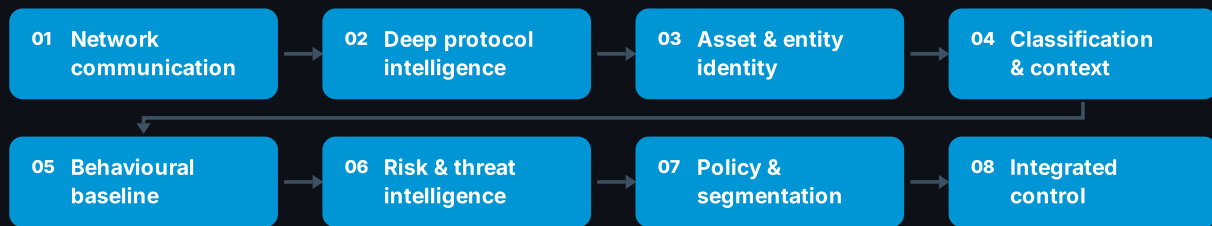


USE CASE COMPENDIUM

WireTrace Use Case Compendium

Fourteen concrete use cases across IT, OT, IoT and building networks: what WireTrace observes, what it produces, who does what, and how you measure the result.



For: Security architects, OT and IT security teams, SOC leads, asset owners and partners

This compendium describes fourteen ways organisations use WireTrace, a **Deep Protocol & Asset Intelligence (DPAI)** platform, on real networks. Each use case follows the same template, so you can compare them, pick the ones that match your priorities, and know in advance what an evaluation should show.

01 How to read this compendium

One template, every time

Challenge states the problem in your terms. **Environment** says where it occurs. **What WireTrace observes** is the network evidence; **Intelligence produced** is what the platform derives from it. **Workflow** lists what actually happens, and by whom. **Integrations, Outcome, Evidence and views** and **Deployment notes** complete the picture.

State and KPIs

Available means the use case relies only on capabilities that ship and work as described. **Conditional** means it depends on a stated condition, such as version evidence or configuration, given in its deployment notes. **KPIs** are measures you track on your own network; they are not WireTrace benchmark figures.

Four groups follow the way most programmes mature: first **know every device**, then **see what matters**, then **detect and investigate**, and finally **act with control**, with your existing tools executing the actions.

#	Use case	OT	IT	IoT	Buildings	State
A. Know every device						
1	Complete asset inventory without touching devices	●	●	●	●	Available

#	Use case	OT	IT	IoT	Buildings	State
2	Unknown and unmanaged device discovery	●	●	●	●	Available
3	Vendor, model and firmware identification	●		●	●	Conditional
4	OT asset inventory and Purdue mapping	●			●	Available
B. See what matters						
5	Vulnerability prioritisation with exploitation context	●	●	●	●	Conditional
6	End-of-life technology discovery	●	●	●	●	Conditional
7	Ransomware exposure reduction and early detection		●			Conditional
C. Detect and investigate						
8	OT command monitoring and protocol behaviour anomalies	●				Available
9	Threat detection and SOC triage	●	●	●	●	Available
10	Remote-access and third-party access detection	●	●		●	Available
11	Investigation from alert to evidence	●	●	●	●	Available
D. Act with control						
12	Dependency mapping to phased micro-segmentation	●	●		●	Conditional
13	Asset intelligence for SIEM and SOC	●	●	●	●	Available
14	Air-gapped threat and vulnerability intelligence	●	●			Available

● marks the environments where the use case most often applies. Every use case runs on the same platform and inventory, so the same deployment serves several of them at once.

Where to start. Asset owners and OT engineers usually begin with use cases 1 to 4. Vulnerability and risk teams add 5 to 7. SOC teams start with 9, 11 and 13. OT security teams add 8 and 12. Isolated and classified sites add 14. All of them run on the same sensors and the same inventory.

1. Complete asset inventory without touching devices

Available OT · IT · IoT · Buildings | Asset inventory, identity, classification

Challenge	"Our register covers laptops and servers. It misses the controllers, cameras, printers and building systems, and we may not scan most of them."
Environment	Plants, substations, hospitals, campuses, airports and data centres where many devices cannot carry an agent or tolerate scanning.
What WireTrace observes	Mirrored traffic decoded to the payload: identity records in industrial, building and network protocols; DHCP, DNS, NetBIOS, mDNS, LLDP and CDP names; SSH host keys and certificates.
Intelligence produced	One durable identity per physical device; domain, type and role with a confidence; for each device, which kinds of evidence are present, missing or stale.
Workflow	1. The network team provides a SPAN, TAP or ERSPAN feed; a sensor is attached and enrolled. 2. Devices appear within minutes and are enriched as evidence accumulates. 3. The asset owner reviews unknown and low-confidence devices and adds custom classification rules where needed.
Integrations	Read-only REST API; optional read-only SNMP polling of switches and routers.
Outcome	An inventory that stays current without touching devices, with the source of every value.
Evidence and views	Asset inventory; asset detail with field sources and visibility assurance.
Deployment notes	Passive by default: the capture interface never transmits. Coverage follows sensor placement; devices behind routers appear by address unless enriched.
KPIs	Percentage of devices with a known type and role; percentage reconciled with the existing register.

2. Unknown and unmanaged device discovery

Available OT · IT · IoT · Buildings | Asset inventory, identity, Policies (licensed)

Challenge	"Devices keep turning up that nobody ordered, owns or patches: a consumer router under a desk, a contractor's laptop, a camera on the production network."
Environment	Campuses, branches, production floors and shared facilities where many parties connect equipment.
What WireTrace observes	The first appearance of a device, what it states about itself, and its peers, protocols and ports.
Intelligence produced	A new device with a durable identity, a normalised manufacturer (a fallback to the network-card maker is labelled as low confidence), a classification where evidence supports one, and its communication history.
Workflow	1. WireTrace records the new device and its evidence. 2. A policy notifies the owning team by email, syslog or webhook and labels the device for review. 3. The team decides whether it belongs, records an owner, or asks the network team to remove it.
Integrations	Email, syslog, webhook and SNMP trap notifications; REST API.
Outcome	Unmanaged devices are found when they appear, and each ends with an owner or a removal.
Evidence and views	Asset inventory by first seen; asset peers and connection history; Activity log.
Deployment notes	Needs sensor coverage of the segments concerned. A device the evidence cannot classify stays unknown, not guessed.
KPIs	Percentage of devices with a known owner and role; median time from first seen to ownership decision.

3. Vendor, model and firmware identification

Conditional OT · IoT · Buildings | Deep protocol intelligence, identity

Challenge	"We cannot judge risk on a controller without its model and firmware, and nobody will log in to three hundred devices to find out."
Environment	Industrial cells, substations, building automation and IoT estates with long-lived embedded devices.
What WireTrace observes	Identity records carried in protocols, such as CIP identity, PROFINET identification data, the BACnet device object, S7 identity and SNMP system descriptions.
Intelligence produced	Manufacturer, model, firmware and serial number where the device states them, each with the evidence that produced it and its freshness.
Workflow	1. Sensors decode identity records during normal operation. 2. The asset owner reviews attributes and sources in the asset detail. 3. Where devices state nothing, the team optionally enables read-only switch polling or credentialed collection for IT and network equipment.
Integrations	Optional read-only SNMP, LLDP and CDP enrichment; REST API.
Outcome	Firmware known, with verifiable evidence, for the devices that state it, and a clear list of those still unknown.
Evidence and views	Asset detail with field-level sources; inventory filtered by firmware.
Deployment notes	Condition: recorded where a device states them, as many industrial controllers, IoT and network devices do, or where optional polling or credentialed collection adds them. Not every device reveals them passively; passive coverage on IT-heavy estates is lower.
KPIs	Percentage of controllers with a known firmware version and stated source.

4. OT asset inventory and Purdue mapping

Available OT · Buildings | Classification, Purdue and communication views (licensed)

Challenge	"Our drawing shows five neat Purdue levels. We do not know whether the network still looks like that."
Environment	Manufacturing, energy, utilities, oil and gas, and building systems.
What WireTrace observes	Industrial protocols such as Modbus, S7comm, EtherNet/IP and CIP, PROFINET, DNP3, IEC 60870-5-104, IEC 61850, OPC UA and BACnet, and the conversations between levels.
Intelligence produced	Controllers, HMIs and engineering workstations classified by type and role; each device on a Purdue level with a stated confidence and a one-line reason; a zone-to-zone communication matrix.
Workflow	1. Sensors are placed at plant or substation aggregation points. 2. WireTrace classifies devices and assigns Purdue levels automatically. 3. OT engineers compare the Purdue view with the intended architecture; unexpected cross-level paths feed use case 12.
Integrations	REST API; PDF reports for engineering and management audiences.
Outcome	An OT level map of the network as it is today, with the reasoning behind each placement.
Evidence and views	Purdue view; communication matrix; classification confidence and basis.
Deployment notes	Passive by default; an OT-safe profile keeps optional active probes away from industrial devices unless explicitly allowed.
KPIs	Percentage of OT devices with an engineer-reviewed Purdue level; number of unexpected cross-level paths.

5. Vulnerability prioritisation with exploitation context

Conditional OT · IT · IoT · Buildings | Vulnerability intelligence, remediation workspace, Asset Risk Score

Challenge	"We have thousands of CVEs on paper and a few maintenance windows a year. Which are real on our devices, and which are being exploited?"
Environment	Estates where patching is slow or constrained, especially OT and embedded devices.
What WireTrace observes	Each device's identified operating system, software, firmware and OT product.
Intelligence produced	Matches to the NVD and OT vendor advisories, prioritised with CISA KEV and FIRST EPSS, each stating how it was matched and whether the version is confirmed on that device; a 0-100 Asset Risk Score with a confidence indicator.
Workflow	1. The vulnerability owner sorts findings into Now, Next and Later lanes with owners, SLAs and change windows. 2. Unpatchable devices go to the containment view; time-limited risk acceptance is recorded where justified. 3. Fixes are tracked as verified when the evidence changes.
Integrations	REST API; policies can notify on known-exploited findings.
Outcome	A short, defensible remediation list based on what is confirmed and exploited.
Evidence and views	Vulnerability workspace; Risk Register; match strength per finding.
Deployment notes	Condition: findings follow the version evidence available. Devices that state no version are not given version-precise findings. IT patch verdicts need optional online advisory sources.
KPIs	Open known-exploited findings on confirmed versions; median age of Now-lane items.

6. End-of-life technology discovery

Conditional OT · IT · IoT · Buildings | End-of-life intelligence, operating system identification

Challenge	"Auditors ask how many unsupported systems we run. For laptops we know; for everything else we guess."
Environment	Estates with long equipment lifetimes: production lines, building systems, laboratory networks, legacy servers.
What WireTrace observes	Operating systems inferred passively with a stated confidence or announced by the device, and product and firmware identities where stated.
Intelligence produced	Operating systems and products flagged as past vendor end of life, using lifecycle data that also works offline.
Workflow	1. WireTrace flags end-of-life technology as devices are identified. 2. The asset owner confirms the flagged products by site and role. 3. Replacement is planned, or compensating controls and risk acceptance are recorded.
Integrations	REST API; CSV export; PDF reports.
Outcome	An evidence-based list of unsupported technology for replacement budgets and audits.
Evidence and views	Inventory filtered by end-of-life status; Risk Register.
Deployment notes	Condition: flags depend on identifying the product and version. Operating system identification is stronger on IT than OT, and OT firmware lifecycle coverage is not complete. Credentialed collection adds exact versions for hosts you choose to scan.
KPIs	Confirmed end-of-life devices per site; percentage with a replacement plan or recorded compensating control.

7. Ransomware exposure reduction and early detection

Conditional IT | Threat detection, Risks & Exposures

Challenge	"Ransomware reaches the plant through IT file shares. We want fewer ways in, and an early warning if it starts."
Environment	File servers and shares, and the IT systems bordering OT.
What WireTrace observes	Clear-text and legacy authentication, weak cryptography, exposed services; file operations on unencrypted SMB; reconnaissance and lateral movement.
Intelligence produced	Exposures in one view, and one corroborated verdict correlating reconnaissance, lateral movement, mass file modification, ransomware extensions and ransom notes on file shares, and unusual exfiltration.
Workflow	1. The security team works through Risks & Exposures to remove clear-text credentials and legacy protocols. 2. If staging or impact is detected, the verdict reaches the Alert Queue and the SIEM; the analyst investigates. 3. The IT team contains affected hosts with its own tools.
Integrations	Syslog to any SIEM; Splunk HTTP Event Collector; webhooks.
Outcome	Fewer reusable credentials and services, and one corroborated alert instead of scattered signals.
Evidence and views	Risks & Exposures; Alert Queue; file activity on shares.
Deployment notes	Condition: file-activity detection works on unencrypted SMB; SMB3-encrypted sessions expose no file operations. Sensors must see file-server traffic.
KPIs	Devices exposing clear-text credentials; time from ransomware verdict to triage decision.

C. DETECT AND INVESTIGATE

8. OT command monitoring and protocol behaviour anomalies

Available OT | OT command monitoring, Protocol Behaviour Baseline

Challenge	"A program download or mode change on a controller can stop a line. We need to know when it happens, who did it, and whether it was planned."
Environment	Process control, manufacturing cells, substations and utility telemetry.
What WireTrace observes	What an industrial conversation does (reads, writes, program transfers, mode changes, exceptions) on Modbus, S7comm, DNP3, IEC 60870-5-101/104, IEC 61850 MMS, Omron FINS, Mitsubishi SLMP/MELSEC and SEL Fast Message.
Intelligence produced	Alerts for unauthorised writes, parameter changes, mode changes and stops, program download and upload, forced I/O, firmware transfers, rogue masters and illegal function codes; once a Protocol Behaviour Baseline is approved, a deviation for any new field or value.
Workflow	1. OT engineers record and approve a Protocol Behaviour Baseline for the cell. 2. WireTrace raises events with source, target and decoded operation. 3. The on-call engineer checks each event against the maintenance plan.
Integrations	Syslog to the SIEM; email and SNMP traps to operations.
Outcome	Every controller change in scope is seen, attributed and reconciled with planned work.
Evidence and views	Alert Queue with decoded operations; Protocol Behaviour Baseline.
Deployment notes	Command monitoring covers the protocols listed. EtherNet/IP, BACnet, OPC UA, PROFINET and S7CommPlus receive identity and discovery only. Baselines take effect after operator approval.
KPIs	Percentage of controller changes matched to a work order; controllers covered by an approved baseline.

9. Threat detection and SOC triage

Available OT · IT · IoT · Buildings | Detection rules, Alert Queue, ATT&CK coverage

Challenge	"Our SOC sees nothing from devices that cannot run an agent, and cannot tell an engineering action from an attack."
Environment	SOCs covering converged IT and OT, building systems and IoT.
What WireTrace observes	Rare destinations, new services, scanning, lateral movement, beaconing, DNS tunnelling and unusual outbound volume; adversary-in-the-middle techniques; matches against public feeds and indicators you supply.
Intelligence produced	Alerts from 90+ deterministic detection rules mapped to MITRE ATT&CK or ATT&CK for ICS, each stating its evidence, with the device's identity and role.
Workflow	1. Alerts arrive in one Alert Queue and are forwarded to the SIEM. 2. An analyst assigns, investigates, escalates, resolves or marks false positive. 3. The detection engineer exports an ATT&CK Navigator layer for gap analysis.
Integrations	Syslog (CEF, LEEF, RFC 5424/3164); Splunk HTTP Event Collector; webhooks; STIX 2.1 and CSV indicators.
Outcome	Network detections with device context that analysts can triage and explain.
Evidence and views	Alert Queue; ATT&CK coverage view.
Deployment notes	Detection follows sensor coverage. WireTrace does not decrypt traffic; encrypted sessions still yield behavioural and certificate evidence.
KPIs	Time from alert to triage decision; percentage of alerts closed with a recorded reason.

10. Remote-access and third-party access detection

Available OT · IT · Buildings | Application recognition, behavioural analysis, exposures

Challenge	"Vendors, integrators and contractors connect in ways we did not approve, and we find out afterwards."
Environment	Plants and buildings with integrator support; IT with outsourced administration.
What WireTrace observes	Remote-administration protocols such as RDP and SSH, 150+ recognised cloud, vendor-cloud and infrastructure applications, new internet communication, and clear-text credentials.
Intelligence produced	For each device, the applications and remote peers it uses and which are new; alerts for new external communication, new services and clear-text credential exposure.
Workflow	1. The security team reviews which devices use remote-access paths. 2. Approved paths are documented; a policy notifies the owner when a new one appears. 3. Unapproved paths are closed by the network team.
Integrations	Email, syslog and webhook notifications; SIEM forwarding.
Outcome	A short, known list of remote-access paths, each with an owner.
Evidence and views	Asset applications and peers; Alert Queue; Risks & Exposures.
Deployment notes	Sensors need to see internet and site-boundary traffic. Customers can add their own application definitions.
KPIs	Remote-access paths without an owner; time from new path to owner decision.

11. Investigation from alert to evidence

Available OT · IT · IoT · Buildings | Investigations and Threat Hunting (licensed), Rumi

Challenge	"After an incident we spend hours stitching logs together before we can say what happened."
Environment	SOC and incident response teams supporting IT and OT.
What WireTrace observes	Recorded network events, decoded protocol fields and flow records, and packet captures recorded on demand from sensors.
Intelligence produced	An investigation with gathered evidence, a timeline and playbooks; each conclusion shows supporting and contradicting evidence and a confidence; related detections group into cases by attack stage.
Workflow	1. The analyst opens an investigation from an alert, asset or indicator. 2. They pivot through the timeline, run guided Threat Hunting queries and capture packets on demand. 3. Rumi, the private AI assistant, summarises; the analyst verifies and records the conclusion.
Integrations	Webhooks and REST API for SOAR platforms; SIEM forwarding.
Outcome	Conclusions a second analyst or an auditor can follow.
Evidence and views	Investigations; Threat Hunting with saved hunts.
Deployment notes	Licensed modules. Packet capture is on demand, not automatic retention. Rumi runs on the WireTrace server and is assistive.
KPIs	Time from alert to documented conclusion; re-opened investigations.

D. ACT WITH CONTROL

12. Dependency mapping to phased micro-segmentation (protect a PLC cell)

Conditional OT · IT · Buildings | Communication map, baselines, traffic rules, violations

Challenge	"We want to isolate a production cell, but every attempt broke something nobody had documented."
Environment	A PLC cell with HMIs, drives, a historian, an engineering workstation and vendor access, on a flat plant network.
What WireTrace observes	All communication to and from the cell by protocol and port, device identities and Purdue levels.
Intelligence produced	A dependency map; an operator-approved Communication Baseline; traffic rules and IEC 62443 zones and conduits as intent; validation results; violations including IT-to-OT conduit crossings and Purdue-level jumps.
Workflow	1. The OT team records a baseline, approves the expected pairs and declares the cell as a zone with its conduits. 2. Proposed rules are tested against observed traffic before anyone relies on them. 3. The customer's firewall team receives the validated traffic rules, with proposed block rules exported as text for the paths to close, and translates them into its own rulebase. 4. WireTrace raises violations and, on a schedule, drift against the baseline.
Integrations	Rule text for iptables, nftables, Cisco IOS and pf; blocklists to pull; syslog, webhook, email and SNMP traps; REST API for NAC and other tools.
Outcome	A cell isolated by your own firewall from validated rules, and a continuous check that it stays isolated.
Evidence and views	Communication map; Traffic Rules and Violations; IEC 62443 zones.
Deployment notes	Conditions: enforcement is performed by the customer's existing controls, using the traffic rules WireTrace has validated against observed traffic. Rule seeding is coarse; validation covers a bounded window; drift runs on your schedule.
KPIs	Undocumented dependencies found before change; rollbacks after enforcement.

13. Asset intelligence for SIEM and SOC

Available OT · IT · IoT · Buildings | Alert forwarding, REST API, durable identity

Challenge	"Our SIEM shows an IP address. By the time we know it was a safety controller, not a printer, the shift has changed."
Environment	Organisations with a SIEM or SOAR platform and a SOC covering non-IT devices.
What WireTrace observes	Identity, type, role, Purdue level, risk and communications of each device, kept current as addresses change.
Intelligence produced	Alerts carrying durable identity, classification and risk; an API exposing assets, changes, risk, vulnerabilities, alerts and threat matches.
Workflow	1. An administrator configures alert forwarding by type and severity. 2. An administrator enables API Access and creates a scoped client. 3. Analysts see device context in the SIEM; automation looks up assets before acting.
Integrations	Syslog (CEF, LEEF, RFC 5424/3164) over UDP, TCP or TLS; native Splunk HTTP Event Collector output; IBM QRadar via LEEF and Microsoft Sentinel via CEF over syslog; JSON webhooks; read-only REST API with OAuth 2.0.
Outcome	Every network alert says what the device is and how much it matters.
Evidence and views	Integration settings; API Access clients.
Deployment notes	The API runs on your appliance and is off until enabled; tokens are scoped, rate-limited and IP-restricted. Standard formats; no dedicated SIEM app.
KPIs	Percentage of SIEM network alerts carrying device type and role; manual asset lookups per incident.

14. Air-gapped threat and vulnerability intelligence

Available OT · IT | Air-gapped operation, offline data refresh, Platform Updates

Challenge	"Our network has no internet connection by design, but we still need current vulnerability and threat data."
Environment	Defence, government, critical national infrastructure and isolated OT sites.
What WireTrace observes	The same evidence as a connected deployment. Analysis, the AI assistant, end-of-life data and identity and classification knowledge all live on the appliance.
Intelligence produced	Indicator matching and vulnerability findings kept current from offline refreshes, with each intelligence area's version and freshness in one place.
Workflow	1. A collection script on any internet-connected machine gathers threat and vulnerability data under the customer's own feed terms. 2. The checksummed bundle crosses through the customer's own transfer process. 3. An administrator imports it; Platform Updates shows the new freshness.
Integrations	None required; internal SIEM forwarding and REST API remain available.
Outcome	Current intelligence on a network that never connects out.
Evidence and views	Platform Updates; vulnerability workspace.
Deployment notes	The appliance never connects out. Identity and classification knowledge improves with each release; refresh cadence follows your transfer process.
KPIs	Age of vulnerability and threat data on the appliance; refresh cycles completed on schedule.

Limits, stated plainly

- WireTrace sees what reaches its sensors. Every use case depends on sensor placement and mirrored traffic at the right points.
- WireTrace does not decrypt traffic. Encrypted sessions still yield identity, certificate and behavioural evidence, but not their content.
- Model, firmware and vulnerability precision follow the evidence available: what devices state, or what optional enrichment collects.
- WireTrace defines, validates and monitors segmentation intent and policy. Your firewalls, NAC and switches execute network control.
- The KPIs in this compendium are measures for you to track on your own network. They are not WireTrace performance claims.

Pick the use case that matters most to you

A WireTrace evaluation starts passively on one mirrored port. Choose the use case you want to prove, and measure it with the KPIs in this compendium on your own network.

Book a demo at wiretrace.io/request-demo or email sales@wiretrace.io