One Pager

Times are Changing

Traditional industries worldwide are undergoing a technological transformation, often referred to as Industry 4.0, smart production, or industrial digitalization. Along with the promising business opportunities this brings, the increasing organizational IT/OT convergence exposes organizations to new cyber risks. Industrial cyber risks can potentially lead to production downtime, loss of intellectual property, physical damage, loss of reputation, and even loss of life.

These risks have in common that even standard procedures for updating and patching vulnerable ICS now involve great complexity.

As the threat landscape continues to evolve, industries must embrace a comprehensive and continuous approach to cybersecurity in order to enjoy the benefits of digitalization. This approach should include ongoing monitoring, and risk prioritization according to potential risk impact and remedy costs. This continuous process should proactively manage and reduce cyber risks, allowing better up-time, productivity, safety, and new smart production opportunities.

OTORIO - an industrial-native, digitally-born company

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.

End-to-end, we're all in

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. It addresses the management of cyber risks in operational processes, as well as interlinked risks in the supply chain. OTORIO's distinctive offering includes variety of service modules, such as:

- a strategic digital risk governance framework
- comprehensive security and risk assessment, along with program maturity development
- OT Penetration Testing (PT), which provides an organizational cyber threat "reality check"
- Ongoing and continuous advance cyber risk management – Industrial Security Operation Center (OT SOC), Cyber Threat Intelligence (CTI), and unparalleled Security Orchestration, Automation and Response (SOAR)
- IT-OT converged Incident Response (IR) and mitigation services

The orchestration and automation of operational security tasks results almost immediately in the ability of the organization to reduce the potential impact of inevitable incidents. OTORIO's SOAR platform uses an intuitive operational User Interface (UI), and is operated by production operational personnel, based on their inherent expertise, with minimal required competence upskilling. We are engaged throughout the entire security process at different touch points. OTORIO enables modern industries and manufacturers safe and sustainable growth without the additional risks associated with Industry 4.0 vulnerability to cyber-attacks.

About

OTORIO was founded in Israel as a JV between Israeli defense professionals and a leading Austrian plant engineering group. This combination brings together over 160 years of industrial engineering and operational technology knowhow for leading industrial customers, in a variety of verticals.

Yair Attar Co-founder and CTO, Mr. Yair Attar is a senior cybersecurity expert with diverse experience in various aspects of cybersecurity, incident response, and threat hunting.