Incident Response & Readiness Services

Preparedness, Response & Recovery for Security Incidents
Aligned to NIST & ISO Standards
Company 86 | www.c86.tech

Executive Summary

The C86 (Company 86) Incident Response & Readiness service enables organisations to prepare for, respond to, and recover from security incidents in a structured, assured, and business-aligned manner. The service is aligned to recognised best-practice standards including the NIST Cybersecurity Framework (CSF), NIST SP 800-61 (Computer Security Incident Handling Guide), and ISO/IEC 27035 (Information Security Incident Management), Cyber Assessment Framework (CAF) and NCSC Guidelines. All services can be consumed separately as required or provided as a complete package on an annual basis.

Security Incidents in a Changing Threat Landscape

The cyber threat landscape is evolving at an unprecedented pace. Threats are becoming more wide-ranging, more targeted, and increasingly sophisticated in nature. Organisation's face a diverse mix of threats, which is increasing in complexity with the adoption of AI. These threats include, advanced persistent threats, ransomware, supply chain compromise, insider risk, and automated attacks leveraging modern tooling and techniques.

Rapid technological advancement is reshaping how organisations operate. Innovations such as cloud platforms, automation, and artificial intelligence (AI) offer significant business benefits, but also introduce new threat vectors and risks if not adopted securely. Many also face a mirid of regulatory obligations requiring clear documented reporting of adherence within their own environment and that of their supply chain.

Incidents such as ransomware, data breaches, supply chain compromise, and insider threats can have significant operational, financial, and reputational impact if not managed effectively.

Service Overview

The C86 Incident Response & Readiness service supports organisations across the full incident lifecycle and is designed in alignment with CAF, NIST and ISO guidance to ensure consistency, repeatability, and regulatory confidence.

Incident Response Readiness Assessment & Planning

C86 performs a structured assessment of incident response readiness aligned to:

- NIST SP 800-61 – Computer Security Incident Handling Guide
- NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover)
- ISO/IEC 27035 – Information Security Incident Management
- CAF - Cyber Assessment Framework

Where gaps are identified, C86 will design and implement incident response plans, playbooks, and escalation models aligned to these standards and tailored to organisational requirements.

Incident Response Retainer

The Incident Response Retainer provides rapid access to experienced incident response professionals who operate in line with NIST, NCSC and ISO-aligned processes, ensuring controlled, auditable, and effective response. This can include addressing the incident on a technical level, working with stakeholders, regulators and media during the incident, forensics and any post incident follow up required.

Post-Incident Services & Continuous Improvement

Post-incident activities can be conducted in accordance with NIST and ISO guidance to ensure lessons learned, root causes addressed, and security controls improved to prevent recurrence. Training and Awareness can also be provided to uplift skills of both the security team and wider team members within the organisation.

Tabletop & Scenario-Based Exercises

Tabletop and scenario-based exercises are designed using NIST and ISO-aligned incident scenarios, testing decision-making, escalation, and communication across technical, executive, and board-level participants.

Key Benefits

- Alignment to recognised NIST, NCSC and ISO best practices
- Improved regulatory and audit confidence
- Faster, more effective incident response
- Reduced risk of repeat incidents

Contact Us

www.c86.tech
info@c86.tech