Security Operations Centre

G-Cloud 15 Service Definition

1. Summary

In today's rapidly evolving digital landscape, the need for robust cybersecurity measures has become paramount for organisations across all industries, including education and research. To effectively safeguard their digital assets, many customers are embracing the concept of a Security Operations Centre (SOC). A SOC is a service dedicated to continuously monitoring, detecting, and responding to security threats on behalf of an organisation. We have designed our SOC service to support our customers to protect, detect, respond and recover from cyber incidents. The Jisc SOC offering will continue to evolve and adapt to the wider threat environment and customer requirements as new technologies emerge and evolve.

As Jisc operates the Janet Network, which is the UK's national research and education network (NREN), this provides us with the ability to gather primary threat intelligence, via live traffic analysis and other systems to help perform threat hunting and offers unique containment capabilities beyond that of other Security Service Providers. This gives us world class threat intelligence opportunities to better support our customers in mitigating potential threats and is something that sets us apart from our competitors. As a result, Jisc is uniquely positioned to offer a best in class SOC service, by utilising and developing the existing and experienced Cyber Division, leveraging the sector renowned and NCSC accredited Cyber Incident Response Team (CSIRT), Cyber Threat Intelligence (CTI) and Defensive Services Teams, which combined offer a comprehensive level of support.

Jisc's Security Operations Centre builds on the trusted cyber security membership services our customers already rely on - including Incident Response, Cyber Threat Intelligence, and Janet Network protections - and combines them with Jisc's Cyber Security Threat Monitoring (CSTM) SIEM platform to provide a powerful, integrated security foundation.

What truly differentiates Jisc's SOC is our expert-led onboarding and continuous service model. As part of onboarding, every organisation takes part in a series of Attack Risk Review and Security Hardening Workshops, delivered by Jisc's cyber security specialists. These sessions are designed to identify likely attack paths, validate logging and detection coverage, and optimise security configurations before the service goes live - significantly reducing risk from day one and ensuring the SOC is tuned specifically to your environment.

On top of this strong foundation, Jisc layers advanced services such as Managed Detect and Respond (MDR) and Vulnerability Management, creating a fully integrated, sector-led SOC capability. This allows Jisc to provide not just alerts, but real security outcomes - helping

organisations protect their systems, detect threats early, respond effectively to incidents, and recover quickly and safely.

Because Jisc is part of and dedicated to the UK education and research sector, our SOC delivers deep sector knowledge, shared intelligence, and collaborative defence that commercial providers simply cannot match.

2. Service Definition

2.1 Service Scope

The SOC is UK based and operates on a 24/7 automated Incident Response basis, with standard alert triaging during core office hours (8am to 6pm). The core service delivered by the SOC provides real-time visibility of your environment enabling the detection, triage, response, resolution, and reporting of cybersecurity incidents.

2.2 Service eligibility criteria

To begin the onboarding process to Jisc's SOC service, the following eligibility criteria must be met:

- Janet Network Connection: Customers wishing to purchase Jisc's SOC service must have a Janet Network IP Connection.
- EDR/XDR Licensing: Customers must already have a Jisc SOC supported EDR/XDR license. Currently these are Microsoft Defender and CrowdStrike Falcon.

2.3 Service Management

Jisc provides the SOC service to ITIL Service Management guidelines. This includes defining and operating incident management and change management procedures and providing the service and deliverables, such as monthly reports and service reviews.

2.3.1 Hours of Service

Jisc's Security Operations Centre (SOC) operates a split hour service.

- Eyes on glass alert triaging and human incident response processes operate during core office hours (8am to 6pm).
- A fully automated alert triage with human incident response operates outside of core office hours on a 24/7/365 basis.

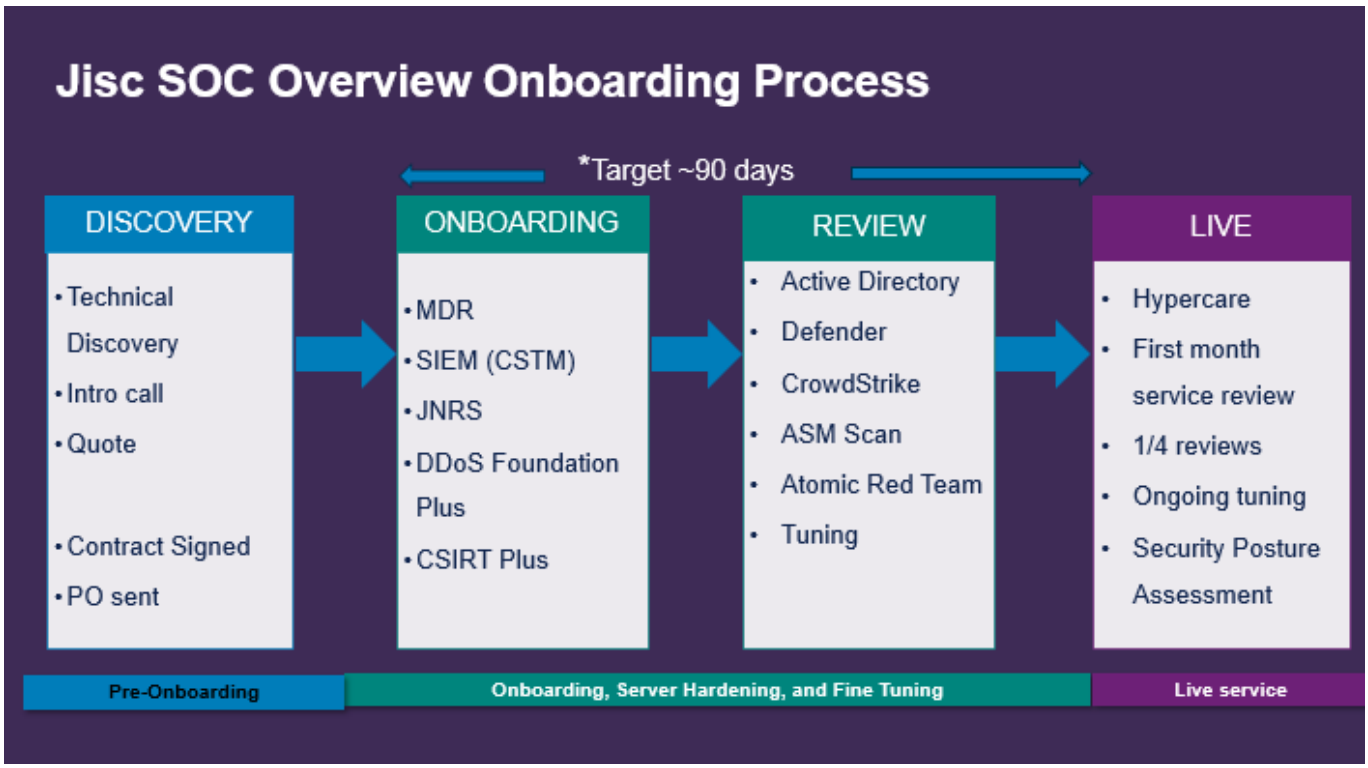
2.4 Information Assurance

We are ISO27001 and Cyber Essentials certified, and use appropriate management infrastructure, network connectivity, staff security clearances and processes to deliver our security services in line with the Cabinet Office Security Policy Framework (SPF), NCSC guidelines (including, but not limited to, UK OFFICIAL) and the Data Protection Act (DPA) principles, all in line with GDPR. Our Cyber Incident Response Team (CSIRT) are NCSC Cyber Incident Response (CIR) Level 2 assured and CREST Accredited.

2.5 Service Pricing and Invoicing

Jisc Security Operations Centre pricing overview is provided in the separate pricing document.

3. Service Operation



Jisc SOC onboarding journey

3.1 Discovery Phase

3.1.1 Assessment

Jisc will ask customers to complete a Technical Discovery document to help establish a baseline understanding of their security posture and operational environment. This includes details on network architecture, key assets, threat landscape, and security priorities. The information gathered will enable Jisc to identify any gaps or required enhancements before integrating the customer with Jisc's SOC.

3.1.2 Scoping

Jisc will review the customers technical requirements and discuss service and capabilities of the SOC service, identifying the following key scoping elements:

- Determine the SOC model (Full/Hybrid)
- Identify data ingestion sources for SIEM
- Identify EDR/XDR requirements EDR/XDR licensing requirements (outside of SOC service cost)
- Critical Asset and Identity review

3.2 Onboarding Phase

3.2.1 Onboarding

The onboarding process is a crucial phase to ensure a seamless transition to our Security Operations (SOC) service. The onboarding process will follow an incremental process of

configuration and ingestion of log sources into the SOC, and can be broken down into the following key elements:

- Managed Detect and Response (MDR): Your existing EDR/XDR consoles will be onboarded onto Jisc's MSSP tenancy empowering the detection and response to threats in real-time through a co-management approach between the customer and Jisc.
- Security Information & Event Management (SIEM): Key system logs will be ingested into Jisc's MSSP Splunk service (CSTM) to facilitate alert correlation and risk-based alerting. This combines the enrichment data from your EDR/XDR console with other logs sources such as Firewalls, Remote Access and Hypervisor solutions which may not have EDR/XDR agents deployed.
- Protective DNS (PDNS): Our expert engineers will help onboard your DNS service onto Jisc's Protective DNS (PDNS) service. The service includes feeds from National Cyber Security Centre (NCSC), Open-source intelligence, commercial providers and other partners to create response policy zone (RPZ) feeds that block malicious domains. These feeds are continuously curated by our cyber threat intelligence team, ensuring that the Protective DNS service can adapt to emerging threats.

3.2.2 Security Hardening Workshops

As part of the SOC service deployment, Jisc will ensure your existing EDR tools are fully configured and optimised. You will also receive dedicated hardening workshops, providing tailored advice and guidance on strengthening your Cloud and on-premise infrastructure, including Active Directory. These sessions help identify configuration gaps, improve resilience, and ensure your environment is aligned with best-practice security standards.

In addition, you will gain access to the Cyber Hub and your SOC dashboard, giving you real-time visibility of events and alerts across your estate. This provides immediate insight into emerging threats, enables faster decision-making, and enhances situational awareness for your security and IT teams.

3.3 Review Phase

3.3.1 Monitoring and Baselining

Once data sources begin to flow into the SOC and EDR/XDR, tools are configured to based practice, robust monitoring practices and accurate baselining of normal behaviour will be established. Fune tuning will be carried out to alert accounting for your organisational behaviours This will allow the SOC team to effectively detect and respond to security threats, minimise the impact of incidents, and maintain the security posture of the organisation. Tuning carries on for the life of the service, growing and adapting to the changes within your organisation over time.

3.4 Service Live State

Following the initial service initiation meeting, and once all services have been confirmed as fully operational, your organisation will transition to a fully live Security Operations Centre (SOC) service, supported by a dedicated period of Hypercare.
During this phase, the SOC team will closely monitor your environment, validate alert flows, and ensure that all integrations and processes are functioning as expected. You will retain access to a dedicated Microsoft Teams space for incident response, as well as a direct point of contact via soc@jisc.ac.uk for all general queries.

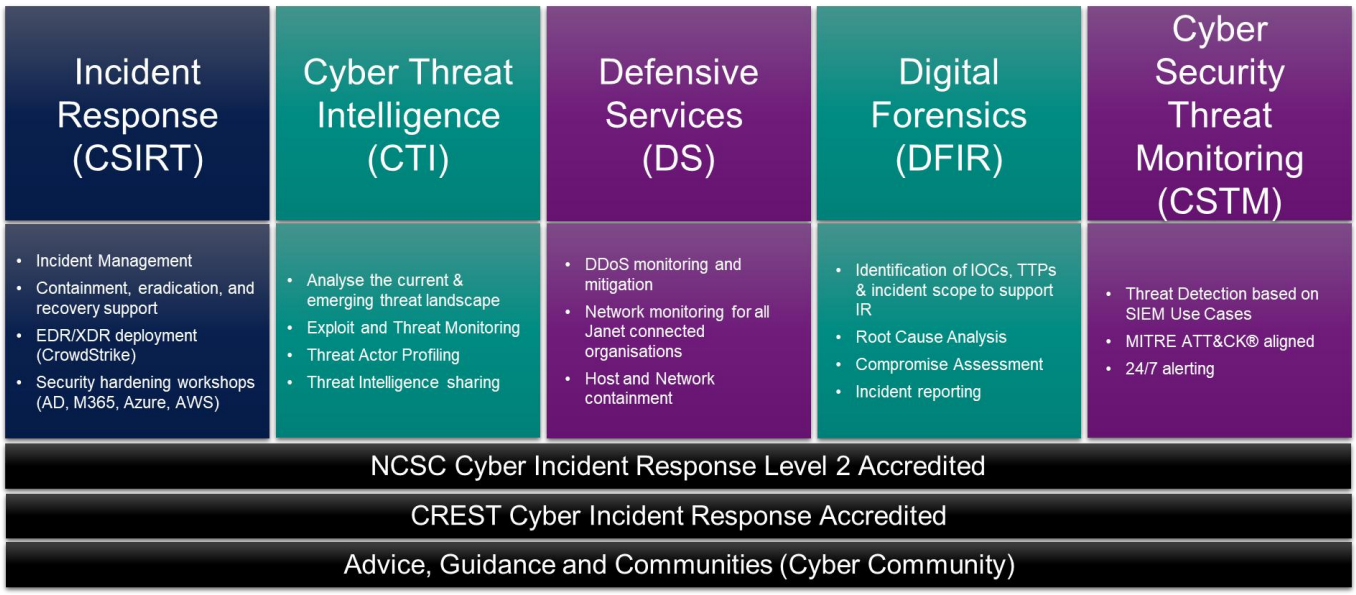
As part of the live service, you will also receive access to a private SOC dashboard, providing visibility of alerts, incidents, and reporting specific to your organisation. In addition, you will have access to the Cyber Hub, a central hub for all Jisc services, offering a single point of access to data, reporting, service updates, and guidance.

The Hypercare period will last for one month and will be followed by a one-month service review. Thereafter, service reviews will take place on a quarterly basis to ensure ongoing alignment, performance, and continuous improvement.

Within the first three months of live service, we will carry out a Security Posture Assessment as part of the SOC offering. This provides a high-level view of your organisation's cyber security maturity, aligned to recognised best-practice frameworks including the CIS Critical Security Controls, Cyber Essentials, and the NCSC 10 Steps to Cyber Security.

The assessment identifies strengths, gaps and priority improvement areas, helping to focus security effort where it delivers the most value. It is repeated annually, enabling you to track progress year on year, demonstrate maturity improvements, and continually strengthen your security posture in response to evolving threats.

4. Capabilities



Jisc SOC Capabilities

Jisc Level 1 and Level 2 analysts will contain genuine causes for concern from false alarms based upon a pre-agree containment strategy with the customer. Where necessary there will be automatic escalation to a Level 3 Security Operations Lead.

4.1 Security Information and Event Management (SIEM)

Using our Security Incident and Event Management (SIEM) tool CSTM, Jisc will aggregate and analyse log data from various sources. This combines the enrichment data from your EDR/XDR console with other logs sources such as Firewalls, Remote Access and Hypervisor solutions which may not have EDR/XDR agents deployed to detect and identify potential security incidents.

4.2 Manage Detect and Response (MDR)

A core component of our Security Operations Centre (SOC) is the management of your EDR/XDR tools (Defender XDR or CrowdStrike) through monitoring of your EDR/XDR host agents. Alert and incident data will be ingested into our CSTM service (Splunk) combined with other Indicators of Compromise (IOCs) to help detect and contain any potential threat.

4.3 Cyber Threat Intelligence

Jisc's Cyber Threat Intelligence (CTI) team identifies, analyses and disseminates the intelligence that underpins all of Jisc's cyber security activities. In addition, the team works closely with Jisc's incident response and defensive services teams, responsible for DDoS mitigation and defence of the Janet Network.

Using in-house expertise and commercial and open-source services, threats and vulnerabilities impacting education and research are monitored and tracked. We work closely with institutions, national agencies and international partners to share actionable threat intelligence to help protect the Janet Network and connected organisations.

- Dark web monitoring
- Vulnerability Intelligence through the Jisc Cyber Community
- Sharing Indicators of Compromise (IOCs) through our MISP platform and monthly/quarterly threat intelligence reports shared through the Jisc Cyber Community
- Provide actionable recommendations

4.4 Threat Hunting

Jisc's highly skilled threat hunters will proactively identify and mitigate potential security threats that may have evaded traditional security tools, using Tactics, Techniques and Procedures (TTPs), and Indicators of Compromise (IOCs) collected through threat intelligence, including incidents seen across the education sector to search for and mitigate any identified threats before they escalate into an incident.

4.5 Effectiveness Testing

To ensure a continuous improvement process, Jisc's Security Operations Centre (SOC) service will perform periodic efficiency testing of the people, processes and technology that makes up the SOC service, including Red Team / Blue Team testing to ensure the system can detect common Tactics, Techniques, and Procedures (TTPs).

4.6 Cyber Incident Response (CIR)

Included with Jisc's Security Operations Centre (SOC) is access to a highly skilled Cyber Incident Response Team (CSIRT), which includes:

- Full cyber incident management support from basic phishing campaigns to major cyber incidents such as Ransomware
- Applied Threat Intelligence to support the management of incidents
- EDR (Endpoint Detect and Response) deployment within 24 hours of engagement
- Digital Forensic investigation / analysis
- Malware analysis

- Further information on our NCSC assured capabilities can be shown here Cyber Incident Response (CIR) Technical Standard (Level 2) v1.5 (ncsc.gov.uk)