Forensic Analysis Services

Forensic Analysis Services from BeSecure

In today's environment, information security forensic analysis is frequently needed to encompass complex networked environments, where investigation needs to encompass an entire operating environment, including a multitude of servers (e.g. file, print, communications and e-mail), as well as remote access facilities.

- Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence through forensic analysis should be collected, retained, and presented in support of potential legal action in accordance with the rules for evidence in the relevant jurisdiction(s).
- Where identified by prior assessment as required for evidential purposes, de facto in the context of a significant information security incident, information security forensic analysis should also be conducted.

Our Forensics Analysis Services involve the use of IT based investigative techniques and tools, supported by documented procedures, to review the designated information security incident(s) in more detail. Our Information security forensic analysis IT based tools comply with standards such that their accuracy cannot be legally challenged, and are always be kept up-to-date in line with technology changes.

BeSecure Forensic Analysis Activities

- Activity to ensure that the target system, service and/or network is protected during the information security forensic analysis from being rendered unavailable, altered or otherwise compromised, including by malicious code (including viruses) introduction, and that there are no or minimal effects on normal operations.
- Activity to prioritize the acquisition and collection of evidence i.e. proceeding from the most volatile to the least volatile (this depends in large measure on the nature of the information security incident).
- Activity to identify all relevant files on the subject system, service and/or network, including normal files, password or otherwise protected files, and encrypted files
- Activity to recover as much as possible discovered deleted files, and other data
- Activity to uncover IP addresses, host names, network routes and web site information
- Activity to extract the contents of hidden, temporary and swap files used by both application and operating system software.
- Activity to access the contents of protected or encrypted files (unless prevented by law).
- Activity to analyze all possibly relevant data found in special (and typically inaccessible) disc storage areas.

besecure
Managed E-Business Security™

- Activity to analyze file access, modification and creation times.
- Activity to analyze system/service/network and application logs. Activity to determine the activity of users and/or applications on a system/service/network. Activity to analyze e-mails for source information and content. Activity to perform file integrity checks to detect Trojan horse files and files not originally on the system. Activity to ensure that extracted potential evidence is handled and stored in such a way that it cannot be damaged or rendered unusable, and that sensitive material cannot be seen by those not authorized. It is emphasized that evidence gathering should always be in accordance with the rules of the court or hearing in which the evidence may be presented Activity to conclude on the reasons for the information security incident, the actions required and in what timeframe, with evidence including lists of relevant files included in an attachment to the main report. Activity to provide expert support to any disciplinary or legal action as required.

About BESECURE

We are a leading provider of Governance, Risk & Compliance (GRC) services, Cyber Security solutions, Managed Security services, Certification Training and Awareness programs, trusted by global organizations across telecommunication, financial services, energy industries and other medium - large enterprises to safeguard their information assets including financial information, intellectual property, trade secrets, Personally Identifiable Information (PII) or information entrusted to them by customers or third parties. We have been recognized from Enterprise Security Magazine to be among the top 10 Cyber Security Consulting/Services Companies in Europe. We offer Governance, Risk, and Compliance Services (GRC Services) that address the audit & assurance, risk & compliance, continuity and incident management needs of our customers. Our second division relates to the delivery of Enterprise Security Solutions that deal with challenging aspects such as fraud prevention, threat detection & response, identity & access management, IoT security, cloud security and information protection, among others. Our Managed Security Services strengthen our customers cyber defence programs often at a fraction of the cost of in-house security resources utilizing BesecureCloud big data and supercomputing capabilities. Through established Security Operations Center and innovative security solution offering as a service we provide the next generation EAL 3+ certified hybridSIEM service supported by big data, threat intelligence and user behaviour analytics. We further enhance our clients' awareness of security by offering comprehensive vendor-neutral business continuity, information security, ISO 27001, risk management certification on premise or e-learning training courses and awareness briefings for executive management, security and system administrators and corporate users. Through established subsidiaries in Belgium, Greece and Cyprus we support customers from Western Europe, Southeast Europe and Middle East.