Kiarah Pettaway
11/05/2024
D431 - Task 1

A1.

Our primary focus in developing an action plan is to ensure thorough evidence collection while being mindful of the company's ongoing operations. Casey (2011) states that a forensic investigation must balance comprehensive data collection with operational continuity. The first step will be outlining the scope of our inquiry, including the who, what, when, where, and why. Following the outline, the briefing will clarify that John Smith is under investigation, with concerns regarding potential unauthorized access and misappropriation of proprietary information (Nelson, Phillips, & Steuart, 2018).

We will clearly define each team member's role, fostering a coordinated approach. Following this preparation, we will secure the environment by limiting access to John Smith's workspace and restricting nearby personnel, thereby safeguarding potential evidence (Vacca, 2005). This document will ensure that only essential personnel are present and preserve John's work area as it was during the timeframe of the reported incident.

A2.

Initially, we will employ write blockers to ensure that there is no alteration of data on John Smith's devices, thus preserving the integrity of the original evidence (Pollitt, 2010). Each step will be documented meticulously in a chain of custody log, recording the time, date, and personnel involved in handling the evidence to ensure transparency and admissibility. To capture a complete and bit-for-bit copy of his hard drive, we will use FTK Imager or EnCase to create forensic images while maintaining the authenticity of the original data (NIST, 2006).

Furthermore, we will utilize Volatility to conduct memory acquisitions, allowing us to preserve volatile data such as active processes and network connections. For network analysis, Wireshark will enable us to inspect any suspicious network traffic or data transfers that may suggest unauthorized access or sharing of proprietary information. Once we have amassed the data, our team will apply hashing algorithms such as MD5 or SHA-256 to verify the authenticity and integrity of the forensic images, establishing a reliable baseline for comparison during the analysis phase (Casey, 2011).

During the analysis phase, we will implement keyword searches and examine metadata to identify pertinent files, emails, and access logs that may indicate a policy violation.

A3.

To maintain the integrity and admissibility of evidence, our team will adhere to the guidelines set forth by ISO/IEC 27037, which establish industry standards for the identification, collection, acquisition, and preservation of digital evidence (Easttom, 2021). Given that the suspected violation involves proprietary information, we will prioritize compliance with the company's

Non-Disclosure Agreements (NDAs) and Acceptable Use Policies (AUPs), which define the legal framework for safeguarding sensitive data (Blythe, Coventry, & Little, 2015).

We will initiate a transparent chain of custody, meticulously documenting each step in the evidence-handling process, including details such as time, date, location, and personnel involved. To ensure data integrity throughout the investigation, we will generate hash values. This comprehensive documentation is crucial to prevent any alteration of evidence immediately after collection and to ensure compliance with the authentication requirements outlined in the Federal Rules of Evidence (FRE) 901 and 902 (Pollitt, 2010).

To further protect the evidence, each item will be labeled, tagged, and securely sealed in tamper-evident packaging to prevent any potential interference or tampering. The evidence will then be stored in a controlled-access environment per FRCP Rule 26(b) concerning evidence preservation (Casey, 2011). As proprietary information may be subject to intellectual property (IP) protections—especially if trade secrets are involved—our team will implement best practices to avoid unauthorized disclosure of this information in compliance with the provisions set forth by the Defend Trade Secrets Act (DTSA) (Sandeen & Rowe, 2017).

By rigorously adhering to NDAs, AUPs, IP laws, and forensic standards, our team ensures that all collected evidence remains legally defensible and aligns with the company's legal and operational objectives.

A4.

Our team will analyze the seized evidence to identify items related to the suspected policy violation. We will initiate this process with keyword searches for proprietary terms, project names, and specific identifiers that may indicate access to or handling sensitive information—methods essential to forensic analysis. Following this, we will conduct a metadata analysis to track file creation, modification, and access timestamps, which will aid in pinpointing any unusual activities that coincide with the suspected unauthorized access (Carrier, 2005).

Furthermore, we will scrutinize communication logs and email records for instances where proprietary information might have breached company policy (Casey, 2011). Additionally, we will analyze network activity logs to uncover any unauthorized data transfers or external access attempts, adhering to best practices in network analysis to identify suspicious connections and data flows (NIST, 2006). This focused approach enables our team to filter relevant data from the broader dataset efficiently, isolating evidence supporting or refuting the alleged policy breach.

A5.

We will begin by correlating evidence from access logs, file metadata, and network activity to establish a consistent sequence of John Smith's actions. This cross-verification will help eliminate ambiguity and enhance the credibility of our findings. Using our established hashing method, we will confirm the integrity of each piece of evidence, ensuring it remains unaltered throughout the investigation.

Once validated, we will construct a detailed timeline of John Smith's interactions with proprietary information, examining timestamps and access patterns to identify unauthorized or anomalous activities. We will then align these findings with potential policy breaches outlined in company agreements, such as nondisclosure agreements (NDAs) and acceptable use policies (AUPs).

This methodology enables us to determine confidently whether John Smith's actions constitute a violation, ensuring that our conclusions are well-substantiated and legally defensible.

A6.

Our team will curate a structured report and presentation that communicates the findings in both technical and non-technical language. We will begin with the executive summary, offering senior management a concise overview of the investigation's purpose, key findings, and conclusions regarding the suspected policy violation. This will allow them to grasp the results quickly without technical details.

Following the summary, we will present a timeline of events that visually illustrates John Smith's interactions with proprietary information. This timeline will effectively demonstrate how each piece of evidence—such as access logs, metadata, and network activity—supports our conclusions. Where appropriate, we will incorporate simplified visuals like charts or diagrams to elucidate patterns of access or data transfers that corroborate the policy breach.

The report will also include an evidence integrity section outlining the chain of custody and hashing methods used to maintain data authenticity. Finally, we will offer actionable recommendations based on our findings, such as potential disciplinary actions, policy updates, or enhanced security measures to prevent similar incidents. By presenting the case in an organized, accessible format, we enable senior management to make informed decisions based on reliable and comprehensible evidence.

Kiarah Pettaway
11/05/2024
D431 - Task 1

Citations

Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (3rd ed.). Academic Press.

Nelson, B., Phillips, A., & Steuart, C. (2018). Guide to Computer Forensics and Investigations (6th ed.). Cengage Learning.

Vacca, J. R. (2005). Computer Forensics: Computer Crime Scene Investigation (2nd ed.). Charles River Media.

National Institute of Standards and Technology (NIST). (2006). Guide to Integrating Forensic Techniques into Incident Response (NIST Special Publication 800-86).

Pollitt, M. M. (2010). "An Examination of Digital Forensic Models." International Journal of Digital Evidence, 1(3).

Blythe, J. M., Coventry, L., & Little, L. (2015). "Unpacking Security Policy Compliance: The Motivators and Barriers of Employees' Security Behaviors." Proceedings of the 2015 ACM Conference on Computer Supported Cooperative Work.

Sandeen, S. K., & Rowe, E. F. (2017). Trade Secret Law and the Defend Trade Secrets Act of 2016: Cases and Commentary. West Academic Publishing.

Carrier, B. (2005). File System Forensic Analysis. Addison-Wesley Professional.