IOT & OT SECURITY SERVICES

Protecting connected devices, critical systems and industrial networks

Smart systems and industrial controls are expanding – and so is your attack surface.
Our IoT & OT Security Services help you identify risks across connected devices, SCADA systems, telemetry, and automation environments. We bridge the gap between IT and engineering to protect operations that can't afford to go offline.

🔍 Why IoT and OT Security Matters

Modern operational environments rely on smart devices, remote monitoring, and industrial control systems — but most were not designed with cybersecurity in mind. These systems are often:

- Legacy or vendor-managed
- Unpatched or unsupported
- Connected to the internet or IT networks
- Lacking authentication or encryption

From local council water plants to smart lighting, from medical devices to manufacturing sensors — your environment may be more exposed than you think.

🧰 What We Offer

✅ IoT & OT Security Assessment

- Asset discovery and network mapping
- Review of protocols (Modbus, DNP3, IEC 60870-5-104, BACnet, etc.)
- Architecture and segmentation analysis (Purdue Model alignment)
- Threat modelling and critical asset identification
- Vulnerability and misconfiguration analysis

✅ Compliance & Governance Alignment

- ACSC OT Security Principles
- IEC 62443 / NIST SP 800-82
- PSPF or ISM guidance
- Policy development and access control recommendations
- Incident response planning for OT scenarios

✅ Secure Remote Access Review

- VPNs, telemetry backhaul, and vendor access pathways
- Audit of jump servers, authentication, and access logging
- Recommendations for segmentation and least privilege access

IOT & OT SECURITY SERVICES

Protecting connected devices, critical systems and industrial networks

👷💼 Who This Is For

- **Councils** managing smart city infrastructure, SCADA water/traffic systems
- **Utilities** operating remote telemetry, sensors, and distributed control systems
- **Not-for-profits** with health tech, assistive devices, or medical IoT
- **Manufacturers** with PLC-driven automation or robotics
- **Organisations** undergoing digital transformation of physical operations

---

💬 What Our Clients Say

"The OT security review helped us identify systems that had never been documented — and were exposed to both our corporate network and the internet. Their recommendations were practical and easy to prioritise."

— IT & Infrastructure Manager, Regional Utility

🎯 What You Can Expect

✔ Visibility into your connected and unmanaged devices
✔ Risk-reduction roadmap for operational environments
✔ Improved resilience for systems that can't afford downtime
✔ Better separation between IT and OT networks
✔ Governance tailored for engineering and operations — not just IT

🔐 Common Risks We Mitigate

- Default credentials on industrial devices
- Unmonitored wireless or serial-to-IP bridges
- Unpatched firmware in field devices
- No incident response process for physical system compromise
- Remote access from third-party vendors with no logging or MFA

📦 Optional Add-Ons

- Ongoing OT vCISO support
- Policy development for OT-specific controls
- Architecture redesign with segmentation recommendations
- Tabletop exercises (power, water, or control failure simulations)
- Integration with broader GRC or MSS platforms

Secure Your Smart & Industrial Systems

We understand the balance between uptime, safety, and security. Let's assess your IoT/OT risk and build a strategy that fits your operational reality.

Schedule Your IoT/OT Assessment

vCISO.One cybersecurity consulting & advisory
29/97 Creek Street, Brisbane City QLD 4000
☎ 1300 067 003
✉ info@vciso.one
vciso.one