OTORIO

RAM²

Kontinuierliches OT-Cyber-Risikomanagement

Vorgeschriebener Schutz für Betriebsnetze

Die digitale Transformation in Produktionsnetzen jeder Art erhöht weiterhin die damit einhergehenden Risiken. Der Einsatz verschiedener Anbieter, manuelle Prozesse und Technologien mehrerer Generationen machen OT-Sicherheit komplex. All diese Faktoren erhöhen die Risiken erheblich, was es herausfordernd macht, die Sicherheitslage zu erfassen und zu verstehen sowie industrielle Betriebsabläufe zu schützen.

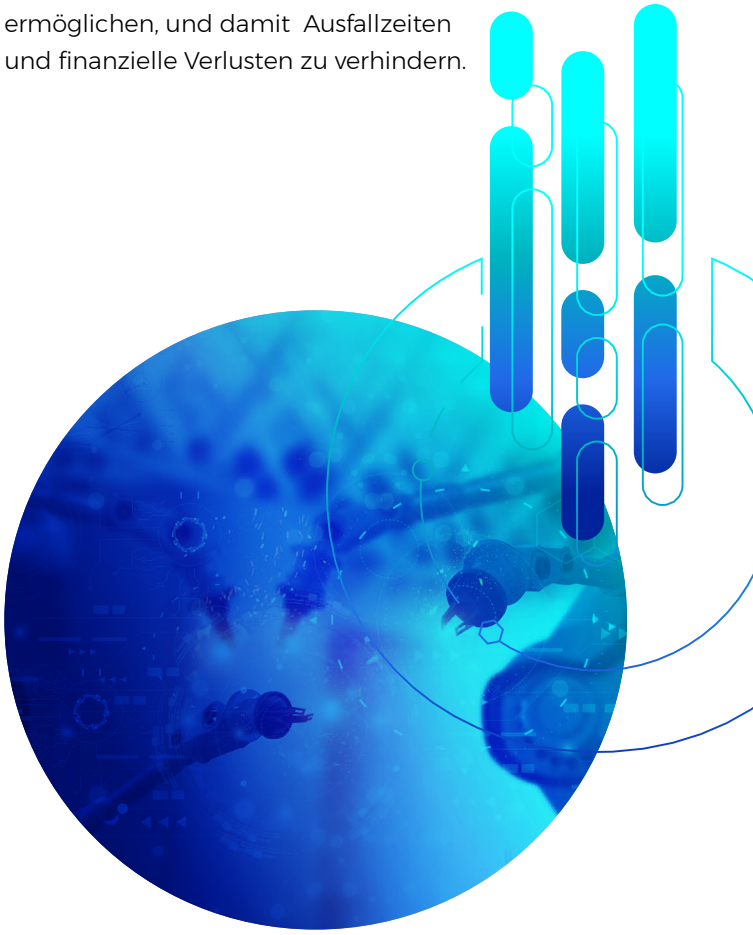
OTORIO's RAM² ist eine OT-Sicherheitslösung mit einem vereinheitlichten Framework, das entwickelt wurde, um Ihnen dabei zu helfen, Cybersicherheitsrisiken proaktiv zu verwalten, widerstandsfähige Betriebsabläufe aufzubauen und operationale Umgebungen zukunftssicher zu machen. Es bietet Ihnen beispiellose konsolidierte Sichtbarkeit Ihrer Firewall, EDR, IDS, PLC, SCADA, DCS, Historians, Engineering-Systeme und mehr. Alle Geräte, Netzwerke und Systeme in der Betriebsumgebung können in Echtzeit gesehen und überwacht werden, sodass Fachleute potenzielle Risiken effizient mit einem proaktiven Ansatz angehen können.

RAM² ermöglicht es Ihnen, die Kontrolle über den Stand Ihrer OT-Security zu übernehmen, indem es erweiterte Geräte-Attribute mit operationalem Kontext, Schwachstellen und Expositionen nutzt. Es liefert detaillierte Berichte, die die kritischsten Schwachstellen proaktiv identifizieren und Warnmeldungen liefern, die nach operationellem Kontext und geschäftlichem Einfluss priorisiert sind.

RAM2 bietet einen **einheitlichen Rahmen für die betriebliche Sicherheit**, um Ihrem Team dabei zu helfen, eine unternehmensweite Sicherheitsstrategie zu etablieren, um Bedrohungen schneller und zuverlässiger zu erkennen, zu priorisieren und zu bekämpfen. Es ermöglicht umfassende Governance und überbrückt Kompetenzlücken. RAM2 beschleunigt Entscheidungsfindung und verbessert signifikant Ihre durchschnittliche Erkennungszeit (MTTD) und durchschnittliche Reaktionszeit (MTTR).

RAM² unterstützt Fachleute mit **von Experten definierten Leitlinien zur Risikominderung**. Best Practises und maßgeschneiderte, praktische Playbooks bieten Schritt-für-Schritt-Anleitungen, um Teams dabei zu helfen, Schwachstellen zu entschärfen und operative Widerstandsfähigkeit sicherzustellen

RAM² lässt sich als Overlay integrieren, um den ROI **der bestehenden Sicherheitssysteme zu maximieren**. Die Plattform integriert sich nahtlos mit einer Vielzahl von Drittanbieter-Tools und -Technologien, um eine tiefergehende kontextbezogene Analyse zu ermöglichen, und damit Ausfallzeiten und finanzielle Verlusten zu verhindern.



Wichtigste Vorteile

- Verbesserung der betrieblichen Widerstandsfähigkeit gegenüber Cybersicherheitsrisiken.
- Skalierbare Integrationen von Drittanbietern mit bereichsübergreifenden Sicherheits- und Betriebsdatenquellen für einen konsolidierten Einblick in OT-IT-IIoT-Betriebsumgebungen.
- Vollständiger und genauer Einblick in den Anlagenbestand, einschließlich der Rolle der Anlagen und ihrer Auswirkungen auf deren Umgebung.
- Wegweisende, Risiko-basierende Priorisierung unter Nutzung einer nicht-invasiven Cyber-Digital-Twin-Technologie zur Analyse von Angriffsvektoren.
- Reduzierung von "Alarm-Müdigkeit" durch das Ausblenden von irrelevanten Ereignissen.
- Automatische Analyse und Identifizierung kritischer Risiken anhand korrelierter Erkenntnisse
- Kontextabhängige, auswirkungsorientierte Priorisierung der kritischsten Risiken.
- Klare, praktische Schritt-für-Schritt-Anleitungen zur Risikominderung, die auf Produktionsumgebungen zugeschnitten sind.
- Out-of-the-box asset und site-level compliance assessment (IEC 62443, NERC CIP, NIST).
- Umfangreiche, granulare Dashboards und Berichte für eine umfassende Bewertung der Sicherheitslage und Governance.
- Verbessern Sie den ROI Ihrer Technologie, Ihrer Mitarbeiter und Ihrer Prozesse, indem Sie RAM² nahtlos auf Ihre bestehenden Sicherheitsmechanismen aufsetzen.

How does it work?

01 Collect Data

Online / offline network Monitoring data

Passive, active and integration-based data collection

02 Enrich and Analyze

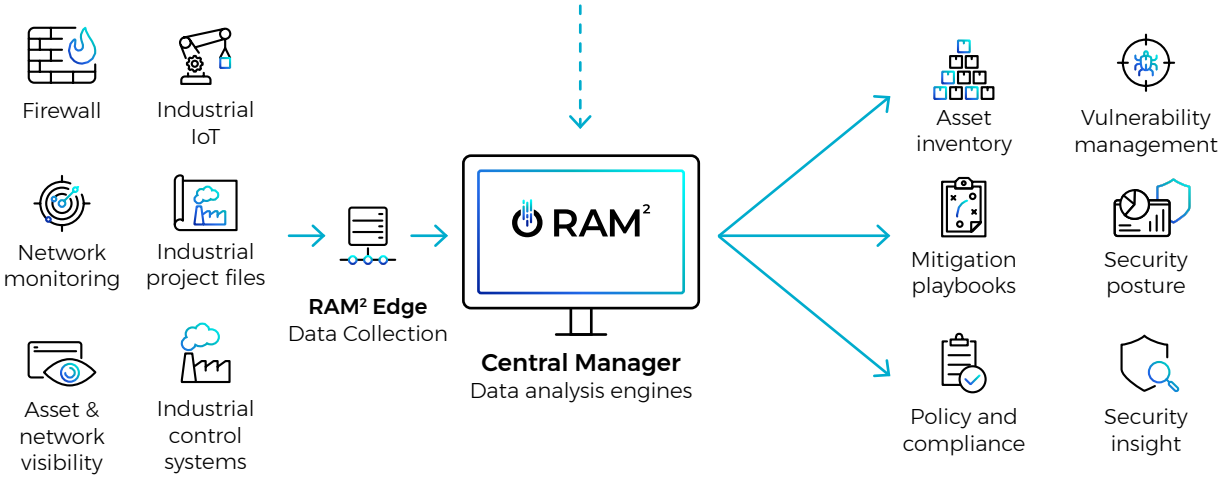
Market-leading vulnerabilities database

Based on OTORIO's research and professional services

03 Deliverables

Dashboards and reports

A unified organizational view of digital risk



Anwendungsfälle & Hauptmerkmale

Erweiterte OT-IT-IIoT-Transparenz

- Vollständige und detailreiche Transparenz für alle OT-, IT- und IIoT-Assets.
- Skalierbare Integrationen mit bereichsübergreifenden Datenquellen
- Passive Netzwerküberwachung und sichere aktive Abfrage der Anlagen
  - Vereinfachte, nicht-intrusive Datenerfassung.
  - Zuordnung von Anlagen und Systemen zu betrieblichen Prozessen
  - Überwacht Veränderungen im Anlagenbestand.
  - Assets auf Ebene 0 werden sichtbar gemacht.
- Integration mit:
  - Endpoint Detection and Response (EDR)
  - Firewalls
  - IDS/IPS
  - Sicherer remote access
  - IT SIEM/SOAR
  - APM/CMMS
  - Identity-and Access-Management
  - Industrielle Systeme (OPC, DCS, Historian, MES und mehr)

Kontinuierliche Überwachung und Bewertung der Sicherheitslage

- Identifizierung von Sicherheits-Fehlkonfigurationen von Anlagen, industriellen Systemen und Security-Systemen.
- Automatische Identifizierung von Lücken in den Sicherheitskonfigurationen der Anlagen und des Netzes, einschließlich der Verwendung von Standard-Zugangsdaten, falsch konfigurierter Sicherheitsparameter und der Security-Systeme selbst, End-of-Life-Anlagen, Verwendung unsicherer Kommunikationsprotokolle und mehr.
- Die Attack-Graph-Analyse liefert präzise Empfehlungen für die proaktive Härtung wichtiger Anlagen. Nicht-intrusive Analyse von Angriffsvektoren durch die Cyber Digital Twin Technologie von OTORIO.
- Anpassbare Dashboards zur Unterstützung einer effizienten Entscheidungsfindung.

Schwachstellenbewertung

- Marktführende Schwachstellen-Datenbank basierend auf OTORIO's eigener Forschung
- Genaue Identifizierung und Zuordnung von öffentlich bekannten Schwachstellen (CVEs)
- Priorisierte Warnungen basierend auf dem operativem Kontext
- Praktische, klare und durchführbare Playbooks zur Risikominderung, mit Alternativen zum Patching

Segmentierungs-Assessment

- Identifizierung von Firewall-Fehlkonfigurationen und Segmentierungslücken.
- Optimierung der Firewall-Regeln.
- Liefert intuitive und nach Prioritäten geordnete Schritte zur Risikominderung.
- Reduziert die Angriffsfläche.

Erkennung von Vorfällen in Echtzeit

- Korrelierte Erkenntnisse auf der Grundlage von Ereignissen aus mehreren Datenquellen, um verdächtige Muster zu erkennen und das "Rauschen" durch gutartige Ereignisse zu reduzieren.
- Nutzung von proprietären Funktionen wie passiver Netzwerküberwachung, SNMP-Traps und mehr, um die Erkennung von Bedrohungen zu verbessern.
- Risikobasierte Alarmierung entsprechend den potenziellen Auswirkungen auf die damit verbundenen betrieblichen Abläufe und geschäftlichen Folgen.
- Automatisierte E-Mail-Benachrichtigungen an die zuständigen Mitarbeiter je nach Betriebsablauf und Schweregrad.

Compliance und Governance

- Sofort einsatzbereite Konformitätsprüfung von einzelnen Anlagen bis hin zu Standorten und dem gesamten Netzwerk.
- Umfangreiche, detaillierte Berichte zu Sicherheitslage und Compliance-Grad.
- Dynamischer und granularer Compliance-Score.
- Mehrere Standards wie NIST 800-82, IEC-62443, NERC CIP sowie eigene Unternehmensrichtlinien
- Compliance-Dashboard.

Use cases & Key Features

Case Management

- Mechanismus, der die Zusammenarbeit von IT- und IT-Teams für eine effiziente Lösung und Risikominderung ermöglicht.
- Verwalten Sie alle relevanten Informationen für Ermittlungen und Schadensbegrenzung an einem Ort.
- Weisen Sie den verschiedenen Beteiligten Aufgaben zu und verfolgen Sie den Fortschritt.

OT kontextabhängige Risikobewertung

- Kontextabhängige Bewertung der Sicherheitslage und der Attack Surface
- Korrelierte Erkenntnisse zur Erkennung potenzieller Angriffe und zur Rauschunterdrückung.
- Identifizierung von Host-, Netzwerk- und IAM-Lücken und Schwachstellen.
- Priorisierung von Lücken auf der Grundlage von Risikokalkulationen einschließlich Auswirkungsanalysen und verschiedenen Bedrohungsstufen.
- Umfassender, granularer Dashboard-Überblick über die Sicherheitslage, von der Anlage über die Geschäftseinheit bis zur Unternehmensebene.
- Umfangreiche und detaillierte Berichte - anpassbar an unterschiedliche Bedürfnisse.
- OTORIO's proprietäre Algorithmen für priorisierte Erkenntnisse über Cyberrisiken
- Praktische, klare und umsetzbare Handlungsanweisungen zur Risikominderung, die auf betriebliche Umgebungen zugeschnitten sind.
- ICS ATT&CK MITRE-basierte Erkenntnisse

Risiko-Entschärfung

- Massnahmen-Empfehlungen zur Risiko-Minimierung
- Bewährte Verfahren zur Absicherung von Sicherheitskonfigurationen und Netzwerkschnittstellen
- Segmentierungsbewertung mit empfohlenen Schritten zur Verringerung des Risikoniveaus
- Praktische, klare und umsetzbare Anleitungen zur Risikominderung, zugeschnitten auf die Betriebsumgebung.
- ICS ATT&CK MITRE-basierte Erkenntnisse.

Zusammenfassung

Die operative Sicherheitsmanagementlösung RAM2 von OTORIO bietet ein umfassendes und praktikables Rahmenwerk, das die Transparenz Ihrer gesamten Betriebsumgebung konsolidiert und Sie in die Lage versetzt, die Kontrolle über Ihre Sicherheitslage zu übernehmen, kritische Schwachstellen zu identifizieren und Cyberrisiken proaktiv zu reduzieren. RAM2 bietet Ihnen von Experten definierte Anleitungen zur Behebung von Schwachstellen und präskriptive Abhilfemaßnahmen, die auf Ihre spezifische Betriebsumgebung zugeschnitten sind, so dass Sie branchenübliche Best Practices implementieren und Ihre Sicherheitskonfigurationen und Netzwerkschnittstellen stärken können. Mit RAM2 können Sie einen sicheren, zuverlässigen und effizienten Betrieb gewährleisten, der für Ihr gesamtes Unternehmen einen unmittelbaren Nutzen bringt.

Über OTORIO

OTORIO hat eine industrietaugliche OT-Sicherheitsplattform entwickelt, die es seinen Kunden ermöglicht, eine integrierte, ganzheitliche Sicherheitsstrategie für industrielle Kontrollsysteme (ICS) und cyber-physische Systeme (CPS). Gemeinsam mit seinen Partnern ermöglicht OTORIO den Fachleuten für betriebliche Sicherheit ein proaktives Management von Cyberrisiken und die Gewährleistung eines stabilen Betriebs. Die Plattform des Unternehmens bietet einen automatisierten und konsolidierten Einblick in das gesamte betriebliche Netzwerk und ermöglicht es Unternehmen, die Kontrolle über ihre Sicherheitslage zu übernehmen, kritische Risiken zu beseitigen und einen unmittelbaren Geschäftswert für das gesamte Unternehmen zu schaffen. Das globale Team von OTORIO kombiniert die umfassende Erfahrung von Top-Experten für Cybersicherheit auf nationaler Ebene mit fundiertem Fachwissen in den Bereichen Betrieb und Industrie.

www.otorio.com

CN 040523