Cyber Security Threat Monitoring

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.

This was made explicit in the NCSC Annual Review 2025, which states: “Cybersecurity is now a matter of business survival and national resilience.” Jisc's Cyber Security Threat Monitoring (CSTM) is a specialised managed SIEM service exclusively for UK education and research institutions, delivering 24/7 threat detection with expert human analysis during core business hours and intelligent automation outside these times.

As the Internet Service Provider for the Janet Network, Jisc provides unmatched sector-wide visibility across hundreds of UK universities and colleges. This unique position enables CSTM to detect education-specific threats—including admissions phishing, research ransomware, and credential attacks—using real-time intelligence that generic SIEM providers cannot access.

CSTM centralises security telemetry collection using Splunk technology from network infrastructure, servers, cloud platforms (Microsoft 365, Azure (Entra), EDR, and security solutions, correlating events to identify genuine threats while filtering out noise. Advanced analytics and risk-based alerting reduce alert fatigue, enabling your team to focus on real security issues rather than false positives.

Key differentiators: Sector-specialist analysts who understand term-time patterns and research collaboration risks; Janet network threat intelligence from across UK education; fully supported onboarding at no extra cost; seamless integration with existing security tools and Jisc's SOC and CSIRT services; 90-day event retention with self-service dashboard.

Ideal for: Higher and further education institutions and research organisations seeking to enhance cyber resilience, meet compliance obligations (GDPR, Cyber Essentials, cyber insurance), protect sensitive student and research data, and demonstrate proactive risk management to boards and regulators—without the cost and complexity of building in-house 24/7 security operations.

Assured delivery: ISO27001 and Cyber Essentials certified, NCSC CIR Level 2 assured incident response, CREST accredited penetration testing expertise. As a not-for-profit membership organisation, Jisc reinvests all profits into the education and research community.

Please note: A Janet IP connection is mandatory for this service. Technical discovery and scoping are required prior to quoting and onboarding.

2. Service Description

2.1 What CSTM Does

CSTM provides continuous security monitoring and threat detection through a unified platform using Splunk technology that correlates security events across your entire infrastructure. Think of it as having expert security analysts watching your systems around the clock—automatically detecting attack patterns and alerting you to genuine threats, not noise.

The service integrates with your existing security tools (firewalls, endpoint protection, authentication systems, cloud platforms) to provide complete visibility across your digital estate. By correlating events that would otherwise appear unrelated, CSTM identifies multi-stage attacks and suspicious patterns that single-point solutions miss.

2.1.1 Service Delivery Model

- Core hours (8am-6pm, Mon-Fri): Skilled security analysts actively monitor alerts, triage events, filter false positives, and contact you about genuine threats
- Outside core hours (24/7/365): Fully automated monitoring with phone alerts for critical issues requiring immediate attention
- Response times: 1-hour response for critical alerts during working hours; 2-hour response during on-call hours

2.2 Supported Data Sources

CSTM integrates with your existing security infrastructure through flexible log ingestion, supporting both on-premise and cloud environments without requiring technology replacement.

You will find a list of the data sources that Jisc currently supports below:

Description	Splunk Marketplace App	Ingest Method
Cisco ASA firewalls	Cisco ASA (Splunk LLC)	Syslog
FortiGate firewalls	Fortinet FortiGate App (Fortinet Inc)	Syslog
Palo Alto firewalls	Palo Alto Networks (Palo Alto Networks)	Syslog
Sophos XG firewalls	Sophos XG (Sophos Integrations)	Syslog
CrowdStrike EDR	CrowdStrike Falcon (CrowdStrike)	Cloud API
Sophos EDR	Sophos Central (Sophos Integrations)	Cloud API
Microsoft Defender	Microsoft Security (Splunkworks)	Cloud API
Office 365 audit logs	Microsoft 365 (Splunkworks)	Cloud API
Azure/Entra audit logs, users, sign-ins, devices, groups, risk	Microsoft Azure (Splunkworks)	Cloud API
Windows event logs	Microsoft Windows (Splunk LLC)	Splunk Universal Forwarder
Unix/Linux event logs	Unix and Linux (Splunk LLC)	Splunk Universal Forwarder

2.2.1 Data Handling

- Retention: 90 days of event data for forensic investigation and compliance
- Sovereignty: All data stored and processed in UK data centres only
- Scalability: Supports institutions from 1,000 to 100,000+ users; pricing based on daily ingestion volume

2.2.2 Integration Support

- Jisc provides full technical guidance during onboarding for:
    - Configuring log sources and forwarding
    - Parsing custom log formats
    - Testing and validation
    - Adding new sources as your environment evolves

2.2.3 Compatibility Questions?

If you have specific data sources not listed, Jisc will assess feasibility during the discovery and scoping phase and throughout live service. Our engineering team will assess integration requirements and provide guidance on optimising log collection for your infrastructure.

2.3 How Detection Works

CSTM employs intelligent, risk-based alerting that distinguishes between isolated events and coordinated attacks:

Notable alerts trigger immediately when high-confidence threats are detected—such as a successful brute force attack gaining system access, or malware execution on endpoints.

Risk-scoring rules track cumulative suspicious behaviour across your infrastructure. Like tracking an intruder's movements around a property, individual actions might seem innocuous, but together they indicate a threat. When cumulative risk exceeds defined thresholds (typically 100 points), an alert triggers for investigation.

This approach dramatically reduces alert fatigue—your team sees genuine threats requiring action, not hundreds of low-level events requiring manual correlation.

Alert categorisation:

- Critical: Active threat requiring immediate investigation and response (phone call for high-confidence IOC + email)
- High: Significant security event requiring prompt investigation (email, 1-hour response)
- Medium: Suspicious activity requiring review (email, 2-hour response)
- Low/Info: Contextual information for awareness (scheduled reports)

2.4 What We Monitor

CSTM detection rules focus on three critical security domains where most breaches occur:

Access Security – We monitor authentication systems to detect and block unauthorised entry:

- Failed login attempts and successful brute force attacks
- Impossible travel (logins from geographically impossible locations within timeframes)
- Suspicious authentication patterns and credential stuffing attacks
- VPN and remote access anomalies
- After-hours access to sensitive systems

Endpoint Security – Inside your infrastructure, we detect attacker behaviour and system compromise:

- Security log clearance and tampering (covering tracks)
- Suspicious PowerShell usage and script execution
- System reconnaissance and network scanning
- Shadow copy deletion (ransomware precursor)
- Unusual process execution and privilege escalation
- Lateral movement between systems

Identity Security – We protect high-privilege accounts and critical access controls:

- Account takeovers and compromised credentials
- Unauthorised changes to security groups and permissions
- MFA modifications and authentication policy changes
- Service account abuse
- Privilege escalation attempts
- Creation of new administrative accounts

Data sources monitored:

- Network devices (firewalls, VPNs)
- Server infrastructure (Windows, Linux)
- Cloud platforms (Microsoft 365, Azure)

- Security solutions (EDR, endpoint protection, email security)
- Applications and databases
- Janet Network telemetry (unique sector-wide visibility)

2.5 Why Risk-Based Alerting Prevents Breaches

Traditional SIEM solutions generate thousands of alerts, overwhelming security teams and causing critical threats to be missed in the noise. CSTM's risk-based approach prevents breaches through:

Smarter threat detection – Automatically correlating events across multiple systems to identify attack patterns, not just isolated incidents. A failed login attempt alone is not concerning; 50 failed attempts followed by a successful login from an unusual location indicates compromise.

Operational efficiency – Your team focuses on investigating real threats rather than triaging false positives.

Adaptive security – Risk scores dynamically adjust based on context. A failed login during term time might score 2 points; the same event at 3am during vacation might score 10 points. User behaviour, time of day, location, and asset criticality all factor into risk calculations.

Pattern recognition – The correlation engine links related events across time and systems. Actions separated by hours or days that together indicate reconnaissance, credential theft, and data exfiltration are identified as a coordinated attack.

Education-specific tuning – Rules account for sector behaviours: research collaboration traffic patterns, student lifecycle activities (enrolments, graduations), term-time vs. vacation patterns, and international research partnerships.

By analysing potential breaches holistically rather than as discrete events, CSTM strengthens your defences and allows your organisation to prioritise resources effectively.

2.6 Service Requirements

Mandatory requirements:

- Active Janet IP connection (CSTM cannot be provided without Janet Network connectivity)
- Technical discovery and scoping to assess your environment and data ingestion requirements
- Designated technical contacts for onboarding and ongoing operations
- Asset and identity information for your domain(s) (servers, critical systems, privileged accounts)

Technical prerequisites:

- Network devices, servers, and applications capable of generating and forwarding security logs
- Appropriate network connectivity and firewall rules for log transmission
- Administrative access to configure log forwarding from existing security tools

Commitment requirements:

- Participation in onboarding process (approximately 4-6 weeks, depending on complexity)
- Response to alerts and incidents as appropriate for your organisation
- Notification of infrastructure changes that may affect monitoring coverage

- Notification of key contact changes
- Quarterly service review participation

2.7 Service Management

Jisc provides CSTM according to ITIL Service Management best practices, including defined incident management and change management procedures, monthly reporting, and quarterly service reviews.

Service Desk and Customer Contact: Jisc provides telephone and email service desk support during core hours (8am-6pm, Monday to Friday, excluding UK public holidays) for logging service requests, change requests, and general queries. Email: cstm@jisc.ac.uk

Service Reviews: Quarterly Service Review Meetings discuss service performance, detection rule effectiveness, emerging threats, recommended improvements, and any enhancements relating to your evolving environment.

Service Level Agreements:

Severity	Response Type	Contact Method	Core Working Hours SLA (8am-6pm Mon-Fri)	On-Call Hours SLA
Critical	Investigation	Phone call and email	1-hour response time, one phone call and email for high-confidence critical alerts	2-hour response time, one phone call and email for high-confidence critical alerts
High	Investigation	Email	1-hour response time	Automated notification
Medium	Incident checked and resolved	Email	2-hour response time	Automated notification
Low	None	Email	Scheduled report	Scheduled report
Info	None	Email	Scheduled report	Scheduled report

What each severity means:

- Critical: Active breach, successful system compromise, ransomware execution, data exfiltration in progress
- High: High-probability threat requiring investigation (successful brute force, account takeover, malware detection)
- Medium: Suspicious activity requiring review (unusual access patterns, reconnaissance attempts)
- Low: Security events for awareness (policy violations, configuration issues)
- Info: Contextual information for trend analysis and reporting

Hypercare period: Following go-live, you receive one month of intensive hypercare support with close monitoring of alert flows, integration validation, and rapid tuning. A formal service review follows at the end of hypercare, then quarterly thereafter.

2.7 Information Assurance

Jisc maintains the following certifications and assurances for CSTM service delivery:

- ISO 27001 certified information security management
- Cyber Essentials Plus certified
- NCSC Cyber Incident Response (CIR) Level 2 assured CSIRT team
- CREST accredited security testing and incident response capabilities
- Compliance with Cabinet Office Security Policy Framework (SPF)
- Adherence to NCSC guidelines including handling of UK OFFICIAL classified information
- Data Protection Act (DPA) and GDPR compliant data processing
- Appropriate staff security clearances and background checks
- Secure management infrastructure and network connectivity

All customer data is processed and stored in accordance with UK data protection legislation. Security logs and telemetry remain your property; Jisc acts as a data processor under GDPR.

2.8 Service Pricing

Pricing for CSTM is based on daily data ingestion volumes and the complexity of your environment. Detailed pricing is provided in the separate G-Cloud 15 pricing document. Contact Jisc for a tailored quote following technical discovery and scoping.

3. Service Features

3.1 Monitoring and Analysis Capabilities

Expert human oversight:

- Skilled security analysts monitoring and triaging alerts during core hours (8am-6pm)
- False positive filtering and threat validation before customer notification
- Investigation support and guidance on appropriate response actions
- Escalation to CSIRT for incident response during working hours

24/7 automated monitoring:

- Continuous threat detection outside core hours (evenings, nights, weekends)
- Phone alerts for critical threats requiring immediate attention
- Automated correlation and risk scoring around the clock
- Event logging and retention for next-day analysis

Advanced detection techniques:

- Correlation engine linking related events across multiple systems and timeframes
- Baseline behaviour modelling to detect anomalous activity specific to your environment
- Machine learning-assisted anomaly detection
- Education-specific attack pattern recognition
- Multi-stage attack identification (kill chain analysis)

3.2 Data Collection and Integration

Comprehensive log ingestion:
- Hybrid environment support: on-premise servers and cloud platforms
- Microsoft 365, Azure
- Network devices: firewalls, VPNs
- Security solutions: EDR, endpoint protection, email security, web gateways
- Server infrastructure: Windows Event Logs, Linux syslogs, authentication services
- Applications and databases
- Janet Network telemetry (unique sector-wide threat visibility)

Flexible integration:
- Works with your existing security stack—no rip-and-replace required
- Support for common log formats: Syslog, Windows Event Log
- 90-day retention of all logged events for forensic investigation and trend analysis

4. Service Benefits

4.1 Sector Expertise You Cannot Get Elsewhere

As the Internet Service Provider for the Janet Network, Jisc occupies a unique position in UK education and research security. Our analysts benefit from:

Network-level visibility: Real-time threat intelligence from across hundreds of universities and colleges. When a phishing campaign targets Cambridge, we detect and protect Manchester within hours. Generic SIEM providers simply cannot match this sector-wide awareness.

Education-specific knowledge: Our analysts understand term-time patterns, research collaboration traffic, student lifecycle activities, and the unique operational rhythms of academic institutions. We distinguish between legitimate collaboration and data exfiltration because we know how education works.

Peer community intelligence: Anonymised threat sharing means your institution benefits from lessons learned across the entire sector. Emerging threats are identified and countered collectively, not institution by institution.

Attack vector recognition: We detect common threats specific to education—admissions phishing, portal credential attacks, research data ransomware, supply chain attacks on education technology vendors—because we see these patterns repeatedly across our customer base.

4.2 Operational Efficiency and Cost Savings

Reclaim your team's time: Stop spending 60-80% of security staff time on alert triage and false positive investigation. CSTM filters the noise, allowing your team to focus on strategic security improvements, user education, and proactive threat hunting.

Avoid in-house SIEM complexity: Building and maintaining SIEM infrastructure requires significant investment: software licenses (£50k-£200k annually), dedicated security staff (3-5 FTEs for 24/7

coverage), ongoing training, and continuous rule tuning. CSTM delivers these capabilities at a fraction of the cost.

Scale without proportional staffing increases: As your institution adopts cloud services, expands research infrastructure, and increases digital operations, CSTM scales with you. No need to hire additional security analysts for each new service.

Leverage expert resources: Access NCSC-assured and CREST-accredited security specialists without the recruitment challenges and salary costs of building this expertise in-house. Average time to hire cybersecurity professionals: 6-9 months. CSTM provides immediate access.

Future-proof investment: Build the foundation for mature security operations. CSTM establishes the logging, correlation, and detection capabilities needed for future SOC services, protecting your investment as your program evolves.

4.3 Risk Reduction and Protection

Avoid catastrophic breach costs: UK education sector breaches average £1.2M-£4.5M in remediation, recovery, regulatory fines, and reputational damage. CSTM's early detection minimises dwell time (average: 21 days industry-wide; under 4 hours with CSTM), dramatically reducing potential damage.

Stop education-targeted attacks: Research institutions face 3x more sophisticated attacks than commercial organisations. CSTM specifically detects admissions phishing, student portal attacks, research data ransomware, and intellectual property theft attempts common in our sector.

Protect research integrity: Nation-state actors and industrial espionage specifically target UK research. CSTM identifies reconnaissance, credential theft, and data exfiltration patterns associated with advanced persistent threats (APTs) targeting research data.

Safeguard student data and institutional reputation: Student data breaches erode trust, trigger regulatory action, and damage enrolment. CSTM helps maintain the data protection standards students, parents, and regulators expect.

Faster detection equals lower impact: Industry average time to detect breaches: 204 days. CSTM's continuous monitoring and expert analysis reduces this to hours, helping you to contain threats before they escalate.

4.4 Peace of Mind

Sleep soundly knowing you're covered: Critical threats trigger phone alerts even at 3am. You'll be notified when it matters, without maintaining 24/7 staff rotas or on-call schedules that burn out your team.

Expert backup when threats are real: During working hours, you have immediate access to CSIRT specialists who can guide response, contain incidents, and coordinate with law enforcement if needed. You're not alone in a crisis.

Board-level confidence: Provide governors and senior leadership with tangible evidence of proactive risk management: threat metrics, detection statistics, incident response times. Demonstrate security investment effectiveness with concrete data.

Safe digital transformation: Confidently adopt cloud services, enable flexible working, and support digital learning knowing that CSTM provides visibility across your expanding attack surface.

Student and staff trust: Demonstrate to your community that you take data protection seriously. CSTM shows you're actively monitoring for and defending against threats to personal and research data.

4.5 Visibility and Understanding

See what you've been missing: Most institutions discover they had security gaps only after a breach. CSTM reveals the threats already targeting you—the reconnaissance, credential attacks, and reconnaissance attempts you never knew existed.

Understand real risks, not assumed risks: Your threat model assumptions may not match reality. CSTM shows where attackers focus, which assets they target, and which vulnerabilities they exploit. Make evidence-based security decisions.

Dashboard visibility for all stakeholders: Within the CSTM platform, IT managers get operational metrics; security analysts get investigation tools; executives get risk summaries. Everyone sees what they need.

Transform from reactive to proactive: Stop learning about threats from incident reports or forensic investigations. CSTM provides the situational awareness needed to anticipate, prevent, and prepare for attacks before they succeed.

4.6 Compliance and Assurance

Demonstrate compliance effortlessly: CSTM provides the logging, monitoring, and incident detection evidence required for Cyber Essentials certification, GDPR compliance, regulatory audits, and governance reporting. Evidence is automatically collected and available on demand.

Meet cyber insurance requirements: Insurers increasingly require security monitoring and rapid detection capabilities. CSTM demonstrates you have controls in place, potentially reducing premiums and ensuring faster claims processing.

Reduce regulatory risk exposure: GDPR fines for data breaches can reach £17.5M or 4% of global turnover. Early detection and rapid containment demonstrate "appropriate technical measures," significantly reducing penalty risk.

Support research funding requirements: Major funders (UKRI, Wellcome Trust, EU Horizon) require data protection assurances. CSTM provides evidence of security controls protecting research data and intellectual property.

Faster incident response documentation: If a breach occurs, CSTM's detailed logging and timeline reconstruction dramatically accelerates incident reporting to ICO (required within 72 hours) and provides the evidence needed for cyber insurance claims.

Audit trail for investigations: Complete forensic timeline of security events supports internal investigations, regulatory inquiries, and law enforcement cooperation if required.

4.7 Growth and Continuous Improvement

Get smarter over time: CSTM continuously refines detection rules based on your environment. As we learn your normal behaviours, detection becomes more accurate and false positives decrease. Your service improves automatically.

Career development for your team: Working alongside professional security operations exposes your staff to advanced investigation techniques, threat intelligence analysis, and incident response procedures. Your team develops skills they couldn't gain in-house.

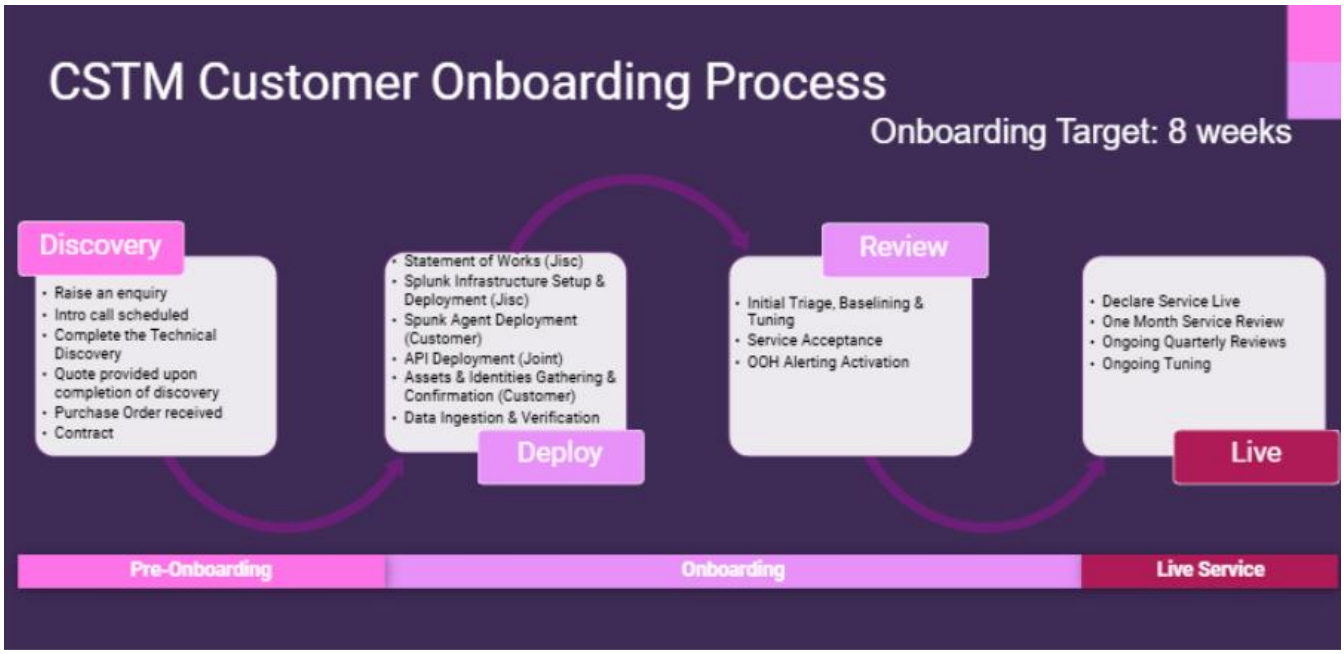
Support digital transformation initiatives: Enable secure adoption of cloud services (Microsoft 365, Azure), flexible working arrangements, international research collaboration, and modern infrastructure without creating security blind spots.

Enable confident innovation: Launch new online services, expand digital research infrastructure, and adopt emerging technologies knowing CSTM will detect if these initiatives introduce vulnerabilities or attract attacker attention.

Foundation for security programme maturity: CSTM establishes the logging infrastructure, detection capabilities, and operational processes needed as your security program matures toward full SOC capabilities, managed detection and response (MDR), or threat hunting services.

Investment protection: As a not-for-profit membership organisation, Jisc reinvests profits into service improvements that benefit the entire education community. Your fees fund better detection, threat intelligence, and capabilities for everyone.

5. Service Operation



5.1 Discovery Phase

Before onboarding, Jisc conducts a thorough assessment of your environment to ensure CSTM is configured optimally for your institution.

Technical discovery: Upon enquiry, you will complete a Technical Discovery document providing:

- Network architecture overview and topology
- Key assets requiring monitoring (servers, databases, critical applications)
- Existing security infrastructure (firewalls, EDR, endpoint protection, logging)
- Cloud services in use (Microsoft 365, Azure)
- Current threat concerns and security priorities
- Approximate user and device counts

Scoping session: Jisc engineers will review your technical requirements in a scoping call to:

- Identify specific data ingestion sources and estimated daily volumes
- Understand your EDR/XDR deployment and integration requirements
- Discuss critical assets and privileged identities for priority alerting
- Explain how CSTM prioritises assets (critical/high/medium) for risk scoring
- Assess network connectivity and log forwarding requirements
- Estimate onboarding timeline based on environment complexity

Quotation: Based on discovery findings, Jisc provides a tailored quote reflecting your expected daily data ingestion volumes and service requirements. Target onboarding timeframe: 8 weeks from Statement of Works approval.

5.2 Deployment Phase

Onboarding process: CSTM onboarding follows an incremental approach, configuring and ingesting log sources progressively to ensure quality and accuracy.

Step 1: Kick-off and Statement of Works
Joint call introducing Jisc engineering team and your technical contacts
Review detailed Statement of Works prepared by Jisc engineers
Outline onboarding process, timelines, and responsibilities
Address technical questions and finalise configuration plan

Step 2: Configuration
Both teams complete configuration tasks outlined in Statement of Works
Your team: Configure log forwarding from security tools, servers, network devices
Jisc team: Configure CSTM to receive and parse your log sources
Jisc engineers provide technical support throughout configuration
Progressive testing as each log source comes online

Step 3: Tuning and Baselining
- CSTM analysts monitor initial alerts and establish behavioural baselines
- Analysis of what "normal" looks like in your environment
- Scheduled calls between your team and Jisc analysts to fine-tune detection rules
- Adjustment of risk thresholds and alert severity levels

- Suppression of known-safe activities and false positive patterns
- Validation that critical threats generate appropriate alerts

Step 4: Service Sign-off
- Internal Jisc readiness review across engineering, analyst, and CSIRT teams
- Confirmation that all log sources are ingesting correctly
- Validation that alerting and escalation workflows function properly
- Final tuning adjustments based on initial monitoring period
- Preparation of service welcome documentation

Step 5: Go-Live
- Final call to review service welcome documentation and operational procedures
- Formal confirmation of go-live date
- Transition to Hypercare support period (one-month intensive monitoring)
- You receive access to CSTM dashboard and Cyber Hub portal
- Alert notifications begin flowing to designated contacts

Target timeline: 8 weeks depending on environment complexity and number of log sources. More complex environments with extensive cloud integration or delays on the customer side may take longer.

5.3 Live Service Operations

Hypercare period (First month): Following go-live, you receive intensive support:
- Close monitoring of alert flows and investigation quality
- Validation that all integrations function as expected
- Rapid response to questions via dedicated email: cstm@jisc.ac.uk
- Additional tuning based on live operational experience
- Weekly check-ins during first month

One-month review: Formal service review following Hypercare covers:
- Alert volumes and types detected
- False positive rates and tuning effectiveness
- Detection coverage assessment
- Recommendations for optimisation
- Transition to quarterly review schedule

Ongoing operations:
- Alert notifications: Critical/High/Medium alerts sent via email (and phone for Critical)
- Dashboard access: Self-service portal for security visibility and investigation
- Cyber Hub access: Central hub for all Jisc services, documentation, and guidance
- Service desk support: cstm@jisc.ac.uk during core hours (8am-6pm Mon-Fri)
- Monthly reporting: Security metrics, threat trends, detection statistics
- Quarterly reviews: Service performance, emerging threats, optimisation recommendations

Continuous improvement: CSTM continuously evolves based on:
- Your environment changes (new infrastructure, cloud services)
- Emerging threat landscape and attack techniques
- Lessons learned from incidents across Janet Network

- Feedback from quarterly service reviews
- New detection capabilities and threat intelligence

5.4 Customer Responsibilities

To ensure CSTM operates effectively, customers are responsible for:

During onboarding:
- Completing Technical Discovery document accurately and thoroughly
- Providing asset and identity information (critical servers, privileged accounts, key systems)
- Designating technical contacts for configuration support
- Completing configuration tasks outlined in Statement of Works
- Providing network access and administrative credentials as needed for log forwarding setup
- Participating in tuning calls and providing feedback on alert accuracy

Ongoing operations:
- Respond to alerts appropriately: Investigate, contain, or escalate based on alert severity and guidance provided
- Report infrastructure changes: Notify Jisc of significant changes (new servers, network topology modifications, cloud service adoption) to maintain monitoring coverage
- Participate in service reviews: Quarterly meetings to discuss performance and optimisation
- Engage CSIRT when needed: For active incidents requiring expert incident response support
- Maintain log source configuration: Ensure log forwarding continues functioning; troubleshoot connectivity issues with Jisc support

Best practices:
- Designate a primary CSTM contact within your IT/security team
- Establish internal procedures for alert triage and response
- Document your response actions for incidents detected by CSTM
- Review dashboard regularly to understand your threat landscape
- Provide feedback on false positives to improve tuning

5.5 Support and Escalation

Service Desk:
- Email: cstm@jisc.ac.uk
- Hours: 8am-6pm Monday to Friday (excluding UK public holidays)
- Purpose: Service requests, change requests, technical support, general queries

Alert escalation:
- Critical alerts: Phone call for high-confidence critical alerts and email during all hours
- High alerts: Email notification, 1-hour response during working hours
- Medium alerts: Email notification, 2-hour response during working hours

Incident response:
- During working hours: Direct escalation to CSIRT available
- NCSC CIR Level 2 assured incident response capabilities
- Coordination with other Jisc security services (SOC, DDoS protection)

Technical support:

- Log source integration assistance
- Dashboard and reporting guidance
- Alert interpretation and investigation support
- Configuration change support

6. Information Assurance and Compliance

6.1 Certifications and Assurance

Jisc maintains comprehensive security certifications and assurances for CSTM service delivery:

- ISO 27001:2013 – Certified information security management system (ISMS) covering all aspects of CSTM service delivery, infrastructure, and data handling.
- Cyber Essentials Plus – Government-backed certification demonstrating technical controls against common cyber attacks. Annual re-certification ensures ongoing compliance.
- NCSC Cyber Incident Response (CIR) Level 2 – Jisc's CSIRT team holds the highest level of NCSC incident response assurance, demonstrating capability to handle sophisticated incidents and nation-state threats.
- CREST Accreditation – Our security specialists hold CREST accreditation for penetration testing and incident response, ensuring professional standards and continuous professional development.
- Cabinet Office Security Policy Framework (SPF) – CSTM complies with government security policy requirements for handling sensitive information.
- NCSC Guidelines – Service delivery follows NCSC best practices including handling of UK OFFICIAL classified information where required.

6.2 Data Protection and Privacy

GDPR and DPA compliance:
- All data processing complies with UK GDPR and Data Protection Act 2018
- Jisc acts as Data Processor; customer remains Data Controller
- Data Processing Agreement (DPA) provided detailing processing activities and safeguards
- Security logs and telemetry remain customer property
- Data retention: 90 days within the CSTM platform; deletion upon service termination

Data security measures:
- Encryption in transit (TLS 1.2+) for all log transmission
- Encryption at rest for stored security telemetry
- Access controls and audit logging for all data access
- Physical security controls for data centre facilities
- Regular security assessments and penetration testing

Data location and sovereignty:
- CSTM infrastructure hosted within UK data centres
- No data processing or storage outside the UK
- Compliance with UK data residency requirements

6.3 Personnel Security

Staff vetting and clearance:
- All CSTM analysts and engineers undergo background checks
- Security clearances appropriate to the sensitivity of data handled
- Ongoing security awareness training and professional development
- CREST-accredited specialists maintain professional standards

Access controls:
- Role-based access to customer data (least privilege principle)
- Multi-factor authentication for all administrative access
- Audit logging of all staff actions within CSTM platform
- Regular access reviews and recertification

6.4 Operational Security

Secure infrastructure:
- CSTM platform hosted in ISO 27001 certified, physically secure UK data centres
- Network segmentation isolating customer data
- Redundant infrastructure for resilience
- Regular patching and security updates

Incident management:
- 24/7 monitoring of CSTM platform itself for security issues
- Incident response procedures for platform security events
- Business continuity and disaster recovery plans tested annually

Continuous assurance:
- Annual external audits for ISO 27001 and Cyber Essentials Plus
- Regular internal security assessments
- Penetration testing of CSTM infrastructure
- Vulnerability management programme

6.5 Compliance Support for Customers

CSTM helps customers demonstrate compliance with:

GDPR (General Data Protection Regulation):
- Evidence of "appropriate technical measures" for data protection
- Security logging for data breach detection and notification (72-hour requirement)
- Audit trail for Data Protection Impact Assessments (DPIAs)
- Documentation for demonstrating accountability

Cyber Essentials / Cyber Essentials Plus:
- Monitoring evidence for security controls
- Logging for audit trail requirements
- Detection of unauthorised software and configuration changes

Cyber insurance requirements:

- Security monitoring and incident detection evidence
- Rapid breach detection and response documentation
- Risk management evidence for underwriting
- Detailed incident timelines for claims processing

Research funding body requirements:

- Data protection assurances for UKRI, Wellcome Trust, EU Horizon funding
- Evidence of security controls protecting research data
- Incident response capabilities for research integrity

Regulatory reporting:

- ICO breach notification support with detailed timelines
- Evidence for regulatory investigations
- Audit trails for sector-specific compliance (education regulations)