Alert Triage Simulation

The mock alert is initially documented as an **Open** high-priority event, requiring immediate investigation due to the potential for malware infection or unauthorized data retrieval.
The triage process involves:

1. **Initial Assessment:** Reviewing the raw log in Wazuh to extract all observables, such as the file hash (MD5, SHA-256), filename, and user associated with the download.
2. **Threat Enrichment (Automated):** The extracted file hash is automatically sent to VirusTotal via a configured integration (often using Cortex/TheHive Analyzers or a SOAR solution like Shuffle/n8n) to validate the file's reputation against multiple security vendors.
3. **Action/Containment:** Based on the VirusTotal results, the analyst determines the next steps. For a positive match (malicious), containment actions (e.g., isolating the host, deleting the file via Wazuh Active Response) are initiated, and the alert status is updated to In Progress or Closed (True Positive).

Automated Validation Summary

TheHive's automation successfully extracted the file hash from the Wazuh alert and queried VirusTotal. The scan results showed that 45/70 security vendors flagged the hash as malicious, confirming it as a True Positive for malware. TheHive automatically logged the VirusTotal report, elevated the case severity, and initiated a host containment task for 192.168.1.108. The automated enrichment significantly accelerated the initial triage process.