SOLUTION BRIEF

TENABLE OT SECURITY AND THE NIS2 DIRECTIVE

Summary:

- NIS2 aims to establish a higher level of cybersecurity and resilience for organisations operating within the European Union.
- The new Directive brings into scope additional industrial sectors and focuses on providing guidelines to ensure uniform transposition in local law across EU member states.
- Member states have until 17th October to transpose NIS2 to national law.
- Organisations should start preparing for this by defining their compliance roadmap and optimising their cybersecurity awareness.

What is new in the NIS2 Directive?

The Directive on the Security of Network and Information Systems (NIS) was first established in July 2016. When introduced, it encompassed operators of essential services intending to strengthen cybersecurity resilience in EU members' critical industries. While somewhat effective, NIS was seen to have limitations, particularly the narrow scope of organisations covered. This was addressed in January 2023, when the European Union adopted a new version of the Directive known as NIS2.

Who is impacted by NIS2?

NIS2 expands the scope of entities covered and has been broken into two categories — **Essential** and **Important**.

ESSENTIAL (EXISTING)	IMPORTANT (NEW)
• Energy • Transportation • Banking and financial infrastructures • Healthcare • Drinking water and wastewater • Digital infrastructure • Public administration • Space	• Automotive • Postal/courier services • Waste Water • Chemical (manufacture, production, distribution) • Food (production, processing, and distribution) • Manufacturing of medical, electronic, transportation, or related equipment • Digital provider • Research

This impacts:

- Any large organisations with a headcount of over 250 employees or over €50 million annual revenue;
- Any medium-sized organisations with a headcount over 50 employees or over €10 million annual revenue from the sectors identified in NIS2.

Member states may extend NIS2 requirements to organisations that do not meet these revenue criteria but who do play a key role in supporting the health, safety, and/or stability of the EU.

Penalties for non-compliance:

For essential entities: Fines up to €10,000,000 or 2% of the total annual worldwide turnover in the previous fiscal year of the company to which the entity belongs (whichever amount is higher).

For important entities: Fines up to €7,000,000 or 1.4% of the total annual worldwide turnover in the previous fiscal year of the company to which the entity belongs (whichever amount is higher).

When does this come into effect?

All EU member states will need to transpose NIS2 into national law by October 17, 2024.

Although no longer bound by EU regulations, the UK government has confirmed it will strengthen its NIS regulations as well.

NIS2 Directive Requirements

EU members need to ensure that their essential and important organisations take appropriate technical, operational and organisational measures to manage the risks posed to the security of their networks and information systems to prevent / minimise the impact of cyber incidents.

As a baseline, NIS2 recommend these cybersecurity risk-management measures be implemented:

1. Policies on risk analysis and information system security
2. Incident handling
3. Business continuity, such as backup, disaster recovery, and crisis management
4. Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers
5. Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure
6. Policies and procedures to assess the effectiveness of cybersecurity risk-management measures;
7. Basic cyber-hygiene practices and cybersecurity training
8. Policies and procedures regarding using cryptography and, where appropriate, encryption
9. Human resources security, access control policies and asset management
10. The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate

Incident Reporting

Whilst NIS required significant cyber incidents to be reported, NIS2 introduces a three-step process for reporting deadlines:

- Within 24 hours of identifying any incident with significant impact an early warning should be communicated to the competent authority or CSIRT.
- This should be followed after 72 hours with a full notification report including the assessment of the incident, severity and impact and indicators of compromise.
- A final report must be communicated within a month.

While detecting incidents is important, the onus for organisations should be on reducing the risks faced and preventing incidents in the first place.

Will compliance with NIS2 equate to stronger security?

Compliance with NIS2 is mandatory, and failure to adhere can result in large fines. However, organisations should not be lulled into a false sense of security that, by ticking the relevant boxes, they are secure. The reality is that adherence with NIS2 principles will strengthen defences, but that does not always equate to being secured.

Organisations should use NIS2 as a guide to minimise their cyber risk and not the defacto standard. The onus has to be on every organisation to implement secure working practices that protect their infrastructure and the sensitive data and critical systems contained.

Preventing cyber incidents requires full visibility into all assets and exposures, extensive context into potential security threats, and clear metrics to objectively measure cyber risk. Organisations that can anticipate cyber attacks will be the ones best positioned to defend against today's emerging threats.

True cyber security requires complete and holistic understanding of the risks that exist within the entire infrastructure. A preventative approach in Industrial cybersecurity is paramount to eliminate many of the core risks associated with the new trends and challenges that are present. When threat actors evaluate a company's attack surface, they're probing for the right combination of vulnerabilities, misconfigurations and identity privileges.

This requires a holistic view of both IT and OT environments, the interdependencies that exist for critical functionality, and determine where weaknesses and vulnerabilities exist.

Once a holistic viewpoint is established, the next step is to identify what would cause theoretical versus practical damage. From this stance, steps can be taken to remediate the risks where possible, or monitor the assets related to the risk for deviations, to attacks.

How can Tenable Help?

Tenable OT Security brings visibility, security, and control to industrial environments, critical infrastructure, building management systems, and more, helping organizations maintain productivity and stay safe from cyber attacks.

Tenable's primary goal is to help customers minimise their cyber exposure to be able to perform risk management and reporting, which is one of the three key pillars of NIS2.

NIS2 MINIMUM GUIDANCE REQUIREMENTS	TENABLE OT SECURITY CAPABILITIES
Policies on risk analysis and information system security	Tenable OT Security enumerates cyber-risk at the asset, site and estate level, feeding into organisation risk management procedures.
Incident handling	Tenable OT Security includes robust, policy-based security and system integrity monitoring and SIEM integration that can be integrated into a wider security incident policy framework.
Business continuity, such as backup, disaster recovery, and crisis management	Tenable OT Security can be a supporting technology for your business continuity, disaster recovery and crisis management programs. For example, Tenable OT Security can track software, firmware and configuration states of many components in industrial networks, giving you independent validation tools to ensure your restore processes have returned failed equipment to their intended working states. Furthermore, Tenable OT Security's event tracking and security monitoring capabilities, including full packet capture, can be a contributing technology to your crisis management process, should that crisis be the result of internal/external or accidental/intentional activity.
Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;	Tenable OT Security provides tooling to track compliance of your IT and OT equipment to your supply chain security standards. Furthermore, Tenable OT Security monitoring helps you track real-time activities and behaviours of your supply chain partners where they interface into your own environment.
Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;	In the OT domain, Tenable OT Security contributes automated inventory discovery, vulnerability discovery and lifecycle management, configuration drift tracking essential in maintenance and comprehensive reporting and validation, supporting technologies in the processes of disclosure and remediation.
Policies and procedures to assess the effectiveness of cybersecurity risk-management measures;	Ensuring policies and procedures can assess the effectiveness of risk management measures requires initial measurement of risk and validation of changes brought about by the measures under test. Tenable OT Security has an array of detection methods for configuration state, vulnerability, network access and risk inference systems that can be an essential contributing technology to such programs.
Basic cyber hygiene practices and cybersecurity training;	Tenable OT Security is an essential supporting technology to your cyber hygiene practice as it provides an array of detection facilities to aid in measurement and reporting.

(Continued)

Policies and procedures regarding using cryptography and, where appropriate, encryption;	Tenable OT Security can support your policies and procedures as it can detect and alarm on the use of cleartext protocols, weak encryption algorithms and commonly exploited protocols.
Human resources security, access control policies and asset management;	Tenable OT Security Supports these control policies via logging communications, to and from your assets, alterations to software, firmware, hardware, software configurations within the network and providing alerting policies targeted over different parts of the day or during specific times such as maintenance periods.
The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.	Tenable OT Security provides audit facilities useful for support in your MFA policies by ensuring computers are appropriately configured to use MFA techniques. Similarly, Tenable OT Security includes security monitoring that can ensure voice, video and text are being transmitted over secure channels.

Specifications and descriptions are subject to change without notice. Tenable disclaims all warranties and guarantees regarding this information. The use of Tenable products alone does not guarantee legal compliance. The information in this document does not constitute legal advice. Customers are solely responsible for compliance with all laws and regulations and should consult their own legal counsel for advice regarding such compliance.

While the NIS2 Directive requires effort, it is essential not only for legal adherence but also for strengthening your organization's cybersecurity posture. Embrace the opportunity to elevate your security measures, safeguard against common threats, and enhance overall
cybersecurity maturity.

Tenable OT Security brings visibility, security, and control to industrial environments, critical infrastructure, building management systems, and more, helping organizations maintain productivity, meet compliance requirements, and stay safe from cyber attacks. Using a patented hybrid discovery approach to safely gain visibility into devices and cyber-physical systems without causing disruption, Tenable OT Security delivers a thorough asset inventory along with deep situational awareness across all global sites, all in a single interface. From vulnerability management and threat detection, to configuration control and reporting, Tenable OT Security lets organizations prioritize action and enables their IT and OT security teams to work better together.

Are you not sure where to start, or need assistance in your security journey? We'd be happy to help you toward your compliance efforts. For more information on how Tenable can help your organization, check out our Tenable OT Security and NIS2 Directive solutions pages.

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.

For More Information: Please visit our Tenable OT Security page
Contact Us: Please email us at sales@tenable.com or visit tenable.com/contact