Spotlight Security Assessment Powered by RAM²

Automated, cyber digital twin based risk assessment

Maximum OT Cybersecurity, Minimum Effort

Cybersecurity officers are some of the busiest security professionals on the planet. That's why OTORIO developed the automated **Spotlight Security Assessment** – to dramatically improve organizational security posture and enhance compliance, with almost no effort.

OTORIO's **Spotlight Security Assessment** is a short yet powerful offline process - with zero interference to your operational environment. Data from your systems is collected and analyzed using automated tools provided by OTORIO. The end result is a comprehensive view of risks, exposures and vulnerabilities, along with a clear and feasible risk mitigation plan – all prioritized according to the potential impact of each risk to your business.

OTORIO's Spotlight was uniquely designed for Operational (OT) and IoT environments, in which patching is less viable– leaving assets often unpatched and unprotected.

You will gain

Automated Data Collection
Proprietary tools tailored to your business

Offline Risk Assessment
Non-disruptive risk analysis and accompanying expert analysis

Cyber Digital Twin Attacks Prediction
Non-intrusive breach and attack simulation on a digital twin of your OT network

Business-Context Prioritization
Prioritization based on actual risk impact on operational continuity

Interactive Dashboards
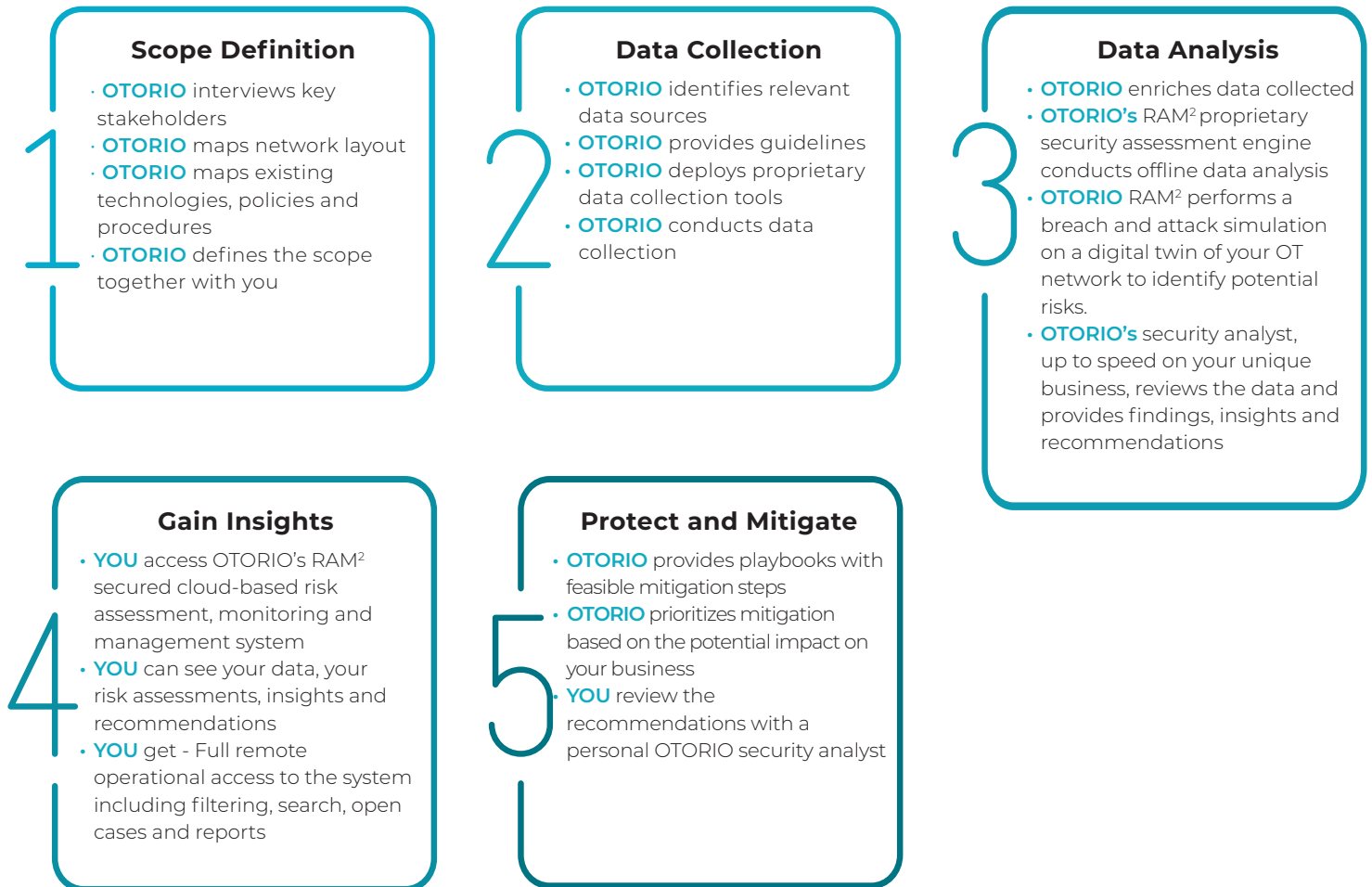A cloud-based system with security posture insights

Cyber Protection Plan
Feasible, actionable and simple risk mitigation playbooks

Personal Cyber Consultant
A personal cybersecurity analyst that understands your business

How Does it Work? Full-Service Security Assessment Workflow

1 Scope Definition

· **OTORIO** interviews key stakeholders
· **OTORIO** maps network layout
· **OTORIO** maps existing technologies, policies and procedures
· **OTORIO** defines the scope together with you

2 Data Collection

· **OTORIO** identifies relevant data sources
· **OTORIO** provides guidelines
· **OTORIO** deploys proprietary data collection tools
· **OTORIO** conducts data collection

3 Data Analysis

· **OTORIO** enriches data collected
· **OTORIO's** RAM² proprietary security assessment engine conducts offline data analysis
· **OTORIO** RAM² performs a breach and attack simulation on a digital twin of your OT network to identify potential risks.
· **OTORIO's** security analyst, up to speed on your unique business, reviews the data and provides findings, insights and recommendations

4 Gain Insights

· **YOU** access OTORIO's RAM² secured cloud-based risk assessment, monitoring and management system
· **YOU** can see your data, your risk assessments, insights and recommendations
· **YOU** get - Full remote operational access to the system including filtering, search, open cases and reports

5 Protect and Mitigate

· **OTORIO** provides playbooks with feasible mitigation steps
· **OTORIO** prioritizes mitigation based on the potential impact on your business
· **YOU** review the recommendations with a personal OTORIO security analyst

Pre-Breach Risk Reduction Plan

OTORIO's **Spotlight Security Assessment** analyzes the security health of your OT, IoT, and IT assets, network devices, endpoint devices, Active Directory, firewalls, and more. The analysis is done automatically based on data collected from your operational network. The data is processed offline by OTORIO's proprietary security assessment engines, OTORIO's automated breach and attack simulation and OT cyber experts. The outcome is a fully prioritized risk assessment and mitigation plan.

Improving your Post-Breach Detection and Response

Spotlight Security Assessment analyzes your traditional detection solutions (antivirus, IDS, EDR, SIEM, etc.), and provides actionable recommendations like configuration changes and best practices. The output of the analysis is a list of feasible action items that dramatically improve the efficiency of your post-breach detection and response while minimizing post-breach operation disruption.

Key Features

Assessment Elements
- Deployment gaps
- Missing security components
- Misconfigurations in security solutions
- Device and software misconfiguration
- Auditing deficiencies
- Unintended relationships between assets
- Segmentation assessment

Supported Data Sources
- OT, IT and IoT assets (controllers, RTUs, CCTVs, etc.)
- Network devices
- Endpoint devices
- Antivirus
- Endpoint Detection and Response (EDR)
- Internet-facing and industrial firewalls
- Intrusion Detection Systems (IDS)
- Active Directory (AD/GPO)
- Endpoint image files
- Network scanner
- Security Information and Event Management (SIEM)

Interactive Dashboards
- Comprehensive security posture overview
- Contextual assets inventory
- Prioritized risks, insights and alerts
- Playbooks and mitigation steps
- Compliance governance overview
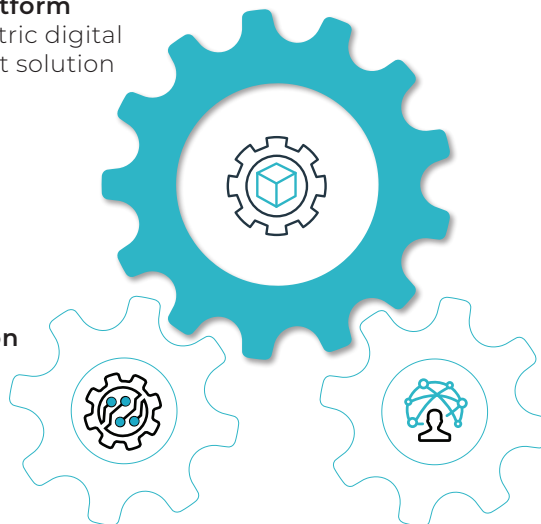- Case management
- Reports

Cyber Protection Plan
- Playbooks prioritized by business impact and dependencies
- Feasible mitigation steps
- Review with a personal analyst
- Detailed report

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

Automated Data Collection
Zero interference to your operational environment

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

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.