XM Cyber

Whitepaper

Understanding the NIS 2 Directive with XM Cyber

How XM Cyber Continuous Exposure Management can help to meet the requirements of NIS 2

Executive Summary

Cyber resilience has become a critical focus for organizations that continually strive to implement robust security practices and incident response procedures that minimize business disruption and operational friction.

In light of these challenges, and the escalating threat landscape and the growing reliance on digital technologies, The European Union has elected to establish a pivotal new Directive, NIS 2, which will guide organizations in strengthening their cybersecurity measures and ensuring operational resilience.

The NIS 2 Directive seeks to ensure that organizations are better equipped to prevent, detect, and respond to cyber threats effectively. As such, compliance with the NIS 2 Directive is essential for organizations operating in the EU to safeguard their digital assets, protect customer data, and maintain trust and confidence in their services amid an evolving cyber threat landscape.

What is the NIS 2 Directive

The NIS 2 Directive aims to ensure consistency of the integrity, overall level of cybersecurity, and the enforcement of legislation across all EU member states. The overall objective is to enhance the cyber resilience of all essential services by strengthening cybersecurity risk-management measures and streamlining incident-reporting obligations throughout the European Union.

The Directive establishes specific requirements for member states in relation to the security of network and information systems and applies to operators of essential services, digital service providers, and critical infrastructure.

The NIS 2 Directive requires member states to adopt a national strategy for the security of network and information systems and designate competent authorities to oversee and enforce the Directive. It also requires operators of essential services in sectors such as energy, transport, healthcare, finance, and key digital service providers to take appropriate security measures and report significant cybersecurity incidents to relevant authorities.

Overall, the NIS 2 Directive plays a crucial role in strengthening cybersecurity resilience across the EU and ensuring the protection of critical infrastructure and digital services.

What are the Objectives of NIS 2?

The objectives of the NIS 2 Directive are aimed at enhancing cybersecurity and operational resilience across the European Union. It's aim is to strengthen the overall cybersecurity posture of organizations by establishing baseline security requirements and standards for the protection of critical services and infrastructure.

Ultimately, by setting out clear requirements and standards for cybersecurity risk management, incident handling, and operational resilience, the Directive aims to promote a culture of cybersecurity awareness and best practices among organizations and stakeholders.

The Specific Goals of the Directive Include:

Improving cybersecurity:

By setting out clear guidelines for cybersecurity risk management, incident handling, and resilience measures, the Directive seeks to mitigate cyber threats and vulnerabilities.

Safeguarding critical infrastructure:

The Directive tries to protect critical services, infrastructure, and essential services which are vital to the functioning of society economy, from cyber threats and disruptions. It does this by promoting a risk-based approach to cybersecurity and operational resilience.

Enhancing trust and confidence:

The NIS 2 Directive aims to enhance trust and confidence in digital services and the overall cybersecurity posture of organizations within the EU.

Ensuring incident preparedness and response:

By requiring the implementation of effective incident response plans, the Directive aims to ensure that organizations can detect, respond to, and recover from cybersecurity incidents in a timely and efficient manner.

Promoting cross-border cooperation:

By promoting collaboration at the regional level, the Directive aims to enhance the collective cybersecurity resilience of the EU as a whole. It seeks to foster a culture of cooperation and information-sharing among EU member states to address cybersecurity threats and incidents more effectively.

Who Does NIS 2 Apply to?

The original NIS Directive previously defined entities into two different categories - operators of essential services (OES) and digital service providers (DSPs). However, this led to some confusion between the distinctions. To address this, the NIS 2 Directive eliminates the distinction between these previous entity types and instead expands the scope of the previous rules by adding new sectors based on their degree of digitalization and interconnectedness and how crucial they are for the economy and society.

The NIS 2 Directive calls for entities to be classified based on their importance, and divided into two categories; essential and important entities, which will be subjected to a different supervisory regime.

By categorizing industries into these two groups, the NIS 2 Directive aims to ensure a consistent level of cybersecurity resilience for critical sectors and digital service providers within the European Union.

The NIS 2 Directive covers entities from the following sectors:

Essential Entities and High Criticality Sectors:

- **Energy** (electricity, district heating and cooling, oil, gas and hydrogen)
- **Transport** (air, rail, water, and road)
- **Banking**
- **Financial Market Infrastructures**
- **Health Sector**
- **Drinking water**
- **Wastewater**
- **Public Administration**
- **Space** (Ground-based infrastructure supporting space-based services)
- **Digital Infrastructure**

Important Entities and Other Critical Sectors:

- **Digital Providers**
- **Postal Services and Courier Service**
- **Waste Management**
- **Research Organizations**
- **Organizations Manufacturing and Product of Chemicals**
- **Organizations Manufacturing and Product of Chemicals**
- **Manufacturing**
- **Food Production, Processing and Distribution**

NIS 2 Requirements

From the NIS 2 Directive Overview: https://www.nis-2-directive.com/

Under NIS 2, essential and important entities must adopt appropriate, proportionate technical, operational, and organizational measures to manage cybersecurity risks. These measures aim to protect network and information systems, as well as to prevent or minimize the impact of incidents on service recipients and interconnected services.

The directive mandates an "all-hazards" approach, meaning that entities must be prepared to address a wide range of threats, from cyberattacks to physical disruptions, ensuring comprehensive protection and resilience in their operations.

The NIS 2 Directive enhances the previous version in four primary areas:

Cybersecurity Risk-Management Measures

Under the NIS 2 Directive, organizations must implement cybersecurity risk-management measures to enhance their cybersecurity resilience. These measures include identifying and assessing cybersecurity risks, implementing security controls, developing incident response and recovery plans, promoting coordinated vulnerability disclosure, securing the public core of the open internet, adopting advanced cybersecurity technologies, providing training and education on cybersecurity, and facilitating information sharing.

By adhering to these measures, organizations can strengthen cybersecurity defenses, improve incident response capabilities, and enhance overall cybersecurity readiness to address and mitigate cyber threats effectively.

Corporate Accountability Including Supply Chain

NIS 2 requires all levels of corporate management to be aware of and held accountable to oversee, approve, and be trained on the entity's cybersecurity measures and cybersecurity risk management processes.

This includes approving security policies, monitoring compliance, and taking steps to manage risks. Board members, C-Level, and other senior leadership can be held personally liable for breach of their duty to ensure compliance, or for the associated risks and/or damages if they do not fulfill their cyber risk management obligations.

Corporate accountability also involves transparency and communication with stakeholders, including regulators, customers, and partners, regarding cybersecurity practices, incident responses, and compliance with the NIS 2 Directive.

Business Continuity and Cyber Resilience

Business continuity refers to the ability of an organization to continue operating and delivering services in the face of disruptive incidents, including cybersecurity events. Communication and timely notifications play a critical role in enhancing cybersecurity resilience and minimizing the potential damage caused by cybersecurity incidents.

Organizations must develop and maintain robust business continuity plans to ensure continuous delivery of essential services and minimize the impact of cybersecurity incidents. These plans typically include measures for preventing, preparing for, responding to, and recovering from disruptions to the organization's operations caused by cyber threats.

Reporting Obligations and Information Sharing

Under the Directive, organizations are accountable for maintaining the security and integrity of their systems, ensuring compliance with requirements outlined in the Directive, and promptly reporting significant cybersecurity incidents to relevant authorities.

Entities must promptly notify their CSIRT or competent authority of significant incidents affecting services to ensure timely response and mitigation of cyber threats. Notification, including cross-border impact details, is essential for effective coordination and communication between relevant parties. Informing affected service recipients of cyber threats and promptly response measures helps minimize the impact of the incident and protect the integrity of services.

NIS 2 Risk Management Requirements

REQUIREMENT		XM CYBER COVERAGE
01	**Risk analysis and information system security**	The XM Cyber Continuous Exposure Management Platform acts as a foundational component to deliver cybersecurity risk analysis, by identifying security exposures across the digital attack surface, validating their exploitability using XM Attack Graph Analysis™ and prioritizing remediation efforts based on the risk they present to business-critical assets and systems. Utilizing a holistic approach that quantifies the exposure risk presented by vulnerabilities, misconfiguration, identity and credential issues, weak security posture, and poor cyber hygiene. These insights can be used to form a baseline of the current security posture that factors in the risk to business-critical assets and operations. They can be leveraged to define proactive defense strategies, policies, and procedures to minimize risk and enhance security defenses.
02	**Incident handling**	The XM Cyber Platform provides rich contextual information to support post-incident investigation and root cause analysis of cybersecurity incidents. The insights provided by the platform can support the initial investigation to help identify the breach point and the attack techniques that may have been leveraged, leading to the incident. Security operations teams can then define response and remediation strategies based on these risk contextual insights.
03	**Business continuity measures (back-ups, disaster recovery, crisis management)**	Although not directly involved in backup and recovery processes, the XM Cyber Platform can help to ensure the integrity of administrative accounts used for system backup and recovery to identify risks to backup credentials and security groups that could impact the recovery procedure.

NIS 2 Risk Management Requirements

REQUIREMENT		XM CYBER COVERAGE
04	**Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers**	The XM Cyber Platform provides two key use case advantages for the assessment and management of supply chain and third-party risk: • Simplification of third-party risk analysis through external exposure intelligence for potential supply chain partners and digital service providers. • Continuous Threat Modeling for the risk presented to business-critical systems from third parties and supply chain, such as VPN connections, Jump hosts, and associated user credentials.
05	**Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;**	The XM Cyber Platform forms a key component of the network and information system lifecycle, from on-boarding through to decommissioning. IT Systems can be continuously monitored for common vulnerabilities and exposures (CVEs) along with misconfigurations and other weaknesses in security posture. This ensures operating systems, applications and software are kept up to date and patches in-line with industry best practices and the wider requirements of the directive. Network and security infrastructure will also be continually monitored and assessed to ensure they meet the required baseline for security standards, and that configuration regarding critical security controls stays within desired thresholds. The XM Platform will also ensure that Identities, Credentials, and Security Groups that are underutilized or no longer required by the business are decommissioned correctly and completely.
06	**Policies and procedures to assess the effectiveness of cybersecurity risk management measures**	The XM Cyber platform provides in-depth risk analysis and operational threat intelligence that can be used to continuously assess the effectiveness of cybersecurity infrastructure, security posture and the cyber hygiene of IT systems and services. Data provided by the platform can be utilized to inform human-led adversary emulation activities in a more efficient manner. This includes testing compensating controls along identified attack paths to critical assets, performing targeted attack emulations designed to validate detection rules and inform detection engineering activities, or to test the efficacy of response procedures. This holistic approach can be used to validate the organization’s ability to mitigate, detect, and continuously respond to known real-world and specific threats, thereby providing an integrated and central component of effective cyber resilience strategy.

NIS 2 Risk Management Requirements

REQUIREMENT		XM CYBER COVERAGE
07	**Basic computer hygiene and trainings**	The XM Cyber platform acts as a key source of intelligence for the cyber hygiene of IT assets, Systems, and Services. This extends to the hybrid attack surface of Cloud Security Posture, security tools, their configuration and integrity, and the hygiene of identity and credential services. The insights provided by the platform can be used to improve security defense, bolster security posture, and enhance network segmentation strategies. The Platform is not directly involved in security training and awareness outside of the intelligence it provides to the Security Operations Teams.
08	**Policies and procedures for the use of cryptography and, when relevant, encryption**	The SCM module for the XM Cyber Platform can assess the configuration of cloud infrastructure, cloud security services, and on-prem security tools, to ensure best practices and vendor recommendations are adhered to for the configuration and management of cryptographic services and data encryption.
09	**Human resources security, access control policies and asset management**	The XM platform can be leveraged to help validate the effectiveness of access control policies, and their adherence to a least privilege methodology, as a key component to Identity and Asset Management. Threat scenarios can be provisioned to support the continuous identification and risk assessment of employees with access to sensitive data and systems. This helps track the confidentiality and integrity of data systems and the privileged identities accessing them, which in turn ensures that entitlements are not excessive or abusable.
10	**Use of multi-factor, secured voice/video/text comm and secured emergency communication**	The SCM module for the XM Cyber Platform can assess the configuration of cloud infrastructure, cloud security services, and on-prem security tools, to ensure best practicesand vendor recommendations are adhered to for the implementation of Multi-factor Authentication (MFA) and Single-Sign-On (SSO) Services.

Recommendations and Actions

NIS 2 is less about the enforcement of impractical requirements or imposing excessive financial burden on organizations through unnecessary standards, and instead aims to increase the cyber resilience programs of organizations providing critical services. Aligning to the NIS 2 Directive should not be thought about in terms of avoidance of financial consequences but instead seen as a guiding light to increase cyber resilience through a proactive approach involving understanding, assessment, and strategic investment that can pave the way for a more secure digital landscape for everyone.

Organizations across the EU should first look to understand if they are in scope for the Directive and under which member states laws they need to adhere.

STEP 1

Perform a gap analysis to identify shortfalls in your current cybersecurity policies, procedures, risk framework, incident handling procedures, and business continuity.

STEP 2

Ensure they have visibility and awareness of all Network and Information Systems, including those provided by third parties and service providers.

STEP 3

Define a Governance Risk and Compliance Framework that includes all areas of focus under Article 21 of the NIS 2 Directive.

STEP 4

Consider adopting a Continuous Threat Exposure Management (CTEM) methodology to drive your alignment to the requirements of the NIS 2 Directive.

The NIS 2 Directive aims to promote a culture of cybersecurity awareness, resilience, and responsibility within organizations and across critical sectors to enhance overall cybersecurity readiness and protect against cyber threats.

Collaboration and Proactive communication form a crucial part in maintaining trust with stakeholders and ensuring a prompt and coordinated response to cyber threats.

The Directive also encourages organizations to prioritize business continuity within their cybersecurity efforts, organizations can enhance their resilience, maintain service availability, protect critical assets, and ultimately safeguard their reputation and operational continuity in the face of cyber threats.

Benefits of Incorporating XM Cyber Into Your NIS 2 Adoption

The XM Cyber platform provides comprehensive coverage for addressing a broad set of the requirements outlined in the EU's NIS 2 Directive. Through its diverse capabilities, the platform plays a vital role in bolstering operational resilience and aligning with regulatory guidelines.

By acting as a foundational component for cybersecurity risk analysis, XM Cyber identifies security exposures across the digital attack surface, assesses their exploitability using XM Attack Graph Analysis™, and prioritizes remediation efforts based on the risks posed to business-critical assets and systems.

XM Cyber helps organizations adopt a holistic approach to quantify exposure risks related to vulnerabilities, misconfigurations, identity issues, weak security posture, and poor cyber hygiene, allowing organizations to establish a baseline of their security posture and develop proactive defense strategies and policies to minimize risks and fortify security defenses.

To enhance incident management and investigation, the XM Cyber Platform provides rich contextual information to aid in post-incident investigation and root cause analysis of cybersecurity incidents. These insights provide value to both a proactive and reactive cybersecurity strategy, enabling security operations teams to formulate response and remediation action plans and future-proof defense strategies.

Quantification of Risk Using XM Attack Graph Analysis™

The comprehensive risk analysis and exposure insights provided through the platform help organizations identify and classify business-critical assets, and quantify the risk presented by vulnerabilities, misconfiguration, weak security posture, and identity issues across their digital attack surface on a continuous basis, to optimize their Risk Management framework.

Accelerate and Enrich Incident Investigation to Aid Recovery and Prevent Future Breaches

Operational threat intelligence and attack path insights enrich advanced Threat Hunting and post-incident investigation. Rich contextual information reported in threat scenarios accelerates incident investigation, and enhances the learning and evolution of the network and information security incident management processes.

Continuous Analysis, Testing, and Security Improvements

The platform delivers a comprehensive, continuous, and automated approach to support network and information system risk assessment and cyber resilience testing. The XM Cyber platform delivers end-to-end testing of the digital attack surface of organizations and their third-party service providers and supply chain.

Effective Mobilization to Drive Compliance Strategy

Flexible remediation guidance provided by the XM Cyber platform plays a crucial role in assisting organizations with compliance to the NIS 2 Directive. By providing detailed and actionable recommendations for addressing security exposures, vulnerabilities, and misconfigurations organizations can prioritize and effectively remediate issues that could pose risks to their operational resilience.

XM Cyber – Supporting Your NIS 2 Journey

Our Continuous Threat Exposure Management (CTEM) methodology encompasses vulnerability assessments, cyber hygiene assurance, identity and credential security, breach attack simulation, security controls testing, and cloud security and posture management all within a single unified platform. This aids audit readiness, uncovers risk, and prevents cyber threats.

Specifically, in the context of the NIS 2 Directive, which emphasizes the importance of robust risk management, incident handling, and operational resilience, the platform's comprehensive exposure insights enable organizations to align their cybersecurity practices with the regulatory requirements outlined in NIS 2.

By offering a structured approach to addressing security issues and improving security posture, the platform helps organizations strengthen their defenses, enhance incident response capabilities, and ultimately enhance their overall operational resilience in line with the Directive.

Furthermore, XM Cyber's remediation guides can provide organizations with clear and actionable steps for addressing vulnerabilities in a timely manner, ensuring that they stay ahead of potential threats and remain compliant with the evolving regulatory landscape. By utilizing the guidance and recommendations offered by remediation guides, organizations can proactively protect their systems and data, reduce the likelihood of security incidents, and demonstrate a commitment to cybersecurity best practices as mandated by the NIS 2 Directive.

XM Cyber