Add value.
Inspire trust.

Our OT Security Services

Ensure the security of your industrial networks

Your challenges

As OT uses both hardware and software to carry out processes aligned with the aims of various departments in an organisation, it can be challenging to pinpoint whose responsibility it is to secure that technology. In some cases where several sensors are connected to a single network worldwide, organisations may find it difficult to keep tabs and secure all of them. The complexity of OT networks therefore makes it an increasingly attractive target for cyber-attacks.

What is OT Security?

OT describes environments comprising of Industrial Control Systems (ICS). These include Industrial Automated Control Systems (IACS), Supervisory Control and Data Acquisition (SCADA) and Process Control Networks (PCN). Cyber risks pertaining to these environments pose a great threat to all of us. The ramifications of cyber-attacks in these domains could lead to calamitous and catastrophic outcomes.

Why is OT Security important for your organisation?

OT has a high inherent risk as compared to IT systems due to weak access control across physical & logical regions, high functionality-dependent design principles, and complexity of personnel involved in various project stages.

Various vulnerabilities have been exploited by hackers worldwide, resulting in loss of public reputation, equipment damage, leakage of sensitive data and information, and even the lives of citizens. Typical contributing factors of vulnerabilities are:

SYSTEMS

- **Complex Off-Boundary Connectivity:** In May 2017, hackers initiated ransomware attacks to German Railway by exploiting open authentications in CCTV system and eventually reached automatic fare collection system and passenger information system, causing loss in revenue and public reputation.

- **Low or No Authentication:** In the cyber-attack to SingHealth in June 2018, the SGH Citrix servers were not adequately secured against unauthorised access. Notably, the process requiring 2-factor authentication ("2FA") for administrator access was not enforced as the exclusive means of logging in as an administrator. This allowed the attacker to access the server through other routes that did not require 2FA.

HUMAN

- **Insufficient Cyber Security Awareness:** In the cyber-attack to Ukraine power grid in June 2017, the operators noticed their mouse cursors moved of their own accord, as the hackers remotely opened the circuit breaker via SCADA system and managed to disrupt the power supply to end users.
- **Low Regulatory Framework:** In the cyber-attack to SingHealth in June 2018, there was no evidence that the Healthcare IT Security Incident Response Framework (SIRF) had been circulated or otherwise communicated widely to staff.

PROCESS

- **Complex Supply Network:** In 2010, Natanz Nuclear Facility in Iran was affected by Stuxnet, resulting in equipment damage and intense relationship with other countries. It was reported that the nuclear facility got an infection from a USB stick from a sub-contractor.
- **Use of Commercial Off-The-Shelf (COTS) Components and Systems:** COTS components and systems are favoured by system integrators due to lower initial cost and cost-effective new upgrades with new features, however credentials are attractive targets for attackers because they often remain unchanged and they can readily be reused to gain administrator-level access. For example, Stuxnet is a malicious computer worm targeting at Siemens S7 PLCs, causing the total breakdown of plant while the same module was used.

Our OT Security Services

- IEC 62443 Audits & Certifications (All major sub-set's)
- OT Advisory services
- OT/ICS Network/architecture review
- IT / OT Security Policy Review
- System Hardening Benchmarks
- Gap Analysis
- Business Recovery Plan
- Cybersecurity Risk Assessment Services for OT/ICS systems & networks
- Vulnerability Scan & Analysis for OT/ICS systems & networks
- ICS/SCADA Penetration Test & analysis
- VAPT services for IoT / IIoT (Device, App & Cloud)
- VAPT services for Medical IoT/IIoT (Device, App & Cloud)
- VAPT services for Automotive IoT/IIoT (Device, App & Cloud)
- e-Learning for Cybersecurity – OT Package (Basic & advanced level)

Your business benefits

- **Minimise risk** – and ensure that your systems are secure by maintaining compliance with the requirements.
- **Improve continuity** – by leveraging on our expertise.
- **Enhance productivity** – by being proactive rather than reactive to reduce the time for system restore.

Why choose TÜV SÜD?

TÜV SÜD's experts have a wealth of experience working with clients on complying OT system with regulatory and industry best standards. We have previously worked with various regulatory agencies in Asia Pacific region, and collaborate with major standards bodies and other cybersecurity frameworks & industry standards. TÜV SÜD can bridge the gap between CII operators and regulatory agencies as we have a strong understanding of what regional cybersecurity agencies and sectorial CII regulators are looking for in terms of the cybersecurity code of practice compliance.

Our Head Offices in South Asia, ASEAN, Middle East and Africa Region

INDIA
Tel: +91 1800 212 2000
Email: info.in@tuvsud.com
www.tuvsud.com/in

SINGAPORE
Tel: +65 6778 7777
Email: info.sg@tuvsud.com
www.tuvsud.com/sg

ABU DHABI
Tel: +971 2 676 7600
Email: info.me@tuvsud.com
www.tuvsud.com/ae

AFRICA
Tel: +27 13 244 1330
Email: info.za@tuvsud.com
www.tuvsud.com/za

Follow us on social media linkedin.com/company/tuvsud

TÜV SÜD South Asia Pvt. Ltd. Solitaire, 4th Floor, ITI Road, Aundh, Pune - 411 007, Maharashtra, India.
1800-212-2000 **info.in@tuvsud.com** **www.tuvsud.com/in**