Proactive OT

Mitigating digital risks and protecting industrial operations

White Paper

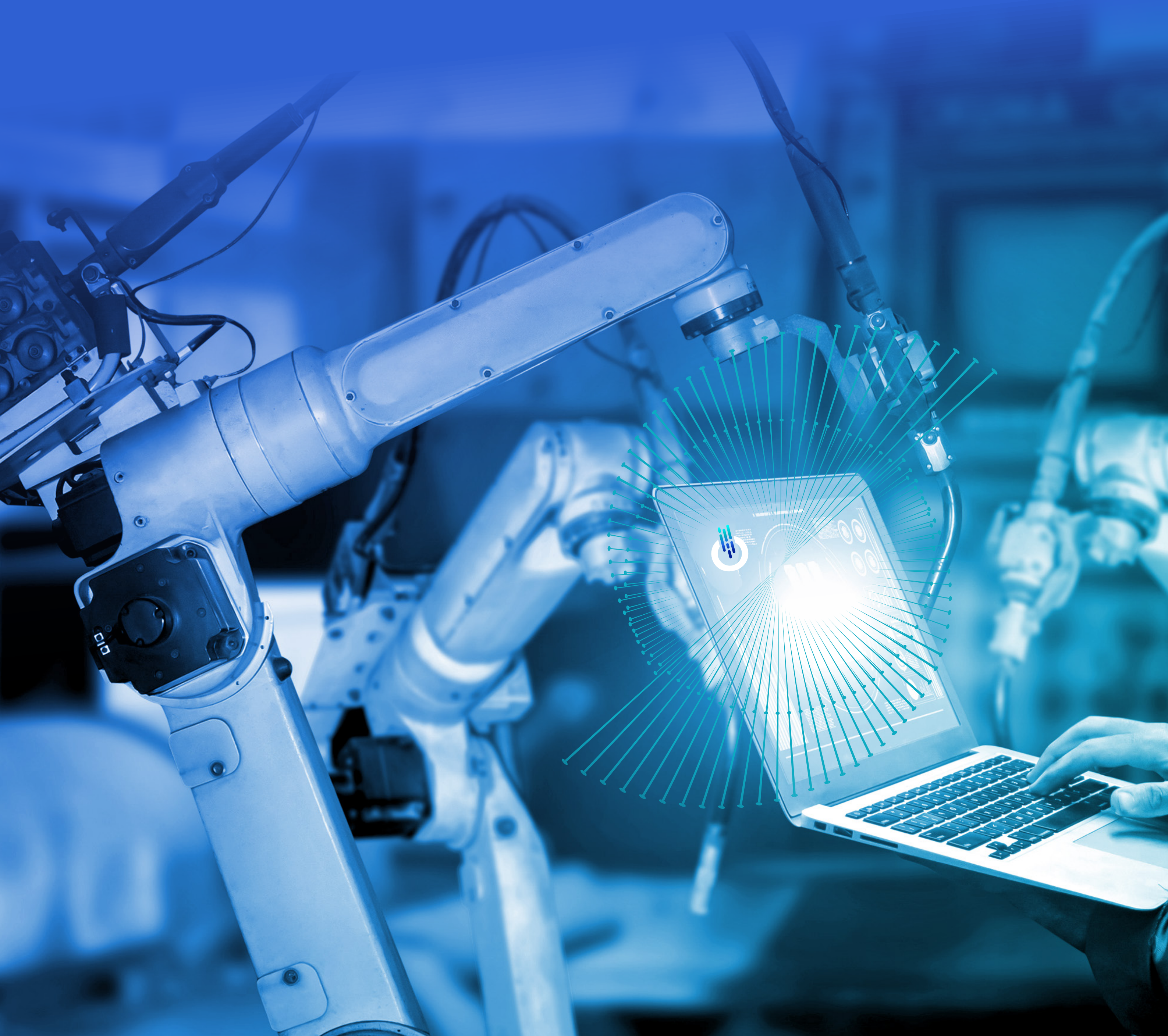


Table of Contents

Overview

With OTORIO Titan, IT and OT teams are truly connected and streamlined for security collaboration.

Managing and reducing the risk of malicious digital attacks on operational technology (OT) is a critical challenge. Industrial operations and business continuity depend on continuous, effective OT security to protect digitally-connected production floors. **According to Gartner, Inc., "[t]hrough 2025, 70% of companies will deploy cyber-physical systems protection platforms as the first step in their asset-centric security journey."** [1]

Manufacturers, critical infrastructure operators, and smart infrastructure companies rely on industrial control systems (ICS) to control their hardware and software powering production. This includes machinery, manufacturing robots, and sensors. Reliable OT security tools empower operational and security teams to proactively mitigate digital risks that impair ICS and the assets they digitally control.

First-generation OT security solutions use intrusion detection systems (IDS). Typically, an IDS is combined with other security measures to protect a company's network.

With firewalls, antivirus, and anti-malware software in place, an IDS provides a second line of defense. But IDS only warns about suspicious activity already taking place; it does not prevent it.

IDS technologies are based on a sensor that uses passive monitoring of network traffic and active querying of assets, analyzes protocols, and performs Deep Packet Inspection (DPI) to detect anomalies. Industrial IDSs use the same technology while also supporting ICS protocols. They monitor the operational network via the span port. By design, IDS technology primarily alerts and reacts to activities as they occur in the network.

That is why a ***proactive*** approach to OT security and cyber-physical systems (CPS) risk management, rather than a ***reactive*** one, is critical. A reactive security posture is largely ineffective, since a breach and operational damage will have already occurred by the time you discover it.

Risks to industrial and operational security continue growing. Ensuring that production operations are ransomware-ready is now an essential security posture requirement for industrial manufacturers and critical infrastructure organizations alike. Any industry anywhere in the world can be affected. Examples include ransomware attacks against Colonial Pipeline in the U.S., a cyber attack on a Toyota supplier that caused the automaker to halt production at 14 Japanese plants, and an attack

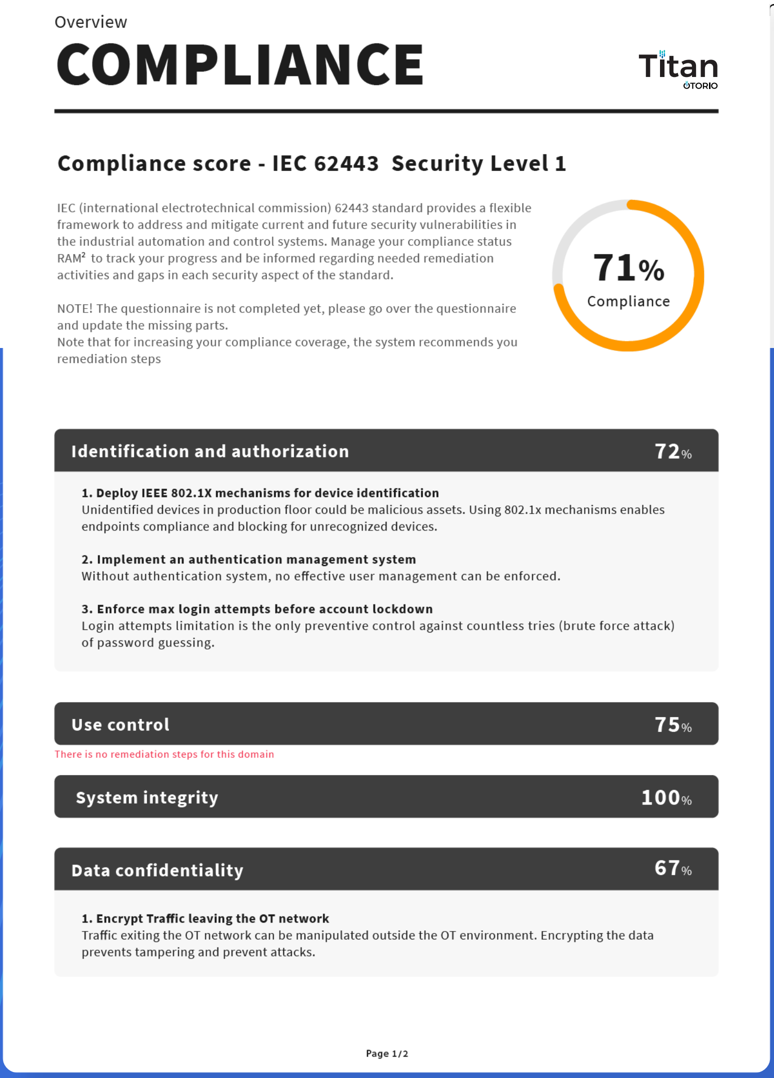
[1] Innovation Insight for Cyber-Physical Systems Protection Platforms, by Gartner Analysts Katell Thielemann and Wam Voster, 2 August 2022 - ID G00753275

and ransomware demand against Germany's building materials manufacturing giant Knauf Group. Every attack impacts an industrial company's business continuity and production operations.

Companies are undertaking digital transformations to increase their efficiency and remain competitive. IT systems are no longer the only digital channel used by manufacturers, critical infrastructure, and smart logistics businesses. Data from IT now connects with OT data and processes. Together, they help bridge the Industrial Internet of Things (IIoT) by connecting data, processes, and people.

This white paper highlights how industrial organizations can enhance the ROI of their first-generation IDS and empower their teams using OTORIO's comprehensive, industrial-native OTORIO Titan OT security solution as an overlay. Alternatively, companies that have not yet implemented OT security into their existing security stack can utilize OTORIO Titan as a comprehensive OT-IT-IIoT solution to lay a solid foundation to proactively manage digital risks and build resilient

ms to



Overview

COMPLIANCE

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 RAM^2 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

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

OTORIO Titan enables automated compliance audits and policy governance.

Achieving Digital Operational Resiliency with OT Security

Industrial companies and organizations undergoing digital transformations and those in the process of implementing security for cyber-physical systems can set tangible and achievable OT security goals. **Here are key objectives to empower your organization's teams to achieve digital operational resiliency.**

Asset Visibility: Closing Gaps and Eliminating Blind Spots

IT-specific asset inventory and monitoring tools are unable to accurately or safely track all OT assets, leaving organizations with manual and siloed collection processes for inventorying assets.

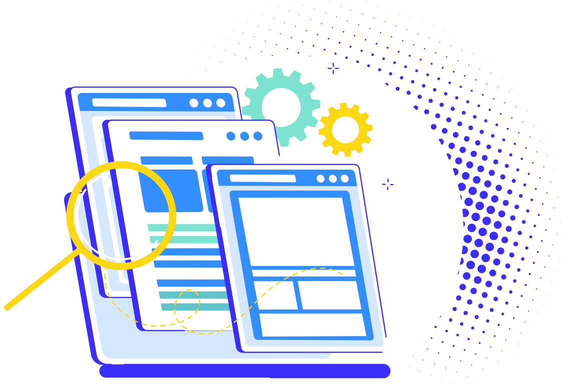
In ICS settings, industrial organizations often struggle to get the level of OT asset visibility they need to manage and secure the full range of technology assets running their industrial operations. Effective risk management requires an asset-centric view of all OT and OT–IT–IIoT network environments. Without it, manufacturers and critical infrastructure are left with gaps and blind spots in asset visibility and exposure to OT security risks.

First-generation network IDS solutions mainly deal with the network layer via passive sniffing and act only where IDS sensors are deployed. Accessible traffic does not represent all relevant network assets and their information. This means that IDS-only solutions have gaps in OT asset and network device visibility.

Extended visibility often requires including assets not accessible by the IDS. These 'blind spots' include dormant assets, those not monitored by the network due to the IDS sensors' accessibility, serial assets not in the IP layer, and those not completely connected to the network that can be added from project files and other sources.

Industrial manufacturers and critical infrastructure require full visibility of their OT asset inventory and network devices.

Without it, they are left with gaps and blind spots that can expose their operations to OT security risks and



To be most effective, an OT security solution should be able to automatically compile a complete asset inventory that covers all IT and OT assets without any gaps. Whether an individual asset, a production site, or an entire organization, asset blind spots can harm your security posture.

OTORIO's Titan OT security platform can compile a complete asset inventory from cross-domain industrial data sources for an organization, even when assets are out of reach of the IDS or when the IDS provides only partial data on them. Its proprietary passive-active querying solution is specifically designed for sensitive operational environments.

OTORIO Titan provides a comprehensive, enriched view and a single source of truth for asset inventory, seamlessly integrating with other digital security tools and industrial solutions.

Enhancing IT-OT Security Collaboration

Most industrial organizations today operate in siloed security environments. It is therefore critical to align IT and OT teams to enable them to collaborate more effectively, close security gaps, and improve operational efficiency. OTORIO Titan enables and enhances IT-OT collaboration for effective risk reduction.

Working with the CISO, a company's IT, OT, and SOC teams need to collaborate closely and effectively to safeguard the entire IT-OT landscape. This includes ICS, SCADA systems, and other processes.

Teams benefit from the central extended visibility of assets and related data from multiple sources in a unified display on OTORIO Titan's dashboard interface. The resulting data transparency is another element that helps teams collaborate with one another.

There is often a lack of collaboration between operational and security teams. The IT team comes in, segments everything, and then leaves the

[2] OT cybersecurity: no longer a niche field, Siemens

OT team to work around the segmentation.

Operational teams once relied primarily on in-house IT for security. The need for secure industrial digital transformation and production in the age of connected OT-IT-IIoT networks spurred the demand for OT security roles.

IT teams are traditionally responsible for securing corporate IT networks and data, preventing malicious attacks, data theft and exposure, malware injection, and similar high-impact criminal activities.

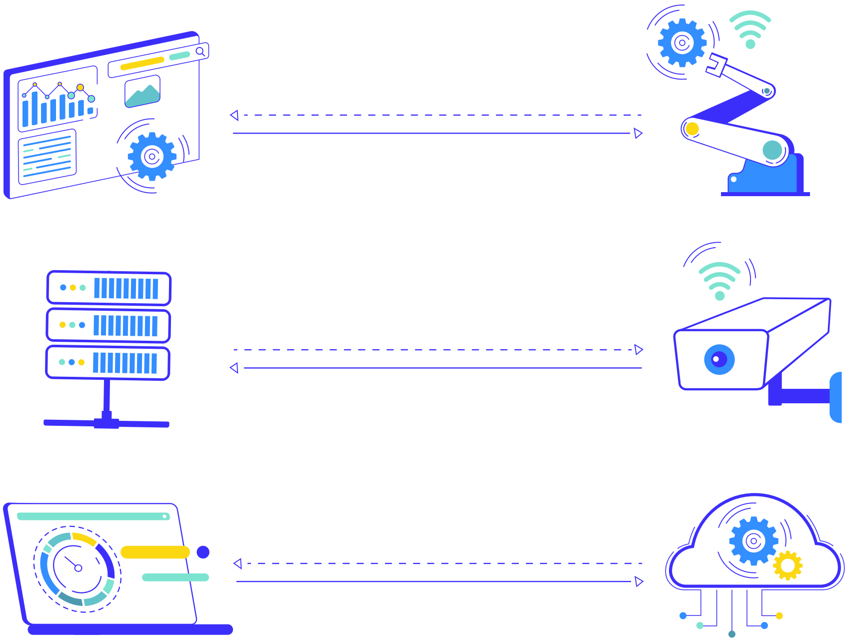
With OTORIO's Titan, IT and OT teams are truly connected and streamlined for security collaboration and effective risk reduction.

OT security professionals are responsible for operational security at industrial organizations. Their varied responsibilities include protecting digital assets, machinery, and production lines from malicious attacks that can shut down plant operations and impact business continuity. Safety, revenue, and supply chain security are all impacted by OT security breaches.

Today's demand for digital OT security professionals far outweighs the supply. According to an executive at ICS manufacturer Siemens, "Experts in OT security are even harder to find than IT experts."[2]

With OTORIO Titan, IT and OT teams are truly connected and streamlined for security collaboration and effective risk reduction. The platform provides clear, prioritized, and contextual risk assessment insights with OT security alerts, whether a single asset, a production line, or the entire organization.

This enables operational and information technology colleagues to understand what triggered an alert, what assets the risk affects, and how it impacts the entire OT-IT-IIoT network. OTORIO Titan allows risks to be mitigated quickly, easily, and effectively. The platform also provides a mechanism for collaboration and creates a common language for the



two teams.

By bridging your organization's ICS/OT security skills gap, you empower teams with a clear, easy-to-implement OT security framework.

Continuous, Proactive Risk Assessment

Wherever you are in your cyber security path, OTORIO is here to help you take the next step. OTORIO Titan empowers and supports organizations at all maturity stages of their OT security journey.

Manufacturers and critical infrastructure organizations must ensure that their operational environments remain secure and uninterrupted to protect business continuity.

This is why a ***proactive*** approach to OT security and cyber-physical systems (CPS) risk management, rather than a ***reactive*** one, is critical. Manufacturing plants, production lines, and critical infrastructure entities cannot afford to react only after their industrial operations and systems are already hacked. The damage is already done.

OTORIO's Titan delivers continuous, proactive OT security risk assessment, management, and monitoring. IDS technologies, however, are primarily reactive, responding to security incidents only after they impact an OT or OT-IT-IIoT aligned environment.

OTORIO Titan takes a different approach, delivering real-time information to constantly assess OT security risks by evaluating the security posture and prioritizing alerts with context. Risk-based alerts are prioritized by their potential impact on the business and its industrial operations.

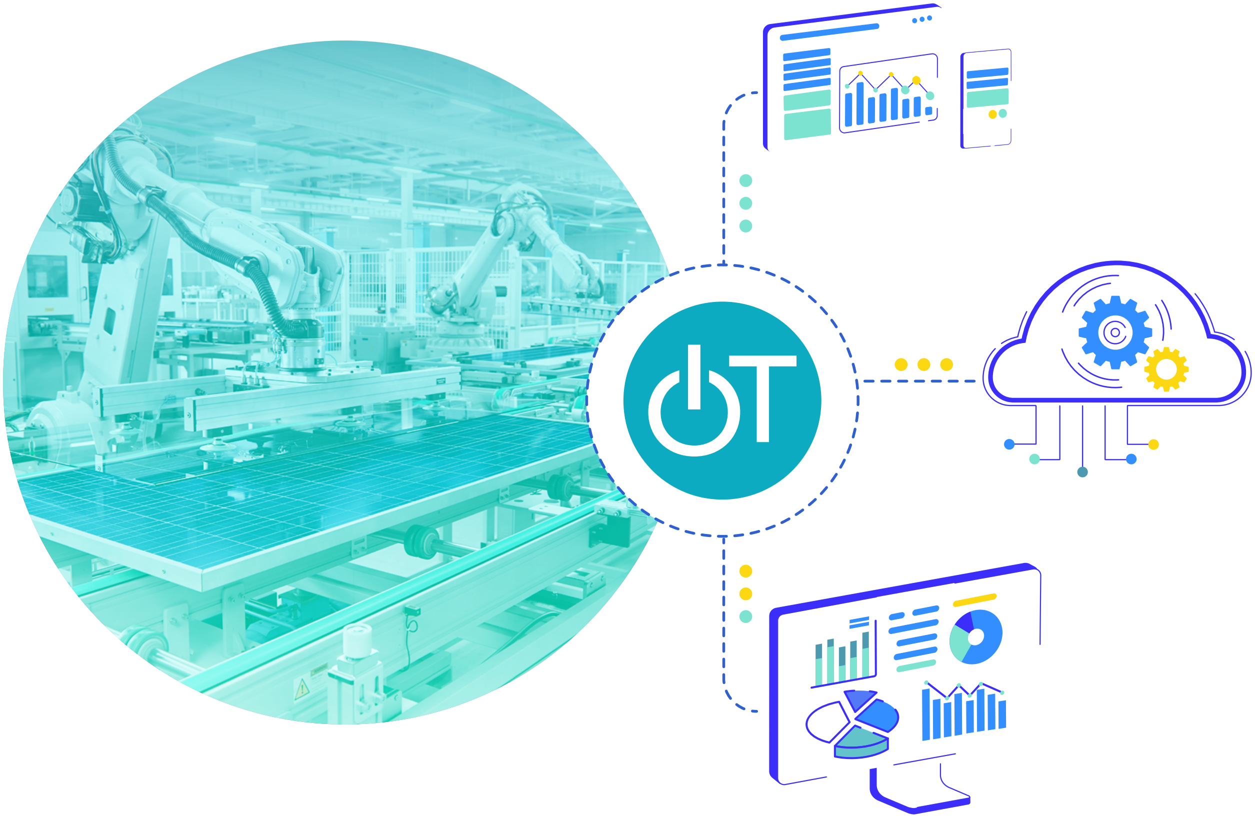
OTORIO Titan's dashboard interface gives CISOs, OT-IT SOC analysts, and operational teams central extended visibility of assets and corresponding real-time data from multiple sources in a unified display.

OTORIO Titan continuously and proactively identifies OT-IT-IIoT vulnerabilities, security gaps, and exposures, including segmentation issues and asset-level misconfigurations.

OTORIO Titan empowers OT asset owners to mitigate risk quickly, efficiently, and effectively to help prevent security breaches from ever happening in the first place. Security analysts and operations teams get clear, practical mitigation playbooks based on existing security controls, walking them through remediation steps.

Reacting to OT security risks only after a breach already happened is too little, too late. That is why car manufacturers developed automatic braking and lane-keeping assistance safety systems: they wanted technology that could proactively prevent car accidents by identifying real-time risks, and then deploy such tools in vehicles themselves to proactively eliminate or reduce the likelihood of a crash.

OTORIO Titan continuously and proactively identifies OT-IT-IIoT



Creating a Digital Twin for Safe Simulations

Another way that OTORIO Titan enhances OT security is by creating a digital twin of the IT/OT network to safely conduct breach and attack simulations of various attack vectors. Teams can collaborate on these security exercises with zero disruption to their production environments.

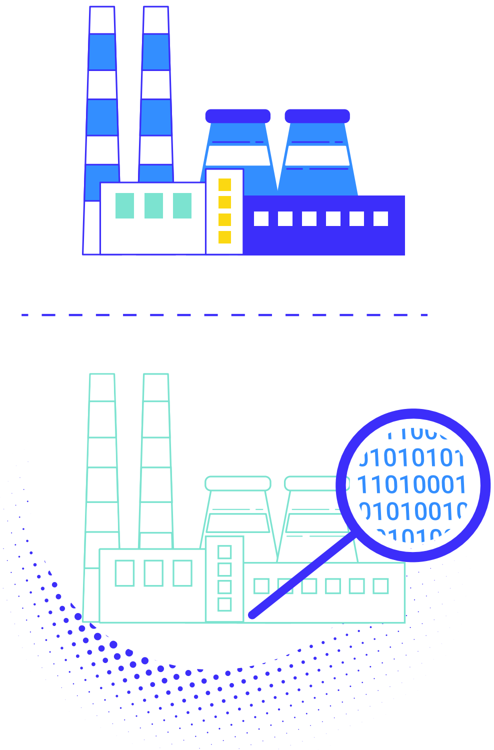
This provides operational and security teams with powerful tools to preempt and proactively remove risks before they can cause any damage. Digital twin technology is also useful for conducting vulnerability assessments and troubleshooting.

OTORIO Titan's digital twin enables risk quantification, prioritization, and explanation of OT security risks.

OTORIO Titan enables noise reduction to eliminate alert fatigue.

Reducing Noise and Alert Fatigue

Many security teams in industrial organizations experience alert fatigue. The IDS technologies driving these alerts are sensor-based. Connected OT-IT-IIoT networks have already expanded attack surface areas. With more sensors on a larger number of production lines, IDS solutions generate an overwhelming volume of events and alerts.



Even experienced SOC teams can be overwhelmed with false positives, irrelevant alerts about ghost assets, and more. Cascading alert notifications make it much harder to detect, analyze, and proactively respond to actual high-priority OT security risks.

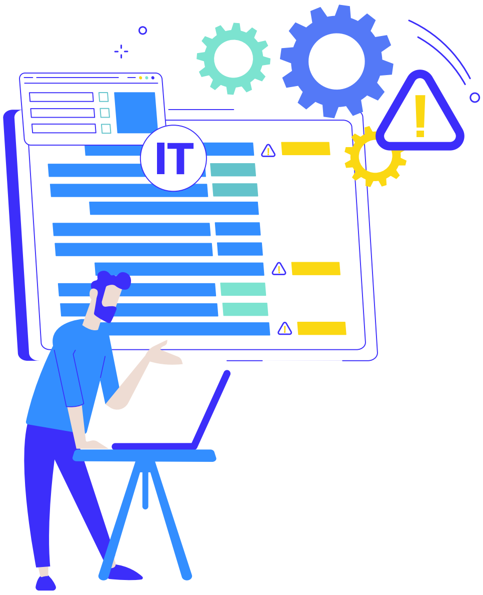
This creates alert fatigue for cyber security teams. Due to resource limitations (human and financial), truly important OT security incidents are likely to be missed or overlooked when alert noise becomes chaotic and unmanageable. This is because IDS systems create too much noise for security analysts to manage effectively, causing them to invest energy on false-positive, low-priority, and meaningless alerts.

Filtering irrelevant data helps reduce the number of insignificant alerts. This includes diminishing and eliminating the number of phantom assets and duplications that IDS systems generate.

The best way to overcome alert fatigue is to filter, contextualize, and prioritize alerts to help eliminate false alarms. Harnessing relevant, accurate insights that have real context immediately helps lower the quantity of insignificant OT security alerts. Proper risk-based prioritization also enables organizations and their security teams to manage large volumes of alerts. When you can accurately prioritize risk, you gain a real-time road map of the most important things to manage and mitigate.

Reducing noise, and, as a result, alert fatigue is also essential for mitigating actual critical security events in a timely manner. The volume of non-prioritized alerts generated by IDS systems greatly increases the workload of SOC teams. One hidden cost of IDS solutions is not knowing which OT security alerts have the highest-priority risk.

Another key benefit of reducing the flood of alert noise created by IDS solutions is that doing so bridges the gap between SOC and operational teams.



Empowering your operational team to proactively reduce OT risks gives you the added benefit of reducing noise from unmanaged assets even more. This also reduces the risk of a successful OT security attack that your SOC team would need to handle.

OTORIO Titan enables noise reduction to eliminate alert fatigue. Unlike traditional IDS solutions, the OTORIO Titan platform prioritizes and contextualizes risk alerts. This helps prevent alert fatigue and empowers SOC and operational teams to collaborate more effectively for security collaboration.

OTORIO Titan's industrial-native solution essentially provides an OT security “analyst-in-a-box” that lets teams focus on the risks that really matter. OTORIO Titan delivers tremendous value by effectively and efficiently prioritizing the mitigation of risks that have a real impact on business operations, including determining which alerts require immediate attention.

Reducing MTTD & MTTR

Key measurements of how well SOC teams manage OT security alerts include whether they are able to improve their Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) to relevant security events. These metrics also enable CISOs, operational teams, and OT and IT analysts to objectively gauge the effectiveness of their security work and collaboration.

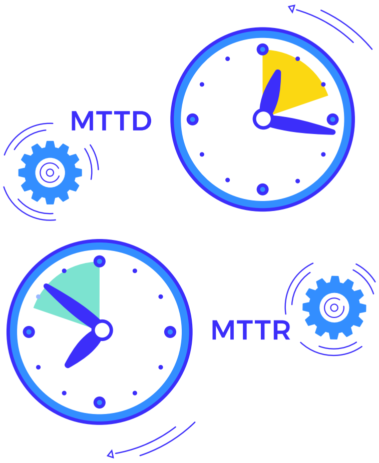
Let’s start by understanding why MTTD and MTTR metrics can be too high. As highlighted earlier, relying primarily on an IDS solution for OT security generates an overwhelming number of non-prioritized alerts that lack any context for the impact they could have on an industrial organization. Even experienced SOC teams can be overwhelmed with false positives, irrelevant alerts from ghost assets, and more. Cascading alert notifications make it much harder to detect, analyze, and proactively respond to actual high-priority OT security risks.

This forces IT and OT analysts to search for vulnerabilities among hundreds or thousands of alerts, and makes analysts rely on siloed methods to inventory them.

OTORIO Titan helps lower MTTD in several ways. Its central extended visibility and unified view for SOC analysts, operational teams, and CISOs gives all stakeholders access to the same prioritized, contextual business alerts. This enables teams to collaborate effectively and transparently to deter and eliminate actual threats using correlated insights.

The ensuing reduction in noise allows teams to use their time more efficiently, focusing on high-priority OT security risks that actually matter. Together, these advantages improve MTTD for industrial professionals whose responsibilities include OT digital and operational security. The less time it takes to detect suspicious patterns in a network, the faster an organization's teams can mitigate real security risks.

OTORIO Titan helps lower MTTD in several ways.



OTORIO Titan also lowers MTTR with a number of features that enhance teams' speed and effectiveness in responding to real OT security risks. Possibly the most impactful of these is giving operational and SOC analyst teams playbooks tailored to their specific OT-IT-IIoT environments, with clear, practical, and feasible steps to immediately start mitigating risks.

Strengthening case management for collaboration among relevant stakeholders enables faster responses by teams. Risk-based prioritization and a focus on the most important actions that an organization should take to reduce OT security vulnerabilities also reduces the time it takes to mitigate risk.

OTORIO Titan reduces the number of successful attacks on an organization by using a proactive approach to risk management and decreasing its digital attack surface, empowering teams to focus on actual threats more efficiently.

Operational teams need to focus on ensuring that production lines at industrial manufacturing and critical infrastructure companies remain ongoing, and that the quality assurance and safety controls in place are secure and reliable. This ensures that the business can continue its operations without interruption. MTTD and MTTR metrics are one measure of how well an organization's teams collaborate with one another to handle these risk mitigation responsibilities.

SOC teams with OT and IT analysts can also use MTTD and MTTR to measure their effectiveness in assessing, monitoring, and managing OT security risks, and to determine whether their collaboration with colleagues works well to reduce these risks. CISOs use MTTD and MTTR metrics to assess whether the teams they manage can identify and mitigate OT security risks in a timely, collaborative, and effective manner.

OTORIO Titan empowers operational and security analysts to use 'out-of-the-box' mitigation playbooks that empower their collaborative responses to OT security risks. OTORIO Titan enables an organization to use a personalized risk mitigation playbook that provides clear, automated, contextualized, and responsive risk elimination and reduction steps based

Automating Compliance Audits and Policy Governance

Energy and utility companies are familiar with building OT security compliance programs to meet regulatory requirements (e.g., NERC CIP, NIST CSF, IEC 62443). These programs usually focus on meeting the requirements of applicable regulatory controls to avoid being fined. This drives the significant allocation of human and financial capital resources to comply with regulations.

The U.S. and E.U. increased the demand for industrial risk and compliance assessments (e.g., TSA/CISA regulations for pipeline owners and operators[3]), in part to avoid costly penalties. OTORIO Titan provides 'out-of-the-box' compliance with industry standards and regulations.

Accelerated digitization and connectivity have eroded the "air gaps" that traditionally protected OT networks from external threats. Increased remote access by employees, vendors, and service providers has expanded the attack surface at critical infrastructure companies even more.

Customers now insist on making clear which parties are responsible for digital and supply chain risks. Contractual obligations and legal clauses are now commonly included in business contracts to clarify risk ownership and standards in commercial relationships. Automating OT security compliance audits and policy governance is an important factor in business agreements.

Corporate boards are increasingly becoming involved and being held accountable for their company's digital risk management, potentially making board members liable for damages stemming from cybersecurity attacks and breaches.

Many industrial organizations make decisions about resource allocation and business opportunities based on risk assessments. They seek to implement standardized frameworks to improve their security posture and reduce digital risks.

[3] **TSA revises and reissues cybersecurity requirements for pipeline owners and operators**, U.S. Transportation Security Administration, July 21, 2022.

The essential nature of the services provided by the energy and utility sectors focuses on availability. Malicious actors are well aware of this sensitive position regarding downtime. Because of this, they believe that energy, power, and utility companies are more likely to pay ransomware demands. The "time to action" window is narrower than ever before, and many companies in critical infrastructure must now comply with multiple cybersecurity policy frameworks. The growth of such regulations continues at a previously unimagined pace.

There has been a dramatic increase in government directives and best practice recommendations in response to digital attacks on operational networks. Illegal hacks to control **Colonial Pipeline**, a **nuclear power plant** in Kansas, and a water-treatment facility[4] in Florida are just a few real-world examples as to why there are sound policies behind compliance directives. Ensuring safety, continuous operations, and an uninterrupted supply of essential resources (e.g. power, clean water, oil, and gas) is a core principle surrounding these regulations.

An organization's internal security risk policies also create the need for regular, automated policy governance audits. Do employees only have authorized access to relevant digital assets that fall under their responsibilities? Who oversees such access, and how? When operations are at risk of human error or malicious activities by disgruntled employees, auditing compliance with such organizational policies is a must.

OTORIO Titan automates regulatory compliance and internal policy governance audits for manufacturers, critical infrastructure, and OT security consultants with risk assessment expertise. The platform facilitates 'out-of-the-box' compliance with industry standards and regulations.

This proactive approach enables effecient industrial digital risk management to strengthen an organization's risk posture, saving time and resources, bridging skill gaps, and maintaining ransomware-ready operations.

OTORIO Titan platform enables compliance audits at any level: from a single asset to an operational process, all the way to an entire organization. This automated OT compliance solution delivers accuracy and consistency, along with clear remediation recommendations.

[4] **"Florida water treatment facility hack used a dormant remote access software, sheriff says"**, CNN, Feb. 10, 2021

Who is Responsible for OT Security?

Operational Teams

The operational team generally includes asset owners, plant operations managers, and automation engineers. This critical team is responsible for ensuring continuous, uninterrupted operations for industrial production and processes.

Being on the operational front line gives this team key insights into the business impact of OT security breaches.

Generally, operational teams possess a lower level of OT security skills, but maintain an essential role in ensuring asset visibility. Instead of waiting and depending on other teams to reduce risks for them, OTORIO Titan empowers operational teams to take action. This streamlines their routines and strengthens communication among IT, OT, SOC team personnel, and CISOs. More importantly, OTORIO Titan serves as a single source of truth among the CISO, operational team, and OT, IT, and SOC teams.

CISOs

The Chief Information Security Officer (CISO) has the highest level of responsibility for OT Security at industrial manufacturers and critical infrastructure operators. They must consider the volume of asset inventory, network traffic, production processes, compliance, and governance requirements when deploying a successful OT security program.

CISOs may already be using first-generation IDS solutions, but they require a 360° view of all OT-IT-IIoT assets. They need to lower noise levels and eliminate alert fatigue. They must ensure effective ROI on their existing OT security investments and oversee compliance with relevant regulatory and internal policy governance requirements.

OTORIO Titan gives CISOs an asset-centric view of their OT-IT-IIoT networks, risks, and vulnerabilities. It also enables them to automate risk assessment, monitoring, management, and mitigation processes. Its “out-of-the-box” automated compliance capability increases efficiency and efficacy, and facilitates compliance.

OTORIO Titan's digital risk assessment helps CISOs evaluate and justify the needed financial investment in OT Security. It lets them present the platform’s contribution to operational safety, reliability, and efficiency to management and board members. It improves ROI for existing security controls, including the IDS, and enhances the SOC team’s efficiency (under the CISO's direction).

The CISO directly oversees OT security after coming from the IT side. OTORIO Titan helps CISOs connect with the operational team to get the necessary context for securing the core business of an industrial organization: safe and continuous operations.

SOC Teams

How do SOC teams effectively manage the sheer volume of alerts that OT security solutions generate? Traditional IDS-only solutions can easily overwhelm OT and IT analysts with a flood of high-volume alerts each day.

Regardless of the skill level or the number of staff, no organization has enough experienced OT security staff on hand to address this challenge. This is a significant challenge that security teams must solve.

Without the ability to recognize true high-priority OT security risks, SOC teams essentially operate in the dark. It is impossible to manually categorize such an enormous alert volume when it lacks operational context and proper prioritization.

OT and IT security analysts cannot manage digital risks effectively if they are overwhelmed with noise from too many alerts. Reducing noise enables analysts to detect actual OT security threats faster. Doing so lowers the Mean Time to Detect (MTTD), a key metric for measuring how well and how quickly industrial organizations can identify high-priority OT security risks. Reducing alert noise also improves the speed at which SOC and operational teams can respond to and mitigate risks (MTTR).

OTORIO Titan provides added value for SOC teams because its automations operate like an “analyst-in-a-box.” It provides context for your operational network by looking at vulnerabilities and assets that can be exploited, offering clear, automated playbooks to mitigate automatically prioritized OT security risks, and giving them business context. It also reduces SOC team alert fatigue and eliminates noise by up to 75%.

OTORIO Titan: The Next Step in Your OT Security Journey

Providing effective, industrial-native OT security for manufacturers and critical infrastructure companies doesn't have to be complicated. OTORIO Titan empowers operational and security teams to proactively manage digital risks and build resilient operations via a technology-enabled ecosystem. With OTORIO Titan, IT and OT teams are truly connected and streamlined for security collaboration. Wherever you are in your cyber security process, OTORIO will help you take the next step. OTORIO Titan empowers and supports organizations at all stages of their OT security journey.

Deployed at industrial manufacturers and critical infrastructure organizations worldwide, OTORIO Titan is proof that SOC analysts, operational teams, and CISOs can collaborate effectively to achieve shared operational security goals. A proactive approach to risk assessment, monitoring, and management will reduce your OT security risks quickly and effectively. Take the next step in your OT security journey, and enhance your organization's security posture so your operations are truly ransomware-ready.

About OTORIO

OTORIO is a leader in OT security solutions, dedicated to safeguarding enterprise IoT and OT environments for enhanced safety, productivity, compliance and resilience. Its flagship platform, OTORIO Titan, provides an all-encompassing suite of applications that brokers IIoT, OT, and CPS security controls into IT workflows, ensuring proactive protection and efficient risk management.

Visit OTORIO.com

OTORIO

This white paper highlights how industrial organizations can enhance the ROI of their first-generation IDS and empower their teams using OTORIO's comprehensive, industrial-native OTORIO Titan OT security solution as an overlay. Alternatively, companies that have not yet implemented OT security into their existing security stack can utilize OTORIO Titan as a comprehensive OT-IT-IIoT solution to lay a solid foundation to proactively manage digital risks and build resilient operations. In each scenario, OTORIO Titan empowers IT and OT teams to be truly connected and streamlined for security collaboration.