Incident Handler's Log

Entry 1

Date: February 18, 2025

Entry: 1

Description:

Analysis of a suspected data exfiltration breach discovered through anomalous network activity. This log outlines the Detection and Analysis phase of the NIST Incident Response Lifecycle since we detected and analyzed suspicious outbound data transfers.

Tools used:

Wireshark network analyzer was utilized to inspect network traffic patterns. It captured and analyzed suspicious outbound connections with large data transfers to unknown IP addresses outside working hours. It detected repeating patterns of encrypted traffic to non-business domains.

The 5 W's:

- Who: An employee in the Marketing department, as determined by IP and system logs.
- What: Unapproved data transfer of 2.3GB to cloud storage service
- Where: Remote online session
- When: February 17, 2025, 23:00-02:00
- Where: Marketing department network area, from computer MKT-WS-042
- Why: Initial investigation suggests potential theft of intellectual property from accessed files

Additional notes:

Enforced instant network access limitation for impacted system. Coordinate with HR and Legal for further actions. Require examination of cloud storage access policy.

Entry 2

Date: February 19, 2025

Entry: 2

Description:

We are studying and deploying Suricata IDS to improve how we are monitoring the network. This falls under the Preparation phase of the NIST Incident Response Lifecycle because we are improving our detection capabilities.

Tools used:

Suricata IDS - Installed and tested custom rules to detect suspicious outgoing connections.

Developed rules that target:

- Transfers of large files at night.
- Links to known bad IP ranges
- Atypical encryption patterns

- Data exfiltration attempts

The 5 W's:
Not applicable - tool implementation activity

Additional observations:
Developed own rule set for auditing cloud storage applications. Must optimize false positives.

Entry 3
Date: 20 February 2025
Entry: 3

Description:
Investigation of a finance department employee-targeted phishing campaign. This scenario covers both Detection and Analysis and Containment stages of the NIST IR Lifecycle.

Tool(s) used:
Not applicable - incident investigation entry

The 5 W's:
- Who: External threat actor impersonating CEO
- What: A targeted phishing attack asking for urgent wire transfers.
- Date: 20 February 2025, 09:15-10:30
- Where: Finance department email systems
- Why: Trying to commit financial fraud using business email compromise.

Additional notes:

Prevented three attempted wire transfers successfully. Implementing additional email authentication measures.

Entry 4

Date: February 21, 2025

Entry: 4

Description:

Splunk SIEM implementation and testing for centralized log analysis. This falls under the Preparation phase, enhancing our ability to detect and respond to incidents.

Tools used:

Splunk SIEM - Configuration for:

- Consuming logs in real-time from significant systems - Dedicated dashboards for security controls - Automatic alerts for suspicious activity - Correlation rules for detecting attack patterns **The 5 W's:** Not applicable - tool implementation work. **Additional notes:** I successfully combined Windows Event Logs, Firewall logs, and IDS alerts. ## Thoughts/Notes **Were there any activities that were difficult?** Setting up Suricata's custom rules was the biggest challenge as we had to find a balance between detecting actual threats and avoiding false positives. This involved many rounds of testing and adjustment to achieve the optimal outcome. **Did your understanding of incident detection and response alter upon finishing this course?** I've come to value how important it is to maintain good records and have a well-defined procedure for handling incidents. The NIST model gives us a handy blueprint that helps ensure we don't overlook any important steps in incident response. Was there a specific tool or idea that you most enjoyed? Working with Splunk SIEM was quite fascinating since it possesses powerful search capabilities and effective methods of presenting data. The capability to correlate events from various data sources provided useful details concerning security trends.