Orange
Cyberdefense

Industrial Security

Orange Cyberdefense helps organizations analyze, plan, integrate and operate OT-specific security systems for your production environment and plant engineering.

Reliable cyber security – mandatory for industry 4.0

The enterprise IT merges with the operational IT in the production environment and the plant controls. This creates additional attack vectors for production control systems. By linking the previously independent production islands, attackers are not only able to access business-critical information, but are increasingly able to manipulate production processes and bring entire plants to a standstill. Recent studies show that the number and professionalism of cyber-attacks on SCADA systems (Supervisory Control and Data Acquisition) and Industrial Control Systems (ICS) have increased dramatically - with consequences that many companies now have to act after years of orientation. In the digitalization of industry, mechanical and plant engineering companies have an important dual function: While they, as operators of plants, digitize their own production and business processes, as technology integrators they offer their customers complete systems and systems. In addition to reliable European standards, production, integration and operation require above all technical solutions and services that have the engineering in their blood and are not half-heartedly derived from IT.

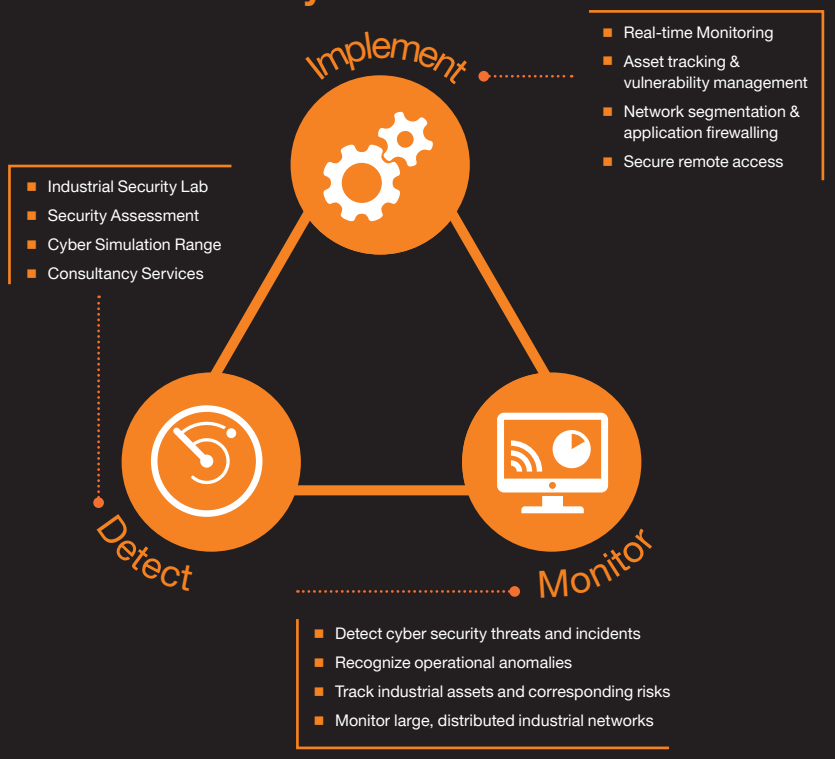
You know that one? „IT and OT walk into a bar...“

Intercultural competence is often required because both sides have different philosophies, approaches and challenges to master. So it is not surprising that safety officers in the factory prioritze issues like reliability and availability of the ongoing production over, for example, network segmentation, vulnerability scanning or patching. Configuration changes may lead to malfunctioning interfaces and cause legacy operating systems to stop working which in turn threatens or compromises production operations.

Expertise in Industrial Security

- Industrial Security Lab & Demo Environment
- hundreds of security monitoring projects in the last 10 years worldwide
- 24x7 Service for IT and OT in our advanced CyberSOCs
- ISO-certified top-level setup, latest technology, optimized processes, experienced security experts
- Cyber Simulation Range for training with OT-specific components
- Dedicated teams for analysis, incident response, forensics and emergency response

360° Industrial Security



Find out more on how to protect your endpoints on:
orangecyberdefense.com/se/ot-iot

Managed Cyber Defense Services for Infrastructure and Production Facility Operators

Orange Cyberdefense's Managed Cyber SOC services increase cyber-attack resilience to production assets and critical infrastructures, and greatly enhance visibility against espionage, tampering and sabotage. If intrusive security concepts can not be implemented, passive monitoring is an effective and compensatory measure. Many solutions derived from IT are not suitable for OT envritonments. Instead, we rely on artificial intelligence (AI) and machine learning with extensive ICS knowledge. This enables us to automatically model and monitor even the largest, heterogeneous industrial plants. From our ISO certified Cyber SOCs all over the globe we monitor your IT and OT infrastructure 24x7.

Security Monitoring for Production Networks

Orange Cyberdefense implements non-intrusive solutions for real-time monitoring of production assets without the need for business interruptions or network disconnects. The solutions work purely passively on different network levels and provide the following functions:

- Identification of ICS assets
- Identification of software versions, vulnerabilities and associated risks
- Complete determination of the traffic topology of all systems and their connections
- Detecting normal behavior based on artificial intelligence and machine learning
- Detecting and alerting to behavioral anomalies, policy violations, critical states or changes, suspicious activity, attacks, etc.
- Customizable visualization by topographic groups, logical levels, system types, protocols, criticality, etc.
- Central monitoring of distributed production networks, including contextual enrichment and SIEM integration

Network-Segmentation & Application Firewalling

Port-based SPI firewalls have become obsolete and are being replaced by Next Generation Firewalls (NGFWs), which are able to support common ICS protocols by default, e.g. Modbus, OPC or IPPC. This enables network segmentation requirements as described for production environments in the ISA-99 or ISO 62443 and ISO 27002 standards to be implemented at various protocol levels and to separate OT networks from the Office IT.

Asset Surveilance & Vulnerabilitymanagement

Within production environments, active scanning of the components, as is common in office IT, is hardly possible. Orange Cyberdefense relies on alternative methods to identify existing systems, software releases and their vulnerabilities. Depending on the system used, the information can be passively extracted from the network traffic or polled periodically by the PLCs / RTUs.

Secure Remote Access

The central remote maintenance and monitoring (remote access) of geographically isolated control systems is a prerequisite in today‘ s production landscapes. However, especially in the case of remote access, it is important to establish secure communication channels between headquarters and remote location, since public transmission channels such as the Internet and 2G or 3G networks (as failover and redundant connection) are frequently used. In addition, the unique identification of users is necessary through the use of strong authentication procedures that prevent potential misuse of access data. Orange Cyberdefense provides proven solutions for every application.

Red Teaming in simulated Production Environments

With the Cyber Simulation Range, a hyper-realistic training environment that Orange Cyberdefense operates in cooperation with the Information Security Hub (ISH) of Munich Airport, we prepare your security experts for the daily challenges of working in a Cyber SOC team. The range includes a variety of components typically found in ICS networks and allows to train a wide range of attack scenarios.

Answers

Orange Cyberdefense‘s industrial security solutions and services provide you with Answers to the following questions:

- Which solutions and services can I apply to legally comply with the guidelines for KRITIS?
- Which security solutions are better suited for production environments than ordinary IT security products?
- What is the danger proposed by malware and backdoors?
- How can I enable my Cyber SOC be to monitor my production facilities?
- What is the maturity of current security monitoring solutions for ICS / SCADA?

Customers

Our customers and prospectives in the field of Industrial Security come from the following sectors:

- Operators of production plants in automotive, chemical, pharmaceutical & aerospace industries
- Plant and equipment manufacturers including vehicle construction
- Energy suppliers and municipal utilities
- Transport and logistics
- State and military institutions

For more information check
https://orangecyberdefense.se

Orange Cyberdefense
Stenbärsgatan 6, 212 31 Malmö

info@se.orangecyberdefense.com
+46 10 202 20 13