Incident handler's journal

Date: 02/11/23	**Entry:** #1
Description	Investigation on incident occurred to small US healthcare provider.
Tool(s) used	**N/A**
The 5 W's	• **Who** caused the incident? The incident was caused by an unethical hacker group. • **What** happened? The company's employees were blocked out from the internal system and unable to access medical records due to a ransomware. • **When** did the incident occur? It occurred on Tuesday at 9:00 am. • **Where** did the incident happen? Internal system. • **Why** did the incident happen? The incident happened due to compromised files attached to phishing emails sent to several employees. After gaining access to the company's system, the hacktivists launched their ransomware by encrypting the data. Their motive seems to be financial, because the group was asking for a large sum of money before releasing the data.
Additional notes	Potential ways of preventing this? Should they pay the ransom? The authorities should be made aware.

Date: 07/11/23	**Entry:** #2
Description	Investigation on malicious file downloaded by employee on their laptop.
Tool(s) used	VirusTotal, which is an online database where you can analyze files and URLs for malicious content such as viruses, worms, trojans, and more. It's a very helpful tool to use if you want to quickly check whether an indicator of compromise like a link or file has been reported as malicious by others in the cybersecurity community. I used VirusTotal to analyze a file hash, which was reported as malicious.
The 5 W's	● **Who** caused the incident? Unknown external threat actor, pretending to be applying for a job role within the company. ● **What** happened? The employee received a phishing email prompting them to download a password protected file. They successfully downloaded and opened the file with the password provided in the same email. Several unauthorized files were downloaded on the employee's laptop, which were flagged by our IDS. The malicious file had the following SHA-256 hash: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b. ● **When** did the incident occur? Today, at 9:30am, we received the first alert. ● **Where** did the incident happen? On the employee's computer. ● **Why** did the incident happen? Social engineering tactic employed by attackers. The employee is part of the HR team and might have thought that the email was a genuine job application from a potential candidate.
Additional notes	Has the email been received by others? The email contains attachments that have been opened by the target. Malicious

	content has already been installed into the target's computer. This requires escalation. Ways to prevent this same scenario from happening in the future could be improving security awareness training for employees.

Date: 07/11/23	**Entry:** #3
Description	Reviewing the port-incident report after a data breach
Tool(s) used	None. As a new member of the team my task was to review the Post-Incident Report.
The 5 W's	• **Who** caused the incident? Unknown external threat actor • **What** happened? An unknown external threat actor managed to steal PII from the company and asked for a ransom in exchange to not divulge the stolen information. • **When** did the incident occur? Approx. Dec. 22, 2022 • **Where** did the incident happen? The company database. • **Why** did the incident happen? The attacker exploited an unknown vulnerability in the e-commerce application which allowed them 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. This vulnerability allowed the attacker to access customer purchase

	confirmation pages, exposing customer data, which the attacker then collected and exfiltrated.
Additional notes	The company did not use IDS or were monitoring traffic in any other way, which made possible for the breach to happen undisturbed. In addition, no authentication process was in place, which meant that any user could access purchase confirmation pages.

Date: 08/11/23	**Entry:** #4
Description	Investigating a potential phishing incident with the use of Google Chronicle.
Tool(s) used	For this investigation I used: • Google Chronicle, which is a cloud SIEM tool from Google. This allows professionals to perform domain searches and obtain any threat intelligence data associated with that domain. This tool is useful because it allows us to retrieve any data regarding any events or assets that might have compromised a specific network. • VirusTotal, which is possible to access through the Chronicle interface. • WhoIs, which is an online tool that helps identifying the owner of a domain, also accessible through the Chronicle interface.
The 5 W's	• **Who** caused the incident? Potential threat actors behind the domain **signin.office365x24.com**. This is categorized as 'drop site for logs or stolen credentials'. It appears that three employees have accessed the site through their devices. • **What** happened?

	An alert was generated indicating that some employees received phishing email containing a suspicious link. Following that, it appears that six POST requests were made to the following URL **http://signin.office365x24.com/login.php**. • **When** did the incident occur? The incident occurred on 31st of January 2023 at 14:40. • **Where** did the incident happen? Several devices. • **Why** did the incident happen? Due to social engineering techniques (phishing emails).
Additional notes	After the analysis I have decided to escalate the issue as the source of the emails appear suspicious and employees have already submitted login details. I have suggested to block the IP addresses associated with the sender and reset passwords for all employees, as immediate steps.

Date: 26/11/2023	**Entry:** #5
Description	Configuring Suricata and using it to trigger alerts on the employee's network.
Tool(s) used	For this activity I used Suricata, which is an open-source intrusion detection system (IDS), intrusion prevention system (IPS), and network analysis tool. Suricata can monitor network traffic and alert on suspicious activities and intrusions. When configured as IPS, Suricata can block malicious activity and traffic. The great thing about this tool is that it allows security teams to set up custom rules to identify and alert on specific patterns or traffic behaviors.
The 5 W's	• **Who**: N/A • **What**: N/A

	• **When:** N/A • **Where:** N/A • **Why:** N/A
Additional notes	I ran Suricata through Bash. I opened a rule file and was able to understand the different components of it (action, header and rule options). After that, I moved onto analyzing an example of a packet capture file containing a sample of network traffic data. I was then able to use the sample to test Suricata rules. It was interesting to view an event log file generated by Suricata in JSON format and identify alerts.

Reflections/Notes:

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

The activities were not challenging per se. I was able to follow the logic of the instructions. However, I realized that giving myself the time to keep practicing with some of the tools (e.g. Suricata) and challenge myself with new scenarios is extremely important. This is mainly because it could take a while to remember how to use them and where to look for things. I believe that this also applies to certain concepts, such as network protocols, which means that I will need to dedicate some time to become more familiar with them.

2. **Has my understanding of incident detection and response changed after taking this course?**

I feel much more confident about my understanding of the different stages of the incident response cycle. The concept that I found the most useful was the triage process, which has widened my overall perspective on how to handle security events. Knowing about triaging made me understand the importance of resource allocation and the necessity to have a degree of certainty that an event is actually a security incident before reacting and responding.

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

I enjoyed practicing with SIEM tools, in particular Chronicle and Splunk. Although it was the first time that I was introduced to such pieces of software, I managed to find my way around them after a few attempts. Admittedly, it might take some time to get used to their interfaces, because there are lots of options and they display a lot of information simultaneously. However, the experience

clarified how monitoring systems with SIEMs fits into the usual day-to-day activities of a cybersecurity analyst.