Incident handler's journal

Date: December 27, 2025	**Entry:** Entry 1
Description	This journal entry documents the analysis of a network alert triggered by suspicious HTTP traffic detected during monitoring activities in the Detection and Response course.
Tool(s) used	• SIEM • Suricata • Chronicle
The 5 W's	**Who caused the incident?** An external IP address attempting to communicate with a web server. **What happened?** An HTTP GET request triggered a signature-based alert indicating potential suspicious network activity. **When did the incident occur?** The incident occurred at the date and time recorded in the network log during the monitoring exercise. **Where did the incident happen?** The incident occurred on the network, targeting a web server over port 80 (HTTP). **Why did the incident happen?** The incident occurred because the network traffic matched a predefined signature designated to detect potentially malicious or unauthorized requests.
Additional notes	The activity helped reinforce how alerts are generated from signatures and how network telemetry differs from alert data. It also demonstrated the importance of documenting incidents clearly using the 5 W's framework.