Paarth Pandey

Incident handler's journal

Date: July 10, 2025	**Entry:** #1
Description	Documenting a cybersecurity incident
Tool(s) used	None.
The 5 W's	• Who: An organized group of unethical hackers • What: A ransomware security incident • Where: At a health care company • When: Tuesday 9:00 a.m. • Why: The incident happened because unethical hackers were able to access the company's systems using a phishing attack. After gaining access, the attackers launched their ransomware on the company's systems, encrypting critical files. The attackers' motivation appears to be financial because the ransom note they left demanded a large sum of money in exchange for the decryption key.
Additional notes	1. How could the health care company prevent an incident like this from occurring again? 2. Should the company pay the ransom to retrieve the decryption key?

Date: July 13, 2025	**Entry:** #2
Description	Network Packet Analysis with Wireshark
Tool(s) used	Wireshark
The 5 W's	• Who: A security analyst investigating packet traffic • What: Used Wireshark filters to analyze protocols, ports, DNS, HTTP, and TCP traffic • Where: A local system with a sample packet capture file • When: During network inspection lab • Why: To learn how to use filters in Wireshark to isolate traffic based on IPs, protocols, ports, and payloads to identify communication patterns or anomalies
Additional notes	1. What security threats could be detected early using packet sniffing tools like Wireshark? 2. How can packet analysis help detect suspicious behavior in real-time?

Date: July 16, 2025	**Entry:** #3
Description	Capturing and analyzing live network traffic using tcpdump in a Linux environment
Tool(s) used	tcpdump, ifconfig
The 5 W's	• Who: A network analyst analyzing Linux VM traffic • What: Used tcpdump to identify interfaces, capture live traffic, apply filters, and inspect traffic stored in pcap files • Where: On a Linux virtual machine • When: During network packet capture and filtering la • Why: To gain practical skills using tcpdump to monitor traffic on specific ports (e.g., port 80), identify traffic direction, examine TCP headers, and capture data for later analysis |
Additional notes	1. How can tcpdump be used to investigate suspicious outgoing connections? 2. Why is it important to disable IP/port lookups during investigations? 3. How does ASCII/hex output help in malware or forensic analysis?

Date: July 17, 2025	**Entry:** #4
Description	Used VirusTotal to analyze a file hash associated with a suspicious email attachment. Investigated indicators of compromise (IoCs) and mapped them to the Pyramid of Pain to assess how difficult it would be for a threat actor to modify these IoCs if defenses were deployed.
Tool(s) used	VirusTotal, Pyramid of Pain framework
The 5 W's	• Who: A SOC analyst analyzing a suspicious file hash received via email • What: Investigated the SHA256 hash using VirusTotal and identified related IoCs such as IP addresses, domains, and malware behaviors • Where: Within a sandboxed environment (VirusTotal's Behavior tab) • When: Shortly after the malicious file was detected on an employee's machine • Why: To determine whether the file was malicious and understand its behavior and threat context through shared threat intelligence
Additional notes	1. File determined malicious with high vendor flag ratio and negative community score 2. Key IoCs identified: a. Hash value: SHA-1 and MD5 variants of the malware b. IP address: 185.225.73.244 (flagged as malicious by multiple vendors) c. Domain: update-checker[.]com (suspicious and previously associated with malware campaigns) d. Network/host artifact: Registry modifications and dropped executable files e. Tool: Uses PowerShell for lateral movement f. TTPs: MITRE ATT&CK tactics such as Execution (T1059), Persistence (T1547), and Command and Control (T1071)

Date: July 20, 2025	**Entry:** #5
Description	Followed the phishing alert playbook to investigate a previously identified malicious email attachment. Evaluated alert details and determined next steps based on severity, message content, and analysis results.
Tool(s) used	Phishing Playbook, VirusTotal, Alert Ticket system
The 5 W's	• Who: An employee who received and opened a phishing email attachment • What: Opened a password-protected spreadsheet from a suspicious sender; this triggered execution of malicious code • Where: Employee's workstation within the financial company's internal network • When: Initial infection at 1:13 p.m., alert generated by IDS at 1:20 p.m. • Why: The employee was tricked by social engineering tactics and entered the provided password, which launched the malicious payload
Additional notes	1. Reasons to escalate the alert: a. The file hash is confirmed malicious by VirusTotal b. The email content includes social engineering techniques and suspicious sender details c. The malicious attachment created unauthorized executables, triggering an IDS alert 2. Ticket status: Escalated 3. Ticket comments: "File hash confirmed as malicious by VirusTotal with 40+ vendor detections. Behavior includes creating unauthorized executables and connecting to suspicious domains. Alert severity medium — escalation required for remediation and further forensic analysis."

Date: July 21, 2025	**Entry:** #6
Description	Reviewed a final incident report involving a significant data breach prior to joining the company. The goal was to understand the incident lifecycle and recommend preventive measures. Focused on identifying what occurred, when, how the company responded, and how to prevent future incidents.
Tool(s) used	Internal Final Report Repository, Security Process Documentation
The 5 W's	• Who: Attackers accessed over one million user records from a mid-sized retail company. • What: Major data breach compromising sensitive user data from e-commerce operations. • Where: Incident affected the e-commerce infrastructure (80% of company revenue). • When: Incident occurred shortly before analyst's onboarding in July 2025. • Why: Attackers exploited vulnerabilities in existing security controls; inadequate monitoring and delayed detection contributed to the breach.
Additional notes	1. Response actions taken: a. The incident response team contained the breach and patched the exploited vulnerability. b. Notified affected customers and regulators as per compliance standards. c. Initiated forensic investigation. 2. Future recommendations: a. Implement centralized logging and SIEM. b. Conduct regular vulnerability assessments. c. Improve user access control and monitoring. d. Enhance incident response readiness with table-top exercises.

Date: July 23, 2025	**Entry:** #7
Description	Completed hands-on lab using Suricata IDS to analyze packet capture data. Wrote and tested a custom rule against sample traffic and examined generated logs (fast.log and eve.json).
Tool(s) used	Suricata IDS, Bash Terminal, jq
The 5 W's	• Who: SOC analyst monitoring employer network traffic. • What: Configured and tested a Suricata rule that triggered alerts on specific HTTP traffic. • Where: Test environment simulating internal-to-external network traffic. • When: Lab executed on July 17, 2025. • Why: To detect “GET” HTTP methods from internal hosts to external networks using a custom signature.
Additional notes	1. Rule used: a. alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"GET on wire"; flow:established,to_server; content:"GET"; http_method; sid:12345; rev:3;) 2. fast.log entries observed: a. Two alerts triggered on traffic from 172.21.224.2 to 142.250.1.139 and 142.250.1.102. 3. eve.json analysis: a. Alert signature: “GET on wire” b. Severity: 3 c. Destination IP for last alert: 142.250.1.102 4. Command highlights: a. sudo suricata -r sample.pcap -S custom.rules -k none b. jq -c "[.timestamp,.flow_id,.alert.signature,.proto,.dest_ip]" /var/log/suricata/eve.json

Date: July 24, 2025	**Entry:** #8
Description	Used Splunk Cloud to ingest and analyze log data from an e-commerce mail server. Focused on identifying failed SSH login attempts for the root user as part of a SIEM platform lab.
Tool(s) used	Splunk Cloud, SPL (Search Processing Language)
The 5 W's	• Who: Security analyst reviewing logs for Buttercup Games' mail server (mailsv). • What: Queried logs for failed SSH login attempts targeting the root account. • Where: Data from /mailsv/secure.log, ingested into Splunk Cloud. • When: Data analyzed on July 20, 2025. • Why: To identify unauthorized access attempts to the mail server's root account
Additional notes	1. Steps followed: a. Activated Splunk Cloud trial and uploaded tutorialdata.zip. b. Searched using index="main" and narrowed to host=mailsv. c. Queried index=main host=mailsv fail* root to find failed root logins. 2. Field breakdown: a. host: mailsv (mail server) b. source: /mailsv/secure.log c. sourcetype: secure-2 3. Observations: a. Multiple failed SSH login attempts to root detected. b. Wildcard searches with fail* helped identify variations like "failed", "failure", etc. c. SPL and field filtering enabled efficient log triage.