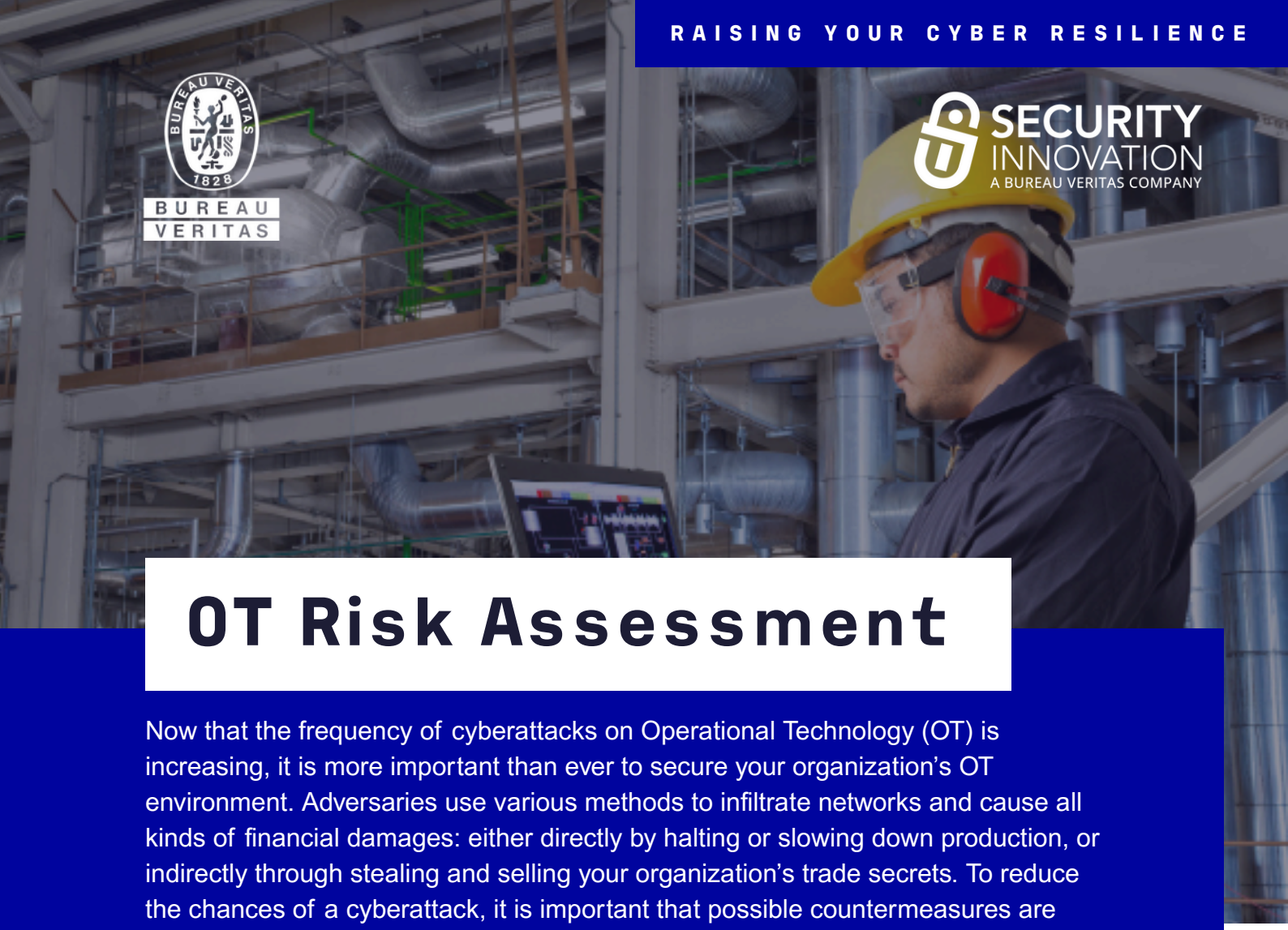

OT Risk Assessment

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. Failing to implement these countermeasures, or implementing them incorrectly, poses a risk to 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 is it possible to understand the effectiveness of existing countermeasures. This in turn makes it possible to consider **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 opposed 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.

Security Innovation's approach to OT risk assessments

Security Innovation 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—a Bureau Veritas Company'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 Security Innovation 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, Security Innovation will provide **tailored and actionable advice** on 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**.

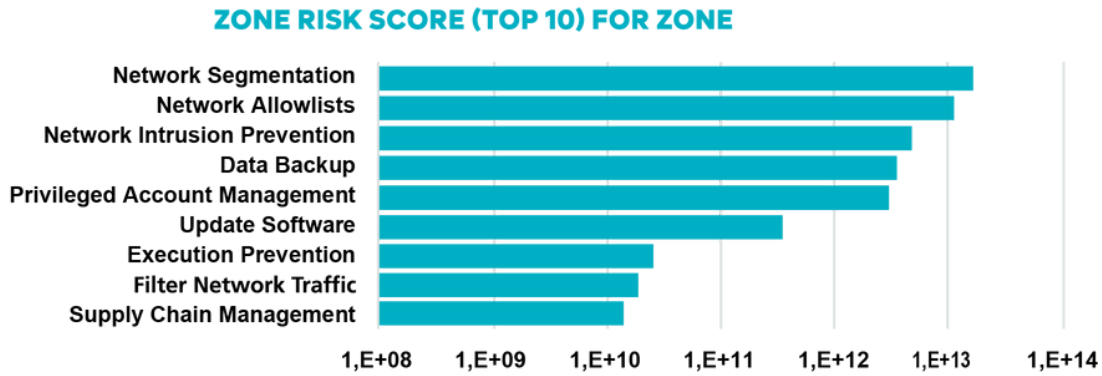

Figure 1. Example of quantitative risk score overview

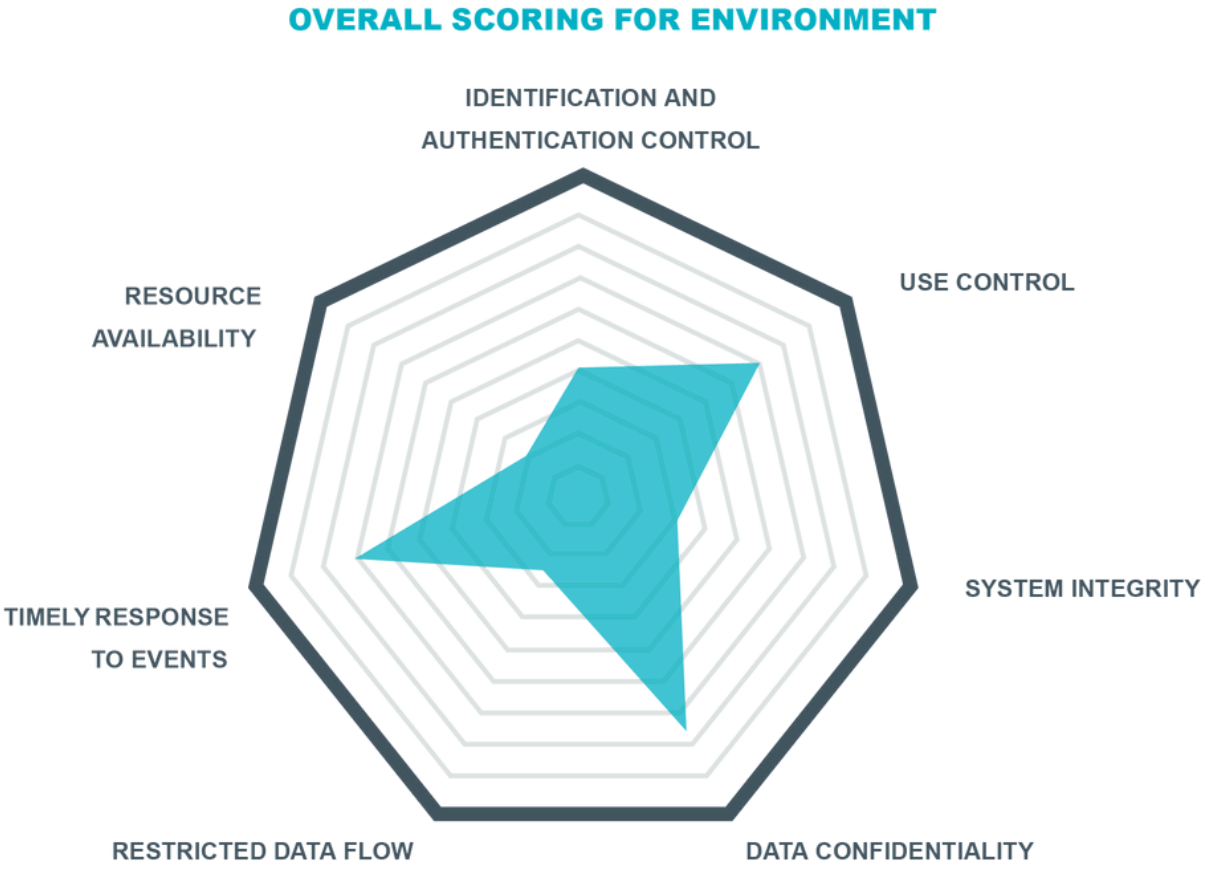

Figure 2. Example of IEC62443 compliance scoring

Why Security Innovation?

Security Innovation 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. Security Innovation 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 Security Innovation 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 Security Innovation understand what is required by the 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. Security Innovation identifies threats and risks to OT systems by continuously investing in the training and education of its dedicated consultants.

Security Innovation 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). Our consultants' cybersecurity and engineering expertise places them at the forefront of global OT security. This enables them to understand our clients' concerns and provide state-of-the-art solutions based on well-recognized standards tailored to each region of the world.

SECURITY INNOVATION
A BUREAU VERITAS COMPANY

About Security Innovation / Bureau Veritas

Security Innovation is a leader in software security, providing comprehensive assessment solutions to secure software from design to deployment, across all environments, including web, cloud, IoT, and mobile. Leveraging decades of expertise and as part of Bureau Veritas, a global leader in Testing, Inspection, and Certification, we seamlessly integrate world-class security into development processes, safeguarding the way companies build and deliver products.

Security Innovation is a Bureau Veritas company. Bureau Veritas (BV) is a publicly listed company specialized in testing, inspection and certification. BV was founded in 1828, has over 80,000 employees and is active in 140 countries.

BUREAU VERITAS 1828

Interested?

Contact us today to start raising your cyber resilience.

sisales@securityinnovation.com

+1 877 839 7598

securityinnovation.com