sysdig SECURE EVERY SECOND.

WHITE PAPER

NIS2 Action Plan for the Cloud CISO

Introduction to NIS2

The Network and Information Systems Directive 2 (NIS2) is an updated European Union directive designed to strengthen cybersecurity across Member States. It replaces the original NIS Directive from 2018, extending its scope and introducing stricter requirements to improve the resilience of a broader critical infrastructure against cyber threats. For organizations in the cloud, understanding NIS2 is crucial for ensuring compliance and strengthening security postures.

Table of Contents

Introduction to NIS2 02

Key findings 04

Recommendations 05

Scope and applicability 06

- Broader sector inclusion
- Enhanced regulatory framework
- Governance and accountability
- Cross-border and supply chain considerations
- Impact felt by cloud organizations

Key requirements for compliance 10

- Risk management and security measures
- Fast incident reporting timelines
- Governance and accountability
- Raising the bar for cybersecurity across the EU

Implications for cloud security 14

- Enhanced security obligations
- Multi-cloud and hybrid environments
- Security operations must evolve to embrace these requirements

Strategies for compliance 17

- Comprehensive risk assessment
- Strengthening incident response
- Supply chain security
- Do the right thing and document it thoroughly

Technological solutions and tools 21

- Cloud security platforms
- Advanced encryption techniques
- Technology serves effective processes and robust architecture

Enhancing cyber resilience 24

- Cybersecurity culture
- Collaboration and information sharing
- Comprehensive cybersecurity is a team sport

Recommended action plan for the cloud-native CISO 27

For cloud-centric organizations, NIS2 represents both a challenge and an opportunity to enhance cybersecurity frameworks [1]. By understanding its requirements and implementing robust compliance strategies, organizations can meet regulatory obligations and significantly strengthen their overall security posture. Embracing NIS2 will ensure that cloud environments are resilient, secure, and capable of withstanding the evolving threat landscape.

Key findings

01

Expanded scope and stringency [2]

NIS2 broadens its applicability to include more sectors and introduces more stringent security measures and incident reporting requirements, significantly impacting cloud service providers, digital infrastructure entities, and cloud-centric organizations.

02

Enhanced security measures [3]

NIS2 mandates robust risk management practices, including advanced encryption, strict access management protocols, and enhanced incident response strategies. These measures ensure both comprehensive data protection and rapid mitigation of cybersecurity threats.

03

Governance and collaboration

The directive emphasizes the importance of senior management accountability in cybersecurity governance. It also promotes enhanced collaboration and information sharing among EU Member States, as well as between public and private sectors, to foster a collective approach to cybersecurity resilience.

1. See Directive 2022/2555, Article 1 for the general provisions outlining the directive's aims and objectives
2. Refer to Article 2 for the scope and applicability of NIS2, which details the expanded sectors covered
3. Refer to Articles 21 and 22 for mandated security measures and risk management practices

Recommendations

By focusing on these areas, you can ensure your organization's robust compliance with NIS2, enhance your cloud security posture, and strengthen your resilience against cyber threats.

Cloud-native CISOs with a responsibility to comply with NIS2 should:

01 **Strengthen risk management practices**[4]**:** Implement continuous risk assessments and threat modeling to proactively identify and mitigate vulnerabilities in cloud environments.

02 **Enhance incident response capabilities**[5]**:** Deploy automated detection and response tools and conduct regular incident response drills to ensure rapid and effective threat mitigation.

03 **Implement robust data protection measures**[6]**:** Utilize advanced encryption techniques and centralized key management systems to secure data at rest and in transit across all cloud platforms.

04 **Ensure comprehensive compliance and governance**[7]**:** Engage senior management in cybersecurity governance, and appoint dedicated security officers to oversee compliance with NIS2 requirements.

05 **Foster collaboration and information sharing**[8]**:** Participate in industry-specific information-sharing platforms and public-private partnerships to enhance threat intelligence and collective cybersecurity resilience.

4. Refer to Article 21 for risk management measures
5. Refer to Article 23 for incident reporting requirements
6. Refer to Articles 26 and 27 for security measures including encryption and access control
7. Refer to Articles 24 and 25 for governance requirements and accountability
8. Refer to Article 29 for rules on information sharing

CHAPTER 01

Scope and applicability

The NIS2 Directive marks a significant evolution in EU cybersecurity regulations, expanding its impact and tightening requirements to enhance the resilience of critical infrastructures and services across Member States. This section delves into the expanded scope and applicability of the updated directive.

Broader sector inclusion [9]

- **Essential entities:** NIS2 extends its coverage to include more sectors now considered critical for societal and economic functions. Initially, NIS included traditional sectors like energy, transport, and healthcare. The new sectors include space, digital infrastructure, and public administration. Including digital infrastructure covers cloud services, data centers, and online marketplaces, directly impacting cloud service providers and digital service providers.
- **Important entities:** This category includes sectors like postal services, waste management, and chemicals. It also significantly impacts digital service providers, including cloud computing, digital payment, and social networking services.
- **Implications for cloud business:** Cloud and digital service providers must now ensure compliance with the NIS2 Directive. This means increased regulatory scrutiny and the need to adhere to more stringent cybersecurity standards and reporting protocols. This includes infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS) offerings that support critical business operations.

Enhanced regulatory framework [10]

Risk management and security obligations

- **Mandatory risk management practices:** NIS2 mandates that all covered entities establish a robust risk management framework. This includes regular risk assessments, implementation of proactive and defensive security measures proportional to the risk, and continuous monitoring to adapt to evolving threats.
- **Specific security measures:** Entities must adopt specific security measures such as network security controls, incident detection systems, data encryption, and access controls. For cloud-based companies, this translates to implementing advanced cybersecurity technologies and maintaining stringent security protocols to protect data and infrastructure.

9. Refer to Annex I and II for the list of sectors and types of entities covered
10. Refer to Articles 21 and 22 for risk management and security obligations

Incident reporting enhancements

- **Timely notification requirements:** Under NIS2, organizations must report significant incidents within a very short timeframe. They have 24 hours to provide an initial report and a detailed follow-up report within the first 72 hours. This rapid reporting is crucial to enabling quick response and coordination beyond the organization's level to mitigate the greater impact of cyber incidents across the EU.
- **Detailed reporting content:** Reports must include information on the nature of the incident, measures taken to address it, and the impact on service continuity. Establish robust incident reporting mechanisms and ensure that incident details are thoroughly documented and well communicated.

Governance and accountability[11]

Executive and organizational responsibilities

- **Senior management involvement:** NIS2 emphasizes the role of senior management in overseeing and ensuring compliance with cybersecurity requirements. This includes the obligation for executives to be knowledgeable about cybersecurity risks and to allocate adequate resources to address these risks. A CISO or CIO should keep the rest of the executive team informed of their organization's cybersecurity posture and risks so they may all make informed decisions in risk management.
- **Designation of security officers:** Organizations must appoint dedicated security officers or equivalent roles responsible for managing cybersecurity policies, incident response plans, and compliance with NIS2 requirements. This role is critical for cloud users in coordinating security efforts across various service offerings and customer environments.

Increased penalties for non-compliance

- **Stricter enforcement and fines:** NIS2 introduces more stringent enforcement measures and higher penalties for non-compliance. Organizations that fail to comply with the directive can face significant fines. The intention is to ensure that cybersecurity is prioritized at all organizational levels.

11. Refer to Articles 24 and 25 for responsibilities of senior management and security officers

Cross-border and supply chain considerations[12]

Inter-EU cooperation

- **Enhanced collaboration mechanisms:** NIS2 promotes greater collaboration between EU Member States to ensure a coordinated response to cybersecurity threats. This includes sharing threat intelligence, coordinating incident response efforts, and harmonizing cybersecurity practices across borders.
- **Implications for multinational organizations:** For cloud organizations operating in multiple EU countries, this means aligning their cybersecurity practices with the directive's requirements across all jurisdictions to ensure seamless compliance and enhanced security posture.

Supply chain security requirements

- **Third-party risk management:** Organizations must assess and manage risks associated with their supply chains, ensuring that third-party vendors and service providers adhere to the same stringent cybersecurity standards. Organizations must implement rigorous vendor management policies, conduct regular security audits, and fulfill contractual obligations for security compliance with their partners and suppliers.

12. Refer to Article 30 for cross-border cooperation and supply chain security

SCOPE AND APPLICABILITY

Impact felt by cloud organizations

The expanded scope and applicability of NIS2 requires cloud-centric companies to adopt comprehensive cybersecurity measures, enhance incident reporting protocols, and ensure executive-level accountability for cybersecurity governance. By understanding and adhering to these requirements, cloud-centric CISOs can better protect their organizations, and contribute to a more secure digital ecosystem within the EU.

CHAPTER 02

Key requirements for compliance

The NIS2 Directive imposes rigorous compliance requirements to bolster cybersecurity across EU Member States. This section examines what this means for the CISO and their team.

Risk management and security measures

Proactive risk management[13]

Continuous risk assessments

- **Regular evaluations:** Organizations must conduct ongoing risk assessments to identify vulnerabilities and potential threats. This includes assessing both internal systems and external dependencies, such as your supply chain.
- **Dynamic threat modeling:** Utilize a threat model to proactively anticipate and mitigate emerging cyber threats that concern your organization and environment.

Comprehensive risk mitigation strategies

- **Technical measures:** Deploy an all-encompassing tech stack that includes advanced security technologies, such as intrusion detection systems (IDS); intrusion prevention systems (IPS); security information and event management (SIEM); cloud-native application protection platform (CNAPP); and security orchestration, automation, and response (SOAR) solutions to detect and prevent cyber threats.
- **Organizational measures:** Establish and document clear policies and procedures for incident management, access control, and data protection to ensure a holistic security approach across the organization.

Baseline security requirements[14]

Incident response frameworks

- **Structured incident response plans:** Develop detailed incident response plans that outline roles, responsibilities, and procedures for handling security incidents.
- **Incident response teams:** Establish dedicated incident response teams (IRTs) trained to handle a broad range of cybersecurity incidents efficiently according to the established incident response plan.

13. Refer to Article 21 for details on risk management requirements
14. Refer to Article 22 for baseline security measures

Business continuity and disaster recovery

- **Continuity planning:** Create and maintain business continuity plans that ensure critical services remain operational during and after a cyber incident.
- **Disaster recovery:** Implement solutions that allow for rapid restoration of systems and data following an incident that disrupts operations.

Supply chain security

- **Third-party risk assessments:** Conduct thorough risk assessments of third-party vendors and service providers to ensure they meet stringent security standards.
- **Security clauses in contracts:** To enforce adherence to NIS2 standards, include specific security requirements and compliance clauses in contracts with third-party vendors.

Fast incident reporting timelines[15]

24-hour initial notification

- **Immediate reporting:** Organizations must report significant cybersecurity incidents to relevant authorities within 24 hours of detection, providing preliminary event details.
- **Communication channels:** Establish clear communication channels with regulatory bodies to facilitate timely reporting.

72-hour detailed reporting

- **Comprehensive incident reports:** Organizations must submit a detailed report outlining the nature of the incident, its impact, and the measures taken to mitigate it within 72 hours of becoming aware of the incident, not in addition to the 24-hour initial reporting window.
- **Post-incident analysis:** Conduct a thorough post-incident investigation using a digital forensics and incident response (DFIR) tool, such as Wireshark, to identify root causes and implement corrective actions to prevent future occurrences.

15. Refer to Article 23 for incident notification requirements

Governance and accountability[16]

Executive accountability

Board-level involvement

- **Cybersecurity governance:** Ensure cybersecurity is a key component of corporate governance, with board members actively overseeing cybersecurity strategies and risk management practices.
- **Resource allocation:** Allocate sufficient resources and budget to cybersecurity initiatives, reflecting the organization's commitment to robust security practices.

Security leadership roles

- **Chief Information Security Officer:** Appoint a CISO or equivalent role responsible for developing and implementing cybersecurity policies, managing incident response protocols, and ensuring compliance with NIS2.
- **Security committees:** Establish security committees that include the CISO and other stakeholders, such as the CTO and CFO, to review cybersecurity policies regularly, assess risks, and recommend improvements.

Designated security officers

Role definition and responsibilities

- **Clear mandates:** Define clear roles and responsibilities for designated security officers, ensuring they have the authority and resources needed to enforce cybersecurity policies.
- **Training and certification:** Provide ongoing training and certification opportunities to ensure security officers are aware of the latest cybersecurity trends and compliance requirements.

Incident management oversight

- **Centralized coordination:** Ensure that security officers coordinate all aspects of incident management, from detection to recovery, to maintain a unified response strategy.
- **Compliance monitoring:** Regularly monitor compliance with NIS2 requirements and reporting on the organization's security posture to senior management and regulatory bodies.

16. Refer to Articles 24 and 25 for governance requirements

KEY REQUIREMENTS FOR COMPLIANCE

Raising the bar for cybersecurity across the EU

The NIS2 Directive significantly raises the bar for cybersecurity across the EU, especially for cloud-centric companies. Organizations can achieve compliance and enhance overall cybersecurity resilience by implementing proactive risk management, adhering to stringent security measures, ensuring rapid incident reporting, and reinforcing governance and accountability. This comprehensive approach meets regulatory requirements and strengthens the organization's defense against an increasingly sophisticated cyber threat landscape.

CHAPTER 03

Implications for cloud security

The NIS2 Directive significantly impacts cloud security practices, necessitating enhanced measures and strategies to ensure compliance and safeguard digital assets. This section explores the extensive cloud security requirements for organizations operating in the EU.

Enhanced security obligations[17]

Data protection

Encryption standards

- **Advanced encryption:** Implement strong encryption protocols for data at rest and in transit to ensure data integrity and confidentiality. This includes using industry-standard encryption algorithms and key management practices.
- **End-to-end encryption:** Adopt end-to-end encryption to protect data from unauthorized access throughout its lifecycle, from creation to storage and transmission.

Data sovereignty compliance

- **Data residency requirements:** Ensure compliance with data residency regulations by maintaining data within specified geographical boundaries as required by NIS2.
- **Cross-border data transfers:** Implement measures to securely handle cross-border data transfers, including compliance with GDPR and other relevant data protection laws.

Access management

Robust Identity and Access Management (IAM)

- **Multi-Factor Authentication:** Implement MFA to add an extra layer of security, ensuring that only authorized users, but not necessarily all users, can access sensitive cloud resources.
- **Role-Based Access Control:** Use RBAC to limit access based on the principle of least privilege, ensuring users have only the permissions necessary for their roles. Monitor and remove unused permissions regularly to reduce the blast radius.

User activity monitoring

- **Continuous monitoring:** Track user activities and access patterns to detect and respond to anomalies that may indicate unauthorized access or potential security breaches.
- **Audit trails:** Maintain detailed audit logs of all access and activities within the cloud environment, enabling thorough investigations and compliance reporting.

17. Refer to Articles 26 and 27 for data protection and access management

Multi-cloud and hybrid environments[18]

Interoperability

Unified security policies

- **Consistent policies across platforms:** Ensure that security policies are uniformly applied across all cloud environments, whether multi-cloud or hybrid, to maintain a consistent security posture.
- **Policy automation tools:** Utilize automation tools to enforce security policies and configurations consistently across different cloud platforms.

API security

- **Gateways:** Implement secure API gateways to control and monitor traffic between cloud services, ensuring that APIs are protected from exploits and unauthorized access.
- **Threat protection:** Deploy an API security solution like a web application firewall (WAF) that can detect and mitigate API-specific threats like injection attacks and data exfiltration.

Centralized monitoring

Integrated security dashboards

- **Unified monitoring tools:** Integrated security dashboards, such as CNAPP, provide a single view of security status across all cloud environments, enhancing visibility and control for authorized users.
- **Real-time alerts and notifications:** Set up alerts and notifications to promptly inform security teams of any suspicious activities or security incidents.

Cloud Security Posture Management

- **Automated compliance checks:** Leverage CSPM tools or your CNAPP to automate compliance checks and ensure continuous adherence to NIS2 requirements across all cloud assets by alerting on non-compliance.
- **Risk assessment and mitigation:** Continuously assess cloud security posture and implement mitigation measures to address identified risks and vulnerabilities.

18. Refer to Articles 28 and 29 for interoperability and monitoring requirements

IMPLICATIONS FOR CLOUD SECURITY

Security operations must evolve to embrace these requirements

NIS2's impact on cloud security is profound. It requires cloud and digital service providers and cloud-centric organizations to adopt comprehensive data protection measures, robust access management, and effective strategies for managing multi-cloud and hybrid environments. By enhancing interoperability, centralizing monitoring, and ensuring consistent application of security policies, organizations can achieve compliance with NIS2 and bolster their overall security posture.

CHAPTER 04

Strategies for compliance

To effectively comply with NIS2, organizations must adopt a comprehensive approach that encompasses risk assessment, incident response enhancement, and robust supply chain security. This section provides an expanded look at strategic compliance measures.

Comprehensive risk assessment[19]

Regular assessments

Frequent risk evaluations

- **Scheduled assessments:** Conduct risk assessments at regular intervals to continuously identify and evaluate new and existing vulnerabilities within your cloud infrastructure.
- **Dynamic threat models:** Utilize threat models that can adapt to changing threat landscapes and emerging technologies.

Holistic approach

- **End-to-end security review:** Perform thorough security reviews covering all aspects of the cloud environment, including network security, application security, and endpoint security.
- **Risk prioritization:** Prioritize risks based on their potential impact and likelihood, allowing for targeted and efficient resource allocation to address the most critical threats.

Use threat intelligence

Leveraging threat intelligence feeds

- **Subscriptions:** Subscribe to reputable threat intelligence services that provide timely updates on emerging threats and vulnerabilities.
- **Integration with security systems:** Integrate threat intelligence feeds with existing security systems, such as SIEM and IDS/IPS, to enhance real-time threat detection capabilities.

Collaborative intelligence sharing

- **Industry collaboration:** Participate in industry-specific threat intelligence sharing programs to gain insights into sector-specific threats and best practices.
- **Public-private partnerships:** Engage in public-private partnerships to access broader threat intelligence resources and collaborate on threat mitigation strategies.

19. Refer to Article 21 for risk assessment strategies

Strengthening incident response [20]

Automated detection and response

Deployment of automation tools

- **AI and ML integration:** Utilize artificial intelligence and machine learning technologies to automate portions of the detection and response processes, improving speed and accuracy.
- **Automated playbooks:** Develop and implement automated response playbooks that can execute predefined actions to mitigate threats immediately upon detection.

Behavioral analytics

- **User and Entity Behavior Analytics:** Deploy UEBA tools to monitor and analyze user behavior patterns, detecting anomalies that may indicate potential security incidents.
- **Anomaly detection systems:** Implement systems that can identify other deviations from normal behavior, triggering alerts and automated responses to mitigate risks.

Incident response drills

Regular simulation exercises

- **Tabletop exercises:** Conduct short exercises that simulate various incident scenarios. These exercises help teams practice response strategies,improve coordination, and discover weak points and mitigation requirements.
- **Full-Scale simulations:** Organize larger simulations involving all relevant stakeholders to test the effectiveness of incident response plans in real-world scenarios.

Post-drill analysis

- **Lessons learned review:** After any exercise, conduct a detailed review to identify lessons learned, areas for improvement, and best practices.
- **Plan updates:** Regularly update incident response plans based on insights gained from drills and simulations.

20. Refer to Article 23 for incident response measures

Supply chain security [21]

Vendor risk management

Rigorous vetting processes

- **Due diligence checks:** Conduct comprehensive checks on all of your third-party vendors and consider reviewing available independent audits, assessing the vendors' security practices and compliance with NIS2 requirements.
- **Security audits:** Conduct regular audits of third-party vendors to verify their adherence to security standards and identify potential risks. Consider using the OpenSSF Scorecard project, which was devised to assist organizations in judging whether their dependencies are safe in the open-source software supply chain: [https://github.com/ossf/scorecard]

Continuous monitoring

- **Real-time vendor monitoring:** Use tools and technologies to continuously monitor vendor activities and security postures, ensuring ongoing compliance with security requirements.
- **Risk mitigation plans:** Develop and enforce plans for vendors identified as high-risk, including additional security controls and oversight.

Contractual obligations

Inclusion of security clauses

- **Security requirements:** All vendor contracts should include detailed security requirements and compliance obligations, ensuring clear expectations and accountability.
- **Liability clauses:** Incorporate liability clauses that hold vendors accountable for breaches or security incidents resulting from their negligence or non-compliance.

Service level agreements

- **Security-specific SLAs:** Define SLAs that specify security performance metrics, such as incident response times, uptime guarantees, and compliance reporting frequency.
- **Regular SLA reviews:** Conduct regular reviews and updates to ensure SLAs remain aligned with evolving security requirements and industry standards.

21. Refer to Article 30 for supply chain security requirements

STRATEGIES FOR COMPLIANCE

Do the right thing and document it thoroughly

Adopting a comprehensive strategy to comply with NIS2 involves thorough risk assessments, robust incident response enhancements, and stringent supply chain security measures. By focusing on these areas, cloud-centric organizations can achieve compliance and strengthen their overall cybersecurity resilience, ensuring they are well-equipped to handle the complexities of the modern threat landscape.

CHAPTER 05

Technological solutions and tools

The NIS2 Directive necessitates the use of robust technological solutions to ensure comprehensive compliance and effective cybersecurity. It's appropriate to examine the key technological tools and strategies critical for cloud service providers and organizations.

Cloud security platforms [22]

Integrated security tools

Unified security management

- **Comprehensive platforms:** Utilize platforms that integrate a broad range of security tools, such as firewall, network, and log visibility, to provide a singular, cohesive security environment.
- **Centralized management consoles:** Implement centralized management consoles, such as CNAPP and SIEM, that allow for unified monitoring, configuration, and management of security policies across all cloud services.

Continuous monitoring and threat detection

- **Real-time detections:** Leverage platforms offering real-time detections to continuously monitor cloud environments for threats and anomalies, such as a cloud detection and response (CDR) tool.
- **Behavioral analysis:** Deploy tools capable of analyzing user and entity behaviors to detect deviations from normal patterns that may indicate potential security incidents.

Access security

Visibility and control

- **Data discovery and classification:** Inventory data across cloud services, ensuring visibility into where sensitive data is stored such as Simple Storage Service (S3) buckets and how that data is accessed through IAM users and roles.
- **Policy enforcement:** Implement IAM to enforce security policies related to data access, sharing, and storage across all cloud platforms.

22. Refer to Article 27 for technological measures and tools

Threat protection

- **Malware detection:** Deploy a CDR tool with advanced malware detection capabilities to scan for anomalous behavior or indicators.
- **Data loss prevention:** Scan for user behavior in the cloud, and where possible, enforce least permissive access on IAM accounts to prevent destruction or accidental loss of sensitive data in the cloud.

Advanced encryption techniques [23]

Data encryption

Encryption standards

- **AES-256 and beyond:** Implement the Advanced Encryption Standard (AES) with 256-bit keys or higher to encrypt data at rest and in transit, providing robust protection against unauthorized access.
- **End-to-end encryption:** Adopt end-to-end encryption solutions to ensure data remains encrypted throughout its lifecycle, from creation to transmission and storage.

Tokenization and masking

- **Data tokenization:** Replace sensitive data elements with non-sensitive equivalents (tokens) with no exploitable value.
- **Data Masking:** To prevent exposure, implement masking techniques to obfuscate sensitive data in non-production environments, such as testing and development.

Key management

Centralized key management systems

- **Key management as a service:** Consider a KMaaS solution to centralize the management of encryption keys and ensure secure key generation, storage, and distribution.
- **Hardware security modules:** Deploy HSMs to provide physical security for key storage and management, protecting keys from unauthorized access and tampering.

Automated key rotation

- **Regular key rotation policies:** Implement automated key rotation policies to periodically change encryption keys, minimizing the risk of key compromise.
- **Secure key exchange protocols:** Use secure protocols such as Diffie-Hellman and Elliptic Curve Diffie-Hellman to exchange encryption keys securely over untrusted networks.

23. Refer to Article 26 for encryption standards and key management

TECHNOLOGICAL SOLUTIONS AND TOOLS

Technology serves effective processes and robust architecture

By leveraging integrated security platforms, CASBs, advanced encryption techniques, and robust key management practices, organizations can enhance their security posture, ensure data integrity, and comprehensively comply with NIS2 requirements. This proactive approach safeguards critical assets and positions organizations to navigate the complexities of modern cybersecurity threats effectively.

CHAPTER 06

Enhancing cyber resilience

NIS2 emphasizes the importance of building and maintaining cyber resilience to protect against evolving threats. For cloud-centric organizations, enhancing cyber resilience involves cultivating a robust cybersecurity culture, fostering collaboration, and embracing advanced technologies. This section details key strategies for cloud CISOs to enhance cyber resilience.

Cybersecurity culture [24]

Training and awareness

Continuous education programs

- **Regular training sessions:** Implement ongoing cybersecurity training programs tailored to different roles within the organization to ensure that all employees know the latest threats and best practices tailored to their position.
- **Phishing simulations:** Conduct regular simulations to train employees to recognize and respond to phishing attacks, enhancing their ability to avoid falling victim to social engineering tactics.

Role-specific training

- **Technical training for IT staff:** Provide specialized training for IT and security teams on advanced security tools, incident response techniques, and emerging threat trends.
- **Executive briefings:** Organize cybersecurity briefings for senior management to keep them informed about the organization's security posture, risks, and compliance requirements.

Policy development

Comprehensive cybersecurity policies

- **Policy framework:** Develop a comprehensive policy framework that covers all aspects of cybersecurity, including data protection, access control, incident response, and compliance with NIS2.
- **Regular policy reviews:** Schedule regular reviews and updates of cybersecurity policies to ensure they remain aligned with current threats and regulatory requirements.

24. Refer to Article 7 for national cybersecurity strategy and awareness

Employee engagement

- **Security champions:** Establish a program where selected employees advocate for cybersecurity best practices within their teams, fostering a security-conscious culture.
- **Incentive programs:** Create incentives to reward employees who demonstrate exemplary adherence to security policies and contribute to improving the organization's security posture.

Collaboration and information sharing[25]

Industry collaboration

Sector-specific information sharing

- **ISAC membership:** Join Information Sharing and Analysis Centers (ISACs) relevant to your organization's industry to receive timely threat intelligence and share best practices with peers.
- **Collaborative platforms:** Participate in forums where organizations can exchange information on emerging threats and effective mitigation strategies.

Joint cybersecurity exercises

- **Industry-wide drills:** Engage in industry-wide cybersecurity exercises to test collective response capabilities and improve coordination among sector participants.
- **Public sector collaboration:** Work closely with public sector agencies to align response strategies and enhance overall sector resilience.

Public-private partnerships

Enhanced threat intelligence sharing

- **Real-time data exchange:** Establish agreements with public-sector agencies to exchange real-time, actionable threat intelligence and early warnings about potential threats.
- **Joint research initiatives:** Use the strengths of both the private and public sectors to develop new cybersecurity technologies and strategies.

Crisis management coordination

- **Integrated response frameworks:** Develop integrated frameworks that align with public sector protocols, ensuring coordinated and efficient response to large-scale cyber incidents.
- **Mutual aid agreements:** Formulate agreements with other organizations and government entities to provide mutual support during significant cyber incidents, enhancing overall response capacity.

25. Refer to Articles 29 and 30 for collaboration and information-sharing frameworks

ENHANCING CYBER RESILIENCE

Comprehensive cybersecurity is a team sport

Enhancing cyber resilience is a multifaceted process. By focusing on continuous training, policy development, and effective information sharing, organizations can build a resilient security posture that not only meets NIS2 compliance but also effectively safeguards against the dynamic cyber threat landscape.

Recommended action plan for the cloud-native CISO

01

Conduct comprehensive risk assessments

- Perform regular, thorough risk evaluations to identify vulnerabilities.
- Utilize dynamic threat modeling to anticipate and address emerging threats.

02

Implement advanced security technologies

- Deploy integrated cloud security platforms and CASBs.
- Use advanced encryption and centralized key management systems.

03

Enhance incident response strategies

- Establish automated detection and response mechanisms.
- Conduct regular incident response drills and simulations.

04

Strengthen governance and compliance

- Engage senior management in cybersecurity governance.
- Appoint dedicated security officers to oversee compliance.

05

Foster collaboration and information sharing

- Join industry-specific threat intelligence platforms.
- Engage in public-private partnerships for broader threat intelligence.

06

Develop robust data protection policies

- Implement end-to-end encryption and robust access controls.
- Ensure compliance with data sovereignty & cross-border transfer regulations.

07

Enhance monitoring and reporting capabilities

- Use centralized monitoring systems for multi-cloud environments.
- Ensure compliance with NIS2's rapid incident reporting requirements.

08

Train and educate employees

- Conduct continuous cybersecurity training and awareness programs.
- Establish a security champions program to promote best practices.

09

Optimize supply chain security

- Implement stringent vendor risk management and security audits.
- Include specific security clauses and SLAs in vendor contracts.

10

Regularly review and update policies

- Continuously review and update cybersecurity policies and procedures.
- Ensure alignment with NIS2 requirements & evolving threat landscapes.

About Sysdig

In the cloud, every second counts. Attacks move at warp speed, and security teams must protect the business without slowing it down. Sysdig stops cloud attacks in real time, instantly detecting changes in risk with runtime insights and open source Falco. We correlate signals across cloud workloads, identities, and services to uncover hidden attack paths and prioritize real risk. From prevention to defense, Sysdig helps enterprises focus on what matters: innovation.

To learn more about Sysdig, visit sysdig.com

REQUEST DEMO →

WP-012 REV. A 7/24