tenable

SOLUTION BRIEF

NIS2 DIRECTIVE:
HOW TENABLE CAN HELP EU ORGANIZATIONS ALIGN WITH THE NEW DIRECTIVE

Background

The NIS2 Directive strives to elevate cybersecurity and resilience standards for organizations within the European Union (EU). Expanding its scope, the new directive emphasizes uniform transposition in local laws across EU member states. To align with NIS2 principles, organizations need to initiate preparation by defining compliance roadmaps and enhancing cybersecurity awareness.

Challenges

The NIS2 Directive is mandatory and accompanied by potential hefty fines. However, mere checkbox compliance doesn't ensure absolute security. While adherence to NIS2 principles strengthens defenses, it should not be the sole standard. Each organization bears the responsibility of implementing secure practices for infrastructure, sensitive data, and critical systems.

Effective cybersecurity demands a comprehensive understanding of risks across the entire attack surface. A preventive approach is vital to eliminate risks like vulnerabilities, missing patches and misconfigurations that threat actors exploit.

Implementing the NIS2 Directive introduces various challenges for organizations:

- Compliance Costs: Meeting NIS2's requirements, especially for smaller organizations, can strain budgets.
- Technical Complexity: Technical challenges arise, especially for large systems, in meeting NIS2 standards and addressing vulnerabilities.
- Harmonization: Aligning NIS2 implementation across EU states is challenging due to different interpretations.
- Incident Reporting: Implementing NIS2's incident reporting is challenging, especially for organizations without prior procedures.

Solution

Tenable provides a range of cybersecurity products to assist organizations in achieving compliance with various cybersecurity frameworks, including alignment with the NIS2 Directive. Tenable's product suite and exposure management platform covers many of the essential aspects required by NIS2, offering comprehensive solutions for improved cybersecurity and risk management protection.

Key Benefits

- **Inventory the Entire Attack Surface**
  Gain visibility of all traditional IT, web, containers and cloud assets that comprise critical network and information systems.
- **Identify Weaknesses**
  Identify vulnerabilities, misconfigurations and other weaknesses that require remediation.
- **Prioritize Remediation**
  Vulnerability prioritization based on factors such as asset accessibility, availability impact, exploitability and threat intelligence efficiently focuses remediation/mitigation.
- **Measure Exposure Over Time**
  Chart progress over time and highlight possible trouble spots.
- **Streamline Reporting**
  Provide reporting to National Competent Authorities of effective implementation of security measures.

How Tenable Helps

Tenable offers a range of cybersecurity products designed to help you align with the compliance measures outlined within the NIS2 Directive, covering many of the aspects required by NIS2. User-friendly interfaces and intuitive tools simplify the process, addressing compliance measures with ease. Expert support is available for tailoring solutions to customer needs.

Vulnerability Management: Tenable's solutions help organizations identify and address vulnerabilities in their network and information systems. This is crucial for complying with NIS2, which requires organizations to implement measures to manage and mitigate cyber risks.

Continuous Monitoring: Tenable's solutions offer continuous monitoring capabilities, allowing organizations to keep a constant watch on their network and information systems. This is important for detecting and responding to incidents as required by NIS2.

Incident Detection and Response: Tenable's tools help aid in the detection of cybersecurity incidents, helping organizations meet NIS2's incident reporting requirements. Quick incident detection and response are essential for compliance.

Compliance and Reporting: Tenable solutions include reporting features that help organizations demonstrate compliance with various cybersecurity regulations. This can be valuable for NIS2 compliance, as organizations are required to report incidents and maintain proper documentation.

Risk Assessment: Tenable's tools assist organizations in conducting risk assessments and evaluating the effectiveness of their cybersecurity risk management measures.

Security Hygiene Practices: Tenable solutions may support organizations in implementing basic cyber hygiene practices and cybersecurity training, which are required by NIS2.

Mapping Tenable Capabilities to NIS2 Directive Requirements for Cybersecurity Risk Management

The table below outlines the capabilities provided by solutions within Tenable's products and maps them to the requirements set forth by the NIS2 Directive:

NIS2 DIRECTIVE REQUIREMENT	HOW TENABLE CAN HELP	TENABLE SOLUTION
Chapter IV, Article 20, Governance		
2. Member States shall ensure that the members of the management bodies of essential and important entities are required to follow training, and shall encourage essential and important entities to offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity.	Training courses and certifications to help customers and partners get the most out of Tenable products and gain access to latest expertise for security best practices.	Tenable Training and Certification
Chapter IV, Article 21, Cybersecurity Risk-Management Measures		

2 (a) Policies on risk analysis and information system security;	Gain insights into assets, systems, vulnerabilities, and cyber and operational risks across the attack surface. Extensive visibility empowers automated definition and enforcement of network security policies, mitigating exposure to potential risks. Provides context for security teams to communicate risk and prioritize the threats that may have the largest impact.	Tenable One;
		Tenable Vulnerability Management;
		Tenable Security Center;
		Tenable OT Security;
		Tenable Cloud Security;
		Tenable Identity Exposure

2 (b) Incident Handling	Provides real-time monitoring of known and unknown assets, tracking vulnerabilities, and identifying threats before breaches occur. Extends to simplified incident response and investigation, with alerting on unusual identity behavior. Audits cloud environments for security incidents, and provides granular control for optimized threat detection in OT security.	Tenable One;
		Tenable Vulnerability Management;
		Tenable Security Center;
		Tenable OT Security;
		Tenable Cloud Security;
		Tenable Identity Exposure

NIS2 DIRECTIVE REQUIREMENT	HOW TENABLE CAN HELP	TENABLE SOLUTION
Chapter IV, Article 21, Cybersecurity Risk-Management Measures		

2 (c) Business Continuity, such as backup management and disaster recovery, and crisis management;	Provides real-time continuous assessment of vulnerabilities, prioritizes threats, and delivers dynamic risk prioritization for your IT, cloud, and OT environments. The 'Toxic Combinations' dashboard enables users to identify and address the most critical risks, optimizing time and resource utilization. Additionally, Tenable OT Security provides configuration snapshots and rollback features for enhanced understanding and control over changes in the OT environment.	Tenable One;
		Tenable Vulnerability Management;
		Tenable Security Center;
		Tenable OT Security;
		Tenable Cloud Security;
		Tenable Identity Exposure

2 (e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;	Tenable Vulnerability Management ensures comprehensive security, handling, and disclosure and goes beyond point-in-time scanning with passive vulnerability detection. Tenable Cloud Security prioritizes risks across various domains, providing visualization of at-risk identities and resources, including hard-to-spot toxic combinations. Tenable simplifies reporting and proactive handling of findings, offering executive stakeholders insights through easy reporting. The ICS security capabilities cover visibility, threat detection, mitigation, asset inventory, vulnerability management, and configuration control, predicting and prioritizing threats for optimal safety in both IT and OT environments.	Tenable One;
		Tenable Vulnerability Management;
		Tenable Security Center;
		Tenable OT Security;
		Tenable Cloud Security;
		Tenable Identity Exposure

2 (f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;	Tenable's comprehensive vulnerability management capabilities, include Predictive Prioritization technology, ensure effective cybersecurity risk-management measures. This technology combines vulnerability data, threat intelligence, and data science to provide a clear risk score, facilitating prioritized remediation. Tenable Cloud Security and OT Security further enhance dynamic prioritization and proactive identification of vulnerabilities, offering automated workflows and detailed reporting to simplify communication for stakeholders across disciplines.	Tenable One;
		Tenable Vulnerability Management;
		Tenable Security Center;
		Tenable OT Security;
		Tenable Cloud Security;
		Tenable Identity Exposure

2 (g) basic cyber hygiene practices and cybersecurity training;	Tenable's solutions streamline basic cyber hygiene practices and cybersecurity training. This enables easy enforcement of RBAC, password policies, and other practices for internal and third-party personnel. Dashboards for tracking cyber hygiene effectiveness and compliance SLAs ensure visibility across multi-cloud and on-prem environments. With remediation guidance and auto-generated least-privilege policies, Tenable simplifies cybersecurity training and encourages knowledge transfer. The exposure management platform further provides a unified view of assets, prioritizing efforts to remediate vulnerabilities and misconfigurations for effective risk management.
	Additionally, training courses and certifications to help customers and partners get the most out of Tenable products and gain access to latest expertise for security best practices.
		Tenable One;
		Tenable Vulnerability Management;
		Tenable Security Center;
		Tenable OT Security;
		Tenable Cloud Security;
		Tenable Identity Exposure
		Tenable Training and Certification

NIS2 DIRECTIVE REQUIREMENT	HOW TENABLE CAN HELP	TENABLE SOLUTION
Chapter IV, Article 21, Cybersecurity Risk-Management Measures		

2 (h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;	Tenable Vulnerability Management and Security Center ensure data security with encryption in transit and storage, employing modern ciphers such as AES-256 and TLS Encryption across various application infrastructure layers. Keys undergo yearly reviews with restricted access, strictly prohibiting key sharing. Plugins within vulnerability management products detect encryption methods, and Tenable OT Security encrypts all communication between devices.	Tenable One;
		Tenable Vulnerability Management;
		Tenable Security Center;
		Tenable OT Security

2 (i) human resources security, access control policies and asset management;	Tenable's products streamline human resources security, access control policies, and asset management. Tenable Vulnerability Management and Security Center allow administrators to assign user roles, controlling permissions for key functions, while Tenable Cloud Security's self-service portal standardizes provisioning and revoking of privileged access. Tenable OT Security automatically discovers and inventories all network devices, offering deep insights into device states. It tracks malware and user-executed changes, providing a full history of device configuration changes for faster recovery and compliance.	Tenable One;
		Tenable Vulnerability Management;
		Tenable Security Center;
		Tenable OT Security;
		Tenable Cloud Security;
		Tenable Identity Exposure

2 (j) 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 provides robust capabilities for secure authentication and communication. Tenable Vulnerability Management and Security Center support MFA, integrate with Federated Identity Providers, and offer custom connections through documented APIs and SDKs. Tenable Cloud Security integrates with federated identity solutions, continuously monitors for anomalies, and displays multi-factor authentication status for user oversight. Tenable OT Security supports both MFA and RBAC for all tooling users.	Tenable One;
		Tenable Vulnerability Management;
		Tenable Security Center;
		Tenable OT Security;
		Tenable Cloud Security;
		Tenable Identity Exposure

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.

With Tenable's exposure management solutions, you can translate technical asset, vulnerability and threat data into clear business insights and actionable intelligence for compliance initiatives or security executives. Combine broad exposure coverage spanning IT assets, cloud resources, containers, web apps and identity platforms, with threat intelligence and data science. This allows you to focus efforts to prevent likely attacks and accurately communicate cyber risk to support optimal business performance.

While the NIS2 compliance journey 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 and vulnerability management maturity.

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 Products and NIS2 Directive solutions pages.

ABOUT TENABLE

Tenable® is the Exposure Management company. Approximately 43,000 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 tenable.com.

tenable