The bridge to possible

Strengthening Cyber Resilience with NIS2 and the Cisco Security Portfolio

Elevating Europe's Cybersecurity with NIS2

The European Union's revised Network and Information Security (NIS2) Directive aims to bolster cybersecurity posture across the EU, addressing the increasing number of cyber threats and evolving landscape. NIS2 establishes a framework for enhanced security, incident handling, and information and sharing to protect IT and OT infrastructure and ensure a high common level of cybersecurity across EU member states.

Cisco Security Portfolio: Comprehensive Cybersecurity

Cisco Security offers an extensive suite of advanced cybersecurity solutions designed to empower organizations to embrace NIS2 with confidence. By integrating a cutting-edge architecture, intelligence, and strategic services, Cisco Security helps protect against the most sophisticated cyber threats.

Outcomes:

Better Efficacy: Reduce your attack surfaces by stopping lateral movement of attacks and reducing risk across the data center and on-prem clouds.

Better Experience: Scales on your terms with a flexible security framework that supports all stages of cloud maturity.

Better Economics: Simplify your multicloud operations by consolidating security tools, unifying controls, and leveraging automation to achieve greater efficiencies.

The bridge to possible

Align to NIS2 with Cisco Security

Risk Management: Implement robust security policies and procedures that align with NIS2's risk management provisions using comprehensive tools and expertise within the Cisco Security portfolio.

Incident Handling: Facilitate rapid incident detection and response in compliance with NIS2 through Cisco XDR and integrated security analytics. Cisco Talos Incident Response (Talos IR) provides a full suite of proactive and emergency services to help you prepare, respond and recover from a breach. Talos IR enables 24-hour emergency response capabilities and direct access to Cisco Talos, one of the world's largest threat intelligence and research groups.

Supply Chain Security: Actively manage vulnerabilities throughout your IT stack and secure remote access to your systems to control risks from suppliers and contractors.

Resilience and Recovery: Enhance system resilience and ensure swift recovery from incidents with Cisco Secure Endpoint, which provides advanced malware protection, detection, and response capabilities to safeguard endpoints from cyber threats. When Cisco Identity Services Engine is integrated with Cisco Secure Endpoint, it enhances an organization's security posture by automatically responding to threats detected on endpoints. Cisco ISE can take immediate action and quarantine the affected device.

Assessing and Training: Conduct regular cybersecurity assessments and trainings with Cisco Talos Incident Response and Cisco Technical Security Assessment Services (CTAS).

Information Sharing: Promote cybersecurity information sharing within and across sectors, supported by Cisco Talos, one of the largest commercial threat intelligence teams in the world.

Partner for a Secure Future

Embrace the NIS2 Directive with Cisco Security as your partner in cybersecurity. Together we can build a resilient digital Europe that stands strong in the face of evolving cyber threats.

The bridge to possible

Cisco Security Portfolio Components

Cisco Cyber Vision

NIS2 Objective Alignment: Visibility into industrial networks and the OT security posture.

Benefits: Provides real-time visibility into industrial control systems and operational technology (OT) assets to assess risks and detect threats to your industrial operations.

Datasheet

Cisco Identity Services Engine

NIS2 Objective Alignment: NIS2 specifically requires implementing a zero-trust approach.

Benefits: ISE enables the creation and enforcement of security and access policies for endpoint devices connected to an organization's network. It plays a significant role in zero-trust architecture.

Datasheet

Cisco Secure Endpoint

NIS2 Objective Alignment: Advanced endpoint protection.

Benefits: Offers continuous monitoring and response capabilities for endpoints, quickly identifying and quarantining malicious files and activity.

Datasheet

Cisco Secure Network Analytics (SNA)

NIS2 Objective Alignment: Enhanced network visibility and detection of threats.

Benefits: Provides real-time monitoring and analytics to detect anomalous activities and potential security incidents across the network.

Datasheet

Cisco Secure Firewall

NIS2 Objective Alignment: Strong network perimeter defense.

Benefits: Delivers industry-leading firewall protection and intrusion prevention, enabling organizations to safeguard their networks against external attacks.

Datasheet

Cisco Duo

NIS2 Objective Alignment: Mandated multi-factor authentication (MFA), secure authentication and access control.

Benefits: Provides MFA and secure single sign-on (SS0) to ensure only authorized users can access critical systems and information.

Datasheet

The bridge to possible

Splunk Enterprise Security

NIS2 Objective Alignment: Reporting Mandate

Benefits: Splunk aligns with the NIS2 Directive by offering real-time visibility into their security data, advanced analytics for detecting and responding to threats, and streamlined compliance reporting, which are critical for adhering to the Directive's stringent requirements on security incident handling, risk management, and information sharing.

Datasheet

Extended Detection and Response (XDR)

NIS2 Objective Alignment: Reporting Mandate

Benefits: Cisco XDR offers a comprehensive security solution that can help organizations comply with the NIS2 Directive by integrating various detection capabilities, automating threat responses, and providing a unified view of threats across the network, endpoints, and cloud environments, which is essential for meeting the Directive's enhanced requirements for proactive threat detection, incident response, and resilience against cyber attacks.

Datasheet

Cisco Vulnerability Management

NIS2 Objective Alignment: Vulnerability Management

Benefits: Cisco Kenna Security provides an advanced risk-based vulnerability management platform that can assist organizations in aligning with the NIS2 by enabling them to prioritize and remediate the most critical vulnerabilities in their systems, thereby enhancing their cybersecurity posture and compliance with the NIS2 requirements for managing security risks and reporting incidents.

Datasheet

Cisco Secure Equipment Access

NIS2 Objective Alignment: Secure authentication and access control.

Benefits: Enables secure remote access to industrial networks to enforce ZTNA policies for suppliers and contractors to remotely configure and troubleshoot ICS and OT assets.

Datasheet

Cisco Secure Email

NIS2 Objective Alignment: Email security and anti-phishing.

Benefits: Protects against email-based threats, including phishing, malware, and business email compromise (BEC).

Datasheet

Cisco Secure Malware Analytics

NIS2 Objective Alignment: Malware analysis and threat intelligence

Benefits: Provides dynamic malware analysis and threat intelligence to help organizations understand and defend against sophisticated cyber-attacks.

Datasheet

The bridge to possible

Cisco Umbrella

NIS2 Objective Alignment: Protection against DNS and cloud-based threats.

Benefits: Delivers a cloud-delivered security platform that blocks malicious internet destinations before a connection is established.

Datasheet

Cisco Secure Web Appliance

NIS2 Objective Alignment: Web browsing security and control.

Benefits: Offers advanced threat defense, data security, and application visibility and control for web traffic.

Datasheet

Supply Chain Security

The Cisco Security portfolio helps secure the supply chain through robust third-party risk management and secure access controls.

- Actively manage vulnerabilities to reduce risks from equipment and software deployed in the environment. Cisco Vulnerability Management helps you identify and prioritize what needs to be patched.
- Control third party access to your networks by enforcing granular policies that limit what remote users can do.
- Cisco uses a repeatable and measurable process designed to increase the resilience and trustworthiness of Cisco products. This is called Cisco Secure Development Lifecycle (CSDL). Standardizing on fewer suppliers makes it simpler to assess and control your supply chain.

Compliance with NIS2 Directive

Risk Management: Cisco Security products support comprehensive risk management and mitigation strategies.

Incident Reporting: Cisco Security solutions enable rapid detection and reporting of security incidents, in line with NIS2 requirements.

Conclusion

The Cisco Security portfolio provides a cohesive and integrated approach to cybersecurity, aligning with the NIS2 Directive's objectives. Organizations leveraging Cisco Security solutions are equipped with the tools and resources necessary to achieve compliance, enhance security, and protect against evolving cyber threats.

1365512039 06/24