OT Cyber Security Intelligence, On Demand

How GILT transforms OT network configurations into queryable security intelligence

The OT Cyber Security Gap

OT networks underpin the control and safety systems of every mission-critical facility — yet their configurations are rarely integrated into broader knowledge management or security monitoring. Switch configurations sit as CLI exports in engineering folders. Firewall rulesets are reviewed manually during periodic audits that may occur only annually. Network segmentation compliance against standards like IEC 62443 is assessed by specialist consultants at significant cost, producing point-in-time reports that begin decaying in accuracy from the moment they're delivered.

Between audits, configurations drift. New firewall rules are added during troubleshooting and never removed. VLAN assignments change during commissioning activities. Port security settings are temporarily disabled and forgotten. Firmware updates are deferred indefinitely. The result is an OT security posture that is understood at a snapshot in time but opaque in between — precisely when continuous visibility matters most. In an environment where a cyber breach can have physical safety consequences, this gap is not acceptable.

How GILT Assists Cyber Security Professionals

- **Switch configuration analysis** — Running and startup configurations from managed industrial switches (Cisco IE series, Hirschmann, Siemens SCALANCE, Belden) are parsed to extract VLAN assignments, port security settings, spanning tree configurations, access control lists, SNMP configurations and management access settings. The logical network topology of the OT environment is reconstructed and made queryable. Ask: "Which ports on SW-OT-03 have port security disabled?" or "Show the VLAN topology for the Level 2 control network."
- **Firewall ruleset intelligence** — Rules from industrial firewalls and DMZ appliances (Palo Alto, Fortinet, Hirschmann EAGLE, Tofino, Cisco ASA) are ingested and normalised into a structured, queryable rule database. Each rule is mapped to its source and destination zones, protocols, ports and associated OT assets. Query: "Show all rules permitting traffic from Level 2 to Level 3 per the Purdue model" or "Which firewall rules allow any traffic from the enterprise network to a PLC subnet?" or "List all permit-any rules across all firewalls." Results include the specific firewall, rule number and configuration context.
- **Network segmentation compliance** — By combining switch configurations, firewall rulesets and asset inventories, GILT reconstructs the actual logical segmentation of the OT network and assesses it against IEC 62443 zone and conduit requirements. Identify segmentation gaps, unauthorised cross-zone communication paths and conduits that lack appropriate security controls — without requiring specialist consultants to manually audit every device. Query: "Which PLCs in Zone 3 can communicate with the enterprise network?" and get a definitive, sourced answer.
- **Configuration drift detection** — Baseline configurations are versioned upon initial ingestion. Subsequent ingestions are automatically compared to detect drift: new firewall permit rules, changed VLAN assignments, disabled port security, modified ACLs, changed SNMP community strings. Unauthorised or undocumented modifications are flagged automatically with before/after comparison and timestamp. This provides continuous monitoring between formal audits.
- **Vulnerability context enrichment** — Device firmware versions extracted from switch and firewall configurations are cross-referenced against CVE databases and vendor security advisories. Vulnerabilities are not just listed — they are assessed in the context of the actual network topology and exposure. A critical CVE on an air-gapped device has different risk implications than the same CVE on a device with enterprise network connectivity. GILT provides this contextual risk assessment automatically.

Standards Alignment

GILT's cyber security framework is informed by the following standards and frameworks:

- **IEC 62443** — Industrial Automation and Control Systems Security. The primary framework governing security in OT environments. GILT's architecture respects zone and conduit segmentation principles and enables continuous compliance assessment.
- **ISO 27001** — Information Security Management Systems. Provides the overarching governance structure for all data handling within GILT's platform.
- **NIST SP 800-82** — Guide to Industrial Control Systems Security. Supplementary guidance for securing ICS and their supporting infrastructure.
- **Australian Essential Eight** — The ACSC's baseline mitigation strategies for cyber security incidents. GILT's operational controls are aligned with all eight mitigation strategies.
- **AESCSF** — Australian Energy Sector Cyber Security Framework, applicable to energy sector engagements and aligned with the NIST Cybersecurity Framework.

OT network data is treated with the highest sensitivity classification within GILT's data handling framework. It is never stored in shared environments and is processed in dedicated, isolated compute instances. All data is encrypted in transit (TLS 1.3) and at rest (AES-256) with per-client HSM-backed key management. All access is logged with tamper-evident audit trails.

Deployment, Reporting & Why It Matters

GILT ingests OT network data through secure, offline methods — no direct connectivity to live OT networks is required. Configuration exports, PCAP files and asset inventories are ingested through controlled, air-gapped transfer processes. GILT operates as a read-only analytical layer that never writes to or connects directly to operational infrastructure, ensuring zero impact on OT network availability.

GILT generates structured security reports suitable for regulatory submissions, board reporting and audit evidence: segmentation compliance matrices, firewall rule audit summaries, configuration drift reports and contextualised vulnerability assessments. Reports are generated on demand or on a scheduled basis, ensuring documentation is always current.

A breach in an OT environment can have physical safety consequences — equipment damage, environmental release, production loss and risk to human life. Continuous visibility into network segmentation, firewall posture and configuration integrity is essential for facilities operating safety-critical systems. GILT provides that visibility as a persistent, queryable intelligence layer — without requiring specialist OT security personnel to manually audit every device. The result is a security posture that is understood continuously, not periodically.