Privia SECURITY

Digital Forensic Incident Response (DFIR) Service

Professional Forensic Services

"Secure Digital Evidence"

The information contained in this document pertains to the Forensic Services performed by Privia Security Information Technology and Consultancy Services Inc. and is of a **general** nature. All information in this document is publicly available.

Queen Elizabeth Olympic Park, 14 East Bay Lane, Plexal, London, England, UK, E20 3BS

info@priviasecurity.co.uk

www.priviasecurity.co.uk

“Collecting and preserving digital evidence is a critical milestone for ensuring justice. With the Forensic Analysis Service, evidence gathered against threats provides a foundation for legal processes.”

The Forensic Analysis Service is designed for tracing the footprints of digital attacks, collecting the obtained data for storage in legal processes and conducting analysis and examination. As a result of security breaches in the cyber realm, preserving digital evidence carries great legal importance. The Forensic Analysis Service ensures that digital evidence to be used specifically in detecting data breaches, leaks, cyberattacks and malicious activities is secured.

Through forensic analysis processes, information about the source of the incident and the details of the attack is collected in accordance with legal compliance. As a result of the conducted analyses, it is determined how the attack was carried out, which systems were affected and which methods were used. The analysis process is critically important for identifying the attacker and reaching a legal conclusion. The advanced technologies and methods used during the forensic analysis process ensure that the analyses are reliable and legally valid. In particular, incident response, digital evidence collection and preservation processes are carried out in accordance with security standards and laws. Procedures such as the chain of custody are implemented to guarantee the legal validity of the data.

Forensic analysis processes cover a broad area, including data recovery, incident response, tracing and digital forensics laboratory work. Our forensic experts examine cyber incidents in detail, report on the digital evidence related to the case and present valid evidence that can be taken to court. With the Forensic Analysis Service, a reliable flow of information required by legal processes is provided. The Forensic Analysis Service ensures that events occurring in the cyber world are clarified.

Service Components

Digital Evidence Collection

During the digital evidence collection process, all traces left in the digital environment after an attack are gathered and preserved for analysis. To maintain the legal validity of the evidence, every step is carefully documented and evidence preservation protocols are followed. Data is protected using special methods so that it remains admissible in legal proceedings. No manipulation is performed on the collected evidence, thereby preserving the integrity of the data.

Case Examination

In the case examination process, the systems, applications, services and devices where the attack occurred are examined in detail from a forensic perspective. Comprehensive analyses are performed to determine the source of the cyber incident and its mode of propagation. The work carried out aims to identify how the incident occurred and which systems were affected. Through case examination, attackers' traces are detailed, revealing the technical, tactical and procedural methods behind the attack.

Operating System (OS) Forensics

OS Forensics involves analyses conducted on operating systems to trace the attacker's actions and traces. Forensic analyses at the OS level examine system logs, user accesses and file operations to uncover the details of the attack. Evidence within the operating system is collected, analyzed and preserved in a manner that maintains legal validity. In particular, the integrity of log files on the system is protected and procedures are followed in compliance with digital evidence preservation protocols.

File System Forensics

File System Forensics covers the detailed examination of file systems. Traces left by the attacker in the file system and any modifications made are analyzed to investigate file manipulations, deleted files, malicious files and access logs. Evidence is obtained regarding exactly when and by whom data was accessed or modified. File System Forensics is especially critical for data recovery operations and provides legally admissible evidence for court proceedings.

Mobile Forensics

Mobile Forensics includes forensic analyses carried out on mobile devices, examining digital evidence obtained from devices such as smartphones and tablets. In these analyses, critical data such as messages, call records, application data and location information within the device are collected. Analyses conducted on mobile devices play an important role in determining the individuals connected to a crime, the timing of the event and the attacker's movements.

Network Forensics

Network Forensics involves analyzing data traffic over the network to gather information about the sources and methods of the attack. Thanks to data obtained from network traffic, it is determined which protocols and connection paths the attackers used. During the analysis process, IDS/IPS logs, firewall records and gateway information are examined in detail. Network forensic analysis determines at which stages and how the attack occurred, enabling preventive measures against similar attacks in the future.

Data Recovery and Analysis

Data recovery efforts are undertaken to access data that was damaged or deleted during an attack. By conducting analyses on file systems and backups, lost data can be retrieved while maintaining data integrity. With the special techniques used in the process, the impact of data loss is minimized and data is restored as much as possible. Data recovery is a crucial phase in the forensic analysis process and the recovered data is protected using special methods to ensure its legal validity.

Log and Trace Examination

In cyber incidents, system, application and service logs/traces are analyzed to understand the source and details of the attack. Log files are used to determine which users accessed systems at which times and what actions they performed. Trace examination work reveals which techniques the attacker used and how they proceeded. The analyses performed are extremely important for identifying the attacker’s identity and the methods they employed.

Forensic Reporting

At the end of the analysis process, all findings are compiled into a detailed report. The prepared report explains how the attack occurred, which systems were affected and which steps were taken. Additionally, the report can be reviewed by technical teams and legal units and replicated for use in legal proceedings. The reports are reliable and verifiable, containing the necessary evidence for court cases.

Digital Evidence Preservation

Ensuring the protection of collected evidence and its secure storage for use in legal processes. Evidence security is maintained in both physical and digital environments to prevent unauthorized access. Secure preservation processes guarantee that evidence remains valid for extended periods. The environments in which evidence is stored are protected by stringent security protocols and monitoring systems.

FAQ

What is forensic analysis?

Forensic analysis encompasses detailed examinations carried out to clarify cybersecurity breaches and use digital evidence as proof in legal processes. Through analyses, the details of the attack are uncovered, evidence is gathered and how the incident occurred becomes understandable. Forensic analysis is conducted in various digital domains, such as file systems, network traffic, mobile devices and operating systems. Digital evidence plays a critical role in elucidating the incident and is securely preserved to ensure legal validity. The findings obtained are reported for legal processes and carry the status of reliable evidence.

In which situations is forensic analysis performed?

Forensic analysis is carried out in many situations, such as data breaches, cyberattacks, detection of malicious software and data losses. When companies or individuals face cyberattacks, the forensic analysis process is activated to reveal the details and impact of the attack. Forensic analysis is crucial for understanding the source of the attack, the methods and techniques used and the scale of the incident. In particular, it plays a critical role in gathering and preserving evidence that will be used in legal proceedings.

Which tools are used in forensic analysis?

Specialized software and tools developed specifically for forensic analysis are used. Among the tools used are EnCase, FTK, X-Ways Forensics and Autopsy. For network traffic analyses, network monitoring tools such as Wireshark are also employed to examine attack vectors and techniques. The tools used collect traces of the attack and analyze user activity and system logs. Hash algorithms are used by these tools to maintain evidence integrity.

How does the evidence collection process work in forensic analysis?

In the evidence collection process, digital evidence at the scene is identified and collected with appropriate tools, then securely stored. The chain of custody protocol is implemented to ensure the integrity and reliability of the collected evidence. The obtained data is preserved using special storage methods so that it can be used as valid evidence in legal proceedings. During the storage and preservation of data, security measures are taken to prevent unauthorized access. Additionally, every operation performed on the evidence is recorded to maintain its legal validity.

How are forensic analysis reports used in legal processes?

Forensic analysis reports are detailed documents that explain the details of the attack and the digital evidence. These reports describe how the incident occurred, which systems were affected and the path followed by the attacker. Reports prepared for use in legal authorities include all findings related to the incident and present reliable evidence. Reports are formatted in a way that all parties involved in the judicial process can understand. Furthermore, the technical details and the evidence underpinning the findings are also included in the report.

How long does the forensic analysis process take?

The duration of the forensic analysis process varies depending on the complexity of the incident and the amount of digital evidence to be collected. In a simple data breach scenario, the analysis process may take a few days, while in large-scale attacks, it can last for months. Each phase—evidence collection, analysis and reporting—requires time. Analyses conducted over extensive and distributed networks or a large number of assets require a longer duration. Additionally, in some cases, system remediation or reconfiguration may further extend the process.

Can the source of the attack be determined through forensic analysis?

Yes, forensic analysis can largely determine the source of the attack. During the analysis process, the attacker's IP address, ports used, malicious software utilized and actions performed on the system are identified. The information obtained shows which devices initiated the attack and how it was carried out. By examining network and system logs in detail, the attacker's path is reconstructed. Identifying the source is critically important for legal proceedings in determining the attacker's identity and uncovering the crime.

What is the chain of custody and why is it important?

The chain of custody is a process that documents who handled the collected digital evidence at each step and how it was processed. The chain of custody is regularly recorded to ensure the legal validity of the evidence. All operations performed during the collection, storage and analysis of evidence are recorded to guarantee reliability. Thanks to this chain, every action performed on the evidence can be traced and the integrity of the evidence is preserved.

How are security vulnerabilities detected in forensic analysis?

In forensic analysis, security vulnerabilities are determined by examining digital traces and system logs. Detailed analyses of the systems where the attack took place reveal the vulnerabilities exploited by the attackers. In particular, by examining network traffic and changes in the file system, it is determined where the security gaps exist. The information obtained is used in post-incident system remediation and in closing security gaps.

Your Trusted Partner in Cybersecurity

Founded in 2018 with a vision for the future of cybersecurity, Privia Security has been committed to delivering high-quality services to its clients from day one. With a strong and capable team, we provide the most reliable and comprehensive solutions across all areas of cybersecurity, ensuring our clients are well-protected in today's digital landscape.

As cyber threats continue to evolve rapidly and grow in complexity, combating them becomes increasingly challenging. At Privia Security, we offer both defensive and offensive cybersecurity strategies powered by cutting-edge technology to meet our clients' evolving needs. Through our innovative R&D products and strategic consultancy, we aim to enhance organizations' cybersecurity maturity and deliver proactive, tailored solutions. We are proud to be safeguarding the digital assets of more than 300 major organizations.

Global and Local Cybersecurity Solutions

Privia Security delivers cybersecurity services across a broad geographical scope, including Europe, Asia, the Middle East, and the Americas. Our specialized teams in Offensive, Defensive, and Forensic operations develop bespoke solutions for organizations operating in diverse sectors such as critical infrastructure, avionics systems, corporate networks, and the military.

In addition, our innovative cyber warfare simulation platform, PriviaHub, offers comprehensive solutions for nations seeking to strengthen their cyber defense capabilities. PriviaHub enables the testing of cyber warfare strategies, execution of simulations, and assessment of expert competencies. Designed to meet the exercise needs of private sector entities, academic institutions, and military organizations, it bridges the gap between training and real-world readiness.

A Secure Future Through Advanced Technology

With R&D centers located in Istanbul, Ankara, London, and at Cumhuriyet Technopark, we are continuously developing value-driven projects for our clients. From penetration tests and red team operations to cybersecurity training and custom enterprise solutions, we are redefining the standards in our industry. Through our slogan "**Privacy For You**" we bring a fresh, innovative perspective to security and privacy—ensuring that our clients' digital futures are secure.

Privia
SECURITY