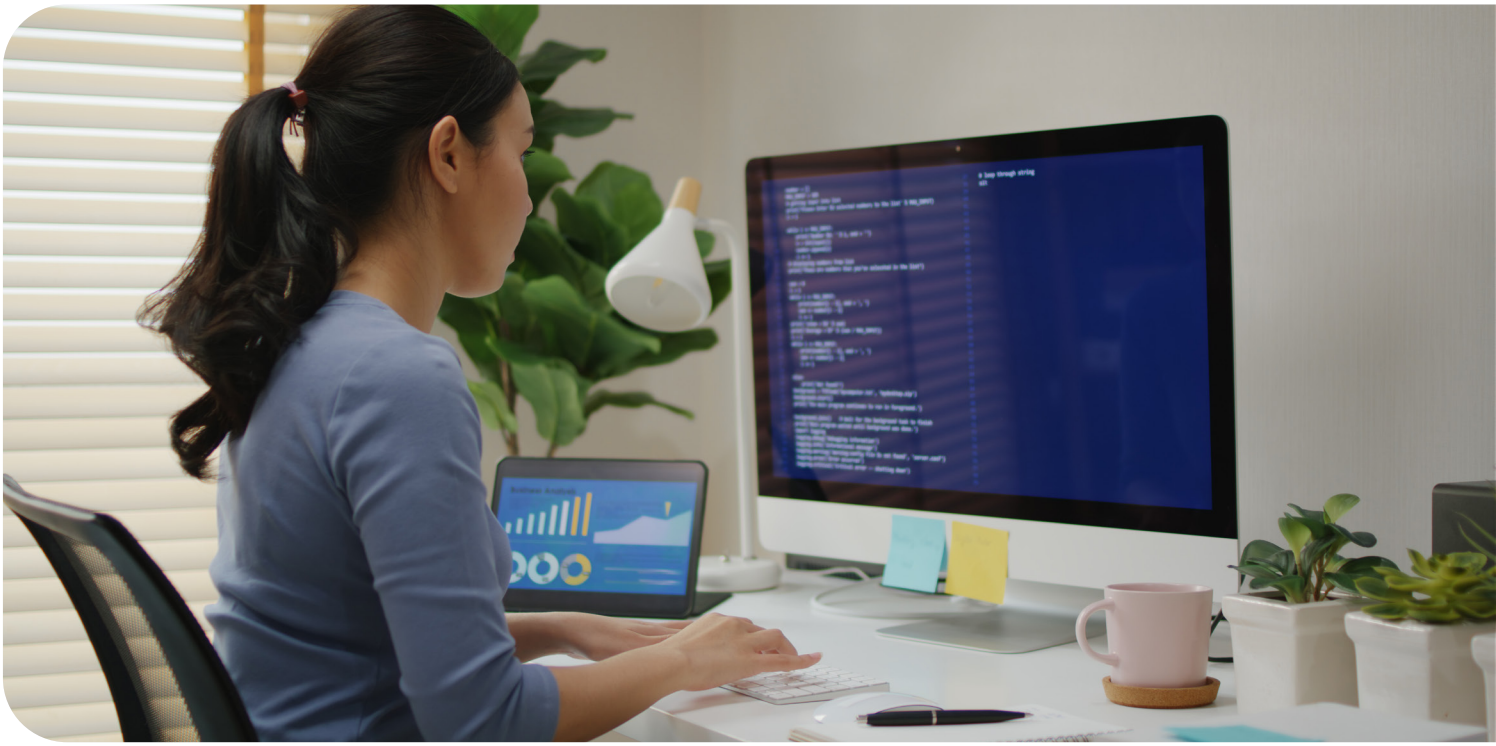
Scheduled credentialed and uncredentialed scans by Qualys, asset discovery and prioritised reporting to shrink your attack surface.

Compliance & Reporting

Monthly security-health dashboards, consolidated scorecards and tailored modules for GDPR, ISO 27001, NIST, NHS and FCA mandates.

Integration & Automation

SOAR playbooks and connectors ingest logs from EDR, ServiceNow, Syslog and more, automating containment actions and ticket creation.



Key benefits

Continuous UK-based coverage	No off-hour gaps or offshore hand-offs.
Slashed dwell time	Average 30 min response for Critical alerts, minimising damage and business impact.
Unified security operations	One partner, one portal, one SLA across SIEM, SOAR and vulnerability management.
Proactive risk reduction	Embedded threat hunting and vulnerability scanning keep you ahead of emerging threats.
Predictable OPEX	Avoid CAPEX on tooling and headcount for a 24×7 SOC; scale log volumes and analyst capacity as needed.

Service details

Implementation

Typically up and running in 3–4 weeks. This period includes discovery workshops, log-collector deployment, Sentinel connector configuration and runbook alignment.

Support Hours and SLAs

- **Security monitoring:** 24×7
- **P1/P2 (Critical/High) response:** 24×7, within 30 min
- **P3 (Medium) response:** 7 am–7 pm Mon–Fri, within 4 hrs
- **P4 (Low) response:** 7 am–7 pm Mon–Fri, within 1 business day

Pricing Structure

Tiered monthly subscriptions based on log ingestion volume, retention period and analyst coverage. All fees are transparent under a fair-use policy - no hidden overages.

Prerequisites

Network access and credentials for log collection agents and Qualys scanners, integration with your ITSM platform; credentials or API access for EDR/AV and infrastructure logs, designated Customer and Escalation Contacts for incident notifications.

Why OneAdvanced for managed SOC?

OneAdvanced combines deep security expertise with a mature, ITIL-aligned delivery framework, fully based in the UK. Our SOC analysts hold industry certifications and security clearances, ensuring data sovereignty and compliance in regulated sectors including healthcare, financial services and government.

Built on market-leading platforms - Microsoft Sentinel for SIEM/SOAR and Qualys for vulnerability management- we offer direct escalation paths into vendor support and pass through any SLA-credit compensation back to you. With quarterly strategy reviews, continuous improvement workshops and transparent, tiered pricing under a fair-use policy, we transform your security posture from a cost centre into a competitive differentiator.

FAQs

What is a managed SOC?

A managed SOC is your 24×7 security operations centre as a service - centralising monitoring, detection and coordinated response so you're always protected.

Why do we need a managed SOC?

Cyber threats never rest. Our SOC ensures continuous defence against ransomware, phishing, insider risk and zero-days with expert analysts and advanced tooling.

Can I trial the service?

Yes. We offer demonstrations and limited trial periods with real-time monitoring to showcase our detection and response capabilities.

How do you keep my data safe?

We use least-privilege connectors, keep logs within your tenant via Azure Lighthouse, and enforce encryption in transit and at rest - meeting GDPR, ISO 27001 and NHS data-sovereignty requirements.

Do you provide compliance support?

Absolutely. We supply audit-ready reports, scorecards and assistance with GDPR, HIPAA, PCI-DSS, NIST, ISO and sector-specific mandates.

oneAdvanced

Ready to secure your organisation around the clock?

Contact your OneAdvanced account manager or email managedit@oneadvanced.com to schedule a scoping workshop and rapid deployment plan.

Microsoft Solutions Partner
Data & AI
Azure

Microsoft Solutions Partner
Digital & App Innovation
Azure

Microsoft Solutions Partner
Infrastructure
Azure

Microsoft Solutions Partner
Security

Microsoft Solutions Partner
Modern Work

+44(0) 330 343 4000 www.oneadvanced.com hello@oneadvanced.com