

Industrial IT-OT Converged Managed SOC

OTORIO's OT SOC service fundamentally enhances plant security operations effectiveness, efficiency and consistency. The IT-OT converged managed SOC continuously monitors the production floor, preemptively scans for digital security gaps, and then highlights and prioritizes actionable risk reduction measures according to their potential business impact.

As an industrial-tailored SOC, it can have a distinct role in maintaining the safety, reliability, and productivity of operational processes. The service leverages deep-domain expertise with proprietary powerful technologies. It orchestrates and automates threat intelligence management, security event monitoring, and incident response processes. The OTORIO SOC enables information sharing and coordination of activity between IT and OT stakeholders, as well as operational impact review for executive management

Safe Industry 4.0 Digitalization

Industry 4.0 digitalization, essential to organizational business growth, introduces ever-growing cyber-related challenges. Security Orchestration, Automation and Response (SOAR) technologies that are integral to the core of the OTORIO IT-OT SOC, enable faster and safer responses to digital operational challenges. They can lead to a proactive reduction in cyber-related losses, based on existing operational personnel and reasonable investments, while also leveraging existing organizational solutions. In today's increasingly complex operational digital environment, utilizing existing solutions through orchestration, automation and enforcement are far more effective than integrating best of breed security controls.

Benefits of the OTORIO OT Risk Assessment

- Native IT-OT converged SOC, monitors OT assets and vertically-agnostic processes
- Forward-looking sources and technologies-rich security orchestration, automation and enforcement driven solutions, proactively counteracting current and future industrial cyber risks
- OT SOC operated by world-leading "special forces" talents, with unique and extensive deep-domain expertise, leveraging proprietary cutting-edge technology combined with in-place security mechanisms
- Decision making support with actionable, industrial risk prioritization
- Ensures fast, focused, comprehensive, and effective operational remediation and mitigation processes and playbooks
- Customized operational and integrated cyber threat intelligence

OTORIO OT SOC Operation Modes

The OTORIO Managed OT SOC can be implemented as a standalone OT SOC, or interlinked with an IT SOC and SIEM. It allows flexible operation with various operation modes such as an All-in, Handshake, and Co-Operated. For remote operation, the remote connection and access to the SOC is protected by OTORIO's unique, secured solution.

- All-in - OTORIO takes full responsibility for SOC operations – T1, T2 and T3.
- Handshake - split responsibility between customer operation (T1) and OTORIO support (T2 & T3).
- Co-Operated - OTORIO (T2 & T3) and a partner (T1)

OTORIO Incident Response (IR) Service

No organization is 100% immune to cyber-attacks, and once an incident emerges, time is critical to reduce the potential impact, and return to normal operations. OTORIO's IR teams are trained to promptly restore the OT network operational integrity, without sacrificing safety conditions. Based on an unmatched national military experience in defending mission critical infrastructures and industrial engineering knowledge, OTORIO's teams have developed a tailored industrial Incident Response approach:

- Take full responsibility immediately after an attack in order to contain and remove the threat
- Find the root cause of the problem
- Investigate back to the source of the attack (identifying who and why)

Use Cases

- Outsource OT real-time risk monitoring and management
- Utilize centralized situational industrial risk management – fuse global plants and processes
- Merge current IT monitoring methods with managed OT monitoring and management
- Orchestrate and automate diverse OT data sources
- Promptly identify cyber attacks by remote, and on-site Incident Response expert teams

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.