5 Essentials for a Complete Industrial OT Security Solution

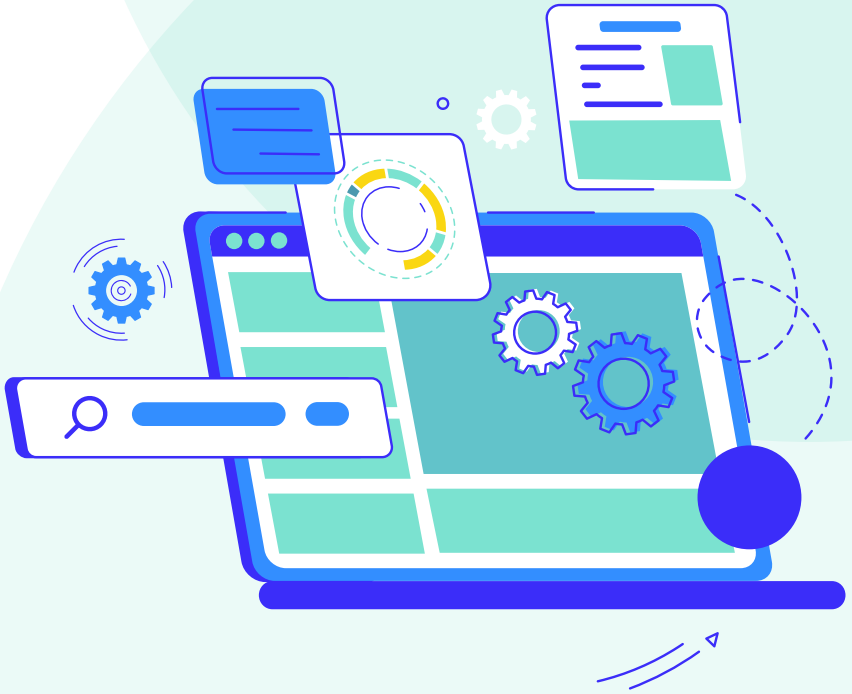
OTORIO

Five industrial OT security essentials

Industrial operational technology (OT) networks are continually targeted. From the hacking of LNG producers just before Russia invaded Ukraine, Toyota's temporary shutdown of 14 factories after a supplier was breached, or compromising a nuclear power plant's ICS and SCADA systems, attacks against industrial operations appear never-ending. Air-gapping production floors is no longer a viable defense.

Mapping and understanding security posture and the complexities of protecting OT networks introduced many risks. Deployed on their own, intrusion detection systems (IDS) are 1) largely reactive, 2) overwhelm security teams with noise, and 3) fail to prioritize alerts by risk, context, and their potential impact. IDS solutions do not mitigate risk, nor prevent malicious attacks that harm business continuity and industrial operations.

Air-gapping production floors is no longer a viable defense



5 Essentials

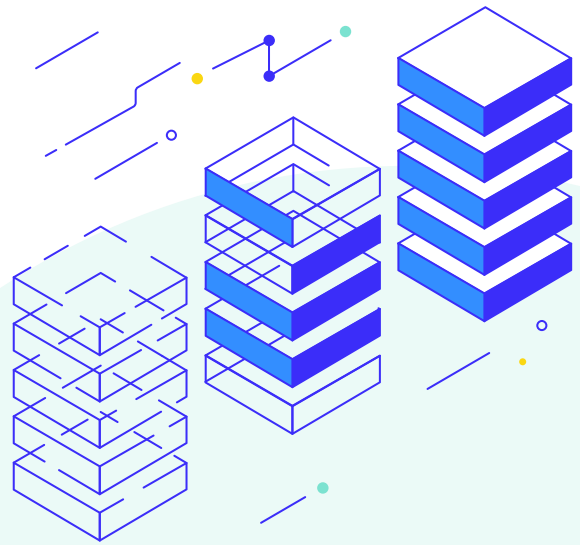
This eBook highlights five (5) essentials for implementing a complete industrial OT security solution:

1. **Comprehensive, 360˚ view of asset visibility**
2. **Proactive, contextual risk awareness**
3. **Clear, feasible steps to mitigate actual high-priority risks**
4. **Improving the ROI of existing OT security investments**
5. **True IT-OT collaboration**

1 Comprehensive, 360° view of asset visibility

IDS solutions lack a full 360° view of the OT environment and all OT–IT–IIoT assets. Comprehensive asset visibility can provide information about:

- Each asset's business impact, operational context, and organizational hierarchy
- Visibility of security controls
- Industrial sources such as OPC, DCS, and project files
- Firewalls
- Web proxies
- Deeper views of each asset and its security configurations
- Management systems (e.g., Active Directory)
- Endpoints and servers
- Network devices and IDS/IPS
- SIEM
- Better operational network coverage
- Many other components



Using IDS alone, your asset inventory visibility is likely to be severely lacking. Data from other security and industrial sources must be included to have a full view of all OT assets and ensure effective risk mitigation. Security teams can't fix what they cannot see.

Reliable and extensive asset inventory

Even Level 0 assets must be visible (e.g., legacy systems, existing critical infrastructure)

The foundation of industrial OT security is based on a reliable, extensive, and complete asset inventory. This requires:

- Complete accuracy; Complete asset inventory is the foundation of industrial OT security
- Centrally extended visibility
- Rating an asset's impact upon operations to ensure correct contextualization
  - Mapping assets to operational processes
  - Minimizing the number of "ghost assets"
- Continuous monitoring of data and changes in asset inventory, without interference with ongoing operations.
- Identifying risks having OT context to create a single source of truth (SSoT)

2 Proactive, contextual risk awareness

- Proactively manage vulnerabilities to cyber risk and lower the risk of a breach because post-breach reactions will be too late
- Reduce an organization's operational attack surface with proper segmentation
- Mitigate OT-IT-IIoT vulnerabilities to prevent hackers from exploiting them
- Harden critical assets and systems against ransomware
- Practical recommendations for proactive actions
- Ensure continuous backup of critical systems for recoverability because there is never a guarantee that breaches can be completely blocked

Case Study:

Real-World Alert Fatigue

Consider the case of a U.S. oil refinery that largely relied on an intrusion detection system (IDS) for its OT security. This created gaps in its security:

- The IDS produced a **high volume of noise** from ghost assets and false-positive alerts. The flood of noise made it much harder to detect and proactively respond to actual threats, causing **alert fatigue** for the refinery's cyber security team.
- Teams lacked the ability to prioritize risk effectively and efficiently, including discerning which alerts required immediate attention. Doing so could help them accurately detect and proactively respond to true OT security risks.
- The oil refinery lacked the ability to connect and leverage data sources and existing technologies to properly understand and secure its operational environment.

Using a comprehensive, reliable OT security solution as an overlay to its existing IDS, the refinery closed OT security gaps and enhanced its security posture.

Risk assessment based on business impact and operational context

An effective OT security solution should perform ongoing contextual risk assessment using data correlated from multiple, cross-domain sources. It should evaluate compliance, policies, and best practices to reduce risk and improve operational resilience.

The solution should prioritize risk mitigations based on their business impact and severity. IDS solutions provide an unmanageable flood of security alerts that cause alert fatigue and lack context-based insights. If provided, they would empower operational and security teams to focus on reducing risks that truly matter, correlated with their publicly known vulnerabilities.

3 Clear, feasible steps to mitigate actual high-priority risks

Mitigation playbooks empower SOC analysts and operational teams

Given the OT skills gap for SOC analysts and operational teams, another essential feature for industrial cyber security solutions is to provide these teams with clear, accurate, and easy-to-use **mitigation playbooks**. They should be suitable for operational environments where downtime is not an option.

The idea is that analysts and operational personnel do not need to be cyber security experts to use the playbooks. Such tools should also be capable of being tailored for an organization's specific industrial environment.

The playbooks should provide context to empower operational and security teams to immediately mitigate actual OT security exposures and vulnerabilities. Patching alone might not be sufficient or possible—especially for legacy OT systems.

Playbook use strengthens an industrial organization's operational resiliency against cyber risks.

Practical mitigation playbooks

Industrial security teams benefit from an advanced risk-quantification solution that matches OT vulnerability prioritzation with the required actions to mitigate them. Clear, feasible mitigation playbooks empower your teams to act immediately and ensure operational resiliency against cyber risks.

Context-specific playbooks also help bridge skill gaps by giving operational teams clear instructions for hardening site-specific OT network risks and vulnerabilities. Such OT risk mitigation aids should be presented in an easy-to-understand, actionable way—tailored to your organization's specific needs (e.g., organizational structure, policies, and workflows). This makes playbooks ideal given the constraints of operational environments.

4 Improving the ROI of existing OT security investments

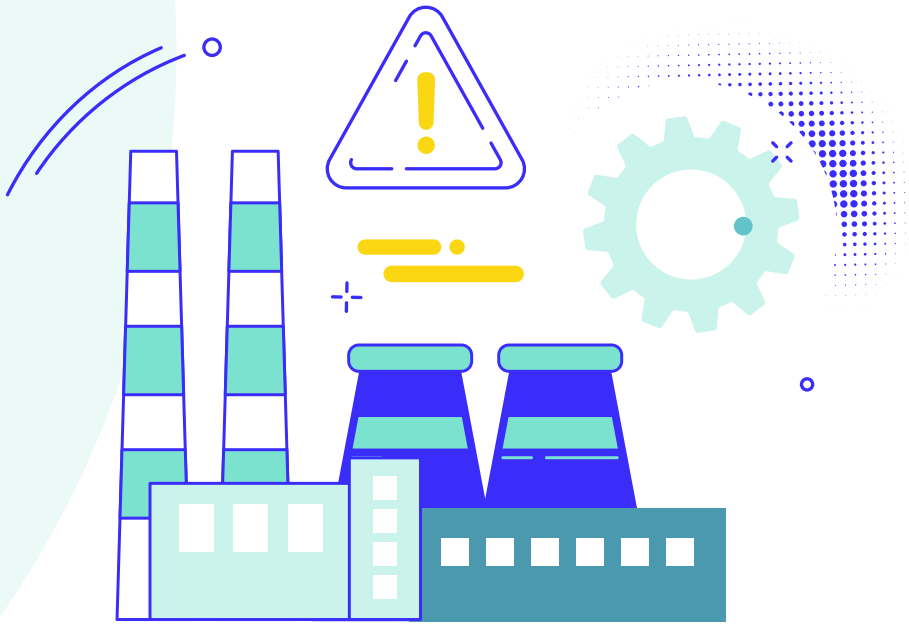
- Whatever OT security tools your organization is already using, they should provide a comprehensive assessment of security controls. That is, they should provide valuable, in-depth, prioritized insights, while reducing the amount of noise generated by existing solutions.
- Enhancing ROI can also be achieved by delivering focused, contextual insights about areas requiring high-priority attention.
- Given that your organization's focus is on industrial security, teams should have an operational, process-driven view of security risks. Insights should have the flexibility to be aggregated at various levels, whether by individual asset, a production floor, or an entire site. This makes it easy to measure improvement in risk reduction over time.

Prioritized, contextual insights enhance the ROI of your existing OT security investments

OT security insights should be contextual so SOC analysts and operational teams can:

- Improve the mean time to detect (MTTD) and respond (MTTR) using cross-domain insights that connect data from multiple sources and automate analysis
- Turn data into meaningful information to prioritize and mitigate risks that matter most
- Use practical playbooks empowering teams to take action
- Gain better visibility of augmented data from previously siloed sources
- Reduce the total cost of ownership (TCO) by eliminating alert noise
- Ensure security controls are properly configured (e.g., EDR agents and proper FW configurations)

SOC/OT–IT analysts need the ability to drill down to raw event details and obtain an understanding of context and urgency



5 True IT–OT Collaboration

- OT and IT teams are still not effectively aligned in industrial organizations. This means that operational and security teams have to depend on one another to collaborate efficiently, manage risk reduction, and perform timely, effective security incident responses.
- To collaborate well, teams should have the essential context that they might lack. Security teams need insights as to how security risks impact operations. Operational teams need to know how disparate security risks are prioritized and their affect on your organization's security posture.
- Operational and analyst teams should both be empowered to take action.

Operational and analyst teams should be empowered to take action

- All teams should understand, in their own profession-specific language, why some OT security alerts are deemed ‘high-priority,’ and what actions are required to mitigate such risks.
- Operational and security teams benefit from using a platform that enables them to collaborate transparently and effectively—including the ability to delegate tasks and track their progress.
- Organizations need to consider differences in teams’ existing workflows, enabling them to easily and effectively integrate OT security tools and processes. This helps enhance collaboration among stakeholders.

OTORIO'S RAM²

OTORIO's RAM² is a comprehensive OT security solution that empowers you to proactively manage cyber risks and build resilient operations.

Running as an overlay, RAM² enhances the ROI for organizations with existing investments in IDS-only solutions. And used by itself, RAM² is a proven, effective, end-to-end OT security solution.

RAM² is deployed at industrial manufacturing, critical infrastructure, and smart logistics organizations worldwide. It provides continuous, proactive risk identification, reduction, and compliance assessment for individual assests, production lines, and/or an entire operational site.

With RAM², IT and OT teams are truly connected, with communications streamlined for security collaboration. OT security leaders and asset owners get a proven, efficient solution to improve operational resilience against cyber risks.

Overview

COMPLIANCE

RAM²

Compliance score - IEC 62443 Security Level 1

IEC (international electrotechnical commission) 62443 standard provides a flexible framework to address and mitigate current and future security vulnerabilities in the industrial automation and control systems. Manage your compliance status RAM² to track your progress and be informed regarding needed remediation activities and gaps in each security aspect of the standard.

NOTE! The questionnaire is not completed yet, please go over the questionnaire and update the missing parts.
Note that for increasing your compliance coverage, the system recommends you remediation steps

71% Compliance

Identification and authorization 72%

1. Deploy IEEE 802.1X mechanisms for device identification
Unidentified devices in production floor could be malicious assets. Using 802.1x mechanisms enables endpoints compliance and blocking for unrecognized devices.

2. Implement an authentication management system
Without authentication system, no effective user management can be enforced.

3. Enforce max login attempts before account lockdown
Login attempts limitation is the only preventive control against countless tries (brute force attack) of password guessing.

Use control 75%

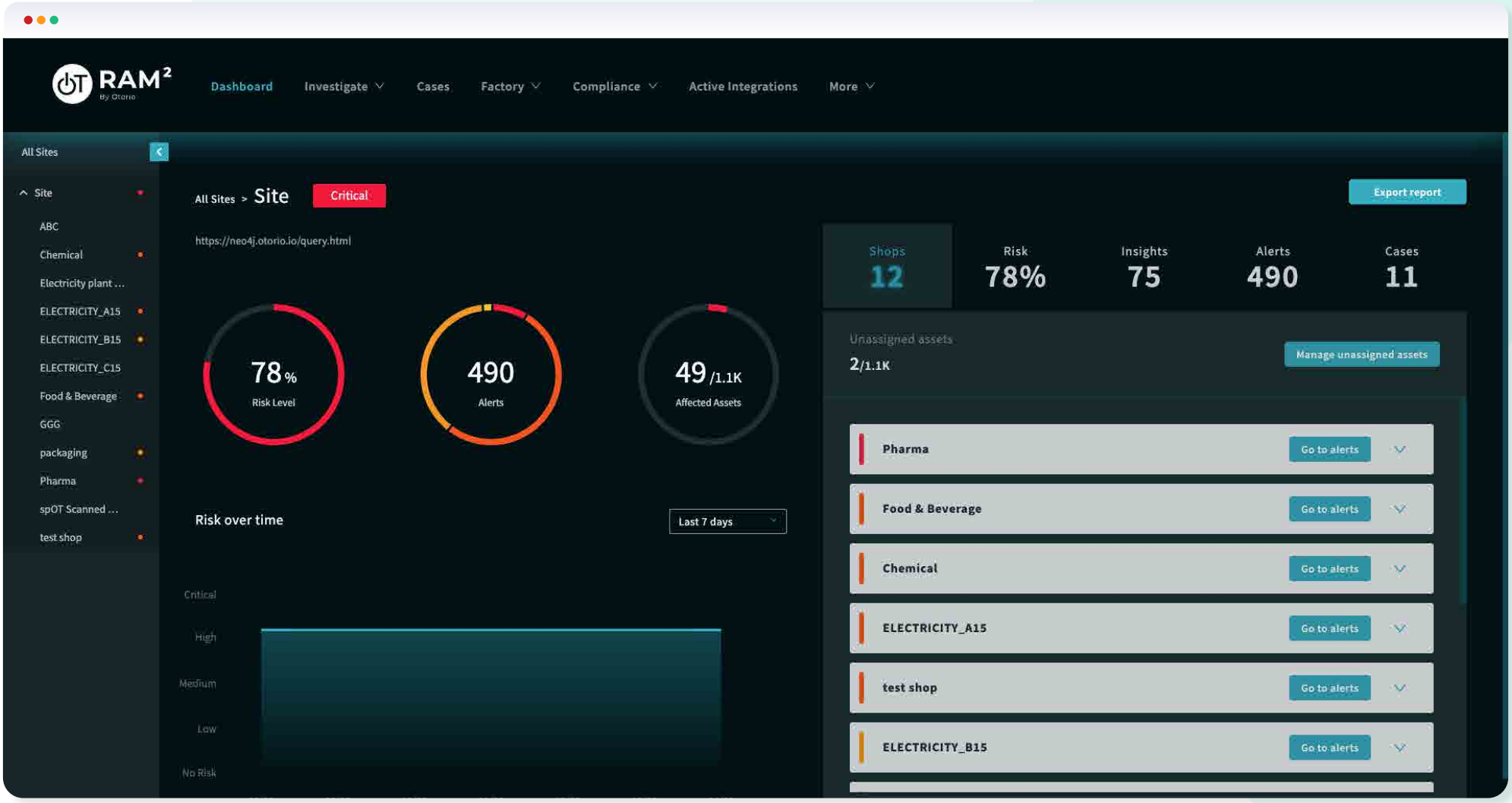
There is no remediation steps for this domain

System integrity 100%

Data confidentiality 67%

1. Encrypt Traffic leaving the OT network
Traffic exiting the OT network can be manipulated outside the OT environment. Encrypting the data prevents tampering and prevent attacks.

Page 1/2



RAM²'s dashboard offers central extended visibility of high-priority OT security risks for SOC analysts, operational teams, and CISOs.

Using OTORIO RAM² as a security overlay closes gaps that IDS solutions fail to address

OTORIO's RAM² enables industrial organizations to:

Improve operational resilience against cyber risks

Enhance ROI of existing IDS and security controls

Preemptively identify, quantify, and mitigate OT risks based on asset criticality

Empower true IT—OT collaboration

Get comprehensive visibility into asset inventory

Have clear, practical, and feasible mitigation playbooks optimized for their specific operational environments

Get unmatched integration capability with third-party tools

Have out-of-the-box compliance and security analysis

Significantly reduce noise and help prevent alert fatigue

Built for the operations and maintenance team

RAM² fosters collaboration between operational teams and SOC analysts.

Many IDS solutions are designed only for cyber security analysts; they lack sufficient value for operational (OT) teams due to skill gaps and lack of experience.

OTORIO's RAM² is different. Used as an overlay with existing IDS tools, it fosters collaboration between operational teams and SOC/IT—OT analysts for safe and reliable production.

- Continuous, proactive protection and risk management for ransomware-ready operational networks
- Full asset inventory coverage of all data sources
- Noise reduction and alert fatigue prevention
- Clear, easy-to-use risk mitigation playbooks tailored for users' operational networks
- Incident management to reduce MTTD and MTTR
- Automated compliance audit and policy governance

Conclusion

OTORIO's RAM² provides a comprehensive, holistic approach to industrial OT security and cyber risk management. Connecting to multiple industrial and cross-domain security sources, it offers comprehensive asset inventory visibility and management that is unmatched by IDS tools.

Its ability to aggregate, assess, and analyze data from multiple sources with OTORIO's market-leading Vulnerabilities Database accurately prioritizes risks. In addition, RAM² filters out false positives, ghost assets, and alert duplication, thereby greatly reducing alert fatigue.

RAM² automates OT security compliance and auditing processes, enabling your organization and understand its OT compliance with industry and market standards (e.g., NIST 800-82, IEC-62443, NERC CIP). Clear, feasible mitigation playbooks enable operational and security teams to collaborate effectively, quickly apply best practices to reduce risks, and ensure that the highest level of OT security is achieved.

About OTORIO

OTORIO is an end-to-end OT security company providing proactive, industrial-native cyber risk management solutions to protect business continuity and ongoing operations at enterprises and organizations worldwide.

Together with our partners, we provide comprehensive risk assessment, monitoring, and management solutions and services for critical infrastructure, smart transit and logistics, and industrial manufacturing organizations, enabling them to effectively secure their digital transformations in OT-IT-IIoT networked environments.

Our global team brings the extensive mission-critical experience of top nation-state cyber security experts combined with deep operational and industrial domain expertise.

OTORIO

Visit OTORIO.com

Contact us for more information: info@otorio.com