tenable

NIS2 Directive

Partner Playbook and Sales Enablement

August 2024

Table of Contents

- NIS2 Directive Overview
- Key Audience & Challenges
- How Can Tenable Help?
- Discovery Questions & FAQs
- Partner Resources
  - Partner Opportunity: Partner Enablement Video
  - NIS2 Directive: Email Nurture Campaign for Partners
  - Additional Resources: Sales Prospecting and Customer-Facing Assets

NIS2 Overview

What is the NIS2 Directive?

- The NIS2 Directive (Network and Information Systems Directive) is a legislative framework established by the European Union to enhance the cybersecurity and resilience of network and information systems across critical sectors. It builds upon the initial NIS Directive, expanding its scope and requirements for organizations.

- NIS2 applies to all EU member states, requiring them to transpose the Directive into national law by October 17, 2024. The Directive expands the number of covered sectors from 7 to 15, protecting more vital areas of society. NIS2 will impact organizations within the EU, especially those in critical sectors such as energy, transportation, finance, health, and digital infrastructure. NIS2 imposes stricter cybersecurity requirements and can lead to legal ramifications for management teams in non-compliant organizations.It aims to ensure that these organizations maintain a high level of cybersecurity, prevent cyber incidents, and handle any incidents that may occur effectively.

- While the NIS2 Directive is specific to the EU, its requirements and potential consequences can have a global impact on organizations that provide services or conduct business within the EU. Companies from outside the EU that fall within the scope of the directive may need to comply with its provisions or risk facing penalties and restrictions on their operations in EU member states.

NIS2 Overview

Goal: Acquisition of greenfield accounts and expansion into existing customers who must comply with the NIS2 Directive

Topic

The NIS2 Directive (Network and Information Systems Directive 2022/2555) enhances cybersecurity in critical verticals, expanding coverage to 15 sectors and imposing stricter requirements.

- Effective October 2024, all EU member states must integrate NIS2 into national laws, with legal consequences for non-compliance. It affects EU Member States based on certain company criteria.
- While specific to the EU, NIS2's impact extends globally, with non-EU companies potentially facing penalties and restrictions in EU states.
- Implementing NIS2 can present challenges, including, but not limited to: compliance costs; technical complexity; different interpretation amongst EU states; and incident reporting.
- EMEA field teams, especially in EU countries, have the opportunity to educate prospects and customers on NIS2 readiness and how Tenable can assist.

Audience

Greenfield and customers in the following criteria:

- **Sales Areas:** Countries in the European Union. Please note while specific to the EU, NIS2's impact extends globally, with non-EU companies potentially facing penalties and restrictions in EU states
- **Segments:** Commercial, Enterprise, Public Sector
- **Job Titles:** IT & Security Practitioners / Security Analysts / VM Managers or Security Leaders / Compliance Officer/ CISO and C-Suite
- **Scope of NIS2:** Next Slides

Scope of NIS2: Essential, Important, or Neither?

Essential Organizations

- Energy
- Transportation
- Banking and Financial Infrastructure
- Healthcare
- Drinking Water and Wastewater
- Digital Infrastructure
- Public Administration
- Space

Important Organizations

- Postal and Courier Services
- Waste Management
- Chemical Manufacturing, Production, and Distribution
- Food Production, Processing, and Distribution
- Manufacturing of Medical, Electronic,Transportation, or Related Equipment
- Digital Providers
- Research

Who is Concerned? Size and Revenue Criteria

Essential Organizations

250+ employees

OR

€50M+ in revenue

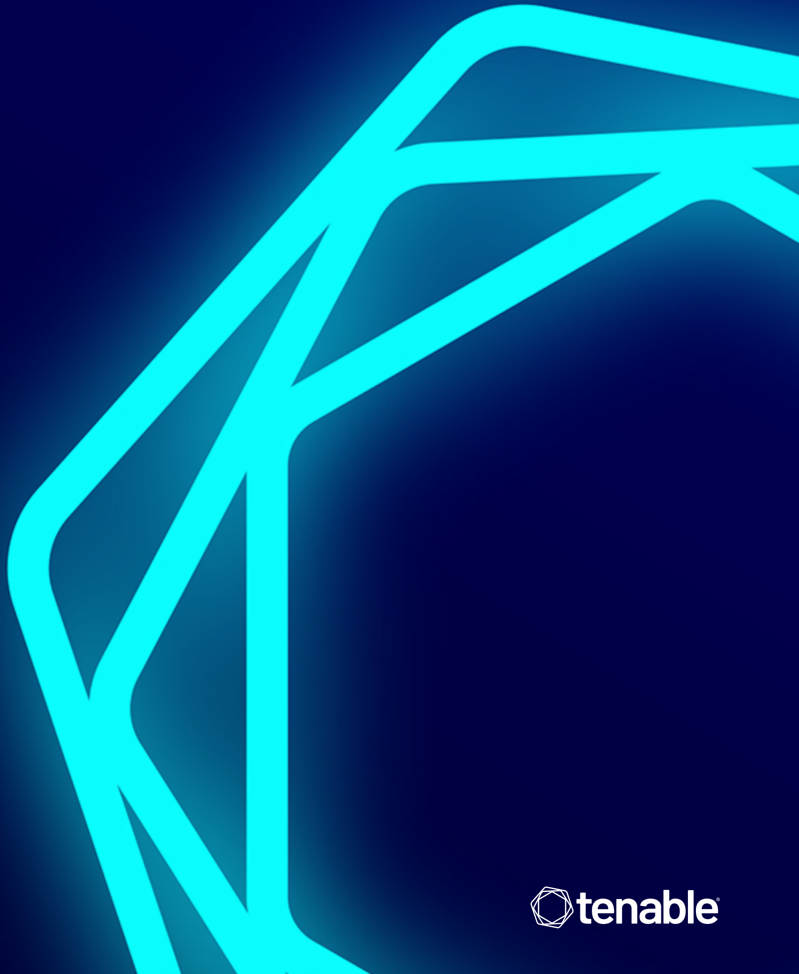
Important Organizations

50+ employees

OR

€10M+ in revenue

Key Audiences & Challenges



Key Audiences & Challenges

CISO or C-Suite

- Owns security for the organization
- Resource and budget constraints
- Reports security and compliance status to executives

Compliance Officer

- Managing multiple audits
- Getting resource commitments for audits
- Reporting compliance status to management

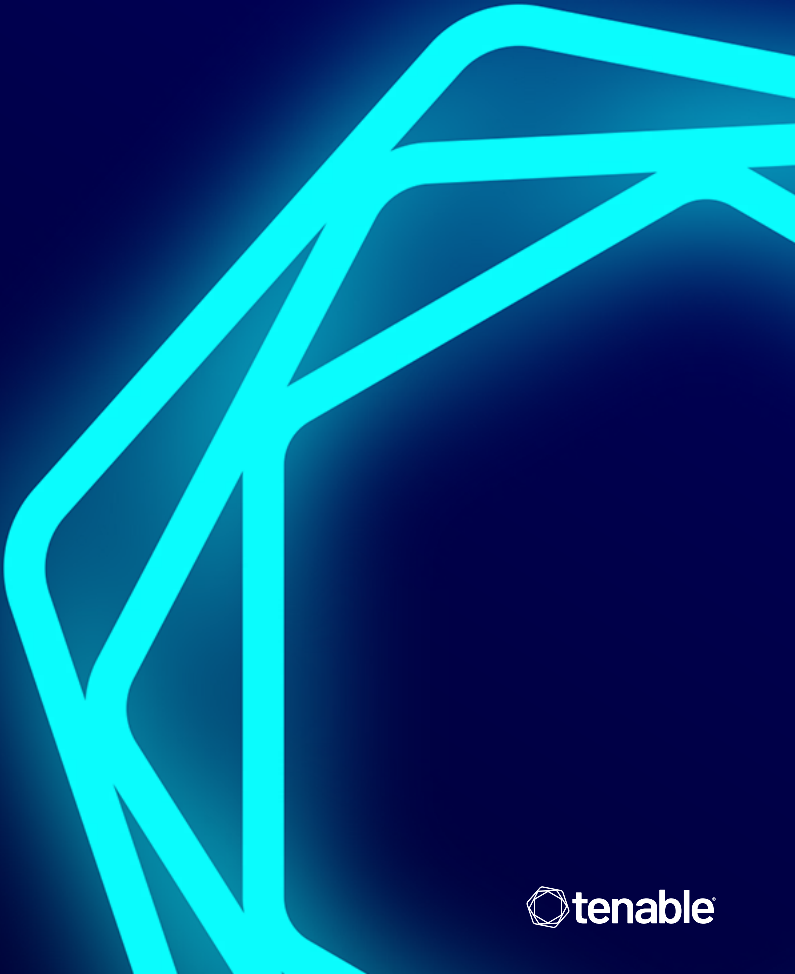
Security/VM Manager or Director

- Increasing staff efficiency
- Prioritizing vulnerabilities
- Measuring and reporting VM status

Security Analyst/ Security Practitioner

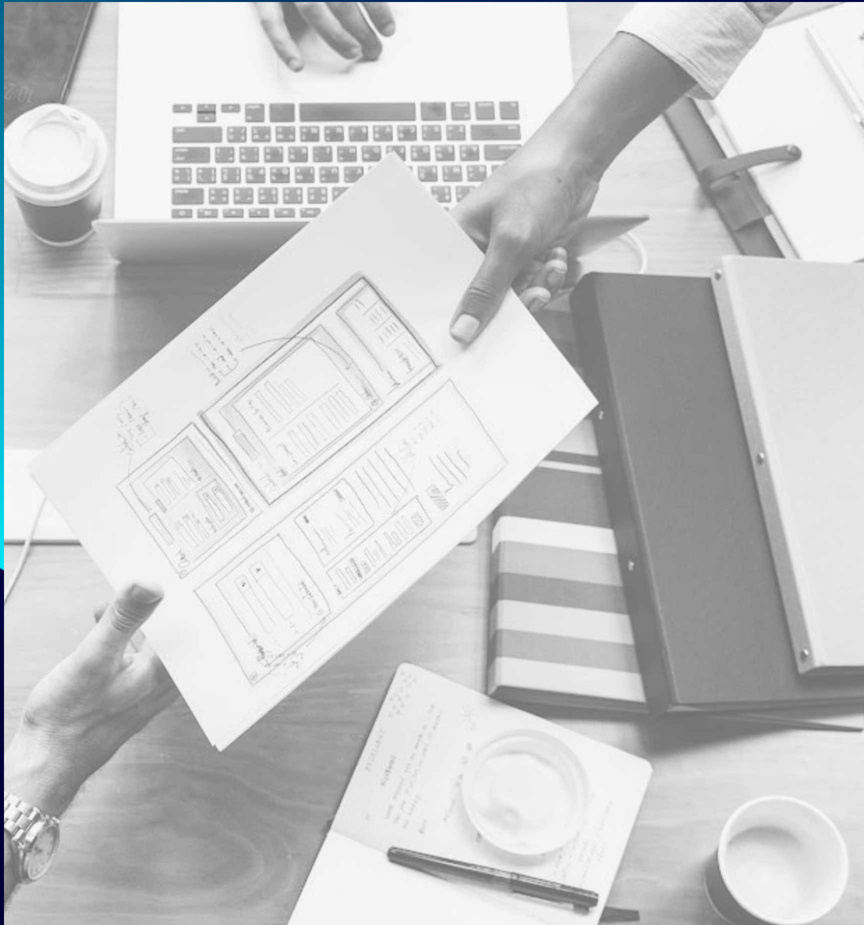
- Managing the expanding IT landscape
- Data overload
- Tracking remediation across multiple teams

How Can Tenable Help?

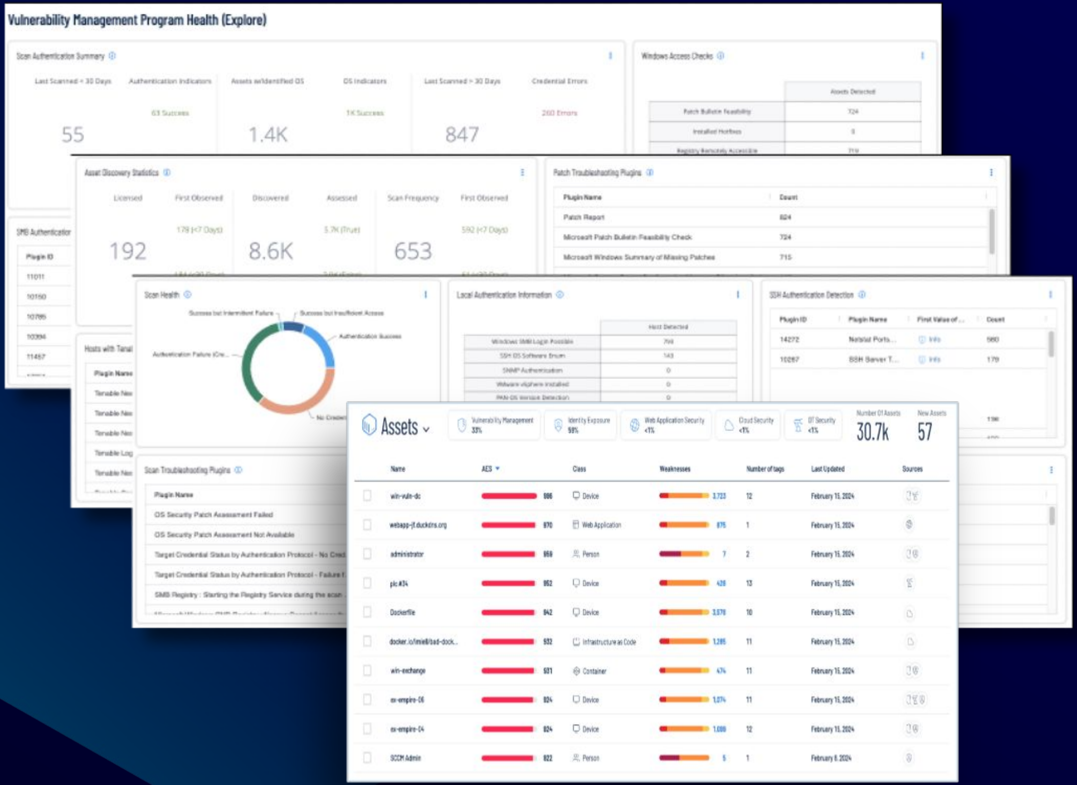


Reduce the risk

Empower security leaders with a business-aligned view of cyber risk across the entire attack surface – clouds, identities, unseen assets, OT/IoT, hybrid apps, and IT – to prioritize true exposure, optimize ROI, and enable secure compliant innovation.



Risk-Based Vulnerability Management



Vulnerability Management Program Health (Explore)

Scan Authentication Summary

Last Scanned < 30 Days	Authentication Indicators	Assets w/identified OS	OS Indicators	Last Scanned > 30 Days	Credential Errors
55	63 Success	1.4K	1K Success	847	260 Errors

Windows Access Checks

	Assets Detected
Patch Bulletin Feasibility	724
Installed Hotfixes	0
Registry Remotely Accessible	719

Asset Discovery Statistics

Licensed	First Observed	Discovered	Assessed	Scan Frequency	First Observed
192	178 (<7 Days)	8.6K	5.7K (True)	653	592 (<7 Days)

Patch Troubleshooting Plugins

Plugin Name	Count
Patch Report	824
Microsoft Patch Bulletin Feasibility Check	724
Microsoft Windows Summary of Missing Patches	715

SMB Authentication

Plugin ID
11011
10150
10785
10394
11457

Hosts with Tenable

Plugin Name
Tenable Nes
Tenable Nes
Tenable Nes
Tenable Log
Tenable Nes

Scan Health

Success but Intermittent Failure
Success but Insufficient Access
Authentication Success
Authentication Failure (Cre…
No Credent

Local Authentication Information

	Host Detected
Windows SMB Login Possible	798
SSH OS Software Enum	143
SNMP Authentication	0
VMware vSphere Installed	0
PAN-OS Version Detection	0

SSH Authentication Detection

Plugin ID	Plugin Name	First Value of…	Count
14272	Netstat Ports…	Info	560
10267	SSH Server T…	Info	179

Scan Troubleshooting Plugins

Plugin Name
OS Security Patch Assessment Failed
OS Security Patch Assessment Not Available
Target Credential Status by Authentication Protocol - No Cred
Target Credential Status by Authentication Protocol - Failure f
SMB Registry : Starting the Registry Service during the scan

Assets

Vulnerability Management 33% · Identity Exposure 59% · Web Application Security <1% · Cloud Security <1% · OT Security <1% · Number Of Assets 30.7k · New Assets 57

	Name	AES	Class	Weaknesses	Number of tags	Last Updated	Sources
□	win-vuln-dc	986	Device	3,723	12	February 15, 2024	
□	webapp-jf.duckdns.org	970	Web Application	875	1	February 15, 2024	
□	administrator	959	Person	7	2	February 15, 2024	
□	plc#34	952	Device	428	13	February 15, 2024	
□	Dockerfile	942	Device	3,578	10	February 15, 2024	
□	docker.io/imiell/bad-dock…	932	Infrastructure as Code	1,285	11	February 15, 2024	
□	win-exchange	931	Container	474	11	February 15, 2024	
□	ex-empire-06	924	Device	1,074	11	February 15, 2024	
□	ex-empire-04	924	Device	1,080	12	February 15, 2024	
□	SCCM Admin	922	Person	5	1	February 8, 2024	

tenable

Vulnerability Management

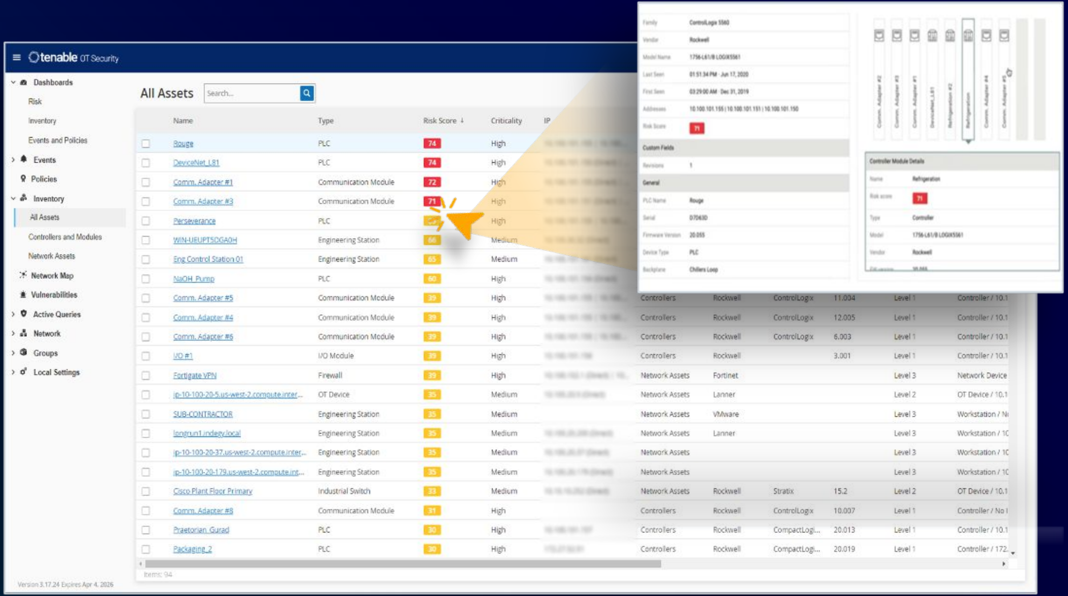
Article 21(2)(a)
Risk Analysis and Information System Security

Article 21(2)(e)
Network and Information Systems Security, including Vulnerability Handling and Disclosure

Article 21(2)(g)
Basic Cyber Hygiene Practices and Cybersecurity Training

OT Exposure

tenable
OT Security



All Assets

□	Name	Type	Risk Score ↓	Criticality	IP						
□	Rouge	PLC	74	High	[illegible]						
□	DeviceNet_L81	PLC	74	High	[illegible]						
□	Comm. Adapter #1	Communication Module	72	High	[illegible]						
□	Comm. Adapter #3	Communication Module	71	High	[illegible]						
□	Perseverance	PLC	[illegible]	High	[illegible]						
□	WIN-UEUPT5DGA0H	Engineering Station	66	Medium	[illegible]						
□	Eng Control Station 01	Engineering Station	65	Medium	[illegible]						
□	NaOH_Pump	PLC	60	High	[illegible]						
□	Comm. Adapter #5	Communication Module	39	High	[illegible]	Controllers	Rockwell	ControlLogix	11.004	Level 1	Controller / 10.1
□	Comm. Adapter #4	Communication Module	39	High	[illegible]	Controllers	Rockwell	ControlLogix	12.005	Level 1	Controller / 10.1
□	Comm. Adapter #6	Communication Module	39	High	[illegible]	Controllers	Rockwell	ControlLogix	6.003	Level 1	Controller / 10.1
□	I/O #1	I/O Module	39	High	[illegible]	Controllers	Rockwell		3.001	Level 1	Controller / 10.1
□	Fortigate VPN	Firewall	39	High	[illegible]	Network Assets	Fortinet			Level 3	Network Device
□	ip-10-100-20-5.us-west-2.compute.inter...	OT Device	35	Medium	[illegible]	Network Assets	Lanner			Level 2	OT Device / 10.1
□	SUB-CONTRACTOR	Engineering Station	35	Medium		Network Assets	VMware			Level 3	Workstation / N
□	longrun1.indegy.local	Engineering Station	35	Medium	[illegible]	Network Assets	Lanner			Level 3	Workstation / 1C
□	ip-10-100-20-37.us-west-2.compute.inter...	Engineering Station	35	Medium	[illegible]	Network Assets				Level 3	Workstation / 1C
□	ip-10-100-20-179.us-west-2.compute.int...	Engineering Station	35	Medium	[illegible]	Network Assets				Level 3	Workstation / 1C
□	Cisco Plant Floor Primary	Industrial Switch	33	Medium	[illegible]	Network Assets	Rockwell	Stratix	15.2	Level 2	OT Device / 10.1
□	Comm. Adapter #8	Communication Module	31	High		Controllers	Rockwell	ControlLogix	10.007	Level 1	Controller / No I
□	Praetorian_Gurad	PLC	30	High	[illegible]	Controllers	Rockwell	CompactLogi...	20.013	Level 1	Controller / 10.1
□	Packaging_2	PLC	30	High	[illegible]	Controllers	Rockwell	CompactLogi...	20.019	Level 1	Controller / 172.

Items: 94

Version 3.17.24 Expires Apr 4, 2026

Family	ControlLogix 5560
Vendor	Rockwell
Model Name	1756-L61/B LOGIX5561
Last Seen	01:51:34 PM · Jun 17, 2020
First Seen	03:29:00 AM · Dec 31, 2019
Addresses	10.100.101.155 | 10.100.101.151 | 10.100.101.150
Risk Score	71
Custom Fields	
Revisions	1
General	
PLC Name	Rouge
Serial	07063D
Firmware Version	20.055
Device Type	PLC
Backplane	Chillers Loop

Controller Module Details

Name	Refrigeration
Risk score	71
Type	Controller
Model	1756-L61/B LOGIX5561
Vendor	Rockwell
FW version	20.055

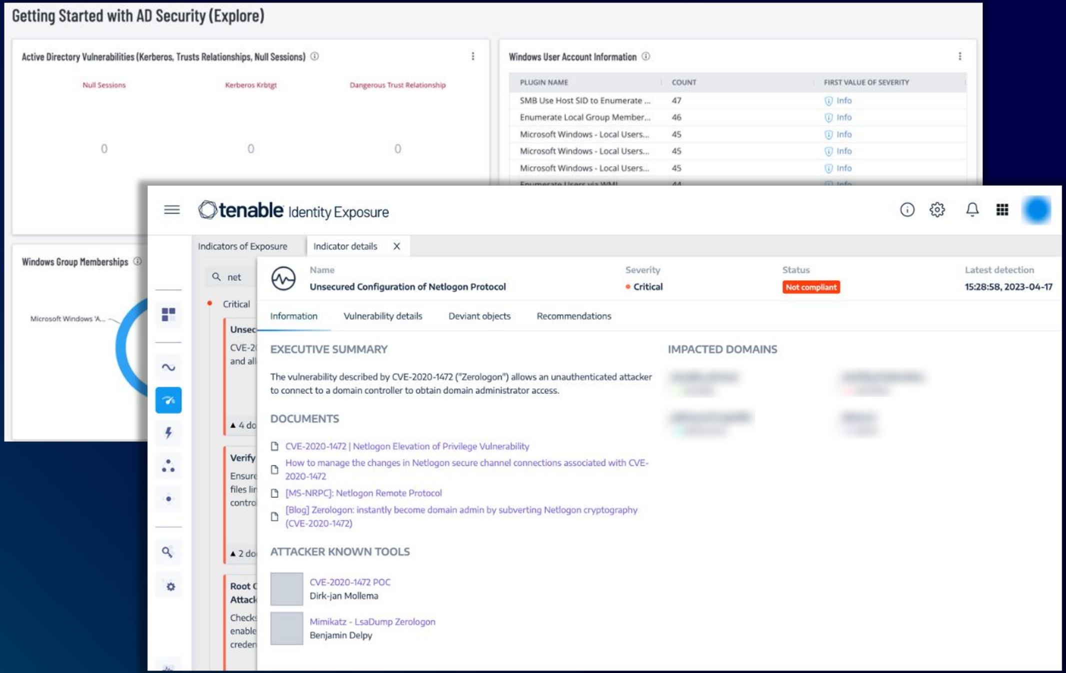
Article 21(2) (b)
Incident Handling

Article 21(2)(a)
Risk Analysis and Information System Security

Article 21(2)(f)
Policies and Procedures for Testing Cybersecurity Risk Management Measures

Article 21(2)(g)
Basic Cyber Hygiene Practices and Cybersecurity Training

Identity Exposure



Windows User Account Information

PLUGIN NAME	COUNT	FIRST VALUE OF SEVERITY
SMB Use Host SID to Enumerate ...	47	Info
Enumerate Local Group Member...	46	Info
Microsoft Windows - Local Users...	45	Info
Microsoft Windows - Local Users...	45	Info
Microsoft Windows - Local Users...	45	Info
Enumerate Users via WMI	44	Info

Name	Severity	Status	Latest detection
Unsecured Configuration of Netlogon Protocol	● Critical	Not compliant	15:28:58, 2023-04-17

EXECUTIVE SUMMARY

The vulnerability described by CVE-2020-1472 ("Zerologon") allows an unauthenticated attacker to connect to a domain controller to obtain domain administrator access.

DOCUMENTS

- CVE-2020-1472 | Netlogon Elevation of Privilege Vulnerability
- How to manage the changes in Netlogon secure channel connections associated with CVE-2020-1472
- [MS-NRPC]: Netlogon Remote Protocol
- [Blog] Zerologon: instantly become domain admin by subverting Netlogon cryptography (CVE-2020-1472)

ATTACKER KNOWN TOOLS

CVE-2020-1472 POC
Dirk-jan Mollema

Mimikatz - LsaDump Zerologon
Benjamin Delpy

IMPACTED DOMAINS

tenable
Identity Exposure

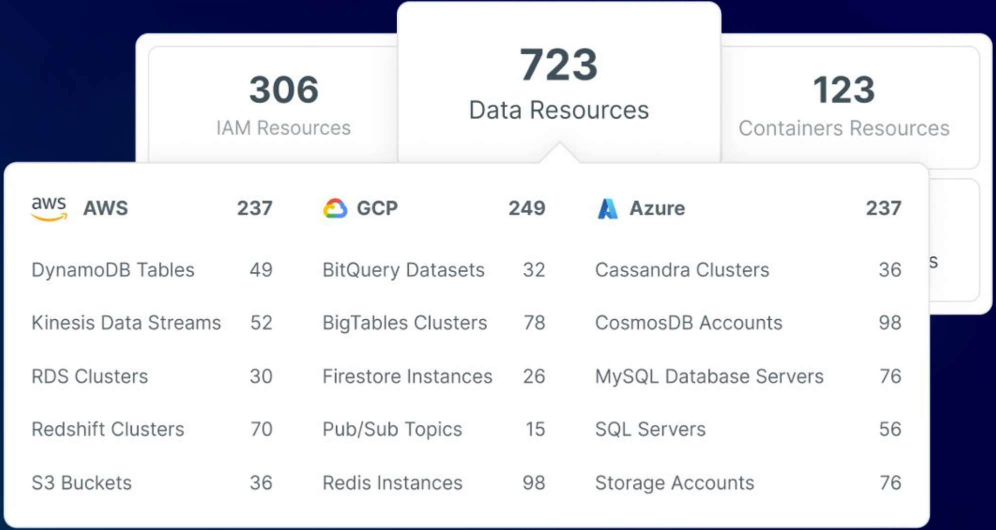
Article 21(2)(g)
Basic Cyber Hygiene Practices and Cybersecurity Training

Article 21(2)(h)
Access Control Policies and Asset Management

Article 21(2)(i)
Use of MFA or Continuous Authentication Solutions

Cloud Exposure

tenable
Cloud Security



306	723	123
IAM Resources	Data Resources	Containers Resources

AWS	237	GCP	249	Azure	237
DynamoDB Tables	49	BitQuery Datasets	32	Cassandra Clusters	36
Kinesis Data Streams	52	BigTables Clusters	78	CosmosDB Accounts	98
RDS Clusters	30	Firestore Instances	26	MySQL Database Servers	76
Redshift Clusters	70	Pub/Sub Topics	15	SQL Servers	56
S3 Buckets	36	Redis Instances	98	Storage Accounts	76

Article 21(2)(a)
Risk Analysis and Information System Security

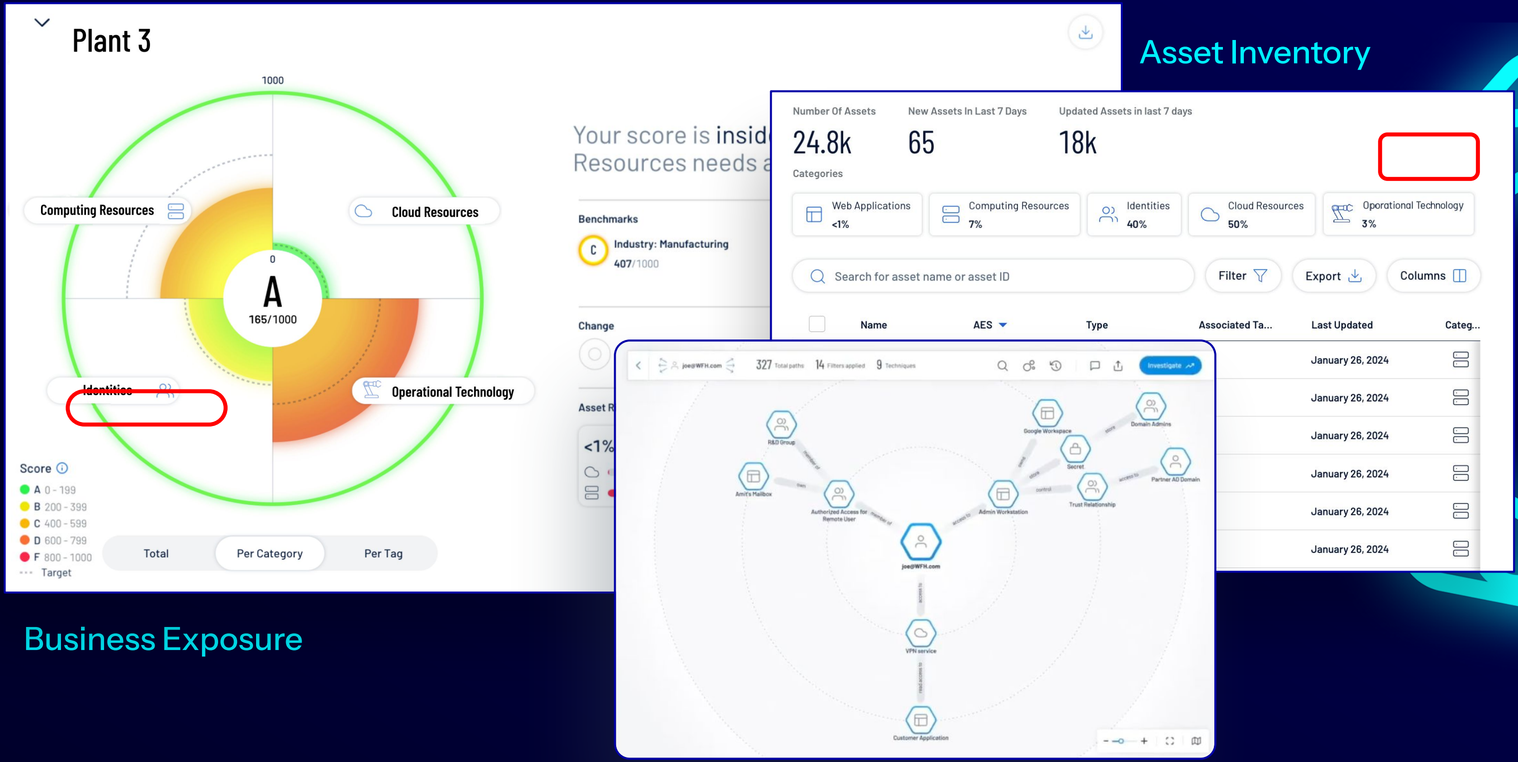
Article 21(2)(e)
Network and Information Systems Security, including Vulnerability Handling and Disclosure

Article 21(2)(g)
Basic Cyber Hygiene Practices and Cybersecurity Training

Article 21(2)(h)
Access Control Policies and Asset Management

tenable one™

Comprehensive Visibility & Exposure Management for NIS2 Risk-Based Governance



Plant 3

1000

0

A

165/1000

Computing Resources

Cloud Resources

Identities

Operational Technology

Your score is insid
Resources needs a

Benchmarks

C Industry: Manufacturing
407/1000

Change

Asset R

<1%

Score

- 🟩 A 0 - 199
- 🟨 B 200 - 399
- 🟧 C 400 - 599
- 🟧 D 600 - 799
- 🟥 F 800 - 1000
- Target

Total | Per Category | Per Tag

Number Of Assets	New Assets In Last 7 Days	Updated Assets in last 7 days
24.8k	65	18k

Categories

Web Applications	Computing Resources	Identities	Cloud Resources	Operational Technology
<1%	7%	40%	50%	3%

Search for asset name or asset ID

Filter | Export | Columns

□	Name	AES	Type	Associated Ta...	Last Updated	Categ...
					January 26, 2024	
					January 26, 2024	
					January 26, 2024	
					January 26, 2024	
					January 26, 2024	
					January 26, 2024	

joe@WFH.com — 327 Total paths — 14 Filters applied — 9 Techniques

Asset Inventory

Business Exposure

Identity-Aware Attack Path Analysis

tenable

Discovery Questions & FAQs

CISO → C-Suite

These questions target decision-makers involved in strategic planning and implementation of IT policies and practices:

- “How much of the NIS2 Directive do you think has been met through your compliance with ISO 27001 or other regulations?”
- “How good is your organisation at evaluating risk and then prioritising measures to mitigate that risk? If we were to say, 1 is low and 10 is high, where do you think you’d sit?”
- “What concerns you most about meeting NIS2? Are your concerns organisational, operational or technological?”
- "What steps has your organisation already taken, or is taking, to prepare for the implementation of the NIS2 Directive?"
- "What challenges or concerns do you anticipate facing in the process of becoming NIS2 compliant?"
- "What resources (personnel, budget, technology) have you allocated towards achieving compliance with the NIS2 Directive?"

Compliance Officer

These questions are best suited for individuals responsible for overseeing the organisation's compliance with regulations and cybersecurity standards.

- "Have you mapped the NIS2 Directive against ISO 27001 (or another standard/regulation) to gauge how prepared your organisation is for NIS2?"
- “How do you plan to ensure continuous compliance with evolving NIS2 requirements?”
- “What solutions and practices are you currently using to address your compliance challenges?” [AND, reflecting on their previous response] “How is that approach falling short to addressing this challenge?

Security/VM Manager or Director

Aimed at those who need to be knowledgeable about upcoming regulations and their impact on the organisation.

- "How familiar are you with the upcoming NIS2 Directive and its implications for your organisation?"
- "In which areas do you feel you need the most support or solutions to meet the NIS2 Directive requirements?"
- “How challenging is it to communicate the importance of the NIS2 Directive (will be law soon) to your Executive?”
- “What’s your role in the overall process? Do you have the necessary relationships with relevant stakeholders and colleagues who will be involved in NIS2?”

Security Analyst/Practitioner

Professionals responsible for evaluating and mitigating cybersecurity risks within the organisation.

- "How familiar are you with the key requirements and changes introduced by the NIS2 Directive, and how do you see these impacting your role and responsibilities?"
- "How are you currently assessing and managing cybersecurity risks, and how do you see this evolving to meet the NIS2 Directive requirements?"
- “Did you find yourself considering challenges that you might not have considered previously?”
- “With the NIS2 Directive on the horizon, how are you involved in preparing your organisation's approach to incident response or vulnerability management? What is your current approach to prioritising and remediating vulnerabilities, and what challenges do you anticipate in meeting the new requirements?”

Frequently Asked Questions

What are the key dates and deadlines for the NIS2 Directive?

The key dates and deadlines for the NIS2 Directive are as follows: (1) Entry into Force: 16 January 2023; (2) Transposition into National Law: 17 October 2024; (3) Identification and Registration of In-Scope Entities: 17 April 2025.

How does the NIS2 Directive fit with the laws and regulations that are already, or soon to be, applicable (LPM, DORA, GDPR)?

The NIS2 Directive interacts with other existing or upcoming regulations such as the LPM, DORA and GDPR. Quite simply, NIS2 are "least measures." If you have already applied equivalent measures (and put in place the monitoring and reporting process, operation and technologies), than the regulation which has already been applied will be considered sufficient in regards to NIS2 application.

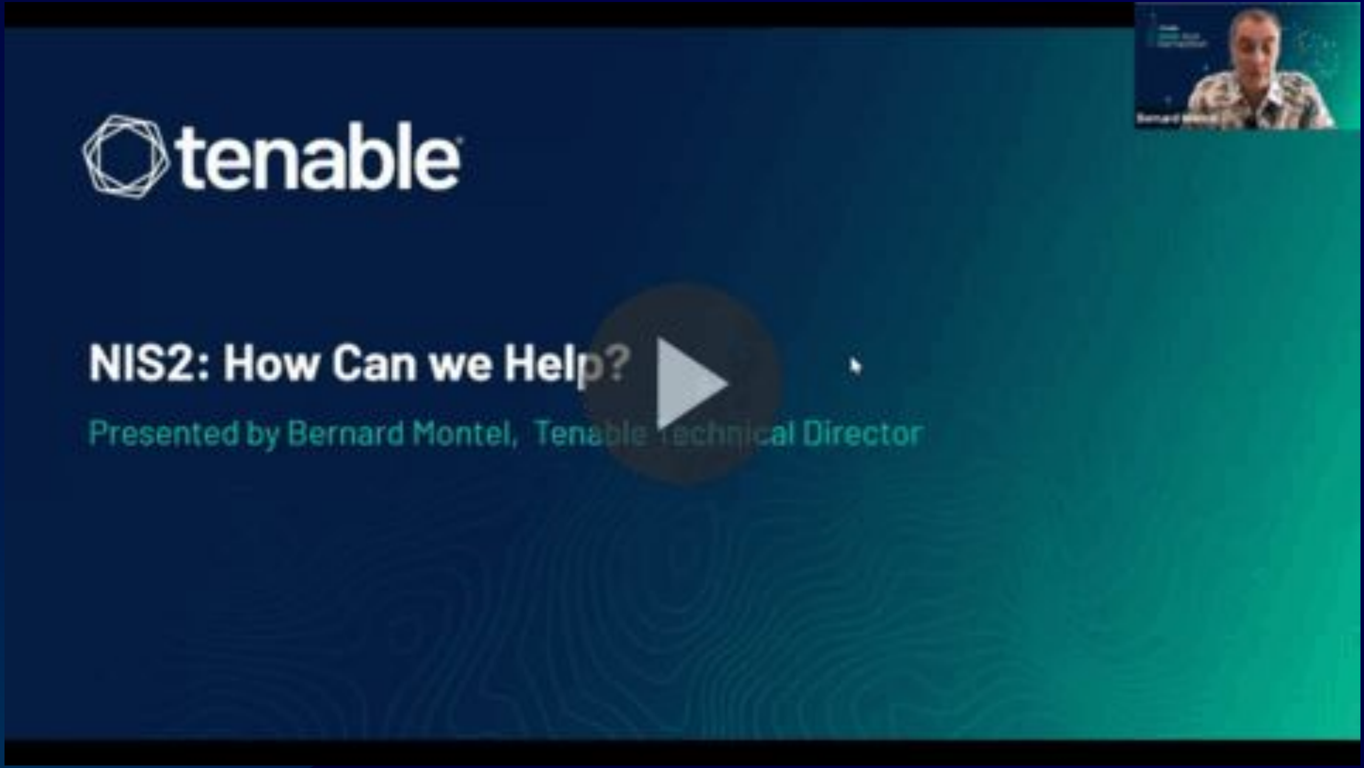
What are the penalties for NIS2 Directive noncompliance?

The penalties for noncompliance are substantial and vary depending on the classification of the entity. The directive prescribes specific penalties for essential and important entities as follows:

- For Essential Entities: Fines of up to €10M or 2% of the total annual worldwide turnover of the company to which the entity belongs, whichever amount is higher.
- For Important Entities: Fines of up to €7M or 1.4% of the total annual worldwide turnover of the company to which the entity belongs, whichever amount is higher.

Partner Resources

Partner Opportunity



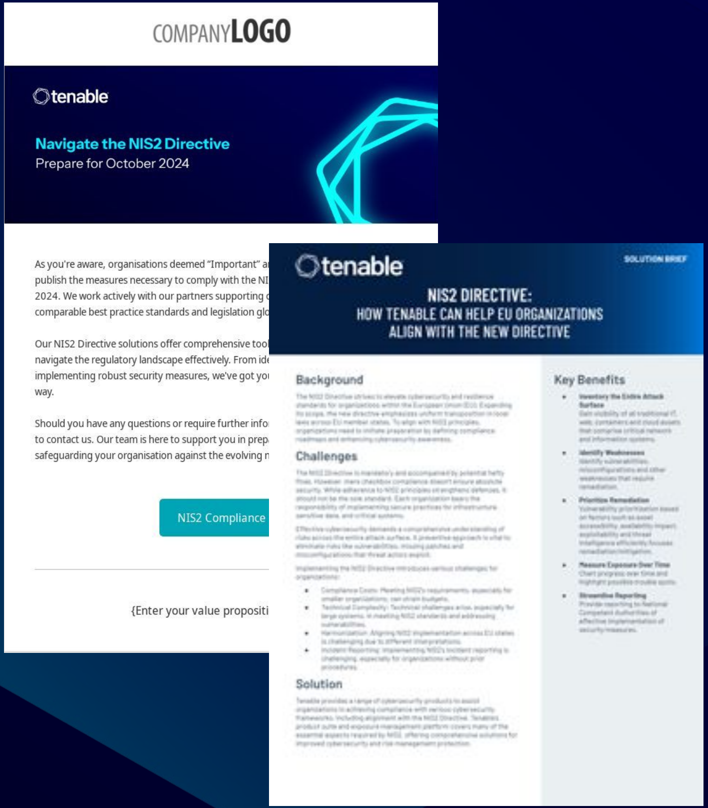
tenable

NIS2: How Can we Help?

Presented by Bernard Montel, Tenable Technical Director

https://videos.tenable.com/watch/XJ4EAf4MGFRwdR8PcfHjh7

Email Nurture Campaign



COMPANYLOGO

tenable

Navigate the NIS2 Directive

Prepare for October 2024

As you're aware, organisations deemed "Important" a
publish the measures necessary to comply with the NI
2024. We work actively with our partners supporting c
comparable best practice standards and legislation glo

Our NIS2 Directive solutions offer comprehensive tool
navigate the regulatory landscape effectively. From ide
implementing robust security measures, we've got you
way.

Should you have any questions or require further info
to contact us. Our team is here to support you in prep
safeguarding your organisation against the evolving n

NIS2 Compliance

{Enter your value propositi

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.

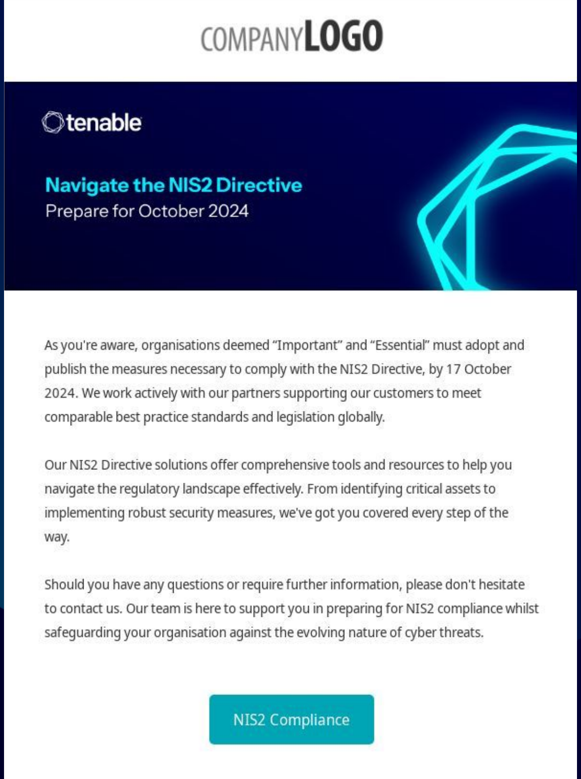
Our ready-to-use campaign includes 4-5 targeted emails designed to drive engagement with key NIS2 compliance resources. You can **customize**, **launch**, and **track** this directly from the Partner Portal.

Visit our Campaigns Page to access and activate this campaign in **English**, **French**, **Italian**, **European Spanish**, and **German.**

tenable

Email Nurture Campaign

Email 1: CTA: Tenable Webpage – Solutions for NIS Directive Compliance



Navigate the NIS2 Directive

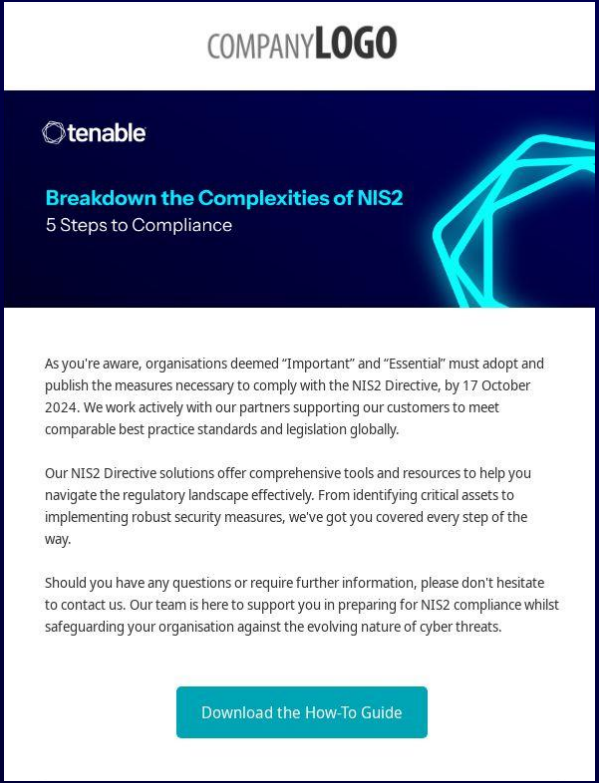
Prepare for October 2024

As you're aware, organisations deemed "Important" and "Essential" must adopt and publish the measures necessary to comply with the NIS2 Directive, by 17 October 2024. We work actively with our partners supporting our customers to meet comparable best practice standards and legislation globally.

Our NIS2 Directive solutions offer comprehensive tools and resources to help you navigate the regulatory landscape effectively. From identifying critical assets to implementing robust security measures, we've got you covered every step of the way.

Should you have any questions or require further information, please don't hesitate to contact us. Our team is here to support you in preparing for NIS2 compliance whilst safeguarding your organisation against the evolving nature of cyber threats.

Email 2: CTA: Checklist – 5 Steps to NIS2 Compliance



Breakdown the Complexities of NIS2

5 Steps to Compliance

As you're aware, organisations deemed "Important" and "Essential" must adopt and publish the measures necessary to comply with the NIS2 Directive, by 17 October 2024. We work actively with our partners supporting our customers to meet comparable best practice standards and legislation globally.

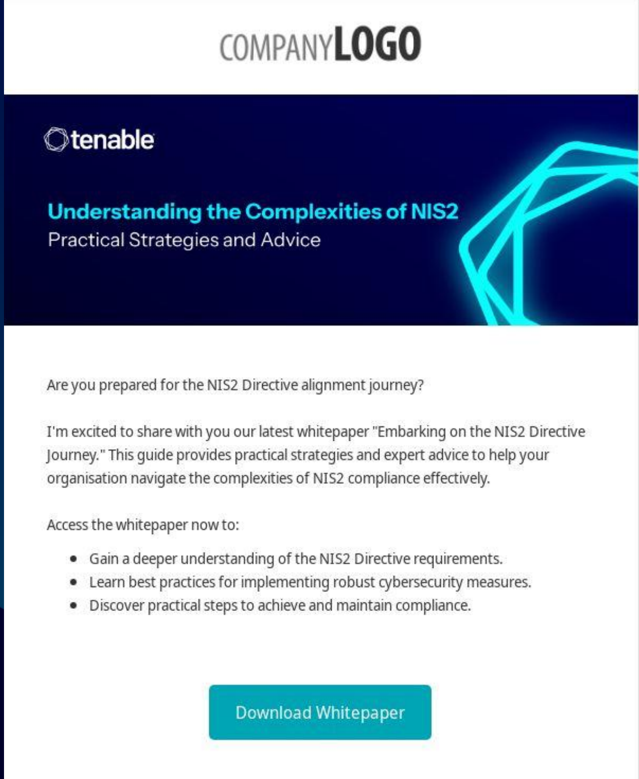
Our NIS2 Directive solutions offer comprehensive tools and resources to help you navigate the regulatory landscape effectively. From identifying critical assets to implementing robust security measures, we've got you covered every step of the way.

Should you have any questions or require further information, please don't hesitate to contact us. Our team is here to support you in preparing for NIS2 compliance whilst safeguarding your organisation against the evolving nature of cyber threats.

tenable

Email Nurture Campaign

Email 3: CTA: White Paper – Embarking on the NIS2 Compliance Journey



COMPANYLOGO

tenable

Understanding the Complexities of NIS2

Practical Strategies and Advice

Are you prepared for the NIS2 Directive alignment journey?

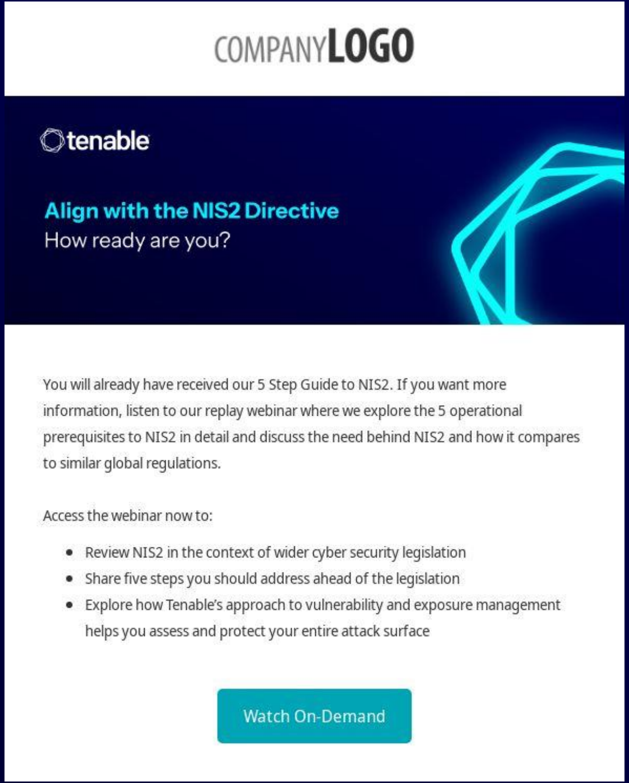
I'm excited to share with you our latest whitepaper "Embarking on the NIS2 Directive Journey." This guide provides practical strategies and expert advice to help your organisation navigate the complexities of NIS2 compliance effectively.

Access the whitepaper now to:

- Gain a deeper understanding of the NIS2 Directive requirements.
- Learn best practices for implementing robust cybersecurity measures.
- Discover practical steps to achieve and maintain compliance.

Download Whitepaper

Email 4: CTA: Webinar Replay – Navigating NIS2: How ready are you? *(English and German only)*



COMPANYLOGO

tenable

Align with the NIS2 Directive

How ready are you?

You will already have received our 5 Step Guide to NIS2. If you want more information, listen to our replay webinar where we explore the 5 operational prerequisites to NIS2 in detail and discuss the need behind NIS2 and how it compares to similar global regulations.

Access the webinar now to:

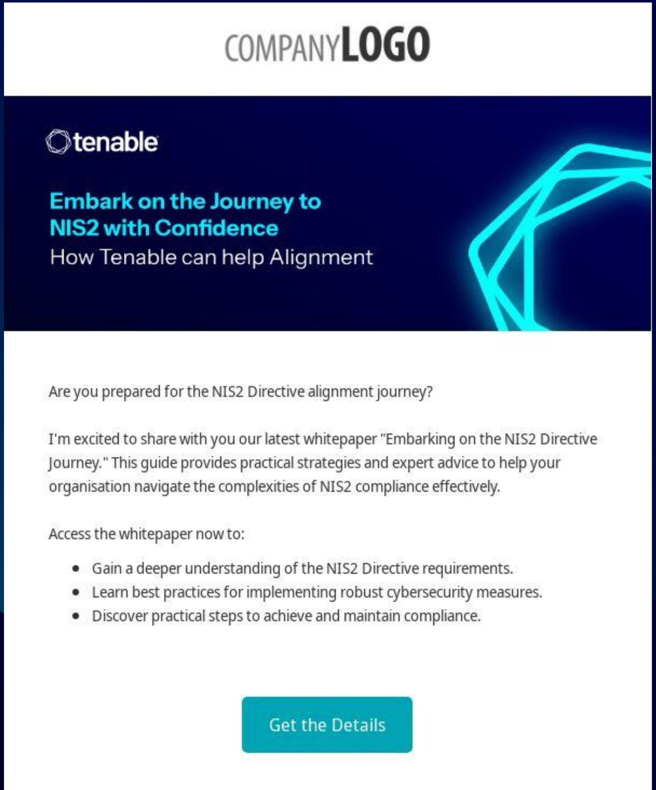
- Review NIS2 in the context of wider cyber security legislation
- Share five steps you should address ahead of the legislation
- Explore how Tenable's approach to vulnerability and exposure management helps you assess and protect your entire attack surface

Watch On-Demand

tenable

Email Nurture Campaign

Email 5: CTA: Solution Overview: NIS2 Compliance - How Tenable Can Help EU Member States Align



COMPANYLOGO

Embark on the Journey to NIS2 with Confidence

How Tenable can help Alignment

Are you prepared for the NIS2 Directive alignment journey?

I'm excited to share with you our latest whitepaper "Embarking on the NIS2 Directive Journey." This guide provides practical strategies and expert advice to help your organisation navigate the complexities of NIS2 compliance effectively.

Access the whitepaper now to:

- Gain a deeper understanding of the NIS2 Directive requirements.
- Learn best practices for implementing robust cybersecurity measures.
- Discover practical steps to achieve and maintain compliance.

Get the Details

Additional Email Campaign Assets

Sales Prospecting Resources

Sales Flows: Available in 5 languages

Leverage our 20-day, multi-step process with emails, voicemails, and LinkedIn InMail to engage prospects, highlight NIS2 compliance, and demonstrate how Tenable supports cybersecurity needs. This flow helps you connect with leads and guide them to NIS2 compliance.

Social Posts

Similar to this Tenable post. Link your social accounts and post directly from the partner portal.

Other Customer Assets

- **Sales Deck:** NIS2 Directive Presentation
- **External FAQ:** NIS2 Directive
- **Solution Brief:** NIS2 Directive: How Tenable VM Helps
- **Solution Brief:** Tenable OT Security and the NIS2 Directive
- **Solution Brief:** Achieving NIS2 Compliance in Multi-Cloud Environments with Tenable Cloud Security
- **Article:** A Look at New in the NIS2 Directive

Visit our **Campaigns Page** in the Partner Portal to access all these resources and activate this campaign in English, French, Italian, European Spanish, and German.

tenable

tenable®