4 CYBERSECURITY MOVES TOP MANUFACTURERS USE TO SECURE OT SYSTEMS AND REDUCE DOWNTIME

Why It Matters

Manufacturers are seeing rising cyberattacks against operational technology, legacy PLCs, and plant-level infrastructure.

Downtime impacts output. IP theft compromises contracts. And alert overload wears out the team.

ThreatDefend, powered by Vijilan, helps secure hybrid OT/IT environments with:

CrowdStrike Falcon EDR, Identity, Discover, and Exposure Management

Cribl Stream to route and filter logs across plant, IT, and cloud networks

Corelight with Zeek to monitor internal movement between control rooms, MES, and engineering zones Hosted on AWS with support for air-gapped and regulated environments

Checklist

- Plant floor devices and controllers protected by Falcon EDR
- Privileged access managed with Falcon Identity
- Asset visibility mapped using Falcon Discover
- Patch priority driven by Falcon Exposure Management
- Logs managed across OT/IT using Cribl Stream
- East-west inspection enabled via Corelight and Zeek

Step 1

CEO: Reduce downtime and production risk across sites and systems

CISO/CTO/CIO: Use Falcon EDR to protect industrial PCs, engineering workstations, and SCADA-connected endpoints

Security Ops: Automatically contain OT-specific malware and reduce response times using behavior-based detection

Step 2

CEO: Demonstrate risk management maturity to regulators and clients

CISO/CTO/CIO: Use Falcon Identity to track privileged access to PLC, HMI, and MES systems

Security Ops: Detect lateral movement tied to password misuse or shared credentials across segmented networks

Step 3

CEO: Protect intellectual property and vendor partnerships with better visibility

CISO/CTO/CIO: Use Falcon Discover and Exposure to find rogue assets and prioritize patching based on OT-specific risk

Security Ops: Cut patch fatigue by focusing remediation efforts where exploitability intersects with availability and safety

Step 3

CEO: Stay ahead of compliance audits without overcomplicating operations

CISO/CTO/CIO: Use Cribl Stream to standardize and redact logs from SCADA and engineering systems

Security Ops: Reduce SIEM ingestion, automate alert routing, and simplify compliance workflows

Protect the line. Secure the plant.

Get a Free OT Cybersecurity Readiness Assessment for Manufacturers

vijilan
IT Security: Enabled

vijilan.com
info@vijilan.com
+1 (954) 334-9988