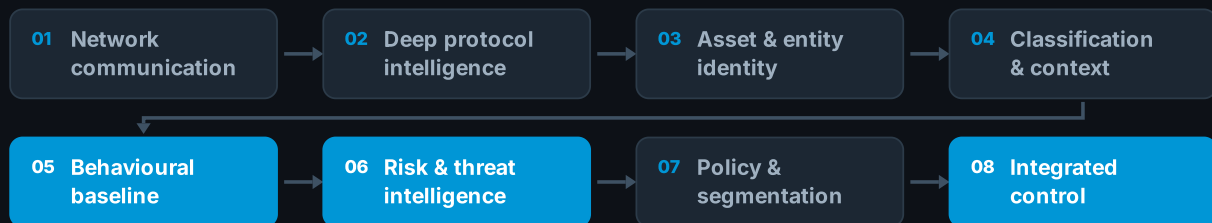


SOLUTION BRIEF

Threat Detection & Security Analytics

Deterministic detection that states its evidence, an analyst workflow from alert to investigation, and vulnerability and risk prioritisation grounded in what each device actually is.



For: SOC analysts and managers, security architects, OT security teams

A detection is only useful if an analyst can tell, quickly, what it saw, why it matters and what to do next. WireTrace detects threats from the network itself, across IT and OT, and **every detection states the evidence it rests on and the device it concerns**, using the same durable device identity that powers the asset inventory.

90+

deterministic detection rules across IT, OT and network-integrity threats

ATT&CK

every technique rule mapped to ATT&CK for Enterprise or ATT&CK for ICS

KEV + EPSS

vulnerability prioritisation by known exploitation and exploit likelihood

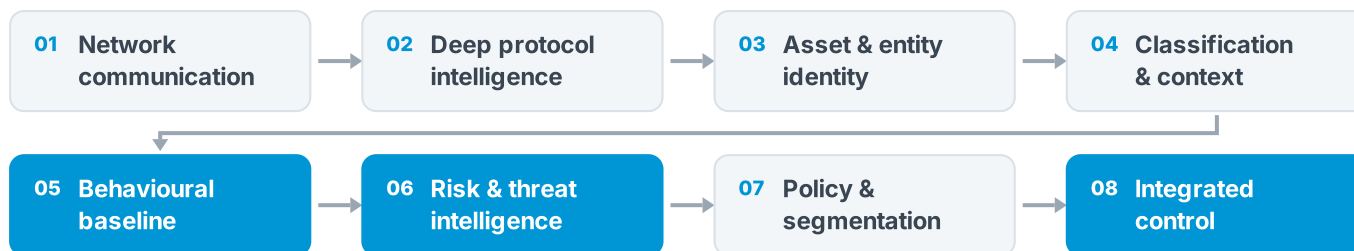
0-100

Asset Risk Score per device, with confidence and a factor breakdown

01 The detection approach

WireTrace is a **Deep Protocol & Asset Intelligence (DPAI)** platform. Its sensors decode protocol payloads; the platform then evaluates **90+ deterministic detection rules** against that decoded evidence. Each rule is mapped to MITRE ATT&CK or ATT&CK for ICS, or declared as a policy or anomaly check, and states the evidence it rests on. The rules are not signatures and do not depend on a statistical model: given the same evidence, a rule reaches the same conclusion, and an analyst can see why.

Because detection runs on decoded protocol fields rather than packet patterns, a rule can ask questions such as *"was this a write to a controller, from a host that has never written to it before?"* and attach the answer to a device identity rather than an address.



The WireTrace platform flow. Highlighted layers are the subject of this document.

02 What WireTrace detects

OT command monitoring

For Modbus, S7comm, DNP3, IEC 60870-5-101/104, IEC 61850 MMS, Omron FINS, Mitsubishi SLMP/MELSEC and SEL Fast Message, WireTrace detects unauthorised writes, parameter changes, controller mode changes and stops, program download and upload, forced I/O, firmware transfers, new or rogue masters and illegal function codes. These are the operations that change a physical process, read from the protocol itself.

WireTrace observes

- A host in the office network opens an S7comm session to a Purdue level 1 controller
- It stops the controller, transfers a program block and restarts it
- That host has never issued commands to this controller before

WireTrace produces

- Alerts for the mode change and the program download, mapped to ATT&CK for ICS
- The controller and the commanding host named by durable identity, with their classification
- The decoded operations as evidence, and an IT-to-OT conduit crossing if segmentation intent is declared

Behavioural and anomaly analysis

First-seen and rare destinations, new services, new internet communication, peer-group differences, scanning, lateral movement, beaconing, algorithmically generated domains, DNS tunnelling and unusual outbound volume, each explained against its baseline.

Network integrity

Adversary-in-the-middle techniques: TLS interception, TCP reset injection, ARP, DHCP and LLMNR poisoning, and DNS manipulation.

Threat-indicator matching

Observed traffic is matched against public threat-intelligence feeds and indicators you supply, as CSV, STIX 2.1 or a commercial feed using your own key: IP addresses, ranges, domains, URLs, file hashes and TLS fingerprints. Connected sites refresh automatically; air-gapped sites import a checksummed bundle from a customer-run collector.

Ransomware

Reconnaissance, lateral movement, mass file modification, ransomware extensions and ransom notes on file shares, and unusual exfiltration are correlated into one corroborated verdict. This works on unencrypted SMB; encrypted SMB sessions expose no file operations, and WireTrace says so.

Web attacks

SQL injection and cross-site scripting attempts in unencrypted HTTP. HTTPS content is not inspected.

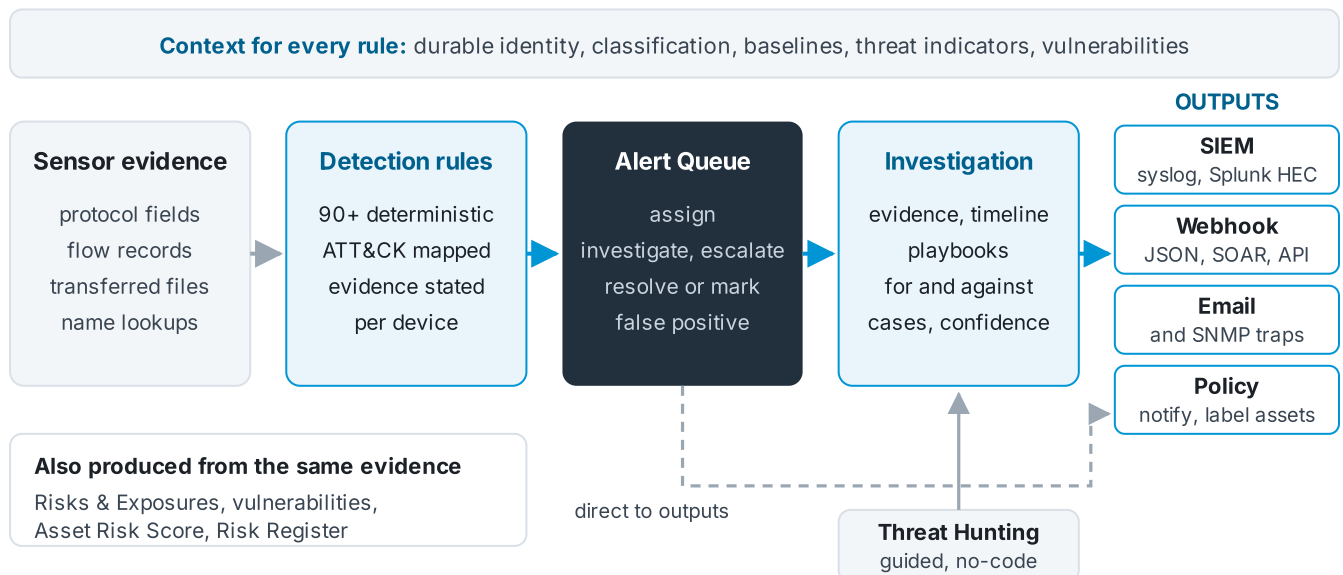
YARA scanning of transferred files

Files transferred over unencrypted SMB and HTTP can be hashed, matched to threat intelligence and scanned with YARA rules you manage. A starter set is included; coverage depends on the rules you add.

ATT&CK coverage you can inspect

The coverage view separates the techniques WireTrace can detect from those actually observed in your environment, and exports an ATT&CK Navigator layer so you can combine it with the coverage of your other tools.

03 From detection to response



Detection to response. Rules evaluate decoded sensor evidence in the context of each device; analysts work alerts in one queue and open investigations; results reach the tools you already run.

- 1 Alert Queue.** All detections land in one queue. Analysts assign, investigate, escalate, resolve or mark false positive, and alerts are forwarded to any SIEM over syslog (CEF, LEEF, RFC 5424/3164, filtered by type and severity) or through the native Splunk HTTP Event Collector output. QRadar ingests WireTrace alerts via LEEF over syslog, and Microsoft Sentinel via CEF over syslog.

- 2 **Risks & Exposures.** Clear-text credentials, weak cryptography, exposed services, OT exposure, network-integrity findings and ransomware activity in one view, with CSV export. This is where standing weaknesses are tracked, separately from alerts.
- 3 **Investigations** (optional module). Any alert, asset or indicator opens an investigation that gathers evidence, builds a timeline and applies investigation playbooks. Each conclusion shows supporting and contradicting evidence and a confidence. Related detections group into cases showing attack-stage progression.
- 4 **Threat Hunting** (optional module). Search recorded network events with a guided, no-code query builder, save and re-run hunts, and pivot results into investigations.
- 5 **Packet capture on demand.** Packet captures can be recorded on demand from sensors for deeper analysis. Alert evidence itself is decoded protocol fields and flow records.

Rumi, the private AI assistant, runs on the WireTrace server and can summarise an investigation in plain language. Facts and counts come from deterministic queries with click-through evidence; Rumi assists the analyst, who verifies before acting.

04 Vulnerability intelligence

WireTrace matches each device's identified OS, software, firmware and OT product to the NVD and OT vendor advisories, and prioritises the results with CISA KEV (known exploited vulnerabilities) and FIRST EPSS (exploit prediction). **Every finding states how it was matched, how strong the match is, and whether the vulnerable version is confirmed on that device.**

Matching needs version evidence. A controller that states its firmware, or a host scanned with credentials, can be matched precisely. A device that states only its product family yields a weaker match, labelled as such, so analysts can tell a confirmed exposure from a possible one.

WireTrace observes

- A controller states its order number and firmware version
- An OT vendor advisory covers that product and firmware range
- The same vulnerability is listed as known exploited
- The controller sits at Purdue level 1 and accepts writes from an IT-zone host

WireTrace produces

- A finding with a strong match and the vulnerable version confirmed
- Priority raised by known exploitation
- A higher Asset Risk Score, with the factors that raised it
- A remediation item in the Now lane, or a containment entry if the device cannot be patched

The **remediation workspace** turns findings into work: Now, Next and Later lanes with owners, SLAs and change windows, time-limited risk acceptance, verified-fix tracking, and a containment view for devices that cannot be patched. **End-of-life intelligence** flags operating systems and products past vendor end of life, using lifecycle data that also works offline; coverage of OT firmware lifecycles is not complete.

05 Asset risk

Every device receives a 0-100 **Asset Risk Score**, calculated as likelihood multiplied by impact, with a separate confidence indicator and a factor breakdown. Likelihood draws on applicable vulnerabilities, exposure, active threats, end-of-life status, hygiene, protocol deviations and policy violations; impact

reflects the device's Purdue level and its safety or control role. The **Risk Register** ranks devices by score and supports time-limited risk acceptance. It is an asset-level register, not an enterprise risk register.

06 Who uses what

Team	What WireTrace gives them
SOC analysts	One Alert Queue with device context on every alert, investigations with supporting and contradicting evidence, guided hunting, and forwarding to the SIEM they already run.
Security architects	An ATT&CK coverage view and Navigator layer, network-integrity and exposure findings, and the evidence to judge where other controls are needed.
OT security and plant engineers	Command monitoring on industrial protocols, OT vendor advisory matching with confirmed-version status, and a containment view for devices that cannot be patched.
Vulnerability and risk owners	Findings prioritised by known exploitation and match strength, Now, Next and Later lanes with owners and SLAs, and a ranked, explainable Risk Register.

Limits, stated plainly

- WireTrace does not decrypt traffic. Ransomware file activity, YARA scanning and web-attack detection apply to unencrypted SMB and HTTP only.
- OT command monitoring covers the protocols listed above. Other industrial protocols, including EtherNet/IP, PROFINET, OPC UA and BACnet, are used for identity and discovery.
- YARA is a capability for rules you manage, not turnkey malware detection.
- Vulnerability findings are only as precise as the version evidence. Definitive patch status for IT hosts relies on credentialed collection and optional online advisory sources.
- Packet capture is on demand; captures are not retained automatically when an alert fires.
- No accuracy or coverage percentages are claimed. The ATT&CK view shows exactly which techniques are covered.

Put your own traffic through it

A WireTrace evaluation on a mirrored port shows which detections fire in your environment, the evidence behind each one, and which vulnerabilities deserve attention first.

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