Incident handler's journal

Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this journal as a way to log the key takeaways about the different cybersecurity tools or concepts you encounter in this course.

Date: February 17, 2025	**Entry:** #1
Description	Documenting a Cybersecurity incident - Ransomware attack at a small healthcare clinic, focusing on the Containment, Eradication, and Recovery phases of incident response.
Tool(s) used	None
The 5 W's	• **Who** caused the incident? An organized group of hackers who are known to target organizations in healthcare and transportation industries. • **What** happened? These threat actors deployed malware via targeted phishing emails (spear phishing), gained access to the organization's systems, and encrypted critical files including medical records. This attack created significant disruptions to the company's day-to-day operations, preventing employees from accessing files and software, and therefore, impacting patient care, revenue, and public trust. • **When** did the incident occur? Tuesday 9:00 AM local time

	• **Where** did the incident happen? At the small U.S. health care clinic specializing in delivering primary-care services. • **Why** did the incident happen? The threat actors were motivated by financial gain. They demanded a large lump sum of money in exchange for the decryption key to restore access to the encrypted files.
Additional notes	• How can this small healthcare clinic prevent a similar security incident from happening again? • What can we learn from prior similar security incidents in the healthcare sector? • Should the company pay the ransom to retrieve the decryption key? What are the legal implications? What is the likelihood of data recovery? Will paying a ransom encourage future attacks? **Preventative Measures:** • **Managerial Controls**: Implement security awareness training focused on recognizing phishing attempts. • **Operational Controls**: Apply principle of least privilege and separation of duties to limit potential impact of compromised accounts. • **Technical Controls**: Email filtering capabilities, anti-ransomware software on the endpoints, and routine offline backups of critical patient data. • **Compliance Considerations**: Follow HIPAA requirements for data protection.

Date: February 24,	**Entry:** #2

2025	
Description	Documenting the containment, eradication, and recovery phases of a security incident involving a password-protected malicious spreadsheet attachment delivered via phishing email to an employee at a financial services company. Analysis conducted to identify various indicators of compromise (IoC) using the Pyramid of Pain framework.
Tool(s) used	VirusTotal was used to analyze a malicious file hash, specifically a SHA256 hash. VirusTotal is a public threat intelligence resource used to analyze suspicious files, domains, IPs and URLs to detect malware and other breaches. The resulting reports, in turn, are shared with the security community. The reports are shared with the security community to improve collective cyber defense.
The 5 W's	• **Who**: A threat actor with an alias of “Def communications” and “Clyde West”, identified in the email. • **What**: A phishing attempt was sent via email to one of the employees asking to download a password-protected spreadsheet containing malicious code. When opened, it executed a malicious payload on the employee's computer. • **When**: July 20, 2022 09:30:14 AM Local Time • **Where**: At a financial services company, specifically on an employee’s workstation. • **Why**: The incident happened because a threat actor or group successfully deployed a payload on the employee’s computer. The attacker’s motivation appears to be establishing command and control within the organization's network. Without prompt detection of this security incident, the attacker may have become an advanced persistent threat (APT) with long-term access to the company’s systems.

Additional notes	1. How could the financial services company prevent an incident like this from occurring in the future? 2. Would managerial controls have prevented this incident from occurring in the first place? 3. What email service provider is this company using? Could a more reputable provider have detected this malicious email via a robust email security solution, potentially preventing the employee from clicking on the link in the first place? 4. Would the principle of least privilege and separation of duties have at least decreased the impact of the incident? **Potential Solutions:** ● **Email Security**: Advanced email filtering with attachment scanning capabilities and password-protected file detection. ● **User Training**: Security awareness training on phishing techniques. ● **Endpoint Protection**: Advanced endpoint detection and response (EDR) solutions that can detect malicious behavior after payload execution. ● **Access Controls**: Principle of least privilege and separation of duties to limit the spread of malware from infected endpoints. ● **Detection Capabilities**: Alert mechanisms to catch suspicious activities before becoming a larger issue.

Date: February 28, 2025	**Entry:** #3

Description	Documenting the configuration and testing of an intrusion detection system (IDS) to monitor network traffic packets and generate alerts for suspicious activities. Focus is placed on the customization of Suricata rules, testing them against packet capture data, and analyzing the alert logs with the goal of exploring and improving IDS.
Tool(s) used	Suricata, an open-source intrusion detection system (IDS), intrusion prevention system (IPS), and network security monitoring tool. This tool inspects network traffic using a robust rule language to identify suspicious and potentially malicious activity. Additional tools include custom.rules file to define detection criteria, sample.pcap packet capture file to test traffic patterns against, and both the fast.log and eve.json output logs to verify rule efficacy and examine alert details.
The 5 W's	Capture the 5 W's of an incident. • **Who**: Me, as security analyst responsible for network traffic monitoring and alert configuration. • **What**: Configuration of custom Suricata rules to detect specific patterns in network traffic that could indicate security threats, followed by testing and log analysis. • **When**: Offline analysis conducted in a lab environment for the purposes of rule development and validation. • **Where**: My organization's network security monitoring environment. • **Why**: To enhance network security detection capabilities by creating valid detection rules that can successfully identify suspicious activity while reducing false positives through iterative testing and refinement loop.
Additional notes	1. How effective is Suricata's rule syntax when identifying specific HTTP

	methods like GET requests? 2. Is the fast.log legacy format used by security analysts anymore? If so, what are the benefits of using this format? 3. My current rule successfully detected HTTP GET requests (signature ID 12345), but how might we modify it to allow legitimate traffic to pass and focus on detecting only suspicious patterns? How do we balance out false negatives and false positives? **Technical Observations:** ● The rule components (action, header, rule options) provide flexibility for creating specific detection criteria. Additionally, IPS can be enabled through the action rule. ● JSON-formatted logs such as eve.json contain more information than fast.log entries, making them more suitable for in-depth and quicker analysis. ● Flow IDs are useful for correlating network flows between different devices. ● Testing rules against packet captures (PCAPs) is an efficient way to validate detection effectiveness before deployment.

Date: February 28, 2025	**Entry:** #4
Description	Review and analysis of a data breach final report as part of the Post-Incident Activity phase. As a new level-one SOC analyst, gaining an understanding of a major security incident that occurred prior to my joining the retail company,

	including its lifecycle: Goal 1: Identify exactly what happened. Goal 2: Identify when it happened. Goal 3: Identify the response actions that the company took. Goal 4: Identify future recommendations.
Tool(s) used	Incident Final Report documentation containing executive summary, timeline, investigation findings, response and remediation actions, and recommendations. This report follows standard incident response documentation practices.
The 5 W's	• **Who**: An unconfirmed threat actor. • **What**: Data breach of 50,000 customer records containing personal identifiable information (PII) and financial information. • **When**: December 28, 2022, at 7:20 PM PT • **Where**: E-commerce web application of a mid-sized retail company. • **Why**: To demand a large sum payment ($50,000) in exchange for not releasing the data to the public.
Additional notes	• The initial ransom demand ($25,000) was deleted because the employee assumed it was spam. How might security awareness training have changed the employee's response to this ransom? • The forced browsing attack represents a fundamental web application security flaw that could have been identified earlier. This incident shows just how critical proper access controls are when protecting PII and financial information. • The six-day gap between first contact (December 22) and the employee's report to the security team (December 28) increased the incident's impact significantly. How did this delay affect the organization's ability to contain the breach?

	• The report specifies that routine vulnerability scans and allowlisting were implemented after the incident. These are basic security controls that should have been in place before the security incident.

Reflections/Notes:

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

Using the Suricata tool was a challenging part of this journey as it was a tool I was completely unfamiliar with. I learned that getting my hands dirty by navigating and attempting to understand the different components through practice of any security tool is very valuable in gaining technical skills. For example, understanding the action, header, and rule through iterative testing helped me grasp what Suricata is truly capable of. Just like anything in life, when learning any tool, narrow-focused practice–and passion–leads you to become an expert.

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

Yes, it's brought me a whole different perspective on the policies and procedures implemented during the detection and response process. As an example, I didn't realize just how much emphasis is placed on reviewing a post-incident activity in order to prevent similar incidents from happening again. I enjoyed the post-incident phase including the detection and analysis phases as I have a passion for solving problems and finding elusive answers to critical problems.

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

VirtusTotal is a tool I enjoyed a lot. It's an incredibly powerful resource that aids in my ability to investigate a malicious file or security breach. I absolutely love the pooled resources and the effectiveness of a strong shared security community. It makes me feel like that I have support when needed and that I don't have to feel alone in my security investigations and analysis.