Team Details

- Team name: Smooth_Operator
- Team leader name: Het Modi
- Team leader email-id: m.hetmodi@gmail.com
- Problem Statement: Cyber-Resilient Infrastructure for Critical Sectors
- Team Members: Chinmay Patel, Aryan Vadhadiya, Jay Shah, Het Patel

INGENIOUS 7.0 HACKATHON

unstop

~SMOOTH OPERATOR~

Problem Overview

Critical digital infrastructures in healthcare, agriculture, and urban systems operate at large scale and are expected to be always available and secure. However, these **systems are increasingly exposed to sophisticated cyber threats**, many of which operate over encrypted traffic and evade traditional security mechanisms.

Our Idea

- An intelligent, behaviour-based security system that **detects zero-day and advanced threats hidden in encrypted traffic without decryption**.
- **Machine learning-driven** anomaly detection enables automated, **rapid threat containment** and delivers an adaptive, **future-ready cyber-resilience layer** for critical infrastructure.

Our Progress

- Implemented kubernetees with horizontal pod scaling.
- Add email on alert/attack functionality.
- Added rate limiting (customisable value) in the node software.
- Added ip blocking in by node.
- Developed a unified setup utility that provisions the complete Kubernetes environment.
- Federated learning on telemetry data.

Proof of Concept

📋 Problem → Solution Mapping

Problem Requirement	Your Solution	Status
Real-time monitoring	Ingest Service + WebSocket	✅
Anomaly detection algorithms	ML Models (LSTM, RF) + Rule Engine	✅
Alerting system with severity levels	Alert Manager (low/medium/high/critical)	✅
Automated response mechanisms	Response Engine + Playbooks	✅
Dashboard showing security status	React Frontend	✅
Simulated attack scenarios	Attack Simulator Scripts	✅
Healthcare/Agriculture/Urban domains	Domain-specific ML models	✅
Scalability	Kubernetes + HPA	✅

Approach

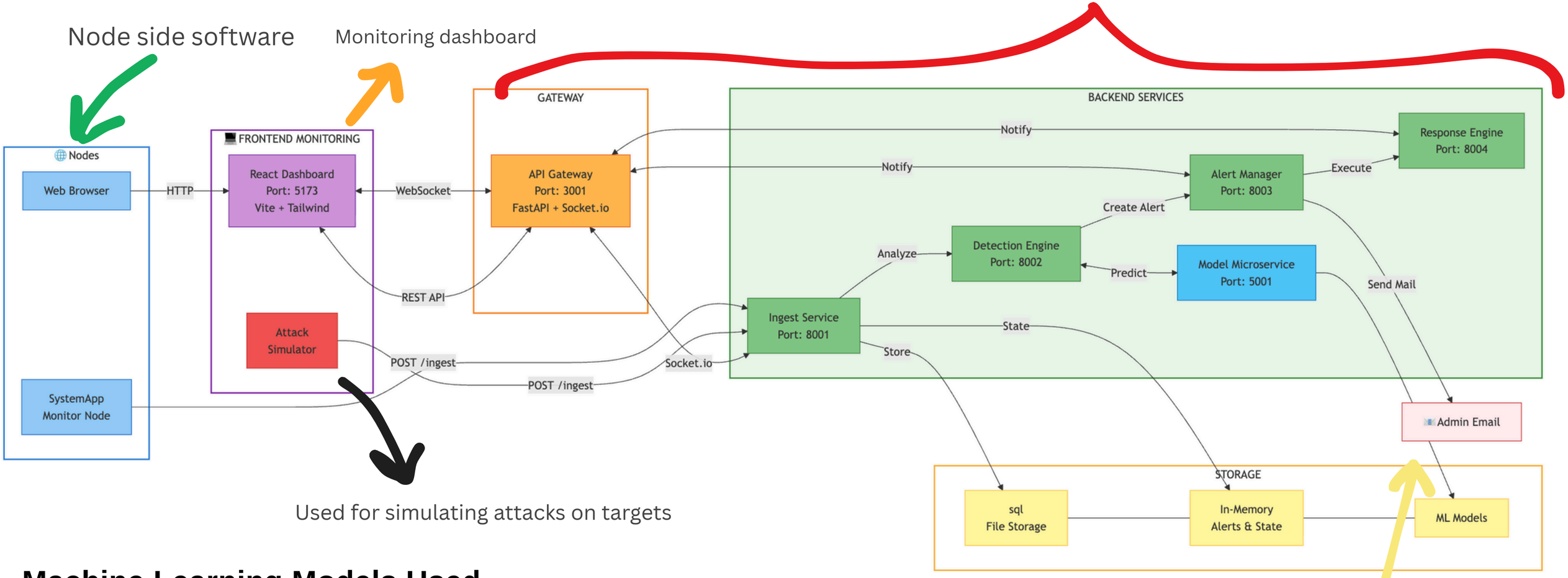
- Traffic Capture & Flow Construction
- **Network traffic is captured at the edge,** extracting timing, volume, and protocol-level metadata.
- Encryption-Aware Routing
- **Rule-Based Analysis for Unencrypted Traffic**
- Unencrypted traffic is inspected using predefined signatures and security rules for fast, deterministic detection.
- Behaviour-Based Analysis for Encrypted Traffic
- **Encrypted traffic bypasses payload inspection and is analysed using flow-level behavioural features.**
- Domain-Aware Model Selection
- The system dynamically selects the appropriate detection model based on the operational context:
  - General Network → **Neural Network Classifier**
  - Agriculture → **LSTM Autoencoder**
  - Healthcare → **LSTM Classifier**
  - Urban → **LSTM Forecaster**
- Threat Scoring & **Decision Engine**
- Automated & Manual Response Execution
- **Federated Learning Feedback Loop**
- **Local learnings are aggregated centrally and redistributed,**

Architecture Diagram

Each service has its own **docker** image which is then scaled on **kubernetees**

Node side software

Monitoring dashboard



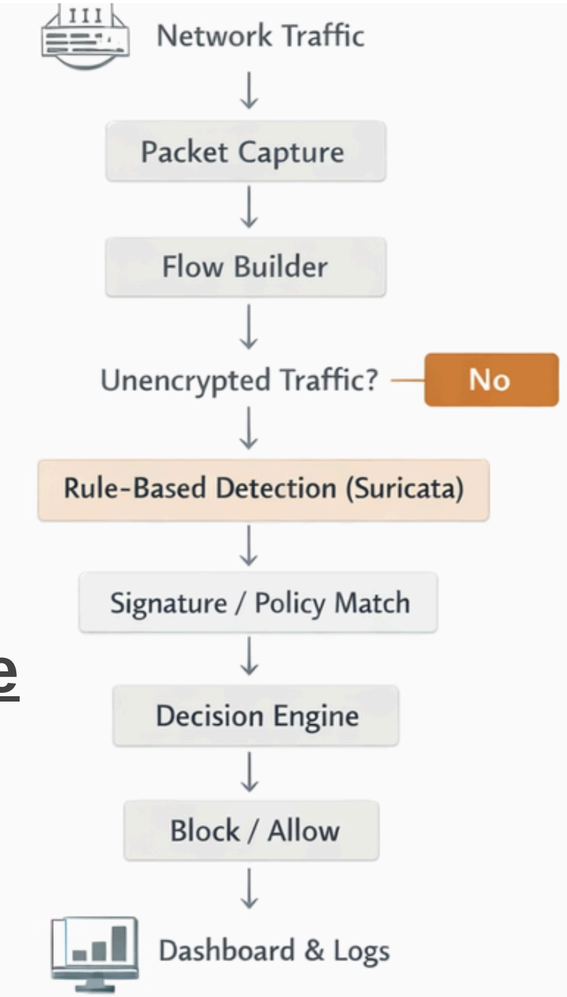
Used for simulating attacks on targets

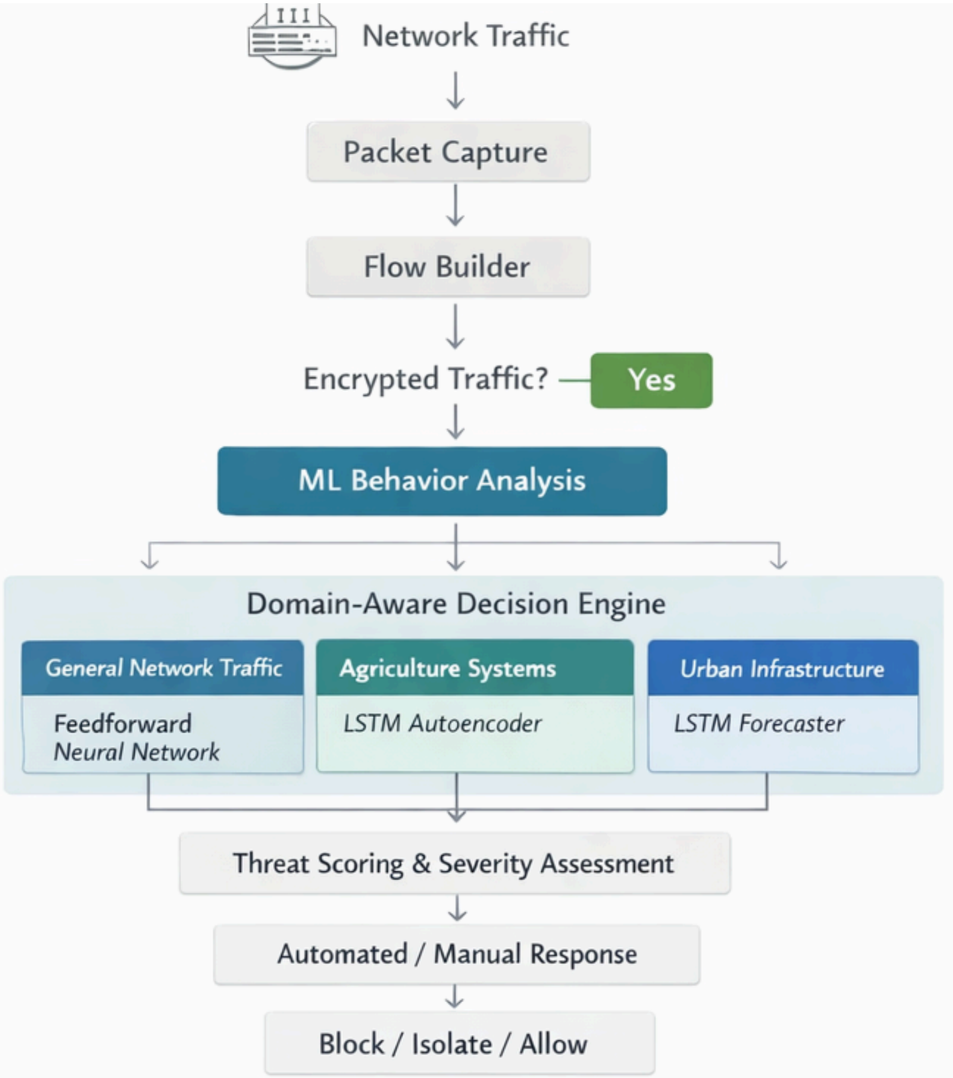
Email notification

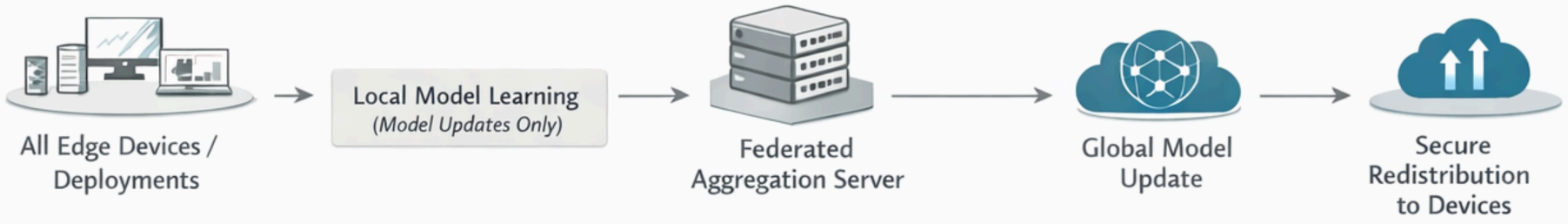
Machine Learning Models Used

1. **Feedforward Neural Network** (PyTorch): **Generic network attack detection** (DDoS, Botnet, Brute Force)
2. **Isolation Forest** (Unsupervised ML): Network flow based anomaly detection on encrypted traffic
3. **LSTM Autoencoder** (Unsupervised): Agriculture sensor spoofing and physics-based anomaly detection
4. **LSTM Classifier** (Supervised): Healthcare IoMT DDoS and traffic surge detection
5. **LSTM Forecaster** (Regression) : Urban traffic flow prediction and grid manipulation detection

Detection engine



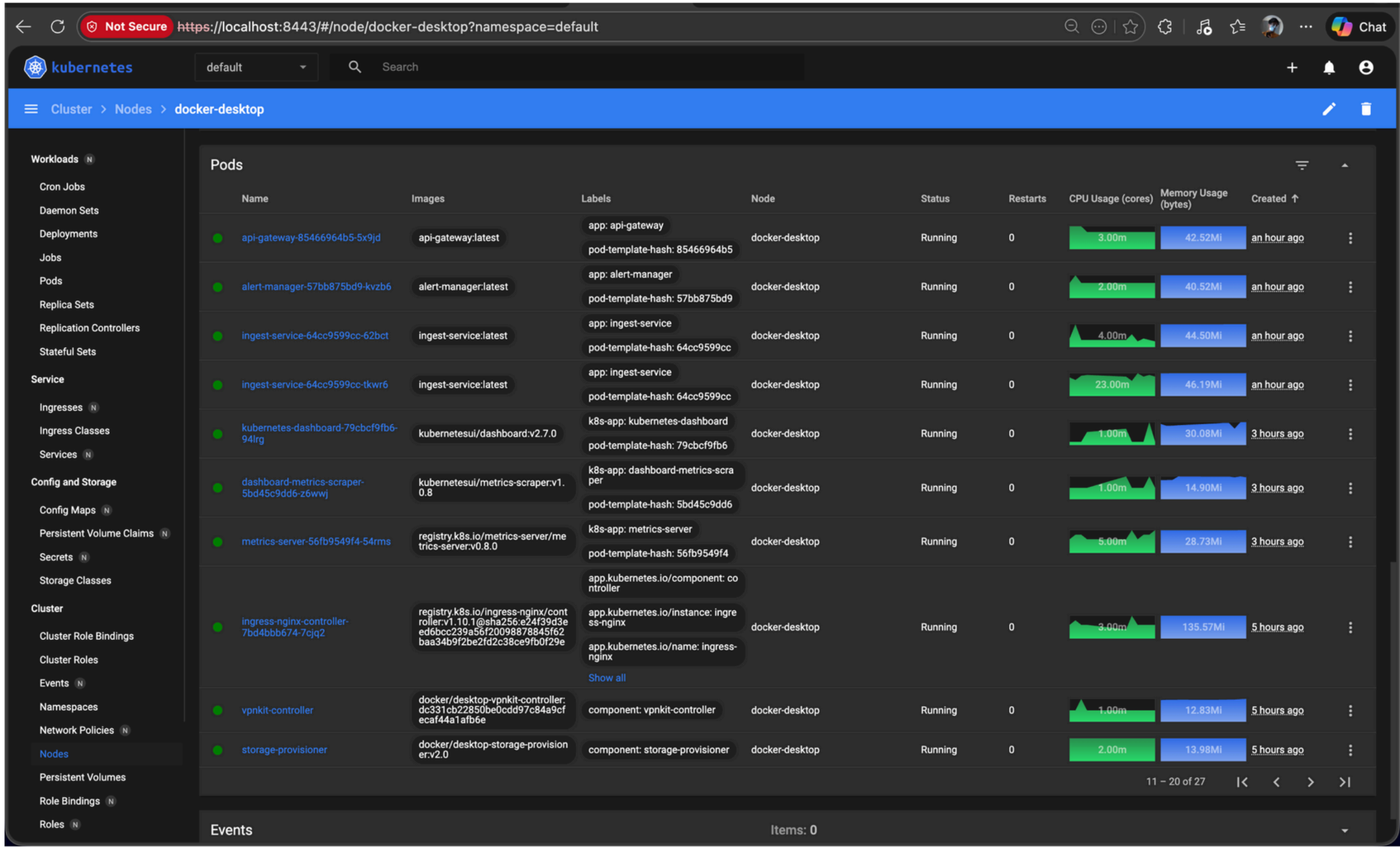




Scalability : Kubernetes

- The platform uses Kubernetes **Horizontal Pod Autoscaler** to dynamically scale services based on real-time resource utilization.
- **Self-Healing Infrastructure**: Failed or compromised pods are automatically recreated.
- **Multi-Replica Critical Services:** Detection, alerting, and dashboard services run with replicas.

```
(base) jay@Jays-MacBook-Air Smooth_Operator % ./k8s/kuber_start.sh
🚀 Starting Threat Ops Kubernetes Deployment...
✅ Kubernetes cluster detected
✅ Docker images found
🚢 Deploying to Kubernetes...
deployment.apps/ingest-service configured
service/ingest-service unchanged
deployment.apps/api-gateway configured
service/api-gateway unchanged
deployment.apps/detection-engine configured
service/detection-engine unchanged
deployment.apps/alert-manager configured
service/alert-manager unchanged
deployment.apps/response-engine configured
service/response-engine unchanged
deployment.apps/frontend configured
service/frontend unchanged
deployment.apps/model-microservice configured
service/model-microservice unchanged
deployment.apps/systemapp configured
service/systemapp unchanged
ingress.networking.k8s.io/threat-ops-ingress unchanged
```



PROJECT FEATURES

ZERO-DAY & ENCRYPTED ATTACK DETECTION

- **Live Packet Capture** : Uses **unsupervised machine learning** to learn effectively detects previously unseen attacks that bypass signature-based security systems

AUTOMATED RESPONSE & POLICY ENFORCEMENT (SOAR)

- Automatically blocks malicious IPs, and escalates alerts based on threat severity and confidence levels.

LAYERED AI DEFENSE ARCHITECTURE

- Ensures early-stage filtering of broad attacks while enabling **deep contextual analysis** for healthcare, agriculture, and urban systems.
  -

REAL-TIME DASHBOARD & VISUALIZATION

- Displays **live telemetry, alert timelines, device status**, and response actions through **WebSockets**.

FEDERATED LEARNING–ENABLED COLLECTIVE DEFENSE

- Only model updates and threat insights are shared and **aggregated centrally** to improve global detection accuracy.

ATTACK SIMULATION & TESTING FRAMEWORK

- Includes **attacker and victim simulation** tools to validate detection and response workflows.

KUBERNETES-BASED SCALABLE DEPLOYMENT

- Uses containerization and Kubernetes orchestration to automatically scale edge services and central components based on traffic load, ensuring high availability, fault tolerance, and consistent performance under attack conditions.

AUTOMATED ALERT GENERATION & SEVERITY CLASSIFICATION

- Transforms detected security issues into human-readable alerts through emails with clear severity levels.

CODE SNiPPETS

ANN - GENERiC NETWORK ATTACKS

```python
train_idx, _ = train_test_split(range(len(tensor_x)), test_size=0.2)
        loader = DataLoader(TensorDataset(tensor_x[train_idx], tensor_y[train_idx]), batch_size=2048, shuffle=True)

        model = GeneralNetworkShield(input_dim=X.shape[1]).to(DEVICE)
        optimizer = optim.Adam(model.parameters(), lr=0.001)
        criterion = nn.BCELoss()

        model.train()
        for epoch in range(3):
            total_loss = 0
            for X_batch, y_batch in loader:
                X_batch, y_batch = X_batch.to(DEVICE), y_batch.to(DEVICE)
                optimizer.zero_grad()
                out = model(X_batch)
                loss = criterion(out, y_batch)
                loss.backward()
                optimizer.step()
                total_loss += loss.item()
            print(f"   Epoch {epoch+1} Loss: {total_loss/len(loader):.4f}")
```

```python
client_id = data.get('client_id', 'unknown')
        client_weights = data.get('weights')

        if not client_weights:
            print(f"[ERR] No weights in payload from {client_id}")
            return jsonify({"error": "Missing weights"}), 400

        print(f"[INFO] Processing update from {client_id} (Keys: {len(client_weights)})")

        client_state_dict = {k: torch.tensor(v).to(DEVICE) for k, v in client_weights.items()}

        pending_updates.append(client_state_dict)
        print(f"[FL] Received FL update from {client_id}. Progress: {len(pending_updates)}/{REQUIRED_UPDATES_FOR_AVG}")

        if len(pending_updates) >= REQUIRED_UPDATES_FOR_AVG:
            print("[FL] Aggregating Global Model (FedAvg)...")

            # FEDERATED AVERAGING ALGORITHM
            avg_weights = copy.deepcopy(GLOBAL_MODEL.state_dict())
            for key in avg_weights.keys():
                # Stack all updates for this key and take mean
                # Ensure all updates have this key
                valid_updates = [u[key] for u in pending_updates if key in u]
                if valid_updates:
                    stacked = torch.stack(valid_updates)
                    avg_weights[key] = torch.mean(stacked, dim=0)

            # Update Global Model
            GLOBAL_MODEL.load_state_dict(avg_weights)
            FL_ROUND += 1
            pending_updates = [] # Reset
            print(f"[SUCCESS] Global Model Updated! New Round: {FL_ROUND}")
```

```python
@app.route('/api/fl/submit-update', methods=['POST'])
def submit_update():
```

FEDERATED LEARNiNG ENDPOiNT

POSTMAN MODEL TESTiNG

POST http://127.0.0.1:5000/api/analyze Send

Docs Params Authorization Headers (9) Body Scripts Settings

none form-data x-www-form-urlencoded raw binary GraphQL JSON

```
{
    "sector": "healthcare",
    "payload": "SELECT * FROM patients WHERE id=1 OR 1=1",
    "sensor_data": [60, 10, 5, 5]
}
```

Body Cookies Headers (6) Test Results 200 OK 70 ms 339 B

{} JSON Preview Visualize

```
{
    "message": "Malicious Web Payload Detected (SQLi/XSS)",
    "source": "Web Gatekeeper",
    "status": "blocked",
    "threat_level": "high"
}
```

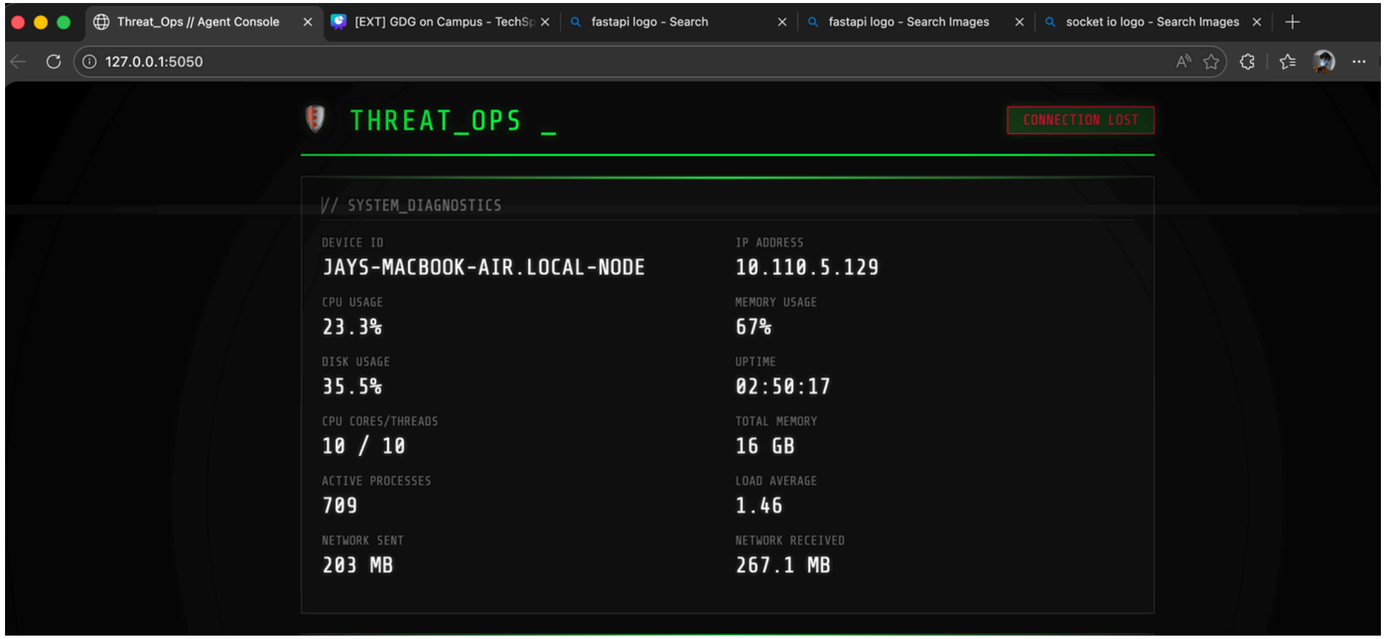
HEALTH CARE ML MODEL

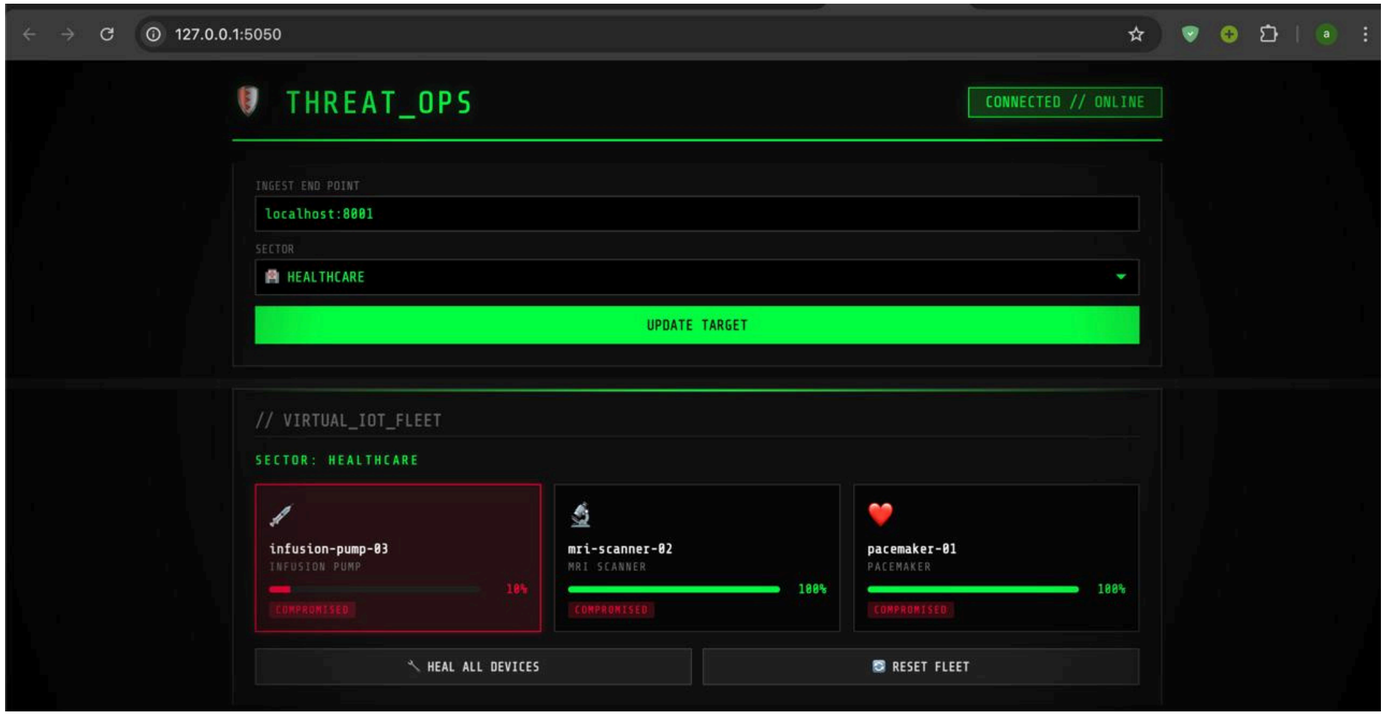
	precision	recall	f1-score	support
Normal	1.00	0.98	0.99	47974
DDoS	0.99	1.00	0.99	51893
accuracy			0.99	99867
macro avg	0.99	0.99	0.99	99867
weighted avg	0.99	0.99	0.99	99867

Accuracy: 0.9910280673295483

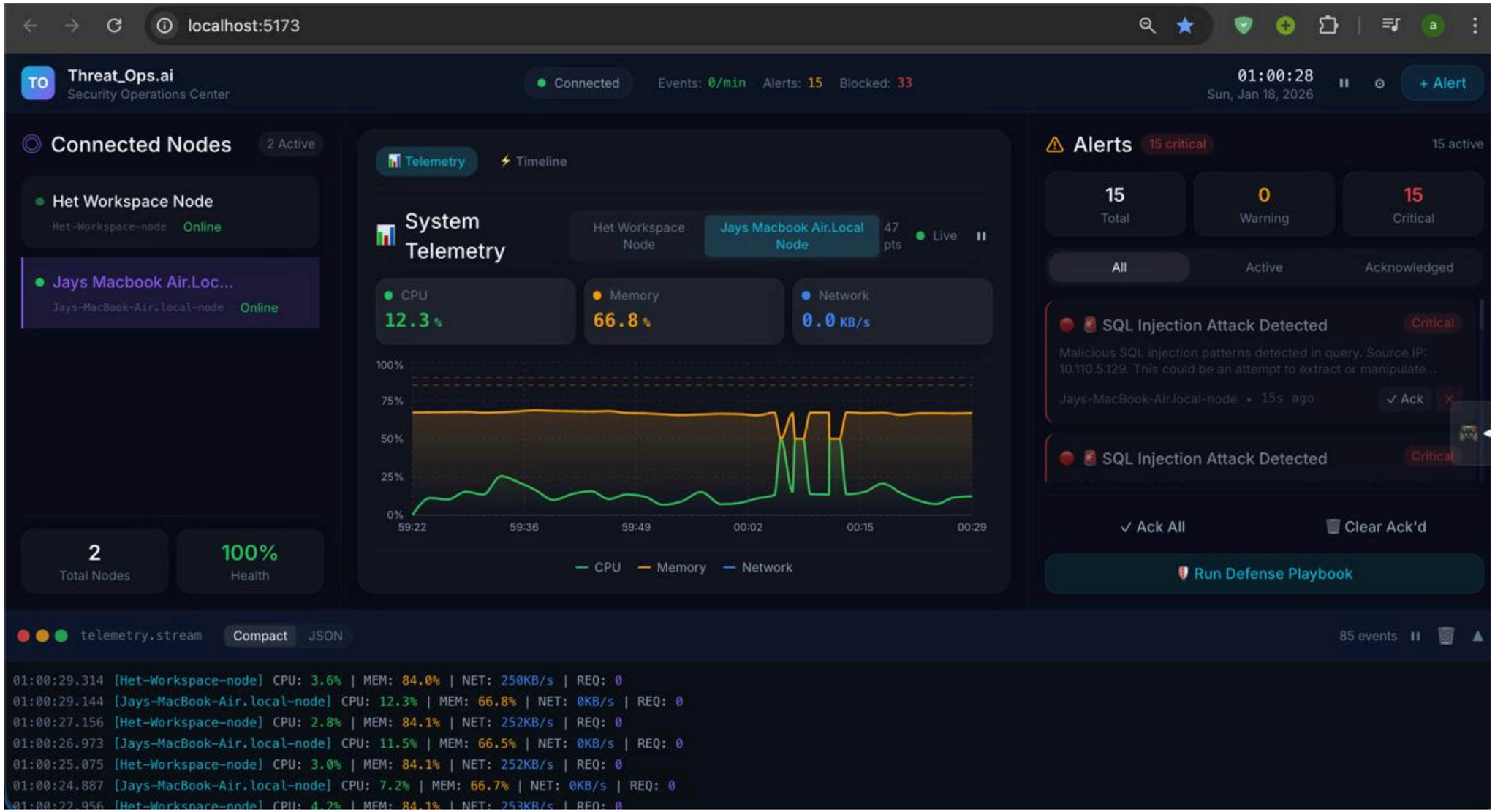
Snapshot of Node software

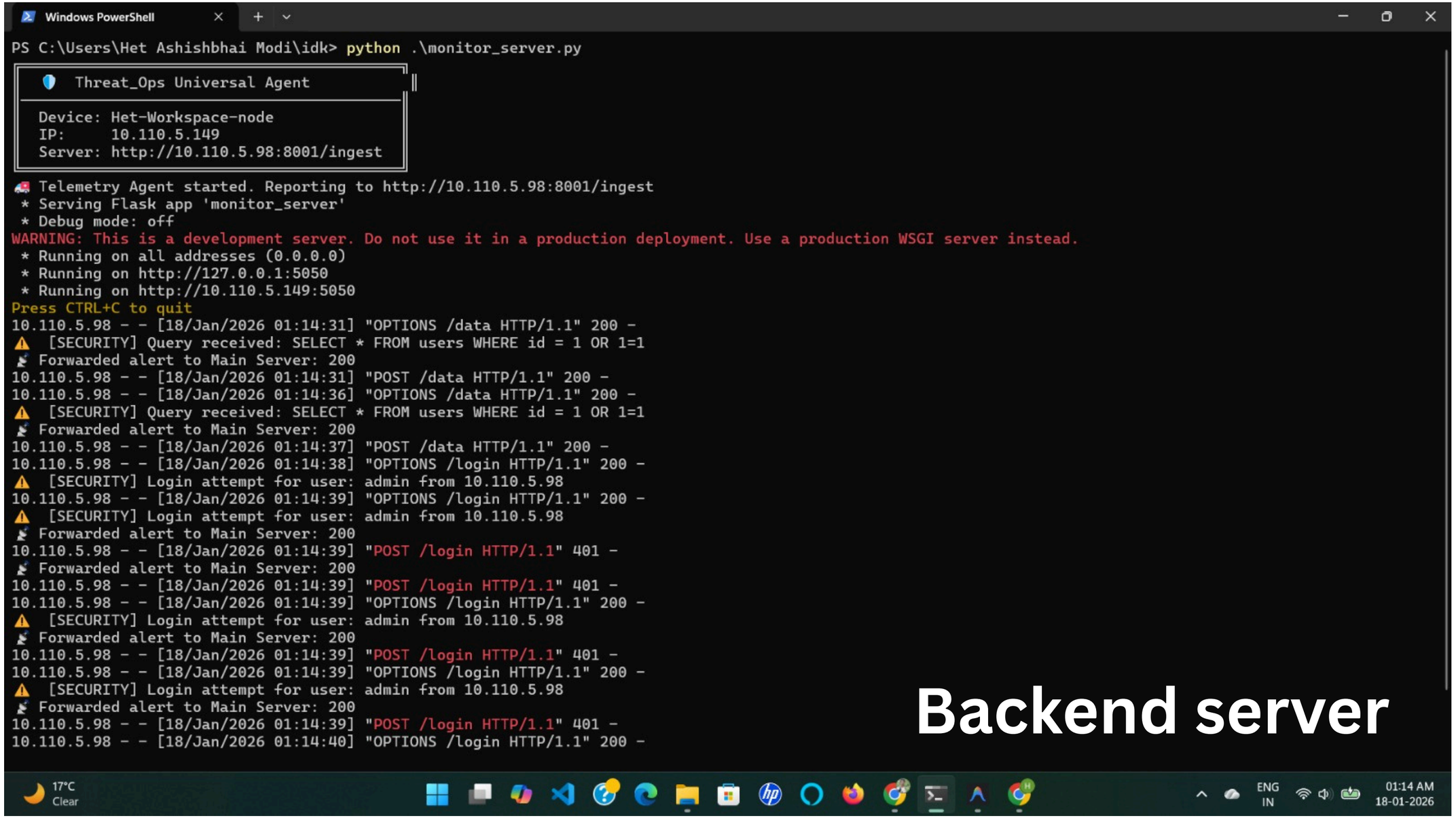
- **Agent** installed on protected machines - runs as a **background daemon**.
- Auto-discovers device identity and sends **real-time telemetry** to our dashboard.
- **Captures attacks** while monitoring **system health.**
- **Cross-platform support** - same agent works on **Windows, Mac, and Linux**
- Supports **headless** systems, using command line arguments.



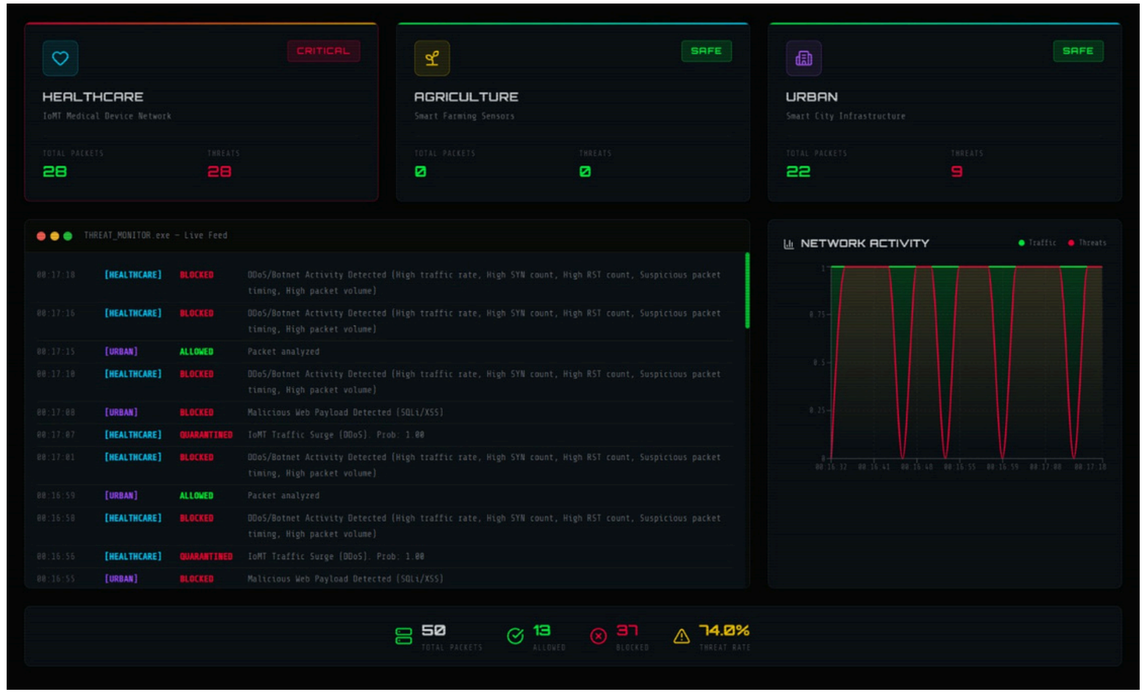


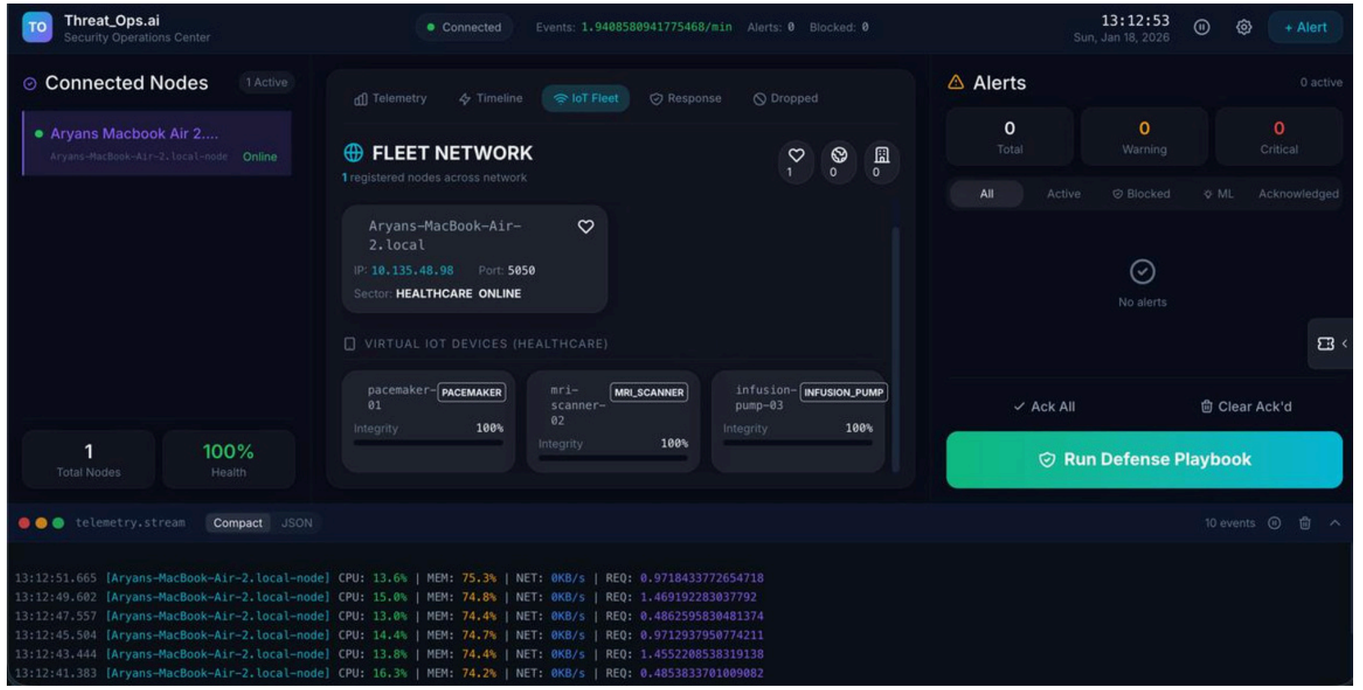
Snapshot of Monitoring dashboard

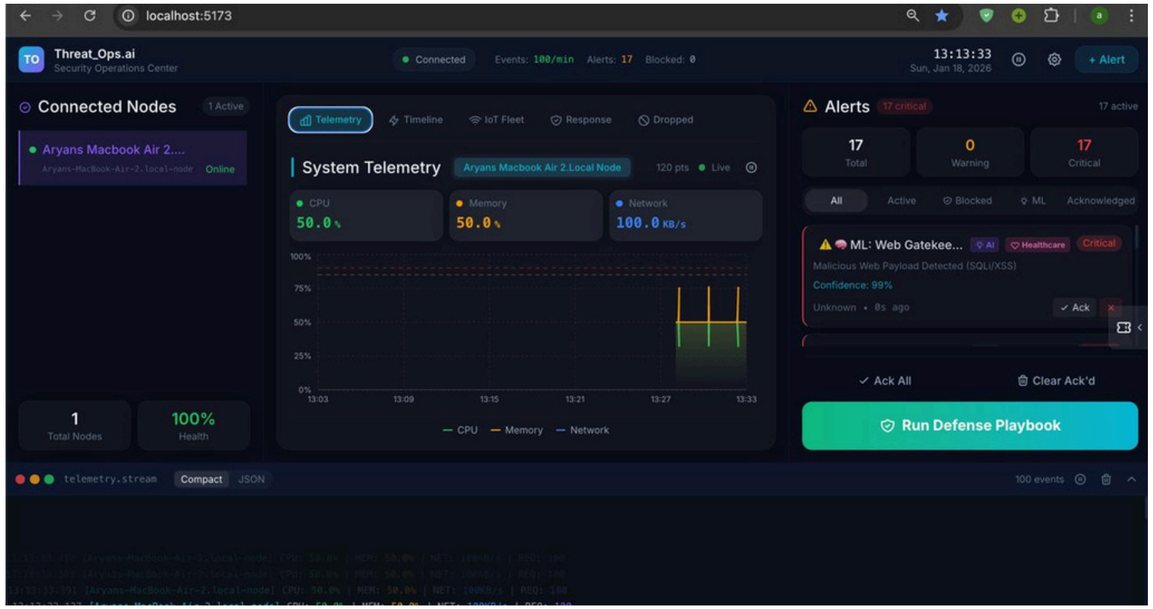


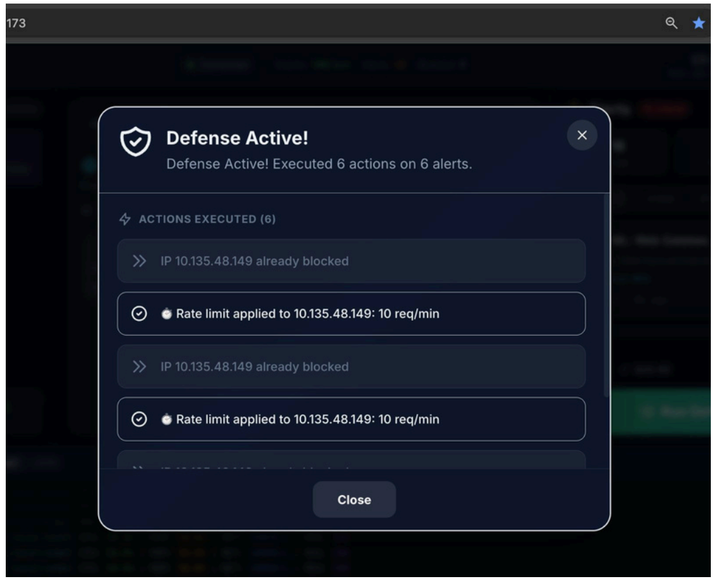


Backend server

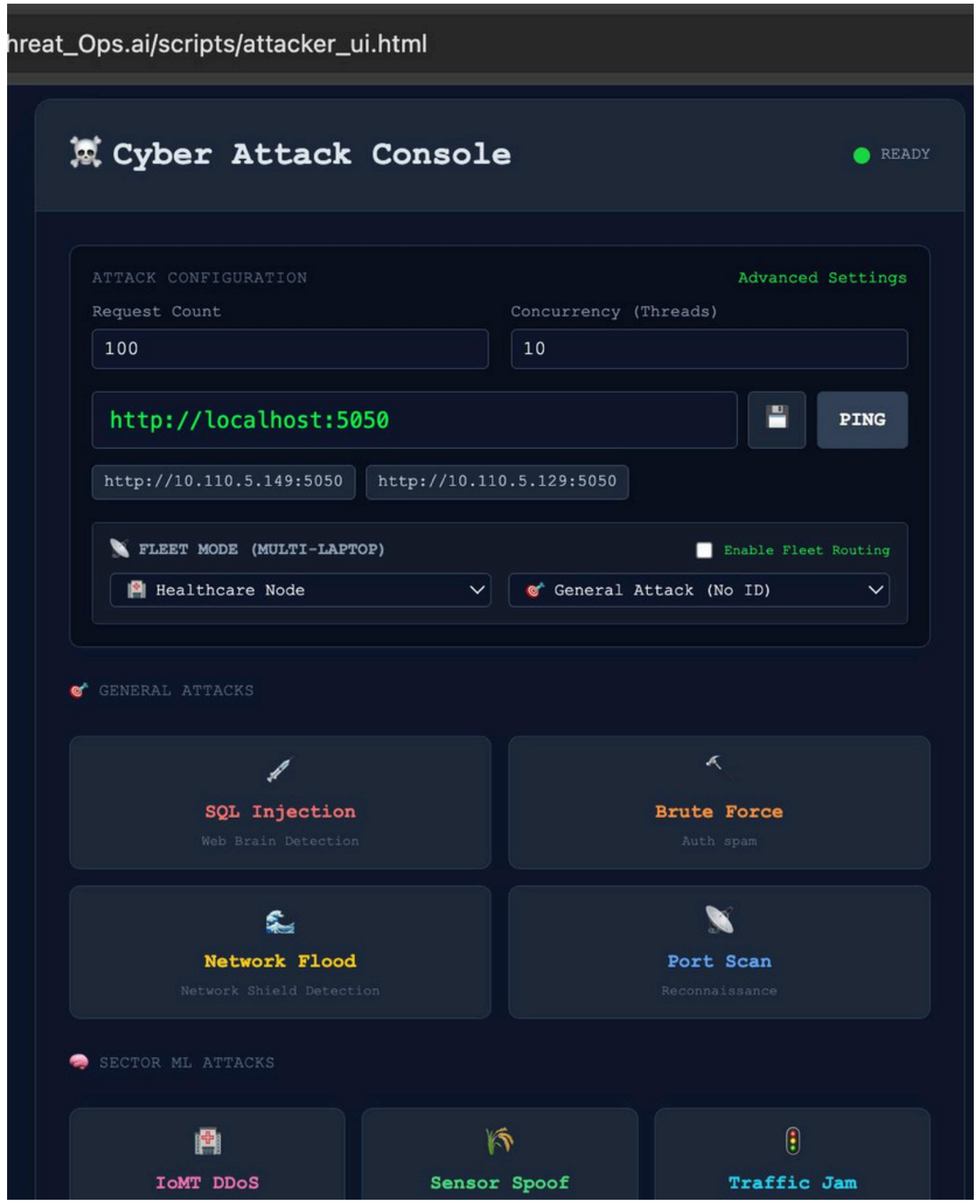

CRITICAL
HEALTHCARE
IoMT Medical Device Network
TOTAL PACKETS
28
THREATS
28
SAFE
AGRICULTURE
Smart Farming Sensors
TOTAL PACKETS
0
THREATS
0
SAFE
URBAN
Smart City Infrastructure
TOTAL PACKETS
22
THREATS
9
THREAT_MONITOR.exe — Live Feed
NETWORK ACTIVITY
Traffic
Threats
50
TOTAL PACKETS
13
ALLOWED
37
BLOCKED
74.0%
THREAT RATE

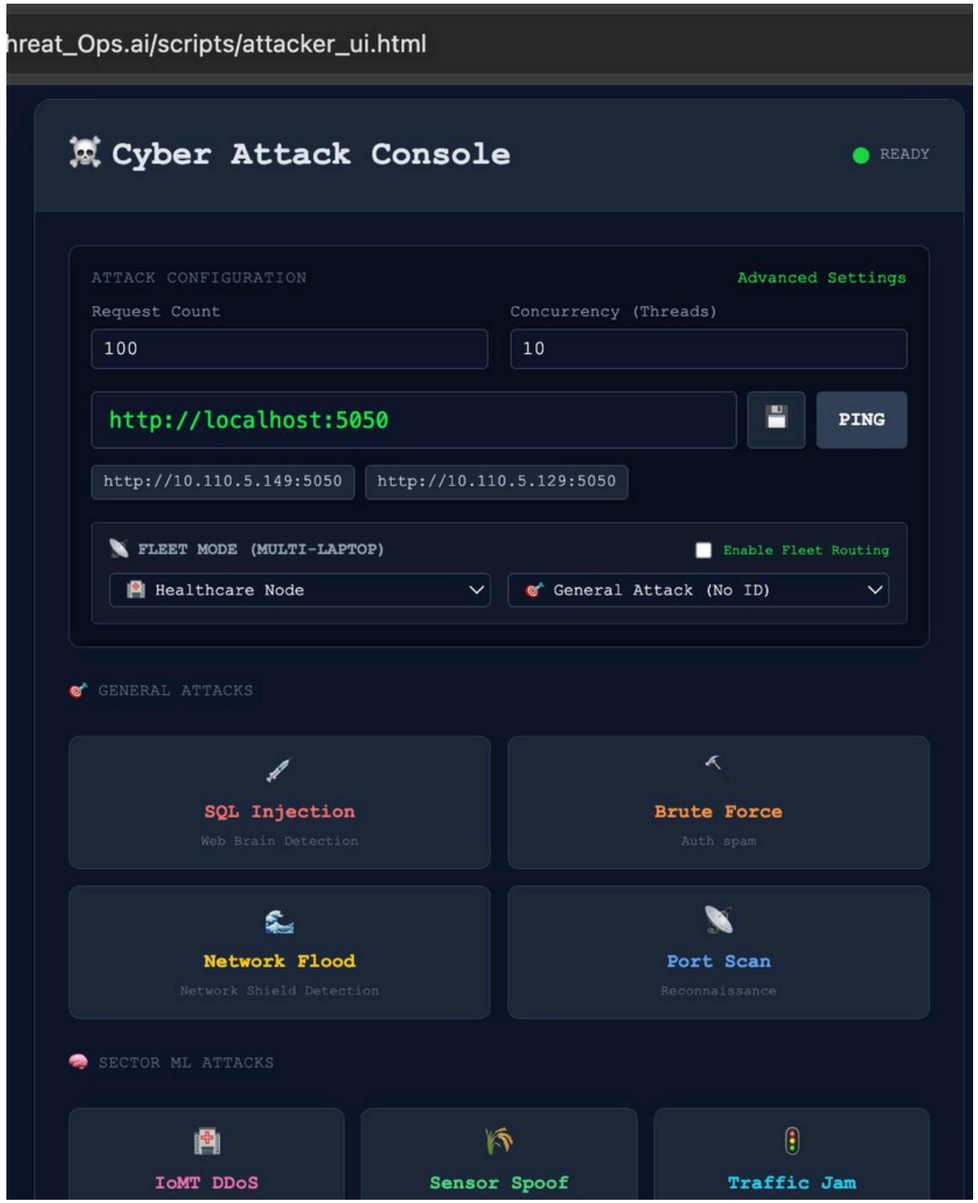

Threat_Ops.ai
Security Operations Center
Connected
Events: 1.9408580941775468/min
Alerts: 0
Blocked: 0
13:12:53
Sun, Jan 18, 2026
+ Alert
Connected Nodes
1 Active
Aryans Macbook Air 2....
Aryans-MacBook-Air-2.local-node
Online
Telemetry
Timeline
IoT Fleet
Response
Dropped
FLEET NETWORK
1 registered nodes across network
Aryans-MacBook-Air-2.local
IP: 10.135.48.98
Port: 5050
Sector: HEALTHCARE ONLINE
VIRTUAL IOT DEVICES (HEALTHCARE)
pacemaker-01
PACEMAKER
Integrity 100%
mri-scanner-02
MRI_SCANNER
Integrity 100%
infusion-pump-03
INFUSION_PUMP
Integrity 100%
Alerts
0 active
0
Total
0
Warning
0
Critical
All
Active
Blocked
ML
Acknowledged
No alerts
Ack All
Clear Ack'd
Run Defense Playbook
1
Total Nodes
100%
Health
telemetry.stream
Compact
JSON
10 events
13:12:51.665 [Aryans-MacBook-Air-2.local-node] CPU: 13.6% | MEM: 75.3% | NET: 0KB/s | REQ: 0.9718433772654718
13:12:49.602 [Aryans-MacBook-Air-2.local-node] CPU: 15.0% | MEM: 74.8% | NET: 0KB/s | REQ: 1.469192283037792
13:12:47.557 [Aryans-MacBook-Air-2.local-node] CPU: 13.0% | MEM: 74.4% | NET: 0KB/s | REQ: 0.4862595830481374
13:12:45.504 [Aryans-MacBook-Air-2.local-node] CPU: 14.4% | MEM: 74.7% | NET: 0KB/s | REQ: 0.9712937950774211
13:12:43.444 [Aryans-MacBook-Air-2.local-node] CPU: 13.8% | MEM: 74.4% | NET: 0KB/s | REQ: 1.4552208538319138
13:12:41.383 [Aryans-MacBook-Air-2.local-node] CPU: 16.3% | MEM: 74.2% | NET: 0KB/s | REQ: 0.4853833701009082

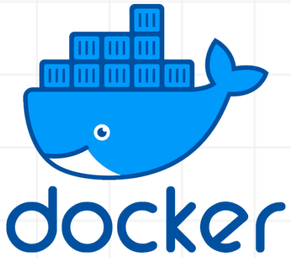

localhost:5173
Threat_Ops.ai
Security Operations Center
Connected
Events: 100/min
Alerts: 17
Blocked: 0
13:13:33
Sun, Jan 18, 2026
+ Alert
Connected Nodes
1 Active
Aryans Macbook Air 2....
Aryans-MacBook-Air-2.local-node
Online
Telemetry
Timeline
IoT Fleet
Response
Dropped
System Telemetry
Aryans Macbook Air 2.Local Node
120 pts
Live
CPU
50.0%
Memory
50.0%
Network
100.0 KB/s
100%
75%
50%
25%
0%
13:03
13:09
13:15
13:21
13:27
13:33
CPU
Memory
Network
Alerts
17 critical
17 active
17
Total
0
Warning
17
Critical
All
Active
Blocked
ML
Acknowledged
ML: Web Gatekee...
AI
Healthcare
Critical
Malicious Web Payload Detected (SQLi/XSS)
Confidence: 99%
Unknown • 0s ago
Ack
Ack All
Clear Ack'd
Run Defense Playbook
1
Total Nodes
100%
Health
telemetry.stream
Compact
JSON
100 events


173
Defense Active!
Defense Active! Executed 6 actions on 6 alerts.
ACTIONS EXECUTED (6)
IP 10.135.48.149 already blocked
Rate limit applied to 10.135.48.149: 10 req/min
IP 10.135.48.149 already blocked
Rate limit applied to 10.135.48.149: 10 req/min
Close

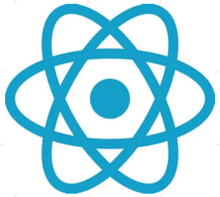
ATTACK SIMULATION

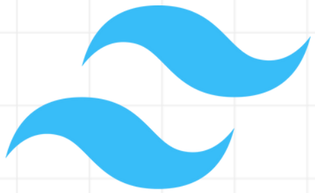






TECHNOLOGIES USED





RESOURCES

DATASET LINKS :

- HTTPS://WWW.KAGGLE.COM/DATASETS/PETERFRIEDRICH1/CICDARKNET2020-INTERNET-TRAFFIC
- HTTPS://DATA.MENDELEY.COM/DATASETS/2BW34GHT8B/2
- HTTPS://WWW.KAGGLE.COM/DATASETS/WISAM1985/IOT-AGRICULTURE-2024
- HTTPS://WWW.KAGGLE.COM/DATASETS/HIMADRI07/CICIOT2023/DATA
- HTTPS://WWW.KAGGLE.COM/DATASETS/EVG3N1J/HTTPPARAMSDATASE