secon.

Cyber Incident Response Readiness.

Be Ready, Not Reactive.

Overview.

Cyber incidents are no longer exceptional events; they are an expected business risk. The difference between controlled recovery and prolonged disruption is determined by how prepared an organisation is before an incident occurs.

Secon's Cyber Incident Response Readiness service ensures your organisation can respond decisively when a cyber event happens. We prepare your plans, people, tooling, and data so response actions are coordinated, evidence is preserved, and recovery is controlled.

Incident response readiness is not about writing plans, it is about ensuring they work under pressure.

Why Incident Response Readiness Matters.

During live incidents, organisations often face incomplete logging, unclear forensic access, conflicting containment actions, and delayed escalation caused by unclear ownership. Response tooling is frequently untested under real conditions, increasing the risk of evidence loss and prolonged impact.

A mature incident response readiness posture addresses these issues in advance, improving time to detect, contain, and recover incidents, while ensuring evidential quality suitable for regulatory, legal, and insurance requirements.

Key Benefits.

Faster, Controlled Response.

Reduce time to detect, contain, and recover incidents through validated response processes, pre-positioned access, and clearly defined decision paths that work under pressure.

Stronger Evidential Assurance.

Preserve high-quality forensic evidence through prepared logging, access, and handling procedures that support regulatory reporting, legal review, and cyber insurance requirements.

Reduced Business Impact.

Limit operational disruption, data loss, and reputational damage by executing coordinated response actions that prevent escalation and uncontrolled lateral spread.

Board and Regulatory Confidence.

Demonstrate to boards, regulators, and auditors that your organisation can respond decisively and effectively to material cyber incidents, not just document intent.

What Incident Response Readiness Delivers.

1. Incident Response Assessment & Benchmarking

- Review and validation of Incident Response Plans and escalation models
- Mapping of roles, authority, and decision ownership
- Maturity assessment aligned to NCSC guidance and ISO/IEC 27035

2. Tooling, Telemetry & Data Readiness

- Validation of endpoint, network, identity, and cloud log coverage
- Verification of forensic access paths and permissions
- Pre-built incident data sets (assets, diagrams, ownership, contacts)

3. Playbooks & Scenario Coverage

- Ransomware and extortion
- Business Email Compromise (BEC)
- Cloud and identity compromise
- Insider threat and data breach
- DDoS and service disruption

Each playbook defines triggers, containment actions, evidence priorities, and escalation thresholds.

4. Simulation & Validation

- Tabletop exercises for technical and executive teams
- Validation of timing, decision quality, and coordination
- Documented lessons learned and remediation actions

5. Response Activation Framework

- Tabletop exercises for technical and executive teams
- Validation of timing, decision quality, and coordination
- Documented lessons learned and remediation actions

Who is this service for?

This service is designed for organisations that operate SOC, MDR, or SIEM services but need validated, well-practised response processes. It is particularly valuable for regulated organisations that require defensible, auditable incident handling. The service also supports security teams that have experienced incidents or near-misses and want to strengthen their response capability, as well as boards seeking assurance that operational cyber resilience is in place.

How We Engage.

Baseline Readiness Assessment

We review your existing incident response plans, supporting documentation, security tooling, access paths, and escalation structures to assess your current response capability and identify priority gaps.

Design & Preparation

We develop or refine incident playbooks, access and permission models, and supporting readiness artefacts to ensure roles, actions, and evidence requirements are clearly defined before an incident occurs.

Simulation & Assurance

We run structured tabletop exercises and validation activities to test response actions, decision-making, and coordination under realistic incident scenarios, capturing lessons learned and improvement actions.

Continuous Improvement

We support ongoing readiness through regular reviews, defined metrics, and refresh cycles that keep plans, tooling, and response capability aligned with evolving threats and business change.

What You Gain.

You gain the confidence that when an incident occurs, your organisation can respond with speed and control.

Roles are clear, evidence is preserved, decisions are timely, and recovery actions are coordinated, reducing operational, financial, regulatory, and reputational impact.

About Secon.

Secon is a specialist cyber security company with over 25 years' experience helping organisations build stronger, simpler defences. From Enterprise Security Architecture and GRC to 24/7 Security Operations and bespoke engineering, we deliver what's needed, without the noise.

Contact Us.

To learn more about Secon's Incident Response Readiness service or to request an initial consultation:

www.seconcyber.com

hello@seconcyber.com

+44 (0) 203 657 070

Cyber Incident Response Readiness