T Security

OT Security

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

Growing OT security challenges

With more connectivity and IT integration, security risks for organizations 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 companies face:

- **Advanced Persistent Threats (APT):** Threats that are carefully planned and remain hidden for a long time within the system.
- **Ransomware:** Ransomware attacks remain a major threat to OT systems – in 40% of incidents, data is successfully encrypted, with average recovery costs reaching $ 1.3 million.*
- **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, impacting pipelines, drilling operations, and power plants.

*The State of Ransomware in Manufacturing and Production Report, 2025

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integration of third-party systems, potential insider threats because of vendors accessing critical infrastructure, outdated software creating new vulnerabilities, and other risks that organizations do not have full visibility on, must be considered as well.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

OT Security with enhanced Threat Detection & Defense

T Security offers 360° security solutions designed to protect the overall industrial environment considering networks, endpoints, data, cloud, and operational technology. AI-based Managed Cyber Defense capabilities allow for real-time threat detection and reduce 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 Managed Cyber Defense services, other capabilities, like OT Security Assessment, Microsegmentation, and SASE, help to further strengthen your OT security.

OT Security Assessment

The service provides visibility into industrial environments by identifying assets, vulnerabilities, network risks, and abnormal activity. By assessing security maturity and highlighting critical gaps, it enables organizations to prioritize improvements, reduce cyber risk, and strengthen operational resilience.

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.

Secure Access Service Edge (SASE)

SASE enables strong OT security by combining networking and security functions within a unified cloud-native platform. Through centralized policy enforcement, Zero Trust access, and end-to-end visibility, it reduces complexity, strengthens protection against evolving threats, and provides secure, scalable connectivity for distributed users, sites, and industrial environments.

An integrated approach to OT Security

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 Security 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 team.

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 of OT Security

- **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 Security

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.

Get in touch with our experts
cyber.security@t-systems.com

Published by

Deutsche Telekom AG
Friedrich-Ebert-Allee 140 , 53113 Bonn, Germany
security.telekom.de
t-systems.com