Incident handler's journal

Reflection for this section and its associated journal:

1. Were there any specific activities that were challenging for you? Why or why not?

Yes, there were difficult parts. The SIEM analysis tool was somewhat confusing as the last project. I wish I'd have a little more exposure and a more difficult task to complete to better understand the system. This was challenging because I felt like I just started to get the hang of the application, and then the assignment was over. The search terms and language were confusing to me, so I had to put in extra time understanding SPL and UDM.

2. Has your understanding of incident detection and response changed since taking this course?

Yes, my understanding of incident detection and response has changed because I better understand what recovery looks like in a security incident. I had no previous knowledge of what recovery may be like, including collaborating with other professionals in recovery. This was definitely one highlight that I learned in this course.

3. Was there a specific tool or concept that you enjoyed the most? Why?

I really enjoyed creating, analyzing, and triggering custom detection rules in Suricata. It was challenging, but I felt like I was really gaining applicable knowledge.

Date: 5/12/2025	Entry: File Hash Security Incident

Description	SHA256 file hash: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b Here is a timeline of the events leading up to this alert: ● 1:11 p.m.: An employee receives an email containing a file attachment. ● 1:13 p.m.: The employee successfully downloads and opens the file. ● 1:15 p.m.: Multiple unauthorized executable files are created on the employee's computer. ● 1:20 p.m.: An intrusion detection system detects the executable files and sends out an alert to the SOC.
Tool(s) used	Virustotal was used to analyze the SHA256 file hash which determined that the file is a type of trojan horse malware that negatively affects network communications.
The 5 W's	Capture the 5 W's of an incident. ● Who: An employee ● What: The employee downloaded and opened which executed a malicious payload onto the system ● When: At 1:13pm ● Where: On the employee's device. ● Why: The employee was tricked into downloading and executing a malicious file
Additional notes	NA

Date: 5/12/2025	Entry: Data Theft

Description	An unauthorized access incident occurred on December 28, 2022, at 7:20 p.m. PT, affecting approximately 50,000 customer records containing personally identifiable information (PII) and financial data. Timeline of Events: ● December 22, 2022 (3:13 p.m. PT): An employee received an extortion email from an unknown sender claiming to have stolen customer data and demanding $25,000 in cryptocurrency. The email was dismissed as spam. ● December 28, 2022: A second email was received from the same sender, this time including a sample of stolen data and increasing the demand to $50,000. The employee reported the incident to the security team, which initiated an investigation.
Tool(s) used	A post-incident final report was used and a “lessons learned” meeting was conducted to help the company learn how to better prevent and manage situations similar in nature in the future.
The 5 W's	Capture the 5 W's of an incident. ● Who: A malicious actor ● What: The malicious actor stole important personal information of customers. ● When: It started on Dec. 22, 3:13pm. ● Where: On the employee’s device via email. ● Why: The root cause of the incident was identified as a vulnerability in the e-commerce web application. This vulnerability allowed the attacker to perform a forced browsing attack and access customer transaction data by modifying the order number included in the URL string of a purchase confirmation page.
Additional notes	NA

Date: 5/11/2025	Entry: Phishing Incident
Description	A small U.S. primary care clinic was hit by a ransomware attack around 9:00 a.m. on a Tuesday. Employees lost access to medical records and systems, halting operations. A ransom note demanded payment in exchange for restoring encrypted files. The attack began with phishing emails containing malicious attachments that installed malware. Once inside the network, attackers deployed ransomware, encrypting critical patient data. The clinic shut down systems and reported the incident to seek assistance.
Tool(s) used	NA
The 5 W's	● Who: An organized group of unethical hackers ● What: A ransomware security incident ● Where: At a health care company ● When: Tuesday 9:00 a.m. ● Why: The incident happened because unethical hackers were able to access the company's systems using a phishing attack. After gaining access, the attackers launched their ransomware on the company's systems, encrypting critical files. The attackers' motivation appears to be financial because the ransom note they left demanded a large sum of money in exchange for the decryption key.
Additional notes	NA

Date: 5/13/2025	Entry: HR Phishing Email

Description	On Wednesday, July 20, 2022, at 9:30 a.m., a phishing email was sent to hr@inergy.com from a spoofed sender, Def Communications (76tguyhh6tg@rt7tg.su, IP: 114.114.114.114). The email impersonated a job applicant and included a malicious attachment named bfsvc.exe, disguised as a password-protected resume. The attachment's hash value matches a known malicious file. The attacker attempted to trick the recipient into opening the file using the password paradise10789, potentially leading to malware execution and system compromise. This incident represents a targeted phishing attempt and should be escalated for investigation and response.
Tool(s) used	A Playbook and flowchart were used to assess and correct the incident.
The 5 W's	Capture the 5 W's of an incident. ● Who: An threat actor ● What: A phishing email was targeted to someone in HR as a possible applicant for a job, the threat actor included a malicious downloadable link. ● When: July 20, at 9:30am ● Where: Local company in the HR department ● Why: The HR employee may or may not have downloaded malicious files, they weren't certain in their report.
Additional notes	NA