

Digital Forensics Capabilities Overview

Our Digital Forensics team conducts comprehensive investigations to capture critical evidence suitable for legal proceedings. For incidents, we determine the scope, impact, and root cause, providing clear and actionable remediation strategies. We prioritize rapid responses, actionable evidence, and legally sound conclusions as a lean and agile alternative to larger providers.

Below are selected forensic services offered by Coalfire, featuring concise descriptions, key activities, and practical examples. If your specific requirements aren't listed, please inform our sales representative of your specific needs.

1. HR Policy Violations and Internal Investigations

Our most common and impactful engagements support HR and internal investigations, including:

- Employee misconduct.
- Unauthorized data access or file transfers.
- Misuse of corporate systems.
- Departing employee IP theft.
- Credential abuse and access misuse.

Example: A financial services firm suspected employee misconduct involving unauthorized data transfer. Our rapid investigation provided definitive evidence, securing critical intellectual property, enabling swift disciplinary action and implementation of stronger internal controls.

2. Compromise Assessment

Proactive detection of unauthorized system activity.

- Identify Indicators of Compromise (IOCs).
- Confirm past or ongoing malicious activity.
- Pinpoint affected systems.

Example: A retail company noticed an increase in failed login attempts across multiple systems. Our team conducted a compromise assessment and found that an attacker had accessed a privileged service account through a previously undetected vulnerability. The assessment allowed the company to contain the threat before customer data was compromised.

3. Data Breach & Exfiltration Investigation

Tracks unauthorized data access and evaluates exposure.

- Evaluate unauthorized data access.
- Track exfiltrated information.
- Identify impacted stakeholders.

Example: A professional services firm received an anonymous tip that its customer contracts were being sold on the Dark Web. Our investigation identified the breach as a result of a misconfigured cloud storage bucket accessed by an external threat actor. We assisted the firm in assessing the full scope of the breach, notifying affected customers, and implementing data loss prevention measures.

4. Advanced Persistent Threat (APT) Investigation

Detects sophisticated, persistent threats in your environment.

- Uncover advanced threat actors.
- Analyze persistent network and endpoint activities.
- Attribute attacks through forensic analysis.

Example: A multinational technology company reported recurring unauthorized access to its internal databases. Our team identified a well-coordinated attack involving credential stuffing, lateral movement, and persistence mechanisms. The forensic investigation discovered multiple compromised endpoints, and the company implemented a zero-trust security model to mitigate future threats.

5. Incident Containment & Remediation Support

Rapid intervention to halt attacks and restore security.

- Implement immediate containment measures.
- Develop thorough remediation strategies.
- Strengthen controls against future breaches.

Example: A financial institution suffered a ransomware attack that disrupted its online banking services. Our forensic team quickly identified the malware strain, isolated infected systems, and worked with IT to restore operations from clean backups. Post-incident, we provided enhanced endpoint security recommendations to reduce the risk of reinfection.

6. Insider Threat Investigation

Focused analysis to address internal security risks.

- Investigate suspected internal threats.
- Collect critical forensic evidence.
- Provide conclusive evidence and recommendations.

Example: A healthcare provider suspected that an employee had accessed patient records without authorization. Our forensic investigation revealed that the employee had exported sensitive medical data onto a personal USB device before resigning. The evidence supported legal action, and on Coalfire's advice, the provider strengthened access controls to reduce the probability of similar incidents.

7. Phishing & Social Engineering Investigation

Examines fraudulent communications to secure accounts.

- Analyze phishing attacks.
- Identify compromised credentials.
- Enhance security through targeted training.

Example: A financial advisory firm experienced a phishing attack that tricked multiple employees into disclosing credentials. Our investigation identified the attacker's infrastructure, traced compromised accounts, and assisted in revoking unauthorized access. We then conducted phishing awareness training and implemented domain-based message authentication policies to strengthen email security.

8. Business Email Compromise (BEC) Investigation

Specialized email breach analysis to prevent future incidents.

- Inspect email logs and compromise indicators.
- Trace unauthorized data exfiltration.
- Recommend robust email security practices.

Example: A law firm discovered that multiple fraudulent wire transfer requests had been sent from a partner's email account. Our forensic analysis uncovered that attackers had bypassed MFA through a phishing attack, gained access to the mailbox, and created auto-forwarding rules to monitor ongoing communications. We assisted the firm in revoking unauthorized access, removing persistence mechanisms, and implementing additional email security controls.

9. Cloud Identity & Access Management Breach

Analyzes breaches of cloud identity solutions.

- Investigate unauthorized identity access.
- Assess privilege escalation risks.
- Strengthen identity security and MFA controls.

Example: A SaaS provider discovered that an attacker had accessed a privileged admin account in their cloud environment. Our forensic team determined that an exposed API token had been exploited, allowing unauthorized access to customer accounts. We assisted with incident response, revoked compromised credentials, and recommended policy changes to enforce stronger access controls.

10. Web Application & Cloud Security Incident Response

Rapid assessment and mitigation of web and cloud breaches.

- Investigate web-based security threats.
- Confirm compromised cloud accounts.
- Evaluate potential lateral data exposure.

Example: A SaaS company experienced a security breach where customer data was accessed without authorization. A forensic investigation revealed that an attacker exploited a misconfigured API endpoint to bypass authentication, allowing them to extract sensitive information. The company required an end-to-end cloud security review to determine the full scope of the attack, assess AWS logs, and identify whether any privilege escalation had occurred.

11. SQL Server Forensics

Detailed forensic review of database compromises.

- Trace database activity and changes.
- Verify data integrity pre- and post-incident.
- Uncover unauthorized data manipulations.

Example: A manufacturing company suspected financial discrepancies in its internal databases. Our forensic team analyzed SQL transaction logs and discovered that a rogue employee had been modifying invoice records to divert funds to unauthorized accounts. The evidence supported internal disciplinary action and helped recover lost revenue.

12. Litigation Support & Expert Witness Services

Expert forensic support for legal proceedings.

- Secure and analyze digital evidence.
- Provide credible expert testimony.
- Assist legal teams and law enforcement.

Example: An e-commerce company was involved in a contractual dispute. A third party alleged that a cybersecurity breach was caused by negligence. Our forensic experts examined network logs and system activity, confirming that the breach originated from a third-party supplier's compromised account, rather than an internal security failure. This evidence helped the company defend itself in court.

Why Coalfire?

World-class Partnerships

Strong partnerships with leading security vendors ensure access to cutting-edge solutions, tailored integrations, and proven reliability. By aligning with industry leaders, Coalfire delivers unmatched value, empowering our clients with the tools they need to stay secure.

Tailored Delivery Experience

Coalfire experts are dedicated specialists in specific frameworks, ensuring tailored solutions for each client. They understand the entirety of our client's business and function as strategic partners rather than just one-time vendors.

Measurable Success

Regularly tracking success and optimizing processes ensures clear progress, accountability, and real-time insights. Coalfire's proactive approach sets us apart, empowering you to adapt quickly, achieve measurable results, and stay ahead of evolving security threats.

For more information visit coalfire.com/cybersecurity-services or [contact us](#).