RAM² Professional
Automated Industrial Digital and Cybersecurity Risk Management

RAM² Professional from OTORIO is a patent-pending, next-generation Security Orchestration, Automation and Response (SOAR) platform for OT security and digital risk management. RAM² Professional seamlessly integrates information from diverse operational and security systems - allowing OT and security teams to better leverage their investment in existing technology and achieve faster ROI.

Operational Continuity for Digitized Industrial Networks

OT networks contain many vulnerable assets which were not designed or maintained with cybersecurity in mind, and remain unpatched and unprotected.

RAM² Professional substantially reduces the risk of production downtime from cyberattacks by providing proactive and actionable risk mitigation steps specifically tailored to OT assets and converged IT/OT/IoT networks.

An Industrial-Native Solution

Discovering, analysing, and monitoring all OT, IT and IIOT assets within the operational environment, RAM² correlates security events and digital risks from across the entire OT network and maps them to operational processes. RAM² proactively identifies risk patterns and presents only meaningful and relevant insights - dramatically reducing alert fatigue and empowering operational and security teams to proactively prevent risks rather than just detecting them.

The platform's user-friendly dashboards simplify OT security - allowing operational teams to continuously assess their security posture while focusing on operational-critical risks. RAM² Professional also facilitates compliance governance, enabling operational teams to easily enforce policies, industrial standards and more.

When cyber incidents require SOC intervention, RAM² facilitates seamless collaboration between operational cyber teams, providing analysts with a tailored workbench for in-depth forensic investigation

Benefits

- Proactively reduce cyber risks in operational networks
- Gain a clear understanding of the overall security posture
- Eliminate alerts fatigue via consolidated insights
- Utilize OTORIO's industrial research vulnerabilities database
- Prioritize risks based on their business impact
- Apply smart resource allocation by focusing on operation-critical tasks
- Tailor the asset inventory to your specific industry
- Utilize automated analyst-in-a-box capabilities
- Achieve continuous compliance monitoring & fulfillment
- Facilitate OT-IT collaboration

RAM² Architecture
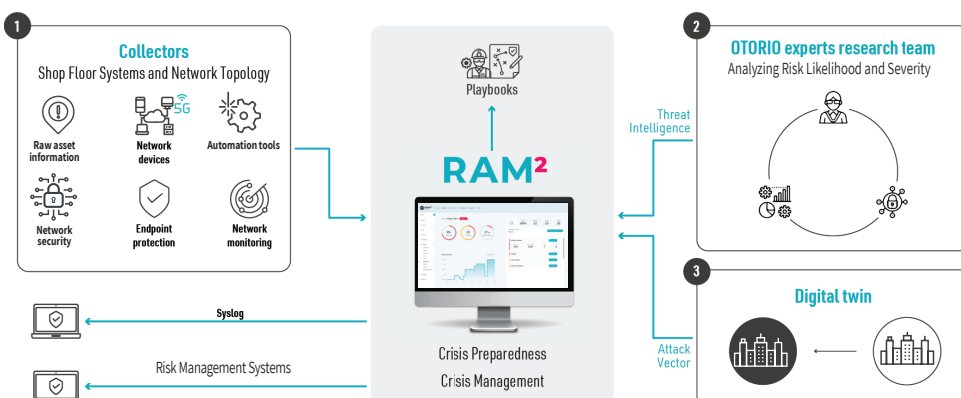
Key Features

Contextual Asset Inventory
· Simplified, non-intrusive data collection
· Discovers all assets within the OT network
· Maps assets to operational processes
· Monitors changes in asset inventory

Industrial Vulnerabilities Assessment
· Distinct OT vulnerabilities discovered by
  OTORIO's research
· Multiple-sources CVEs
· Maps vulnerabilities to assets
· Correlate severity with operational impact
· Presents feasible mitigation steps

Network Segmentation Assessment
· Identify segmentation gaps
· Intuitive and prioritized action items
· Reduces the attack surface

Detailed Dashboards
· Comprehensive security posture overview
· Compliance governance dashboard
· Granularity - from smallest business unit to
  enterprise level

Reports
· Rich and granular reports
· Customizable for different needs

Prioritized Cyber Risk Insights and Playbooks
· Cross-site research based insights
· OTORIO's proprietary algorithms
· Feasible mitigation playbooks

Breach and Attack Simulation
· Digital twin of the OT network
· Breach & Attack Simulation to predict potential attack
  vectors

Continuous Compliance Tracking
· Simplify compliance governance
· Dynamic and granular compliance score
· Compliance fulfillment recommendations
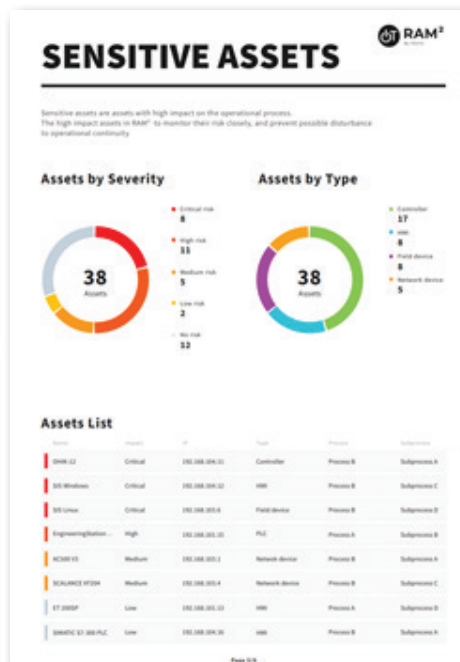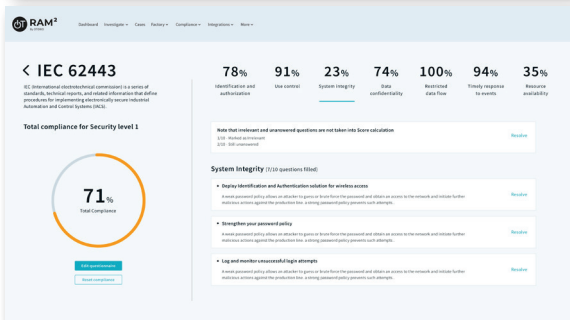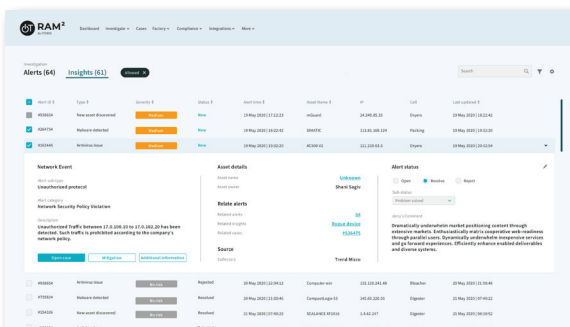· Multiple policies, e.g. NIST 800-82, IEC-62443

Case Management
· Open and assign cases from insights
· Prioritize tasks
· Monitor risks mitigation progress

Integrations
· Endpoint Detection and Response (EDR)
· Firewalls
· IDS/IPS
· Secured Remote Access
· IT SIEM/SOAR
· APM/CMMS
· Active Directory
· Industrial Systems (OPC, DCS, Historian, MES)

Clear and Concise Reports

OTORIO's RAM² Solutions Family

RAM² Essentials is an easy-to-use risk mitigation and compliance management solution that enables focusing only on risks with high operational impact.

RAM² Professional features contextual assets visibility, risk prioritization based on operational impact, continuous compliance, alerts correlation, meaningful insights, case management, digital twin, breach and attack simulation, and SIEM integrations.

RAM² Enterprise provides central management for RAM² Essentials or RAM² Professional deployed in multiple sites, providing a transparent organizational governance capability.

	RAM² Essentials	RAM² Professional
RAM² Single-Site		
Contextual Assets Inventory	✓	✓
Assets Changes Management	✓	✓
Vulnerabilities Assessment	✓	✓
Proprietary OT Vulnerabilities Database	✓	✓
Asset Vulnerability Risk Score Based on Operational Impact	✓	✓
Granular Dashboards	✓	✓
Prioritized and Feasible Mitigation Steps	✓	✓
Continuous Compliance Management	✓	✓
Network Segmentation Assessment	✓	✓
Granular Reports	✓	✓
Meaningful Cross-Site Research-Based Insights		✓
Case Management		✓
Mitigation Playbooks		✓
Digital Twin		✓
Breach and Attack Simulation		✓
IT SIEM/SOAR Integration		✓
APM/CMMS Integration		✓
RAM² Enterprise		
Governance of Multiple RAM² Sites	✓	✓
CISO Dashboards and Insights	✓	✓
Enterprise-Level Risk Assessment	✓	✓
Enterprise-Level Compliance Governance	✓	✓
Enterprise-Level Reports	✓	✓
Aggregated Insights		✓
Risks Trends and Statistics		✓
Cross-Sites Compliance Analysis		✓

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.