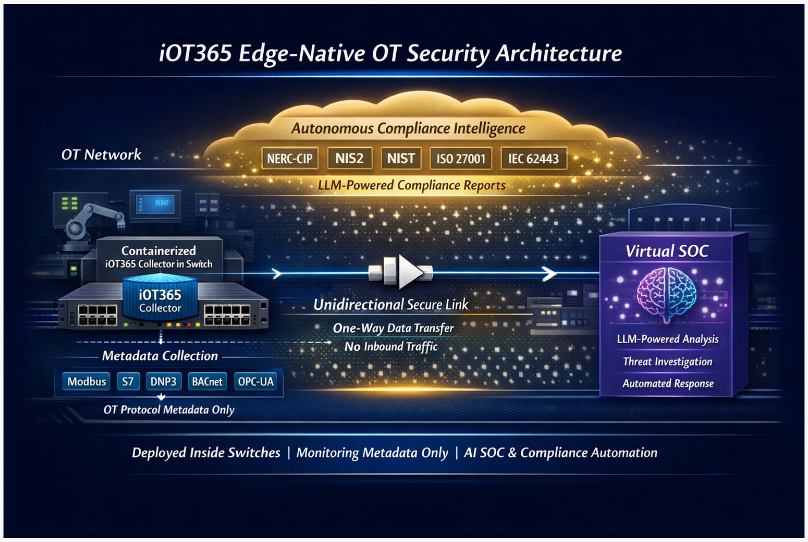
EINPRESSWIRE

iOT365 Confirms Containerized OT Security Collector Deployment Inside Industrial Switches

iOT365 confirms containerized OT security collectors running inside industrial switches, enabling AI-powered SIEM, virtual SOC and autonomous compliance.


iOT365 Edge-Native OT Security Architecture
Autonomous Compliance Intelligence
NERC-CIP
NIS2
NIST
ISO 27001
IEC 62443
LLM-Powered Compliance Reports
OT Network
Containerized
iOT365 Collector in Switch
iOT365
Collector
Metadata Collection
Modbus
S7
DNP3
BACnet
OPC-UA
OT Protocol Metadata Only
Unidirectional Secure Link
One-Way Data Transfer
No Inbound Traffic
Virtual SOC
LLM-Powered Analysis
Threat Investigation
Automated Response
Deployed Inside Switches | Monitoring Metadata Only | AI SOC & Compliance Automation

iOT365 edge-native OT cybersecurity architecture with containerized collectors running inside industrial switches, enabling AI-driven SIEM, virtual SOC, and autonomous compliance monitoring.

NEW YORK, NY, UNITED STATES, March 12, 2026 /EINPresswire.com/ -- iOT365 Confirms Containerized OT Security Deployment Inside Industrial Switches

New Edge-Native Architecture Enables AI-Native OT SOC and Autonomous Compliance Intelligence for Critical Infrastructure

New York, USA — iOT365 today announced the successful validation of its containerized OT cybersecurity collector deployed directly inside industrial network switches, confirming a new edge-native architecture designed to simplify cybersecurity deployment across operational technology (OT) environments while enabling continuous AI-driven monitoring and compliance automation.

With this architecture, iOT365 introduces a new category of Edge-Native OT Cybersecurity—where security monitoring, AI-driven analysis, and autonomous compliance operate directly within network infrastructure rather than through external security appliances.

This deployment model allows organizations to introduce cybersecurity monitoring without installing additional hardware sensors, without interrupting operations, and without impacting industrial processes. The iOT365 collector operates as a containerized application within supported industrial switches, using dedicated compute and memory resources isolated from switching functions.

By embedding security monitoring directly at the network edge, iOT365 eliminates the traditional complexity of external sensors, network taps, and additional monitoring appliances while

> The easy deployment, stable 24/7 operation, and unified AI-driven OT security and compliance platform allow organizations to gain real visibility and protection without impacting industrial operations”
>
> *Alexander Tartakovsky*

preserving the stability and performance of industrial operations.

Instead of capturing full packet payloads that can overload OT networks, the platform analyzes protocol-aware metadata from industrial communication flows, providing deep visibility into OT environments while maintaining extremely low bandwidth consumption.

This lightweight approach enables stable 24/7 monitoring across isolated industrial sites, including critical infrastructure environments where operational continuity and deterministic network behavior are essential.

The validated deployment reinforces the strength of the iOT365 unified OT cybersecurity ecosystem, which integrates multiple capabilities into a single platform:
- ML-powered IDS for industrial protocol anomaly detection
- AI-powered SIEM designed specifically for OT environments
- AI-native Virtual SOC powered by large language models (LLM)
- Autonomous Compliance Intelligence aligned with global regulatory frameworks

Security telemetry collected by the containerized collectors is securely transferred to an isolated central analysis environment, where iOT365’s AI analytics engine correlates events, filters noise, and prioritizes alerts. This process dramatically reduces false positives and ensures that security teams receive clean, actionable detections that require real attention.

For highly sensitive environments, the architecture supports unidirectional data transfer, allowing operational networks to remain fully isolated while security telemetry flows securely to the monitoring environment.

The platform’s AI-native OT SOC introduces a new operational model for industrial cybersecurity. Using large language models trained on OT security knowledge, the system assists analysts by explaining alerts, investigating anomalies, correlating attack patterns, and generating operational guidance.

This approach significantly accelerates investigation workflows while reducing the burden on security teams responsible for protecting complex industrial environments.

At the governance layer, iOT365 introduces Autonomous Compliance Intelligence, enabling organizations to continuously align cybersecurity monitoring with major global regulatory frameworks.

The platform supports automated compliance mapping and reporting across standards, including:

- NIS2 Directive
- NIST Cybersecurity Framework (CSF)
- NIST SP 800-53 security controls
- NERC-CIP
- IEC 62443
- ISO 27001

Using its LLM-powered compliance reporting engine, iOT365 can automatically generate audit-ready compliance reports that map detected events, monitoring coverage, and system configurations directly to regulatory requirements.

This capability transforms compliance from a manual documentation process into a continuous, automated security governance function.

Alexander Tartakovsky, Founder and CEO of iOT365, commented:
"The easy deployment, redundant architecture, and stable 24/7 operation of the iOT365 platform allow organizations to control the entire chain of OT cybersecurity and compliance through a unified ecosystem. By deploying directly inside network switches without impacting operations, we deliver real protection and visibility with clean detections—without compromises and without overloading manufacturing or operational environments."

The successful validation of containerized collector deployment inside industrial switches confirms iOT365's vision for edge-native OT cybersecurity, where security monitoring, threat detection, and compliance intelligence operate as a unified system designed specifically for industrial networks.

By combining lightweight edge deployment, AI-driven security analytics, and autonomous compliance automation, iOT365 enables critical infrastructure operators to strengthen cybersecurity resilience while maintaining operational stability.

About iOT365
iOT365 provides an AI-powered OT cybersecurity and compliance platform for critical infrastructure. The platform combines ML-based intrusion detection, AI-driven SIEM, an AI-native virtual SOC, and Autonomous Compliance Intelligence. Lightweight collectors run inside industrial network switches, enabling non-intrusive monitoring, high-confidence detection, and automated compliance aligned with NIS2, NIST, NERC-CIP, IEC 62443, and ISO 27001.

Vyatcheslav Anisimov
iOT365 Inc.
+1 332-280-4993
email us here

Visit us on social media:
LinkedIn