Recorded Future®

Implement NIS2 Directive Requirements with Recorded Future Intelligence Cloud

The NIS (Network and Information Systems) Directive was established by the European Union to provide guidance on the cybersecurity resilience of critical infrastructure and essential services. The second version of NIS expands on the previous directive by addressing some gaps and shortcomings identified over the past few years.

The Directive focuses on:

- **Implementation of robust security measures**
- **Development of documented incident response plans**
- **Prompt reporting of significant incidents to national authorities**
- **Foster cross-border cooperation**

NIS2 highlights the importance of risk management, supply chain security, and development and maintenance of robust incident response plans. In order to adapt to these requirements, there are some key areas for businesses to focus on

- **Implement both proactive and reactive processes to mitigate risk**
- **Focus on third-party suppliers as a part of your organization's attack surface**
- **Streamline processes for incident response**

How Can Recorded Future Help?

Gain a complete view of your threat landscape to identify what matters to you

- **Quickly identify top threat actors of interest, especially targeting your third-parties**
- **Determine most concerning malware based on your company's technologies**

Implement security controls and make adjustments as necessary

- **Understand the technical parameters of malware used in threat actor campaigns to close specific ports**
- **Update block lists with continuously validated IP addresses and domains for command & control (C2), botnet and remote access trojan (RAT) infrastructure**
- **Automatically reset passwords in an identity access management (IAM) system with recently stolen credentials**

[1] IBM Cost of a Data Breach 2023

Mitigate software threats originating from 3rd and 4th party vendors

Enrich vulnerabilities on scanned third-party products with data on weaponization

Dynamic risk scoring for third-parties, updated in real-time

Detect new threats with context

Receive a notification within minutes of a potential breach impacting a key third-party, such as a database offered for sale

Detect references to your brand and “secret” keywords on ransomware extortion sites to quickly understand the severity of potential leaked documents

Decrease time to respond and report

Equip users with essential information, updated in real time, on their threat landscape

Reduce time spent searching, summarizing, and writing reports by hours

Recorded Future AI answers your questions about threat patterns, implications, and intelligence sources

Contact us to schedule a discussion on how you can get ahead of the NIS2 Directive and protect your business.