SOC-SIEM Incident Detection System Report

Project Overview

This project demonstrates a simplified Security Operations Center (SOC) workflow using SIEM principles to detect suspicious SSH login activity. It includes log collection, parsing, and rule-based threat detection using Python.

Step 1: Log Collection & Understanding

- SSH Service Setup (systemctl start/enable/status ssh)
- SSH Connection Attempts (failed logins, permission denied)
- User Management (adduser, passwd)
- Viewing SSH logs (/var/log/auth.log)

Step 2: Log Parsing (Python)

- Extract IP address
- Extract timestamp
- Extract event type (login failed/success)
- Combine all in parse_ssh_log()

Step 3: Threat Detection Rules

- Rule 1: Detect repeated failed logins
- Rule 2: Detect brute-force attacks
- Rule 3: Flag suspicious IPs
- Rule 4: Detect suspicious success after failures

Screenshots to Include

- SSH service status
- SSH login attempt with failure
- User creation and password update
- Raw SSH logs

SOC-SIEM Incident Detection System Report

- Parsed log output
- Rule match output

Technologies Used

- Python (log parsing and rule logic)
- Linux (SSH service and log generation)
- Jupyter Notebook (analysis and documentation)

Author

Aziz Ul Haq

Cybersecurity & Data Science Enthusiast

Rawalpindi, Pakistan

GitHub:

https://github.com/Azizulhaq-professional/Aziz-Cybersecurity-Labs/tree/main/SOC_SIEM_Incident_Detection_System