Magenta Industrial Security

Protection against cyber attacks for networked IT/OT systems

T · · ·   **ERLEBEN, WAS VERBINDET.**

Magenta Industrial Security Explained in 60 seconds

Networked production facilities are increasingly becoming the target of cyber attacks, IT and OT systems need protection:

- Consulting on building hardened architectures and secure processes of networked IT/OT systems.
- 24/7 operation of an integrated IT/OT SOC for protection against cyber attacks
- Detection of anomalies and attacks by Azure Defender for IoT-criticality assessment and initiation of defensive measures by certified analysts
- Defense against sabotage and data theft based on real-time analysis of data traffic

Advantages

- Comprehensive visibility into the protection of all IT and OT systems through integrated Security Operation Center
- Presentation of the threat situation for assets and systems with technical support of Azure Defender for IoT on a central dashboard

- Access to Deutsche Telekom Security's cyber security expertise from successful protection of own CRITIS-relevant systems and networks
- Prevention of damage due to production downtime and theft of intellectual property

Fields of application for **Magenta Industrial Security**

Manufacturing and automotive
Non-intrusive anomaly detection along the entire value chain, protection of R&D, production, and logistics

Energy provider
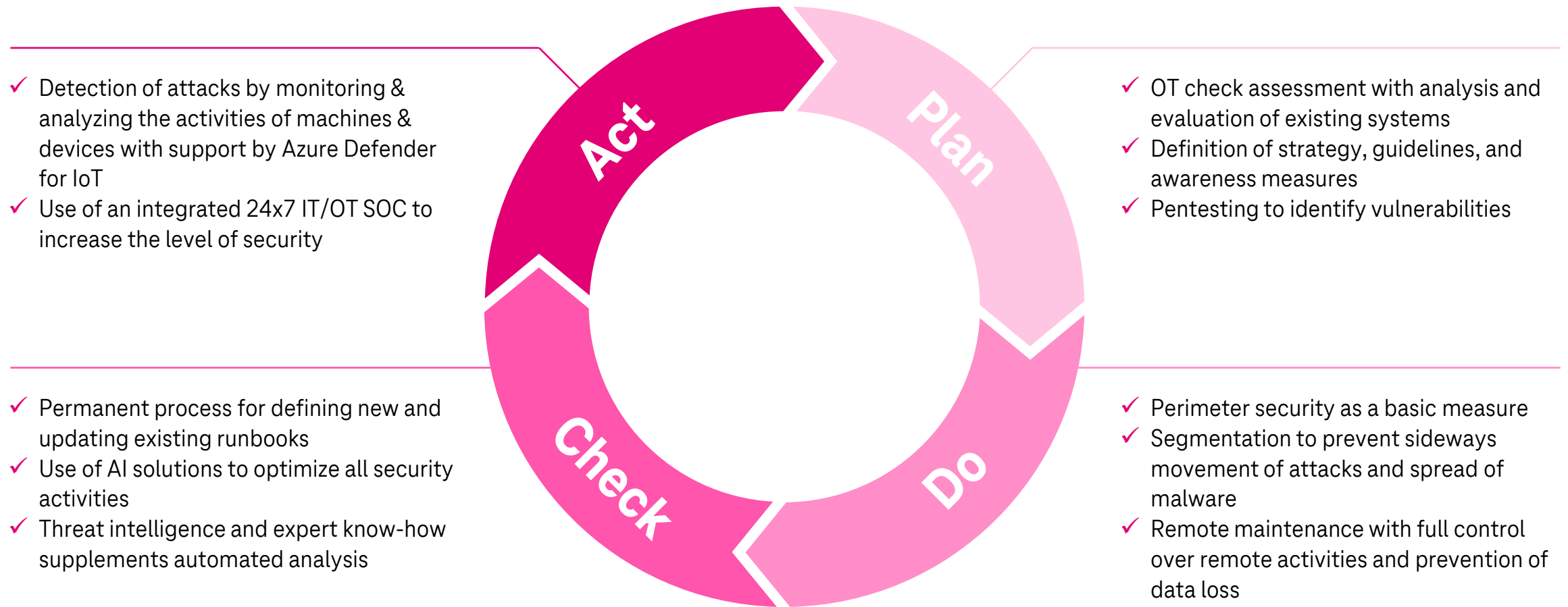In addition: Compliance with CRITIS requirements

How we comprehensively protect networked IT and OT systems.
Security from integrated IT/OT Security Operation Centers

Legend:
- Log
- Appliance
- Software
- Sensor — Microsoft Azure
- Firewall
- Internet

Comprehensively secure your IT/OT systems against cyber attacks:
Via system architecture hardening, passive and active defenses, and AI.

Act
- Detection of attacks by monitoring & analyzing the activities of machines & devices with support by Azure Defender for IoT
- Use of an integrated 24x7 IT/OT SOC to increase the level of security

Plan
- OT check assessment with analysis and evaluation of existing systems
- Definition of strategy, guidelines, and awareness measures
- Pentesting to identify vulnerabilities

Check
- Permanent process for defining new and updating existing runbooks
- Use of AI solutions to optimize all security activities
- Threat intelligence and expert know-how supplements automated analysis

Do
- Perimeter security as a basic measure
- Segmentation to prevent sideways movement of attacks and spread of malware
- Remote maintenance with full control over remote activities and prevention of data loss

Our protection for your networked IT/OT systems:
Integrated, modular, comprehensive

Managed Services

- Industrial Threat Detection **Microsoft Azure**
- Industrial Firewall

OT-SOC   **IT-SOC**

- Alarm handling
- Reportings
- Playbooks
- Incident Orchestration
- Response
- Threat Intelligence Services

Professional Services

- Orientation workshop
- Security checks
- Check vulnerability assessment
- Check penetration testing
- Asset inventory

- Assembly and installation services for reselling

Best of Breed

- Industrial ID **Microsoft Azure**
- OT-Firewall
- Remote Access

Magenta Industrial Security