WIRETRACE

COMPLIANCE MAPPING GUIDE

Continuous Compliance Evidence from the Wire

WireTrace generates audit-ready compliance evidence automatically from observed network traffic. Asset inventories, communication flows, access control validation, encryption posture, and segmentation evidence are always current - replacing periodic manual assessments. This guide maps WireTrace capabilities to specific control requirements.

The WireTrace Approach

- **Continuous, Not Periodic** - Evidence generated from live traffic every day, not collected manually once per audit cycle.
- **Evidence-Based, Not Self-Reported** - Findings derived from actual network behavior. Observed facts, not questionnaire responses.
- **Operationally Useful** - The same data that satisfies auditors drives daily security operations: incident investigation, risk prioritization, change monitoring.

IEC 62443 - Industrial Automation Security

Requirement	WireTrace Evidence	How It Works
Zone & Conduit (3-2)	Zone boundaries mapped from observed traffic. Cross-zone communications documented.	Passive traffic analysis identifies cross-zone communications with protocol detail.
Asset Inventory (2-1, 3-2)	Continuously updated inventory of every industrial asset.	Multi-signal classification from protocol fingerprints, MAC, DHCP, behavior.
Access Control (3-3)	Communication patterns showing which devices access which systems.	Protocol-level inspection of controller communications and commands.
Network Monitoring (3-3, 4-2)	Continuous monitoring with behavioral deviation alerting.	Per-device, per-protocol baselines with full context on deviations.

NCA OTCC - Saudi OT Cybersecurity Controls

Requirement	WireTrace Evidence	How It Works
OT Asset Management	Complete OT asset inventory with vendor, model, firmware.	Passive discovery from observed industrial protocol communications.
OT Network Security	Segmentation evidence, cross-zone detection, lateral movement alerts.	Zone boundary monitoring from traffic analysis. Purdue level assignment.
OT Monitoring	Continuous monitoring. Behavioral deviations, unauthorized commands.	Protocol-aware baselines detect command pattern and polling changes.
OT Incident Mgmt	Protocol-level forensic evidence for investigation.	Historical records of all communications, commands, connection changes.

NCA ECC - Essential Cybersecurity Controls

Requirement	WireTrace Evidence	How It Works
Asset Management (2-2)	Comprehensive IT/OT/IoT asset inventory.	Passive protocol analysis identifies every communicating device.
Network Security (2-7)	Segmentation validation, unauthorized access detection.	Cross-segment communication monitoring with protocol detail.
Continuous Monitoring (2-12)	Real-time monitoring with deviation and threat alerting.	Behavioral baselines, IoC matching, attack surface analysis.
Vulnerability Mgmt (2-3)	CVE correlation prioritized by real exposure.	NVD, CISA KEV, EPSS matching against observed assets and firmware.

ISO 27001 - Information Security Management

Requirement	WireTrace Evidence	How It Works
A.8 Asset Management	Continuously updated asset inventory with classification.	Multi-signal passive discovery and weighted classification.
A.9 Access Control	Communication pattern evidence per device.	Protocol-level access monitoring and unauthorized peer detection.
A.10 Cryptography	TLS certificate inventory. Self-signed and expired detection.	TLS handshake inspection extracts certificate fields.
A.12 Operations Security	Change monitoring: new devices, services, configurations.	Continuous traffic analysis detects network behavior changes.
A.13 Communications	Segmentation evidence. Cleartext protocol detection.	Protocol-aware inspection of unencrypted and cross-segment flows.

HIPAA - Healthcare Security Rule

Requirement	WireTrace Evidence	How It Works
164.310 Device Inventory	Complete medical device inventory by vendor and function.	Proprietary medical protocol parsing.
164.312 Access Controls	Access pattern evidence for ePHI system communications.	Protocol-level EMR, PACS, clinical gateway monitoring.
164.312 Transmission Security	Encryption posture per connection. Cleartext ePHI detection.	TLS inspection and protocol analysis.
164.312 Audit Controls	Continuous communication audit trail per medical device.	Every communication logged with protocol detail.

Evidence Types Generated

- Asset inventories - complete, continuously updated device inventories with vendor, model, OS, firmware, network role
- Communication flows - protocol-level documentation of device communications and commands
- Security findings - cleartext credentials, expired certificates, exposed interfaces, unprotected protocols
- Segmentation evidence - cross-zone and cross-segment communication documentation
- Change records - new devices, removed devices, configuration changes, behavioral deviations

From Periodic Audits to Continuous Evidence

wiretrace.io | sales@wiretrace.io