ThreatPulse

Predictive OSINT & Early-Warning Cyber Radar

Paltmann Capital OÜ — Tartu, Estonia — paltmann.capital@gmail.com

Executive Summary

ThreatPulse is a dual-use Open Source Intelligence (OSINT) engine that monitors decentralized adversary communications. By bridging the gap between raw underground chatter and structured intelligence, ThreatPulse provides corporate and state-aligned security teams with actionable, machine-readable alerts hours before threats are indexed by traditional global vulnerability databases.

The Problem: The Broken State of Defense

Modern cyber threats move faster than traditional threat intelligence can track. Adversaries and hacktivists automate their offensive capabilities across encrypted and highly fragmented communication nodes. Consequently, Security Operations Centers (SOCs) suffer from profound alert fatigue, lacking the resources to manually monitor, translate, and filter unstructured deep-web noise. Defense must automate its intelligence.

The Doctrine: Mathematical OPSEC

ThreatPulse operates on a philosophy of Mathematical OPSEC. Rather than utilizing expensive, always-listening keyword scanners, our proprietary engine treats adversary chatter as time-series data. We apply lightweight statistical process control to ignore baseline organic noise. The system triggers deep localized NLP (Natural Language Processing) classification strictly when mathematical volume anomalies occur, isolating the true signal.

Core Capabilities

- **Spike-Triggered Detection:** Utilizes predictive baseline modeling to flag statistically significant deviations in communication volumes, detecting zero-days, credential leaks, and botnet formations before exploitation.
- **Interoperable Ontology:** AI-driven contextualization strictly categorizes raw adversarial intercepts into standardized frameworks (e.g., MITRE ATT&CK), establishing a foundation structurally prepared for STIX/TAXII export.

- **Zero-Delay Push Architecture:** Circumvents the inefficiency of traditional "pull" API dashboards by delivering real-time, structured JSON payloads directly to corporate SIEM/SOAR infrastructure and internal communication grids (Slack/Discord).
- **CRA-Aligned Defenses:** Engineered with EU Cyber Resilience Act (CRA) principles, providing highly structured data outputs designed to support "Expert-in-the-Loop" firewall remediation to mitigate autonomous hallucinations.

Strategic Value & ROI

Designed for CISOs, MSSPs, and defense contractors, ThreatPulse shifts cybersecurity from a reactive posture to predictive readiness. By combining standard deviation modeling with localized Large Language Models, ThreatPulse reduces the Mean Time To Detect (MTTD) for emerging vulnerabilities with an extremely lightweight computational footprint.