SERVICE DEFINITION

CYBER INCIDENT RESPONSE

BARRIER

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

Barrier Networks Limited
272 Bath Street, Glasgow, G2 4JR
Tel: 0141 356 0101

SERVICE OVERVIEW

Barrier Networks NCSC Assured Cyber Incident Response (CIR) Service significantly improves your organisation's ability to respond swiftly and effectively to cyber-attacks.

We deliver this service by leveraging cyber threat intelligence feeds to help shape our response operations. Intelligence-led response services put your resources where you need them most so that you get the best results. Our service engages multiple layers of defence to provide a comprehensive approach that helps you better prepare, manage, respond to, and recover from incidents quickly and effectively.

Our security operations centre and incident response staff consist of a wide spectrum of skills and experience. The team at Barrier work directly with cyber threat intelligence providers to help protect against all types of threat actors.

Our threat intelligence services quickly improves your ability to detect new and emerging threat actors. We can help you evaluate and develop security incident response policy and provide rapid assistance during an attack. Acting as your partner, we can assist with all aspects of your response, from removing hackers or ransomware from your network through to providing training and support for communications teams.

With our service you can lean on our expertise to help you assess and design a security strategy that scales with business growth, reduces cost, and mitigates cyber risk.

SERVICE FEATURES

- Enhance your cyber resilience against cyber-attacks.
- Integrate cyber threat intelligence into your security operations.
- Improve protection against system exploitation and social engineering.
- Prepare management and technical staff to respond to cyber-attacks.

SERVICE OUTCOMES

- **Emergency Cyber Incident Response:** Our service can help improve response to cyber security incidents. We identify, contain, and eradicate threat actors and malware from IT systems. This service provides a combination of the following incident response services:
    - Incident triage
    - Recommendation for containment actions
    - Technical support (for containment, analysis and forensics)
    - Incident management or management support
- **Cyber Incident Exercising (CIE) Tabletop Exercise (TTX):** Our consultants conduct a working session to evaluate incident scenarios, assured by NCSC.
- **Cyber Incident Response Plan and Process Development:** Our consultants work with the organisation to develop a Security Incident Response Process to support coordinated response and communications for cyber security incidents, as defined in the TTX. This provides a framework for the Barrier SOC to execute pre-agreed actions when responding to an incident on behalf of our customer.
- **Cyber Risk Technical Assessment:** A CRTA provides an increased level of assurance that technical cyber risk is being reduced to an acceptable level within a business. It is conducted by an experienced security architect who reviews the security architecture and deployed technical controls to identify where gaps in the security posture may be present.

SUPPORT LEVELS & EXCLUSIONS

24 x 7; Response in 30 minutes.

Access to IR Team via phone, portal and email.

BARRIER NETWORKS

272 Bath Street
Glasgow, United Kingdom
G2 4JR

info@barriernetworks.com
+44 (0)141 356 0101

BARRIER