Incident handler's journal

Date: 3/27/25	**Entry:** 1
Description	This entry documents a ransomware incident that occurred at a small U.S. healthcare clinic after a phishing email led to system compromise.
Tool(s) used	Email filtering tools Endpoint detection and response (EDR) software SIEM (Security Information and Event Management) system Antivirus software
The 5 W's	• **Who caused the incident?** An organized group of unethical hackers was responsible for the incident. • **What happened?** A phishing email containing a malicious attachment was downloaded by a user. This triggered ransomware that encrypted the clinic's files. • **When did the incident occur?** The incident occurred on Tuesday at 9:00 a.m. • **Where did the incident happen?** The incident happened at a small healthcare clinic in the United States. • **Why did the incident happen?** The incident occurred because an employee unknowingly opened a malicious attachment in a phishing email, which allowed the attackers to deploy ransomware.
Additional notes	This incident highlights the critical importance of employee cybersecurity

	awareness training, particularly around email phishing. The organization should review and update its incident response plan and consider implementing stronger email filtering and endpoint protection tools. Backup procedures should also be evaluated to ensure data can be restored without paying a ransom.

Date: 3/27/25	**Entry:** 2
Description	This entry documents an investigation using Wireshark to analyze a packet capture (.pcap) file from a user accessing a website. Filters were applied to study IP addresses, protocols, DNS queries, and specific TCP packet details.
Tool(s) used	**Wireshark** (Network packet sniffer and analyzer)
The 5 W's	● **Who caused the incident?** This was not a malicious incident but an investigation of legitimate web traffic generated by a user visiting a website. ● **What happened?** The user visited opensource.google.com, generating network traffic that included DNS queries, TCP connections, and HTTP requests. ● **When did the incident occur?** The exact time is unspecified, but it was during a captured browsing session analyzed using the packet timestamps. ● **Where did the incident happen?** The traffic was captured on a network device used by the user accessing the website. The packet analysis was conducted locally in Wireshark. ● **Why did the incident happen?** This analysis was part of routine security training or monitoring to understand how to use Wireshark for traffic inspection and filtering. ●

Additional notes	This scenario reinforced practical skills in filtering, navigating packet layers, and understanding protocols like ICMP, TCP, and DNS.

Date: 3/27/25	**Entry:** 3
Description	This entry documents the investigation of a suspicious password-protected spreadsheet file downloaded by an employee. The file was found to contain a malicious payload. A SHA256 hash was generated from the file and checked against VirusTotal to identify associated indicators of compromise (IoCs).
Tool(s) used	SHA256 Hashing Tool VirusTotal
The 5 W's	• **Who caused the incident?** An unknown threat actor sent a phishing email containing a malicious attachment to an employee. • **What happened?** The employee downloaded and opened a password-protected spreadsheet from the email, which then executed a malicious payload. • **When did the incident occur?** The exact time is not specified, but the alert was received during the SOC's monitoring period and promptly investigated. • **Where did the incident happen?** The incident occurred on a company-issued computer used by an employee at a financial services firm. • **Why did the incident happen?**

	The employee was tricked by a phishing email and unknowingly opened a malicious file. The attacker used social engineering by including the password in the email to lower suspicion.
Additional notes	• The SHA256 hash provided a unique signature of the file, allowing for malware identification without needing to execute the file. • VirusTotal revealed additional IoCs such as associated IP addresses, URLs, and file behaviors linked to known malware strains. • The SOC team should review email security policies and implement sandboxing for suspicious attachments. • End-user awareness training should be reinforced to prevent future incidents. • The file should be blocked across the network and endpoint detection rules updated based on the hash and any associated IoCs.

Date: 3/27/25	**Entry:** 4
Description	This entry covers the resolution of a phishing alert involving a previously investigated malicious file hash. The response followed the organization's phishing playbook and flowchart to determine the appropriate actions and update the incident alert ticket.
Tool(s) used	• Internal Alert Ticketing System • VirusTotal (from previous activity)

	- Phishing Incident Response Playbook
The 5 W's	- **Who caused the incident?** A threat actor sent a phishing email with a malicious, password-protected spreadsheet attachment. - **What happened?** The employee opened the file, and a malicious payload was executed. The SOC confirmed the file's SHA256 hash was linked to known malware. - **When did the incident occur?** The phishing alert was triggered shortly after the file was downloaded and opened. This timeline was identified via the alert timestamp and verified hash. - **Where did the incident happen?** The incident occurred on a company-managed workstation within the financial services organization's internal network. - **Why did the incident happen?** The user fell victim to a socially engineered phishing email. The included password encouraged trust and led to the execution of the malware.
Additional notes	- The alert ticket was updated with the investigation findings. - **Ticket status was set to "Closed"** since the malicious file hash was verified, the endpoint was isolated, and the appropriate response actions were taken per the playbook. - The **ticket comments** noted that the phishing email led to the download of a malicious attachment which was confirmed via SHA256 hash comparison. - The decision to close the ticket was based on completing all playbook steps, confirming the threat, containing the device, and documenting

	the findings. • Future actions should include follow-up user awareness training and reviewing email filtering rules.

Date: 3/27/25	**Entry:** 5
Description	This entry reflects a post-incident activity review of a major data breach report at a mid-sized retail company. The goal was to identify what happened, when it occurred, how the company responded, and what recommendations were made to prevent future incidents.
Tool(s) used	• Internal Final Incident Report • NIST Incident Response Lifecycle Framework
The 5 W's	• **Who caused the incident?** A malicious attacker exploited a vulnerability in the company's e-commerce platform. • **What happened?** A **data theft** incident occurred, exposing over **one million users' data** due to a security vulnerability in the web application. • **When did the incident occur?** The report outlines the timeline, which includes the initial breach, detection, and subsequent response phases. The exact dates are

	detailed in the **Timeline** section of the report. • **Where did the incident happen?** The incident occurred in the company's **e-commerce web application**, which accounts for the majority of their sales. • **Why did the incident happen?** The attacker exploited a **forced browsing** vulnerability in the web app due to inadequate access control measures. ●
Additional notes	• The **root cause** of the incident is described in the **Investigation** section of the report. • The attacker bypassed access controls and accessed sensitive user data using forced browsing techniques. • In response, the company: • **Implemented access control mechanisms** • **Conducted routine vulnerability scans** • The company also provided **identity protection services** to affected users, showing strong post-incident recovery and customer support. • This case highlights the importance of secure web application development and routine security testing. • Reviewing this report helped reinforce the **Post-Incident Activity** phase in the NIST Incident Response Lifecycle.

Date: 3/27/25	**Entry:** 6

Description	This entry documents an optional hands-on activity using **Splunk Cloud**, where the goal was to search for suspicious activity involving failed SSH logins to the root account on Buttercup Games' mail server. The activity involved uploading log data, exploring Splunk's Search Processing Language (SPL), and applying filters to identify security-relevant events.
Tool(s) used	• **Splunk Cloud** • **Search Processing Language (SPL)** • Tutorial data (tutorialdata.zip) containing access, authentication, and mail logs
The 5 W's	● **Who caused the incident?** The potential threat actor(s) attempting unauthorized SSH logins, possibly using brute force methods, triggered the security alert. ● **What happened?** A series of failed SSH login attempts were made targeting the **root account** on the company's mail server. ● **When did the incident occur?** The specific timestamps of the login attempts were visible in the log entries during Splunk analysis. ● **Where did the incident happen?** On the **Buttercup Games mail server**, based on log data uploaded and queried through Splunk Cloud. ● **Why did the incident happen?** The failed SSH login attempts may indicate a **probing or brute-force attack** trying to gain unauthorized access to a critical system account.
Additional notes	Recommended next steps would include: • Reviewing firewall and IDS/IPS logs for matching activity • Blocking IPs showing repeated failed logins • Enforcing multi-factor authentication and disabling remote root logins

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.