COALFIRE

DATA SHEET

Digital forensics and incident response (DFIR)

Help for when you need it most

Phones, tablets, computers, and cloud storage have become integral parts of the lives of billions of people worldwide. These electronic products have digital footprints that aid investigators in recovering from compromises, solving crimes, providing intelligence, and bringing criminals to justice.

Preparing your organization

Many organizations lack the skills required to properly evaluate security incidents, which could include computer, mobile phone, and cloud forensics and incident response. Would you be able to respond to a cybersecurity incident effectively and efficiently?

Now more than ever, you must be vigilant and concerned with security. To defend against known and emerging threats, you need an effective incident response plan.

Whether an external attack results in a data breach or an employee intentionally compromises sensitive information, it's vital to investigate incidents and take necessary post-incident steps. With our proven investigative methodologies, tools, and extensive experience, our analysts can help your organization when you need it most.

If you're uncertain about your organization's ability to respond to an incident, ask these questions. If you answer no to any of them, contact Coalfire — we can help.

- Does your organization have an incident response plan?
- Have you tested the plan in the past year?
- Do you have forensic capabilities?
- Do you have technical capabilities to execute the plan?

Types of DFIR services

- **Breach response analysis:** Find out what happened during a compromise and how you can remain protected moving forward.
- **Forensic assurance:** Validate an internal investigation and remediation actions.
- **Employee misuse and misconduct investigations:** Review employees who have been accused of violating your HR policies.
- **Theft of restricted data:** Evaluate your systems for evidence of exfiltration of business-critical data.
- **Unauthorized access:** Investigate the access log to folders and files within an internal system.
- **Credit card fraud:** Assess compromised credit card exposure on ecommerce systems and point-of-sale (POS) terminals.
- **Cellular and mobile device investigations:** Capture system images of mobile devices for digital forensic analysis.

Benefits of having a DFIR strategy

- Improve response time, reducing exposure to data loss and reputational and financial damage.
- Earn the trust of your customers, partners, and investors,
- Align your incident response program to best practices and industry standards.
- Take a more efficient, effective, and predictable approach to cyber events and incidents.

Suspect a breach or require DFIR services?

The faster you can remediate a data security breach, the faster it stops the loss of data, limits fines, and minimizes the impact to your reputation. If you need DFIR services, email **DF@Coalfire.com**.

Why Coalfire?

- Experienced providers of incident response services
  - Comprising former federal law enforcement officers and government contractors specializing in cyber operations, our DFIR team holds numerous forensic certifications.
  - Our dedicated digital forensic analysts have completed hundreds of cases for law enforcement and enterprises and delivered expert testimonies in courts within the U.S., the UK, and across the European Union.
  - We can support investigations across multiple time zones and continents.
- Insights to help you remediate issues quickly
  - Our objective approach to security means we support your organization's critical business needs and follow any unique requirements to help you through the process, so you can get back to business as usual.
  - We provide thorough, unbiased recommendations that help you move beyond a breach and prevent future compromises.
  - Leveraging deep experience in emerging IT architectures, we determine the risks they present to your compliance posture and help you identify a successful path through the investigation process.
  - Along with assessment and certification services, we offer a broad set of advisory and testing services.
- Payment system and technology experts
  - We bring domain knowledge in cloud, embedded systems, encryption, IoT, mobile, and virtualization technologies, as well as insight into how they are leveraged in payment environments.
  - As a Qualified Security Assessor (QSA), we are qualified to understand an environment that may have undergone a credit card breach.
- Cloud experts
  - Whether your system is on premises, in the cloud, or in a hybrid environment, we know how to investigate it quickly and effectively.
  - Through our work with all the major cloud service providers, we've developed a detailed understanding of security architectures.

Take immediate action if you suspect a breach.

Contact Coalfire's DFIR team.

DF@Coalfire.com | 833-954-2422 (U.S.) | +44 0800 260 6436 (UK)

COALFIRE

About Coalfire

The world's leading technology infrastructure providers, SaaS companies, and enterprises – including the top 5 cloud service providers and 8 of the top 10 SaaS businesses – rely on Coalfire to strengthen their security posture and secure their digital transformations. As the largest firm dedicated to cybersecurity, Coalfire delivers a comprehensive suite of advisory and managed services, spanning cyber strategy and risk, cloud security, threat and vulnerability management, application security, privacy, and compliance management. A proven leader in cybersecurity for the past 20 years, Coalfire combines extensive cloud expertise, advanced technology, and innovative approaches that fuel success. For more information, visit **Coalfire.com**.

DS_DFIR_01282022