OT Security for Industries

Comprehensive OT-IT infrastructure security against emerging threats to ensure maximum efficiency

T··Systems

Growing OT Security Challenges

With more connectivity and IT integration, security risks for industries with Operational Technology (OT) & Industrial Control Systems (ICS) environments have grown rapidly – potentially leading to downtime, supply chain disruption, production losses, litigations, and more.

Some common OT security risks that industries face:

- **Advanced Persistent Threats (APT):** Threats that are carefully planned and are capable of remaining hidden for a long time within the system.
- **Ransomware:** Ransomware attacks on OT industries are rising. For instance, 56% of manufacturing companies were attacked in 2023 alone.*
- **AI-based Threats:** Attackers are launching AI-based phishing attacks, Internet of Things malware, and supply chain attacks with more precision and on a larger scale.
- **Zero-Day Vulnerabilities:** Attackers are exploiting vulnerabilities that have not been fixed yet – allowing breaches to take place without early detection.
- **Insecure Remote Access:** Risks related to unauthorized or insecure access to OT systems are growing with increased cloud computing and networking.

In addition to these threats, risks in the supply chain due to the integration of third-party systems, potential insider threats because of vendors accessing critical infrastructure, outdated software creating new vulnerabilities, and other risks that organizations do not have full visibility on, must be considered as well.

Apart from organizational risks and losses, attacks on OT systems can pose a threat to the safety of not just employees, but also the environment and the public. To reduce these risks, organizations need modern security solutions.

The State of Ransomware in Manufacturing and Production Report, 2023

OT Security with Enhanced Threat Detection & Defense

T-Systems offers 360° security solutions designed to protect the overall industrial environment considering networks, endpoints, data, cloud, and operational technology. The AI-based capability in Managed Detection and Response (MDR) allows for real-time threat detection and reduces false positives – highlighting only real threats. Additionally, our Security Operations Center (SOC) monitors activities 24/7 to respond to and mitigate security risks in the early stages.

We offer a Tiered SOC approach to:

- Monitor all security-relevant processes of networked IT and OT systems
- Detect security incidents in real-time and report the threat situation
- Strengthen resilience to ensure continuous production and system uptime
- Integrate an end-to-end concept instead of security silos for better visibility and protection

This is achieved through continuous alarm handling, response coordination, reporting, threat awareness, and platform administration. In addition to our MDR services, our other capabilities, such as OT Security Assessment, Microsegmentation, and Infrastructure Security, help to further strengthen your OT security.

OT Security Assessment

OT Security Assessment improves network visibility, provides asset discovery, and identifies vulnerabilities. It includes network sensor installation, visualization, risk monitoring, and anomaly detection.

Microsegmentation

OT-IT networks can be segmented to reduce the attack surface and contain breaches. Networks with critical infrastructure can be protected with additional security policies applied to those segments.

Infrastructure Security

Securing infrastructure is vital to protect networks and systems from cyber threats. This involves safeguarding physical and virtual components to ensure resilient IT and OT environments. Modern security solutions help maintain stable operations and availability.

An Integrated Approach to OT Security

Consulting → **Implementation** → **Managed Services**
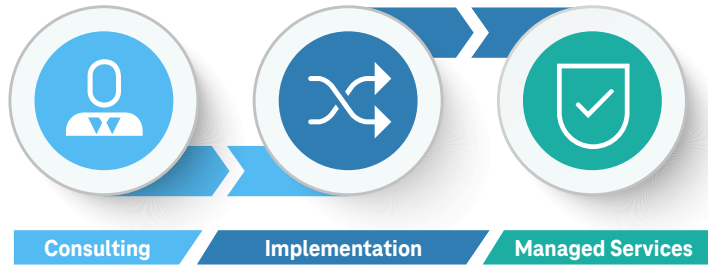
Consulting

With thorough assessments, we check the company's OT-IT security integration and posture to uncover existing vulnerabilities and security risks in the system.

This also enables us to discover all existing OT-IT assets to create a detailed inventory – to ensure the most suitable security approach will be applied to all assets.

In addition to gap assessments, our OT Security service also comprise a maturity mapping, building a cyber defense roadmap, and risk planning.

Implementation

Based on the results of the assessments and the organization's needs and priorities, our OT Security services are integrated into the existing IT infrastructure.

Managed Services

T-Systems has worldwide SOC services with capabilities of SIEM[1], SOAR[2], and XDR[3]. Our security professionals act as an extended team to your in-house security teams.

We offer 24/7 monitoring of OT-IT networks to detect anomalies and potential threats in real time. Our SOC teams are responsible for not just detecting threats but also responding to them.

[1] *SIEM: Security Information and Event Management*

[2] *SOAR: Security Orchestration Automation Response*

[3] *XDR: Extended Detection & Response*

Benefits to Industries

- **Loss Reduction:** Prevent financial loss caused by cyberattacks and data breaches.
- **Risk Mitigation:** Minimize operational risks and protect critical infrastructure.
- **Business Continuity:** Ensure uninterrupted operations and quick recovery from incidents.
- **Improved Resilience:** Build a robust and resilient OT environment capable of withstanding severe attacks.
- **Enhanced Productivity:** Maintain high productivity levels by securing operational processes.
- **Compliance:** Adhere to European industrial and critical infrastructure frameworks such as KRITIS, NIS2, and more.
- **Competitive Advantage:** Gain competitive advantage by demonstrating robust security measures to clients and stakeholders.

Why T-Systems?

With one of the largest SOCs, an advanced technology stack, and a high-quality partner ecosystem we can meet dynamic OT-IT security needs. We understand the modern threat landscape, and our experience in catering to numerous large customers worldwide helps us deliver top-notch security. We offer tailor-made services that fit your requirements and secure your OT-IT infrastructure in the long run.

Start with an OT Security assessment. Contact us today.

Expert Contact

Andreas Pecka
Head of International Sales and
Pre-Sales Cyber Security
a.pecka@t-systems.com

ᛢ· · Systems