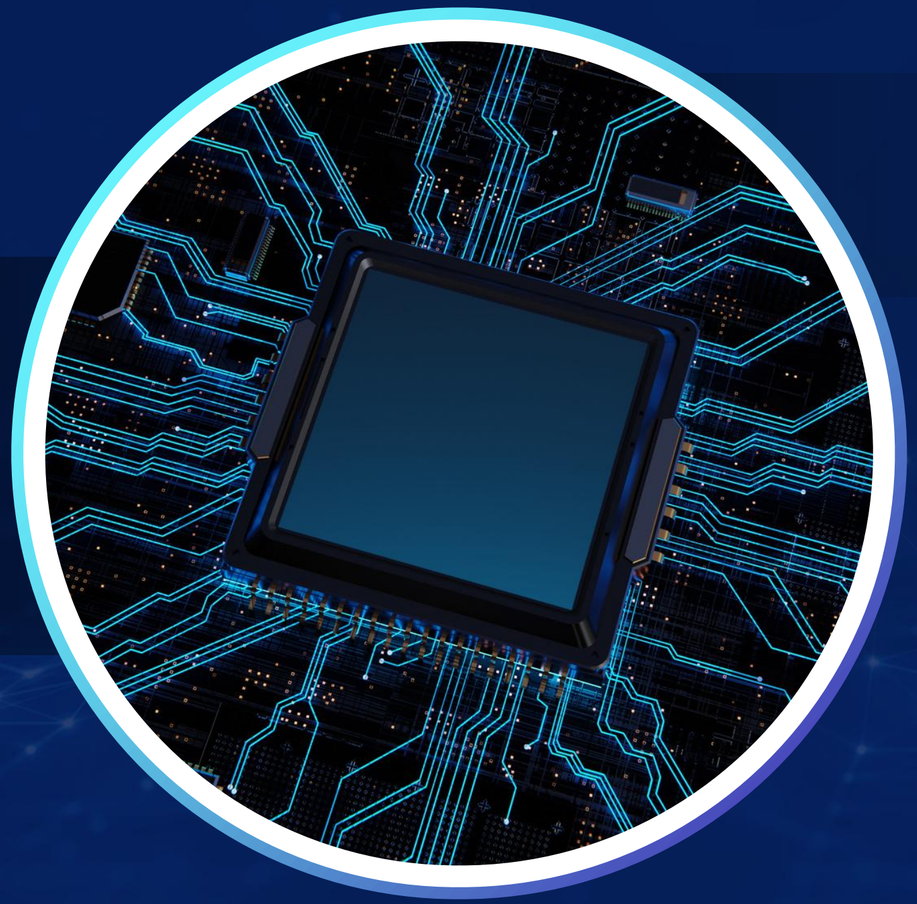
MINI-SOC PROJECT

https://github.com/Eng-Ahmed-Emad/A_mini_SOC-Project



Project Overview

This project proposes the development of a mini Security Operations Center (SOC) that combines three powerful tools:

- Wazuh SIEM for centralized log collection, analysis, and alerting.
- Atomic Red Team for simulating adversary techniques aligned with the MITRE ATTACK framework.
- VirusTotal API integration for automated detection and verification of malicious files on Linux systems.

By integrating these technologies, the project replicates a realistic SOC workflow — from log ingestion and correlation, to adversary emulation, to automated threat intelligence validation.

Objectives

- Deploy a Wazuh-based SIEM to collect and analyze security events from Linux hosts.
- Simulate common adversary techniques (e.g., brute force, privilege escalation, malware execution) using Atomic Red Team.
- Integrate VirusTotal API for automated file hash submission and malicious file detection.
- Generate real-time alerts and incident triage reports mapped to the MITRE ATT&CK framework.
- Document the SOC architecture, detection use cases, and incident workflows.

OUR TEAM

POULA YOUSSEF

EBTIHAL RAGAB

AHMED EMAD

MENNA MOHAMED

DOHA MOHAMED

WHY WAZUH?

USE CASES

Endpoint security	Threat intelligence	Security operations	Cloud security
Configuration assessment	Threat hunting	Incident response	Container security
Malware detection	Log data analysis	Regulatory compliance	Posture management
File integrity monitoring	Vulnerability detection	IT hygiene	Workload protection

STEPS

- **Install Ubuntu Server (VM)** – Create a dedicated virtual machine for the SOC manager.
- **Update System Packages** – Run updates to ensure stability and security.
- **Install Wazuh Manager** – Set up the SIEM for log collection and analysis.
- **Install OpenSearch & Dashboard** – Enable visualization and alert monitoring.
- **Deploy Wazuh Agent** – Install agents on Windows/Linux endpoints to collect logs.
- **Register Agents** – Connect agents to the Wazuh Manager for monitoring.

STEPS

- **Configure Log Sources** – Collect Windows Event Logs, Sysmon, and Linux syslog.
- **Enable Detection Rules** – Apply Wazuh's ruleset for threat detection.
- **Enable File Integrity Monitoring (FIM)** – Track changes in critical files/directories on Windows & Linux.
- **Integrate VirusTotal API** – Enrich alerts with threat intelligence data.
- **Run Atomic Red Team Tests** – Simulate real-world attack techniques.
- **Verify Alerts** – Check if Wazuh detects and generates alerts correctly.

STEPS

Investigate & Respond – Analyze alerts, isolate systems, and take response actions.

Document Results – Summarize detection performance and lessons learned.

Create Custom Dashboards – Build tailored views for alerts, FIM, and attack simulations.

Simulated Attacks (Atomic Red Team)

- 🛑 Brute Force Login Attempts – repeated failed logins
- 🔑 Privilege Escalation – sudo abuse on Ubuntu
- 🐉 Malware Execution – malicious binaries & scripts
- 📤 Data Exfiltration – outbound suspicious traffic
- 🧬 Process Injection – tampering with legitimate processes

Detection Effectiveness

- ✅ Brute Force → alerts triggered after threshold logins
- ✅ Privilege Escalation → sudo misuse flagged
- ✅ Malware Execution → suspicious process behavior detected
- ✅ Data Exfiltration → flagged by outbound traffic rules
- ✅ Process Injection → abnormal process behavior detected
- ✅ VirusTotal Integration → malicious files auto-removed

Alerts before vs after attack (Windows)

wazuh.

info@wazuh.com
https://wazuh.com

Alerts summary

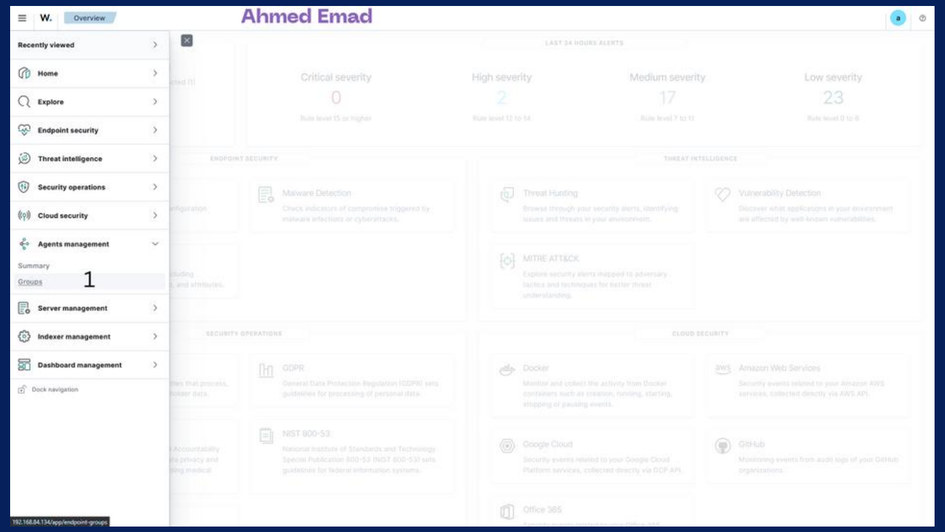
Rule ID	Description	Level	Count
60106	Windows Logon Success	3	3
506	Wazuh agent stopped.	3	1

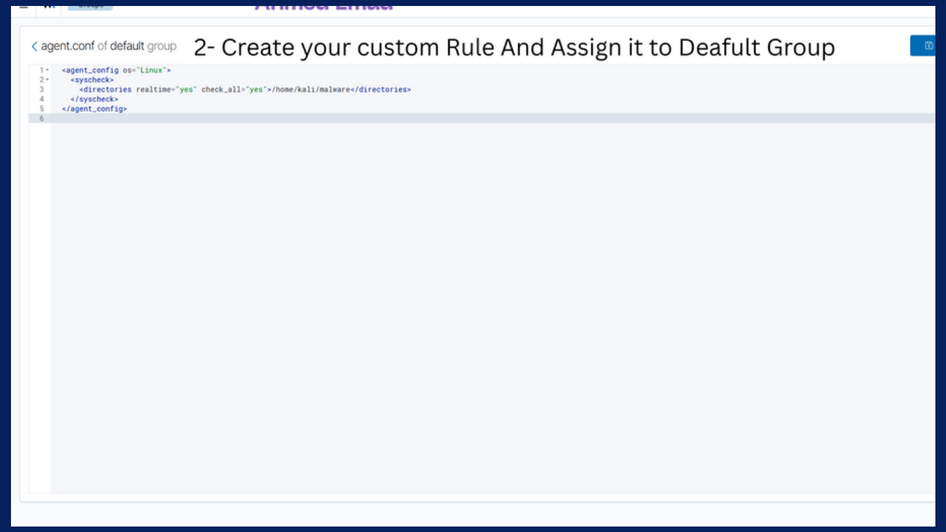
wazuh.

info@wazuh.com
https://wazuh.com

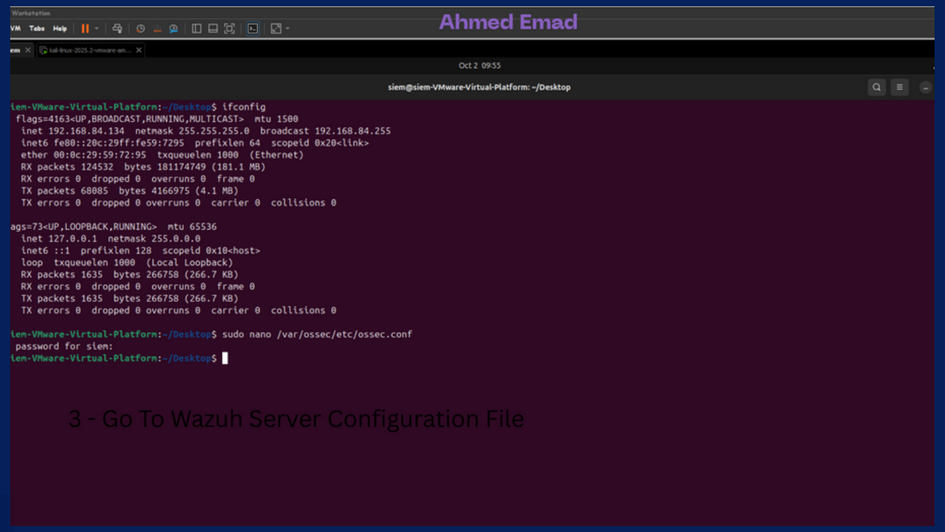
Alerts summary

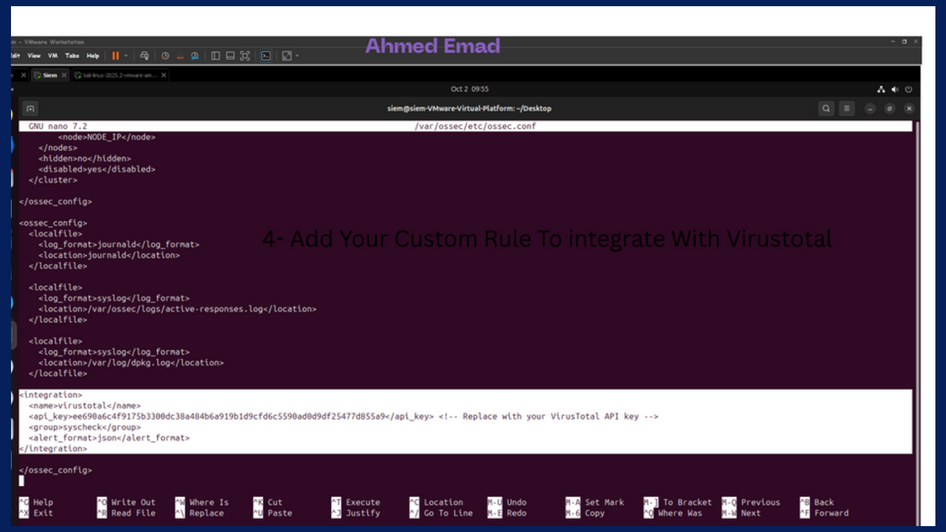
Rule ID	Description	Level	Count
60106	Windows Logon Success	3	340
67018	System shutdown initiated.	3	11
553	File deleted.	7	8
506	Wazuh agent stopped.	3	3
550	Integrity checksum changed.	7	3
61138	New Windows Service Created	5	2
60747	WMI service started successfully.	3	1

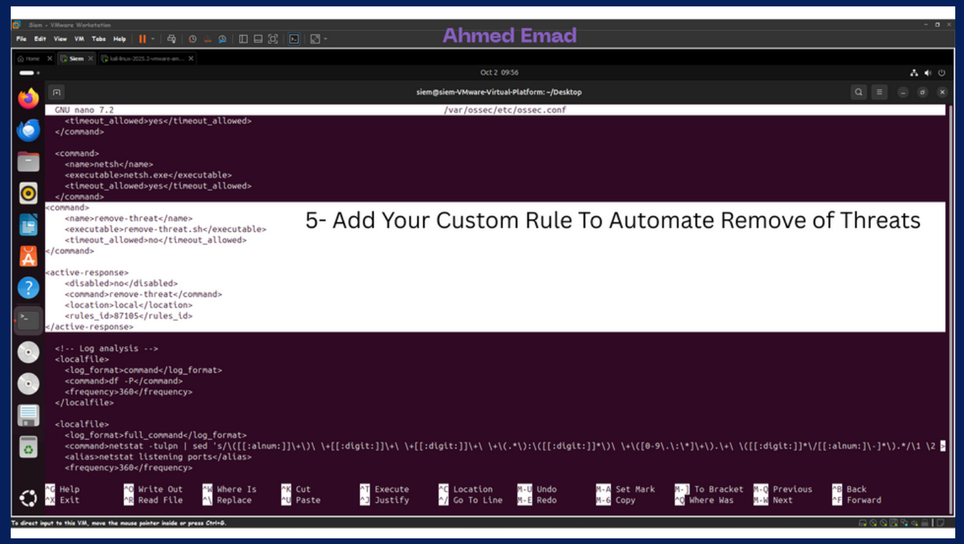




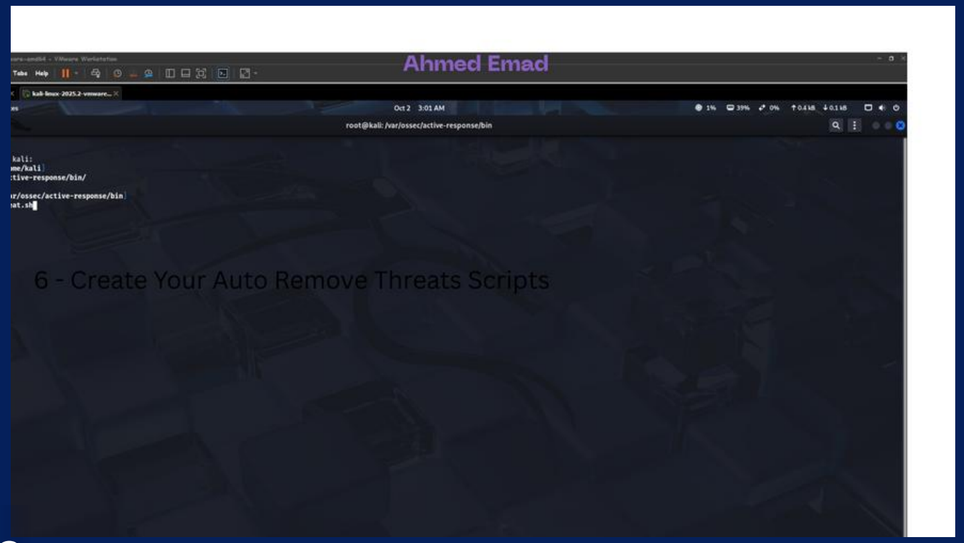
VirusTotal Integration in Mini SOC

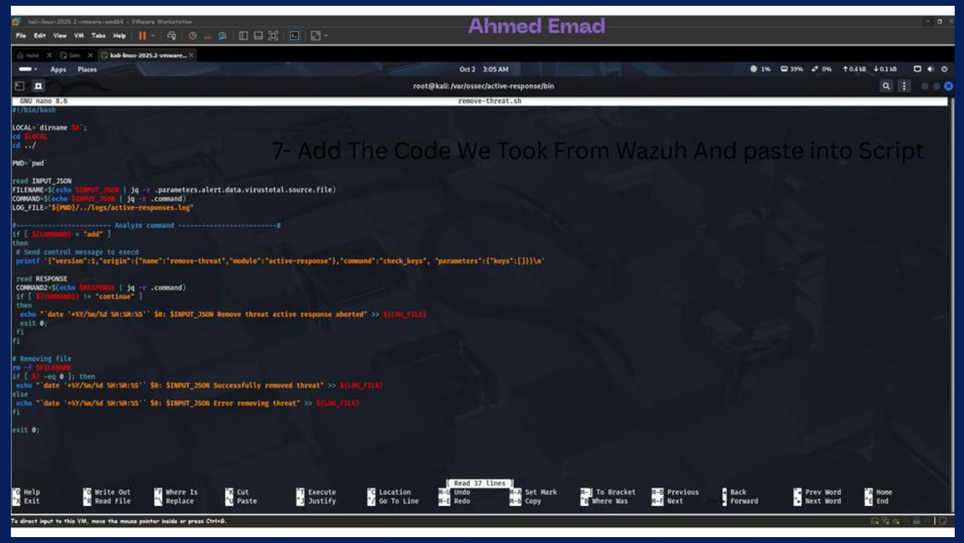





Ahmed Emad
5- Add Your Custom Rule To Automate Remove of Threats


Ahmed Emad
6 - Create Your HoneyPot On Kali Age


Ahmed Emad
6 - Create Your Auto Remove Threats Scripts


Ahmed Emad
7- Add The Code We Took From Wazuh And paste into Script

Alerts after attack (Linux+FIM+Virustotal)

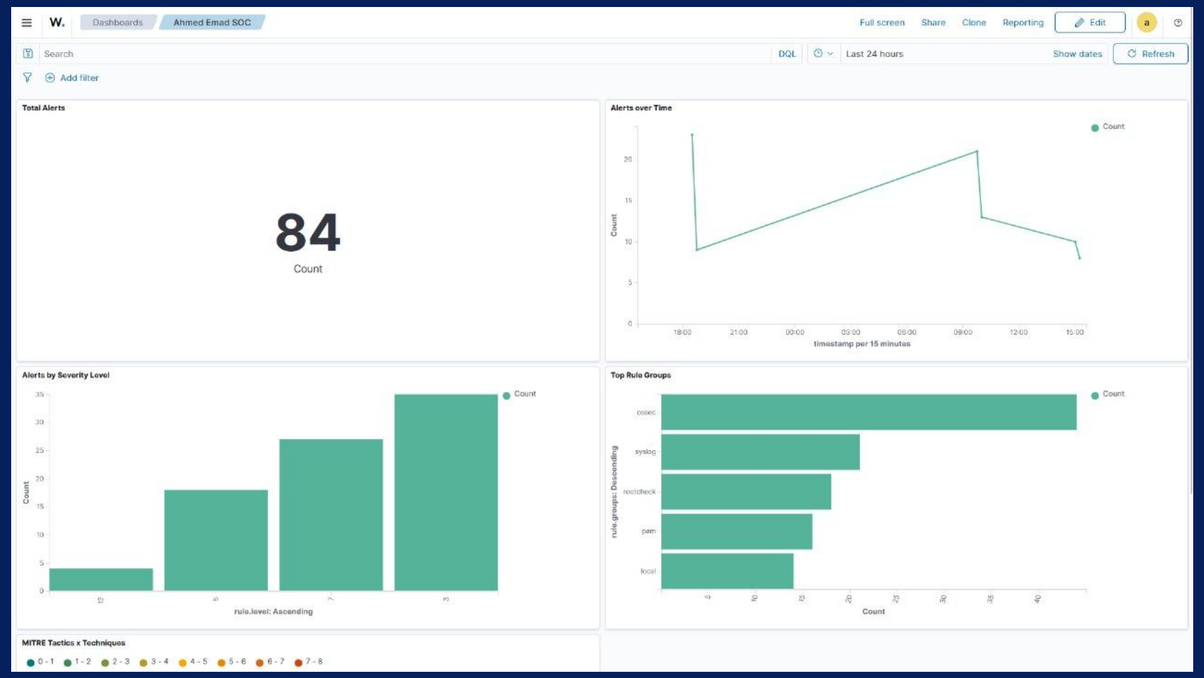
wazuh.

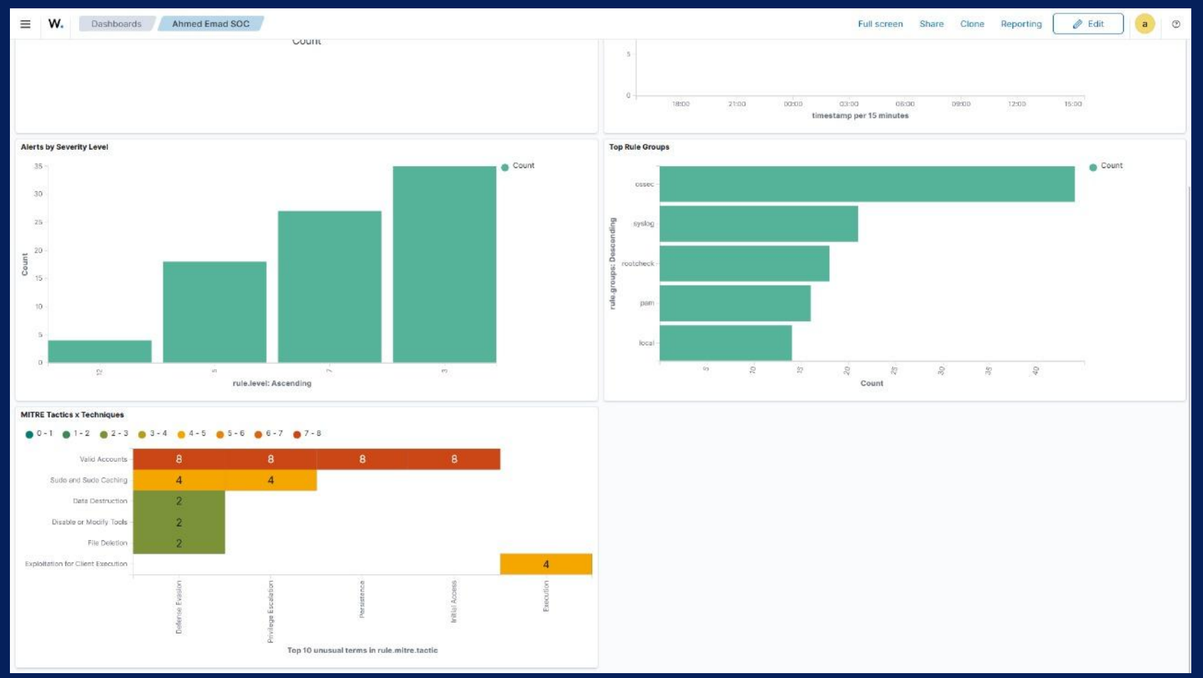
info@wazuh.com
https://wazuh.com

Alerts summary

Rule ID	Description	Level	Count
510	Host-based anomaly detection event (rootcheck).	7	78
40704	Systemd: Service exited due to a failure.	5	30
5502	PAM: Login session closed.	3	23
5501	PAM: Login session opened.	3	20
503	Wazuh agent started.	3	12
506	Wazuh agent stopped.	3	12
5402	Successful sudo to ROOT executed.	3	8
553	File deleted.	7	8
657	Active response: active-response/bin/remove-threat.sh - add	3	8
554	File added to the system.	5	7
87105	VirusTotal: Alert - /home/kali/malware/ecir - 66 engines detected this file	12	6
87103	VirusTotal: Alert - No records in VirusTotal database	3	6
2902	New dpkg (Debian Package) installed.	7	4
2904	Dpkg (Debian Package) half configured.	7	4
533	Listened ports status (netstat) changed (new port opened or closed).	7	4
1004	Syslogd exiting (logging stopped).	5	3
87105	VirusTotal: Alert - /home/kali/malware/ecir - 65 engines detected this file	12	2
100201	File added to /home/kali/malware	7	2
2901	New dpkg (Debian Package) requested to install.	3	2
5403	First time user executed sudo.	4	2
87104	VirusTotal: Alert - /home/kali/malware/3omda2.txt - No positives found	3	2

Created a custom dashboard





RISK MANAGEMENT

Risk Assessments

Identified key risks (misconfigurations, API limits, delays) and applied mitigation strategies.

Policy Development

- Access Control → Strong authentication & least privilege enforced.
- Log Management → Centralized log collection in Wazuh, retained for analysis & compliance.
- Incident Response → Defined thresholds, rapid triage, and automated actions (e.g., quarantine, block).
- Malware Handling → Files auto-scanned with VirusTotal; malicious files quarantined/deleted.
- Continuous Improvement → Regular tuning of rules, scheduled attack simulations, and policy updates.

THANK YOU FOR YOUR ATTENTION

https://github.com/Eng-Ahmed-Emad/A_mini_SOC-Project