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: 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:	**Entry:**
12 February 2025	01

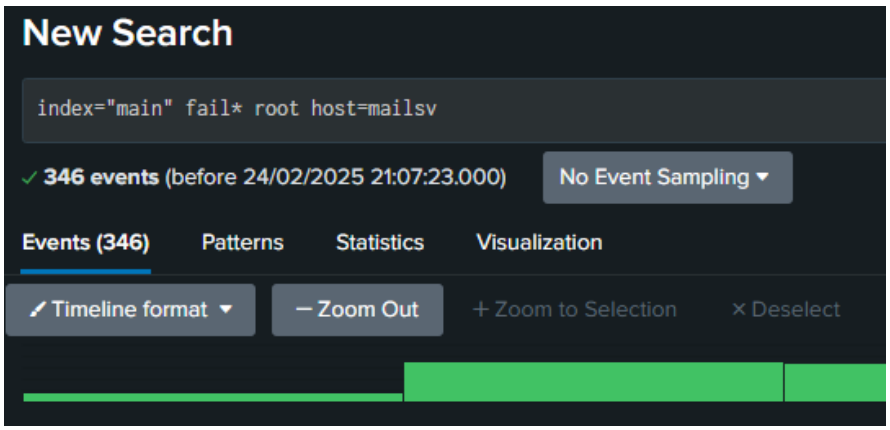
Description	A small U.S. health care clinic reported a ransomware attack at approximately 09:00AM leading to employees being unable .
Tool(s) used	None
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? **Organized group of unethical attackers** • **What** happened? **Attackers gained access to medical files of US healthcare clinic using phishing email then encrypted the files** • **When** did the incident occur? **Approximately 09:00 AM on Tuesday** • **Where** did the incident happen? **Small US healthcare clinic** • **Why** did the incident happen? **Attackers successfully used phishing email to install malware on employee's computer**
Additional notes	Include any additional thoughts, questions, or findings.

Date: 12 February 2025	**Entry:** 02
Description	By searching for the SHA256 hash value on VirusTotal, the security operations centre team was able to uncover indicators of compromise associated with a malware that was downloaded from an email on an employee's computer of a financial services company. The malware appears to be known as Flagpro which was known to be used by the BlackTech group. Email content: From: Def Communications <76tguyhh6tgftrt7tg.su> <114.114.114.114> Sent: Wednesday, July 20, 2022 09:30:14 AM

	To: <hr@inergy.com> <176.157.125.93> Subject: Re: Infrastructure Egnieer role Dear HR at Ingergy, I am writing for to express my interest in the engineer role posted from the website. There is attached my resume and cover letter. For privacy, the file is password protected. Use the password paradise10789 to open. Thank you, Clyde West Attachment: filename="bfsvc.exe"
Tool(s) used	VirusTotal
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? **BlackTech cyberattacker group** ● **What** happened? **Malicious file, known as Flagbro, was sent to an employee's computer through an email. The malicious file was in the form of a password-protected spreadsheet file.** ● **When** did the incident occur? ○ **The employee received the email at 1:11PM.** ○ **The employee opened the email, downloaded the file, then opened it at 1:13PM.** ○ **Multiple unauthorized files were opened on the employee's computer at 1:15PM** ○ **An intrusion detection system detected the executable files then alerted the SOC at 1:20PM** ● **Where** did the incident happen? **On an employee's computer at a financial services company** ● **Why** did the incident happen? **Employee downloaded malicious file attached to email**
Additional notes	● File hash of malware:

	54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b • Malware was reported by AlienVault OTX to be Flagpro which is known to have belonged to BlackTech group (https://otx.alienvault.com/pulse/61cdba240cd1f98f6a1e138f)

Date: Record the date of the journal entry.	**Entry:** 03
Description	ButterCup Studios, an organization I am working with, reported possible security issues with their mail server. I use Splunk to examine the logs to determine if there are failed SSH logins for their root account.
Tool(s) used	Splunk
Additional notes	Importing the secure.log file from their mailsv folder onto Splunk, I made a query index=”main” host=mailsv fail* root: • index=”main” will look into the main repository of the database • host=mailsv will look for the mail server as the data source • fail* root will look for anything related to the root that has a message starting with “fail” in it.



The search results show 346 events.

Upon inspection, the events are related to failed passwords for root.

Date: 12 February 2025	**Entry:** 04
Description	At a financial services company, I received an alert that an employee received a phishing email. Upon inspection, there appears to be a suspicious domain name called signin.office365x24.com. Using Google Chronicle, I investigated this domain.
Tool(s) used	Google Chronicle
Additional notes	After using Google Chronicle, here are my findings: ● Three systems that appear to be employee computers accessed the suspicious domain: ○ rogers-spence-pc ○ emil-palmer-pc ○ coral-alvarez-pc ● The suspicious domain resolves to an IP of 40.100.174.34 ● Three POST requests were made to that IP address ● In the same IP address, POST requests were also sent to a domain called https://signin.office365x24.com/login.php and signin.accounts-gooqle.com

---

Reflections/Notes:

Through the labs, I have learned to use various SIEM tools (Splunk, Chronicle) and to utilize publicly available resources (VirusTotal) to conduct my analysis on malware. I am more comfortable with looking through logs to spot anomalies.