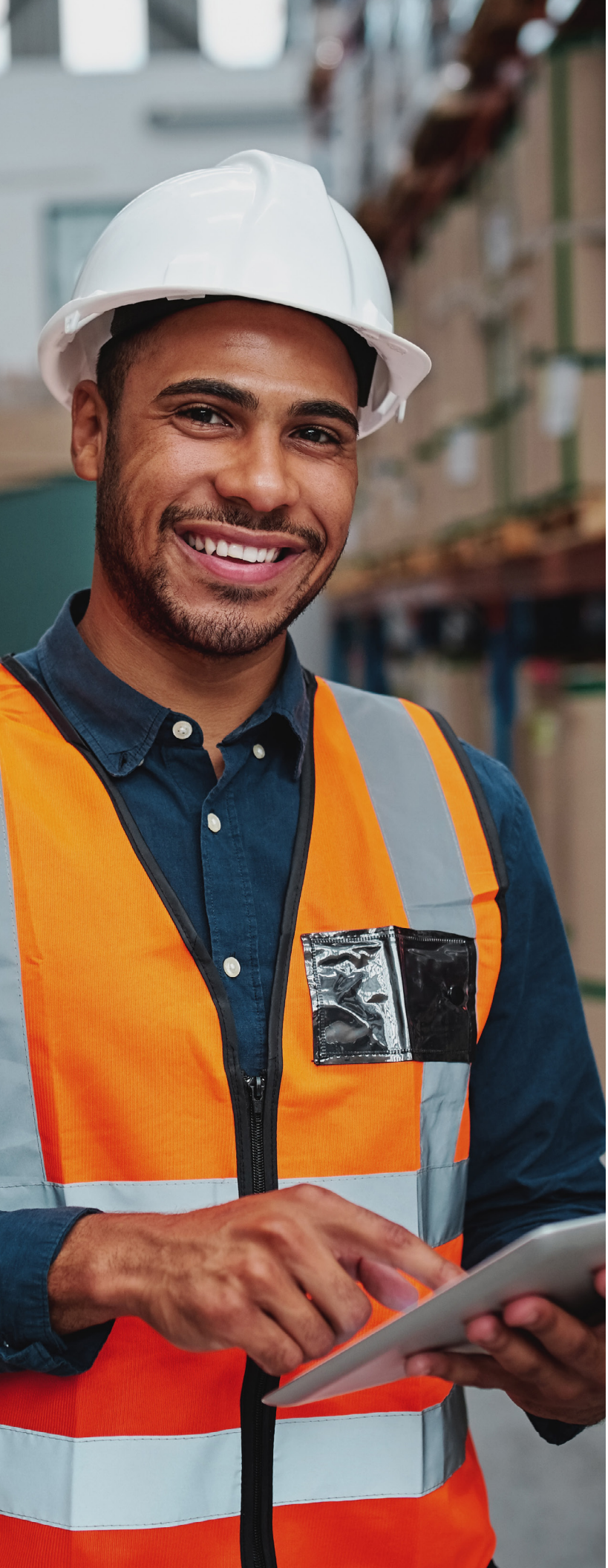


kyndryl

Point of view

Navigating Operational Technology (OT) Transformation with Integrated Security

Rigorous OTSM is key to improving organizational cyber resilience and operational technology return on investment

Highlights

- IT systems don't have a clear role in supporting industrial and manufacturing system environments
- Attackers are leveraging vulnerabilities in OT environments and making them part of their attack strategies
- To advance OTSM efforts, organizations can start with a cyber resilience maturity assessment on the current state of their OT security and Zero Trust model adoption
- An OT cybersecurity roadmap will help define requirements and accelerate implementation

Executive summary

Operational Technology Systems Management is growing in importance. Organizations use OTSM strategies to cut risks and lower operational costs, especially for cyber resilience and protecting critical operational infrastructure and industrial control systems (ICS) from cyberattacks. ICS is the increasingly connected array of digital devices, networks, and controls used in industrial processes. A rigorous OTSM approach is key to improving the overall cyber security of the organization and return on investment of OT.

The differences between OT and IT

OT systems are built to last ten to twenty years, as opposed to the five-year lifecycles of traditional information technology (IT) equipment. IT systems which support data-driven computing don't have a clear role in supporting power grids, building controls, and other cyber-physical systems of industrial and manufacturing environments. This is where OT systems come into play. OT is often controlled by manufacturing engineers, process control engineers, or instrumentation and controls technicians. These systems are critical for functional physical processes, such as power generation and transmission or manufacturing production.

OT systems contain many embedded devices running on firmware developed by specific original equipment manufacturers (OEMs) that are not built with open management interfaces. Programming these systems often means accessing OEM-specific tools to update or reconfigure them.

Definition of Operational Technology Systems Management

OTSM is about how hardware is configured, patched, managed, and deployed, how software is developed and deployed, and how teams respond to incidents. Organizations use OTSM to both cut risks and lower operational costs, especially with respect to cyber security and protecting operational infrastructure and ICS from cyberattacks.

Greater connectivity across system environments offers the hope of leveraging the cloud for advanced predictive maintenance analysis. Managing sites through centralized, remote access can result in more efficient use of labor. Operational efficiency can be improved by adjusting control parameters. Such financial drivers are so significant that the idea has been branded as Industry 4.0.

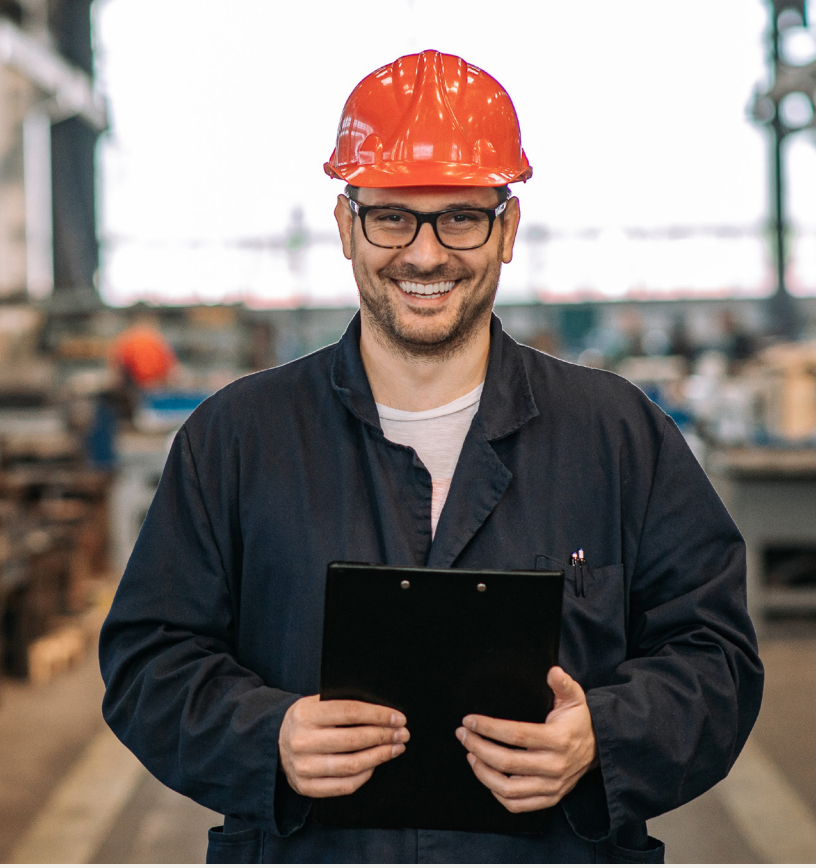
However, as such systems connect, security becomes a much bigger issue. For example, systems which are air-gapped or on an "island" from enterprise IT are isolated from internet access and communication applications such as email and cloud interfaces. Still, these systems are increasingly accessing the enterprise infrastructure to take advantage of scale and the power of big data analytics. This can pose risks to the entire organization.

As a result, while IT network access and greater connectivity are added benefits, they can come with increased threats. Examples include exposure to ransomware, hacking for espionage, terrorism, or nation state conflicts, and other potential disruptions of physical processes that can cause damage.

Given factors such as organizational boundaries, lack of skills of IT personnel on OT systems, or regulatory requirements, IT service management practices do not generally supply adequate OT system protection. Further, OT staffs are already under efficiency and headcount pressures. At the same time, many foundational elements of cyber security may not be present in OT.

Examples can include inaccurate inventories, outdated database configurations and patches, and poorly executed account and user access management. In part, these potential vulnerabilities occur because tools often don't feature common open management interfaces.

Physical networks may not be logically connected, and staff may be overwhelmed with system availability, and not focused on documentation or asset attributes. Additionally, given the sensitive, unique, and embedded nature of OT assets, there is also increased complexity and risk of deploying tools and or automation—all of which can slow OTSM adoption.



What drives the current increased focus on OTSM?

- Security concerns are top of mind for OT professionals.
- IoT and Edge devices are increasingly used throughout manufacturing facilities.
- Much of the OT environment is connected to the cloud and the IT networks, but often is not equipped for preventive action—and is at times unmonitored.
- Attackers are leveraging vulnerabilities in the OT environment and making them part of their attack strategies.
- Increases in vulnerable attack surface can result in OT facilities disruption from security breaches.
- It is increasingly common for the privileged users and administrators to have their access compromised because of weak Identity and Access Management (IAM) strategy and governance.

Growing convergence with IoT and Industry 4.0 connectivity

Increased IoT and Industry 4.0 connectivity between industrial operations and the internet and cloud is driving the need for robust OT Systems management programs. Organizations have trialed and proved connected plant initiatives for a decade. In the past few years, organizations pivoted from trial to wide-spread adoption – and this wave keeps growing. Based on multiple analyst views, these initiatives are set to increase dramatically over the next five years.

Whether it be OEMs connecting to wind turbines to regularly update the programs or monitoring the flow of fluids through a valve to tune for maximum output, we already see such connections occurring. As connectivity explodes, network protection alone will grow increasingly untenable as a solution to OT security. This begs the question: How do we use OT Systems Management program to protect ICS as convergence grows?

Robust OT cyber security and embracing OTSM

OTSM maturity is critical to protect increasingly connected industrial systems and to ensure OT cyber security measures are defending critical infrastructure from targeted and untargeted attacks. To develop robust OT cyber security roadmaps and foundations, organizations with OT systems (everything from manufacturing process controls to building control systems and security access systems) should embrace the concept of OTSM, paralleling their ITSM best practices, but within the unique environments of operating systems.

A robust OT Systems Management program (Figure 1) is underpinned by a security operations center and incident response planning. Proper visibility and access to the underlying endpoints and network data leading to insight into all hardware and software in the network are key. Also important are systems updates to reduce cyber vulnerabilities, automation for significant operational tasks, consistent reporting and monitoring, network segmentation, and finally, strong identity and access controls.

Eight foundational elements of a robust OT Systems Management program

1. Create an OT security operation center (SOC) function and develop incident response (IR) plans with IT SOC and physical OT responders
2. Build effective advanced security controls with proper visibility and access to the underlying endpoints and network data
3. Establish insight into all hardware and software in the network to ensure vulnerabilities are identified quickly
4. Properly update and configure systems to reduce opportunities for cyberattacks
5. Update for operationally efficient systems to provide automation on key operational tasks
6. Consistently report and monitor across IT and OT for simplified progress documentation
7. Segment the network as much as possible
8. Enable strong identity and access controls with multi-factor authentication (MFA) at layer 3 between IT and OT

Figure 1. 8 elements of a robust OTSM program

The future of OT cyber security

The North American electric utility industry over the past decade has adopted an increasing set of requirements of OT systems management. Figure 2 features a selected list of the major frameworks.

Despite updates, many of these sets of cyber security standards were established prior to the presence of IoT, cloud, and today's increasing endpoint vulnerabilities. As those areas expand, the need for endpoint security and Zero Trust management continues to grow.

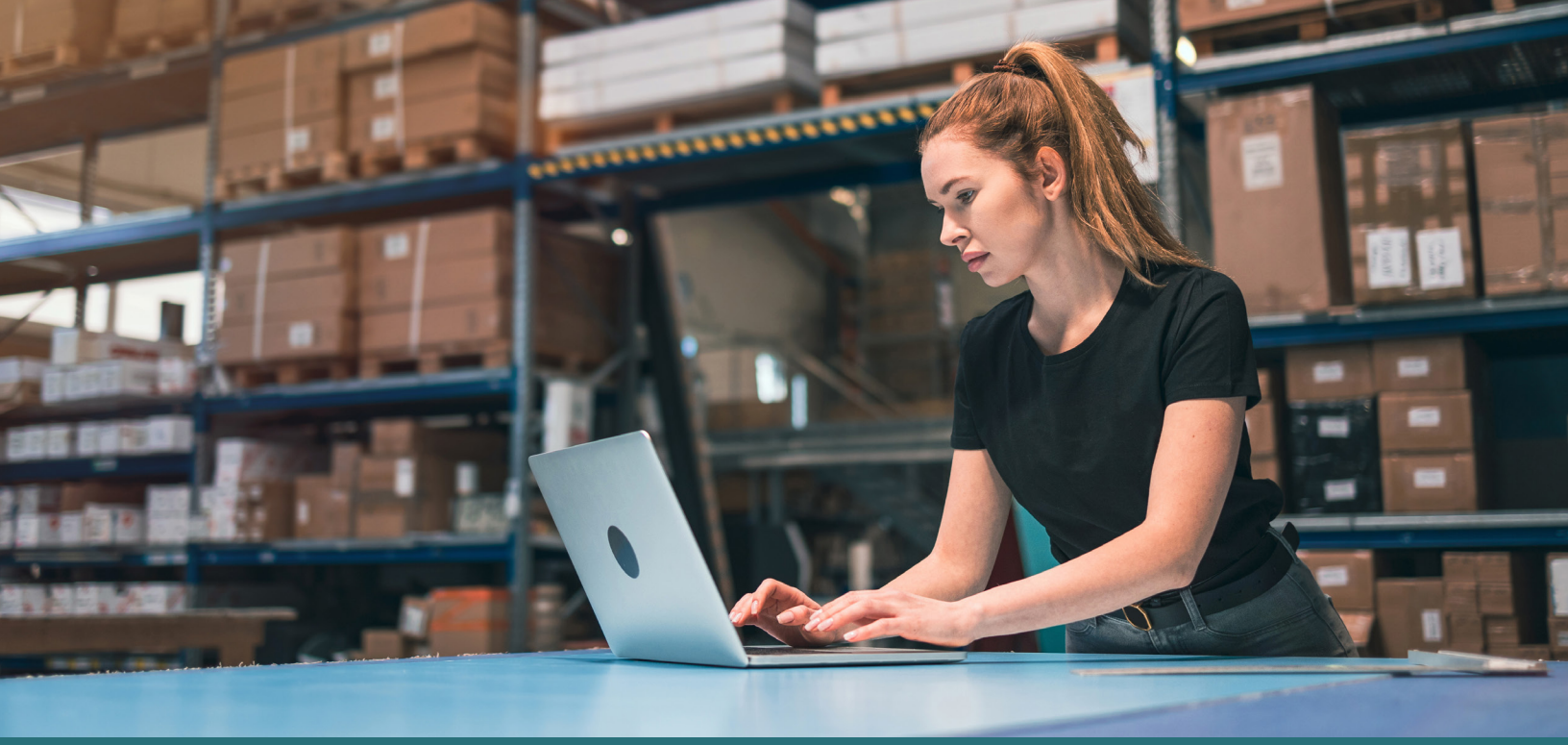
The reality is that most OT environments do not manage all the endpoints. Therefore, as these new requirements emerge, most will be relying on time-consuming manual tasks to gather critical reporting for the C-suite or regulators. Many will be using different OEM tools to try to patch systems manually or with an inefficient system by system approach. Most won't have automated asset inventory or vulnerability assessment to provide real-time visibility, so will rely on manual teams to gather this information into spreadsheets or lists.

OT security assessment and planning

The IDC predicts that by 2024, 70% of G2000 customers that have IT and OT initiatives will embark on new programs or double their spending with service partners as they race to infuse digital resiliency into their operations.[1] The Zero Trust model is fast becoming a basic security requirement for any organization.

And it is mission critical for OT environment security that identity and access management (IAM) at Purdue[2] level 3 become a priority for every organization, to include MFA implementation at access opportunities.

Enterprises that want to start or improve OTSM efforts should start with a cyber resilience maturity assessment, an analyses of physical security gaps, and Zero Trust model assessment and implementation. From there, an OT cybersecurity roadmap will help define requirements and accelerate implementation.



Partial list of regulatory and compliance models or standards for the OT industry

- → **NIST CSF**—NIST is the National Institute of Standards and Technology at the U.S. Department of Commerce. NIST supports a voluntary cybersecurity framework (CSF) designed to help organizations understand, manage, and reduce cybersecurity risk to better protect their data and networks.
- → **NSA Zero Trust Security Model**—The National Security Agency (NSA) of the United States supports a Zero Trust security model that eliminates trust in any one element, node, or service by assuming that a breach is inevitable or has already occurred.
- → **CIS Controls**—This is a set of priority actions supported by the Center for Internet Security (CIS) which help protect organizations and data from cyber-attack vectors.
- → **NERC CIP**—The North American Electric Reliability Corporation (NERC) developed a set of Critical Infrastructure
  Protection (CIP) Reliability Standards for all stakeholders affected by the reliability of the North American bulk power system.
- → **CMMC**—The Cybersecurity Maturity Model Certification (CMMC) is the United States Department of Defense framework designed to protect the defense contractor industrial base from cyberattacks.
- → **ISA/IEC 62443**—This is a series of standards from International Electrotechnical Commission (IEC) that provide specific guidance for securing industrial control systems (ICS). ISA/IEC 62443 includes asset management, security risk management, security program management, and incident response standards.
- → **Control Systems Security Program (CSSP)**—This is a program developed by the Department of Defense (DoD) to help DoD contractors and suppliers secure their control systems.
- → **ISO 27001**—ISO 27001 is an Information security management standard that provides organizations with a structured framework to safeguard their information assets and information security management system (ISMS), covering risk assessment, risk management and continuous improvement.
- → **Cybersecurity Capability Maturity Model (C2M2)**—This enables organizations to evaluate their cybersecurity capabilities and optimize security investments. It uses a set of industry-vetted cybersecurity practices focused on both information technology (IT) and operations technology (OT) assets and environments. While the U.S. energy industry led development of the C2M2 and championed its adoption, any organization—regardless of size, type, or industry—can use the model to evaluate, prioritize, and improve their cybersecurity capabilities.

Figure 2. Selected regulatory and compliance models for OT

Kyndryl and OTSM

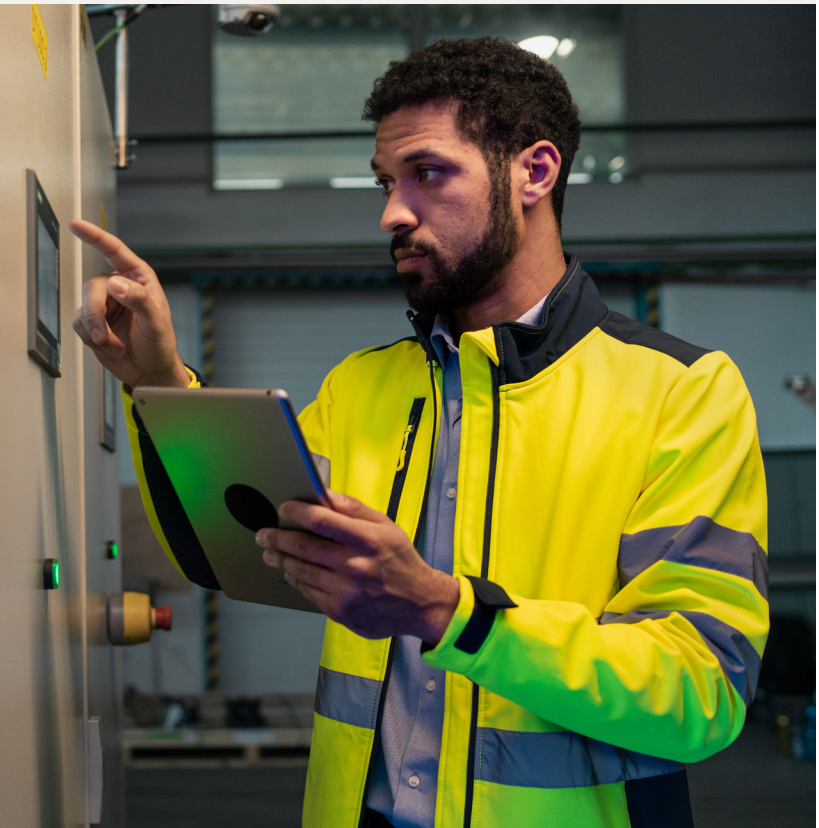
Kyndryl is a highly qualified OTSM provider with significant expertise. A prevention-first strategy focused on a deep understanding of the client environment from a focused assessment sets Kyndryl apart. We deliver the vital infrastructure, support, and services across cloud, IoT, edge, networking, security, data, AI and analytics.

Technical expertise

As a service provider to critical infrastructure, commerce, financial, manufacturing, and associated users of operational technology, Kyndryl has comprehensive knowledge about the need for cyber resiliency and the requirements clients have of their OT security. Integrated segmentation methodology, signal integrity, access control with 24/7 OT SOC wrapped around a focused assessment produces successful outcomes for Kyndryl clients.

Industry experience

Kyndryl has technology experts with decades of plant floor experience. We have the capabilities and blueprints to guide manufacturers through the challenge of modernizing their IT and OT environments and addressing the complexities of digitizing and modernizing their plant floor environment. Underpinning the transformation activities is cybersecurity across all layers, including IT, OT, network, edge, data and applications, as a central and integral part of the journey.



Kyndryl OTSM methodology and key capabilities for customers

Kyndryl's overall OTSM approach is based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0:

1. **Identify:** define a roadmap and action plan to build or improve the current cyber resilience plan
2. **Protect:** protect against attacks by discovering vulnerabilities before they are exploited
3. **Detect:** detect unknown threats with advanced analytics
4. **Respond:** respond effectively to cyberattacks and other outbreaks
5. **Recover:** recover access to critical applications and data
6. **Govern:** establish a centrally managed governance structure and risk management strategy

Kyndryl provides a comprehensive list of as-a-service OT offerings which help customers simplify and speed efforts to dramatically improve their OTSM capability. For instance, we offer OT Security-as-a-Service as well as SCADA-as-a-Service. SCADA, a technology system that collects data in real time and provides rapid analysis, is an acronym for supervisory control and data acquisition.

We apply an organized operational technology security methodology to understand your current security needs, gaps, and the daily challenges unique to your environment. Kyndryl OTSM solutions include a Cyber Resilience Maturity Assessment remote 1-day workshop, a physical security gap analysis, a Zero Trust Maturity Assessment, an OT cybersecurity roadmap, an OT Security Maturity Assessment, an OT Exposure Assessment and a Connected Factory Maturity Assessment.

Cyber Resilience Maturity Assessment 1-day remote workshop

Kyndryl Cyber Resilience Maturity Assessment (CRMA) is a remotely facilitated, one-day assessment workshop to help determine your readiness level to respond to and recover from an adverse event in your OT environment. Suitable for any mix of technology, regardless of vendor, this assessment measures your organization's ability to process new OT cyber risks, identifying where existing resilience capabilities are sufficient and where there are gaps or weaknesses.

For example, during the one-day assessment workshop, our experts evaluate controls across 23 key categories to determine the maturity level. We also examine more than 100 controls based on the current and target state and explore how to better align with NIST's five phases of an effective cyber resilience preparedness and response program. With these, and additional results from all the factors assessed in the CRMA, we create a customized roadmap and action plan for improvement.

Physical security gap analysis

Customers are challenged with providing a safe work environment that not only secures their employees but also limits access to sensitive data and systems. Kyndryl conducts a physical security gap analysis by initially evaluating factors such as your current access control and CCTV systems, camera placement and coverage, and card reader encryption. We identify the common and less-common threats which many companies struggle with. Weaknesses could involve tailgating, which allows bad actors entry to the workplace, or incomplete video coverage of indoor and outdoor areas. Additional physical security risk situations include:

- Employees sharing their ID badges, making the installation and use of any access control system an ineffectual measure
- Separate, unintegrated access and control of video surveillance systems
- Lack of automation tools (AI) to detect threats
- Aging technology to support system expansion and upgrades
- Lack of systemic management of security systems

Zero Trust Maturity Assessment

Securing an ever-accelerating agile business requires context. The Kyndryl Zero Trust Maturity Assessment (ZTMA) helps you to establish context on your own OT security challenges. Kyndryl ZTMA is a security and resiliency consulting offering helping you to overcome entry barriers on your Zero Trust journey.

The ZTMA is a critical assessment of your OT environment against manufacturing industry standard Zero Trust principles. It helps to align business and IT priorities to your individual security risks and compliance requirements. The Kyndryl ZTMA:

- Provides a vendor-agnostic Zero Trust security roadmap
- Is designed to identify and help reduce your risks around IT security and business agility
- Follows a formal use case-based approach to help mature new or existing Zero Trust capabilities across multiple security disciplines for faster Zero Trust adoption

The OT cybersecurity roadmap

A customized cybersecurity roadmap is a fundamental tool which defines an organization's security baseline and lays out a sequence of remediation activities. It addresses prioritized risk and securing the infrastructure, including:

- Comprehensive OT risk assessment
- Prioritized portfolio of initiatives
- Clear articulation of the desired end state
- Timelines, metrics, and interim objectives
- Resource requirements, such as human capital and technology

The Kyndryl OT cybersecurity roadmap acts as a playbook for the journey toward maturity and compliance. Without a clear roadmap, security often becomes a series of ad-hoc or one-off initiatives, with problems or bugs from lack of budget and gaps in security.

OT Security Maturity Assessment

This assessment helps you to understand your OT security posture and better define your strategy. You will gain comprehensive insights and precise knowledge about the status and resilience of OT environment which will in turn empower your organization to securely access your OT environment without compromising safety or introducing risks. It helps you to:

- Discover unknown devices
- Know your critical vulnerabilities and gaps
- Understand the risk of your facilities
- Understand the most relevant attacks and act accordingly
- Use industry relevant cybersecurity frameworks and tools
- Understand your security posture and focus your efforts

This assesses the state and maturity of OT cyber resilience and defines key steps to build the foundation of risk-based cybersecurity management. The phases are developed according to the most representative standards and frameworks (NIST CSF, ISA/IEC-62443) and created as modular defense strategy.

OT Exposure Assessment

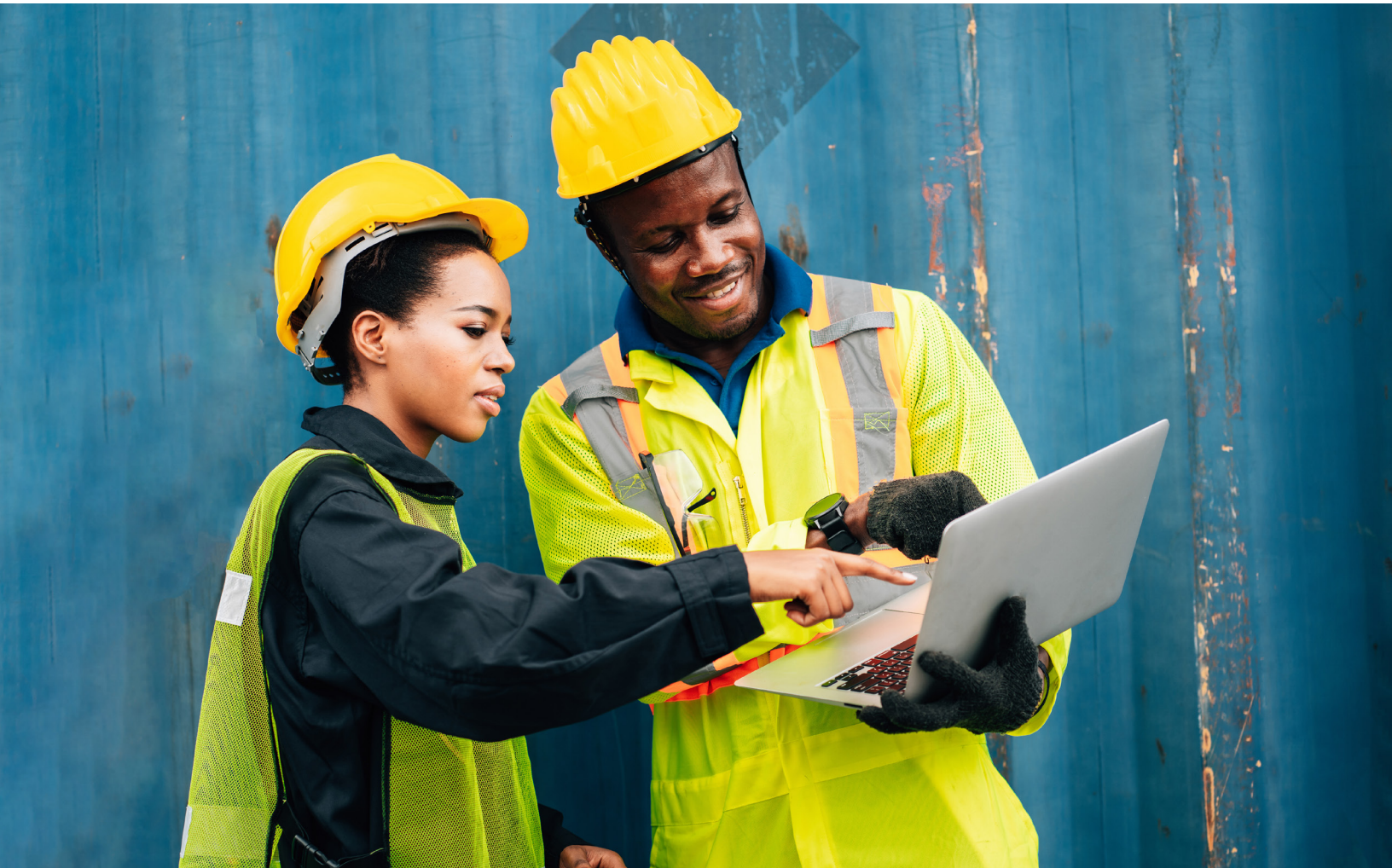
This assessment helps you with a comprehensive review of your company's Industrial exposure to the outside world, network infrastructure, architecture, and security posture. It encompasses identifying gaps, inefficiencies, and opportunities for modernization, with tailored recommendations designed to enhance performance, security, and reduce risk through the implementation of advanced technologies, automation, and best practices. Some of the key highlights of this assessment include:

- Advanced security measures: Preparation for zero trust architecture and micro-segmentation to protect against modern cyber threats
- Automated network management: Introduce automation tools to streamline operations, reduce errors, and improve efficiency
- Full visibility into data flows and production controls
- Risk assessment of all the production components and de-risk strategies
- Identification of all suspicious flows and possible malicious traffic

Connected Factory Maturity Assessment

This assessment conducts a comprehensive evaluation of a manufacturing organization's readiness to leverage real-time data for optimizing operations through secure networks, automation and advanced analytics. It helps in develop a compelling business case for a connected factory, demonstrating the potential return on investment by analyzing the current maturity levels. The assessment comprises study of:

- Current state of digital transformation, people and processes
- OT assets, connectivity, protocol compliance, system modernity, and Internet of Things (IoT) and Industrial Internet of Things (IIoT) readiness
- Current practices, integration and standards of OT cybersecurity with focus on observability, leadership
- Network and access tech stack and protocols, endpoints, agility to deploy new end points, networks and observability
- Connected workers, smart tools, IoT devices, and machinery within a secure framework
- Industrial data lakes and big data, AI applications, and the maturity of Industrial data flow.



Preventing and minimizing OT security incidents

Increasingly connected industrial systems and expanding attack vulnerabilities are driving the need for OTSM maturity, including adoption of the Zero Trust model. These are critical to ensure OT cyber security measures are protecting critical infrastructure from incidents and damage. Evaluations of cybersecurity preparedness, physical security gaps, and ZTMA readiness help manufacturers evaluate their OT security. These, along with the cybersecurity roadmap, can help organizations prevent and minimize breaches, revenue losses, and reputational damage from OT security incidents.

Kyndryl capabilities

Kyndryl is highly experienced in securing critical infrastructure in some of the most complex and high-risk industries, globally. Our expertise in networking and cyber resilience coupled with our ecosystem of 5G, cybersecurity and OT solutions partners enables us to provide cutting edge solutions tailored to manufacturing customers to enable automation via generative AI, improve operations and worker safety, and transform industrial operations.

Kyndryl's integrated approach helps manufacturers protect and recover their operations quickly to minimize operational disruptions, brand damage and financial loss. Recognized as a cyber resilience leader by top analysts including NelsonHall and Omdia, we leverage insights from our 30+ years of experience in securing complex IT and OT environments.

This experience helps us bring in a unique perspective to our manufacturing customers. Manufacturers are at different stages along the path to secure their Industry 4.0 IT and OT infrastructure. We meet them where they are, with assessments and then co-create the right solution to help them improve their infrastructure agility, security and performance, reduce costs, and meet the needs of their business.

Why Kyndryl?

Kyndryl has deep expertise in designing, running, and managing the most modern, efficient, and reliable technology infrastructure that the world depends on every day. We are deeply committed to advancing the critical infrastructure that powers human progress. We're building on our foundation of excellence by creating systems in new ways: bringing in the right partners, investing in our business, and working side-by- side with our customers to unlock potential.

For more information

Connect with an expert to discuss your IT and OT Transformation and Cybersecurity. Explore the website to learn more on how we successfully bridge IT and OT through a zero-trust lens. Visit us at kyndryl.com.

kyndryl

1. IDC FutureScape: Worldwide Future of Operations 2024 Predictions, Oct 2023 - Doc #US48535322 https://www.idc.com/research/viewtoc.jsp?containerId=US48535322

2. Instrument Society of America. Purdue Model. Theodore J. Williams (1992) The Purdue enterprise reference architecture: a technical guide for CIM planning and implementation.