Alert Triage Practice

Objective:

The objective of this task is to perform alert triage by analyzing a security alert, assigning an appropriate priority, and validating indicators of compromise using threat intelligence platforms.

Alert Triage Details

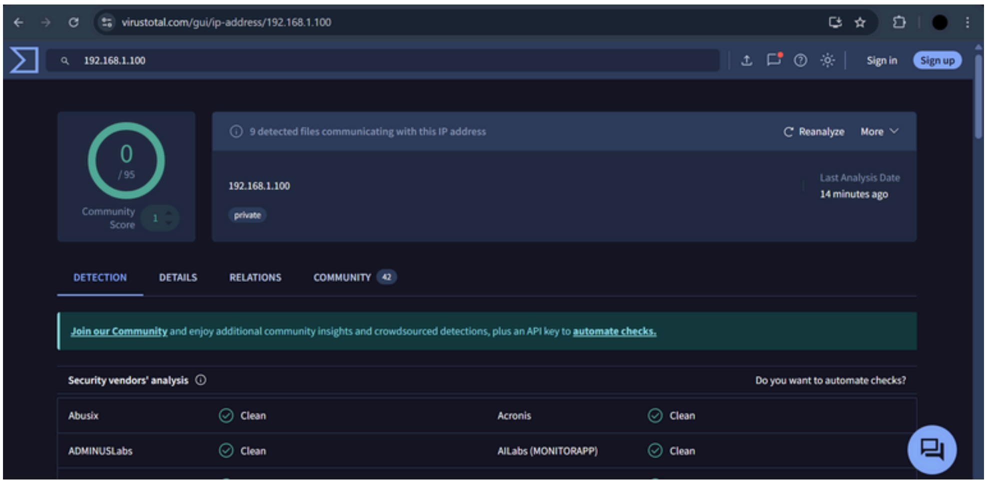
Alert ID	Description	Source IP	Priority	Status
2	Brute-force SSH	192.168.1.100	Medium	Open

Threat Intelligence Validation

Tool Used : VirusTotal

Indicator Checked:

IP Address: 192.168.1.100



virustotal.com/gui/ip-address/192.168.1.100

192.168.1.100

9 detected files communicating with this IP address

192.168.1.100

private

Last Analysis Date
14 minutes ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Abusix	✓ Clean	Acronis	✓ Clean
ADMINUSLabs	✓ Clean	AILabs (MONITORAPP)	✓ Clean

Threat Intelligence Findings

The source IP address 192.168.1.100 was analyzed using VirusTotal. The IP address is classified as a private address and showed no malicious detections from security vendors. The alert was identified as a possible brute-force SSH attempt, assigned Medium priority, and kept open for monitoring.

Outcome:
No immediate escalation was required. The alert was monitored for further activity as part of routine SOC operations to avoid false positives.

Key Learning:
This task improved understanding of alert triage, IOC validation, and decision-making using threat intelligence tools.