RAM²

Risk assessment monitoring & management

Industrial-tailored Security Orchestration and Automation Platform

The Risk Assessment Monitoring & Management platform, RAM², is OTORIO's unparalleled industrial-tailored Security Orchestration, Automation and Response (SOAR) platform. The RAM² offers industry-first comprehensive, centralized, simplified and automated industrial cyber risk management solution.

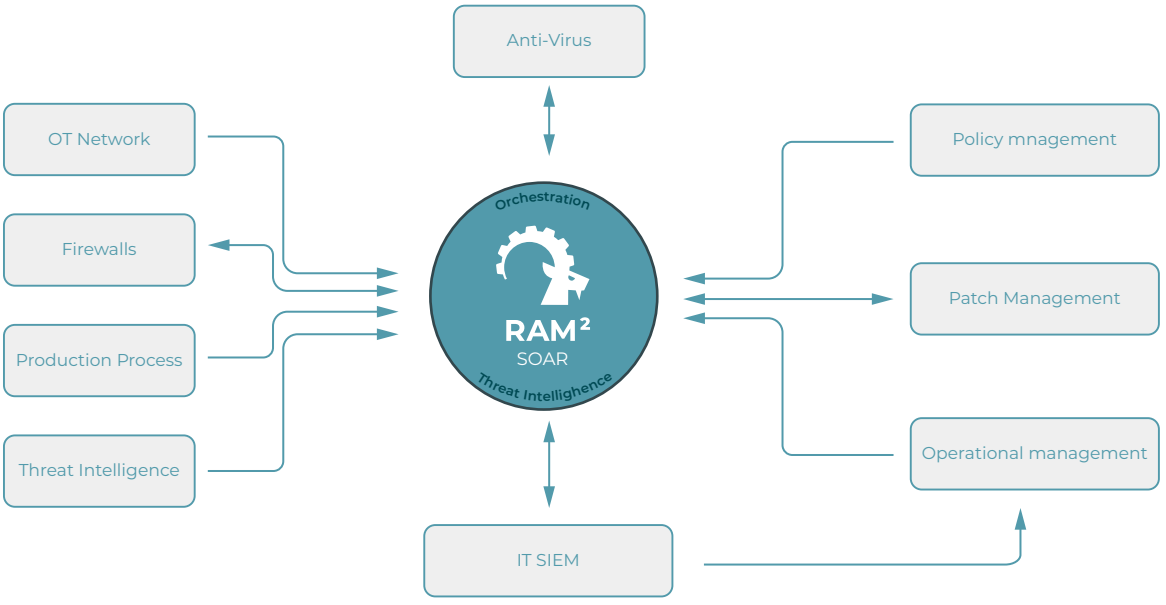
OTORIO

RAM² for On-Going Operations

RAM² easily integrates a variety of production floor data sources (e.g. OT, IT, security logs and network data) and provides actionable common view based on powerful machine analytics. The customized dashboard supports Business Information Security Officer (BISO) and operations' engineers to carry their daily tasks. By presenting on-going focused compliance status and comprehensive operational OT-IT converged asset view, RAM² enables continuous cyber risk management.

Safe Industry 4.0 Digitalization

OTORIO's industrial security orchestration and automation platform meets the upcoming industry 4.0 challenges. RAM² guides you safely through network complexity caused by distinct layers and assets diversity, orchestrates and automates complex and exhausting manual procedures and unifies a variety of management platforms (e.g. OT, IT and security) into a centralized coherent, simple and holistic OT network view.
Ongoing identifying risks and their potential operational impact enables real-time actionable reporting for the different stake holders. By continuously highlighting compliance and organizational policy gaps with industry-relevant regulations (NIST, ISA/IEC, NERC-CIP, IMO, etc.), RAM² decision-making-support maintains the safe digitalization transition with a prioritized, preemptive and effective security operation process.



IT-OT Security Orchestration and Automation

Orchestration and Automation of operational security tasks result in immediate organizational ability to prioritize action and reduce the potential impact of inevitable incidents. OTORIO's SOAR platform uses an intuitive industrial User Intereface, enabling easy operations by production operational personnel with their own knowledge base.

- Industry-first OT security orchestration and automation platform
- Continuous management, qualification and remediation of production cyber risks
- Plan, monitor and enforce segmentation between assets and zones
- Unified, centralized and holistic OT network view
- Simplified prioritization of operations and supply chain risks
- Improved production resiliency, efficiency and consistency
- Continuous compliance assessment of industry relevant regulations and organizational policies
- Decision supporting tools integration; Threat intelligence, known vulnerabilities and patch impact predictions.
- Preemptive attack graph analysis engine

Use Cases

- Continuous comprehensive operational OT-IT converged asset visibility and actionable cyber risk management
- Automating exhausting manual processes for improved effectiveness and efficiency
- Prioritize resource allocation according to potential impact
- On-going focused compliance and organizational policies status

OTORIO - a global leader in safe Industry 4.0 digitalization.

OTORIO is an industrial-native advanced Managed Security Service Provider, founded by Israeli defense cyber security experts partnering with global leading 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 upcoming 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.

OTORIO

OTORIO

www.otorio.co | info@otorio.co

SPOT

Suply chain vulmerability management

Comprehensive supply-chain cyber risk management

OTORIO's Supply-chain Pre-installed OT cyber risk discovery tool, is an offline portable platform, uniquely tailored to be operated by production-floor personnel.

The spOT enforces supply-chain vendors compliance to relevant regulations and organizational policies and preemptively identifies stealthy cyber vulnerabilities and operational misconfigurations.

OTORIO

Tighter Production Floor Integration Control

spOT enables Business Information Security Officer (BISO) and operational teams a tighter control over the production floor.
The spOT scan is based on best practices, open source and proprietary researched vulnerabilities. The platform's proprietary, industrial-tailored scan engine was developed by world-leading cyber and engineering experts to enable safe OT integrations of lines, machines and assets into the production floor.

Safe Industry 4.0 Digitalization

Introducing a new line, machine or other asset into the production/process network is not straight forward process and risk-free in today's cyber threat landscape.
Besides potential impact on production and business continuity, the new insertion must be confirmed to meet organizational and regulatory policies.
Early discovery of misconfiguration, outdated firmware or protocol, unnecessary communication, policy deviations, or hidden malware, is critical to policy adherence. Exhausting manual procedures in a limited-resource procedure prevents production floor personnel from attending easily fixed cybersecurity risks before they impact production. When manual verification is time consuming and extends the machine introduction cycle period, the spot, being an automatic, fast and simple scanning tool is a powerful business driver.

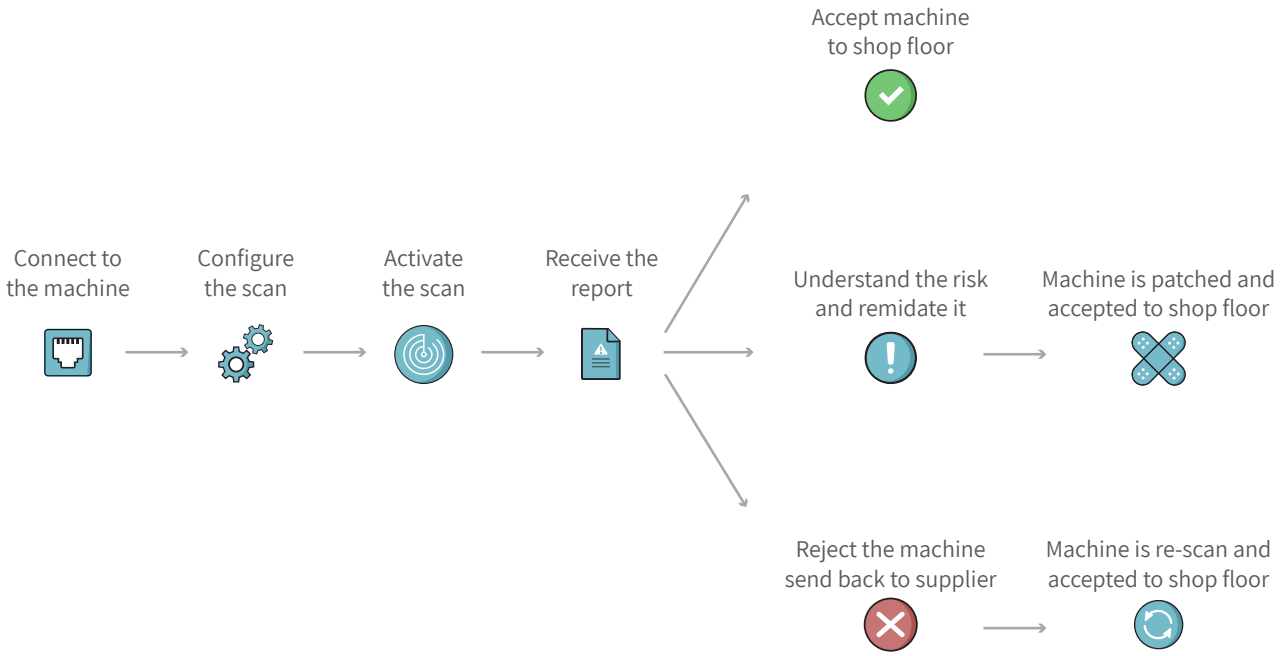
spOT Benefits

OTORIO's spOT delivers automatic threat and vulnerability reports as well as remediation guidelines, based on best industry practices and unique threat intelligence incorporation. The spOT reporting capabilities assist in decision making for enforcement of both proprietary and industry regulated policy and compliance, as well as maintaining an ongoing vendor risk scoring history.

- Automatic, fast and industrial intuitive supply-chain vulnerability assessment
- Simplified supply-chain offline assessment for pre-installed IT-OT assets by production on-site personnel
- Pre-introduction OT inventory management and baseline configuration enforcement
- Supervise, verify and collect vendor-based operational-related statistics history
- Automatically generated report significantly speeds up a new machine, cell or line acceptance cycle into the production floor
- Easily integrated with existing asset management and patch management tools and allows secure patch download and verification.

Use Cases - reporting types

- Outdated and vulnerable firmware or operation system
- Policy and compliance deviation
- Weak or default credentials
- Vulnerable protocols and implementations
- Compliance with vendor best practices and accompanying recommendations
- Stealthy malware



OTORIO - a global leader in safe Industry 4.0 digitalization.

OTORIO is an industrial-native advanced Managed Security Service Provider, founded by Israeli defense cyber security experts partnering with global leading 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 upcoming 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.

OTORIO

www.otorio.co | info@otorio.co

OTORIO
Industrial cyber risk management solutions

Industrial-tailored Cyber Risk Assessment for Safe Digitalization

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

Safe Industry 4.0 Digitalization

OTORIO Risk Assessment has a comprehensive and realistic approach to evaluating the effectiveness of the production cyber resilience. It assesses industry 4.0 benefits together with security and risks costs.
The outcome of the assessment is a potential-impact prioritized maturity roadmap, significantly reducing the ease of an attacker breaching into the OT network and carrying out a successful attack. The 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, design a long-term cyber maturity plan, enabling the organization to safely continue its digitalization journey.

OTORIO's IT-OT Penetration Test

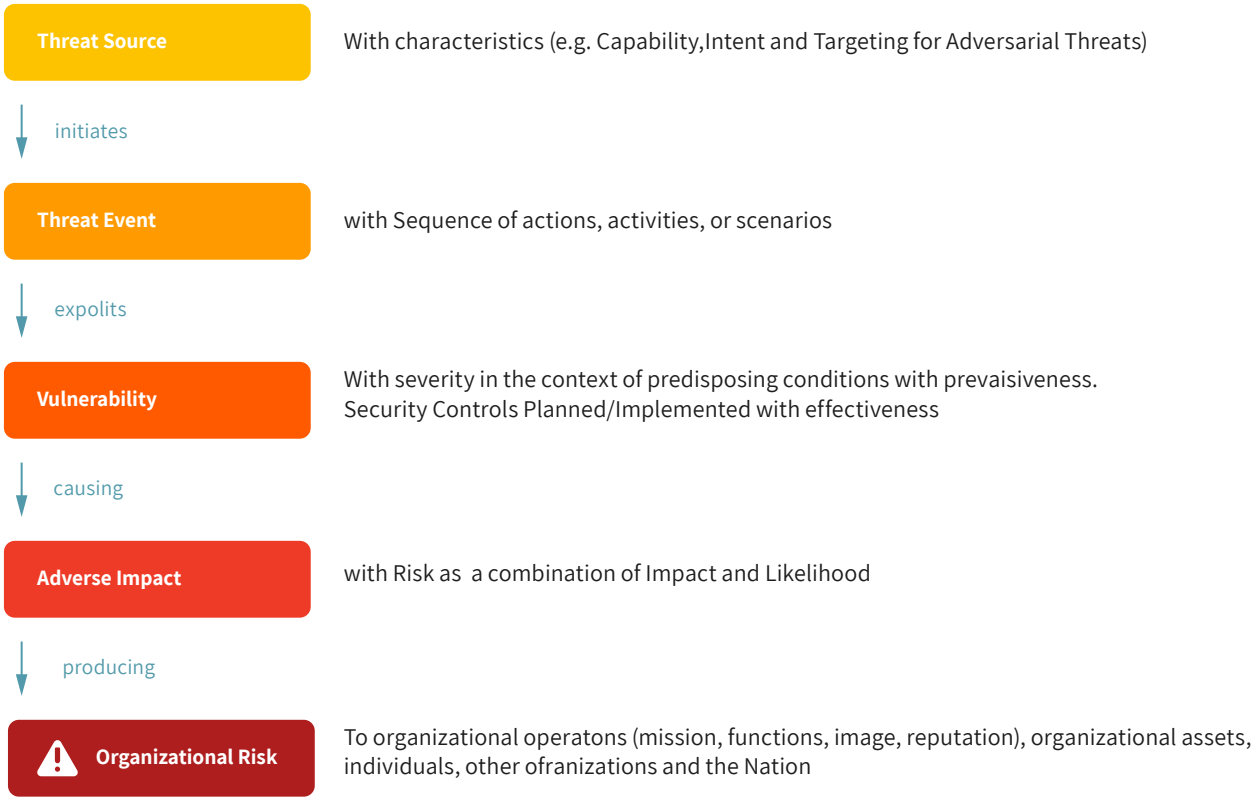
In today's frequently changing digital environment, traditional static modeling is simply ineffective. Hands-on Penetration Testing (PT) provides an organizational cyber threat "reality check" which enables prioritization of mitigation processes and resource allocation.
Based on an unmatched nation state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

OTORIO's OT Risk Assessment Benefits

- A comprehensive IT-OT converged environment assessment, including network, assets and processes
- A customized maturity roadmap to safe digital growth
- An assessment report concluding the compliance gaps with a clear and concise plan to meet with the regulation (e.g. NIST, IEC 62443, NERC CIP and IMO)
- OTORIO uses world-leading expert hacking teams to perform realistic red team assessments (Penetration Testing) that complements customary paperwork and creates a factual representation of the organization's security posture.

Use Case

- Identifying and prioritizing cyber risks to actionable items necessary to ensure production continuity.
- Compliance gap analysis, part of the organization GRC with particular and public regulations.
- Avoiding potential attacks by foreseeing attack vectors with non-obtrusive attack scenarios with mitigation controls.
- Creating tailor-made cyber maturity road map to enhance cyber resilience



OTORIO - a global leader in safe Industry 4.0 digitalization.

OTORIO is an industrial-native advanced Managed Security Service Provider, founded by Israeli defense cyber security experts partnering with global leading 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 upcoming 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.

OTORIO

OTORIO

www.otorio.co | info@otorio.co

OTORIO
Industrial cyber risk management solutions

Industrial IT-OT Converged Managed SOC

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

As an industrial-tailored SOC, it has a distinct role in preserving 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. OTORIO's SOC enables information sharing and action coalition with IT and OT stakeholders as well as operational impact reflection for executive management.

Safe Industry 4.0 Digitalization

The industry 4.0 digitalization, essential to the organization's business growth, introduces ever growing cyber-related challenges.

Security Orchestration, Automation and Response (SOAR) technologies that are tailored to OTORIO's IT-OT SOC core, enable faster and safer attendance to digital operational challenges. They enable a proactive reduction of cyber-related loss based on existing operational personnel and reasonable investment, while 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 control.

OTORIO's OT Risk Assessment Benefits

- Native IT-OT converged SOC; Monitoring OT assets and vertical-agnostic processes
- Forward-looking sources and technologies-rich security orchestration, automation and enforcement driven solutions, proactively counteracting current and upcoming industrial cyber risks.
- OT SOC operated by world-leading "special forces" talents having 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
- Ensuring fast, focused, comprehensive and effective operational remediation and mitigation processes and playbooks
- Customized operational and integrated cyber threat intelligence

OTORIO's OT SOC Operation Modes

OTORIO's Managed OT SOC can be implemented as a standalone OT SOC or interlinked with an IT SOC and SIEM. It allows operation flexibility with various operation modes such as an All-In, Handshake and Co-Operated. When the SOC operation is remote, 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. OTORIO's IR teams are trained to promptly restore the OT network's operational integrity without sacrificing its safety conditions.
Based on an unmatched nation state military experience in defending mission critical infrastructures and industrial engineering knowledge, OTORIO's teams have developed a tailored industrial Incident Response approach:

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

Use Case

- Outsourcing OT risk real-time monitoring and management
- Utilizing centralized situational industrial risk management – fuse global plants and processes
- Converged current IT monitoring means with managed OT monitoring and management
- Orchestrating and automating the OT diverse data sources
- Prompt identification of cyber attacks with immediate, remote and on-site Incident Response experts' team

OTORIO - a global leader in safe Industry 4.0 digitalization.

OTORIO is an industrial-native advanced Managed Security Service Provider, founded by Israeli defense cyber security experts partnering with global leading 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 upcoming 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.

OTORIO

OTORIO

www.otorio.co | info@otorio.co