New World Forensics
CUSTOM FORENSIC SOLUTIONS

New World Forensics LLC
JRuiz@nwf.bz
WWW.NWF.BZ
888-322-4038

Conducting an insider threat and data theft investigation utilizing digital forensics involves systematic steps and the use of specialized tools and methodologies to detect, analyze, and mitigate the threat. Here's how our company approaches this matter:

1. Preparation and Incident Response Plan

Objective: Establish a clear protocol for handling potential security breaches.

- Incident Response Team: Assemble a multidisciplinary team including IT, legal, HR, and public relations experts.

- Communication Plan: Define how the team will communicate internally and with external stakeholders.

- Forensic Readiness: Ensure that systems are configured to log all necessary events and that evidence collection procedures are in place.

2. Detection of Insider Threat

Objective: Identify potential indicators of compromise through various detection mechanisms.

- Behavioral Monitoring: Use User and Entity Behavior Analytics (UEBA) tools to detect anomalies in user activities.

- Access Logs: Regularly review logins, file access, and network activity to spot unusual patterns.

- Data Leakage Prevention (DLP) Tools: Implement DLP tools to identify and alert on potential data exfiltration.

3. Initial Investigation

Objective: Validate the alert and determine the preliminary scope of the incident.

- Incident Triage: Quickly assess the severity and extent. Prioritize based on potential impact.

- Preservation of Evidence: Ensure digital evidence is preserved without alteration. This may involve creating bit-by-bit copies of hard drives and other storage media.

- Timeline Reconstruction: Use logs and other artifacts to create a timeline of the user's actions.

4. In-Depth Forensic Analysis

Objective: Conduct a thorough investigation to uncover the full extent of the insider threat.

- Digital Evidence Collection:

  - Workstation Analysis: Review the suspect's computer for unauthorized software, deleted files, and other anomalies.

  - Network Analysis: Analyze network traffic for signs of data exfiltration.

  - Email Examination: Review email communications for evidence of data sharing or malicious intent.

- Artifact Analysis:

  - File Metadata: Investigate file creation, access, and modification details.

  - Browser History: Check for unusual web activity that might indicate data exfiltration or communication with external entities.

5. Interview and Corroborate

Objective: Corroborate digital evidence with physical interviews and other investigative techniques.

- Interviews: Conduct interviews with the suspect and colleagues to gather verbal evidence and verify timelines.

- Cross-Verification: Verify digital evidence against other sources like security cameras, physical access logs, etc.

6. Risk Mitigation and Immediate Actions

Objective: Contain the threat and prevent further damage.

- Access Revocation: Immediately revoke the suspect's access to all company systems and facilities.

- System Hardening: Address vulnerabilities that the suspect exploited.

- Data Recovery: Attempt to recover deleted or stolen data if possible.

7. Reporting and Documentation

Objective: Create a detailed report for internal review and legal purposes.

- Incident Report: Document findings, methodologies, and timelines. Include visual aids like charts and tables.

- Chain of Custody: Ensure that all evidence is logged with a proper chain of custody for legal proceedings.

- Legal Considerations: Work with legal to determine the next steps, which could include prosecution.

8. Post-Investigation Review and Improvements

Objective: Learn from the incident to strengthen the overall security posture.

- Debriefing: Conduct a thorough debriefing with all stakeholders.

- Policy Changes: Update security policies and practices based on lessons learned.

- Training: Enhance employee awareness training to prevent similar incidents in the future.

Tools Commonly Used:

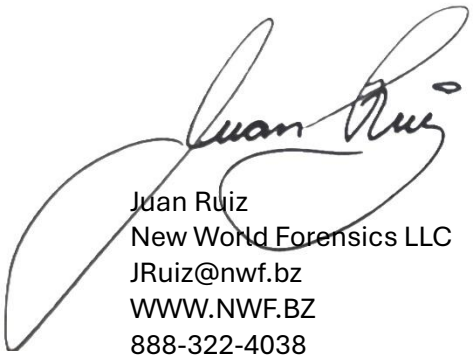
- Forensic Software: EnCase, FTK, Cyber Triage, and Sleuth Kit for disk and memory analysis.

- Network Monitoring: Wireshark for packet analysis, IDS/IPS systems.

- Log Analysis: SIEM tools like Splunk or LogRhythm.

- Email Analysis: Tools such as ExMerge or MailXaminer.

Addressing an insider threat and data theft using digital forensics is a meticulous process that requires attention to detail and coordination across multiple departments. Ensuring thorough preparation, leveraging the right tools, and following a structured approach can effectively mitigate risks and protect the organization's assets.



Juan Ruiz
New World Forensics LLC
JRuiz@nwf.bz
WWW.NWF.BZ
888-322-4038