Incident handler's journal

Date: August 28, 2025	**Entry:** #1
Description	This entry documents the response to a potential phishing and malware incident, following a security playbook. The investigation begins in the **Detection & Analysis** phase by verifying the alert and moves into the **Containment, Eradication, & Recovery** phase as steps are taken to isolate the host and remove the threat, as dictated by the playbook.
Tool(s) used	• Incident Response Playbook • Email Security Gateway / Filter • Endpoint Detection and Response (EDR) / Antivirus Software • SIEM Tool for log correlation
The 5 W's	• **Who** caused the incident? An external threat actor using a sophisticated phishing email that impersonated a known and trusted company vendor. • **What** happened? An employee reported a suspicious email. Analysis confirmed the email contained a malicious link which, when clicked, downloaded a malware dropper onto the employee's workstation. The official playbook for "Phishing with Malware Payload" was immediately activated to guide the response. • **When** did the incident occur? The email was received at approximately 9:15 AM IST. The employee clicked the link and reported the suspicious behavior at 9:30 AM IST on August 28, 2025.

	- **Where** did the incident happen? The incident occurred on a user workstation (workstation-075) within the corporate network. The initial point of entry was the employee's corporate email inbox. - **Why** did the incident happen? The incident occurred because the employee was successfully deceived by a social engineering attack (phishing). The underlying vulnerability was a combination of a momentary lapse in user awareness and a sophisticated phishing lure that bypassed initial email filtering.
Additional notes	The playbook was highly effective in providing a structured, step-by-step response, which prevented confusion and ensured no critical steps were missed. This incident underscores the importance of continuous employee security awareness training to strengthen our human firewall.

Date: August 30, 2025	**Entry:** #2
Description	This entry details the process of using **Suricata**, an open-source Intrusion Detection System (IDS), to analyze network traffic. The focus was on understanding its rule-based signatures, configuration files, and the different types of log outputs it generates for security monitoring.
Tool(s) used	**Suricata (IDS/NSM):** The primary tool used for network traffic analysis and alert generation. **Linux Command-Line Interface (CLI):** Used to navigate directories (/etc/suricata/rules/), view configuration files (suricata.yaml), and read log files.

The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? N/A - This was a proactive analysis and skill-building activity, not an incident response. • **What** happened? I examined Suricata's rule files to understand its signature syntax, including the **Action**, **Header**, and **Rule Options**. I then analyzed a Suricata log file (eve.json) to see how these rules translate into actionable alerts and network telemetry logs. • **When** did the incident occur? This analysis was conducted on August 30, 2025. • **Where** did the incident happen? The activity was performed within a Linux (Ubuntu) virtual machine environment where Suricata was installed and configured. • **Why** did the incident happen? The purpose was to develop practical skills in using a Network Intrusion Detection System (NIDS) for network security monitoring and to understand how to interpret its output for threat detection and investigation.
Additional notes	Suricata's eve.json log format is incredibly powerful for investigations. Its structured JSON output and the use of a flow_id to correlate all related events from a single network conversation are major advantages. Understanding its rule syntax is fundamental for customizing the IDS to a specific environment and reducing false positives.