Incident handler's journal

Date: 10/23/2023	**Entry:** 1
Description	This is a brief overview of a security incident that occurred at a small U.S. healthcare clinic, which caused severe disruptions to their business operations.
Tool(s) used	None.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? A group of unethical hackers who are known to target organizations in the healthcare and transportation industries. • **What** happened? A ransomware security incident took place. The unethical hackers employed phishing email tactics to access the company's network successfully. The phishing emails contained a malicious attachment that installed malware on an employee's computer once it was downloaded. Once the attackers gained access, they encrypted critical files. The employees were unable to access necessary patient data, which forced them to shut down their computer systems and caused significant disruptions to their business operations. • **When** did the incident occur? The incident happened on a Tuesday morning, approximately at 9:00 a.m. • **Where** did the incident happen? The incident occurred at the healthcare clinic. • **Why** did the incident happen? The incident occurred because the employees of the healthcare clinic were not aware of phishing social engineering attacks, and they fell victim to downloading a malicious attachment, which led to a ransomware attack.

Additional notes:	Quarterly cybersecurity training courses should be implemented to educate and help the company's employees be aware and prevent future phishing attacks from being successful.

Date: 10/27/2023	**Entry:** 2
Description	I determined that a file was malicious using information from a VirusTotal report.
Tool(s) used	VirusTotal.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? An advanced threat actor. • **What** happened? I received an alert about a suspicious file being downloaded on an employee's computer. An employee received an email containing an attachment. The attachment was a password-protected spreadsheet file. When the employee opened the file, a malicious payload was then executed on their computer. • **When** did the incident occur? The incident occurred during working hours. • **Where** did the incident happen? The incident happened at a financial services company. • **Why** did the incident happen? The incident occurred due to the employee not having the security awareness to avoid immediately downloading attachments from emails without verifying the validity of an attachment.

Additional notes	

Date: 10/27/2023	**Entry:** 3
Description	I used an incident response playbook to complete an investigation into a phishing attempt, and I resolved the alert.
Tool(s) used	Phishing incident response playbook.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? A malicious attacker. • **What** happened? I received a phishing alert about a suspicious file being downloaded on an employee's computer. After investigating the email attachment file's hash, the attachment has already been verified maliciously. • **When** did the incident occur? The incident occurred at 1:13 p.m. on July 20, 2022. • **Where** did the incident happen? The incident happened at a financial services company. Specifically, the attack was induced via a phishing email attempt that proved to be successful. • **Why** did the incident happen? The incident occurred because the employee of the financial services company quickly downloaded the attachment from an unknown sender without verifying the integrity of the attachment.
Additional notes:	A yearly cybersecurity awareness training should be conducted to inform employees of the many methods that malicious threat attackers may employ to

	gain access to sensitive information, systems, or devices.

Date: 10/29/2023	**Entry:** 4
Description	I reviewed a final report during the post-incident activity phase of the NIST Incident Response Lifecycle.
Tool(s) used	National Institute of Standards and Technology (NIST) Incident Response Lifecycle guidelines.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? A malicious threat actor outside of the organization. • **What** happened? The threat actor stole customer data by performing a forced browsing attack. They accessed 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. • **When** did the incident occur? The incident occurred at approximately 3:13 p.m. PT on December 22, 2022. • **Where** did the incident happen? The incident happened on the organization's e-commerce web application. • **Why** did the incident happen? The incident happened because there was a vulnerability in the e-commerce web application, which allowed the threat actor to modify the order number included in the URL string of purchase confirmation pages.

Additional notes:	To prevent future recurrences, the organization should implement the following actions: ● Perform routine vulnerability scans and penetration testing. ● Implement the following access control mechanisms: -Implement allowlisting to allow access to a specified seat of URLs and automatically block all requests outside of this URL range. -Ensure that only authenticated users access authorized content.

Date: 11/02/2023	**Entry:** 5
Description	I used Splunk Cloud to perform a search and investigation to identify whether there are any possible security issues within Buttercup Games' mail server.
Tool(s) used	Splunk Cloud.
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? A malicious threat actor. ● **What** happened? The threat actor attempted SSH logins for the root account within Buttercup Games mail server. ● **When** did the incident occur? March 06, 2023, at 1:39 a.m. ● **Where** did the incident happen? The incident occurred on the Buttercup Games mail server. ● **Why** did the incident happen? The threat actor wanted to gain access to sensitive data from Buttercup games mail server by attempting SSH logins for the root account.

Additional notes:	Security analysts for Buttercup Games should continue to monitor log files within their mail server to determine if any additional SSH logins will be attempted by threat actors in the future.

Date: 11/02/2023	**Entry:** 6
Description	I performed a query using Chronicle to investigate a security incident involving phishing.
Tool(s) used	Chronicle.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? An external malicious threat actor. • **What** happened? 16 assets accessed a malicious domain a total of 37 times. Several POST requests were made to the /login.php page. An additional POST request was made using the 40.100.174.34 IP address. This POST request indicates that an asset may have been phished. Eight more assets were affected by this POST request. There are two associated domains with this IP address (signin.accounts-gooqle.com, signin.office365x24.com) • **When** did the incident occur? The incident occurred on January 31, 2023, at 2:40 p.m. • **Where** did the incident happen? The incident happened at a financial services company within an employee's inbox. • **Why** did the incident happen? Multiple employees from the financial services company received and visited the malicious domain. Several employee assets were impacted by the phishing campaign, as logs

	show that login information was submitted to the suspicious domain via POST requests.
Additional notes	Employees from the financial services company should be cautious whenever they receive suspicious emails from addresses they do not recognize. Additionally, security analysts from the financial services company should add the malicious domains and IP addresses to their firewalls to block incoming traffic coming from those sources. Lastly, security analysts should be vigilant and monitor future attempts that may be made using similar phishing email tactics.