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: October, 2025	**Entry:** #1
Description	Overview and description of packet captures.
Tool(s) used	Wireshark, command line utility TCP, SolarWinds, etc..
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident: Possible hackers within or outside a company network • **What** happens: DDos attack, malware infection, unauthorized access • **When** did the incident occur: Establish a timeline, filter dates accordingly • **Where** did the incident happen: Within a company or outside a company? • **Why** did the incident happen: Political gain, monetary gain, leaking information
Additional notes	This is a focused overview of possible scenarios and how packet captures can help.

Date: October, 2025	**Entry:** #2
Description	AWS services outage
Tool(s) used	CloudWatch, CloudTrail, AWS Health Dashboard
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident: AWS, Amazon • **What** happened: Major cloud service outage affecting multiple companies • **When** did the incident occur: October 20th, 2025 • **Where** did the incident happen: Widespread • **Why** did the incident happen: Internal DNS Failures
Additional notes	Insight into a company quality issue that can lead to possible vulnerabilities

Date: October, 2025	**Entry:** #3
Description	Overview of what the post incident review is and the cycle
Tool(s) used	Multiple
Steps	• Preparation: The setup before the incident • Detection and Analysis: Discovering and analyzing suspicious activity • Containment Eradication and Recovery: Isolate specific systems, mitigate spread of damage, eradicate issue if possible • Post-incident Activity: Learn from the incident, things done well and things done not so well
Additional notes	N/A

Date: October, 2025	**Entry:** #4
Description	Overview of Suricata
Tool(s) used	Suricata
Overview	Threat detection systems can regulate incoming traffic and block suspicious activity. It can analyze packets on a deep level and find hidden threats within those packets.
Additional notes	Free, open source, no cost

Date: October, 2025	**Entry:** #5
Description	Splunk Overview
Tool(s) used	Splunk
Overview	Widely used data processing tool. It is able to access many different types of cloud services, able to perform high efficiency automation and alerting
Additional notes	N/A