Cyberfort

Digital Forensics and Incident Response (DFIR)

SERVICE OVERVIEW

Prepare, respond and recover from cyber security incidents through Cyberfort Incident Response and Digital Forensics services

Introduction

Cyberfort's Digital Forensics and Incident Response (DFIR) service supports our customers at all stages of Cyber Security Incidents, from pre-breach (preparation, planning, policies, scenarios) through critical in-breach activities (such as containment, isolation, analysis and response) and continuing to support you throughout the lifetime of an incident to include post breach expertise and activities (including in-depth forensics, expert witness, chain of custody and root cause analysis).

A 75% surge in attacks Year on Year, coupled with an increasing average incident cost globally of over £4M which is further compounded by an increase in regulation and regulator activities all serve to demonstrate why the right DFIR partner with the expertise, experience and scale to support this changing landscape is critical for customers.

As an all-encompassing cyber security provider, Cyberfort has extensive capabilities in DFIR together with extensive subject matter expertise in both offensive and defensive Cyber Security. Our resources combine industry standard certifications and decades of experience mitigating, responding to and investigating incidents for high risk and highly regulated organisations including nation state, CNI, financial and other key sectors.

Working with our customers, we prepare, test and evidence the capabilities to respond to a crisis, providing clear actionable improvement plans that support security posture and compliance as we onboard to our service. When our customers have an incident, Cyberfort deploys our DFIR professionals quickly and utilises advanced tooling and techniques, together with the context of your organisation, its risks, mitigations and controls.

The service is connected to, and understands your business, rather than relying solely on technology and tooling – Because we understand your organisation and how the incidents is affecting your customers, supply chain, regulators, resources, systems and operations, we prioritise response activities around your critical business areas, delivering faster, more effective and increased efficiency outcomes.

Every business that relies on IT infrastructure, handles sensitive data, or operates in a regulated industry benefits from having Cyberfort's DFIR service. Whether preparing and evidencing your capabilities, responding to an attack, investigating suspicious activity, or proactively improving security, Cyberfort's DFIR service delivers faster, more efficient response to critical incidents, delivering significant risk mitigation, ROI, and playing a critical role in your cyber security resilience.

Cyberfort Digital Forensics and Incident Response (DFIR) Services

Cyberfort offers a robust, comprehensive solution for digital forensics and incident response (DFIR), designed to help organisations effectively handle and recover from cyber incidents while ensuring compliance with legal and regulatory requirements.

Our expert team has extensive experience in incident containment, analysis, and remediation, making Cyberfort a trusted partner for any organisation looking to safeguard their critical assets and mitigate the damage of a cyber attack. With a focus on swift, professional response, we ensure organisations are prepared for, respond to, and recover from a broad range of security incidents, all while maintaining data integrity and compliance.

Cyberfort

Digital Forensics (DF) Services

Cyberfort's Digital Forensics services form the foundation of our cyber incident response offerings, specifically focused on acquiring, analysing, and preserving digital evidence. Our DF team specialises in forensic imaging, which involves securely capturing data from digital devices, networks, and cloud environments. This process is essential to maintain the chain of custody and ensure the immutability of critical data, especially when this information might later be used in court or regulatory investigations.

Cyberfort's forensic experts dive deep into digital artefacts such as files, emails, and system logs, meticulously uncovering traces of malicious activity. Whether it's identifying unauthorised access, tracing malware execution, or performing a detailed review of network traffic, our team is equipped with the skills to provide clear, actionable insights.

These capabilities provide critical insights that support not only internal investigations but also legal actions, such as supporting organisations in claims of cyber insurance, or aiding in legal and criminal proceedings.

Our expertise spans

Network Forensics
Identifying and analysing network traffic to detect unauthorised access and data exfiltration.

Endpoint Forensics
Examining devices (computers, mobile phones) to uncover data theft, malicious software, or insider threats.

Cloud Forensics
Investigating incidents within cloud environments, ensuring evidence is collected in compliance with provider guidelines.

Log File Analysis
Reviewing system logs to track unauthorised activity or system malfunctions.

Malware Analysis
Detecting, isolating, and analysing malicious software to understand the scope of an attack.

Incident Response (IR) Services

When an organisation faces a cyber attack, fast and efficient response is crucial. Cyberfort's Incident Response services are designed to help businesses contain, mitigate, and recover from incidents while minimising operational downtime. Cyberfort's IR process follows a proven methodology that includes:

Identification
Rapid detection of security breaches or other cyber threats.

Analysis
Comprehensive evaluation of the incident's impact and scope.

Containment
Immediate steps taken to isolate affected systems and prevent further damage.

Remediation & Recovery
Restoring systems to full functionality while eradicating threats.

Root Cause Analysis
Investigating the cause of the breach to prevent future occurrences.

Cyberfort specialises in handling a wide range of incidents, including data breaches, ransomware attacks, insider threats, and more. Our IR services don't end when the immediate threat is mitigated; we also offer post-incident reviews to assess the organisation's response and implement improvements. This helps ensure that the organisation's future defences are stronger and more resilient to new and evolving threats.

DFIR & Forensic Readiness Services

At Cyberfort, we understand that preparation is key to minimising the impact of a cyber incident. Our Digital Forensics and Incident Response (DFIR) services not only include post-incident support but also focus heavily on proactive preparation for potential incidents. We help organisations build strong incident response capabilities by:

Developing incident response plans
Tailored playbooks and strategies to deal with specific types of attacks, ensuring swift and effective response.

Tabletop exercises
Simulation-based workshops that test an organisation's response to cyber incidents, improving readiness through realistic scenarios.

Crisis scenario modelling
Crisis management strategies designed to protect reputations and manage the fallout of high-impact cyber incidents.

Forensic readiness
Ensuring systems are set up to quickly collect and preserve digital evidence that might be needed for legal or regulatory purposes.

Additional services include assisting with compliance to meet legal and regulatory requirements, supporting cyber insurance claims, and providing guidance for managing public relations during and after an incident.

Cyberfort

10 Key areas Cyberfort can help organisations to build a robust and responsive Incident Response plan

Cyberfort

Incident Identification

We can help IT teams to define the types of incidents that the organisation is most likely to face. This could include data breaches, ransomware, insider threats, and DDoS attacks. Clear definitions ensure that every team member knows when an incident has occurred.

Crisis scenario modelling

Based on our experience of dealing with a range of cyber incidents we take the time to understand how your organisation operates and help IT leaders to define and designate specific roles within the incident response team, including incident commander, communications lead, legal advisor, and forensic analyst. Making sure each role has a clear understanding of their responsibilities during an incident.

Communication Strategy

We have a range of templates and industry best practices available which can enable the development of clear internal and external communication plans. This includes when and how to notify stakeholders, employees, customers, and regulatory bodies. Ensuring the plan has predefined templates for incident announcements.

Containment Procedures

Working with customers and understanding their IT environment means Cyberfort Incident Response experts can include steps in an Incident Response plan to isolate affected systems to prevent the spread of an attack. Having predefined procedures for short-term and long-term containment can significantly reduce the impact of an attack.

Evidence Collection and Preservation

Based on 20+ years cyber security experience Cyberfort can define protocols for collecting and preserving digital evidence to support investigations, legal actions, or insurance claims. Proper chain-of-custody procedures can also be integrated into the plan.

Root Cause Analysis

Ensuring the plan includes a structured approach for conducting a thorough root cause analysis. Identifying how and why the incident occurred helps prevent future incidents of the same nature.

Recovery Process

We can help IT teams to plan for the full restoration of services, ensuring that systems are clean and operational. This includes patching vulnerabilities, reinstalling systems, and conducting post-incident testing to confirm the issue is resolved.

Regulatory Compliance

Making sure the Incident Response plan aligns with legal, regulatory, and compliance requirements. This includes data breach notifications and industry-specific mandates like GDPR or HIPAA.

Regular Testing and Updates

Incident response plans must be tested regularly, through simulations and tabletop exercises, to ensure they work effectively under real-world conditions. Regular updates ensure the plan stays aligned with the evolving threat landscape.

Post-Incident Review

Once the immediate threat is resolved, Cyberfort can undertake a post-incident review to evaluate the effectiveness of the response and identify areas for improvement. This analysis can feed into future training and readiness.

Key Service Inclusions

Cyberfort's DFIR services offer a comprehensive range of inclusions, ensuring your organisation has the necessary tools to detect, respond, and recover from security threats. These services include:

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.

Network, Endpoint, Cloud, and Mobile Device Forensics
Expertise in investigating security breaches across a variety of environments.

Cyber Threat Intelligence
Analysis of threat actor activity, delivering actionable insights to mitigate future risks.

Technology Recovery
Restoring critical infrastructure and systems after a cyber incident.

Malware Analysis
Providing in-depth analysis of malicious software found in environments.

Criminal and Legal Support
Assistance with criminal proceedings and legal cases through our trusted partners.

Tabletop Workshops
Regular workshops (one included annually) focusing on executive crisis management and incident response.

Cyberfort

Final Thoughts

Cyberfort's DFIR services provide organisations with the tools, expertise, and support needed to manage cyber incidents with confidence.

By combining digital forensics, incident response, and incident readiness, Cyberfort helps organisations prepare for and evidence readiness, mitigate the impact of cyber attacks and ensures compliance with regulatory bodies.

Whether you need assistance responding to an ongoing attack or preparing for future incidents, Cyberfort is your trusted partner for digital security. Reach out today to ensure your organisation is prepared for any cyber threat.

For more information on our Cyber Security services please contact us at the details below:

+44 (0)1304 814800 | info@cyberfortgroup.com | https://cyberfortgroup.com

We look forward to working with you

Cyberfort