Secura
A BUREAU VERITAS COMPANY

OT Risk Assessment

Now that the frequency of cyberattacks on Operational Technology (OT) is increasing, it is more important than ever to secure your organization's OT environment. Adversaries use various methods to infiltrate networks and cause all kinds of financial damages: either directly by halting or slowing down production, or indirectly through stealing and selling your organization's trade secrets. To reduce the chances of a cyberattack, it is important that possible countermeasures are identified and implemented. Not, or incorrectly, implementing these countermeasures is a risk for your organization.

Why conduct a risk assessment?

A cyber risk assessment assists in structurally determining **which cyber risks are present in your environment**. Only after explicitly identifying these risks, it is possible to understand the effectiveness of (existing) countermeasures. This in turn makes it possible to reason about **new countermeasures**; if they are needed, and their possible effectiveness. Furthermore, assessing the severity of the identified risks enables **deciding** on and **prioritizing** countermeasures, and make an **informed decision** if the costs of implementing them weigh up against the potential consequences.

Moreover, performing a risk assessment will create a complete overview of the **strengths and weaknesses** within your organization. This overview can in turn be used to **improve preparedness** during a cyberattack or prevent one by addressing the identified weaknesses.

Why is an OT-tailored risk assessment necessary?

As oppposed to IT, risks in OT environments do not only affect the **confidentiality, integrity, and availability** of data or processes, but can also impact the facilities' **reliability, performance, and safety**. Furthermore, the different types of **Industrial Control Systems (ICS)**, such as **PLCs, DCSs and SCADA systems** require unique attention as they are the backbone of any OT environment. To correctly assess risks and propose countermeasures in such environments, these differences should be taken into consideration.

Secura's approach to OT risk assessments

Secura uses its own proprietary asset-driven risk assessment methodology named **"Quantitatively Assessing Risk in Operational Technology" (QAROT)**. This methodology complies with **IEC 62443-3-2** and incorporates the strengths of **MITRE's ATT&CK for ICS and ISO 31010**. Combining these standards enables us to do risk assessments beyond just compliance. Together with our clients we define the IEC 62443-3-2-required **target security levels**, on which we systematically base the assessment objectives. QAROT furthermore incorporates other standards from the IEC 62443 family, such as -3-3 and -4-2, to give coherent and **actionable advice** based on the fundamental security requirements that these standards describe. Furthermore, QAROT makes use of Secura's publicly available **Operational Technology Cyber Attack Database (OTCAD)** when establishing the severity of identified risks.

QAROT methodology

QAROT uses a top-down approach to **identifying and assessing risks**: it derives applicable countermeasures by considering all assets within an OT environment. These countermeasures are based on ATT&CK for ICS and are combined with IEC 62443-3-3 and -4-2 to objectively assess their implementation and effectiveness within the system under consideration. This combination allows Secura to structurally **identify potential shortcomings** and the **risks** that they pose. The assessment starts by creating a **zone & conduit diagram** based on the organization's network drawings and asset inventory. The diagram contents are discussed together with the client during a workshop to ensure that they correctly represent the assessed environment. In consecutive workshops we determine together with our client the **impact of possible adversary goals**, and we establish the **achieved security levels** of existing asset- and zone/conduit-based **countermeasures**.

Results

For each of the shortcomings identified during these workshops, Secura will provide **tailored and actionable advice o**n how to address them. Through QAROT's proprietary calculations the identified risks are quantitatively scored and ranked, which helps in the **comparison and prioritization**. Moreover, by using IEC 62443's fundamental requirements, the sufficiently implemented mitigations are categorized so the client can quickly see compliance within different cyber security areas. We deliver these overviews, the **identified risks** including our **recommendations**, and a **follow-up plan** in a report which we will present in a **close out meeting**.

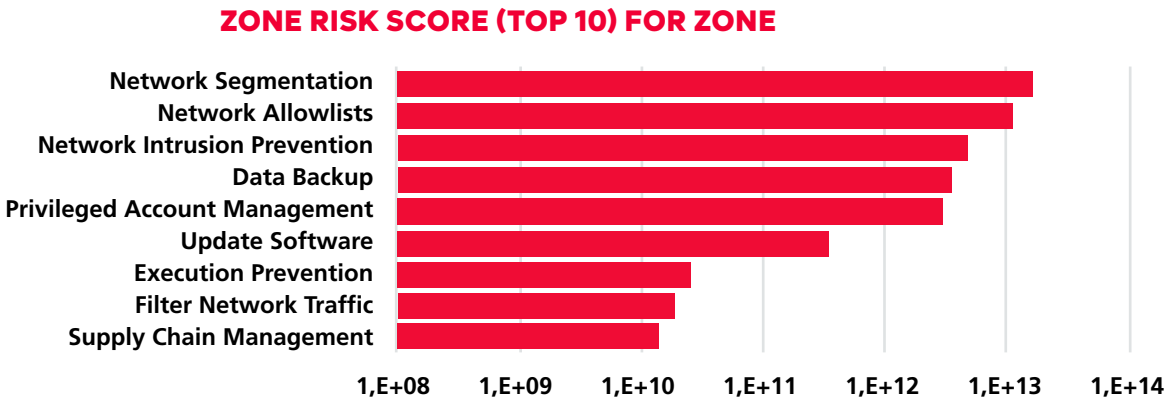

Figure 1. Example of quantitative risk score overview

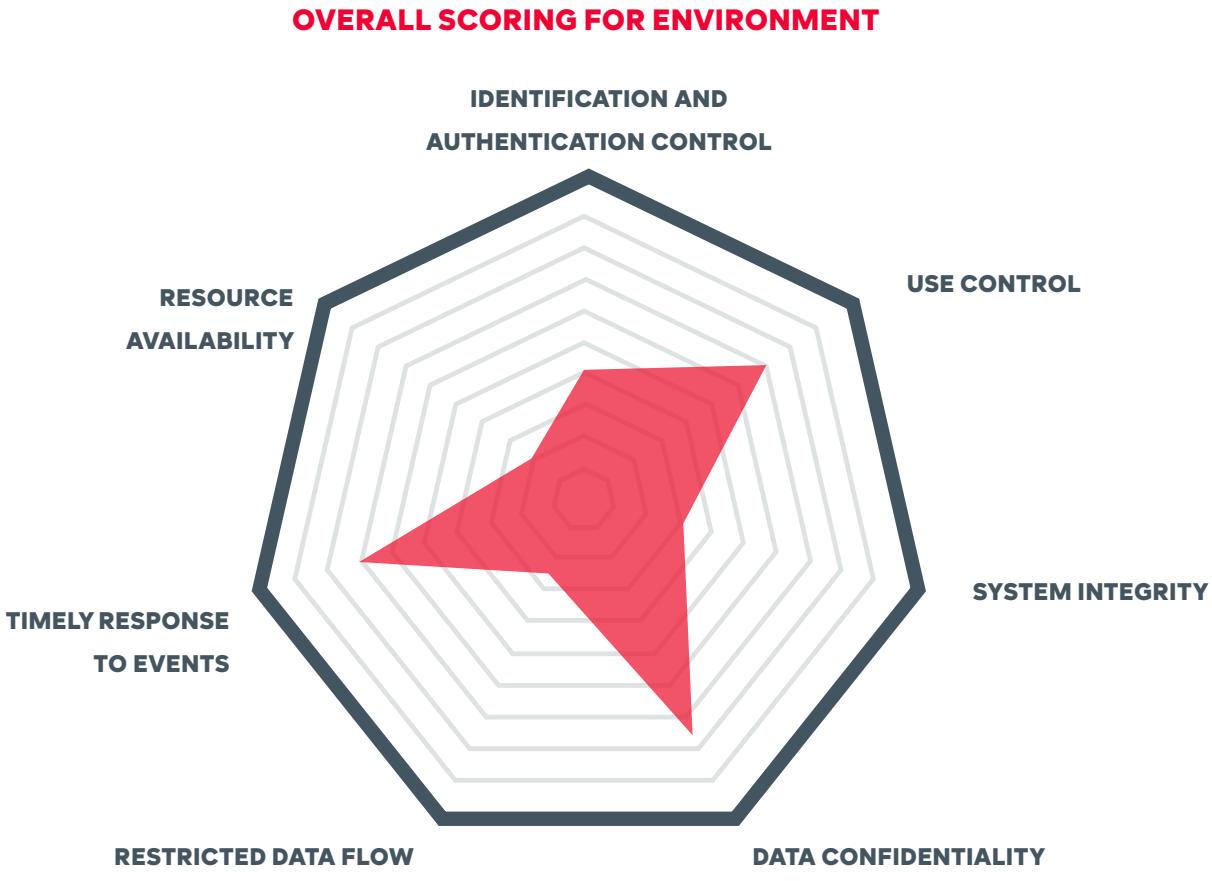

Figure 2. Example of IEC62443 compliance scoring

Why Secura?

Secura believes it is important that OT security is addressed to the highest level achievable, considering the impact a cybersecurity attack may have on health, safety and the environment. We support organizations across various industries in their journey to improve their OT security. Secura is experienced in delivering security and visibility for some of the world's most complex OT networks including Europe's largest manufacturing facility and other various key players in critical infrastructure. We guide organizations in **understanding risks, gaps and vulnerabilities in industrial control systems** by using a layered approach considering the **NIS and NIST compliance frameworks** for critical infrastructure. The value of Secura comes forth in **approaching OT security from well-known and internationally recognized ICS standards** required by the regulations of various countries or distinct areas in the world.

Not only does Secura understand what is required by world's most known and accepted ICS standards, but our **team of experts also possesses the necessary engineering understanding to identify and interpret the impact of vulnerabilities** in distinct OT environments consisting out of Stand-Alone, Distributed and/or Supervisory Control and Data Acquisition systems. Secura **identifies threats and risks** to OT systems by continuously investing in the training and education of its dedicated consultants.

Secura requires that its consultants have the right **cybersecurity and engineering knowledge** including but not limited to control loops, plant organization (as per ISA-88), architecture, data flows, connectivity and commonly used diagrams such as process flow diagrams and piping and instrumentation diagrams to identify specific cyber risks related to PLCs, PACs, RTUs and Safety Instrumented Systems (SIS). The cybersecurity and engineering understanding of our consultants bring them at the forefront of OT security in the world translating to understanding the concerns of our clients and providing state-of-the-art solutions based on well-recognized standards for each distinct area of the world.

Secura
A BUREAU VERITAS COMPANY

Interested?

Contact us today:

Follow us:

+31 88 888 3100
info@secura.com
secura.com

BUREAU VERITAS 1828
BUREAU VERITAS
Shaping a World of Trust