



WHITE PAPER

## **How To Comply With The NIS2 Directive**

# NIS2 DIRECTIVE

## WHAT IS IT AND HOW TO COMPLY

Cyber-attacks are becoming more frequent, more sophisticated, and more damaging. The tenth edition of ENISA's Threat Landscape proves this. To help defend against the growing impact of cyber threats, the European Union recently adopted the revised version ("NIS2") of the Network and Information Security Directive ("NISD"), which provides legal measures to improve the overall level of cybersecurity in the EU, and among others, the EU-wide cooperation on incidents and threats.

Below, we will describe what's in the NIS2 Directive and how organizations can comply with the Directive.

## WHAT IS THE NIS2 DIRECTIVE

The NIS2 Directive is a piece of European Union (EU) legislation that aims to improve the security and resilience of network and information systems across the EU.

The NIS2 Directive requires certain operators of essential services (OES) and digital service providers (DSPs) to take appropriate security measures and report significant security incidents to the relevant national authority. OES are organizations that provide critical infrastructure services in sectors such as energy, transport, and healthcare, while DSPs include online marketplaces, cloud computing services, and search engines.

The NIS2 Directive sets out a range of security requirements that OES and DSPs must adhere to, including implementing risk management measures, ensuring network and information system security, and having incident response plans in place. The Directive also requires OES and DSPs to regularly review and test their security measures to ensure their effectiveness. National authorities in EU member states are responsible for enforcing the NIS2 Directive and may carry out audits and inspections to ensure compliance. The

Directive also provides for cooperation and information-sharing between national authorities in the event of cross-border security incidents.

Overall, the NIS2 Directive aims to promote a culture of cybersecurity across the EU and improve the resilience of critical infrastructure and digital services against cyber threats. By complying with the requirements of the Directive, OES and DSPs can strengthen their security posture and reduce the risk of cyber incidents.

## WHAT IS THE US EQUIVALENT TO NIS2

The US equivalent to the NIS (Network and Information Systems) Directive is the Cybersecurity and Infrastructure Security Agency (CISA), which is responsible for protecting the nation's critical infrastructure from cyber threats. CISA is a federal agency within the Department of Homeland Security (DHS) that works with public and private sector organizations to manage cyber risk and build a more secure and resilient infrastructure.

CISA was created in 2018 by the Cybersecurity and Infrastructure Security Agency Act, which consolidated several existing agencies and programs into



a single entity responsible for cybersecurity and infrastructure security. CISA's mission is to "defend against today's threats and collaborate to build more secure and resilient infrastructure for the future." It provides a range of services and resources to help organizations manage cyber risk, including threat intelligence, incident response, vulnerability assessments, and risk management guidance.

Overall, while there are some differences in the specific approaches and requirements of the NIS2 Directive and CISA, both aim to enhance the cybersecurity and resilience of critical infrastructure by promoting risk management, incident response, and collaboration between public and private sector entities.

## HOW PLIXER HELPS YOU COMPLY WITH THE NIS2 DIRECTIVE

The Plixer platform gives you Deep Network Observability that allows you to see and understand what's happening in your IT environment at a glance. The Plixer platform provides you with a Network Detection and Response (NDR) solution to ensure that threats are identified early and stopped before they cause damage—regardless of where vulnerabilities are in your IT environment.

Unlike prevention tools that attempt to stop attackers from getting onto the network, the Plixer platform gives you Deep Network Observability that bridges cloud and on-premises environments to provide real-time, end-to-end visibility for anomaly detection and correlation, network and application performance, and traffic patterns and trends.

Plixer's platform provides comprehensive network visibility from the corporate network to the public cloud, making it the most comprehensive NDR solution on

the market. A sampling of its capabilities include:

- **Zero Trust Network Access (ZTNA) validation:** Confirming Zero Trust provides secure remote access to applications and services based on defined access control policies. Assets are mapped to transaction flows, and traffic flows are continuously monitored to identify anomalous behaviors.
- **Lateral movement detection:** Recognizes abnormal patterns in authentications by watching traffic as it's moving across the network—server to server, host to host, host to server, and within the data center.
- **Command & Control (C2) communication detection:** Detecting both active and passive C2 traffic thwarts attackers from issuing instructions to compromised devices, downloading additional malicious payloads, and sending stolen data outside the network.
- **Data movement detection:** Identifies abnormal network traffic patterns to stop attackers from exfiltrating sensitive data from staging devices.
- **Abnormal activity across the IT environment detection:** Using traffic baselining and anomaly detection, identifies abnormal activity, such as endpoints that access high-value locations for the first time.
- **Data exfiltration detection:** Sees data as it leaves the network through centralized controls by using abnormal outbound data traffic volumes, URL and DNS request information, and by leveraging threat intelligence feed data.
- **Endpoint Analytics:** Gain real-time insights into device identity, location, and behavior and risk data—as well as the ability to identify and respond to threats automatically. This helps organizations track assets (laptops, desktops, IoT, OT, and more), strengthen security and compliance, and mitigate risk.
- **Cloud threat detection:** Ingests cloud flow



logs, aggregating and orchestrating network detections across hybrid multi-cloud environments without having to deploy probes or reconfigure cloud networks.

Plixer's platform helps organizations address several of the NIS2 Directives measures, both explicitly and implicitly, by helping boost your security posture. Here are the various ways Plixer helps you comply with NIS2:

### **Threat detection**

Analyzed NetFlow and IPFIX data can identify potential security threats, such as suspicious network activity or traffic to known malicious IP addresses. By analyzing network traffic patterns, companies can detect anomalies and take appropriate action to prevent or mitigate potential security incidents.

While the NIS2 Directive does not explicitly mention "threat detection" as a requirement, it does require operators of essential services (OES) and digital service providers (DSPs) to take steps to prevent and minimize the impact of security incidents on their networks. This includes detecting potential security threats and vulnerabilities in their systems.

Under Article 14 of the NIS2 Directive, OES and DSPs are required to implement "appropriate and proportionate technical and organizational measures to manage the risks posed to the security of network and information systems which they use and offer for use." This includes measures to prevent and detect security incidents and actions to respond to and recover from security incidents. In addition, under Article 16 of the NIS2 Directive, OES and DSPs are required to have "incident response plans and procedures" in place to ensure a "coordinated and effective response" in the event of a security incident.

So, while "threat detection" is not an explicit requirement, not having early threat detection puts your organization in a compromised position. Plixer gives

you wide visibility of your IT environment, allowing you to see threats that bypass other controls, and monitor suspicious behavior across the network.

### **Incident response**

The NIS2 Directive recognizes the importance of incident response in maintaining the security and resilience of network and information systems. It requires OES and DSPs to have incident response plans and procedures in place and to work closely with Computer Security Incident Response Teams CSIRTs to ensure a coordinated and effective response in the event of a security incident. The NIS2 Directive explicitly mentions incident response in several places, including:

- Article 14 requires operators of essential services (OES) and digital service providers (DSPs) to take measures to prevent and minimize the impact of security incidents on their networks. This includes measures to respond to and recover from security incidents, as well as measures to detect and prevent security incidents.
- Article 16 requires OES and DSPs to have "incident response plans and procedures" in place to ensure a coordinated and effective response in the event of a security incident.
- Article 17 requires Member States to establish CSIRTs to facilitate cooperation and information-sharing between Member States and to support OES and DSPs in responding to security incidents.

In the event of a security incident, analyzed Plixer can show you the source and scope of the incident. Plixer collects data from across your IT environment and provides incident correlation, MITRE ATT&CK® mapping, and long-term forensics to aid your investigation and response efforts. Plixer provides extensive response capabilities. This includes both automatic responses, such as sending commands to a firewall so that it drops suspicious traffic, as well as



manual responses through threat hunting and incident response tools. With full network visibility, you can push alert data into existing solutions—network access control (NAC), firewalls, web application firewalls and SIEM/SOAR tools—fine-tuning the desired alarm frequencies, thresholds, and patterns.

Additionally, with integrations (SIEM/SOAR, EDR, ticket management systems, etc.) you can leverage Plixer’s data and alarms to trigger an automated response in your existing security controls.

### Compliance reporting

The NIS2 Directive requires operators of essential services and digital service providers to report significant security incidents to the relevant national authority. The NIS2 Directive includes several provisions related to compliance reporting, including:

- Article 14(3) requires operators of essential services (OES) and digital service providers (DSPs) to document the security measures they have taken and to keep these documents up to date.
- Article 14(5) requires OES and DSPs to notify the relevant national authority of any “incidents having a significant impact on the continuity of the essential services” they provide.
- Article 19 requires Member States to establish “a monitoring and reporting mechanism” for assessing the implementation of the NIS2 Directive within their jurisdiction.

The Plixer platform helps satisfy compliance reporting efforts by providing real-time visibility into network activity and helping to document the nature and scope of security incidents. Customizable reporting and dashboards allow you to easily track mission-critical data points. Long-term data retention allows you to dig deep into network traffic data to root-cause incidents and fully understand the severity of a particular incident.

### Risk management

Risk management is a crucial component of the NIS2 Directive. The Directive includes several provisions related to risk management, including:

- Article 14(1) requires operators of essential services (OES) and digital service providers (DSPs) to take “appropriate and proportionate technical and organizational measures” to manage the risks posed to the security of their networks and information systems.
- Article 14(2) requires OES and DSPs to take into account “state of the art, the costs of implementation and the nature, scope, context, and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.”
- Article 15 requires Member States to ensure that OES and DSPs identify and assess the risks posed to the security of their networks and information systems and take steps to manage these risks.
- Article 17(1) requires Member States to establish CSIRTs to facilitate cooperation and information-sharing between Member States and to support OES and DSPs in identifying and managing security risks.

Plixer supports your risk management efforts by identifying potential security risks and vulnerabilities in the network. By analyzing network traffic patterns, companies can identify areas of the network that may be at higher risk of attack and take appropriate measures to mitigate those risks.

Additionally, the Plixer platform has Endpoint Analytics as a native capability. Endpoint Analytics gives IT, network, and security operations teams deep visibility and tight control over network endpoints (PCs, mobile devices, VMs, IoT devices, OT, etc.). Gain real-time insights into device identity, location, and behavioral data, as well as the ability to identify and respond to



threats automatically. This helps organizations track assets, strengthen security and compliance, and mitigate risk.

Endpoint Analytics also automatically assesses and determines endpoint security risk. The score is an aggregate of four distinct vulnerability scores: operating-system-related risks, device-related risks, communications-related risks, and risks identified by external device management/security solutions (such as [Tenable.io](#)). When investigating potential threats or active incidents, teams can use the risk score to accelerate response times.

### **Network performance monitoring**

The NIS2 Directive does not specifically mention “network performance monitoring” as a requirement, as its focus is primarily on cybersecurity and the protection of critical infrastructure. However, network performance monitoring can be an important aspect of maintaining the availability and resilience of network and information systems, which are key objectives of the NIS2 Directive.

Under Article 14 of the NIS2 Directive, operators of essential services (OES) and digital service providers (DSPs) are required to implement “appropriate and proportionate technical and organizational measures to manage the risks posed to the security of network and information systems which they use and offer for use.” This includes measures to ensure the availability and resilience of these systems in the face of security incidents and other disruptions.

Network performance monitoring can help OES and DSPs identify and troubleshoot issues that could affect the availability and resilience of their systems. By monitoring network traffic and performance metrics such as latency, packet loss, and throughput, organizations can quickly identify and diagnose issues that could impact network performance and take corrective action to prevent disruptions. This can help to ensure that critical infrastructure and services

remain available and accessible, even in the face of security threats or other disruptions.

The Plixer platform goes beyond the traditional NDR solution set by providing powerful network performance monitoring intelligence within the same platform. These capabilities are built into the platform, allowing you to both secure and optimize your IT environment from a single solution.

### **Take action before an attack**

For security teams to bolster their cybersecurity postures, they need to address several areas. In particular, OES and DSPs will have to account for:

- The complex threat landscape and increasing attack surface
- Merging IT and OT security and technologies
- Changing cybersecurity regulation

Digitalization, automation, the Internet of Things (IoT), hybrid- and multi-cloud environments, and more are creating massive changes in today’s enterprise networks. With each new area comes a potential vulnerability and an opportunity for cybercriminals to exploit those vulnerabilities.

As more operational systems become digitized and interconnected, [OT and ICS systems have become the target of attacks](#). Previously these technologies may have been isolated or based on arcane software that made them difficult to attack, but this is no longer the case, and the division between OT and IT systems has essentially disappeared. But securing a hybrid OT/IT system requires new skills and ways of thinking. Security tools and procedures that can account for a hybrid system—with new and legacy equipment—is also necessary.



## SUMMARY

Without protection against threats to OT and ICS systems, companies remain vulnerable to attacks that can take control of their operations or freeze operations. Beyond financial and reputational harm, an OT attack has the potential to damage critical infrastructure, disrupt economies, and put lives at risk.

Plixer helps organizations bolster their security posture and meet compliance measures by providing a powerful NDR solution. Uninvited threats and disruptions can ruin your day and disrupt your business, while you burn time and resources trying to figure out what's happening and why. Act confidently with Plixer.


Join the new network defense revolution today and [book a demo](#).

## ABOUT PLIXER

Plixer gives you visibility and context of every network transaction so you can better understand what's happening in your IT environment. Our 20+ years of network monitoring and management solutions help us provide innovative solutions that help you secure and optimize your digital enterprise. Supercharge your business defense with AI-powered visibility and insight that goes beyond traditional NDR.

 [sales@plixer.com](mailto:sales@plixer.com)

 [plixer.com](https://plixer.com)

 68 Main St Ste 4  
Kennebunk, ME 04043



©Plixer, LLC. All rights reserved. Plixer and Scrutinizer are trademarks of Plixer. All other brand names are trademarks or registered trademarks of their respective companies.

The content in this document is for informational purposes only and is subject to change by Plixer, LLC without notice. While reasonable efforts have been made in the preparation of this publication to ensure its accuracy, Plixer, LLC assumes no liability resulting from technical or editorial errors or omissions, or for any damages resulting from the use of this information. Unless specifically included in a written agreement with Plixer, Plixer, LLC has no obligation to develop or deliver any future release or upgrade or any feature, enhancement, or function.