Security Operations Centre

G-Cloud Service Definition

Table of contents

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 Security Operations Centre (SOC) service to support our customers to protect, detect, respond and recover from cyber incidents. The Jisc Security Operations Centre (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 Managed 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 Security Operations Centre (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 SOC offering includes enhancements to the existing cyber security membership benefits (Incident Response, Cyber Threat Intelligence, Janet Network protections, etc) combined with Jisc’s SIEM, Cyber Security Threat Monitoring (CSTM) service as the foundation. Layering additional security services, such as MDR (Managed Detect and Respond) and vulnerability management to provide a sector leading Security Operations Centre (SOC) that supports customers to Protect, Detect, Respond and Recover from cyber incidents.

2 Service Description

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 Security Operations Centre (SOC) service, the following eligibility criteria must be met:

- **Janet Network Connection**: Customers wishing to purchase Jisc's Security Operations Centre (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.

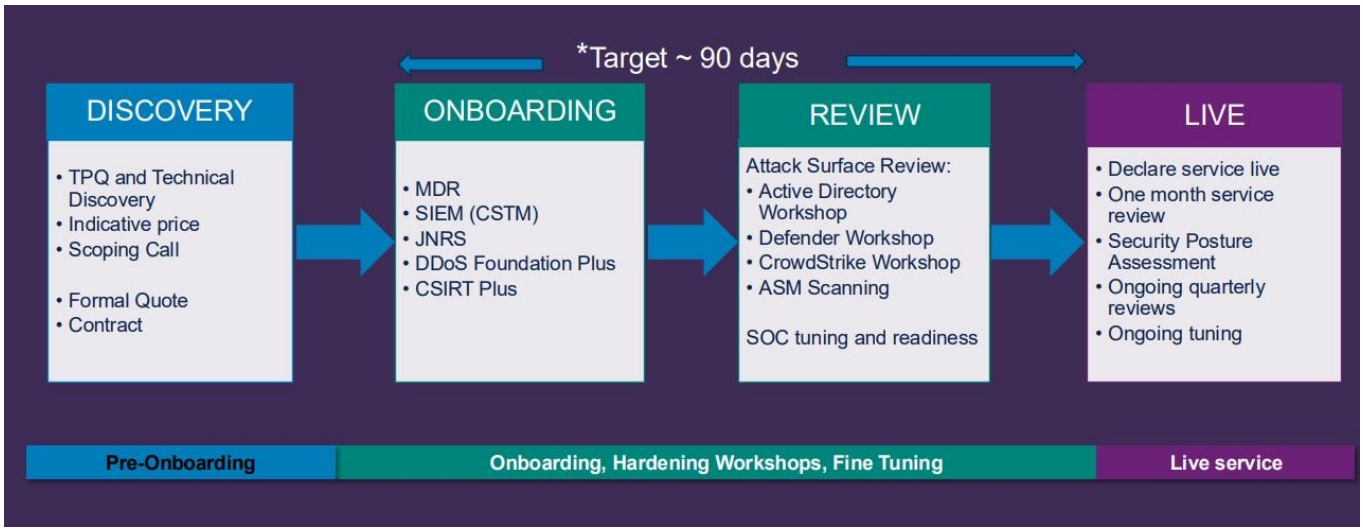
2.4 Information Assurance

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 assess the customers existing base security posture through a 'pre-onboarding' self-assessment questionnaire based upon CIS (Centre for Internet Security) controls, to ensure basic security controls are applied to reduce the risk of compromise, any non-conformities to the assessment will be worked on with the member prior to onboarding to 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 CrowdStrike and/or Defender 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

As part of the Security Operations (SOC) service deployment process, Jisc will ensure your existing EDR tools (CrowdStrike or Defender XDR) are fully configured and provide advice and guidance on security hardening your Cloud and On-Prem infrastructure, including Active Directory.

3.3 Review Phase

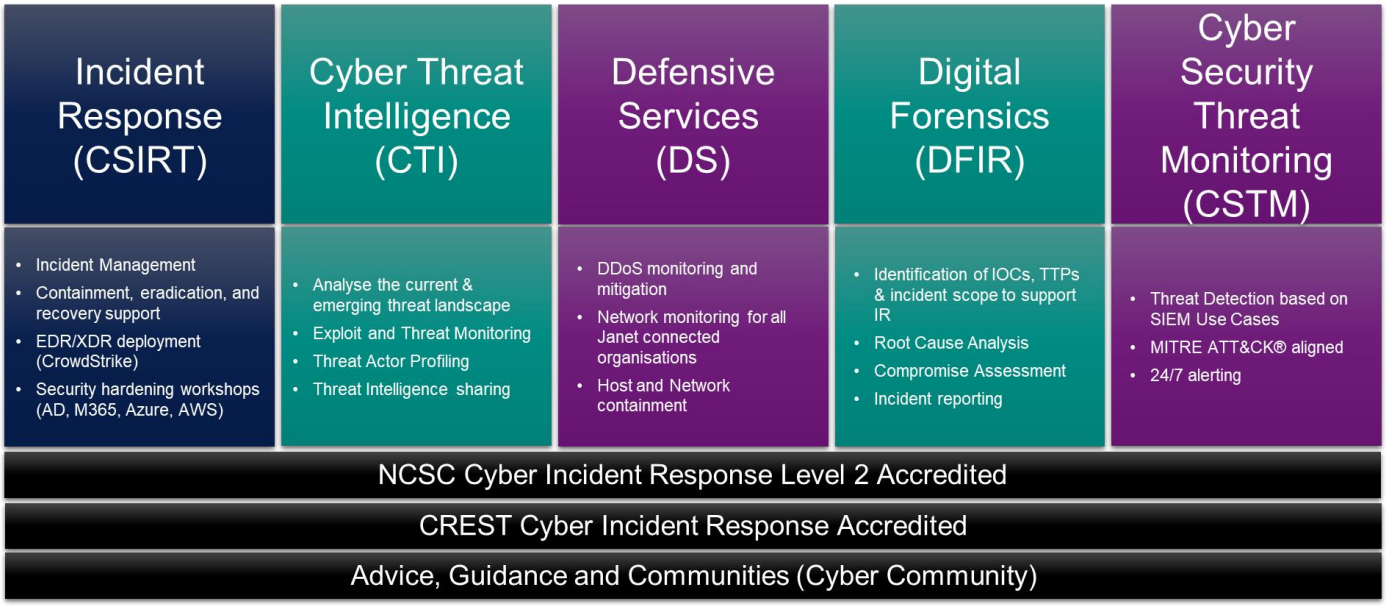
3.3.1 Monitoring and Baselining

Once data sources begin to flow into the Security Operations Centre (SOC) and EDR/XDR, tools are configured to based practice, robust monitoring practices and accurate baselining of normal behaviour will be established. 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.

3.4 Service Live State

Following an initial service initialisation meeting and confirmation that all services are online, the Security Operations Centre (SOC) will move into a live state.

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 & 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 (CTI)

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 Network Protection

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 Managed Security Service Providers. Network Protection services included within Jisc membership and enhanced through the Security Operations Centre (SOC) include:

  - **Foundation Plus DDoS mitigation service:** Round the clock protection against DDoS attacks on your Janet connection
  - **Primary Name Service (PNS):** Our service allows you to publish and manage DNS records on a central nameserver through a secure web portal. It is supported by secondary nameservers to provide high availability and gives that added peace of mind. This helps maintain business continuity, including web presence and email, even if your internet connection is down following a ransomware attack or other issue.
- **Protective DNS (Jisc PDNS):** The service includes feeds from National Cyber Security Centre (NCSC) and other security researchers 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 is able to adapt to emerging threats.

4.6 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).

4.7 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)

5 Additional Security Services

Jisc is a trusted technology advisor and ally of the Further Education (FE), Higher Education (HE), Research and public sectors. We provide best-in-class security advice, engineering and support and work as part of your team to transfer knowledge at every step. As a not-for-profit membership organisation, we are an allied technology partner, and we reinvest our profits back into the communities we earn them in.

Together, our associated security services provide a full suite to support you on your cyber security programme from start to finish. They can be taken in sequence to support your entire cyber security journey or selected as needed to enhance just those parts of your programme where you need support.

5.1 Critical Services Protection

Critical services protection adds an additional layer of defence to help you 'keep the lights on' and maintain business continuity. By choosing critical services protection, you can show you're doing what you can to maintain access to business-critical services, helping you to maintain your organisation's reputation and protect the bottom line.

5.2 Cyber Essentials

When getting certification, you want to work with a trusted certification body who understands the needs of your sector. In response to demand, we offer Cyber Essentials and Cyber Essentials Plus as a service. Use this to obtain a Cyber Essentials certificate and to get the essential advice and guidance you need.

5.3 Cyber Security Assessment

The cyber security assessment service: a tailored, cost-effective process to help you meet audit and compliance needs. The service helps you to evaluate, analyse and improve your security posture, on a one-off or ongoing basis, according to your needs.

All work is carried out by our in-house cyber security experts -– who are experienced, trained and certified. And because it's a tailored service, we are able to scope the work to your exact requirements. That makes it cost-effective for you.

5.4 Penetration testing

We offer a CREST-accredited penetration testing service, which helps you identify vulnerabilities, assess risks, and take corrective action, all at a cost-effective daily rate. All work is carried out by our in-house cyber security experts, who are experienced, trained, and certified.

This service is provided on a time-bound or scope-bound basis, so you only pay for the days you need. This means it's cost-effective for you and can be adapted to your needs and budget.

5.5 IT Health Check

As a CREST-accredited organisation, we offer a comprehensive ITHC service which comprises a series of controlled vulnerability scans and security control checks, designed to deliberately identify and expose security vulnerabilities that might be present in your IT environment.