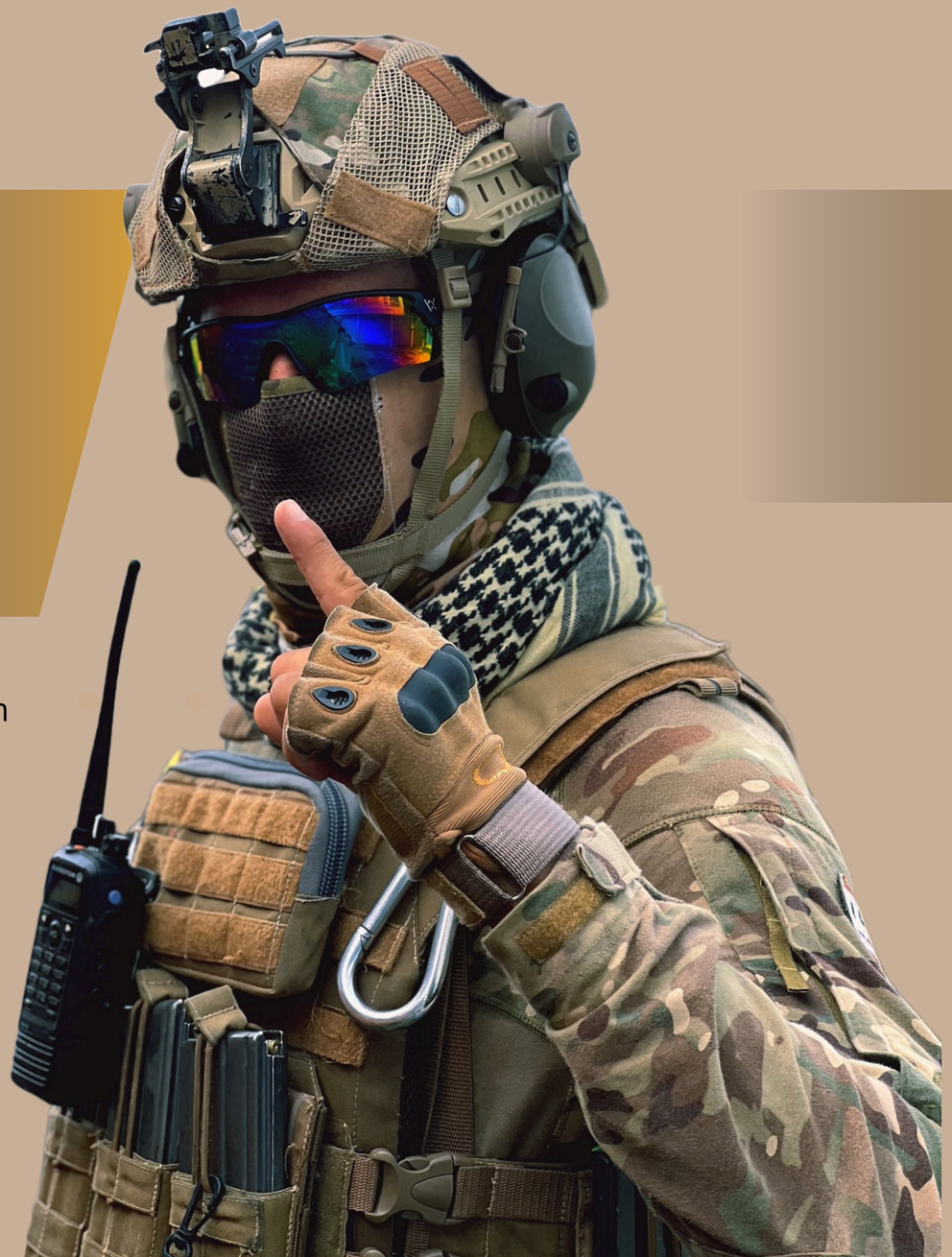
INDIAN ARMY TERRIER
CYBER QUEST 2025

QUANTUM-ENHANCED CYBER THREAT SHIELD FOR NATIONAL DEFENSE

AI + Quantum Intelligence for early ransomware detection



Team Name: CyberHawk

Mission Need (Problem)

- Defense networks face **AI-assisted ransomware**
- Early stage detection is critical (pre-encryption)
- Classical tools struggle with scale & evasive patterns
- Need: Faster, smarter, proactive threat intel

Notes: Stress “left-of-boom” detection—catch behaviors before payload detonates.

Threat Model & Data

💻 *Host Signals*

- Process trees & execution flow
- Registry modifications
- File operations
- API call anomalies

🌐 *Network Signals*

- DNS queries & TLS metadata
- Lateral movement patterns
- C2 (Command & Control) footprints
- Suspicious traffic anomalies

Dataset Strategy

- Public threat intelligence logs
- Benign vs. staged ransomware behaviors
- Synthetic augmentation for zero-day attacks

Proposed Solution - AI-Powered Ransomware Defense

Core Pipeline

- **Data Ingestion** → Collect host + network logs in real time
- **Feature Extraction** → Convert behavior signals into vectors
- **AI Models**
  - LSTM / Autoencoder → Detect anomalies
  - Isolation Forest / One-Class SVM → Flag rare behaviors
- **Decision Engine** → Risk scoring & classification
- **Response Layer** → Alert SOC / auto-contain ransomware

AI-Driven Ransomware Defense Architecture

Host Logs

- Process Trees
- File Ops
- Registry Edits

Network Logs

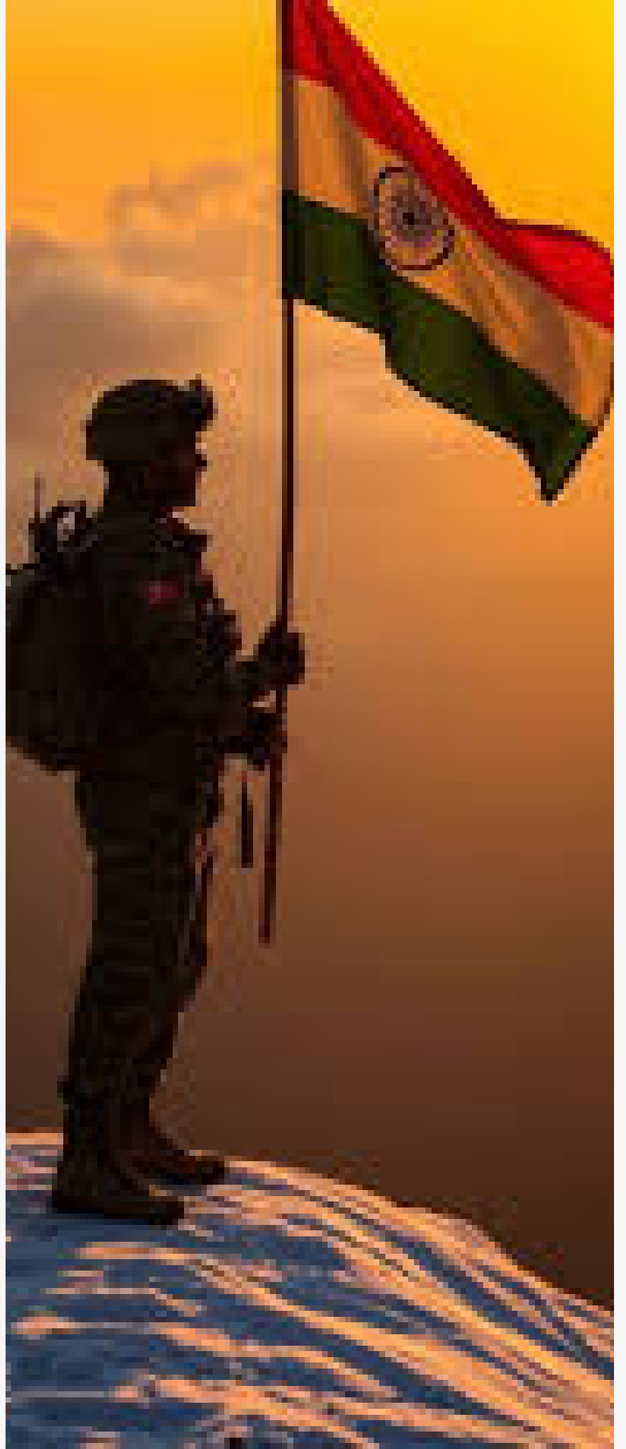
- DNS
- TLS Metadata
- Lateral Movement

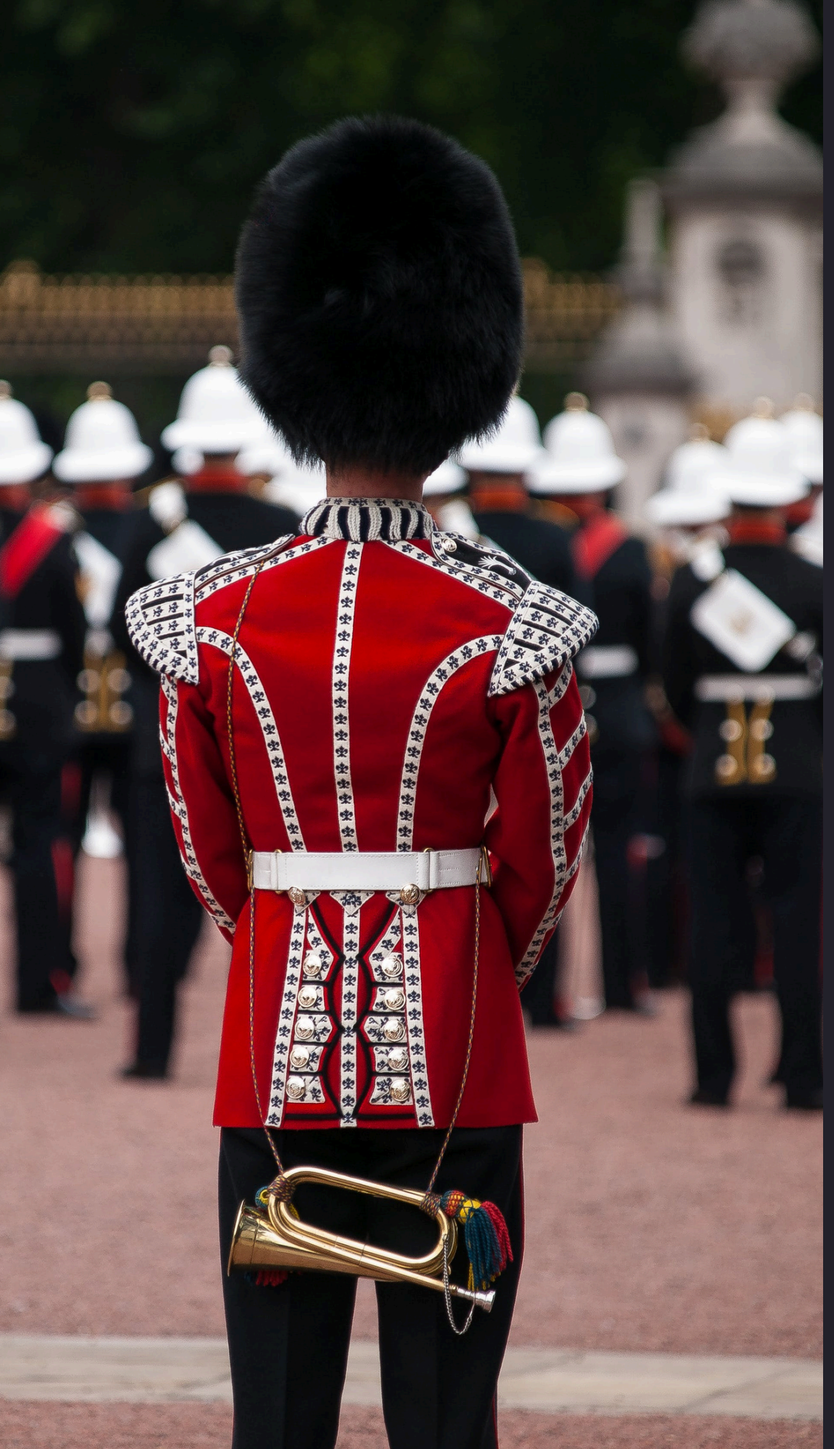
AI Engine

- LSTM, Autoencoders
- Isolation Forest
- One-Class SVM

Defense Layer

- SOC Alerts
- Auto-Contain





Key Innovations

- **AI-powered Detection Beyond Signatures** → Detects unseen ransomware using behavior learning, not just signature matching.
- **Quantum ML Edge** → Leverages Qiskit/PennyLane to handle complex attack patterns.
- **Synthetic Data Augmentation** → Covers rare, zero-day like scenarios.
- **Lightweight Deployment** → Cloud-ready & compatible with defense IoT networks.
- **Proactive Defense** → Automatic isolation & alerting to minimize damage.

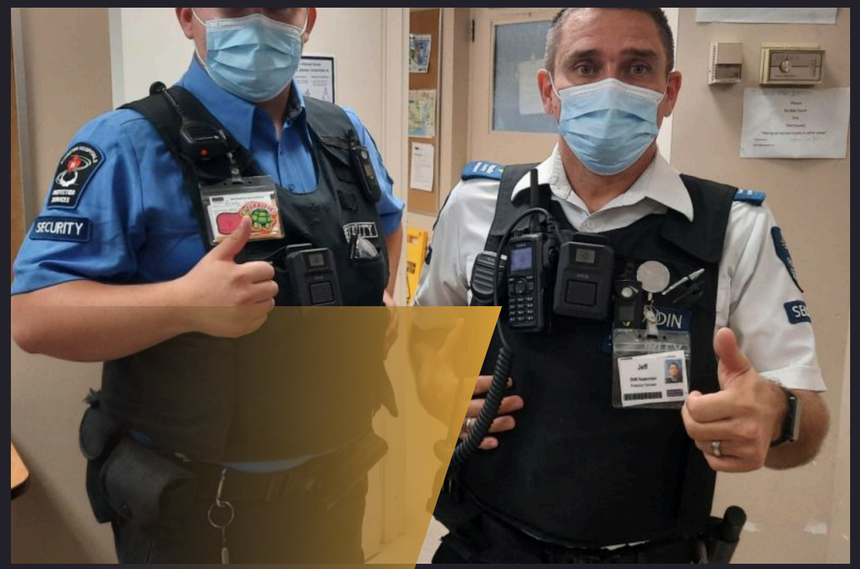
Prototype Plan (36-Hour Finale)

- 0–6h → Data prep + Baseline LSTM
- 6–14h → Autoencoder + Anomaly Scoring
- 14–22h → QML Classifier + Feature Embedding
- 22–28h → Score Fusion, Thresholds, Alerts
- 28–36h → Streamlit Dashboard + Demo Script

Evaluation & Success Criteria

- TPR @ Low FPR → Detect without flooding alerts
- Precision → Minimal false alarms
- Detection Latency → Alert before encryption (sub-second)
- Robustness → Stress-tested under obfuscation, mimicry, noise

Defense Impact & Integrations

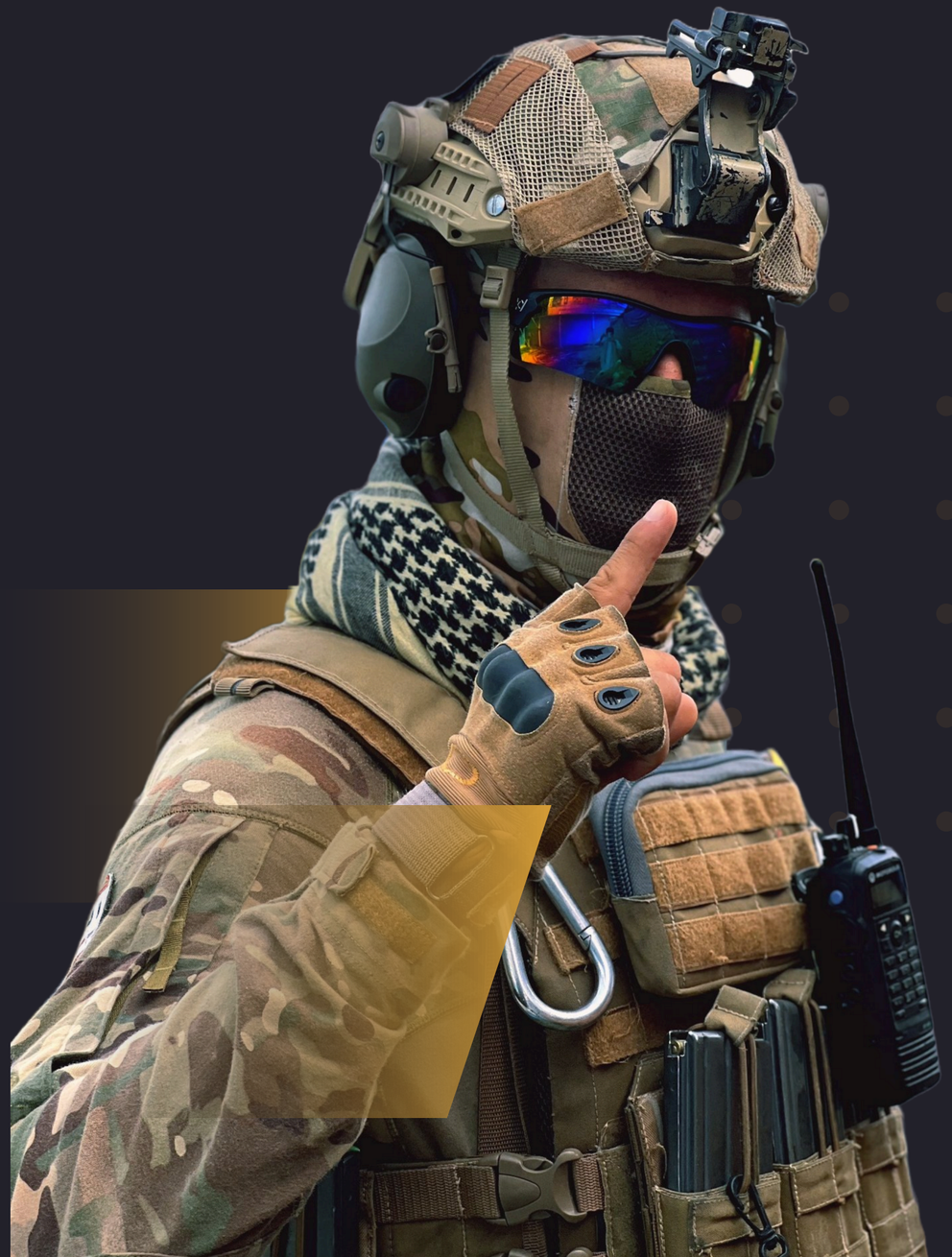


01 Proactive SOC: stop spread before blast radius

02 Scalable: edge agent + central brain

03 Interoperable: SIEM/SOAR hooks (isolate host, revoke creds)

04 Roadmap: post-quantum crypto logs; cross-domain (smart grids, comms)



Thank You

Jai Hind