AMICIS GROUP

Together, we'll build cyber resilience.

Amicis Group Delivery
G-Cloud 15
Service Description –
SOC/SIEM Service
January 2026

hello@Amicisgroup.co.uk

www.Amicisgroup.co.uk

hello@Amicisgroup.co.uk
www.Amicisgroup.co.uk

Security Operations Centre (SOC) / SIEM Service

Service definition

The SOC / SIEM service provides continuous security monitoring, detection and analysis of security events using a centralised Security Information and Event Management (SIEM) platform. The service collects, normalises and correlates security logs and telemetry from agreed data sources to identify potential security incidents, suspicious activity and policy violations.

The service combines automated detection with analyst triage to deliver actionable security insights, support incident investigation and improve visibility of the customer's security posture. The service focuses on monitoring, alerting and analysis and does not include incident remediation unless explicitly agreed.

Typical service inclusions

- Onboarding and configuration of agreed SIEM platform
- Ingestion of security logs from in-scope data sources
- Normalisation and correlation of security events
- Configuration of detection rules and use cases
- Continuous monitoring of ingested telemetry
- Analyst triage and validation of security alerts
- Severity-based alerting and notification
- Support for investigation through event analysis
- Regular security monitoring and trend reports
- Ongoing tuning of detection logic to reduce false positives

Deliverables

- Security alerts and notifications aligned to agreed severity levels
- Monitoring and incident summary reports
- Event and log data to support incident investigation
- Documentation of onboarded data sources and use cases
- Service performance and activity summaries

Service characteristics

- Continuous monitoring on a 24x7 basis unless otherwise agreed
- Scoped to agreed data sources, log types and environments
- Dependent on customer-provided access and log availability
- Analyst-supported detection and alerting

hello@Amicisgroup.co.uk
www.Amicisgroup.co.uk

- Scalable based on log volume and number of data sources
- Delivered using industry-standard SIEM technologies
- Does not guarantee detection of all security incidents
- Complements, but does not replace, incident response services