Beta Team

42Beirut x Teknologiia Hackathon

Project Summary

An AI-powered automation system that analyzes network security logs, enriches them with threat intelligence multi API calls and uses multiple AI models to accurately classify threats with minimal false positives.

Technology Stack

- **Platform:** Docker + N8N workflow automation
- **AI Models:** OpenAI GPT-4, DeepSeek, Google Gemini
- **Threat Intel:** AbuseIPDB, VirusTotal, IPQualityScore, AlienVault OTX,ThreatFox, IPgeolocation.
- **Visualization:** HTML and JS
- **Alerts:** Slack notifications

How It Works

1. Setup

- Ubuntu Linux VM (16GB RAM, 100GB storage)
- Docker containers for N8N automation
- API keys configured for 6 threat intelligence services
- Had few setbacks the VM kept on lagging and crashing

2. Log Parsing

- Read CSV firewall logs (IPs, ports, protocols, attack types)
- Validate and structure 25+ fields per entry
- Extract existing security indicators (malware, anomaly scores, severity)

3. Risk Scoring

Calculate risk score (0-100) based on:

- Anomaly score from logs (30 points)
- Malware indicators (25 points)
- Attack signatures (25 points)
- Severity level (20 points)
- IDS/IPS alerts (15 points)
- Sensitive ports (20 points)

Smart Filter: Only events scoring ≥40 get deep enrichment (saves 66% API costs)

4. Threat Intelligence Enrichment

For high-risk events, query 6 APIs to gather:

- IP reputation scores and abuse reports
- Malware associations and IOC databases
- Proxy/VPN/Tor detection
- Network information (BGP/ASN)
- Open ports and vulnerabilities
- Historical threat data

Rate Limit Strategy: Process in batches of 100, wait 15 seconds between batches

5. AI Analysis

Send enriched data to 3 AI models simultaneously:

- **OpenAI GPT-4:** Complex reasoning
- **DeepSeek:** Technical pattern recognition
- **Google Gemini:** Fast, balanced analysis

Each model provides:

- Classification (TRUE_POSITIVE / FALSE_POSITIVE)
- Confidence score (0-100%)
- Evidence and reasoning
- Recommended actions

Consensus Algorithm:

- If all agree → Boost confidence by 10%
- If 2/3 agree → Use weighted vote
- Final classification = majority decision weighted by confidence

Conclusion

This project successfully demonstrates how automation, threat intelligence, and AI can work together to improve security operations. By combining 6 data sources with 3 AI models, the system achieves high accuracy while reducing analyst workload.