Alert Triage with Automation

1. Objective

This report contains the details of the task including Triage Simulation, and Automated Validation. The goal of this task is to:

- Develop skills to simulate adversary behaviors to enhance SOC preparedness and validate controls.

2. Introduction

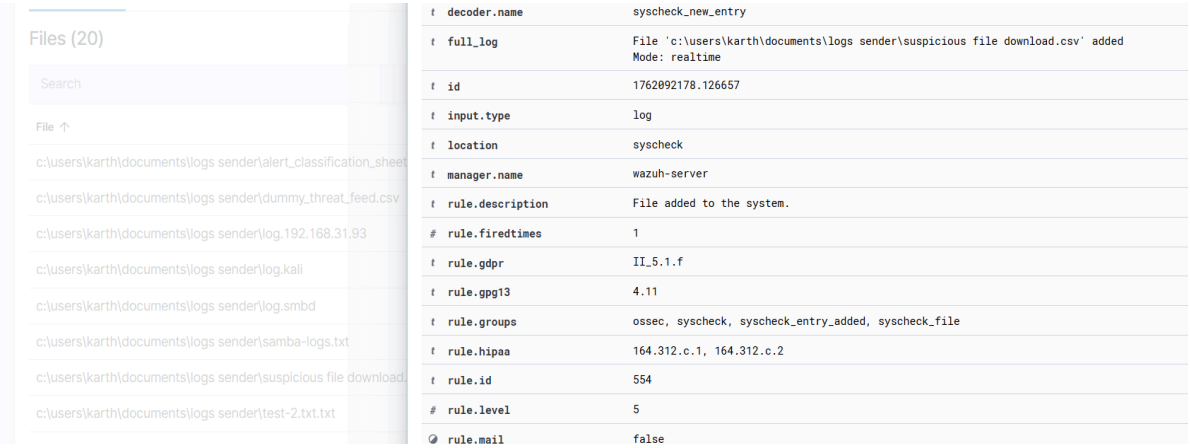
Effective alert triage is essential for maintaining a strong security posture in any organization. This task focuses on evaluating and validating security alerts using automation to streamline incident response. By leveraging tools such as Wazuh for alert monitoring, VirusTotal for threat intelligence, and TheHive for case management, analysts can quickly determine the severity of potential threats. Through a simulated alert investigation and automated hash verification, this exercise demonstrates how integrated security platforms enhance accuracy, reduce manual workload, and accelerate decision-making during incident handling.

3. Tools

- Wazuh setup using official Wazuh documentation . https://documentation.wazuh.com/current/quickstart.html
- TheHive https://docs.strangebee.com/thehive/installation/installation-methods/
- VirusTotal https://www.virustotal.com/gui/home/upload

4. Triage Simulation

Analyzing a mock alert (e.g., “Suspicious File Download”) in Wazuh and documenting its metadata that includes Alert ID, Description, Source IP, Priority, and Status. Triage simulation is a process of reviewing and prioritizing security alerts like examining alerts, determining how severe they are, deciding which one requires immediate response, and filtering out false positives.



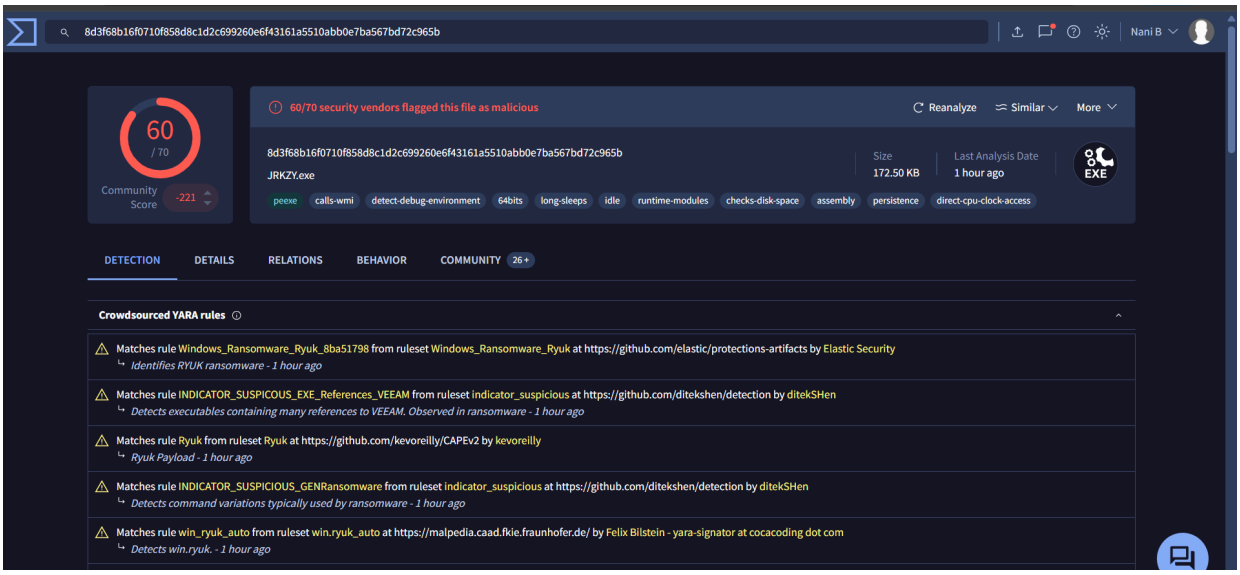
4.1 Triage Simulation Metadata

The below table contains the metadata of the analysis of a mock alert.

Alert ID	Description	Source IP	Priority	Status
005	File Download	192.168.31.58	High	Open

5. Automated Validation

Automated validation means it is a process of using validation tools automatically verify whether a security alert represents a valid threat or not. It does not require any human intervention. In this Task configuring TheHive tool to automatically check file hashes with VirusTotal.



5.1 Summary of Automated Validation

Automated validation in TheHive integrates VirusTotal to quickly verify file hashes from Wazuh alerts. The system enriches alerts with threat intelligence, showing detection scores and reputation details. This automation reduces manual workload, speeds up decision-making, and helps analysts confirm whether a file is malicious, suspicious, or safe before escalation.