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: 27/10/2023	**Entry:** #1
Description	This journal is being recorded as a result of a security breach at a small United States of America health care clinic specializing in delivering primary-care services. The assets of the company has been locked with a ransomeware.
Tool(s) used	No cybersecurity tool is used yet.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? • **What** happened? • **When** did the incident occur? • **Where** did the incident happen? • **Why** did the incident happen? The incident was caused by a group of unethical hackers who attacked the company's network by sending malicious emails to several employees of the health care company. When the employees downloaded the emails, critical files and softwares

	were locked. With a display of a ransome on the screen of the devices. The incident occurred at 9:00 am, Tuesday morning. The incident happened at the company's head office, in the United States. The incident happened because the threat actors sent malicious emails to the company's employees.
Additional notes	From the data breach, it is observed that pivotal defense in-depth structure is not in place. Adding to that, the employees are yet to be trained on the importance of cybersecurity and how to spot an attack – especially social engineering.

Date: 29/10/2023	**Entry:** #2
Description	Tan employee at a financial service company received an email with a malicious attachment. The employee went ahead to download and open the file, which immediately started to execute malicious code in the employees personal computer. That, immediately alerted the SOC with an indication of compromise (IoC) sent via the Intrusion Detection System (IDS).
Tool(s) used	Intrusion Detection System (IDS), Security Information and Event Management (SIEM) tool.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? The incident was caused by a malicious file attached in an email sent

	the company's employee. ● **What** happened? **At 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. ● **When** did the incident occur? The incident occurred at exactly 1:20 PM. ● **Where** did the incident happen? The incident happened in an employee's PC. ● **Why** did the incident happen? The employee downloaded and opened a malicious file attached in a mail sent to her by threat actor.
Additional notes	It is on record that the malicious that was executed in the employee's PC was a ransomeware.

Date: 29/10/2023	**Entry:** #3
Description	There was an alert ticket sent to the company's SOC. This was as a result of a malicious email containing an attachment – if opened, will download malicious code in the computer.
Tool(s) used	Playbooks, IDS, SIEM, and SOAR tools

The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? The event was caused by a malicious email with an attachment sent from a threat actor impersonating a job seeker. • **What** happened? The employee downloaded the attachment in her computer, which in turn downloaded malicious codes in the computer. • **When** did the incident occur? The incident happened at July 20, 2022; 1:20 PM. • **Where** did the incident happen? The incident happened at the office, during work hours. • **Why** did the incident happen? The incident occurred because the threat actor took advantage of an available job vacancy in the financial services company; by sending a malicious email containing an attachment to a HR officer.
Additional notes	From the header to the body of the email, there are some clear indications that the email could be malicious. These includes typographical errors, difference in the sender's name and his/her email address, and above all, the hash code of the malicious file has been recorded by over 50 security crowdsourcing platforms – like VirusTotal.

Date: 30/10/2023	**Entry:** #4
Description	A threat actor exploited a zero-day in the e-commerce website of a retail

	company.
Tool(s) used	Wireshark, tcpdump, Burpsuit, SOAR, and SIEM tools
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? The incident was caused a black hat hacker. ● **What** happened? The unethical hacker gained access to thousands of customer data via the e-commerce website of the retail company. This was as a result of a vulnerability in the website of the company. ● **When** did the incident occur? The incident was discovered on December 28, 2022, at 7:20 p.m., PT. ● **Where** did the incident happen? The incident took place in the website of the retail company. A zero-day was exploited. ● **Why** did the incident happen? The incident happened and vulnerability exploited by forced browsing, due to a zero-day in the web app of the company. As stated by the security team during their investigation: “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. This vulnerability allowed the attacker to access customer purchase confirmation pages, exposing customer data, which the attacker then

	collected and exfiltrated.”
Additional notes	The most pertinent question to be asked now is, “has the zero-day been fixed?”. If yes, that is awesome! Beyond that zero day, there could be other vulnerabilities in the company’s web app. Therefor, the best solution here is to run an extensive but offensive penetration testing activities on the website, it’s source code, and critical infrastructures. All PII in the app’s database should be encrypted. Adding to that, Access Control mechanisms must be implemented.

Reflections/Notes:

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

I really found the activity using Splunk Enterprise challenging. I registered for a new free account, but receive no confirmation email from the Splunk system/team. After multiple number of trying, I continued with the Google Chronicle project, instead.

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

Yes, pleas. In summary, I believe that my overall understanding has about incident detection and response has changed, and I am confidently equipped with more knowledge and understanding about what it takes to excel in incident response. After taking this course, my understanding of incident detection and response has definitely evolved. At the beginning of the course, I had some basic understanding of what detection and response entailed, but I didn't fully understand the complexity involved. As I progressed through the course, I learned about the lifecycle of an incident; the importance of plans, processes, and people; and tools used.

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

Truly, I enjoyed using Suricata – an IDS, IPS, and network security monitoring (NSM) tool. The way the tool is used ordinarily to achieve extraordinary results in breathtakingly inspiring! I LOVE IT.