

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.

Files (20)

Search

File ↑

- c:\users\karth\documents\logs sender\alert_classification_sheet
- c:\users\karth\documents\logs sender\dummy_threat_feed.csv
- c:\users\karth\documents\logs sender\log.192.168.31.93
- c:\users\karth\documents\logs sender\log.kali
- c:\users\karth\documents\logs sender\log.smbd
- c:\users\karth\documents\logs sender\samba-logs.txt
- c:\users\karth\documents\logs sender\suspicious file download
- c:\users\karth\documents\logs sender\test-2.txt.txt

t_decoder.name	syscheck_new_entry
t_full_log	File 'c:\users\karth\documents\logs sender\suspicious file download.csv' added Mode: realtime
t_id	1762892178.126657
t_input.type	log
t_location	syscheck
t_manager.name	wazuh-server
t_rule.description	File added to the system.
# rule.firetimes	1
t_rule.gdpr	II_5.1.f
t_rule.gpg13	4.11
t_rule.groups	ossec, syscheck, syscheck_entry_added, syscheck_file
t_rule.hipaa	164.312.c.1, 164.312.c.2
t_rule.id	554
# rule.level	5
@rule.mail	false

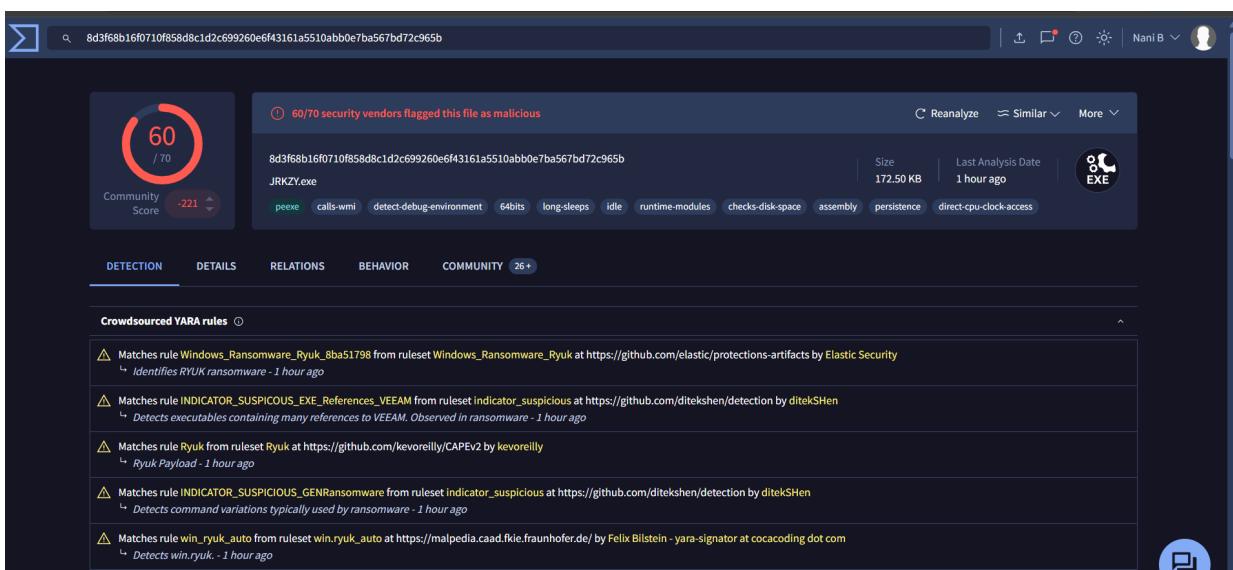
4.1 Triage Simulation Metadata

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.



The screenshot shows a file analysis result for a file with hash 8d3f68b16f0710f858d8c1d2c699260e6f43161a5510abb0e7ba567bd72c965b. The file is identified as JRKZY.exe. The analysis results indicate that 60/70 security vendors flagged the file as malicious. The file size is 172.50 KB and the last analysis date is 1 hour ago. The file is categorized as EXE. The analysis details section shows the following Crowdsource YARA rules:

- Matches rule Windows_Ransomware_Ryuk_8ba51798 from ruleset Windows_Ransomware_Ryuk at https://github.com/elastic/protections-artifacts by Elastic Security. Description: Identifies RYUK ransomware - 1 hour ago.
- Matches rule INDICATOR_SUSPICIOUS_EXE_References_VEEAM from ruleset indicator_suspicious at https://github.com/ditekshen/detection by ditekSHen. Description: Detects executables containing many references to VEEAM. Observed in ransomware - 1 hour ago.
- Matches rule Ryuk from ruleset Ryuk at https://github.com/kevoreilly/CAPEv2 by kevoreilly. Description: Ryuk Payload - 1 hour ago.
- Matches rule INDICATOR_SUSPICIOUS_GENRansomware from ruleset indicator_suspicious at https://github.com/ditekshen/detection by ditekSHen. Description: Detects command variations typically used by ransomware - 1 hour ago.
- Matches rule win_ryuk_auto from ruleset win.ryuk_auto at https://malpedia.caad.fkie.fraunhofer.de/ by Felix Blitstein - yara-signator at cocacoding dot com. Description: Detects win.ryuk. - 1 hour ago.

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.