

CENTRI FOR SIEM



ABOUT US

At Barrier, our mission is to help our customers build cyber resilience and develop strategies to defend against cyber-attacks. We have developed a portfolio of services and solutions that suit customers small and large, in both the private and public sector. Our portfolio encompasses security consultancy, solutions from innovative vendors to mitigate attacks, through to managed services that proactively detect attacks and provide swift incident response measures.

We have built a practice dedicated to providing assurance that systems are resilient to attack. We provide penetration testing services to check the effectiveness of the deployed controls against real-world attacks, and we can implement a vulnerability management system to maintain levels of operational resilience.

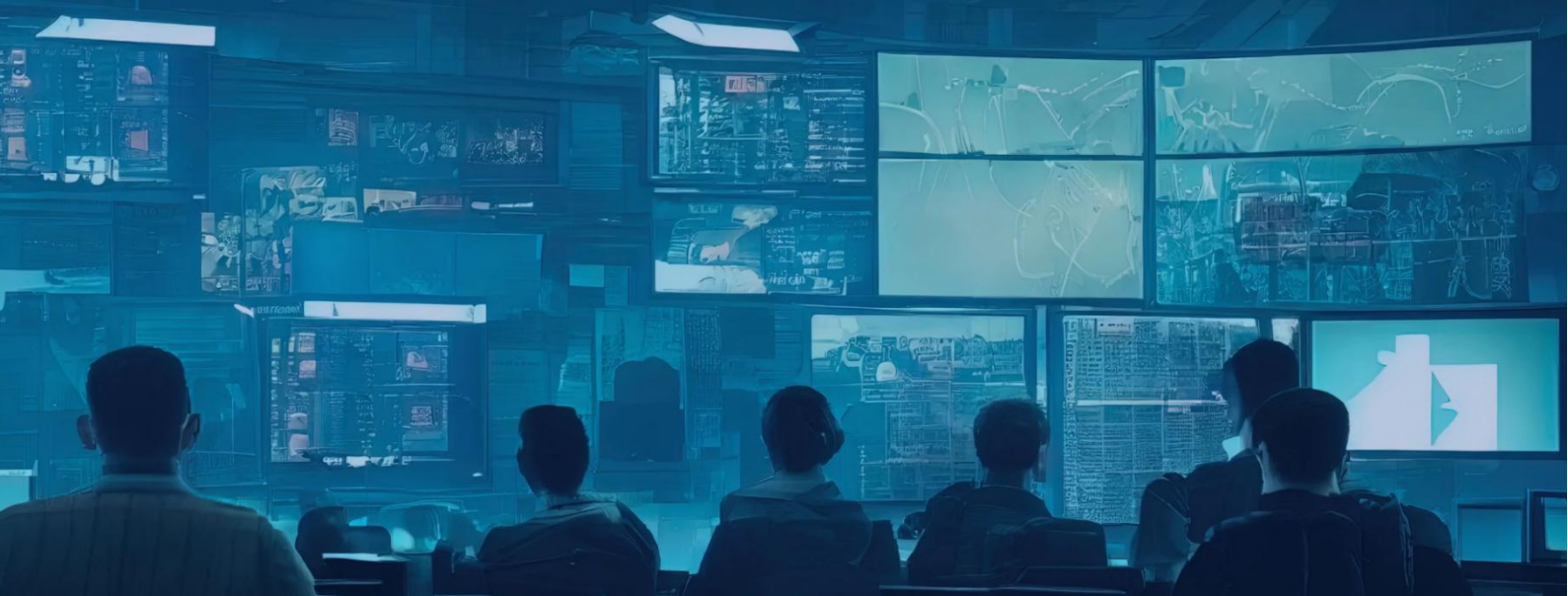
Our aim is to build trust and understanding of how our customers' organisation functions. Our work takes us across all sectors, with strong references in the Finance Sector, Data Hosting, Legal, Local Government, MOD, and the wider Public Sector.

Established in 2006, we are a cybersecurity-focused solutions and service provider. Our customers trust Barrier as a strategic part of their cybersecurity team and here's why:

- Our knowledge of the cybersecurity industry helps select the right solutions
- Our experience helps organisations build cohesive cyber resilience strategies
- Our people are empowered to work closely with our customers to forge strong partnerships
- Our services become an intrinsic part of our customer's security operations

The copyright in this work is vested in Barrier Networks Limited and the document is issued in confidence for the purpose for which it is supplied. It must not be reproduced in whole or in part or used for tendering or manufacturing purposes except under direct agreement or with the consent in writing of Barrier Networks Limited.

No information as to the contents or subject matter of this document or any part thereof arising directly or indirectly therefrom shall be given orally or in writing to any third party, being an individual firm or company, or any employee thereof without the prior consent in writing of Barrier Networks Limited.



SERVICE OVERVIEW

Barrier's Centri for SIEM service provides real-time visibility, analytics, centralised log management, and automated compliance – all conducted from our embedded CREST-accredited Security Operations Centre (SOC).

SERVICE FEATURES

- **Asset Discovery:** Automated discovery and visibility of on-premises and cloud assets, identifying connected devices, configurations, running services, vulnerabilities, and active threats.
- **Vulnerability Assessment:** Continuously monitor assets for emerging vulnerabilities using scanning – including light-touch and authenticated scans – to identify vulnerable software, malicious processes, and signs of compromise.
- **Intrusion Detection:** Early detection and response using cloud, network, and host intrusion detection, analysing traffic to identify attacks, malware, anomalies, and signs of compromise across the organisation.
- **Behavioural Monitoring:** Establish normal system and network activity and detect deviations indicative of operational issues or potential security incidents.
- **Incident Response Orchestration:** Centralised security operations platform that automates and coordinates incident response, integrates disparate tools, and reduces detection-to-response time.
- **Threat Intelligence:** Automatically ingests intelligence from the Open Threat Exchange, leveraging global community data on emerging threats, including malware, botnets, C2 traffic, and advanced persistent threats.
- **Cyber Incident Intervention Procedure (Optional Add-On):** Structured, 24/7 SOC-led intervention process for active threats, using predefined scenarios, playbooks, and RACI roles to contain, remediate, and protect customer environments.
- **Scalable Delivery:** Cloud-based architecture and SOC operating model that scales monitoring, processing, and response capabilities in line with organisation size, complexity, and data volume.

SERVICE DELIVERABLES

- **Structured Technical and Operational Onboarding:** Inclusive of a security consultation workshop with Barrier analysts, a solution High Level Design (HLD), Service Handbook, RACI matrix, and Service Acceptance document.
- **Initial Tuning and Baselining:** Establishing normal behaviour patterns, reduction of false positives, and optimisation of detection rules for the organisation's environment and risk profile across a bedding in period of three months.
- **24x7 Threat Detection and Response:** Operational within the boundaries of the Centri for SIEM Service Level Agreements.
- **Break/Fix Maintenance:** Included for all managed service software and hardware components.
- **Monthly and Quarterly Service Reporting:** Ongoing performance management reporting inclusive of incident reporting, service capacity, key service metrics, and threat intelligence information.

SERVICE OUTCOMES

- **End-to-End Security Visibility:** Centralised collection and correlation of security telemetry across on-prem, cloud, and endpoint assets to support informed risk and incident management decisions.
- **Enhanced Compliance with Industry Security Regulations:** Alignment of security practices with key regulatory requirements alongside automated compliance reporting for frameworks like GDPR and ISO 27001.
- **Proactive Threat Detection:** Continuous monitoring using signature-based and behavioural detection mechanisms to identify security events and incidents at an early stage.
- **Event Contextualisation and Noise Reduction:** Behavioural analysis and enrichment to prioritise security events based on operational context, reducing false positives and improving efficiency.
- **Coordinated Incident Response:** Integrated orchestration and SOC-led response processes to minimise Mean Time to Detect and Mean Time to Respond in line with defined response playbooks.
- **Actionable Threat Intelligence:** Ongoing integration of curated threat intelligence feeds to enhance detection accuracy and support timely identification of known threats and malicious activity.

SERVICE LEVEL AGREEMENTS

Priority	Impact	Response	Resolve
P1: Critical	Degraded service outage causing severe operational impact.	30 minutes	1 business day
P2: High	Degraded service affecting a number of users but lacks significant operational impact.	1 hour	1 – 2 business days
P3: Medium	Issues affecting a single user or a very small group of users.	24 hours	3 business days
P4: Low	Requests for advice or guidance & change requests which are not time sensitive.	48 hours	5 – 7 business days

NB: For large or complex incidents, varying factors may influence resolution times.

SERVICE CHANGES

Upon a customer's request, Barrier can carry out changes to the service. Customers are allocated a fixed number of change requests per month. These changes can range from standard to complex and will be determined by a Barrier engineer upon receipt of the request. Complex changes may require additional consultancy time at additional cost – this will be discussed and agreed with the customer prior to any change being carried out.



BARRIER NETWORKS

272 Bath Street
Glasgow, United Kingdom
G2 4JR

✉ info@barriernetworks.com

☎ +44 (0)141 356 0101

