sysdig

Unlock the Power of NIS2

What you need to know

July 17, 2024 First EU-CyCLONe report

(Cyber Crisis Liaison Organisation Network)

NIS2 and DORA: It's in the Box

Deep dive into the technical aspects of NIS2 and DORA compliance.

READ NOW \rightarrow

Article 16, European cyber crisis liaison organisation network (EU-CyCLONe) H. EU-CyCLONe is established to support the coordinated management of Tagres-selae cybersecurity incidents and crises at operational level and to ensure the regular exchange of elevant information among Member States and Union insttions, bodies, offices and agencies. 2, EU-CyCLONe shall be composed of the repress of Member States' cyber crisis management auth Well as, in cases where a potential or ongoing las presecurity incident has or is likely to have a sig is in cases where a potential or ongoing las presecurity incident has or is likely to have a sig ison shall participate in the activities of EU-CyCLONe to apport the secure exchange of information. Whenker States ensuring secure exchange of information. Whenker States ensuring secure exchange of information.

October 17, 2024

Deadline for EU Member States to transpose NIS2 into national law NIS2 Countdown: What Security Leaders Need to Know Provides overview of key NIS2 requirements and best practices.

WATCH NOW \rightarrow

Every Second Counts: Delivering Secure, Compliant Financial Services in the Cloud

Engage with industry leaders and discuss challenges and opportunities.

WATCH NOW →

January 16, 2023 NIS2 Directive comes into effect

Cloud Security Regulations in Financial Services

Introduce NIS2 and its implications for the financial services industry.

READ NOW \rightarrow



The First CNAPP with Out-of-the-Box NIS2 and DORA Compliance Highlight your product's capabilities in addressing NIS2 and DORA

READ NOW \rightarrow

October 18, 2024

NIS2 provisions begin to apply across EU Member States

April 17, 2025

Deadline for Member States to identify essential and important entities

Cloud Security and Compliance: A Smarter Approach to Keeping Your Head Above Water

Position your company as a thought leader in cloud security and compliance

READ NOW \rightarrow

NIS2 Action Plan for the Cloud CISO

Offer a step-by-step guide for CISOs to implement NIS2 compliance

READ NOW \rightarrow

Major requirements

introduced by NIS2



Risk management

- Implement policies for risk analysis and information system security
- Establish **incident handling** procedures
- Ensure business continuity and crisis management
- Implement supply chain security measures, including supplier assessments

Reporting

- Report significant incidents **within 24 hours** (initial notification)
- Provide an update within 72 hours
- Submit a final report within one month

0) 0)

Governance and accountability

- Management bodies must approve cybersecurity measures and oversee implementation
- Provide cybersecurity training to staff and raise awareness

Technical measures

- Implement multi-factor authentication and continuous authentication solutions
- Ensure secure network and information systems
- Apply encryption and access control policies

Compliance and auditing

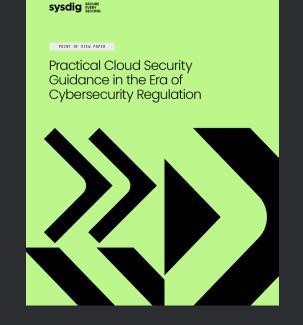
- Undergo regular audits and security assessments
- Maintain compliance documentation

Take the next step

Practical Cloud Security Guidance in the Era of Cybersecurity Regulation

Provide actionable advice to help organizations navigate the complex regulatory landscape





Not headquartered in the European Union?

The NIS2 Directive applies to non-European companies under certain conditions:

- Service providers that offer services within the
 EU or process data of EU individuals under NIS2
- You may need to designate a legal representative for the EU if your business is under NIS2
- Sectors in scope of NIS2: energy, transport, financial services, healthcare, digital services, government, manufacturing

Resource hubs

Security Practitioners

Achieve resilience with NIS2 and DORA



C-Suite

Secure your digital future with Sysdig

LEARN MORE →

sysdig

INFOGRAPHIC

COPYRIGHT © 2024 SYSDIG, INC. ALL RIGHTS RESERVED. ING-010 REV. A 01/25

About Sysdig

In the cloud, every second counts. Sysdig stops cloud attacks in real time by instantly detecting changes in risk with runtime insights and open source Falco. We correlate signals across workloads, identities, and services to uncover hidden attack paths and prioritize the risks that matter most.

CONTACT US \rightarrow