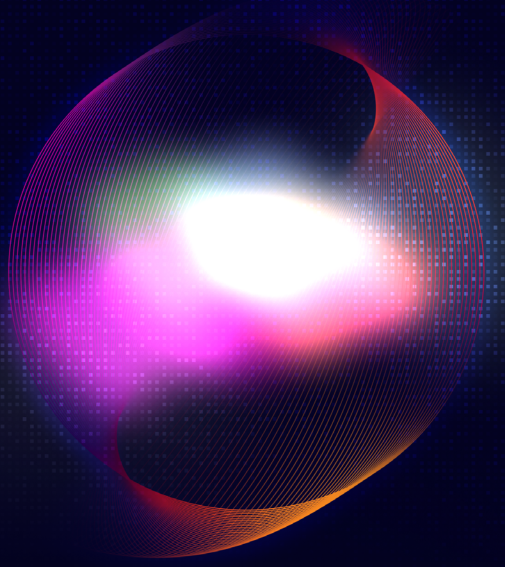
EXCLUSIVE NETWORKS

OT Security Partner Playbook

This playbook is part of the Exclusive Networks OT Security Center of Excellence — helping partners protect what's next through integrated IT/OT cybersecurity.



Start Here
Which partner are you?

IT-to-OT – Expanding from IT security into OT

Expanding-OT – Scaling existing OT practice

ICS-to-IT – Adding cybersecurity to industrial systems

The OT Difference

	IT	OT
Priority	Confidentiality	Availability
Downtime	Tolerable	Planned
Updates	Regular	Rare
Lifespan	3-5 years	15-25 years

Rule: OT security cannot disrupt operations

The Solutions

FORTINET

Security (firewalls, segmentation, Zero Trust)

NOZOMI NETWORKS

Visibility (asset discovery, threat detection, compliance)

Where to Sell

Manufacturing – Today's factories depend on connected IT, IoT and OT systems, including industrial control systems (ICS) with cyber resilience.

Electric Utilities - Smart grid control centers must communicate with their substations for power reliability and comply with NERC CIP standards.

Healthcare - Unprotected IoT devices threaten hospitals and healthcare organizations.

Retail - Brand protection is as essential as securing production and supply chains in Retail.

Prioritize deals when you hear any of these near-term OT triggers:

- Compliance prep: NIST 800-82, ISA/IEC 62443, NERC-CIP, TSA, DoD OT
- Cyber insurance requirements tied to OT visibility/segmentation
- OT asset visibility request (discover/map/baseline)
- Recent incident/outage or ransomware impacting production
- Plant disruption tied to IT/OT connectivity or rising OT anomalies
- IT/OT convergence initiative underway
- New plant build / modernization or SCADA/ICS refresh cycle
- SOC asking for OT telemetry/detection
- OT moving to IP / smart factory: IIoT, sensors, SD-WAN, cloud monitoring

Keep an eye out for search intent signals including:
"OT network visibility," "ICS threat detection," "SCADA security requirements."

Discovery Call

Ask:

1. What OT systems run operations?
2. How connected are OT and IT?
3. What visibility exists?
4. What compliance applies?
5. Biggest OT security concern?

What you'll hear → What to sell:

- "Don't know what's connected" → Nozomi
- "Can't patch" → Fortinet segmentation
- "Need compliance" → Nozomi reporting
- "Legacy vulnerable" → Fortinet + Nozomi

Handle Objections

"Have IT security" → OT needs different protocols and tools
"Too expensive" → What's one hour downtime worth? 12-month ROI typical
"Too complex" → Start with visibility, add protection. Phased.
"Prefer single vendor" → Best-in-class solves complex problems. Bigger deals.

Exclusive Networks Support

People: Practice Managers, Pre-Sales Engineers, Technical Advisors

Resources: Workshops, playbooks, materials

Services: Assessments, POC support, tailored OT SOC/MDR

Key Terms

Purdue Model = ICS segmentation framework
CPS = Cyber-Physical Systems
SCADA = Supervisory Control and Data Acquisition
ICS = Industrial Control Systems
NERC CIP = Energy compliance
IEC 62443 = Industrial security standard

Get Started

1. Choose your path
2. Visit [https://pages.insights.exclusive-networks.com/unify-it-and-ot-security]
3. Email [info_na@exclusive-networks.com]
4. Register first opportunity

Protect What's Next. Unify IT and OT Security.

Contact your Exclusive Networks OT Practice Manager to access CoE resources, and technical enablement.