The NIS2 Directive

SOPHOS

The EU Network and Information Security (NIS) directive was the first piece of EU-wide legislation on cybersecurity that came into force in 2016. However, to address the limitations identified within the current framework and to respond to the growing cybersecurity threats in the EU in the wake of digitalization and Covid-19, the European Commission has replaced the NIS Directive with the NIS2 Directive that introduces more stringent supervisory measures for national authorities, stricter enforcement requirements, and aims at harmonizing sanctions regimes across Member States. The NIS2 Directive entered into force on January 16, 2023, and the Member States have 21 months, until October 17, 2024, to transpose the directive into national law.

The NIS2 Directive aims to strengthen security requirements in the EU by expanding its scope to more sectors and entities; taking into account measures like risk analysis and information system security policies, incident handling, and supply chain security; and streamlining reporting obligations, among others. In case of non-compliance, NIS2 requires member states to provide for hefty penalties: €10 million or 2% of global turnover (whichever is higher) for essential entities and €7 million or 1.4% of global turnover (whichever is higher) for important entities.
NIS2 imposes direct obligations on the management bodies for implementation and supervision of their organization's compliance with the legislation. Non-compliance could potentially lead to the imposition of a temporary ban from discharging managerial responsibilities on the senior management of the entity, including the C-Suite level executives.

This document maps out how Sophos solutions offer effective tools to support organizations in addressing Chapter IV of the NIS2 Directive, **Cybersecurity Risk-Management Measures And Reporting Obligations,** and eventually help them to comply with the NIS2 Directive.

Specifications and descriptions are subject to change without notice. Sophos disclaims all warranties and guarantees regarding this information. The use of Sophos 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.

NIS2 Directive - Chapter IV, Cybersecurity Risk-Management Measures and Reporting Obligations

NIS2 DIRECTIVE REQUIREMENTS	SOPHOS SOLUTION	HOW IT HELPS
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.	**Sophos Training and Certifications**	Training courses and certifications to help partners and customers get the best out of Sophos security deployments; access to latest know-how and expertise for security best practices.
	Sophos Phish Threat	Provides simulated phishing cyberattacks and security awareness training for the organization's end users. Courses cover a wide range of topics from phishing and cybersecurity overview lessons, through to data loss prevention, password protection and more.
Chapter IV, Article 21, Cybersecurity risk-management measures		
2. Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems... based on a) policies on risk analysis and information system security;	**Sophos Intercept X** **Sophos Intercept X for Server**	Integrates innovative technology like deep learning, anti-exploit, and anti-adversary into malicious traffic detection with real-time threat intelligence to help prevent, detect, and remediate threats with ease across all devices and platforms.
	Sophos Firewall	Leverages Sophos' industry-leading machine learning technology (powered by SophosLabs Intelix) to instantly identify the latest ransomware and unknown threats before they get on your network. Delivers advanced protection from the latest drive-by and targeted web malware, URL/Malicious site filtering, Web Application Filtering, Cloud-based filtering for offsite protection.
	Sophos Cloud Optix	Continuously monitors and detects drift in configuration standards, and prevents, detects, and automatically remediates accidental or malicious changes in resource configuration.
	Synchronized Security feature in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls – stopping advanced attacks.
	Sophos Managed Detection and Response (MDR)	24/7 threat detection and response identifies and neutralizes advanced cyber-attacks that technology alone cannot stop.
2. b) incident handling;	**Sophos Managed Detection and Response (MDR)**	Continuously monitors signals from across the security environment, including network, email, firewall, identity, endpoint, and cloud technologies, enabling us to quickly and accurately detect and respond to potential cybersecurity events. Full incident response service is included as standard, providing 24/7 coverage delivered by IR experts. Includes full root cause analysis and reporting. Our average time to detect, investigate and respond is just 38 minutes.
	Sophos Rapid Response Service	Enables fast assistance, identifying and neutralizing active threats against your organization – delivered by an expert team of incident responders.
	Synchronized Security in Sophos products	Shares telemetry and health status, enabling coordinated isolation, detection, and malware remediation across servers, endpoints, and firewalls.

NIS2 DIRECTIVE REQUIREMENTS	SOPHOS SOLUTION	HOW IT HELPS
2. c) business continuity, such as backup management and disaster recovery, and crisis management;	**Sophos Managed Detection and Response (MDR)**	Ensures the information security aspect of business continuity management with 24/7 detection of and response to security incidents across the IT environment, leveraging human expertise, AI, and advanced technologies.
	Sophos Intercept X **Sophos Intercept X for Server**	Integrates innovative technology like deep learning, anti-exploit, and anti-adversary into malicious traffic detection with real-time threat intelligence to help prevent, detect, and remediate threats with ease across all devices and platforms. Includes rollback to original files after a ransomware or master boot record attack. Provides forensic-level remediation by eradicating malicious code as well as eliminating nasty registry key changes created by malware.
	Sophos Cloud Optix	Monitors AWS, Azure and GCP accounts for cloud storage services without backup schedules enabled and provides guided remediation.
2. d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;	**Sophos Intercept X with XDR**	Provides comprehensive defense in depth against threats that get in via third-party suppliers using AI, exploit prevention, behavioral protection, anti-ransomware and more. Plus, powerful XDR functionality enables you to automatically identify suspicious activity, prioritize threat indicators, and quickly search for potential threats across your endpoint and servers.
	Sophos Managed Detection and Response (MDR)	Delivers expert threat hunting and remediation as a fully managed service. Sophos specialists work around the clock to proactively hunt for, validate, and remediate potential supply chain threats and incidents on your behalf.
	Sophos ZTNA	Safeguards against supply chain attacks that rely on supplier access to your systems via very granular access controls. This cloud-delivered solution validates user identity, and device health and compliance before granting access to resources. It authenticates requests from trusted partners, irrespective of the location.
2. e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;	**Sophos Managed Detection and Response (MDR)**	Our threat-hunting experts monitor and investigate alerts from across the network, leveraging network, firewall, cloud, email, and endpoint security tools to identify and investigate suspicious activities and protect personal data wherever it resides. Sophos NDR generates high-caliber actionable signals across the network infrastructure to optimize cyber defenses. Sophos MDR proactively responds to vulnerability disclosure by the client. On notification, a full investigation is initiated that looks for signs of exploitation. If necessary, Sophos MDR will remediate the incident and provide guidance on how to harden the environment against future exploitation. A full human-authored report is provided in response to the disclosure investigation.
2. f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;	**Sophos Managed Detection and Response (MDR)**	Investigates and assesses potential security risks across the full environment 24/7, leveraging world-leading threat intelligence from Sophos X-Ops to identify risk levels and prioritize response.
2. g) basic cyber hygiene practices and cybersecurity training;	**Sophos Training and Certifications**	Training courses and certifications to help partners and customers get the best out of Sophos security deployments; access to latest know-how and expertise for security best practices.
	Sophos Phish Threat	Provides simulated phishing cyberattacks and security awareness training for the organization’s end users. Courses cover a wide range of topics from phishing and cybersecurity overview lessons, through to data loss prevention, password protection and more.
2. h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;	**Sophos Central Device Encryption**	Protect devices and data with full disk encryption for Windows and macOS. Verify device encryption status and demonstrate compliance.
	Sophos Email **Sophos Firewall**	Offers TLS encryption and support for SMTP/S along with full push-base, and optional pull-based portal encryption.
	Sophos Mobile	Enforces device encryption and monitors compliance relative to encryption policy.

NIS2 DIRECTIVE REQUIREMENTS	SOPHOS SOLUTION	HOW IT HELPS
2. i) human resources security, access control policies and asset management;	**Sophos Managed Detection and Response (MDR)**	Threat-hunting experts monitor and correlate information system activity across the full IT security environment, identifying and investigating suspicious activities by regularly reviewing records of information system activity, such as audit logs, access logs, access reports, and security incident tracking reports.
	Sophos Firewall	User awareness across all areas of our firewall governs all firewall policies and reporting, giving user-level controls over applications, bandwidth, and other network resources.
	Sophos Central	Keeps access lists and user privileges information up to date. Procedures are in place to ensure that access rights are revoked if individuals no longer meet the conditions to receive access (e.g., because they change position or leave the company).
	Sophos ZTNA	Enables better security and more agility in quickly changing environments by making it quick and easy to enroll or decommission users and devices. Continuously validates user identity, device health, and compliance before granting access to applications and data.
	Sophos Cloud Optix	Inventory management across multiple-cloud providers with continuous asset monitoring and complete network topology and traffic visualization.
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	**Sophos Firewall**	Supports flexible multi-factor authentication options including directory services for access to key system areas.
	Sophos ZTNA	Continuously validates user identity, device health, and compliance before granting access to applications and data.
	Sophos Central	Protects privileged and administrator accounts with advanced two-factor authentication.
	Sophos Cloud Optix	Monitors AWS/Azure/GCP accounts for Root user and IAM user access with MFA disabled so you can address and ensure compliance.
Chapter IV, Article 23, Reporting obligations		
4. Member States shall ensure that, for the purpose of notification under paragraph 1, the entities concerned submit to the CSIRT or, where applicable, the competent authority: d) a final report not later than one month after the submission of the incident notification under point (b), including the following: ***(i) a detailed description of the incident, including its severity and impact;***	**Sophos Managed Detection and Response (MDR)**	On notification, a full investigation is initiated that looks for signs of exploitation. If necessary, Sophos MDR will remediate the incident and provide guidance on how to harden the environment against future exploitation. A full human-authored report is provided in response to the disclosure investigation.
4. Member States shall ensure that, for the purpose of notification under paragraph 1, the entities concerned submit to the CSIRT or, where applicable, the competent authority: d) a final report not later than one month after the submission of the incident notification under point (b), including the following: ***(ii) the type of threat or root cause that is likely to have triggered the incident;***	**Sophos Managed Detection and Response (MDR)**	Sophos MDR investigates and assesses potential security risks across the full environment 24/7, leveraging world-leading threat intelligence from Sophos X-Ops. Full root cause analysis by Sophos MDR enables the environment to be hardened and response plans and strategies to be updated to incorporate learnings.
	Sophos XDR	Goes beyond the endpoint, pulling in rich network, email, cloud and mobile data sources to give you an even broader picture of your cybersecurity posture with the ability to drill down into granular detail when needed. With data from each product flowing into the Sophos Data Lake, you can quickly answer business critical questions, correlate events from different data sources and take even more informed action. For eg., you can cross-reference against network information to get a broader view of an incident or what happened to devices that were knocked offline in an attack.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

2023-03-15 RC-NA (PS)

SOPHOS