Framework Foundations: EU NIS2 Directive

Introduction to to the NIS2 Directive

The EU Network and Information Security (NIS2) Directive, effective January 16, 2023, giving Member States until October 2024 to adopt the directive into national law. It's important to note that compliance deadlines and specific requirements may vary slightly by country as Member States integrate the directive into their national legal frameworks.

Who is Affected?

The NIS2 Directive applies to a broad range of sectors and entities, including large enterprises (with over 250 employees or more than €50 million turnover) and medium-sized enterprises (with over 50 employees or more than €10 million turnover) from impacted sectors. It also covers public administration entities at central and regional levels, except those involved in national security, defense, or law enforcement.

NIS2 defines two categories of entities:

- Essential entities: Energy, transport, healthcare, drinking water, wastewater, digital infrastructure, banking, ICT service management, public administration, space
- Important entities: Postal services, chemical products, digital providers, research, food, waste management, manufacturing

Both categories share requirements but differ in supervision and penalties. Entities must comply if they operate or provide services in any EU country, no matter where they are based.

Objectives

- Strengthen cybersecurity in critical and essential sectors.
- Broaden the scope to cover more entities and industries.
- Require incident reporting and strong security practices.
- Enhance accountability via governance and risk management.

Key Requirements

To achieve compliance, organizations must implement a comprehensive set of technical, operational, and organizational controls. These requirements are grouped to reflect the directive's emphasis on governance, resilience, and security:

Governance & Oversight

- **Corporate Accountability:** Senior management must oversee cybersecurity strategy and receive training on security measures.
- **Security Policies & Audits:** Organizations must implement formal security policies, conduct regular audits, and effectively manage vulnerabilities.
- **Supervisory Measures:** Essential entities are subject to proactive and reactive supervision, including inspections and audits; important entities face lighter oversight.

Technical Controls

- **Access Control:** Enforce role-based access, multi-factor authentication, and monitoring of access to critical systems.
- **Cryptography:** Establish encryption policies to protect sensitive data in transit and at rest.
- **Supply Chain Security:** Extend cybersecurity requirements to third-party vendors and service providers.

Operational Resilience

- **Incident Reporting:** Essential entities must report incidents within 24 hours; important entities within 72 hours.
- **Risk Management:** Conduct regular risk assessments and implement appropriate security measures.

Role of ISO 27001 in NIS2 compliance

While ISO 27001 is not explicitly required by NIS2, it is:

- Encouraged in the preamble as a relevant international standard.
- Supported by ENISA by mapping ISO 27001 clauses to NIS2 requirements for compliance.
- Widely adopted as a framework for managing information security risks.

Benefits of aligning with ISO 27001

- Helps meet NIS2's risk management and governance expectations.
- Provides a clear, organized method for implementing security controls and managing incident response.
- Enhances cyber resilience and regulatory readiness.

How Cisco + Splunk Support Compliance

Combining Cisco and Splunk solutions delivers a powerful, integrated approach to meeting compliance requirements. Together, they provide comprehensive visibility, advanced analytics, and streamlined incident response to help organizations align with regulatory frameworks such as NIS2. Table 1 (on the following page) outlines key NIS2 clauses, describes how Cisco and Splunk support compliance for each, and lists the products that support compliance with the clause.

Table 1. Cisco and Splunk Solutions for NIS2 Compliance

Requirement	How Cisco + Splunk Support Compliance	Relevant Products
Risk Analysis	Real-time visibility, risk scoring, and threat detection across IT/OT environments	Cisco Cyber Vision, Cisco Secure Network Analytics, Cisco XDR, Cisco Secure Equipment Access, Cisco Secure Endpoint, Splunk Enterprise Security, Splunk Asset & Risk Intelligence
Business Continuity and Recovery	Integrated platforms for incident response, automated workflows, and disaster recovery	Cisco XDR, Splunk SOAR
Cryptography	VPN, encryption, and secure communications	Cisco Secure Client (including AnyConnect)
Assess Cyber Risk Management	Continuous monitoring, analytics, and evaluation of security measures	Cisco Secure Network Analytics, Cisco Cyber Vision, Cisco XDR, Cisco Identity Services Engine, Cisco Secure Endpoint, Splunk Enterprise Security, Splunk UBA, Splunk Asset & Risk Intelligence, Talos Threat Intelligence, Talos Incident Response Services
Incident Handling	Centralized management, automated response, and threat intelligence	Cisco XDR, Cisco Secure Endpoint, Cisco Secure Malware Analytics, Cisco Talos, Cisco Secure Firewalls, Splunk SOAR, Splunk Attack Analyzer, Splunk Enterprise Security
Information Sharing	Threat intelligence sharing and real-time updates	Talos Threat Intelligence, Cisco XDR, Cisco Secure Firewall, Cisco ISE, Cisco Cyber Vision, Splunk Platform, Splunk SOAR, Splunk Enterprise Security
Access Control	Policy-based access, segmentation, and multi-factor authentication	Cisco ISE, Cisco Duo, Cisco Secure Firewall, Cisco Secure Client, Cisco Secure Access, Cisco Cyber Vision
Network/IS Acquisition and Maintenance	Security monitoring, vulnerability management, and secure development lifecycle	Cisco Secure Network Analytics, Cisco Secure Client, Cisco Secure Endpoint, Cisco Duo, Meraki Systems Manager, Cisco Cyber Vision, Cisco Firepower, Splunk ITSI, Splunk Enterprise, Splunk SOAR, Splunk Asset and Risk Intelligence (ARI), Splunk Attack Analyzer

NIS2 Compliance with Cisco Security + Splunk

Cisco and Splunk together provide a powerful foundation for NIS2 compliance. Cisco's integrated security architecture delivers unified visibility, control, and threat response across hybrid environments, while Splunk's advanced analytics and automation capabilities enhance detection, investigation, and response at scale.

Unlike fragmented point solutions, Cisco provides a unified platform that brings together networking, security, observability, and collaboration. Splunk complements this with powerful data correlation and analysis across diverse sources, enabling faster insights and automated workflows.

By choosing Cisco and Splunk, organizations can break free from vendor silos and fragmented tooling. This joint approach supports a more efficient and scalable path to NIS2 compliance – ensuring operational resilience, regulatory alignment, and business continuity in today's complex digital landscape.

Resources

For more information and guidance on NIS2 compliance, please refer to the following resources:

- NIS2 Compliance for Industries
- NIS2 Directive: Challenges to Opportunities
- NIS2 Compliance for Industrial Operations
- Strengthening Cyber Resilience with NIS2 and the Cisco Security Portfolio