Alert Triage Simulation

Alert Identification : Access the alert in Wazuh and verify core details: alert ID, source IP, rule level, file name, hash, user account, and timestamp. Confirm why the alert is marked High priority. Determine whether the activity deviates from normal user behavior or matches known threat patterns.

Indicator Validation and Risk Assessment : Extract the file hash and validate it using VirusTotal (manually or automated via TheHive). Analyze detection ratio, reputation score, first-seen date, and related indicators. Assess whether the file is confirmed malicious, suspicious, or unknown. Evaluate potential business impact if the threat is real.

Decision and Case Handling : Based on validation results, update the alert status (Open, Escalated, Closed). If malicious indicators are confirmed, create or escalate a case in TheHive and document findings. If inconclusive, recommend monitoring or deeper investigation. Ensure actions align with predefined SOC response thresholds.

Result

TheHive was integrated with Cortex to automatically analyze file hash observables using the VirusTotal analyzer. Upon adding a SHA256 hash to the case, the system triggered an automatic reputation check. The analysis returned multiple engine detections, confirming malicious classification. Results were attached to the case, enabling faster triage and informed escalation decisions.