CAMBRIDGE
CYBER ADVISERS

SIEM, SOAR & MDR

Service Definition Document. Version 1.0

19 January 2026

SIEM, SOAR & Managed Detection & Response (MDR)

1. Introduction

This Service Definition Document describes the **Security Incident & Event Management (SIEM), Security Orchestration, Automation & Response (SOAR) & Managed Detection & Response (MDR)** service offered by Cambridge Cyber Advisors (CCA) under the G-Cloud 15 framework. The service provides organisations with advanced monitoring, automated response capabilities, and expert-led threat detection to strengthen operational security and reduce the impact of cyber threats.

Modern organisations face increasingly sophisticated attacks that bypass traditional security controls. Effective detection and response requires a combination of real-time monitoring, automated workflows, threat intelligence, and skilled analysts capable of identifying and responding to malicious activity at speed.

CCA's SIEM, SOAR & MDR service combines security engineering, operational monitoring, threat hunting, and incident response aligned to NCSC, MITRE ATT&CK, and NIST standards. The service delivers enhanced visibility, rapid response, and continuous improvement of an organisation's security operations capability.

2. Service Overview

The SIEM, SOAR & MDR service provides a comprehensive approach to threat detection, automated response, and continuous monitoring across cloud and on-premise environments. The service supports organisations in building, optimising, or outsourcing their security operations capability.

Activities include:

- SIEM platform deployment, configuration, and optimisation
- Use case development and correlation rule engineering
- Log ingestion, normalisation, and enrichment
- SOAR playbook design and automation of response workflows
- Threat detection, alert triage, and incident escalation
- Threat hunting and behavioural analytics
- Integration of threat intelligence feeds
- Continuous monitoring and MDR analyst support
- Operational reporting and KPI development
- Post-incident analysis and tuning
- Executive and technical debrief sessions

Service Features

- Comprehensive SIEM engineering and optimisation
- SOAR automation and playbook development
- 24/7 or business-hours MDR monitoring options

- Threat intelligence-driven detection
- Alert triage, investigation, and escalation
- Threat hunting and behavioural analytics
- Integration with EDR, cloud, network, and identity telemetry
- Use case development aligned to MITRE ATT&CK
- Operational dashboards and reporting
- Optional incident response and forensics support

Service Benefits

- Improves visibility across cloud, hybrid, and on-premise environments
- Reduces detection and response times through automation and expert analysis
- Strengthens operational resilience and reduces business impact
- Enhances alignment with NCSC, ISO 27001, and regulatory requirements
- Improves SOC efficiency and reduces alert fatigue
- Supports Zero Trust and modern security operations models
- Provides continuous assurance through proactive threat hunting
- Enables informed decision-making through operational reporting

3. Service Scope

The service includes, but is not limited to, SIEM engineering, SOAR automation, MDR monitoring, threat hunting, and operational reporting. Activities may include log onboarding, use case development, playbook creation, alert triage, incident escalation, and continuous tuning of detection logic.

4. Delivery Methodology

CCA follows a structured, phased approach using our standard methodology:

- Scoping and Planning
- Platform Review and Data Onboarding
- Use Case and Playbook Development
- Operational Monitoring and Threat Hunting
- Analysis, Reporting, and Continuous Improvement

5. Deliverables

- SIEM Configuration & Use Case Report
- SOAR Playbook Catalogue
- MDR Operational Reporting Pack
- Threat Hunting Summary

- Incident Escalation Reports
- Risk Register and Impact Analysis
- Prioritised Remediation Roadmap
- Optional Advisory and Implementation Support Outputs

6. Service Levels

- Engagement commences within 10 working days of contract award
- SIEM/SOAR configuration report within 10 working days of assessment completion
- MDR reporting delivered weekly or monthly depending on service tier
- 24/7 or business-hours monitoring options available

7. Governance and Assurance

Activities align with NCSC guidance, ISO 27001, MITRE ATT&CK, and NIST incident handling standards. Where required, engagements will be managed by a CCA Project Manager.

Backup and Restore

Not applicable.

Reporting & Analytics

Outputs include operational dashboards, detection metrics, threat hunting reports, incident summaries, and tuning recommendations.

Incident Management

The service provides detection and escalation; full incident response is available as an optional add-on.

Disaster Recovery

Not applicable.

Availability

CCA delivery teams are available Monday–Friday, 09:00–17:30 UK time, with optional 24/7 MDR coverage.

8. Security and Data Protection

- Confidential handling of customer data
- UK-based monitoring and engineering team
- Secure environments for log and alert processing
- Data retained for 30 days then destroyed
- GDPR, NCSC, and ISO 27001-aligned practices

GDPR & Data Privacy

- Personal data minimisation
- DPIA support available
- Findings anonymised unless requested otherwise

Accreditations

- ISO 27001-aligned practices
- NCSC-aligned methodologies

Staff Security Clearance

SC-cleared staff available upon request; BPSS as a minimum for all CCA consultants.

9. Customer Responsibilities

Customers must provide access to systems, logs, stakeholders, and relevant data sources to support monitoring and detection.

Technical Requirements

- Access to SIEM/SOAR platforms (or deployment support)
- Log source access and configuration permissions
- Contact details for key personnel

Supported Browsers/Devices

Not applicable.

Access Restrictions

Customer must designate authorised individuals for scope approval, change requests, and receipt of outputs.

10. Service Constraints

Activities are limited to agreed scope and may require controlled windows for log onboarding, rule deployment, or playbook testing.

11. Pricing

- Pricing is engagement-based and determined by scope, duration, and complexity. Pricing is based on:
  Number of log sources and integrations
- Complexity of SIEM/SOAR platforms
- MDR service tier (business hours or 24/7)

- Threat hunting and tuning requirements

Engagement duration

Typical engagements range from 4–12 weeks depending on breadth and complexity.
Day-rate pricing is available and compliant with G-Cloud pricing rules.

Ordering and Invoicing Process

Ordering is typically completed via Purchase Order following confirmation of service purchase. CCA will invoice at the end of every calendar month, providing a detailed breakdown of services delivered, including VAT/expenses. Consolidated invoices can be provided. Invoices may be issued electronically or via post.

12. Exit and Offboarding

- Findings delivered
- Knowledge transfer completed
- Data destroyed within 30 days (certificate available)

Onboarding

- Requirements workshop
- Scope definition
- Stakeholder identification
- Communication validation

Offboarding

- Walkthrough of findings
- Delivery of reports
- Optional remediation workshop
- Secure data destruction

Training Provided

- SIEM/SOAR awareness session
- Threat detection and response briefing
- Optional tabletop exercises

13. Termination

- Standard G-Cloud termination terms apply
- Customer may terminate with notice; work completed to date will be invoiced
- Provider may terminate only under defined exceptions (e.g., breach of Rules of Engagement or safety concerns)

14. Contact and Support

A delivery manager is assigned for each engagement. Support is available via email and phone during delivery hours.

Included as standard:

- Email and phone support during the engagement
- Delivery manager assigned
- Access to reporting team for clarifications

Enhanced support packages available for continuous monitoring and MDR services.