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: 6/3/2025.	**Entry:** #1
Description	A small U.S. health care clinic experienced a security incident in which a hacker encrypted the organization's sensitive data by mass emailing employees with a phishing email containing a malicious attachment.
Tool(s) used	None
The 5 W's	Capture the 5 W's of an incident. • **Who:** A group of Unethical hackers. • **What:** Unethical hackers encrypted companies' sensitive data, resulting in disruptions in business operations and loss of medical records inaccessible to employees. • **When:** The incident happened on Tuesday morning at around 9:00 am. • **Where:** U.S. Healthcare clinic specializing in primary health care services. • **Why:** Unethical hackers sent phishing emails with a malicious attachment that were downloaded by employees in the company, which resulted in the loss of access to medical records. The hackers demanded a large sum of money in exchange for the decryption key.

Additional notes	• How to prevent future phishing attempts? • Should the ransom be paid in exchange for the decryption key?

Date: 6/5/2025	**Entry:** #2
Description	An employee received an email containing an attachment that, once downloaded, executed a malicious payload. I'm tasked with determining the extent of the malicious file.
Tool(s) used	• VirusTotal to analyze the file hash: **54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b**
The 5 W's	Capture the 5 W's of an incident. • **Who:** Advanced threat actor BlackTech, which has been previously reported using the malware Trojan FlagPro. • **What**: An employee received an email with an attachment: a password-protected spreadsheet file. The password was also included in the email. Once the file was opened, it executed a malicious payload, which alerted the security team. • **When**: The security event took place at 1:20 pm when an intrusion detection system (IDS) alerted the security team. • **Where**: The incident took place at a financial services company. • **Why**: The incident occurred due to an employee downloading a malicious file and accessing it with the password specified in the email.

	BlackTech performed this attack in an attempt to perform cyber espionage.
Additional notes	**Additional Timeline of Events** • 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.

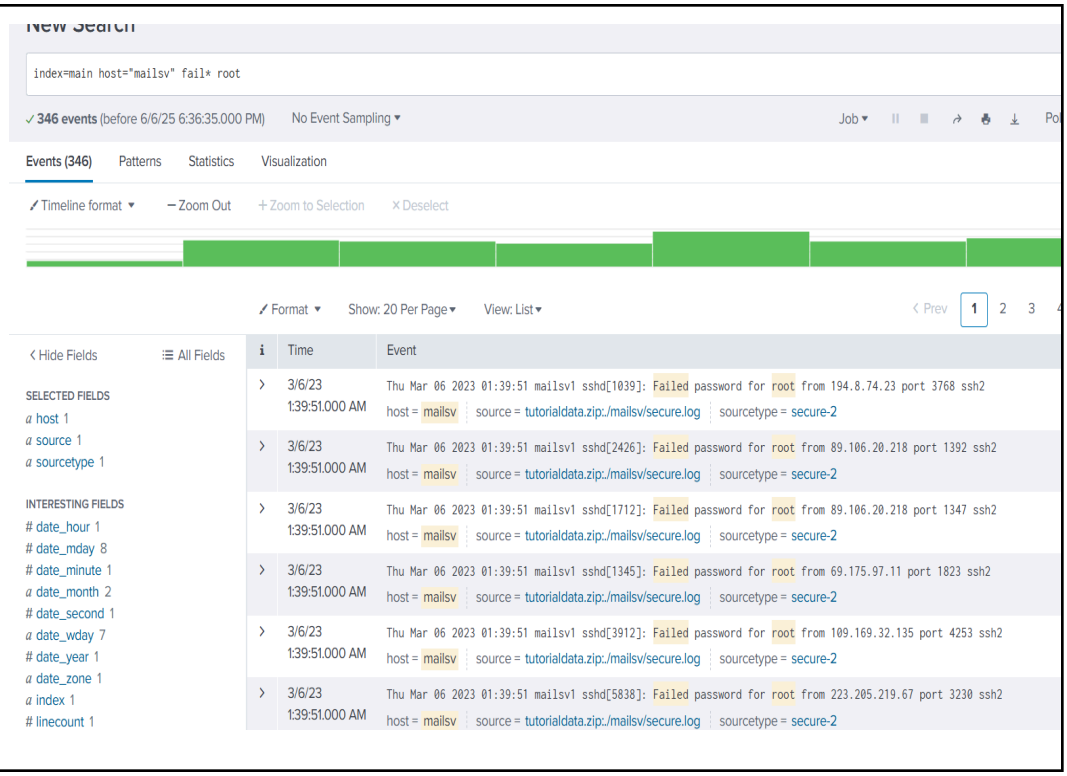
Date: 6/5/2025	**Entry:** #3 (Continuation of Entry #2)
Description	The file from Entry #2 was determined to be malicious. I must refer to the incident response playbook to resolve this issue immediately.
Tool(s) used	• Phishing Incident Response Playbook • VirusTotal to analyze file hash: **54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b**
The 5 W's	Capture the 5 W's of an incident. • **Who**: A member of the advanced threat actor Blacktech. He/she goes by the alias, Clyde West. • **What**: The attacker sent the malicious attachment named **bfsvc.exe** with the file password to an employee to execute a malicious payload.

	• **When**: The attacker sent the email on Wednesday, July 20th, 2022, at 9:30 am. However, the employee downloaded and accessed the file at 1:13 pm, which led to multiple executable files being created at 1:15 pm. These files were later detected by the intrusion detection system (IDS) at 1:20 pm. • **Where**: The incident took place at a financial services company. • **Why**: The incident occurred due to an employee downloading a malicious file and accessing it with the password specified in the email. BlackTech performed this attack in an attempt to perform cyber espionage.
Additional notes	• The Security Incident was escalated to a Tier 2 SOC analyst.

Date: 6/5/2025	**Entry:** #4
Description	A mid-sized retail company, which also conducts operations in e-commerce, experienced a security breach involving a data breach of over one million customers. In addition, 50,000 customers' personal identifiable information (PII) and financial records were accessed.
Tool(s) used	• Incident Final Report used for reference
The 5 W's	Capture the 5 W's of an incident. • **Who:** An unethical hacker. • **What**: An unethical hacker performed a forced browsing attack to access customer transaction data by modifying the order number

	included in the URL string of the purchase confirmation page, exposing customer data, which the hacker then exfiltrated. • **When**: The incident occurred on December 28, 2022, at 7:20 pm. • **Where:** The incident occurred at a mid-sized retail company. • **Why**: The security incident happened due to a vulnerability in the e-commerce web application. The hacker demands $50,000 in cryptocurrency to avoid releasing the information to the public.
Additional notes	• The organization collaborated with the public relations department to disclose the data breach to its customers. • The organization offered free identity protection services to customers affected by the incident. • The cause of the attack was a single log source showing an exceptionally high volume of sequentially listed customer orders. • The organization will improve its security posture by implementing routine vulnerability scans and penetration testing. • The organization will improve its security posture by implementing access control measures.

Date: 6/6/2025	**Entry:** #5
Description	As a security analyst at an e-commerce store, Buttercup Games, I am tasked with identifying whether a security issue has occurred with the mail server. I'm tasked with exploring failed Secure Shell (SSH) logins for the root account.
Tool(s) used	• Splunk • Splunk Data
The 5 W's	Capture the 5 W's of an incident. • **Who**: A possible threat actor attempting to log in to a user's account. • **What**: The logs seem to show an unusual number of login failures on March 6, 2023, at 1:39:51.000 on the mail server. • **When:** The failed secure shell (SSH) logins for the root account appear to have taken place on March 6, 2023, at 1:39:51.000 am. • **Where:** The incident took place at an e-commerce store, Buttercup Games. • **Why**: A threat actor is most likely trying to get access to users' accounts on the mail server. Additionally, the attacker may be using Botnets to conduct the brute force attack, as there are a variety of different IP addresses and port numbers conducting the attack simultaneously at 1:39:51.000 am.
Additional notes	**Selected Log Entry For Reference**


New Search
index=main host="mailsv" fail* root
✓ 346 events (before 6/6/25 6:36:35.000 PM)
No Event Sampling
Job
Events (346)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
Format
Show: 20 Per Page
View: List
Prev
1
2
3
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
date_hour 1
date_mday 8
date_minute 1
a date_month 2
date_second 1
a date_wday 7
date_year 1
a date_zone 1
a index 1
linecount 1
Time
Event
3/6/23 1:39:51.000 AM
Thu Mar 06 2023 01:39:51 mailsv1 sshd[1039]: Failed password for root from 194.8.74.23 port 3768 ssh2
host = mailsv source = tutorialdata.zip:./mailsv/secure.log sourcetype = secure-2
3/6/23 1:39:51.000 AM
Thu Mar 06 2023 01:39:51 mailsv1 sshd[2426]: Failed password for root from 89.106.20.218 port 1392 ssh2
host = mailsv source = tutorialdata.zip:./mailsv/secure.log sourcetype = secure-2
3/6/23 1:39:51.000 AM
Thu Mar 06 2023 01:39:51 mailsv1 sshd[1712]: Failed password for root from 89.106.20.218 port 1347 ssh2
host = mailsv source = tutorialdata.zip:./mailsv/secure.log sourcetype = secure-2
3/6/23 1:39:51.000 AM
Thu Mar 06 2023 01:39:51 mailsv1 sshd[1345]: Failed password for root from 69.175.97.11 port 1823 ssh2
host = mailsv source = tutorialdata.zip:./mailsv/secure.log sourcetype = secure-2
3/6/23 1:39:51.000 AM
Thu Mar 06 2023 01:39:51 mailsv1 sshd[3912]: Failed password for root from 109.169.32.135 port 4253 ssh2
host = mailsv source = tutorialdata.zip:./mailsv/secure.log sourcetype = secure-2
3/6/23 1:39:51.000 AM
Thu Mar 06 2023 01:39:51 mailsv1 sshd[5838]: Failed password for root from 223.205.219.67 port 3230 ssh2
host = mailsv source = tutorialdata.zip:./mailsv/secure.log sourcetype = secure-2

Reflections/Notes:

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

I didn't specifically find any of the activities too challenging. However, learning new cybersecurity tools and implementing them into the activities did take me some time to fully grasp.

Has your understanding of incident detection and response changed since taking this course?

My understanding of incident detection and response has changed after taking this course. I now understand that incident response is a complex process involving many procedures. The course taught me the importance of documenting every aspect of an incident, such as the 5 W's: who, what, when, where, and why. The course taught me that asking these questions and effectively documenting an incident can lead to successfully responding to an incident.

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

I enjoyed using almost all the tools throughout these activities. I enjoyed using VirusTotal to analyze the extent of malicious packets and referring to playbooks to respond to an incident while appropriately escalating the situation as needed. Additionally, I enjoyed learning to read logs and query using the SIEM tool, Splunk.