Securing Critical Infrastructure in the Age of State-Sponsored Attacks

Empowering Autonomous Cyber Defense with TruContext Agentic AI

Date: September 5, 2025

Critical infrastructure—power grids, water systems, transportation networks, and financial institutions—has become a prime target for state-sponsored cyberattacks. These attacks are no longer theoretical: recent FBI warnings about Russian cyber actors targeting U.S. infrastructure underscore the urgency of the threat.

In this high-stakes environment, **traditional perimeter defenses and manual monitoring are no longer sufficient**. What's needed is an intelligent, autonomous system that can detect, reason, and act—*before* adversaries succeed. That's where Visium's TruContext platform delivers a decisive advantage.

The Challenge: Legacy Systems, Sophisticated Threats

Critical infrastructure environments are notoriously complex—often blending modern IT with decades-old operational technology (OT). This hybrid landscape is difficult to secure, and the consequences of a breach are severe: power outages, transportation paralysis, and national security risks.

State-sponsored actors like APT33 and APT39 exploit these vulnerabilities with precision. Their attacks are persistent, well-funded, and tailored to bypass conventional defenses.

The Solution: TruContext Agentic AI

TruContext is more than a visibility platform—it's an *agentic Artificial Intelligence ("AI") system* that autonomously defends critical infrastructure. By combining graph analytics with intelligent agents, TruContext continuously maps, monitors, and mitigates cyber risk across complex environments.

Key capabilities include:

- **Autonomous Threat Detection:** TruContext agents monitor ICS/SCADA environments in real time, detecting anomalies like unauthorized PLC commands or sensor drift—often the first signs of compromise.
- **Contextual Reasoning:** AI agents evaluate threats in context—factoring in asset criticality, historical behavior, and threat intelligence to prioritize response.
- **Proactive Mitigation:** TruContext can simulate attack paths, identify lateral movement potential, and recommend or initiate containment actions autonomously.

This is not just situational awareness—it's *situational intelligence that acts*.

Case Study: 2025 Judiciary Case Management System Attack

The recent breach of the federal Judiciary's case management system illustrates the stakes. A sophisticated, state-sponsored intrusion compromised sensitive legal data and disrupted operations. Had TruContext been deployed, its agents could have:

- Detected anomalous access patterns in real time
- Mapped the attacker's lateral movement across systems
- Triggered automated alerts and containment protocols

This is the power of agentic AI: *speed, precision, and autonomy*.

Public-Private Collaboration: A Shared Defense

Securing critical infrastructure requires a unified front. TruContext supports secure, role-based data sharing between government agencies and private operators—enabling coordinated incident response and shared threat intelligence.

By serving as a common platform for cyber situational awareness, TruContext fosters a culture of *collective resilience*.

Conclusion: From Reactive Defense to Autonomous Resilience

The threat to critical infrastructure is growing—and evolving. To stay ahead, organizations must move beyond reactive defense and embrace *autonomous, intelligent protection*.

Visium's TruContext platform delivers agentic AI that doesn't just observe—it defends. It empowers critical infrastructure operators to detect, reason, and respond to threats in real time—building a more secure, resilient future for our most vital systems.