tenable®

CYBERSECURITY FOR THE MANUFACTURING SHOP FLOOR

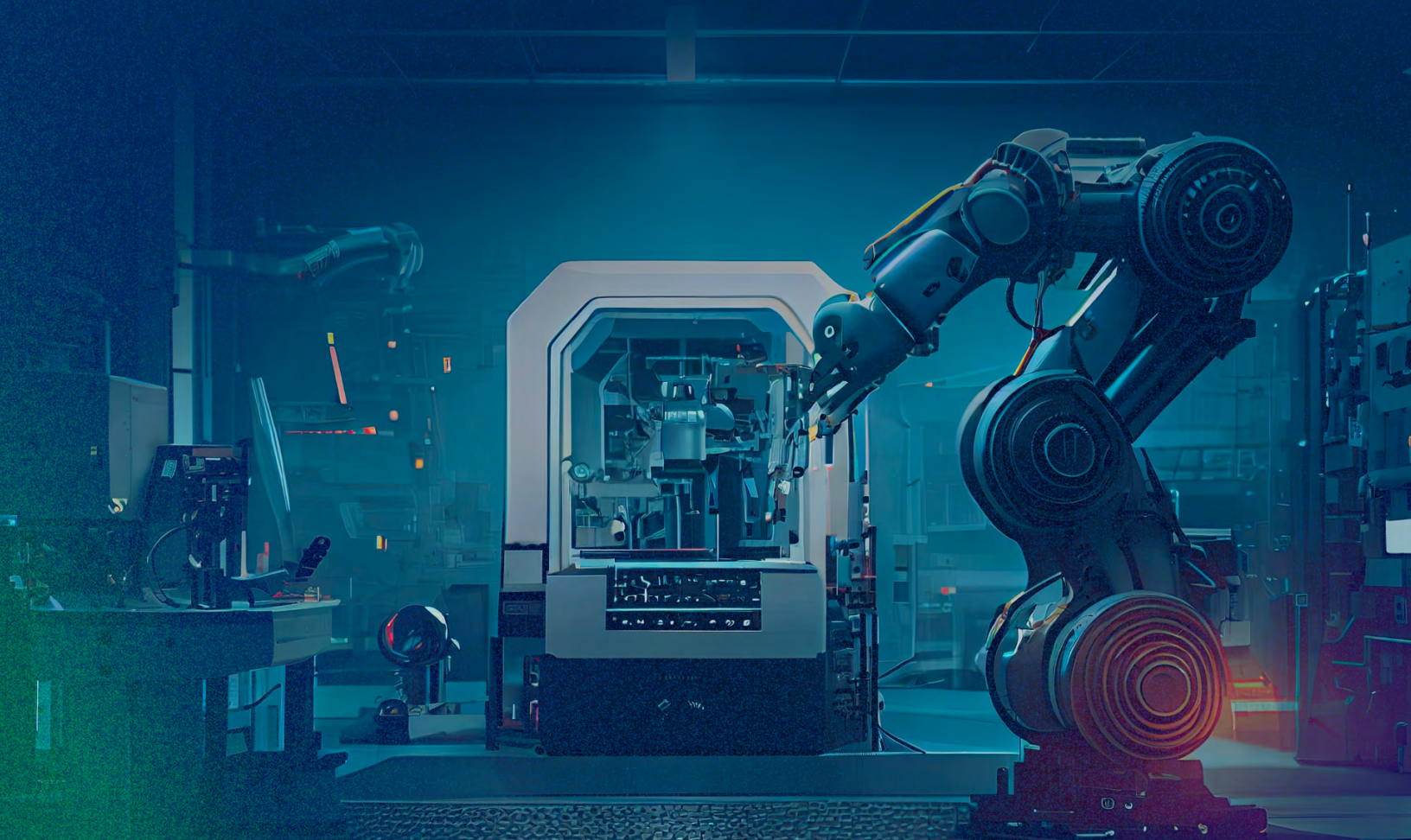


Table of Contents

DIGITIZATION IN MANUFACTURING

Digitization in manufacturing goes back to the early days of automation when manufacturers first began using computer systems to manage and control production processes. Since then, digital transformation has completely revolutionized the manufacturing plant floor, enhancing efficiency and productivity while improving quality control, reducing cost and increasing flexibility and customization. With the advent of Industry 4.0[1], organizations are becoming more agile, interconnected and data-driven, allowing them to adapt to rapidly changing market demands.

Based on a global study published by consulting firm Deloitte, manufacturers have seen a 10% increase in production output, an 11% increase in capacity utilization and a 12% increase in labor productivity by implementing smart factory digitization initiatives. Additionally, they can speed new products to market by reducing innovation development time by as much as 30%[2]. By embracing digital transformation, manufacturers can position themselves for success in an increasingly competitive and dynamic market.

However, the advantages of digitization have come at a price. According to Deloitte's 2023 manufacturing industry outlook, cyberattacks will continue to be a critical challenge in 2023[3]. As manufacturers adopt more connected technologies, new and often unprecedented challenges arise, putting productivity, safety and security at risk. Without thorough visibility and understanding of the operational technology (OT) ecosystem on your factory floor and the IT systems that support it, along with the right safeguards in place, your challenges will only compound, wreaking havoc on your organization's manufacturing operations.

CYBERSECURITY CHALLENGES BROUGHT ON BY DIGITIZATION

The integration of advanced digital systems and interconnected networks has transformed factories into complex cyber-physical environments. While this digital revolution promises immense benefits, it also brings on challenges that must be addressed to ensure the security and resilience of manufacturing operations.

Some of these challenges are:

An expanding attack surface: The digitization of factories expands the attack surface, providing more entry points for cybercriminals. With interconnected devices, sensors and systems, there are more potential vulnerabilities that can be exploited, increasing the risk of cyberattacks.

Vulnerabilities in legacy and cyber-physical system: Many manufacturing facilities still rely on legacy systems and equipment that can lack modern security controls. Integrating these systems with new digital technologies can create compatibility issues and expose vulnerabilities that cyberattackers can target. Many OT systems aren't able to receive regular updates due to the downtime required for patching. In fact, 47% of manufacturing cyber breaches are attributed to vulnerability exploits[4]. Once you know about the vulnerabilities in the environment, the challenge becomes knowing which to prioritize for remediation.

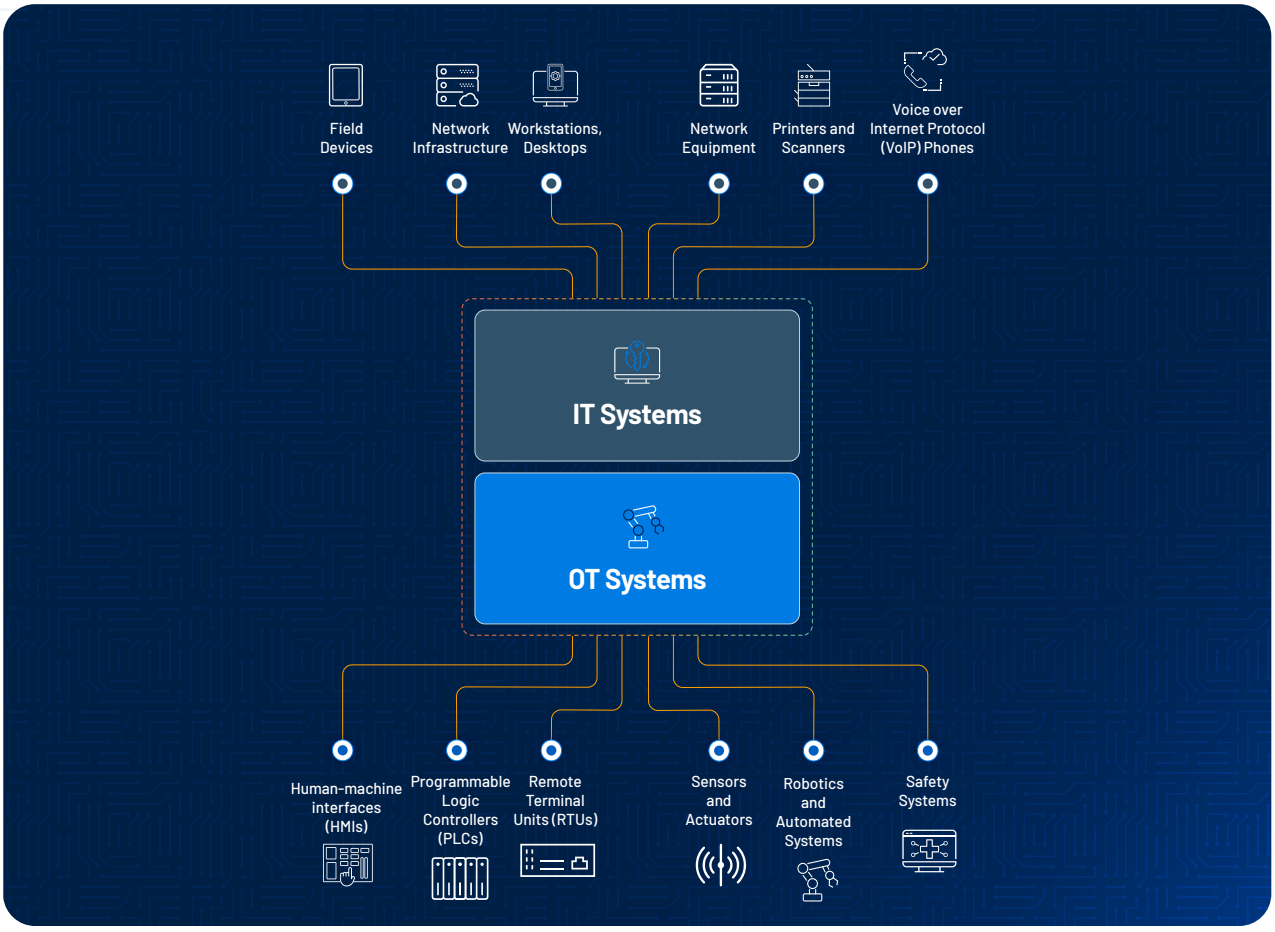
Insider threats: The digital transformation process often involves changes in workforce roles, skill requirements, and access privileges. Insiders with malicious intent, or those who inadvertently compromise security practices, can pose a significant risk to manufacturing operations, resulting in unplanned downtime. Depending on the size of the organization and the specific industry, unplanned downtime can cost anywhere from $90,000 to $6.4 million per hour of lost productivity. The vast majority of organizations (98%) claim that only one hour of downtime costs more than $100,000[5] per hour.

Evolving threat landscape: As manufacturers adopt digital technologies, they become targets for a wide range of cyberthreats, including ransomware, phishing attacks, industrial espionage and nation-state attacks.

The challenges and risks posed are a result of interconnected networks that extend across the factory floor and represent high value targets threat actors look to attack. Understanding where these threats exist and implementing robust security measures is paramount to safeguarding the integrity and functionality of the production line.

WHERE THREATS CAN EXIST IN MANUFACTURING ENVIRONMENTS

Manufacturing environments often comprise a complicated ecosystem of interconnected OT and IT devices — OT to automate production and IT to manage the OT systems. IT devices can make up half of the modern manufacturing environment. It is critical to understand the asset makeup and use a solution vendor that can provide you with holistic coverage and security across your IT and OT environment. Threats to OT systems can include unauthorized access, tampering, malware, exploitation of vulnerabilities in firmware or software and social engineering attacks. Threats to IT systems can include malicious code, tampering, and exploitation of vulnerabilities in firmware or software, network intrusions, denial-of-service (DoS) attacks and malware.



The above list is not all encompassing, but gives you a frame of reference to understand how the attack surface in a manufacturing environment can be much larger than one would assume. It is comprised of assets that security teams need to take an inventory of and maintain visibility on at all times. Threat actors patiently wait for an opportunity to exploit vulnerabilities on IT and OT devices to serve as a point of disruption and potential jumping-off point to cross into an organization's corporate network, and vice versa.

REQUIREMENTS FOR SECURING IT AND OT ON THE FACTORY FLOOR

To mitigate risks of disruption to your manufacturing operations and data compromise, manufacturers need to prioritize cybersecurity as part of their digital transformation initiatives. Securing an OT environment requires a holistic approach that involves a combination of technical controls, policies, and procedures to minimize the risk of a successful cyberattack.

Manufacturers should continuously assess their security posture and consider the following as foundational capabilities when building their OT security strategy:

- **Asset inventory:** Visibility of IT and OT devices — including their model, family, type, firmware version, operating system version, hardware version and serial number — is crucial for maintaining a proper inventory of everything in the manufacturing environment's attack surface.
- **Vulnerability management:** Vulnerability management is critical for maintaining a proactive and effective cybersecurity program for the mix of modern and legacy systems present in manufacturing environments.
- **Threat detection:** Intrusion detection capabilities in a manufacturing environment are essential for early threat warning, insider threat discovery and malware detection. Added bonus: this capability can aid in reducing the likelihood of unplanned downtime.
- **Configuration management:** As the threat landscape continues to evolve, it is vital to monitor device configurations. Human error or possible malicious activity can cause unplanned downtime, compromising the safety and productivity of the manufacturing ecosystem.

Manufacturers prioritize operational continuity and efficiency. Any disruption to production can have significant financial consequences. Traditional cybersecurity tools may generate false positives or cause downtime due to the sensitive nature of OT devices in manufacturing environments. As a result, IT-based cybersecurity tools can be intrusive or disruptive to the production processes. Addressing cybersecurity challenges requires a specialized solution designed explicitly for complex OT environments.

"The focus should be not only on **cyber defense** but also on the resiliency and continuity of businesses in the event of a cyberattack. **Increasing monitoring efforts** to check for abnormal behavior of information technology and operational technology as quickly as possible can prevent catastrophic damage."

Source: Deloitte, 2023 manufacturing industry outlook, August 2022.

HOW TENABLE OT SECURITY HELPS MANUFACTURERS

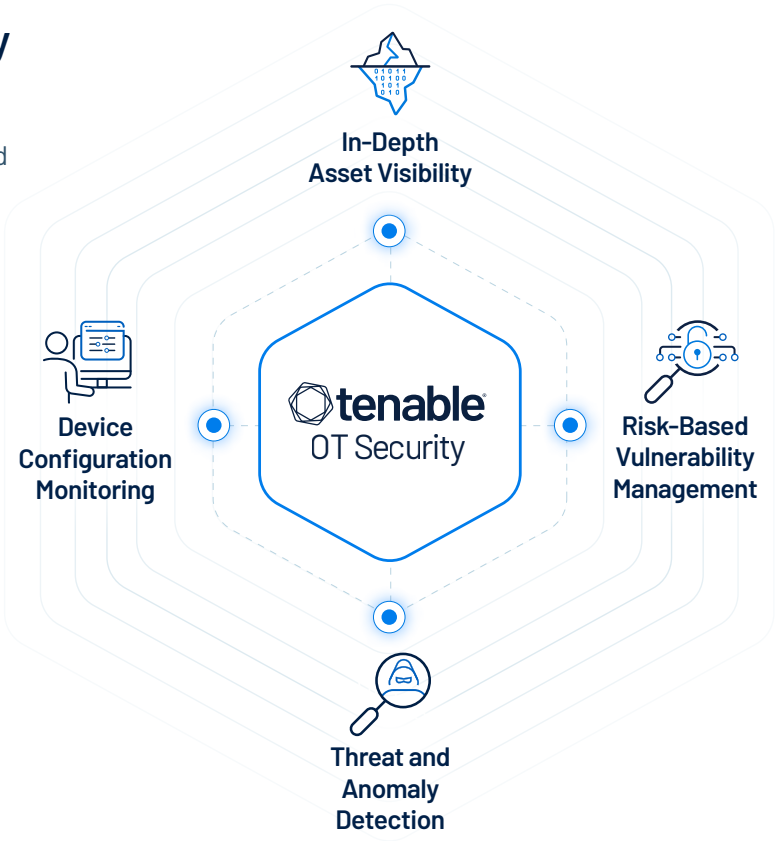
Tenable OT Security (formerly Tenable.ot) is a market-leading cybersecurity solution designed to protect complex OT environments by focusing on securing the network that controls physical processes. Specifically designed to address the unique needs and challenges of OT systems, Tenable OT Security enables manufacturers to detect threats and respond to cybersecurity incidents in real time.

FEATURES AND CAPABILITIES INCLUDE:

In-Depth Asset Visibility

Tenable OT Security provides visibility of specialized OT and traditional IT devices in the environment for a centralized view of the manufacturing attack surface. Having visibility across both domains allows organizations to comprehensively monitor, manage, and secure their entire infrastructure. It also enables organizations to identify all entry points and potential weak links where cyberattackers may attempt to gain unauthorized access or exploit vulnerabilities.

Tenable OT Security uses a hybrid asset discovery approach, passively monitoring to discover devices communicating on the network and, once they are classified, scanning IT assets with Nessus — Tenable's flagship vulnerability scanner — while safely querying OT assets using their native protocols. Tenable OT Security maps all connected devices, systems and network components, tracking firmware and OS versions, internal configurations, running software and user data, as well as serial numbers and backplane configuration for both IT and OT equipment.



Risk-Based Vulnerability Management

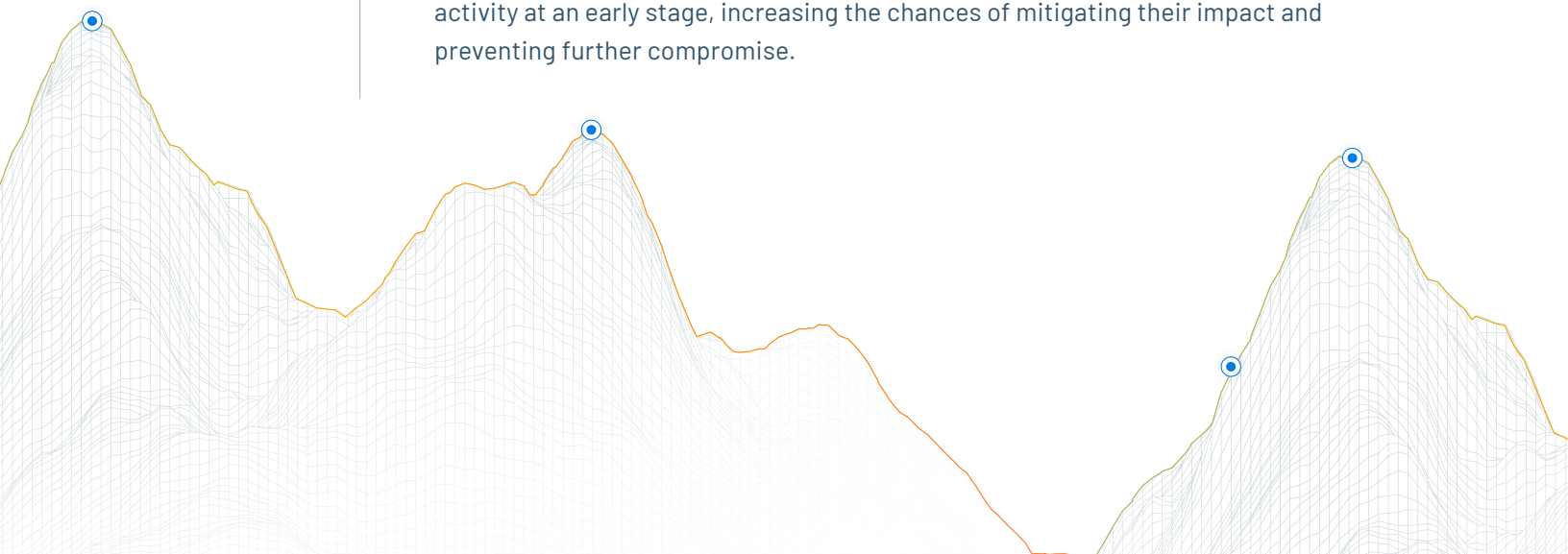
Tenable OT Security's vulnerability assessment capabilities help identify and mitigate security "soft spots" within a manufacturing organization's OT systems, networks and applications. By proactively addressing vulnerabilities, organizations can reduce the risk of successful cyberattacks.

Tenable OT Security incorporates asset criticality ratings (ACR) to help security practitioners identify the assets critical to the operation environment. It also layers on a vulnerability priority rating (VPR) to calculate the exploitability of the vulnerabilities present in the environment, helping security practitioners prioritize remediation of the vulnerabilities that pose the greatest risk to an organization. This enables organizations to focus their resources on the most critical areas of their infrastructure. By using a risk-based vulnerability management approach, organizations can reduce the risk of successful cyberattacks and minimize the potential impact of security breaches.

Threat and Anomaly Detection

Tenable OT Security continuously monitors manufacturing environments for threats and anomalous activity, providing early warning of potential cybersecurity incidents. This is achieved by detecting anomalies in traffic patterns, such as excessive traffic requested of an asset. Additionally, threats can be detected using out-of-the-box and customizable policy rules — for example, events where a controller setting deviates from an approved parameter.

Tenable OT Security's robust intrusion detection system (IDS) engine leverages Suricata rules written by the Tenable Research team to identify threats that may be lurking in the manufacturing environment. This combination of detection technologies enables security practitioners to identify insider threats from malicious employees, misconfigurations and exposure to malware. Rapid and early detection allows organizations to identify security incidents or suspicious activity at an early stage, increasing the chances of mitigating their impact and preventing further compromise.



Device Configuration Monitoring

As the sophistication and frequency of cyberattacks continue to increase, manufacturers need to maintain vigilance and adapt their security measures accordingly. Tenable OT Security captures a snapshot of device configuration, firmware version, software updates, complete ladder logic, diagnostic buffer and tag structure, to identify a known "good" state as the baseline setting. Once the baseline is established, Tenable OT Security keeps track of a full history of controller versioning and ongoing activities, monitoring for changes to device configurations and behavior in real time.

By capturing complete baseline snapshots of IT and OT devices, security practitioners can identify deviations or unauthorized modifications that may indicate security risks, misconfigurations or potential attacks. Device configuration monitoring enables organizations to support audits and assessments by capturing and documenting configuration changes and activities, all of which are difficult data points to gather from a heterogeneous environment without extraordinary amounts of manual work. Additionally, visibility of device-level configurations enables security professionals to keep pace with the evolving threat landscape by identifying malicious behavior as well as misconfigurations that can significantly impact manufacturing operations.

Tenable combines the above capabilities with an unmatched reputation for cybersecurity expertise, thought leadership and customer support, to ensure manufacturing customers can successfully safeguard against cybersecurity threats, now and in the future.

About Tenable

Tenable® is the Exposure Management company. More than 40,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include approximately 60 percent of the Fortune 500, approximately 40 percent of the Global 2000, and large government agencies.

Learn more at www.tenable.com.

CONCLUSION

In conclusion, digitization in manufacturing has brought significant benefits and opportunities for organizations. The integration of digital technologies and the adoption of Industry 4.0 principles have revolutionized manufacturing operations, leading to increased efficiency, productivity and flexibility. Manufacturers have experienced tangible improvements, including higher production output, increased capacity utilization and improved labor productivity.

However, along with these advantages come cybersecurity challenges that must be addressed. The expanding attack surface, legacy system vulnerabilities, insider threats and the evolving threat landscape pose risks to the security and resilience of manufacturing operations. Traditional cybersecurity tools are not sufficient in addressing these challenges due to the unique operational constraints in manufacturing environments, as well as the sensitive nature of legacy OT devices.

Tenable's market-leading OT security solution is designed specifically for the challenges faced by manufacturers, providing in-depth asset visibility, risk-based vulnerability management, threat and anomaly detection, and device configuration monitoring. Manufacturing customers can rely on Tenable's reputation for developing cutting-edge cybersecurity products, thought leadership and supporting customers to overcome cybersecurity challenges. By prioritizing cybersecurity and implementing Tenable OT Security, manufacturers can safeguard their operations, mitigate risks, and position themselves for success in the digital era.

Sources

- McKinsey, "What Are Industry 4.0, the Fourth Industrial Revolution, and 4IR?" August 17, 2022.
- Rick Burke et al., "Reshoring or localization on your mind?" Deloitte Insights, September 16, 2021.
- Deloitte, 2023 manufacturing industry outlook, August 2022.
- IBM, X-Force Threat Intelligence Index, 2020
- Pingdom Team, Average Cost of Downtime per Industry, January 9, 2023.