DIGITAL FORENSICS AND INCIDENT RESPONSE

"The power of forensic analysis at your fingertips."

Digital Forensics and Incident Response (DFIR) investigate and responds to cyber incidents such as data breaches, network intrusions, and malware attacks. It involves collecting and analyzing digital evidence to identify the scope of the incident, contain it, and recover from it. DFIR includes various techniques and tools such as forensic imaging, malware analysis, network analysis, and log analysis. DFIR aims to minimize the damage caused by cyber incidents and prevent them from recurring.

IS YOUR ORGANIZATION DFIR READY?

Digital Forensic and Incident Response (DFIR) services protect against the harmful impact of cyber incidents in the following ways. If your organization does not have any of the following capabilities, your organization is not DFIR ready.

Early detection

DFIR helps detect cyber incidents early, allowing organizations to respond quickly and prevent further damage. According to IBM's 2021 Cost of a Data Breach Report, organizations that could detect and contain a data breach in less than 200 days saved an average of $1.2 million.

Effective response

DFIR provides a comprehensive approach to managing cyber incidents, including investigation, containment, and recovery. A study by the Ponemon Institute found that organizations with a well-defined incident response plan had an average cost savings of $1.23 million per breach.

Mitigation of damage

DFIR helps mitigate the damage caused by cyber incidents. For instance, ransomware attacks can result in data loss and business interruption. A report by Cybersecurity Ventures found that global ransomware damage costs are predicted to reach $20 billion by 2021, up from $11.5 billion in 2019. DFIR services can help prevent such incidents and mitigate the impact if they occur.

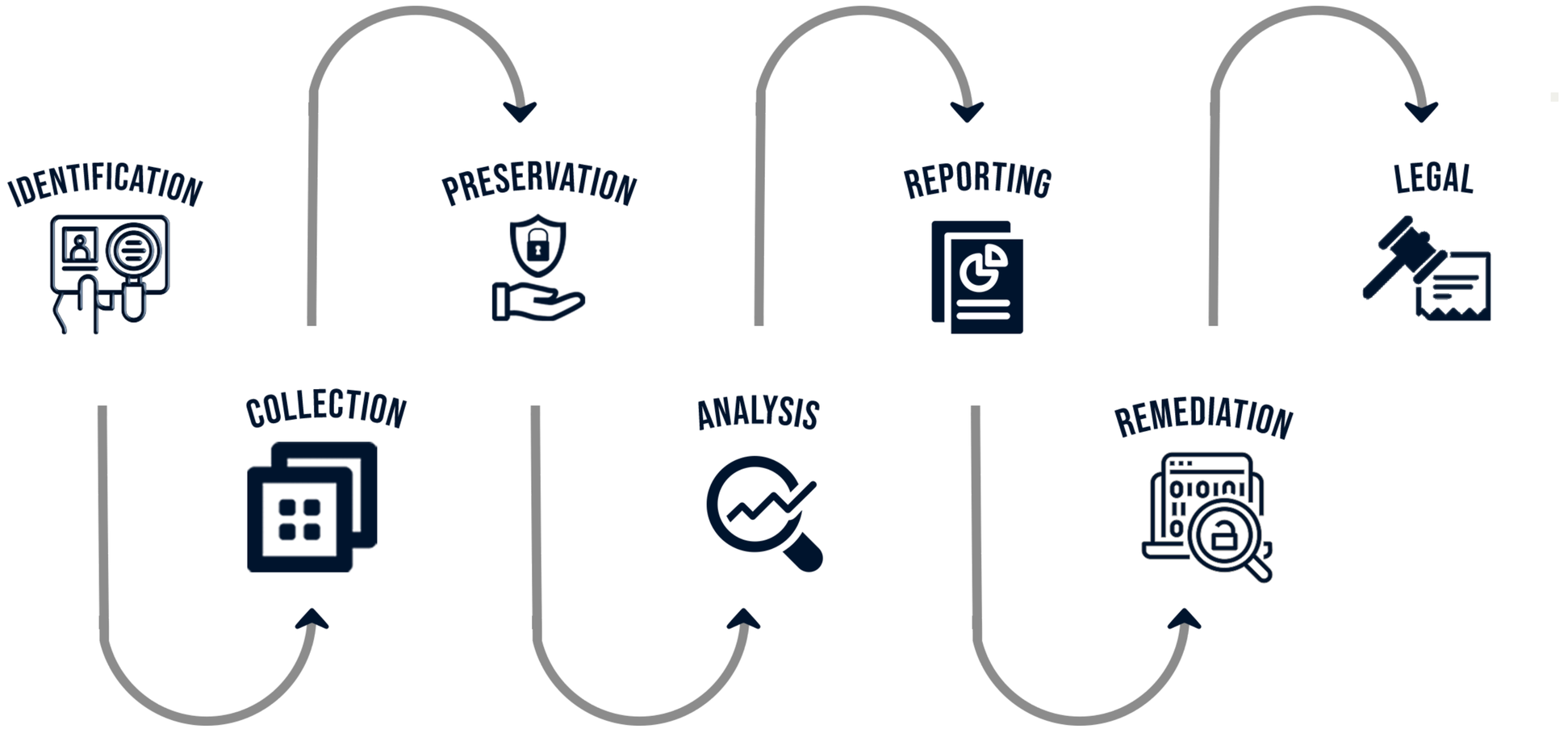
Prevention of future incidents

DFIR helps organizations identify vulnerabilities and prevent future incidents. For instance, a vulnerability assessment can help identify weaknesses in an organization's network or system, which can be addressed before cybercriminals exploit them.

APPROACH & METHODOLOGIES

- **Identification:** This involves identifying the scope of the incident, the affected assets, and the potential impact of the incident.
- **Collection:** This involves the collection of evidence, such as network logs, system images, and other relevant data.
- **Preservation:** This involves preserving the integrity of the evidence collected by following proper chain of custody procedures.
- **Analysis:** This involves analyzing the collected evidence to identify the incident's cause and extent and determine the best course of action.

- **Reporting:** This involves preparing a comprehensive report of the findings and recommendations for the future prevention of similar incidents.
- **Remediation:** This involves taking steps to mitigate the incident's impact and prevent similar incidents from occurring in the future.
- **Legal:** This involves ensuring that all legal requirements and obligations are met during the investigation and reporting phases, including compliance with data privacy and security laws.



TYPES OF DFIR SERVICES

- **Network Forensics:** Investigation of network traffic to identify potential security breaches, malware infections, or other unauthorized activities.
- **Memory Forensics:** Analysis of a computer's volatile memory (RAM) to identify evidence of malicious activity or to recover data that may have been lost due to a system crash.
- **Malware Analysis:** Reverse engineering of malware to identify its purpose and functionality, as well as develop techniques for detecting and removing it from infected systems.
- **Cybercrime Investigations:** Investigation of cybercrimes such as hacking, data breaches, and identity theft.
- **Incident Response:** Rapid identification, containment, and mitigation of security incidents to minimize their impact on an organization.
- **Forensic Data Recovery:** Data recovery from damaged or corrupted digital storage devices such as hard drives, USB drives, and memory cards.
- **Forensic Accounting:** Analysis of financial data to identify potential fraud or other financial crimes.
- **Social Media Investigations:** Collection and analysis of information from social media platforms to support investigations into cybercrimes, fraud, and other types of criminal activity.
- **Digital Evidence Analysis:** Analysis of digital evidence such as emails, chat logs, and other electronic communications to support investigations and legal proceedings.
- **Cyber Threat Intelligence:** Collection, analysis, and dissemination of intelligence about potential cyber threats and vulnerabilities, as well as developing strategies and tools for defending against them.

WHY US?

DFIR services involve investigating and responding to cyber incidents such as data breaches, network intrusions, and malware attacks. Outsourcing these services can be beneficial for several reasons:

- **Specialized expertise:** Provides customer access to specialized expertise that may be available in various ways and have a team of experienced professionals investigating and responding to cyber incidents. We have the necessary skills, knowledge, and tools to handle even the most complex cases.
- **Cost-effective:** Building an in-house DFIR team can be expensive, requiring hiring and training staff, acquiring the necessary tools and equipment, and maintaining the infrastructure. DFIR can be cost-effective since we already have the necessary infrastructure and expertise.
- **Faster response time:** DFIR incidents require a rapid response to minimize damage and prevent further compromise. Can help reduce the response time as experts are available 24/7 and ready to respond quickly to incidents.
- **Reduced liability:** DFIR incidents can result in legal and financial consequences. Can help organizations to follow industry best practices and meet legal and regulatory requirements.
- **Scalability:** Incidents can occur anytime and require an immediate response. DFIR provides the flexibility to scale up or down as per the organization's needs.

CONTACT US

CONTACT US NOW!

+1.612.532.5539 mohammed@archlightsolutions.com www.archlightsolutions.com