ALERT TRIAGE WITH AUTOMATION

Notes

Activities:

- Simulated alert triage using ELK as a substitute for Wazuh.
- Manual validation of file hashes using VirusTotal.
- Case creation in TheHive to document alerts and artifacts.

Tools Used:

- ELK Stack (Elasticsearch & Kibana) – to host and view alerts.
- VirusTotal – to check file hashes and gather threat intelligence.
- TheHive – to create cases and store alert artifacts.

Tasks Completed:

- Created a mock alert in ELK for “Suspicious File Download.”
- Extracted the SHA256 hash of the downloaded file from ELK.
- Manually queried VirusTotal with the file hash to get detection results.
- Manually created a case in TheHive, including alert details and file hash as an artifact.
- Documented alert and VirusTotal results, summarizing the findings.

Alert	Description	Source IP	Priority	Status	File Hash	VirusTotal Detection
005	Suspicious File Download	192.168.1.102	High	Open	e3b0c44298fc1c149afbf4c8996fb924	0/70

Outcome:

- Successfully simulated automated triage without full integration.
- Verified file hashes against threat intelligence.
- Documented all relevant information in TheHive for future reference.

Observations:

- Automation with TheHive and Cortex could not be fully tested due to Elasticsearch connectivity issues.
- This manual process demonstrates the steps for alert triage, validation, and documentation in a SOC environment.