Operational Use Case Playbooks

Practical guides for security operators showing how to use WireTrace for specific operational scenarios. Each playbook covers the objective, the WireTrace features involved, the workflow, and the expected outcome.

OT SECURITY

OT Incident Investigation

When suspicious activity is detected on an OT network - an unexpected PLC command, unauthorized engineering station access, or cross-zone communication - use WireTrace to investigate with full protocol-level context.

WORKFLOW

- Navigate to the asset in question in Asset Inventory - review its classification, communication peers, and protocol history
- Check Security Insights for related findings: unauthorized commands, behavioral deviations, zone violations
- Review the asset's communication timeline - which devices it communicated with, over which protocols, and when
- Examine protocol-level detail: Modbus function codes and register values, S7Comm parameters, DNP3 commands
- Cross-reference with Threat Detection for IoC matches or behavioral anomalies on the same asset

Outcome: Protocol-level forensic evidence for the incident - what commands were sent, by whom, when, and whether they deviate from established baselines.

HEALTHCARE

Clinical Device Audit

Biomed teams need an accurate inventory of every medical device on the network for accreditation surveys, procurement planning, and risk assessments. Use WireTrace to generate a live audit in minutes instead of weeks.

WORKFLOW

- Navigate to Asset Inventory - filter by device type: ventilators, patient monitors, infusion pumps, imaging systems, lab analyzers
- Review each device's classification: manufacturer, model family, clinical function, firmware details
- Check communication patterns: which EMR/PACS/gateway systems each device communicates with
- Validate network segmentation: confirm devices are on their designated clinical VLANs
- Export the inventory as CSV for biomed records or accreditation evidence

Outcome: A complete, continuously updated clinical device inventory with manufacturer, model, function, and network behavior - generated from traffic, not manual spreadsheets.

ENTERPRISE IT

TLS Certificate Hygiene Review

Expired, self-signed, and weak TLS certificates create blind spots and attack surface. Use WireTrace to audit every certificate observed on the network without scanning a single host.

WORKFLOW

- Navigate to Security Insights - select the TLS category to see all certificate-related findings
- Review self-signed certificates: identify which services use them and assess whether they are expected or problematic
- Check expiring certificates: sort by expiry date to prioritize renewals before service disruptions
- Examine weak cipher negotiations: identify connections using deprecated TLS versions or weak cipher suites
- Use Asset Details to see the full certificate chain per device - subject, issuer, validity, and key strength

Outcome: A complete TLS certificate inventory derived from observed traffic - with self-signed, expired, and weak certificates identified for remediation without active scanning.

COMPLIANCE

Compliance Audit Preparation

Preparing for IEC 62443, HIPAA, ISO 27001, or NCA audits typically requires weeks of manual evidence collection. Use WireTrace to generate audit-ready evidence from live traffic in hours instead of weeks.

WORKFLOW

- Asset Inventory: Export a complete asset inventory with vendor, model, OS, firmware, and network role for the framework's asset management requirement
- Communication Flows: Document which devices communicate with which systems, over which protocols - for access control and network security requirements
- Security Insights: Gather encryption posture evidence - TLS usage, cleartext protocol detection, certificate health - for cryptography and transmission security requirements
- Segmentation: Provide cross-zone communication evidence showing whether segmentation policies are enforced in practice
- Change Records: Show network change history - new devices, removed devices, new services - for operations security and change management requirements

Outcome: Audit-ready evidence package generated from observed traffic - asset inventories, communication flows, encryption posture, segmentation proof, and change records - without manual evidence collection.

OT SECURITY

OT Network Segmentation Assessment

Verify whether Purdue model segmentation policies are enforced in practice. Use WireTrace to identify cross-zone communications that violate intended isolation between OT levels.

WORKFLOW

- Review Asset Inventory to verify Purdue level assignments for PLCs (Level 1), HMIs (Level 2), and engineering stations (Level 3)
- Check Security Insights for cross-zone communication findings - Level 1 devices communicating directly with Level 3 systems
- Investigate unexpected communication peers: engineering station IPs appearing in PLC communication logs
- Review protocol-level detail: are these legitimate operational commands or unauthorized access attempts?
- Document findings for IEC 62443 zone/conduit mapping requirements

Outcome: Evidence-based segmentation assessment showing actual cross-zone communications from observed traffic - not theoretical firewall rule reviews.

ENTERPRISE IT

Shadow IT and Unmanaged Device Sweep

Identify every device communicating on the network that does not appear in the corporate CMDB or asset register. Use WireTrace to find shadow IT, rogue endpoints, and forgotten infrastructure.

WORKFLOW

- Navigate to Asset Inventory - sort by discovery date to find recently appeared devices
- Filter by device types commonly associated with shadow IT: consumer IoT, smart TVs, personal devices, unauthorized servers
- Review SSDP/mDNS/DHCP hostname data to identify device make and model
- Check LLDP/CDP data to determine physical switch port location for each unknown device
- Cross-reference with CMDB: any device in WireTrace but not in the CMDB is an unmanaged asset

Outcome: A complete list of unmanaged and shadow devices with vendor, type, physical location, and communication behavior - for remediation or CMDB reconciliation.

Built for Security Operations, Not Just Auditors

Every WireTrace capability is designed for daily operational use - not just compliance checkboxes.

sales@wiretrace.io