U2opia™

Advanced Cybersecurity with SITU-X:

Real-Time Entity Level Intelligence on Zero-Trust Architecture

January 16, 2025

From groundbreaking research to leading-edge cybersecurity solutions

SITU-X represents a strategic alliance between cutting-edge research and enterprise innovation. This unique platform combines **SITU's** advanced anomaly detection and cybersecurity research from **Oak Ridge National Laboratory (ORNL)** with the enterprise-grade distributed AI infrastructure of **Xenese™**, delivering the next-generation cybersecurity intelligence.

Research-driven innovation

- Developed at ORNL with funding from DOE, DoD, and DHS to safeguard mission-critical systems.
- Built through multidisciplinary research in data science, AI, and national security sciences.

A collaborative consortium

- U2opia acquired SITU from ORNL and integrated it with Xenese™, forming a consortium to merge advanced AI/ML, entity-level intelligence, and zero-latency solutions on distributed node technology.

Real-time threat intelligence

- SITU-X delivers adaptive, real-time cybersecurity solutions, and enhances existing investments by complementing platforms like BeyondTrust and Splunk.

Our advanced capabilities deliver real-time cyber intelligence and resilient security solutions

Intelligent Threat Detection

- **Entity-Level Models:** Millions of supervised and unsupervised probabilistic models for advanced anomaly detection.
- **Distributed Analytics:** Detects and mitigates threats instantly across hybrid and distributed environments.

Contextual Insights at Scale

- **Probabilistic Scoring:** Prioritizes threats with advanced anomaly scoring using sliding time windows.
- **Contextual Analysis:** Tracks behavior patterns to uncover low-and-slow attacks and complex threats.

Resilient Security and Compliance

- **Zero-Trust Architecture:** Ensures secure, immutable infrastructure.
- **GenAI-Powered Actions**: Delivers prescriptive analytics and automated recommendations for faster response.

Distributed Hybrid Integration

- **Scalable Infrastructure:** Processes massive data volumes across edge, on-premises, and cloud.
- **API and Privilege Monitoring**: Real-time detection of misuse and vulnerabilities in privileged access.

Navigating the DoD's evolving cyber threat landscape: Key challenges in Defense

Top Cyber Threat Challenges

1. **Detecting Advanced Persistent Threats (APTs):** Stealthy nation-state attacks blend into normal traffic, evading traditional systems.

2. **Managing Overwhelming Data Volumes:** Petabytes of daily data overwhelm analysts with false positives.

3. **Preventing API & Privileged Access Exploits:** API misuse and credential theft lead to undetected breaches.

4. **Ensuring Resilience in Distributed Environments:** Hybrid and edge environments create visibility gaps and latency issues.

Cyberattack Rates and Volumes

1. **Incident Reporting Trends (2017-2022):** Reports **surged** from 780/month in 2020 to 1,240/month in 2021, normalizing to **602/month in 2022**.

2. **Federal Cybersecurity Incidents (2022):** **800,944** cyber-crimes reported, with financial losses rising **50% to $10.3 billion.**

3. **Defense Sector Trends:** **300%** increase in cyberattacks since 2018, with an average breach cost of $5.46M.

References: 2023 DoD Cyber Strategy Summary, DoD Cyber Crime Center (DC3) Annual Report.

Responding to DoD Cybersecurity challenges with SITU-X advanced capabilities (1)

1 Detecting Advanced Persistent Threats (APTs)

Problem Solved: SITU-X uncovers APT behaviors that blend into normal traffic, enabling real-time defense.

- **Entity-Level ML Models:** Tracks user, device, and API behaviors to uncover subtle deviations.
- **Probabilistic Anomaly Scoring:** Prioritizes complex behaviors with likelihood scores.

2 Managing Overwhelming Data Volumes

Problem Solved: SITU-X reduces analyst overwhelm by filtering petabytes of daily data, eliminating false positives, and highlighting critical threats for faster response.

- **Automated Anomaly Detection:** Filters false positives with millions of autonomous models.
- **Petabyte-Scale Processing:** Ingests and analyzes vast streaming data in real-time.

Responding to DoD Cybersecurity challenges with SITU-X advanced capabilities (2)

3 Preventing API & Privileged Access Exploits

Problem Solved: SITU-X uncovers APT behaviors that blend into normal traffic, enabling real-time defense.

- **API Behavior Monitoring:** Detects unusual patterns, privilege escalation, and geo-locations
- **Prescriptive GenAI Insights:** Recommends remediation actions like revoking keys or blocking access.

4 Achieving Resilience Across Distributed & Hybrid Environments

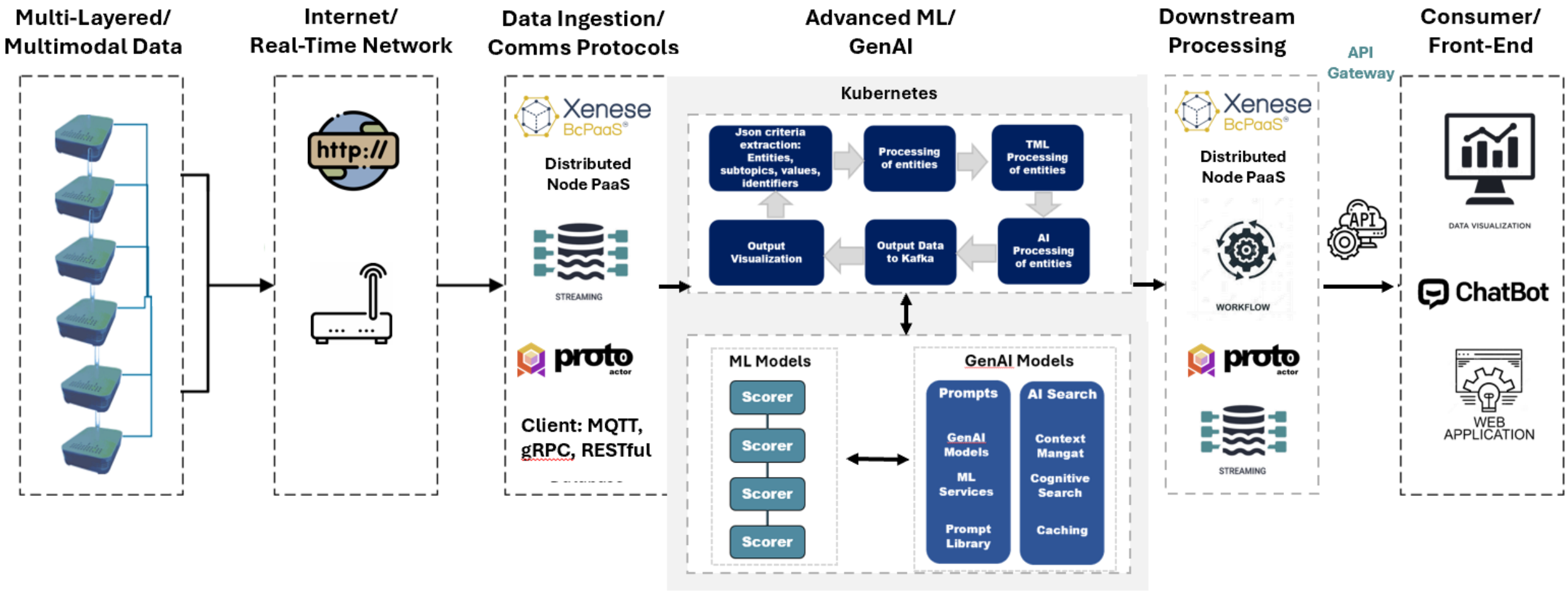
Problem Solved: SITU-X ensures resilience by closing gaps and reducing latency with distributed AI and real-time edge processing.

- **Distributed AI Infrastructure:** Processes data at the edge for low-latency insights
- **Zero Trust Architecture:** Secures systems with real-time, continuous verification.

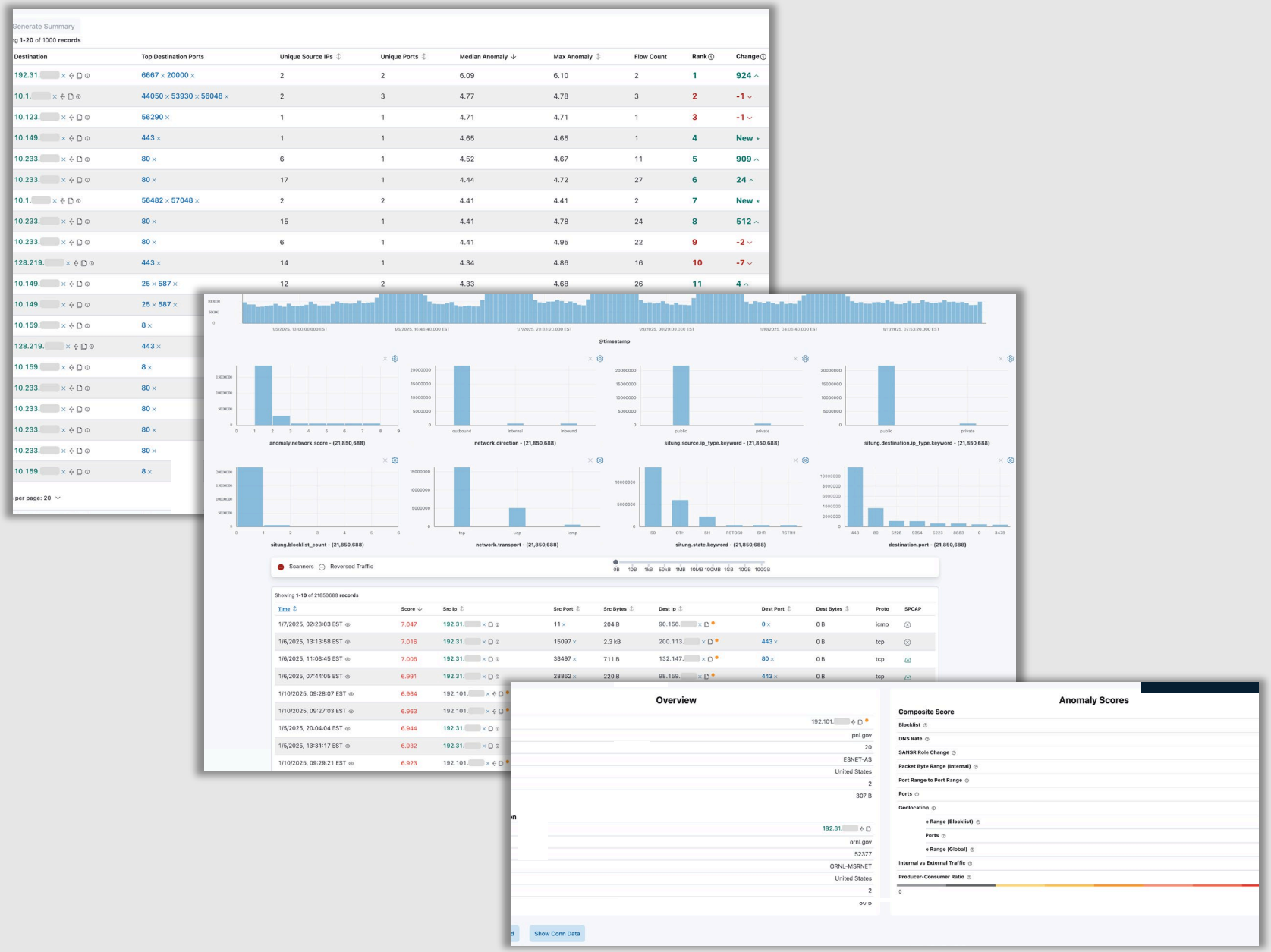
We built differentiation from the start with the latest advances in Fast ML and Actor Models

Capabilities	SITU-X	BeyondTrust	Splunk	CrowdStrike	Palo Alto Networks	Google Mandiant
1. **Entity-level Autonomous, in-memory, ML models** for real-time threat detection at scale	✓	X	X	X	X	X
2. **Petabyte-scale** data ingestion with Distributed AI	✓	X	✓	X	✓	✓
3. **GenAI-powered prescriptive analytics** for real-time threat remediation	✓	X	X	X	X	X
4. **Entity-level autonomous, in-memory, AI prompts** for real-time threat analysis	✓	X	X	X	X	X
5. **Actor model scale framework on Node technology** (immutable cryptography)	✓	X	X	X	X	X
6. **Distributed edge processing** with zero latency	✓	X	X	✓	✓	✓
7. **Integrated API behavior monitoring** and privilege escalation detection	✓	✓	X	X	X	✓
8. **Cross-platform integration** and visibility (on-prem, cloud, hybrid)	✓	✓	✓	✓	✓	✓
9. **Dynamic scaling**, **resilient processing, and fine-grained parallelism** through actor models	✓	X	◐	X	◐	◐

Transactional ML, GenAI, and real-time streaming define the uniqueness of our architecture



SITU-X DEMO


Generate Summary
Destination
Top Destination Ports
Unique Source IPs
Unique Ports
Median Anomaly
Max Anomaly
Flow Count
Rank
Change
@timestamp
anomaly.network.score - (21,850,688)
network.direction - (21,850,688)
situng.source.ip_type.keyword - (21,850,688)
situng.destination.ip_type.keyword - (21,850,688)
situng.blocklist_count - (21,850,688)
network.transport - (21,850,688)
situng.state.keyword - (21,850,688)
destination.port - (21,850,688)
Scanners
Reversed Traffic
Overview
Anomaly Scores
Composite Score
Show Conn Data

Achieving Enhanced Business Outcomes with SITU-X's Advanced Cyber Defense Capabilities

- **Reduce Detection Time:** Advanced AI/ML-driven platforms can reduce threat detection and response time by **up to 96%** (Ponemon Institute, 2023).

  SITU-X Impact: Real-time streaming intelligence identifies threats faster, minimizing potential dwell time and damage.

- **Lower False Positives:** AI-enhanced cybersecurity solutions **reduce false positives by 70-90%**, improving operational efficiency (Gartner, 2024).

  SITU-X Impact: Tailored entity-level models filter noise, allowing analysts to focus on real threats.

- **Improve Analyst Productivity:** Automation and advanced analytics **increase security team productivity by 40%**, enabling teams to handle more incidents effectively (Deloitte Cyber Risk Report, 2022).

  SITU-X Impact: Automated anomaly detection and prescriptive insights reduce manual effort.

Reflecting on the Recent Treasury Hack—How SITU-X Could Have Made a Difference

The Incident

- In December 2024, hackers **exploited API vulnerabilities** in third-party cybersecurity software to access U.S. Treasury systems. They bypassed security, obtained sensitive access using stolen API keys, and infiltrated workstations undetected.

If SITU-X Had Been in Place:

Entity-Level Intelligence	**API behavior would have been tracked in real-time, flagging unusual usage patterns and privilege escalations.**
Probabilistic Anomaly Detection	**Sliding-time windows would have identified irregular API calls, such as unexpected geo-locations or excessive access attempts, by scoring deviations in real-time**
Distributed AI for Resilient Defense	**The SITU-X Distributed AI infrastructure would have ensured low-latency response and detection directly at the edge.**

Thanks for your time.

U2opia™

Contact Us

Website: www.u2opiatech.com
Key Contact: Joaneane Smith
Email: Jsmith@u2opiatech.com