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: 2/16/2026	**Entry:** 001
Description	There was a security incident at a small U.S. health care clinic which severely disrupted business operations.
Tool(s) used	None.
The 5 W's	At 9:00 AM Tuesday, an employee at the U.S. health care clinic received a phishing email that contained a malicious attachment. The attachment was then downloaded to the device as the user mistook the email for a legit sender/attachment, deploying ransomware into the system/device. The ransomware held a note from an organized group of unethical hackers that stated that the files were encrypted and demanded money for the decryption key. Because of this business operations were completely halted as needed assets were not available.
Additional notes	How much is the ransome for? Do we have backups that we can recover instead of paying? Has this group and type of ransomware been seen before? Do we have user training? We might want to up user training, implement SMTP rules on the firewall, or consider SaaS such as proofpoint to quarantine and have threat intelligence on emails. Healthcare is highly attacked via phishing

	and PHI needs to be protected/HIPAA compliance is a must.

Date: 2/17/2026	**Entry:** 002
Description	A ticket came in regarding a phishing email
Tool(s) used	Virus Total
The 5 W's	Def Communications/Clyde West (76tguyhh6tgftrt7tg.su) sent a phishing email to hr@inergy.com at 9:30:14 AM local time, July 20th 2022 about being interested in the posted engineering role. This email was opened and the user might have opened the attachment “bfsvc.exe” that was attached to the email. The Phishing Incident Response Playbook was used to evaluate the email, it was deemed as suspicious then the file hash was input into Virus Total which said it was malicious. Upon further investigation it was found that it was a Trojan. Because of these signs, the ticket was escalated to Tier 2 SOC analysts.
Additional notes	User training might be a good idea or SaaS such as Proofpoint which uses sandbox environments and records if an attachment was opened.

Date: 2/17/2026	**Entry:** 003
Description	Suricata needs configured and triggered an alert
Tool(s) used	Suricata
The 5 W's	On 2/17/2026 at 1:25 PM local time, I reviewed the custom.rules file in Suricata to see how it was laid out. It was set to alert when the HTTP protocol traffic on the home network on any port was sent to an external network on any port. The rules stated that the alert message was “GET on wire”, that the flow is established with the server, and look for the word GET within the http_method. The sid was 12345 and the signature’s revision version was3. Using the sample.pap files, I triggered the custom.rules file. I reviewed the fast.log to see alerts generated by the suricata rule then examined the eve.json output to see the severity property, extract only the timestamps, flow id, alert signature, protocol, and destination IP and see how the flow id worked. After everything I was able to see how the custom.rules worked, how to trigger an event, and how to read the logs made from Suricata.
Additional notes	How can this be applied to a security event? What protocols do attackers take advantage of the most? How custom can you make these signatures?

Date: 2/17/2026	**Entry:** 004
Description	A data theft and ransom have taken place. An Investigation was launched and the situation was remedied.

Tool(s) used	SIEM tools which held application access logs
The 5 W's	December 22nd 2022 at 3:13 Pm local time, an employee received an email from an external sender which stated that the external user has stolen customer data and wanted $25,000.00 $ of cryptocurrency to not leak the info. The employee deleted the email. on December 28th 2022 the same employee got another email from the same external sender which included a sample and a demand of 50,000.00$. The investigation has taken place from December 28th – 31st 2022. Root cause was concluded to be a vulnerability in the e-commerce website where the attacker was able to perform a forced browsing attack to access customer transaction data. Logs were analyzed and indicated tat the attack access the info of thousands of purchase confirmation pages. This was proved via a high volume of sequentially listed customer orders. Public relation disclosed the data breach to customers and offered free identity protection. The team concluded that allowlisting to specific URLs and block outside requests will be implemented and that only authenticated users are authorized to access content.
Additional notes	I think we should also out IPS or IDS systems in place for alerts, if we had them in place it could have been addressed sooner.

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: Pack sniffing and logs are critical to understand the flow of your network and understanding normal protocol and behavior is critical when trying to make and use signatures in Suricata.