G-Cloud 15

Service Definition

Crisis Simulation Testing

Table of Contents

1. Service Overview

Cyberfort's Crisis Simulation Testing service delivers peace of mind by providing realistic, scenario-driven cyber incident simulations that test an organisation's ability to detect, respond, recover and learn from cyber security incidents.

Our simulations are powered by attack emulation simulation platforms, realistic incident artefacts (including technical and business "injects"), and delivery expertise from our experienced DFIR and incident response specialists. All crisis simulations are based on real-world incidents that our DFIR team has responded to, ensuring scenarios reflect authentic attacker behaviours, realistic timelines, and the challenges organisations face during high-impact cyber incidents.

We'll deliver an innovative security service underpinned by cyber security best practices, delivered by skilled consultants using approved methodologies aligned to standard frameworks and resilience outcomes. Service management works alongside our technical and executive facilitators from day one, providing the right people, the right structure, and the right tools to deliver meaningful and measurable improvements.

We pride ourselves on the ability to deliver a holistic approach by considering the organisation in its entirety. Our crisis simulations test not only technical capabilities, but also the operational and executive decisions that determine whether an incident becomes a disruption or a controlled event.

Cyberfort's Crisis Simulation Testing service includes the following key elements:

- **Attack emulation simulation platforms:** Controlled, safe replication of real-world attacker techniques and behaviours
- **Realistic incident artefacts:** Logs, alerts, emails, screenshots, chat transcripts, "breaking news", and business impact injects
- **Technical coverage:** SOC workflows, detection engineering, triage, containment, eradication and recovery validation
- **Executive coverage:** Decision making, governance, escalation, communications, and crisis leadership actions
- **Facilitated delivery:** Expert-led simulation management, role-based participation, and outcome tracking
- **Evidence and improvement:** Post-exercise reporting with measurable timelines, gaps, recommendations and an improvement plan

1.1 Service Detail

Cyberfort's Crisis Simulation Testing service includes the following capabilities and services:

1.1.1 Realistic crisis simulation testing based on real-world incidents

Our crisis simulations are not generic tabletop exercises. Each scenario is based on real incidents that our DFIR teams have managed, refined and validated through real response activity, ensuring credibility and realism throughout.

Simulations can be tailored to your organisation's priorities, including:

- Ransomware and extortion scenarios
- Cloud identity compromise
- Data breach and unauthorised access

- Insider threat and privilege misuse
- Supply chain compromise and third-party risk events
- Operational disruption affecting critical services

1.1.2 Technical and executive coverage across the full incident lifecycle

Cyber incidents are rarely "just technical". Our service tests full operational capability across both frontline responders and decision-makers, including:

Technical coverage includes:

- Security monitoring and alert handling
- Triage and incident classification
- Threat hunting and investigation
- Containment and remediation steps
- Recovery planning and execution
- Evidence capture and escalation routes

Executive coverage includes:

- Governance decision-making (Gold/Silver/Bronze where applicable)
- Risk ownership and prioritisation during crisis
- Communications and reputational considerations
- Legal/regulatory response readiness
- Supplier and stakeholder coordination
- Business continuity decisions and trade-offs

This ensures the simulation validates both "hands-on keyboard" response and leadership accountability.

1.1.3 Attack emulation and simulation platforms

Cyberfort uses attack emulation simulation platforms to replicate adversary behaviours and event sequences safely and in a controlled manner. This provides realism in technical signals and artefacts without impacting live operations.

Our approach supports:

- Safe emulation of attacker techniques (TTPs)
- Repeatable test conditions for measured improvement
- Controlled escalation and scenario pacing
- Realistic outputs such as alerts, logs, and system behaviour

This enables organisations to test security capabilities as close to real incident conditions as possible.

1.1.4 Realistic artefacts, injects and scenario-driven pressure testing

To ensure exercises replicate real-world stress, confusion, and escalation complexity, we provide realistic injects and artefacts, such as:

- Security alerts and logs aligned to the scenario
- Suspicious emails, user reports and service desk tickets

- Identity compromise indicators and audit trails
- Stakeholder communications and executive “injects”
- Press/media prompts and regulator-style information requests
- Timed business impact updates (service outage, operational disruption)

This enables teams to respond to an incident that feels authentic, with realistic ambiguity and time constraints.

1.1.5 Alignment to organisational risk and operating context

We tailor crisis simulations to align with:

- Your critical services and business priorities
- Your infrastructure landscape and tooling
- Your incident response processes and playbooks
- Your risk appetite and governance model
- Your regulatory and assurance requirements

This ensures exercises deliver outcomes that are directly applicable to your organisation’s operating reality and improvement goals.

1.1.6 Evidence and Reporting

Cyberfort provides evidence-led outputs designed to demonstrate value, improve capability, and support assurance. Reporting typically includes:

- Exercise timeline and key decision points
- Detection, response and escalation performance indicators
- Observations on strengths, gaps, and blockers
- Recommendations and prioritised improvement actions
- Governance and operational process findings
- Tactical improvements (SOC playbooks, escalation) and strategic improvements (resilience maturity)

Where required, reporting can be aligned to customer formats and governance requirements.

1.1.7 Continuous improvement and repeatable maturity development

Crisis simulation testing is most valuable when used as part of a maturity cycle. Cyberfort supports repeatable exercises to validate:

- Improvements implemented since prior exercises
- Operational consistency across teams
- Readiness against evolving attacker techniques
- Long-term resilience improvements over time

Our simulations are designed to produce measurable progress, not just awareness.

1.1.8 Security

Cyberfort's Crisis Simulation Testing service is governed by stringent security policies, procedures and controls. Simulation activities are delivered with safety and control to ensure:

- No unintended disruption to live services
- Clearly defined scope and approval boundaries
- Controlled execution of technical simulation components
- Appropriate handling of sensitive organisational information

Confidential and structured handling of exercise outcome

2. Onboarding and Offboarding Support

2.1 Deployment and phasing

To simplify engagement delivery, Cyberfort provides structured onboarding and planning to ensure exercises run effectively with minimal disruption:

- Scoping and requirements workshop
- Stakeholder identification and role definition
- Scenario selection and tailoring
- Confirmation of exercise rules (safe boundaries)
- Scheduling, logistics and communications planning
- Pre-brief sessions for participants where required

We deliver exercises virtually, onsite, or through a hybrid approach depending on customer needs.

3. Service Management Approach

3.1 Service Delivery Teams

Cyberfort delivers crisis simulations through a cross-discipline team to ensure realistic delivery and meaningful outcomes across technical and executive domains, typically including:

- **Exercise Director / Lead Facilitator:** Oversees scenario control, pacing and delivery quality
- **DFIR Lead:** Ensures realism based on lived incident response experience and inject content
- **Technical Simulation Specialist / Red Team Support:** Controls attack emulation components and technical artefacts
- **SOC / Detection Specialist:** Validates monitoring, alert handling and operational response steps
- **Executive Facilitator:** Supports governance decision-making, communications and escalation testing
- **Service Management Lead:** Coordinates engagement activity and ensures deliverables and reporting

This ensures the exercise is delivered with the credibility and control required to produce measurable improvements and meaningful assurance outcomes.

4. Commercials & Pricing

4.1 Ordering & Invoicing Process

Please contact us for a quote via email at bidmanagement@cyberfortgroup.com

Orders are processed on receipt of a purchase order.

Prior to commencement of any work ordered via the G-Cloud framework, Cyberfort requires client acceptance of the order and also completion of a Call-Off Contract.

Clients are invoiced on a monthly basis or according to agreed milestones.

4.2 Service pricing model

Cyberfort's pricing for Crisis Simulation Testing links clearly to Resources Based Pricing detailed in our SFIA rate card framework.

Please refer to our Pricing document for more details.

4.3 Minimum contract period

Contract terms will be provided at the time of quotation, based on specification. These will not exceed the maximum contract constraints of the G-Cloud framework.

5. Governance Compliance

Cyberfort confirm that we will deliver our services to clients in line with all industry and Government recognised standards, best practice and legal regulations, including but not limited to the following:

5.1 GDPR

We adhere to the legal and statutory requirements outlined in the UK Data Protection Act 2018 and the General Data Protection Regulations (GDPR). Our organisation has a current registered Information Commissioners Office (ICO) certificate for Data Protection.

5.2 Government and industry standards

Throughout the life of any contract, our consultants will ensure that all service standard principles are adhered to so that clients can be assured that all delivered outcomes conform with Government and industry standards and expectations. Our teams are deeply experienced in operating services, to deliver outcomes and outputs that fully comply with:

- The principles defined in the Government's Service Standard and Technology Code of Practice (TCoP).
- The Government Functional Standard (GovS 007: Security), ensuring that the stated principles (for example security objectives are aligned to government policy and organisational objectives) are applied to all projects.
- Open standards supported include TOGAF, NIST-CSF, ISO/IEC27000, SANS and OWASP.
- Regulation frameworks including, Cyber Security and Resilience Bill, Digital Operational Resilience Act (DORA), and NIS2 Directive.
- Government Cyber Security Strategy, including National Cyber Security Centre (NCSC).
- As an NCSC assured Cyber Security Consultancy, we are members of the NCSC Assured Consultancy Scheme Community Network and leverage the CiSP (Cyber Information Sharing) platform.

5.3 Quality Management

Further, we have a fully implemented Quality Management System (QMS) and are certified to ISO 9001:2015 International Standard, which details our policy, objectives and processes, as well as demonstrating how our QMS framework enhances client satisfaction whilst ensuring consistent delivery of product and services is maintained to meet client, statutory and regulatory requirements.

Our delivery is underpinned by certifications and associated management systems including:

- ISO:27001
- ISO:14001
- ISO:9001
- ISO:45001
- Cyber Essentials Plus
- CREST Certified Body CE
- CREST Penetration testing
- NHS Digital Toolbox
- PCI DSS
- DSPT
- NCSC Cyber Security Consultancy
- NCSC CHECK ITHC

About Cyberfort

Cyberfort's all-encompassing Cyber Security Services

At Cyberfort we provide a range of customers with all-encompassing Cyber Security Services. We are passionate about the cyber security services we deliver for our customers which keeps their people, data, systems and technology infrastructure secure, resilient and compliant.

Our business offers National Cyber Security Centre assured Consultancy services, Identification and Protection against cyber-attacks, proactive Detection and Response to security incidents through our security operations centre and a Secure and Recover set of Cloud solutions which keeps data safely stored, managed and available 24/7/365.

Over the past 20 years we have combined our market leading accreditations, peerless cyber security expertise, strong technology partnerships, investment in our future cyber professionals and secure locations to deliver a cyber security experience for customers which enables them to achieve their business and technology goals in an ever-changing digital world.

Cyberfort

Care about the impacts we make on the Environment, Social and Governance.

We are passionate about empowering our employees, suppliers, customers, and the cyber security ecosystem to create a better world for our business and the communities we participate in, for example:

As a member of Neurodiversity in Business (NiB) and Disability Confident Employer

Cyberfort are supporting those with physical and neurodiverse disabilities, by disarming barriers for people with disabilities and ensuring equal opportunities for all.

Cyberfort are inspiring and attracting young people to the world of cybersecurity.

We support the development of their passion for technology through Apprenticeships, Graduate Schemes, CyberFirst and school education/awareness.

We are committed to achieving net zero carbon emissions by 2050.

Cyberfort have clear plans and activities that deliver environmental benefits by increasing the energy efficiency of our operations, reduce our waste, and protect our communities.

Our Values

Teamwork | Curiosity

Ownership | Agile | Innovative

Cyberfort

Accreditations

We are proud of the extensive list of industry and government accreditations we hold. We understand the need for independent validation when entrusting the security of valuable or sensitive data to a third party.

Our Vision

To be an integral part of the cyber security ecosystem, providing assured, highly skilled and reliable security services to businesses and government departments. Embodying the UK Cyber Security Strategy, through trusted partnerships we aim to empower businesses and government departments with confidence, making the world a safe and secure place to conduct business.

Our Mission

To provide our customers with an agile and innovative approach to help them overcome their cyber security challenges. Through a collaborative approach with our customers we design, build and operate their cyber security environments resulting in a secure and resilient infrastructure, providing a safe environment for employees, service users and stakeholders to conduct their business in the knowledge that their critical data remains safe in an ever-changing digital world.

www.cyberfortgroup.com

For more information, please contact us on:

01304 814800

info@cyberfortgroup.com