OTORIO

Expertise At Your Service

Industry 4.0 is here, delivering smart technology that enables the automation of traditional manufacturing and industrial practices. But the digital transformation exposes machines, processes, and data to cyberattacks.

OTORIO world-class industrial cybersecurity experts offer tailored services powered by RAM^2, OTORIO's digital and cyber-risk management system. The services enable industrial companies to safely attain the benefits of Industry 4.0 in the face of cybersecurity risk and exposures.

By engaging with OTORIO Services, companies can accurately assess their technologies, people, and processes, and advance toward the most effective levels of cyber resilience and incident response.

Comprehensive Services Approach

OTORIO offers a full range of services at four levels of engagement:

- **Discovery.** One-off focused assessment of vulnerabilities, exposures, and compliance gaps. The result is easy-to-adopt recommendations for essential improvements to the security posture.
- **In-Depth Assessments.** Comprehensive studies covering a wide risk surface, including adversary simulations, architecture reviews, risk assessments, and human-factor evaluations, leading to a dramatic increase in operational cyber resiliency. Assessments include a non-intrusive breach-and-attack simulation on a digital twin of your OT network.
- **Preparedness.** Significant improvement of the effectiveness of the company's security operations, and reduction of human errors. The result is empowered employees and efficient SOC operations.
- **Response.** Evaluation of incident response capabilities with timely and effective reaction to incidents whenever they occur. At the end of the process, your team will be ready to deal successfully with the next cyberattack.

Highlights

- World-class OT cybersecurity expertise at your service
- Thorough assessment of current OT cybersecurity posture
- Planning and improved OT cybersecurity, compliance, governance, and adoption of best practices
- Penetration testing and adversary simulations
- Examination and tailoring of OT Policies for maximum security and resiliency
- Accurate prioritization of spend and budget planning
- Rapid Incident Response team on call

DISCOVERY

- Minimal engagement
- Immediate results
- Gain visibility of gaps and exposures

IN-DEPTH ASSESSMENT

- Comprehensive security posture visibility
- OT cybersecurity by-design

PREPAREDNESS

- Improved security operations
- Reduce human-errors

RESPONSE

- Optimize recovery time
- Efficiently respond to incidents

DISCOVERY

Attack Surface Discovery
Implementation of OTORIO's passive reconnaissance process for discovering company assets as they would be seen by a potential attacker without exposing any company assets. Mapping of all Internet-facing services to company assets, simulating worse-case attack scenarios.

Compliance Gap Assessment
Examine how well the environment is aligned with industrial cybersecurity standards and compliance. Review of the results to determine the processes and best practices to achieve compliance.

Scenario-Based Security Assessment
Review of the current cybersecurity process based on specific scenarios of ransomware, focusing on remote access for third parties and employees, and logging and monitoring.

Vulnerability Scanning
Identifying and prioritizing vulnerabilities in the operational network. At the end of the process, OTORIO provides a list of IP addresses prioritized by the ease of discovery along with the complexity of exploitation and the severity of potential impact.

IN-DEPTH ASSESSMENT

Penetration Test
Penetrating the customer's external network, leveraging real-world attacker tactics, techniques, and procedures. Demonstrating how attackers can reach the OT environment. Test results are presented in a focused report, prioritizing the identified attack vectors according to their potential business impact. Using a step-by-step technical description of the attack vectors, the report describes an effective and efficient mitigation roadmap.

Red Teaming
Full-scope, multi-layered breach-and-attack simulation on a digital twin of your OT network designed to measure how well the company's people, networks, applications, and physical security controls can withstand an attack from a real-life, adversary. The goal-based approach measures security readiness and awareness, ultimately assessing security planning and preparation, and the ability to cope with specific threats.

Social Engineering
Assessment of the effects of a broad range of malicious activities accomplished through human interactions, using psychological manipulation to trick users into making security mistakes and giving away sensitive information. Determination of how well company employees are prepared to identify and ward off social engineering attacks.

Automation Review
Architecture evaluation along with a review of authentication, authorization, accounting, cyber processes, connection to third parties and to the customer. Designed for vendors who wish to review the cybersecurity implementation in automation solutions.

Architecture Review
Review of the existing security program, performing a security risk assessment and evaluating the OT environment for existing protection, detection, and response capabilities. The review includes a careful analysis of the security architecture, firewall policies and rules, and segmentation in the OT network. Based on the review, specific recommendations for improvement are delivered.

PREPAREDNESS

Awareness Training
Employee training delivered by OTORIO global experts makes sure that all personnel recognize and understand organizational and personal cyber threats, empowering them with the basic tools and processes to help reduce the effects of always-present cyber threats.

OT SOC-as-a-Service
Next-generation IT/IoT/OT SOC services fundamentally enhance the effectiveness, efficiency, and consistency of OT security operations. OTORIO's OT cyber experts continuously monitor the operational network and help customers to combat cybersecurity threats that target industrial networks. Companies can take advantage of OTORIO experts, expertise, and facilities to create and staff their SOC or extend their own SOC capabilities.

Threat-Hunting
A proactive investigation that looks for dormant malware and malicious activity in the OT network. Always equipped with the latest signatures of recent OT-related malware, and based on the company's architecture and critical assets, the OTORIO team proactively identifies and prevents threats to trademark secrets, crown jewels, and operations before damage can be caused.

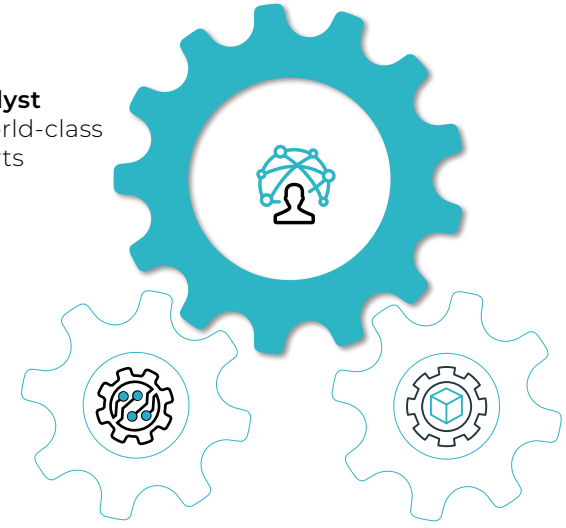
Security Policy Creation
Examination and tailoring of OT policies to make sure they address cybersecurity challenges. The service covers a variety of policies including Security Policies, Identity and Access Management, Backup Procedures, Supplier Management, Physical and Environmental Security, Compliance, and more.

RESPONSE

Incident Response Readiness Assessment
Assessment of the company's readiness to deal with the next inevitable cyber attack. Provision of tailor-made security best practices and incident management recommendations.

Incident Response-as-a-Service
This on-call or retainer service helps companies quickly respond to and recover from cyber-attacks, especially in industrial environments. OTORIO IR experts promptly remove attackers from the environment and prevent their return. Data is recovered and operations are returned to proper function. Lessons learned are implemented to continuously improve cybersecurity and IR, and to prevent future security incidents.

Personal Cybersecurity Analyst
Tailor-made services from world-class industrial cybersecurity experts



Automated Data Collection
Zero interference to your operational environment

Cyber Digital Twin platform
Market-leading OT-centric digital cyber risk management solution

OTORIO Service Programs

Program	Description	Benefit	Individual Services
Discovery	Focused assessment of vulnerabilities using advanced, unique tools developed by OTORIO along with world-class experts	Easy-to-adopt recommendations for significant improvements to security posture	· Attack Surface Discovery · Compliance Gap Assessment · Scenario-Based Security Assessment · Vulnerability Scanning
In-Depth Assessments	Comprehensive evaluations, including adversary simulations, architecture reviews, risk assessments, and human-factor appraisals	Dramatic increase in operational cyber resiliency	· Penetration Testing · Red Teaming · Social Engineering · Automation Review · Architecture Review
Preparedness	Across-the-board appraisal of the effectiveness of current cybersecurity operations and human factors along with comprehensive recommendations for improvement	Improved alertness and readiness across the company and staff to deal with the never-ending barrage of cyber threats	· Awareness Training · OT SOC-as-a-Service · Tailored Threat-Hunting · Security Policy Creation
Response	Assessment of the current state of incident response and IR services with uncompromising recommendations that enable rapid response, business recovery, and implementation of lessons learned learned	Rapid, effective, and complete response to inevitable OT cyber incidents, and continuous improvement	· Incident Response Readiness Assessment · Incident Response-as-a-Service

About OTORIO

OTORIO delivers next-generation OT security and digital risk management solutions that ensure reliable, safe and efficient industrial digitalization. The company combines the professional experience of top nation-state industrial cybersecurity experts with cutting edge digital risk management technology to provide the highest level of protection to the manufacturing industry.