Veraptos — Autonomous Security Response & Incident Automation for Modern Web3

Why Veraptos?

Veraptos is an operational, agentic security automation platform I built from scratch—engineered for hybrid enterprise, blockchain/Web3, and DeFi environments where incident response speed and automation are critical.
It's designed to **accelerate the full IR lifecycle**: detection, triage, coordination, and post-incident improvement—across cloud, on-prem, and decentralized stacks.

Key Capabilities & Chainlink Alignment

- **End-to-End Incident Response Automation**
  - Runbook-driven response—automates high-severity incident lifecycle (detection, scoping, containment, recovery, post-mortem).
  - On-call readiness: ingest, escalate, and coordinate cross-team and cross-stack incidents, integrating with both on-chain and off-chain data.
- **Detection Engineering & Enrichment**
  - Sigma-inspired detection modules—custom logic for alerting on real blockchain and DeFi threats, endpoint, cloud, and protocol anomalies.
  - Integrates with leading SIEM, cloud telemetry, and API sources; parses and enriches data in real time (Python, Go).
  - Built-in threat intelligence and enrichment pipelines to reduce false positives and deliver high-signal alerts.
- **Security Automation & IR Tooling**
  - Modular response playbooks: automate common containment and remediation actions across endpoints, cloud, and Web3 infrastructure.
  - Automated enrichment (Jupyter, Lambda functions, etc.) for rapid scoping and decision-making.
  - Tabletop simulation and response exercises for continuous improvement.
- **Red Team Simulation & Threat Modeling**
  - Emulates attacker TTPs (Web2 + Web3)—from phishing to smart contract abuse—testing both controls and detection resilience.
  - MITRE ATT&CK and OWASP mapping for business-focused reporting.
- **Built for Remote-First, Global Teams**
  - Production-tested for distributed, async teams—incident handoff, stakeholder comms, and runbook clarity are first-class features.

Direct Technology Alignment

- **Programming & Automation:** Python (core), Go (pipelines), Bash; ready to extend to Rust for advanced use cases.
- **Detection as Code:** Sigma-style rules; rapid authoring and tuning for new threat signals.

- **Orchestration:** LangGraph for multi-agent workflow, Playwright for browser-based testing, Docker for reproducibility and isolated testing environments.
- **Cloud & Web3:** Native support for AWS, GCP, Lambda, and Chainlink-compatible Web3 telemetry.
- **DevOps and CI/CD:** Automated deployment and integration with common SaaS (Slack, Jupyter, GitHub Actions).

Operational Value for Chainlink Labs

- **Incident Command Ready:**
  Veraptos automates the IR lifecycle, serving as both the "incident commander's" toolkit and the backbone for repeatable response across blockchain and DeFi ecosystems.
- **Detection + Response in One Pipeline:**
  Reduce time-to-detect and time-to-contain by combining high-signal detection with automated enrichment and runbook-driven actions.
- **Continuous Improvement:**
  Every incident is a learning cycle—Veraptos feeds post-mortem findings directly into updated detection and response logic, closing the feedback loop.

Example Use Cases

- **Major DeFi Incident:**
  Veraptos triages and escalates cross-protocol anomalies, launches automated containment, coordinates with relevant Chainlink and protocol teams, and auto-generates a post-mortem with actionable improvements.
- **Detection Pipeline Modernization:**
  Instantly deploy new Sigma-style detection rules for emerging Web3 threats (oracle manipulation, flash loan attacks), with automated test and tuning cycles.
- **Remote Incident Handover:**
  Secure, auditable handoff of ongoing incidents across timezones, ensuring global coverage and no loss of context.

Veraptos IR Automation Workflow

- **Phase 1:** Automated discovery & strategy, integrating with external threat feeds and on-chain data.
- **Phase 2:** Multi-agent execution—autonomous credentialed scans, protocol analysis, and agentic remediation actions.
- **Phase 3:** Reporting & handoff—findings stored, alerts sent, and post-incident improvement captured.

Veraptos is not a research project—it's a hands-on, productionized system for modern incident response in complex, hybrid, and blockchain-centric environments.