Industrial-tailored Cyber Risk Assessment for Safe Digitalization

The OTORIO industrial risk assessment process is tailored to production floor requirements, incorporating OT threat modelling, 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, threat modeling assessment, ease of exploitation, and potential impact on productivity, safety, and reliability.

Safe Industry 4.0 digitalization

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 costs. The outcome of the assessment is a prioritized, potential-impact maturity roadmap, used to significantly reduce the chances of attackers breaching the OT network and executing successful attacks. This 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 Point-of-Contact, also design a long-term cyber maturity plan, assisting the organization in its safe, digitalization journey.

OTORIO's IT-OT penetration test

In today's ever-changing digital environment, traditional static modelling is simply ineffective. Hands-on Penetration Testing (PT) provides an organization with a cyber threat "reality check", used to prioritize mitigation processes and allocate resources. Based on unmatched national military experience in hacking mission critical infrastructures, OTORIO's teams have developed a tailored approach to industrial Penetration Testing.

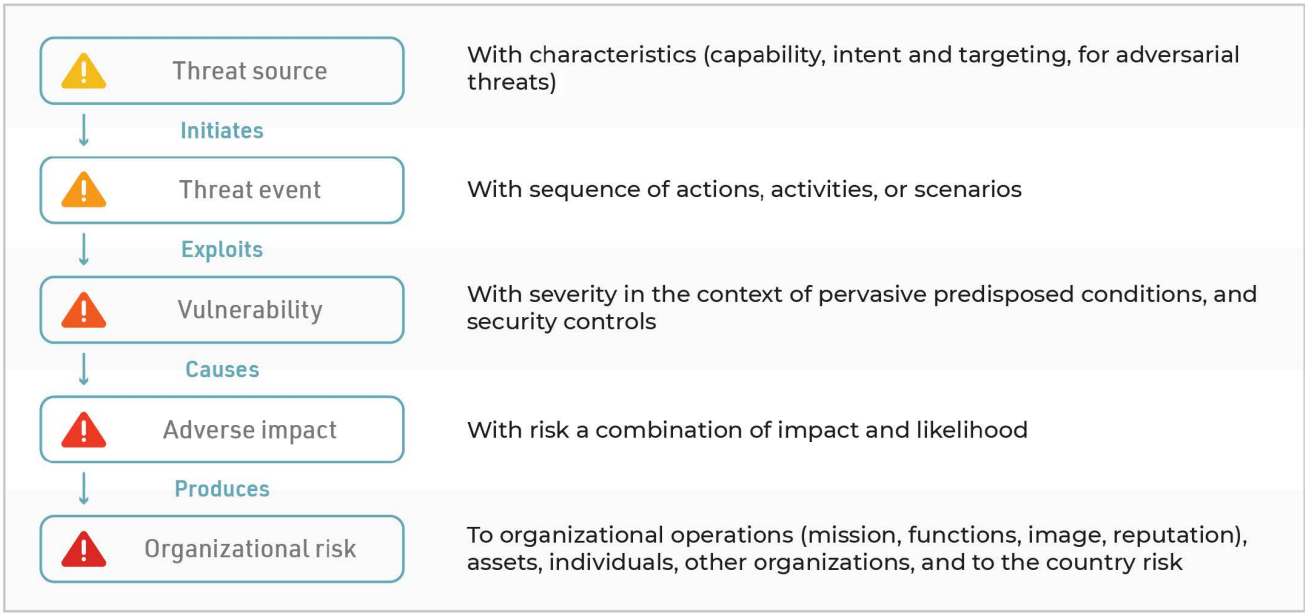
Test results are presented in a concise report which identifies technical attack vectors in the organizational security process and relates them to the business process. This provides the end user with an effective mitigation road map.

OTORIO's IT-OT penetration test

- Performs a comprehensive IT-OT converged environment assessment, including network, assets, and processes
- Produces a customized maturity roadmap for safe digital growth
- Generates an assessment report showing compliance gaps, with a clear and concise plan to achieve regulation compliance (e.g., NIST, IEC 62443, NERC CIP, IMO)
- Uses world-class, leading expert hacking teams to perform realistic, red team assessments (Penetration Testing) that complement customary assessment paperwork, and create an estimate 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 governance, risk management, and compliance (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 - Industrial-native cyber and digital risk-management solutions provider

OTORIO is an advanced Managed Security Service Provider, founded by Israel i defense cybersecurity experts, partnered with a leading global plant engineering group. OTORIO's unparalleled forward-looking products and services are delivered by world-class "special forces" talent, 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.