activebytes
innovations

Datasheet

CYBER FORENSICS

ActiveBytes keeps abreast of the ever-changing cyber environment and threats. By partnering with our forensics, you are assured of your readiness before, during and after an attack. With us you can find peace of mind when navigating the complexity of digital incidents, such as fraud, theft and industrial espionage. We offer fully managed cyber forensics services to identify the compromised elements of the IT infrastructure, isolate them and forensically preserve the data evidence for analysis.

We understand that enterprises face many issues with computer forensic matters. To help them address the potential challenges, our computer and cyber forensics team offers a full range of services across the forensic, discovery, and investigative lifecycles. With a focus on authentication and chain of custody preservation, our technical team uses court-tested and defensible techniques to collect and preserve information. We analyze the devices, system, network communication and memory image so that accurate conclusions can be drawn regarding the security incident. Through our blend of people, methodology and technology, we can provide rapid reporting and an understanding of the systems attacked to help triage the data at risk.

We have our own methodology that ensures that all requirements are met when collecting digital evidence from workstations, servers, external media and network or security technologies.

Our Approach

- Data collection and preservation
- Internal and incident response
- Forensic analysis and data analytics
- Detect insider theft
- Study information stolen
- Disaster recovery
- Responder services

activebytes innovations

Stages of The Investigation

Identification 1

In the identification phase, potentially responsive electronic documents are identified for further examination and review

Collection & Preservation 2

We extract potentially relevant information from its native source. During preservation, data is placed in a legal hold to ensure precision, integrity, authenticity etc.

Processing 3

The processing phase involves forensics analysis and data analysis of collected information. This is typically performed by specialized software, and can include the extraction of text and metadata, removing of duplicates, performing keyword searches and converting files

Detect insider theft 4

If any insider is part of the data breach, then it will be proved during the analyzed data

Study stolen information 5

An insight into the data stolen can reveal the motive behind the attack

Disaster recovery 6

The recovery process becomes more effective when the lost data is extracted and reconstructed through forensics

Respond 7

The report from our team will include a detailed summary of results from analysis and actionable information to aid response in the containment, eradication and recovery phase

Key Features

- Details of the incident including the data that was compromised and the time of the incident
- Uncovering the responsible insiders if any
- Discover the weakness in your security system that led to the attack
- Identify and traces paths of Advanced Persistent Threats (APT)
- Expert report admissible in a court of law
- Ethical conduct ensuring complete confidentiality and sensitivity

Benefits

- Recover he data deleted by the adversary
- Retrace hacker's steps and map the tools used in attack
- Know the duration of unauthorized access in the network
- Identify possible motive of the attack

Contact us

contact@active-bytes.com +971 50 513 3973

www.active-bytes.com