CDC ON

Securing the IT-OT Convergence – Why Legacy Systems Need a Unified SOC Platform

Introduction – The Industrial Attack Scenario

Picture this: At a petroleum refinery in western India, the IT SOC detects unusual outbound network traffic from a workstation. Meanwhile, an operator in the OT control room notices strange fluctuations in pump behavior on a SCADA console.

The IT security team investigates, but they don't have visibility into the OT network. The OT engineers, on the other hand, don't know how to interpret IT threat alerts. Hours pass while the two teams escalate and coordinate. By the time the root cause is identified, attackers have already disrupted refinery operations, causing financial losses, safety risks, and reputational damage.

This is the new normal. IT and OT are converging, but cyber defenses often remain siloed. Attacks don't respect these boundaries — and defenders can no longer afford to either.

The Challenge of IT-OT Convergence

The convergence of IT, OT, and IoT has unlocked enormous operational efficiencies. Yet, it also introduces serious cybersecurity challenges:

- **Siloed Monitoring:** IT SOCs and OT NOCs run in parallel with minimal integration, creating dangerous blind spots.
- **Legacy Devices:** OT often depends on decades-old equipment that standard cybersecurity tools cannot integrate with.

- **IoT Proliferation:** Billions of IoT devices expand the attack surface, often with minimal built-in security.
- **High Stakes:** In OT, cyberattacks are not just about data loss — they can stop production, damage infrastructure, and put lives at risk.
- **Compliance Pressure:** Energy, petroleum, and manufacturing industries face strict requirements for reporting and operational resilience.

Why Traditional SOC Tools Fall Short

Even advanced commercial SOC platforms were largely built with IT environments in mind. This creates fundamental gaps in converged environments:

- **SIEMs**: Optimized for IT logs but blind to OT protocols like MODBUS, DNP3, or IEC 60870-5.
- **XDR Platforms**: Rarely account for embedded IoT or industrial endpoints.
- **Agent-Based Security**: Most OT devices cannot run agents, leaving them outside visibility.
- **Fragmented Tools**: Multiple standalone tools mean analysts juggle dashboards instead of responding to threats.

The result? Security teams waste time, attackers exploit blind spots, and critical operations remain exposed.

The CDC-ON Approach

CDC-ON was built to eliminate these blind spots. It's a unified, analyst-first cyber defense platform that integrates **SIEM, SOAR, XDR, UEBA, Threat Intelligence, and Vulnerability Analysis** into one solution — and it works seamlessly across IT, OT, and IoT environments.

Key capabilities include:

- **Unified Visibility:** One platform for IT, OT, and IoT monitoring, reducing silos.

- **Legacy Support:** CDC-ON integrates even with decades-old OT systems where standard tools cannot be deployed.
- **Protocol-Aware Analytics:** Native support for OT/ICS protocols (MODBUS, DNP3, etc.), ensuring anomaly detection across SCADA and industrial systems.
- **Behavioral Analytics:** UEBA models applied not only to users but also to devices, machines, and control systems.
- **Hybrid Deployment:** Supports cloud, on-prem, or air-gapped environments, making it ideal for sensitive infrastructure.
- **Code-Level Customization:** As a fully OEM-controlled platform, CDC-ON can be tailored to each client's unique IT-OT ecosystem.

Use Cases of IT-OT Convergence with CDC-ON

1. **Energy Sector (Power Grids & Utilities)**
    a. Detects unusual SCADA command traffic before it disrupts grid stability.
    b. Automates cross-domain workflows, ensuring IT and OT incidents are correlated instantly.
    c. Supports NCIIPC and CERT-In compliance with real-time reporting.
2. **Petroleum Refineries & Distribution**
    a. Monitors IoT-enabled sensors (temperature, flow, pressure) alongside OT control systems.
    b. Provides a single console for IT teams and refinery operators to view threats in real-time.
    c. Enables forensic investigation post-incident with complete visibility across domains.
3. **Manufacturing Plants**
    a. Tracks deviations in production line equipment behavior without disrupting operations.
    b. Integrates legacy PLCs and ICS devices into the SOC view, extending protection across the plant floor.
    c. Optimizes uptime by reducing false positives and ensuring rapid response.

Business Benefits

Adopting CDC-ON for IT-OT convergence delivers:

- **Reduced Blind Spots:** Full-spectrum visibility across IT, OT, and IoT environments.
- **Operational Continuity:** Protects core industrial processes from cyberattacks that cause downtime.
- **Analyst Efficiency:** Low-code playbooks and AI-assisted automation reduce MTTR and analyst fatigue.
- **Future-Readiness:** Scales from a single refinery or plant to nationwide, multi-site deployments.
- **Lower TCO:** By consolidating multiple SOC tools into one, CDC-ON reduces tool sprawl and integration costs.

Conclusion

As industries digitalize, the line between IT, OT, and IoT is blurring. Unfortunately, cyber attackers have already adapted to exploit this convergence. Traditional SOC tools, designed for siloed IT systems, cannot meet the demands of industrial environments.

CDC-ON changes that equation. With unified visibility, legacy support, and protocol-aware analytics, it gives petroleum, energy, and manufacturing organizations the resilience they need to operate securely in the digital era.

For PSUs and enterprises managing critical national infrastructure, this is not just about security — it's about ensuring operational reliability, compliance, and trust in the systems that power economies and protect lives.