Mahdi Ghaznawy

Investigative Plan of Action

Strategy for Evidence Collection and Organizational Impact Minimization

To maximize evidence collection while minimizing disruption to the organization, our team will follow a structured and discreet approach. We will first conduct a preliminary risk assessment to determine the scope of the potential breach and identify key systems where evidence might be located. The collection process will prioritize capturing volatile data, such as system logs and active memory, before moving to non-volatile storage, like hard drives and external devices. To minimize operational disruptions, we will perform imaging of hard drives rather than direct analysis on live systems. Additionally, we will schedule forensic activities during non-peak hours and work closely with IT personnel to ensure business continuity.

Tools and Techniques for Evidence Gathering, Preparation, and Analysis

Our team will utilize both hardware and software forensic tools to conduct an accurate investigation. We will use write-blockers to prevent data from being unintentionally modified for evidence gathering. Digital Forensic tools like EnCase, FTK (Forensic Toolkit), and Autopsy will be utilized for disk imaging, data carving, and file system analysis. Network logs will be analyzed by tracking data transmissions with tools like Splunk and Wireshark. We will create cryptographic hashes of the collected evidence using SHA-256 or MD5 techniques to authenticate and protect the evidence. Our preparation procedure will include appropriate documentation of chain-of-custody logs to preserve evidence integrity throughout the investigation.

Collection and Preservation of Evidence Using Standardized Procedures

To ensure compliance with forensic best practices, our team will adhere to industry-standard procedures such as those outlined in the National Institute of Standards and Technology (NIST) and the International Organization on Computer Evidence (IOCE). We will first isolate and secure affected devices to prevent tampering. Next, forensic images will be created using write-protected tools to maintain the original state of digital evidence. Data logs from servers, employee access records, and emails will be collected and preserved. Each piece of evidence will be labeled, documented, and stored in a secured forensic lab with restricted access. We will also follow strict chain-of-custody protocols to maintain the integrity of the evidence.

Examination of Seized Evidence for Policy Violation Correlation

Our forensic examination will begin with keyword searches and file analysis to identify proprietary documents that may have been accessed or transferred by John Smith. We will use timeline analysis to reconstruct his digital activity and verify whether unauthorized data exfiltration occurred. Email analysis, USB device logs, and internet browsing history will be reviewed for potential communication or transmission of proprietary information. Additionally, file metadata will be analyzed to check for signs of document modification, deletion, or unauthorized access attempts. Our team will also conduct hash comparisons against company proprietary files to determine if they were copied or altered.

Approach for Drawing Conclusions from Digital Evidence

Our team will apply a systematic methodology to draw valid conclusions based on numerous digital evidence sources. We will compare logs, timestamps and access records to develop a timeline of events. Behavioral analysis will determine if John Smith's actions are in line with normal employee behavior or constitute deliberate misconduct. In case direct evidence is insufficient, we will look for circumstantial evidence, including unusual login patterns, unauthorized software program installations, or data transfers to external devices. Our conclusions will be based on objective findings and satisfy the burden of proof for disciplinary and legal action.

Presentation of Case Details and Conclusions to Senior Management

Our investigation will lead to a forensic report summarizing our investigation, the methodology, collected evidence, and conclusions. The report will be formatted to be clear and understandable for senior management and legal personnel. Charts, diagrams, and timelines will be used to illustrate key points. We will make a formal presentation of key evidence, analysis outcomes, and recommended actions. Legal or policy implications will be talked about with the legal team. Finally, we'll make recommendations for improving data security policies and preventing further breaches.