Solution Brief

RAM² with FortiSIEM

Technologies combine for IT and OT Cybersecurity

Overview

There is a growing need for cyber security teams to extend their visibility into converged IT, OT (Operational Technology) and IIoT networks. CISOs, SOC analysts and MSSPs are looking for integrated monitoring and control that allow them to protect the core business of industrial organizations. OTORIO's RAM² informs, contextualizes and enriches FortiSIEM to provide protection, enforcement, remediation, and overall risk reduction for the OT environment.

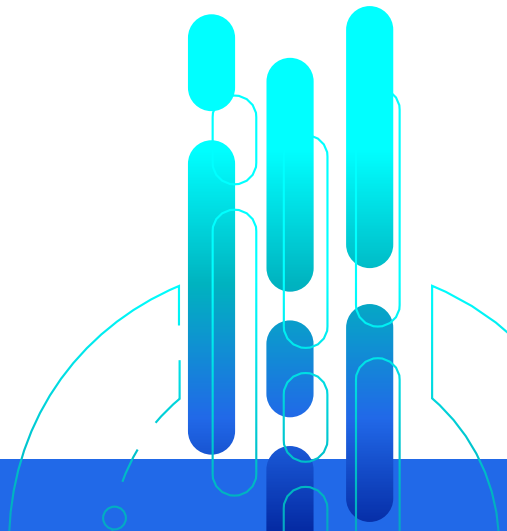
The Challenges

OT governs critical infrastructure and is a primary target for attack. Digital innovation increases risk across all industries and organizations face a number of security challenges:

- Complexity is overwhelming (e.g., multi-vendor, multi-generation, distributed operations, alert fatigue and more).
- Lack of visibility in the converged environment (IoT to IIoT).
- IT security tools are not suitable for OT protection.
- Lack of business context for risk prioritization.
- Lack of industrial know-how in the SOC.
- Organization-wide compliance auditing.

Highlights

- Secures IT/OT convergence by integrating OTORIO's contextual OT cyber risk information with FortiSIEM
- Improves operational continuity with ongoing OT risk assessment and reduction
- Bridges the OT security skills gap via automated analysis and a mitigation playbook
- Offers practical remediation actions that minimize production interference (e.g., patching on the production floor)



RAM² with FortiSIEM

The Solution

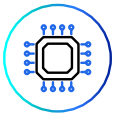
Fortinet and OTORIO's technology partnership addresses these challenges together, and enables secure industrial growth with FortiSIEM and OTORIO's RAM² solutions. OTORIO RAM² provides a complementary OT-specific solution for asset inventory, vulnerability management, threat detection, security posture assessment, compliance and risk mitigation plans. FortiSIEM combines the analytics traditionally monitored in separate silos of the security operations center (SOC) and network operations center (NOC), providing an organization a more holistic view of its security and business continuity. Together, FortiSIEM's and RAM²'s integrated security architecture delivers proactive OT security risk detection with OT-contextual prioritization and remediation capabilities.

RAM² with FortiSiem enables security leaders to:

Gain visibility on all OT and IT networks across hundreds of facilities from a single console, including OT-specific capabilities (e.g., protocols, integration with industrial systems, processing of industrial project files).

Use OTORIO's platform for smart contextualized alerts with prioritization when an anomaly is detected, and modify firewall policies to block it.

Incorporate a global OT-IT-IIoT threat intelligence feed that enables visibility and vulnerability management for advanced threats and zero-day attacks.



Use artificial intelligence (AI) to profile system behavior and detect anomalies in real time.

Noise reduction and a single source of truth (SSOT) concerning OT.

Provide proactive pre- and postbreach protection, rather than only reacting post-breach.

Out-of-the-box compliance for IT and OT standards and regulations.

How it works

OTORIO's RAM² is an OT cyber security risk management platform that enables operations security leaders to proactively protect critical operational processes, and reduce the time to assess, manage, and mitigate risks. RAM² ingests data from the entire Fortinet Ecosystem in addition to a variety of security and industrial sources (e.g., PLC, DCS, SCADA, Historians, Engineering systems) within the OT environment.

RAM² provides a complete and accurate industrial asset inventory. It identifies IOCs (indications of compromise) as well as vulnerabilities and IOEs (indications of exposure), and automatically correlates these indicators to identify suspicious patterns and risk scenarios that may affect the safety, efficiency, and reliability of industrial processes. RAM² provides contextualized prioritization based on OTORIO's unique risk calculation engine, taking into account the potential impact on production operations and business goals. RAM² also provides out-of-the-box compliance audits according to common industrial security standards (e.g., IEC 62443, NERC CIP and NIST) leveraging the results of deep asset inspection, SCADA systems, and the entire ICS network.

By processing offline data such as industrial project files, industrial firewall configurations, PCAPs, RAM² provides extended visibility into operational networks, including areas which are not accessible to continuous monitoring. The platform filters irrelevant events that are generated by multiple siloed sources in industrial networks, and provides correlated insights that are enriched by enhanced and robust threat intelligence of OTORIO's security experts. By distributing RAM²'s alerts and insights to FortiSIEM, we reduce the noise and assist in efficient and scalable protection of integrated OT/IT security teams.

RAM² with FortiSIEM

Use Case

Detection of an attack and its impact on operations

Cyber attacks that target industrial operations may be spread over a long period of time, making it hard to understand the complete flow of events and identify the relation between specific events to changes in the state of operational processes. RAM² identifies high-risk scenarios automatically by correlating disparate data points to identify suspicious patterns. RAM² monitors network activities, events from additional Fortinet products (e.g., FortiGate and FortiEDR). It adds industrial context based on information from industrial systems, OT asset states and vulnerabilities, how critical they are, and their position within the operational hierarchy. This allows RAM² to inform FortiSIEM about detection insights that describe a complete attack chain. For example, a hypothetical scenario might include an attack that starts with lateral movement from IT to OT, continues with the unauthorized installation of suspicious code, followed by a change in an asset's state. RAM² insights enable immediate detection of the attack with contextual prioritization that leads to effective response to help safeguard the organization's business continuity..

Proactive Protection and Compliance

There are multiple attack vectors that can disturb industrial operations. Some of these can exploit misconfigurations of existing security controls in the corporate IT network, or even the internet, to reach critical OT network assets. Vulnerable assets, segmentation gaps, or lack of proper access control will enable attackers to reach assets that are critical to operations.

RAM² allows security teams to proactively protect OT environments and reduce the risk of successful attacks. It does so by:

- Providing maximum visibility into industrial asset inventory
- Identifying asset vulnerabilities, gaps, and exposures in security configurations of industrial systems
- Assessing firewall rules configurations between:
  - IT and OT
  - Operational processes
- Ensuring coverage of endpoint protection.

It also provides an asset and network-level compliance audit according to industrial security standards.

Required actions are prioritized and accompanied by mitigation plans that are tailored to any constraints specific to the industrial environment. This way security teams can proactively reduce risks to help prevent breaches and strengthen organizational resilience.a clear asset inventory, identifies vulnerabilities, gaps and exposures, and assesses segmentation between operational processes in the network. Use spOT Assessment to expedite technical cybersecurity risk assessments for clients. Data from a variety of Fortinet products (e.g., FortiGate, FortiNAC, FortiEDR) will be correlated with data from other systems and assets. spOT Assessment enables auditors and consultants to identify risk scenarios and provide reports that provide customers with extraordinary value.

About OTORIO

OTORIO's industrial-native OT security platform enables industrial organizations to achieve an integrated, holistic security strategy. Together with its partners, OTORIO empowers operational security practitioners to proactively manage cyber risks and ensure resilient operations. OTORIO's global team brings the extensive mission-critical experience of top nation-state cyber security experts combined with deep operational and industrial domain expertise.

CN 130422