OT Cybersecurity Engineer

Descrição da função

The OT Cybersecurity Engineer is responsible for ensuring the secure operation of Operational Technology (OT) environments within the organization. This role focuses on designing, implementing, and maintaining cybersecurity measures to protect OT assets, collaborating with stakeholders, and supporting incident response and risk mitigation strategies.

- **Connectivity Strategy Implementation:** Adapt and execute Group Sector Cyber-Security strategies within IAPAC factories to establish secure and practical connection standards for edge devices and cloud/data centers, ensuring alignment with local operational realities.
- **Legacy System Modernization:** Design and support deployment of protocol conversion gateways or physical isolation solutions for brownfield assets that do not support modern security protocols, enabling secure digital integration.
- **Standardization of Interface:** Define and maintain unified interface standards (e.g., OPC UA configurations, REST API requirements) to support the seamless integration of Smart Factory modules (such as AGVs, ASRS, and Visual Inspection systems) within the plant network.
- **Digital Factory Project Lifecycle Management:** Participate in the planning phase of new digital factory projects (Security by Design) to ensure newly introduced smart devices and systems comply with the company's OT security baseline requirements.
-
- **Solution Design & Implementation**
  - Define secure configuration and patching strategies for OT systems.
  - Assign OT assets into machine groups and classify secondary security measures (e.g., line segmentation, secure configuration).
  - Create and implement short-term risk mitigation measures for business-critical assets.
  - Determine security classification and group similar assets for targeted protection.
- **Collaboration & Governance**
  - Partner with stakeholders to develop and shape mitigation strategies for cybersecurity threats.
  - Provide input to support incident response processes and facilitate network segmentation to ensure integrity.
  - Maintain cybersecurity governance for special engineering applications in alignment with group sector policies.
  - Act as a central OT cybersecurity contact for plants, business units, and IT.
- **Operational Support**
  - Perform periodic maintenance checks of OT security infrastructure.
  - Identify and assess risks (operational, safety, business) associated with patch implementation.
  - **OT Device Firmware Management:** Support and coordinate

Identificação da vaga
REF93267S

Local
Su Zhou Shi

Nível de liderança
Leading Self

Modalidade de trabalho
Hybrid Job

Pessoa jurídica
ContiTech China Rubber & Plastics Technology Ltd.

firmware upgrades for OT devices (e.g., PLCs, HMIs, Network Switches) to ensure critical security patches and feature updates are applied correctly.
    - Support the rollout of standard OT cybersecurity solutions and coach plant teams on best practices.
- **Technical Leadership**
    - Recommend security products, services, and procedures to enhance OT system architecture.
    - Facilitate the partitioning of systems into zones and conduits, and conduct testing/evaluation of new cybersecurity technologies.
    - Perform integration activities: design, install, configure, test, commission, and handover to OT asset owners.
    - Support implementation and configuration of IT/OT network controls to protect the OT environment.
    - Work with architects to shape security controls, remote access, and overall OT infrastructure architecture.
- **Reporting & Documentation**
    - Responsible for creation and maintenance of OT cybersecurity KPIs.
    - Conduct requirement analysis and document the current OT situation in plants.
- **Digital Factory Support**
    - Responsible for creation and maintenance of OT cybersecurity KPIs.
    - Conduct requirement analysis and document the current OT situation in plants.

Requisitos

- Advanced English proficiency.
- Advanced project management skills, including budget responsibility.
- Expert knowledge in secure edge device network integration, OPC UA/MQTT security concepts, certificate-based network communication, and OT network protocols (Profinet, Ethernet IP, Modbus, OPC UA).
- Advanced understanding of secure middleware communication and OT to IT communication (machine/HMI to SCADA, MES, ERP, Cloud).
- Basic knowledge of Manufacturing Execution Systems (MES) and SCADA systems.

O que oferecemos

We want our employees to do well with us. That's why we offer them not only an exciting job in an international technology group, but also numerous additional offers such as flexible and hybrid working, sabbaticals and other benefits.

Ready to drive with Continental? Take the first step and fill in the online application.

Quem somos

Continental develops pioneering technologies and services for sustainable and connected mobility of people and their goods. Founded in 1871, the technology company offers safe, efficient, intelligent and

affordable solutions for vehicles, machines, traffic and transportation. In 2022, Continental generated sales of €39.4 billion and currently employs around 200,000 people in 57 countries and markets.

The ContiTech group sector develops and manufactures, for example, cross-material, environmentally friendly and intelligent products and systems for the automotive industry, railway engineering, mining, agriculture and other key industries. Guided by the vision of “smart and sustainable solutions beyond rubber,” the group sector draws on its long-standing knowledge of the industry and materials to open up new business opportunities by combining various materials with electronic components and individual services.