Incident handler's journal

Date: 2/18/22	**Entry:** 1
Description	Brief: A scenario describing a Phishing attack that resulted in Ransomware. A hospital system was unable to access patient records and work related applications, and a ransom note was visible on employee devices requesting a large sum of money to grant the encryption key to the now encrypted hospital data. The root cause of the incident was a successful phishing email that contained a malicious attachment that was opened and downloaded onto an organization machine. The attack has been performed by an organized group of unethical hackers.
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	Capture the 5 W's of an incident. • **Who:** Group of unethical hackers • **What**: A successful phishing email downloaded malware onto a company machine that was able to encrypt company data to initiate a ransomware attack. • **When**: The event began with the phishing download, but the ransom event began this Tuesday 9:00 am. • **Where**: Employee machine for the initial phishing and later across all devices on the network. • **Why**: Clicking and downloading of a malicious link in a phishing email.
Additional notes	Company training needs to take place to prevent future events. All relevant authorities need to be notified.

	How is a ransom event like this resolved?

Date: 2/18/22	**Entry: 2**
Description	At a financial company an alert comes that a suspicious file has been downloaded onto an employee machine. After investigation a email file attachment is found and the hash for that file is already verified to be malicious.
Tool(s) used	SEIM tool, virus total website, Alert Ticket, Playbook
The 5 W's	Capture the 5 W's of an incident. • **Who**: email from malicious actor, • **What**: email was sent to the HR department with a suspicious link • **When**: event occurred this morning • **Where**: Event occurred on an HR machine • **Why**: email posing as an inquiring into an engineering role opening
Additional notes	Ticket has been escalated due to malicious file to SOC lvl 2 'name' as of 2/18/22 10:30am Project Notes: Pyramid of Pain Alert Ticket: Alert Ticket

---

Date: 2/18/22	**Entry:3**

Description	Brief: Recently hired at a company with a security incident and am reviewing the final report. Full Scenario: Recently brought on to a mid-sized retail company who handles 80% of their retail sales through their website via e-commerce. Before my hire a data breach resulted in 50,000 accounts being compromised. My team is working to prevent future incidents and as part of my training, I have been tasked with reviewing the final report.
Tool(s) used	Previous Attack Final Report
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? • **What** happened? • **When**: Attack occurred Dec 28, 2022 at 7:20pm PT • **Where** did the incident happen? • **Why** did the incident happen?
Additional notes	On Dec 22, 2022 an employee received a ransom style email claiming they had customer data and demanded an exchange of $25,000 in crypto to have the data back. This email was deleted and unreports because the employee assumed the email was spam. A follow up email from the attacker was sent to the same employee on Dec 28, 2022 with a demand now of $50,000 and a sample of the stolen data. Which was then escalated to the security team. Which prompted an investigation. The source of the attack was a vulnerability in the e-commerce web page allowing the attacker to perform a forced browsing attack to gain customer transaction data by modifying the order number in the order confirmation page. After investigating logs, the attacker was able to perform this attack and gain thousands of purchase confirmation pages.

	Collaboration was made with the PR team to relay this to the customers, and we offered free ID protection services to customers affected. After investigating the event, the source of attack was very clear due to an exceptionally large increase in volume of sequentially listed customer orders. Future preventative steps will include: routine vulnerability scans and pen testing Allowlisting to allow access to specified web urls Ensure only authenticated users are authorized access to content. The employee did a good job not clicking or engaging with the suspicious email because it may have been a phishing attempt. However, the event could have been resolved sooner had they escalated the event the first time it came to them in the future. It should be made clear to send anything suspicious to the security department, not just to ignore emails suspected to be phishing.

Date: 2/18/2022	**Entry: 4**
Description	Review Packets with Splunk
Tool(s) used	Splunk
The 5 W's	Query ‘index==main’ in the ‘all time’ time frame returns all packets within the sample data set. Query of ‘index==main host==mailsv’ returned all data from the mail server Query of ‘index == main host==mailsv fail* root’ returned all packets from the mail server that contained fail and the word root.

Additional notes	Txt file with addition information and findings: Splunk_Chronicle_intro.txt

---

Date: 2/18/2022	**Entry: 5**
Description	Review of Timeline data in Chronicle for domain: signin.office365x24.com
Tool(s) used	Chronicle
The 5 W's	Assets recorded in this log: 6 Ashton-davidson-pc Bruce-monroe-pc Coral-alvarez-pc Emil-palmer-pc Jude-reyes-pc Roger-spence-pc Post requests were made by: Ashton-davidson-pc Emil-palmer-pc An Resolved ip of 40.100.174.34 is also present Investigation of its timeline shows one additional POST events warren-morris-pc It also has a domain listed as:MICROSOFT-CORP-MSN-AS-BLOCK
Additional notes	Txt file with addition information and findings: Splunk_Chronicle_intro.txt

Date: Record the date of the journal entry.	**Entry:** Record the journal entry number.
Description	Provide a brief description about the journal entry.
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? • **What** happened? • **When** did the incident occur? • **Where** did the incident happen? • **Why** did the incident happen?
Additional notes	Include any additional thoughts, questions, or findings.

Date: Record the date of the journal entry.	**Entry:** Record the journal entry number.
Description	Provide a brief description about the journal entry.
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? • **What** happened? • **When** did the incident occur? • **Where** did the incident happen? • **Why** did the incident happen?
Additional notes	Include any additional thoughts, questions, or findings.

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.