NIS2 (Network and Information Security 2) – A Best Practices Guide

What is NIS2?

NIS2 stands for the second iteration of the EU's Network and Information Systems Directive. It is a set of cybersecurity regulations designed to improve the resilience and security of network and information systems across the EU. NIS2 requires organizations that provide essential services, such as energy, finance, healthcare, and transportation, to implement robust cybersecurity measures and report certain types of security incidents. The directive also establishes a cooperation framework between EU member states to share information and coordinate response to cyber incidents. Overall, NIS2 aims to improve the protection of critical infrastructure and enhance the cybersecurity posture of the EU. The key elements are:

- Cybersecurity law for the EU.
- Higher protection standards will be required.
- More sectors are under its scope.
- Reporting incidents will now be mandatory.
- Increased supervisory powers are granted.
- EU-wide harmonization of regulations.

What steps can you take to achieve NIS2 compliance?

1. Identify your critical infrastructure:

Identifying your critical infrastructure is essential to protect your most valuable assets.

- Determine which assets are critical to your business operations.
- Assess the risks to those critical assets.
- Use automated threat detection to identify potential risks and vulnerabilities in real-time.

Vectra AI can help you identify your critical infrastructure by continuously monitoring your network and cloud environments, providing real-time visibility into the security posture of your entire infrastructure. Learn more about the Vectra AI Threat Detection and Response platform.

2. Develop an incident response plan:

Developing an incident response plan is crucial for minimizing the impact of a security breach.

- Define roles and responsibilities for responding to security incidents.
- Establish procedures for reporting and investigating security incidents.
- Use threat intelligence to prioritize response efforts and minimize the impact of security incidents.

Vectra AI can help you develop an incident response plan by providing real-time threat detection for both known (with Suricata) and unknown threats, automated incident response capabilities and metadata for forensic analysis to help you quickly detect and respond to security incidents.

Learn more about Vectra AI Attack Signal Intelligence™ and Vectra Match.

3. Conduct regular security assessments:

IRegular security assessments are necessary for identifying vulnerabilities in your systems and addressing them before they can be exploited.

- Use vulnerability scanning tools or penetration tests to identify vulnerabilities in your systems.
- Conduct red team exercises to identify potential weaknesses in your security defense.
- Use automated vulnerability management and patch management tools to quickly remediate identified vulnerabilities.

Vectra AI can also assist with security assessments by running regular blue team workshops to identify potential weaknesses. You can also engage other third parties to provide dedicated pen-test services. You can register for a Vectra AI Blue Team Training Workshop.

4. Keep your software up to date:

Keeping your software up to date is essential for protecting your systems against known vulnerabilities.

- Use automated patch management tools to ensure that all software is up to date.
- Use vulnerability management tools to identify and remediate known vulnerabilities.
- Implement software whitelisting to prevent unauthorized software from being installed on company devices.

Vectra AI regularly releases updates to ensure that the platform is always up to date and protects you against known and unknown threats. Visit the Vectra AI Support Page.

5. Train your employees:

Your employees are your first line of defence against cyberattacks. Training your employees on cybersecurity best practices is essential for preventing security breaches.

- Provide regular cybersecurity training to all employees.
- Conduct phishing simulations to test employees' susceptibility to social engineering attacks.
- Implement a strong password policy and educate employees on password hygiene.

Vectra AI hosts regular webinars focused on informing customers on the latest cyber tech trends and delivers red and blue team workshops to help security professionals hone their cyber defence skills. Visit the Vectra AI Blog Posts.

6. Monitor your network for anomalies:

Monitoring your network for anomalies is essential for detecting security breaches as early as possible.

- Use behavioral analytics to detect anomalous activity on your network.
- Implement intrusion detection and prevention systems to prevent and respond to security incidents.
- Use machine learning algorithms to quickly identify and respond to threats in real-time.

Vectra AI can help you monitor your network for anomalies by providing industry leading Attack Signal Intelligence™, automated incident response capabilities and behavioral analytics to identify anomalies that may indicate a security breach. Vectra can provide coverage for networks, cloud, SaaS (software as a service) and identity environments. With native integrations to leading EDR (Endpoint Detection and Response) providers Vectra AI can provide coverage for all five attack surfaces. Vectra AI Managed Detection and Response services are available to help organizations who lack the required resources and skills to deliver a comprehensive internal service.

Learn more:

Vectra AI Network Detection and Response (NDR)

Vectra AI Identity Threat Detection and response for Azure AD (Active Directory)

Vectra Cloud Threat Detection and Response for AWS (Amazon Web Services)

Vectra AI Cloud Threat Detection and Response for M365

Vectra MDR (Managed Detection and Response) Services

7. Develop a disaster recovery plan:

Developing a disaster recovery plan is crucial for minimizing the impact of a security breach and ensuring that your business can continue to operate in the event of a security incident.

- Define recovery time objectives (RTOs) and recovery point objectives (RPOs) for critical systems.
- Implement data backup and restoration procedures to ensure that critical data can be recovered in the event of a security incident.
- Test your disaster recovery plan regularly to ensure that it is effective and up to date.

Vectra AI can help disaster recovery by providing automated incident response capabilities and forensic analysis to help you quickly detect and respond to security incidents.

Take a tour.

How Vectra AI protects against ransomware

What is NIS2?

The timeline to implement NIS2 can vary depending on the size and complexity of your organization's network and infrastructure, as well as the level of maturity of your existing cybersecurity program. However, in general, it is recommended to start planning for NIS2 implementation as soon as possible to ensure that your organization is prepared for the evolving threat landscape. Here is a potential timeline for implementing NIS2:

1. Assessment and planning (3-6 months):

This phase involves conducting a comprehensive assessment of your organization's current security posture to identify gaps and areas of improvement. This can include identifying critical assets, reviewing policies and procedures and conducting vulnerability assessments and penetration testing. Based on the findings, you can develop a roadmap and timeline for NIS2 implementation.

2. Implementation (6-12 months):

This phase involves implementing the necessary technical and organizational measures to comply with NIS2. This can include implementing security controls and tools, such as intrusion detection and prevention systems, firewalls, and SIEM (Security Information and Event Management) solutions, as well as establishing processes for incident response, vulnerability management and security awareness training.

3. Testing and validation (1-3 months):

This phase involves testing the effectiveness of the implemented measures to ensure that they meet the requirements of NIS2. This can include conducting security assessments, penetration testing, and tabletop exercises to validate the effectiveness of the implemented security controls and incident response procedures.

4. Compliance and ongoing maintenance (ongoing):

Once NIS2 is fully implemented, ongoing maintenance and compliance monitoring is necessary to ensure that the organization remains compliant with the regulation. This can include conducting periodic security assessments and vulnerability scans, monitoring for anomalous behavior, and maintaining up-to-date security policies and procedures.

Who should be involved?

Implementing NIS2 is a significant undertaking that requires the involvement of multiple stakeholders across an organization. The following individuals and teams should be involved in the implementation process:

1. Executive Leadership:

Executive leaders should be involved in NIS2 implementation to provide support and funding for the initiative. They should also ensure that the security program aligns with the overall business objectives and risk appetite of the organization.

2. IT and Security Teams:

IT and security teams are responsible for implementing the technical and operational measures required for NIS2 compliance. This includes implementing security controls, such as firewalls and intrusion detection and prevention systems, and establishing processes for vulnerability management and incident response.

3. Legal and Compliance Teams:

Legal and compliance teams should be involved in NIS2 implementation to ensure that the organization meets the regulatory requirements of the regulation. They should also be involved in developing policies and procedures related to data protection and incident response.

4. Human Resources:

Human resources teams should be involved in NIS2 implementation to ensure that employees are trained on security policies and procedures, and that appropriate background checks and access controls are in place for employees who handle critical assets.

5. Business Units:

Business units should be involved in NIS2 implementation to identify critical assets and assess the impact of security incidents on business operations. They should also be involved in developing business continuity and disaster recovery plans to ensure that critical business functions can continue in the event of a security incident.

6. External Partners:

External partners, such as third-party vendors and contractors should be involved in NIS2 implementation to ensure that they meet the security requirements of the organization. This includes conducting due diligence and contract reviews to ensure that third-party partners have adequate security controls in place.

It is essential to ensure that all stakeholders are involved in NIS2 implementation to ensure that the security program aligns with the overall business objectives and risk appetite of the organization. Additionally, engaging with a trusted cybersecurity partner, such as Vectra AI, can help organizations streamline the implementation process and ensure that all necessary stakeholders are involved.

Summary

Implementing NIS2 requires a comprehensive approach to cybersecurity that includes identifying critical infrastructure, developing an incident response plan, conducting regular security assessments, keeping software up to date, training employees, monitoring the network for anomalies and developing a disaster recovery plan. Vectra AI can help your company succeed in implementing NIS2 by providing coverage, clarity, and intelligent control aligned with native integrations with other leading cybersecurity solution vendors such as Microsoft, CrowdStrike, SentinelOne, Splunk, IBM QRadar, Amazon Security Lake, Palo Alto Cortex XSOAR, and many others.

Vectra AI solutions are also available via KPMG, Capgemini, Orange Cyber Defense, AT&T, NTT Data, and Dell technologies

Learn more about NIS2

Learn more about Vectra AI

Connect with a Vectra AI security expert

Get a Demo

Upcoming Events and Webinars

About Vectra

Vectra® is the leader in cyber threat detection and response for hybrid cloud. Vectra's patented Attack Signal Intelligence™ detects and prioritizes threats across public cloud, SaaS, identity, and networks in a single platform. Vectra's Attack Signal Intelligence goes beyond simple anomaly detection to analyze and understand attacker behavior. The resulting high-fidelity signal and deep context enable security operations teams to prioritize, investigate and respond to cyber attacks in progress sooner and faster. Organizations worldwide rely on the Vectra platform and MDR services to stay ahead of modern cyberattacks.

For more information please contact us:
Email: info@vectra.ai | vectra.ai