Incident Handler's Journal

## Date: 2025-06-14

Entry: 1

Description:  
Investigated suspicious outbound traffic pattern indicating a potential malware beacon.

Tool(s) used:  
Wireshark, Suricata

The 5 W's:

* Who: A compromised internal workstation
* What: Repeated external HTTP connections to an unusual IP address
* When: 2025-06-12 at 14:23 EDT
* Where: Sales department subnet (192.168.20.0/24)
* Why: Endpoint was infected with malware from a phishing email

Additional notes:  
Incident entered the Detection and Analysis phase of the NIST IR lifecycle. Required escalation to Tier 2 SOC analyst.

## Date: 2025-06-10

Entry: 2

Description:  
Used Splunk to analyze login patterns and detect anomalies.

Tool(s) used:  
Splunk

Additional notes:  
Queried logins using SPL, visualized login frequency, and isolated suspicious activity after hours.

## Date: 2025-06-13

Entry: 3

Description:  
Documented incident involving brute-force SSH attack attempts.

Tool(s) used:  
Suricata, Fail2Ban

The 5 W's:

* Who: External IP from Russia (195.123.45.67)
* What: Multiple failed SSH login attempts within a short time
* When: 2025-06-13 from 01:00 to 01:30 EDT
* Where: Production server (10.0.0.5)
* Why: Automated brute-force scan targeting SSH services

Additional notes:  
Detection and Containment phases; IP was blocked, and Fail2Ban rules were tuned for SSH protection.

## Date: 2025-06-11

Entry: 4

Description:  
Used VirusTotal to validate the legitimacy of a suspicious file hash.

Tool(s) used:  
VirusTotal

Additional notes:  
Uploaded the hash and received a match with a known ransomware signature. Escalated per protocol.

# Reflections/Notes

* One of the most challenging activities was using Suricata to write custom rules. The syntax required attention to detail, and troubleshooting rule errors was difficult at first.
* My understanding of incident detection and response has improved significantly. I now appreciate the layered process of identifying, investigating, and responding to threats using real tools and logs.
* I particularly enjoyed working with Splunk. Its powerful search capabilities and real-time visualization of data made pattern recognition much easier and intuitive.