G-Cloud 15

Service Definition

Digital Forensics and Incident Response (DFIR)

Table of Contents

1. Service Overview 1
   1.1 Service Detail 1
2. Onboarding and Offboarding Support 5
   2.1 Deployment and phasing 5
3. Service Management Approach 6
   3.1 Service Delivery Teams 6
4. Commercials & Pricing 7
   4.1 Ordering & Invoicing Process 7
   4.2 Service pricing model 7
   4.3 Minimum contract period 7
5. Governance Compliance 8
   5.1 GDPR 8
   5.2 Government and industry standards 8
   5.3 Quality Management 8
6. About Cyberfort 9

1. Service Overview

Cyberfort's Digital Forensics and Incident Response (DFIR) service delivers peace of mind by supporting customers at all stages of cyber security incidents: from pre-breach preparation and readiness, through in-breach containment, isolation, investigation and response, and continuing through post-breach forensic investigation, chain of custody and root cause analysis.

We'll deliver an innovative DFIR service underpinned by cyber security best practice and delivered by experienced professionals with decades of experience responding to and investigating incidents for high-risk and highly regulated organisations. Our DFIR service combines specialist forensic capability with real-world incident response expertise across network, endpoint and cloud environments, ensuring fast, professional response and effective recovery aligned to the customer's critical business priorities.

We pride ourselves on a holistic approach: we connect our response activities to the context of your organisation, its risks, mitigations and controls, rather than relying solely on technology and tooling. This enables Cyberfort to prioritise response activities around your critical business areas and reduce business impact, disruption and recovery time.

Cyberfort's DFIR service comprises the following key elements:

- **24x7 Incident Response Hotline:** Immediate access to Cyberfort's Incident Response team.
- **Incident Response Retainer:** Guaranteed 4-hour response time for critical incidents.
- **Dedicated Incident Response Manager:** Assigned during high-severity incidents to streamline communications.
- **Digital Forensics:** Acquisition, analysis and preservation of digital evidence with robust chain of custody.
- **Network, Endpoint and Cloud Forensics:** Investigation coverage across enterprise and cloud environments.
- **Malware Analysis:** Isolation and analysis of malicious tooling to understand scope and impact.
- **Cyber Threat Intelligence:** Understanding threat actor behaviours to mitigate future risks.
- **Technology Recovery:** Support to restore infrastructure and systems safely after an incident.
- **Criminal and Legal Support:** Assistance through trusted partners for legal and criminal proceedings.
- **Tabletop Workshops:** Regular workshops (one included annually) focusing on executive crisis management and incident response readiness.

1.1 Service Detail

Cyberfort's Digital Forensics and Incident Response (DFIR) service includes the following capabilities and services:

1.1.1 Prepare, respond and recover from cyber security incidents

Cyberfort supports customers before, during and after cyber incidents. Our service provides structured preparation and readiness activities, rapid incident containment and response, and post-incident forensics to ensure customers can recover quickly and strengthen resilience against future attacks.

This includes planning activities such as incident response policies, scenarios and readiness improvements, alongside operational response activities such as isolation, analysis and recovery support.

1.1.2 A proven incident response methodology

Cyberfort's incident response activities follow a proven methodology designed to reduce business impact and restore operational capability quickly:

- **Identification:** Rapid detection of breaches and threats
- **Analysis:** Assessment of scope and impact
- **Containment:** Isolation actions to prevent spread and additional damage
- **Remediation & Recovery:** Restore systems and eradicate threats
- **Root Cause Analysis:** Identify how the incident occurred and prevent recurrence

Our IR services also include post-incident review activities to strengthen future defences and improve resilience to evolving threats.

1.1.3 Digital forensics as the foundation of incident response

Cyberfort's Digital Forensics services focus on acquiring, analysing and preserving evidence across devices, networks and cloud platforms. This includes forensic imaging to support immutability and chain-of-custody requirements where evidence may be needed for regulatory, insurance or legal proceedings.

Our forensic specialists investigate artefacts such as files, emails and system logs to uncover attacker activity including unauthorised access, malware execution and suspicious network traffic.

1.1.4 Coverage across network, endpoint and cloud environments

Cyberfort delivers DFIR investigation capability across a broad range of environments and incident types:

- **Network Forensics:** Detect unauthorised access and data exfiltration
- **Endpoint Forensics:** Investigate data theft, malware and insider threats
- **Cloud Forensics:** Evidence collection aligned to provider guidelines
- **Log File Analysis:** Identify unauthorised activity and failures
- **Malware Analysis:** Understand malicious behaviour and scope of compromise

This breadth enables a complete and defensible investigation across customer infrastructure and technology platforms.

1.1.5 Incident readiness and forensic readiness support

Cyberfort helps organisations minimise impact by strengthening incident readiness in advance of a breach. This includes:

- Developing incident response plans and playbooks

- Forensic readiness to capture and preserve evidence efficiently
- Crisis scenario modelling to support governance and reputation management
- Tabletop exercises to test readiness and improve outcomes

We provide actionable improvement plans as part of onboarding and readiness uplift, supporting resilience and compliance outcomes.

1.1.6 Evidence collection, chain of custody and compliance outcomes

Cyberfort applies evidence handling practices designed to preserve integrity and support legal/regulatory processes. This includes chain of custody controls and support for downstream requirements such as cyber insurance, reporting and legal proceedings.

Where required, we can support customers with communications and regulatory-aligned response planning to manage the operational and governance impacts of cyber incidents.

1.1.7 Key areas supported within an Incident Response Plan

Cyberfort can support customers in developing and improving incident response plans across key areas including:

- Incident identification
- Containment procedures
- Communication strategy
- Evidence collection and preservation
- Root cause analysis
- Recovery process
- Regulatory compliance alignment
- Regular testing and updates
- Post-incident review
- Crisis scenario modelling

This ensures operational readiness, clear ownership, and measurable improvement over time.

1.1.8 Evidence and Reporting

Cyberfort provides clear, actionable outputs aligned to incident response, investigation and assurance needs, including:

- Incident timeline and activity summary
- Scope of compromise and impact assessment
- Evidence handling and investigation artefacts
- Threat actor behaviour and malware analysis summary
- Root cause findings and remediation priorities
- Recovery recommendations and resilience improvement actions

1.1.9 Security

Cyberfort's DFIR service is governed by robust security policies, procedures and controls designed to ensure safe delivery, protect sensitive information, and preserve evidence integrity.

Our service supports strong security outcomes by helping organisations:

- Prepare for and evidence readiness
- Reduce incident impact and disruption
- Recover faster and more safely
- Strengthen controls and resilience through lessons learned.

2. Onboarding and Offboarding Support

2.1 Deployment and phasing

Cyberfort provides structured onboarding and planning activities to ensure readiness is established early and response capability is well understood, including:

- Scoping and stakeholder mapping
- Review of current IR policies and playbooks
- Defining critical systems and business priorities
- Establishing incident engagement routes
- Supporting tabletop exercises and readiness improvements

During an incident, Cyberfort deploys DFIR professionals quickly and prioritises response actions around critical business services, delivering faster and more effective outcomes.

.

3. Service Management Approach

3.1 Service Delivery Teams

Cyberfort delivers DFIR through a cross-discipline team combining forensic expertise, response leadership, and recovery support, typically including:

- Incident Response Lead / Incident Commander
- Dedicated Incident Response Manager (for high-severity incidents)
- Digital Forensics Specialist
- Network & Cloud Forensics Specialists
- Malware Analyst
- Threat Intelligence Support
- Recovery and Remediation Support Specialists

This ensures customers receive rapid access to specialist support with the experience, capability and scale required to manage cyber incidents with confidence.

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 DFIR 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