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: November 25, 2024.	**Entry: 1**
Description	Review details of the security incident and document the findings. U.S Health Care clinics specializing in delivering primary-care services were victims of a malicious hacker.
Tool(s) used	N/A
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? An organized group of Unethical Hackers. • **What** happened? Encrypted important company files disrupting business operations, hackers asking for ransomware for decryption • **When** did the incident occur? Incident occurred on Tuesday at 9:00am. • **Where** did the incident happen? U.S Healthcare company • **Why** did the incident happen? The malicious hacker uses phishing on employees to infiltrate the systems by making them click on the emails with malicious file attachments and download them infecting the files, causing them to become encrypted and needing the encryption key to decrypt. With this, the hackers demanded money by installing ransomware.

Additional notes	Does the company give security training to employees?

Date: December 28, 2022	**Entry: 2**
Description	Retail company experiences a security incident where an individual gained unauthorized access to customer PII and financial information. The malicious individual is asking for $50,000 in cryptocurrency in exchange for the customers' information, making this ransomware.
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? Unauthorized Individual (attacker) • **What** happened? Attacker got ahold of customers' PII and financial information. Using ransomware for the company to pay for their data back. • **When** did the incident occur? December 28, 2022 at 7:20pm. PT • **Where** did the incident happen? Retail Company's E-commerce web application. • **Why** did the incident happen? Attacker found 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	Vulnerability scans should be done more frequently so incidents like this are less likely to occur.

Date: December 25, 2024	**Entry:3**
Description	Security Analyst at a financial services company, alert received that employee received a phishing email in their inbox.
Tool(s) used	Chronicle
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? Unauthorized Individual • **What** happened? Phishing emails were sent. • **When** did the incident occur? July 08, 2023 • **Where** did the incident happen? Financial Service Company • **Why** did the incident happen? Malicious attacker trying to get employee's information like credentials or where they live.
Additional notes	6 people accessed the domain that the phishing emails were sent, and we have concluded that the domain is malicious. From virus total, 12 security vendors marked the domain as malicious. Shows that successful POSTs were used to collect sensitive information about the employees. Ensure these people are secured: Ashton Davidson, Bruce Monroe, Coral Alvarez, Emil Palmer, Jude Reyes, Roger Spence, Amir David, and Warren Morris. the attackers used GET for these names. POST successfully acquired Warren Morris, Ashton Davidson, and Emil Palmer. Associated domains is a sibling, login.office365x24.com, and a parent domain office365x24.com

Date: December 25, 2024	**Entry:4**
Description	Security analyst working at e-commerce store Buttecup Games. Identify whether there are any possible security issues with the mail server.
Tool(s) used	Splunk
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? NA • **What** happened? Failed SSH logins from the root • **When** did the incident occur? December 25, 2024 • **Where** did the incident happen? Buttercup Games e-commerce store mail server. • **Why** did the incident happen? Unauthorized users trying to log into the root
Additional notes	Check up on the root account, make sure it isn't compromised.

Date: December 22, 2024	**Entry:5**
Description	Security Analyst that must monitor traffic on the employer's network. Configure Suricata and use it to trigger alerts.
Tool(s) used	Suricata

The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? Myself • **What** happened? Triggered a rule to see if alerts work • **When** did the incident occur? 12/23/2024 • **Where** did the incident happen? Employer's network • **Why** did the incident happen? Employer wanted to have network monitored, had to configure Suricata to trigger the right alerts to the corresponding rules.
Additional notes	Include any additional thoughts, questions, or findings.

Date: December 16, 2024	**Entry: 5**
Description	Level one SOC analyst at a financial services company. Received an alert about a suspicious file being downloaded on an employee's computer.
Tool(s) used	VirusTotal, Pyramid of Pain
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? Malicious Phishing email. • **What** happened? A phishing email was sent to an employee and they downloaded a malicious file. Multiple unauthorized executable files are created on the employees computer. • **When** did the incident occur? 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. • **Where** did the incident happen? Financial Services Company, employee's computer. • **Why** did the incident happen? Employee accessed a malicious file through an email they received.
Additional notes	SHA256 hash file was created of the malicious file sent to the employee in an email. 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b This hash was then used in VirusTotal and a finding showed that 59 out of 72 security vendors flagged this file as malicious, meaning there's an 81% chance it's malicious. Detection verdicts include: malicious, suspicious, unsafe, and negative descriptions. Also the community gave this file a score of -223. In the behavior section of virustotal, the sandboxes known as Yomi Hunter, DAS-Security Orcas, and CAPE sandbox all flagged this file as MALWARE.

Need another journal entry template?

If you want to add more journal entries, please copy one of the tables above and paste it into the template to use for future entries.

Reflections/Notes: Record additional notes.