Alert Triage with Threat Intelligence

1. Objective

This report contains the details of the task including Triage Simulation, and IOC Validation.

The goal of this task is to:

- Learn validation of Indicators of Compromise along with simulation of Triage.

2. Introduction

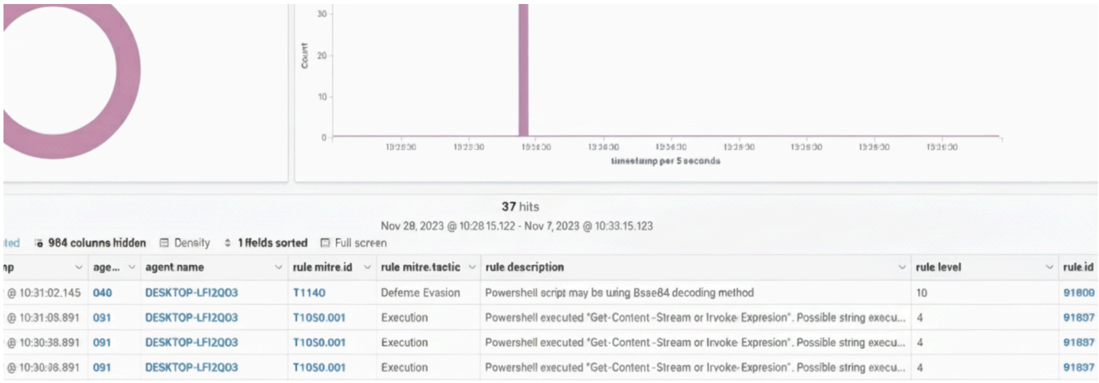
Alert Triage with Threat Intelligence is a process of using actionable information about the threats to help security teams to investigate, and respond to alerts efficiently. It includes Simulation of triage it means testing security team's ability to quickly identify, and respond to the incidents. IOC validation using tools like Alienvault OTX, and VirusTotal to check Or identify the IOCs whether they are malicious or not.

3. Tools

- Wazuh setup using official Wazuh documentation .
  https://documentation.wazuh.com/current/quickstart.html
- Alienvault OTX
  https://otx.alienvault.com/
- VirusTotal
  https://www.virustotal.com/gui/home/upload

4. Triage Simulation

Analyzing a mock alert (e.g., "Suspicious Powershell Execution") in Wazuh and documenting its metadata that includes Alert ID, Description, Source IP, Priority, and Execution. Testing The SOC teams how they analyze and respond to the incidents.



37 hits

Nov 28, 2023 @ 10:28 15.122 - Nov 7, 2023 @ 10:33.15.123

ted 984 columns hidden Density 1 fields sorted Full screen

np	age...	agent name	rule mitre.id	rule mitre.tactic	rule description	rule level	rule.id
@ 10:31:02.145	040	DESKTOP-LFI2QO3	T1140	Defense Evasion	Powershell script may be uing Bsae64 decoding method	10	91800
@ 10:31:08.891	091	DESKTOP-LFI2QO3	T10S0.001	Execution	Powershell executed "Get-Content -Stream or Irvoke Expresion". Possible string execu...	4	91837
@ 10:30:38.891	091	DESKTOP-LFI2QO3	T10S0.001	Execution	Powershell executed "Get-Content -Stream or Irvoke Expresion". Possible string execu...	4	91837
@ 10:30:08.891	091	DESKTOP-LFI2QO3	T10S0.001	Execution	Powershell executed "Get-Content -Stream or Irvoke Expresion". Possible string execu...	4	91837

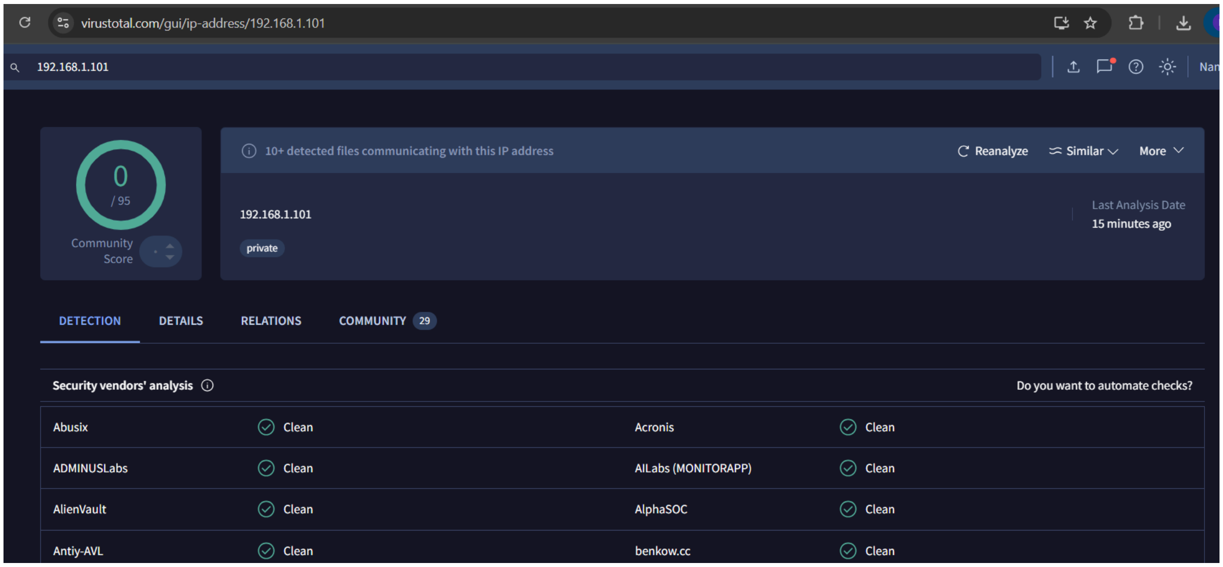
4.1 Triage Simulation Metadata

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

Alert ID	Description	Source IP	Priority	Status
004	Powershell Execution	192.168.1.101	High	Open

5. IOC Validation

IOC stands for Indicators of Compromise . IOC validation is done by using tools like Alien -valut OTX, and VirustTotal. Cross-referencing the alerts IP or hash with VirusTotal and OTX. Summarizing the findings.I found the IP address (192.168.1.101) as an Indicator of compromise. For IOC validation, the alert's source IP **192.168.1.101** was checked in VirusTotal and AlienVault OTX. VirusTotal reported no associated malware hashes, indicating no risk, while OTX also not showed any suspicious activity report linked to phishing attempts. Overall, the IOC is not suspicious and not required any monitoring.



virustotal.com/gui/ip-address/192.168.1.101

192.168.1.101

0 / 95 Community Score

10+ detected files communicating with this IP address

192.168.1.101

private

Last Analysis Date 15 minutes ago

Security vendors' analysis

Do you want to automate checks?

Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AILabs (MONITORAPP)	Clean
AlienVault	Clean	AlphaSOC	Clean
Antiy-AVL	Clean	benkow.cc	Clean