Risk Management

Industrial-tailored Cyber Risk Assessment for Safe Digitalization

The OTORIO industrial risk assessment process is tailored to production floor requirements. We incorporate OT threat modeling, regulation requirements, and the management risk appetite into a cyber maturity road map. Our assessment teams utilize national cyber expertise to identify and prioritize the industrial organization's attack surfaces, according to attack vectors, ease of exploitation, and potential impact on productivity, safety, and reliability.

Safe Industry 4.0 Digitalization

The OTORIO Risk Assessment is a comprehensive and realistic approach to evaluating the effectiveness of organizational production cyber resilience. It assesses Industry 4.0 benefits together with security and risk cost.

The outcome of the assessment is a prioritized potential-impact maturity roadmap, which can be used to significantly reduce the ease of an attacker breaching the OT network and carrying out a successful attack. The assessment report provides a customized mitigation plan, starting with the short-term improvement of the organizational and production floor security postures. OTORIO assessment teams, together with the customer's designated operational POC, also design a long-term cyber maturity plan, assisting the organization to safely continue its digitalization journey.

OTORIO's IT-OT Penetration Test

In today's ever-changing digital environment, traditional static modeling is simply ineffective. Hands-on Penetration Testing (PT) provides an organizational cyber threat "reality check", which can be used to prioritize mitigation processes and resource allocation. Based on unmatched national military experience in hacking mission critical infrastructures, OTORIO's teams have developed a tailored approach to industrial Penetration Testing. Test results are presented in a concise report which, in addition to identifying technical attack vectors in the organizational security process, also relates them to the business process, thus offering a prioritized, effective, and efficient mitigation road map.

Benefits of the OTORIO OT Risk Assessment

- Performs a comprehensive IT-OT converged environment assessment, including network, assets and processes
- Produces a customized maturity roadmap to safe digital growth
- Produces an assessment report showing compliance gaps, with a clear and concise plan to achieve compliance (NIST, IEC 62443, NERC CIP, IMO)
- Uses world-leading expert hacking teams to perform realistic red team assessments (Penetration Testing) that complement customary assessment paperwork, and create a representation of the organization's actual security posture.

Use Cases

- Identify and prioritize cyber risks into actionable items, to ensure production continuity
- Perform compliance gap analysis, as part of the organizational GRC with organization-specific and public regulations

- Use mitigation controls to prevent potential attacks by anticipating attack vectors with non-obtrusive attack scenarios
- Create a tailor-made cyber maturity road map to enhance organizational cyber resilience

OTORIO - a global leader in safe Industry 4.0 digitalization

OTORIO is an advanced Managed Security Service Provider, founded by Israeli defense cybersecurity experts, partnered with a leading global plant engineering group. OTORIO's unparalleled forward-looking products and services are delivered by world-leading "special forces" talents, leveraged by proprietary cutting-edge technology.

OTORIO's solution counteracts current and future industrial cyber risks, ensuring safe Industry 4.0 digitization, as an integral part of the operational life cycle. OTORIO's broad offering addresses the different stages and challenges a traditional industry faces when setting out on the journey of digital transformation.

Diagram

Threat Source -- with characteristics (capability,intent and targeting, for adversarial threats)

initiates

Threat Event -- with sequence of actions, activities, or scenarios

exploits

Vulnerability -- With severity in the context of pervasive predisposed conditions, and security controls planned/implemented with effectiveness

causes

Adverse Impact -- with risk a combination of impact and likelihood

produces

Organizational Risk -- To organizational operations (mission, functions, image, reputation), organizational assets, individuals, other organizations, and to the country