

iOT365 Defines a New Multi-Vector Detection Model for Post-Quantum OT Security

Preparing critical infrastructure for cyber threats that may have no historical signatures, indicators, or known attack patterns.

NEW YORK, NY, UNITED STATES, June 16, 2026 /EINPresswire.com/ -- New cybersecurity framework helps critical infrastructure operators identify previously unseen attack behaviors by correlating network, operational, hardware, industrial protocol, and remote access intelligence.

iOT365, an AI-powered [OT cybersecurity](#) platform for critical infrastructure, today announced its

Multi-Vector OT Threat Detection Architecture, a pioneering cybersecurity capability designed to help industrial organizations detect advanced and previously unknown cyber threats in an era increasingly shaped by artificial intelligence and future post-quantum computing capabilities.

“

Post-quantum threats may introduce attack techniques with no historical signatures or indicators. Critical infrastructure requires the ability to detect the unknown before operations are affected.”

*Alexander Tartakovsky,
Founder & CEO, iOT365*

For decades, cybersecurity technologies have relied primarily on signatures, known indicators of compromise, threat intelligence feeds, and previously observed attack techniques. As adversaries gain the ability to automate reconnaissance, generate novel attack paths, and exploit previously unseen combinations of techniques, organizations responsible for critical infrastructure face a growing challenge: how to detect attacks that have no historical precedent.

“The most significant cyber threats of the next decade may not resemble anything we have previously encountered,” said Alexander Tartakovsky, Founder and CEO of iOT365.

The infographic for iOT365 features a central shield logo with the text 'iOT365' and 'FOR IMMEDIATE RELEASE'. Below this is the headline 'Pioneering OT Cybersecurity for the Post-Quantum Era'. The main body of the infographic is a circular diagram with eight segments, each representing a different detection layer or capability: 'IP + URL + HASH Threat DB Global Threat Intelligence', 'CVE Vulnerability Intelligence', 'LAYER 3 Network & Communication Behavior', 'IDS Intrusion Detection System', 'OT ANOMALIES Operational & Process Anomalies', 'SRA Secure Remote Access', 'LAYER 2 Network Identity & Behavior', and 'HW & RESOURCE ANOMALIES Hardware & Resource Anomalies'. To the left of the diagram, a section titled 'ABP POWERED ANOMALY DETECTION' describes 'AI-Behavioral Processing Correlating Multi-Vectors Detecting the Unseen Before Impact' and lists three benefits: 'Correlates multiple weak signals across operational layers', 'Detects previously unknown attack behaviors', and 'Reduces risk, downtime, and operational impact'. Below the diagram, four key features are listed: 'Multi-Vector Visibility', 'Early Detection of Advanced Threats', 'Operational Resilience', and 'Built for Today. Ready for What's Next. Prepared for the Post-Quantum Era'. At the bottom, a dark blue bar lists industries where iOT365 is trusted: 'POWER GENERATION', 'UTILITIES', 'MANUFACTURING', 'TRANSPORTATION', 'OIL & GAS', and 'GOVERNMENT', along with the website 'www.iot365.io'.

iOT365 pioneers Multi-Vector OT Threat Detection to help critical infrastructure prepare for unpredictable AI-driven and post-quantum cyber threats.

"We believe the future of cybersecurity depends on understanding how operational environments normally behave and identifying when that behavior changes, regardless of whether the attack technique itself is known."

A New Detection Model for Emerging Threats

Rather than relying solely on known attack signatures, the iOT365 Multi-Vector Detection Architecture continuously evaluates operational behavior across multiple intelligence sources, including:

- Layer-2 network behavior and identity changes
- Layer-3 communication patterns
- Industrial protocol activity
- Vulnerability intelligence (CVEs)
- Threat intelligence (IP, URL, and Hash databases)
- Hardware and resource anomalies
- Operational process behavior
- Secure Remote Access activity
- AI-powered anomaly detection

By correlating these signals simultaneously, the platform can identify attack behaviors that may not yet have signatures, threat intelligence indicators, or documented attack procedures.

Detecting Weak Signals Before Operational Impact

Many advanced attacks begin with activities that appear benign when viewed independently, including unauthorized discovery activity, new network identities, unexpected engineering workstation communications, abnormal hardware utilization, unusual remote access behavior, or changes in controller communication patterns.

While any single event may not warrant investigation, correlating indicators across multiple operational layers can reveal the early stages of sophisticated attack campaigns.

During deployments within critical infrastructure environments, iOT365 identified coordinated sequences of anomalous activities involving unauthorized discovery behavior, unexpected engineering communications, abnormal hardware utilization, and new network identities. By correlating these indicators in real time, the platform generated actionable alerts that enabled investigation before operational disruption occurred.

Secure Remote Access as a Security Intelligence Layer

To address one of the most frequently targeted attack surfaces in industrial environments,

iOT365 integrates Secure Remote Access directly into its Multi-Vector Detection Architecture.

The capability provides centralized RDP, SSH, VNC, and web-based access management, session monitoring and recording, user activity auditing, and vendor access governance. By treating remote access activity as an additional intelligence source, the platform correlates user behavior with operational, network, and hardware events to provide a more complete view of potential threats.

Preparing Critical Infrastructure for the Post-Quantum Future

The iOT365 platform combines OT IDS, SIEM, SOC Operations, Compliance Intelligence, Secure Remote Access, and AI-powered behavioral analytics within a unified architecture designed to strengthen resilience against both current and emerging threats.

Currently deployed across critical infrastructure environments, including power generation facilities, iOT365 helps operators improve visibility, accelerate detection, and strengthen cyber resilience without interrupting industrial operations.

About iOT365

iOT365 is an AI-powered OT cybersecurity platform designed for critical infrastructure, power generation, utilities, manufacturing, transportation, ports, airports, and other continuously operating environments. The platform unifies OT Intrusion Detection, SIEM, SOC Operations, Compliance Intelligence, Secure Remote Access, and AI-powered operational visibility through a passive deployment model that enables rapid implementation without operational interruption.

Media Contact

Slava Anisimov
COO, iOT365

Email: contact@iot365.io

Website: <https://www.iot365.io>

Vyatcheslav Anisimov
iOT365 Inc.
+1 332-280-4993

[email us here](#)

Visit us on social media:

[LinkedIn](#)

[YouTube](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/919893927>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.