Real-Time Threat Hunting and Incident Response Toolkit

Project Report: Real-Time Threat Hunting and Incident Response Toolkit

Submitted by: Jagadeesh Kumar S

This project showcases a simulation of a Security Operations Center (SOC) alert system using Suricata IDS and a custom Python script. It captures real-time network traffic, detects suspicious activities, and sends email alerts for high-severity threats. This serves as a hands-on demonstration of threat detection, alerting, and incident response skills.

Features

- Real-time traffic analysis with Suricata
- Alert generation and parsing via Suricata's eve.json
- Custom Python script to scan logs and identify high-severity alerts
- Automatic email notification to SOC analyst or admin
- Cron scheduling support for automation

Setup Instructions

1. Install Suricata on Kali Linux:

```
$ sudo apt update && sudo apt install suricata -y
```

2. Start Suricata in live mode:

```
$ sudo suricata -i eth0 -l /var/log/suricata
```

3. Save the Python script at: /opt/threat-monitor/email-alert.py

4. Make it executable:

```
$ sudo chmod +x /opt/threat-monitor/email-alert.py
```

5. Run Suricata with PCAP (optional):

```
$ sudo tcpdump -i eth0 -w test.pcap -c 10
```

```
$ sudo suricata -r test.pcap -l /var/log/suricata
```

6. Run the Python alert script:

```
$ sudo /opt/threat-monitor/email-alert.py
```

Python Script Summary

- Parses /var/log/suricata/eve.json

- Looks for high or medium severity alerts in the last hour

- Sends an email alert with details (requires mailutils or equivalent setup)

User Manual

To use the toolkit:

1. Start Suricata with: sudo suricata -i eth0 -l /var/log/suricata

2. Generate traffic or simulate attack using tools like Metasploit

3. Run the Python script to scan logs and generate alerts

4. Check email inbox for alerts

Future Enhancements

- Integrate MongoDB or Elasticsearch for long-term alert storage

- Build a frontend dashboard with Flask/Django

- Add PDF/CSV report generation of daily alerts

- Add webhook or Slack alert support