Comprehensive OT risk assessments of industrial systems and critical infrastructure

As industrial systems become more connected with non-factory IT, they also become more exposed to cyber threats and vulnerabilities. The cost of industrial business interruptions and the devastation to communities and economies that an attack could generate are high. These are key factors for organisations looking to analyse the potential risks as a basis to update the protection of their industry or critical infrastructure.

We offer you an OT Risk Assessment service for your industrial production or your critical infrastructure.

The security risks are evaluated in production facilities as well as in critical infrastructure and recommendations to mitigate risks are provided. The method used performs a qualitative risk assessment based on the possible impacts, identified threats and vulnerabilities whilst under consideration of the used security controls.

Benefits Summary

- Gain comprehensive risk analysis of OT environment based on business impact and likelihood
- Detailed and prioritised recommendations considering all dimensions people, process and technology
- Risk Assessment adapted to international standards, can be combined with an IT Risk Assessment
- Achieve a business aligned decision basis for your Risk Treatment Plan
OT Risk Assessment in detail

- **Kick-off**
  - Definition of the scope of the OT Risk Assessment based on the most important business processes
  - Identification of the reference points, such as the standard to be applied and the context criteria e.g. likelihood criteria, impact etc.
  - Gathering of useful data to understand the OT architecture, systems and network communications, as well as the existing security controls
    > For example network plans, descriptions of OT systems, processes and responsibilities
  - Missing information will be evaluated via interviews. Optionally the OT Asset discovery Service can supplement the data gathering

- **Data Gathering**
  - Gathering of useful data to understand the OT architecture, systems and network communications, as well as the existing security controls
    > For example network plans, descriptions of OT systems, processes and responsibilities
  - Missing information will be evaluated via interviews. Optionally the OT Asset discovery Service can supplement the data gathering

- **Perform Impact Assessment**
  - An impact assessment will be executed jointly with the asset owner and business responsible during a workshop for the identified OT assets at risk

- **Perform Risk Assessment**
  - The Risk Assessment will be performed based on the identified threats & vulnerabilities, as well as the impact identified to OT systems. The likelihood that adverse events may arise from those threats and vulnerabilities is analysed

- **Results Review Workshop**
  - The results will be reviewed with the customer to ensure all inputs and assumptions are aligned to verify the accuracy of findings
    - Based on the Risk Assessment output for non-tolerable risks, mitigation activities will be discussed and aligned with the customers risk appetite

- **Final Report and Presentation**
  - A final report will be presented to the customer implementing any findings from the Review Workshop. The suggested risk mitigations will be documented in a treatment plan including a roadmap for recommended further activities

**Main deliverables**
- OT Risk Assessment Report and Management Presentation
- Agreed Treatment plan including roadmap for further activities

**Contact us for more information.**