Alert Triage with Automation – Suspicious File Download

An alert titled “Suspicious File Download” was generated in the SIEM environment and required triage and validation using automated threat intelligence integration. The objective was to assess severity, validate indicators, and streamline response using automation.

Triage Simulation

Alert ID	Description	Source IP	Priority	Status
005	File Download	192.168.1.102	High	Open

Initial analysis indicated that host 192.168.1.102 downloaded an executable file from an external source. Due to the potential risk of malware delivery, the alert was classified as High priority pending validation.

Automated Threat Intelligence Validation

Automation was configured within TheHive to automatically submit the downloaded file hash to VirusTotal for reputation analysis. The playbook workflow included:

1. Extract file hash from alert
2. Query VirusTotal API
3. Append reputation result to case
4. Escalate if malicious score exceeds threshold

Validation Summary (50 Words)

Automated validation identified the downloaded file hash as malicious, with multiple detections reported in VirusTotal. TheHive automatically updated the case with reputation details and flagged the alert for escalation. Automation reduced analysis time, improved consistency, and enabled rapid containment of potentially harmful file activity.