

# 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 Directive focuses on:

Implementation of robust security measures

Development of documented incident response plans

Prompt reporting of significant incidents to national authorities

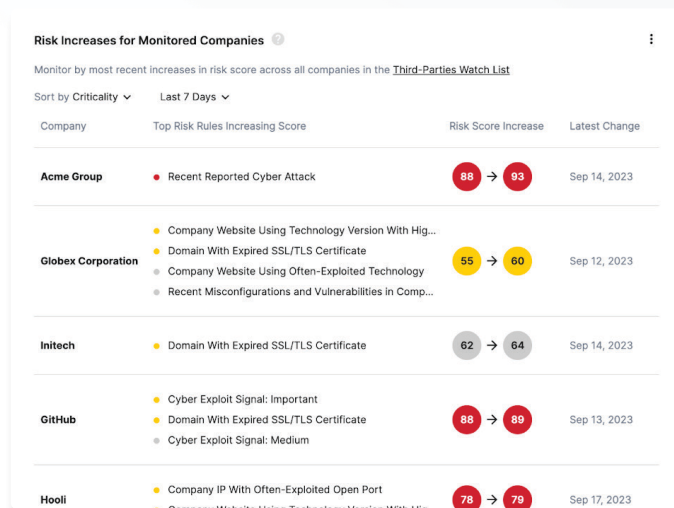
Foster cross-border cooperation

Given that NIS2 will impact even more sectors than previously and includes new recommendations and requirements, it's suggested that organizations start preparing for compliance.

## What's different in NIS2?

### Increased focus on supply chains and third-party risk

66% of organizations are not confident their vendors would notify them of a data breach<sup>1</sup> and 15% of breaches identified a supply chain compromise as the source of a data breach. It is not sufficient to just be aware of internal risks to mitigate attacks.



The screenshot displays a table titled "Risk Increases for Monitored Companies" with a subtitle "Monitor by most recent increases in risk score across all companies in the Third-Parties Watch List". The table has columns for "Company", "Top Risk Rules Increasing Score", "Risk Score Increase", and "Latest Change". It lists several companies with their respective risk score changes and the reasons for the increase.

Company	Top Risk Rules Increasing Score	Risk Score Increase	Latest Change
Acme Group	Recent Reported Cyber Attack	88 → 93	Sep 14, 2023
Globex Corporation	Company Website Using Technology Version With Hig... Domain With Expired SSL/TLS Certificate Company Website Using Often-Exploited Technology Recent Misconfigurations and Vulnerabilities in Comp...	55 → 60	Sep 12, 2023
Initech	Domain With Expired SSL/TLS Certificate	62 → 64	Sep 14, 2023
GitHub	Cyber Exploit Signal: Important Domain With Expired SSL/TLS Certificate Cyber Exploit Signal: Medium	88 → 89	Sep 13, 2023
Hooli	Company IP With Often-Exploited Open Port Company Website Using Often-Exploited Technology	78 → 79	Sep 17, 2023

- Gain a real-time view of the cyber risks organizations face.
- Identify emerging threats to your third parties with real-time alerts on security incidents, breaches, and a wide variety of risky security practices
- Protect your organization from emerging risk with access to Recorded Future's exclusive sources
- Enhance third-party assessment quality and speed with quantitative risk scores

<sup>1</sup> IBM Cost of a Data Breach 2023

## Incident Reporting

Under NIS2, organizations may be required to submit an early warning within 24 hours of any significant incident and a full notification report within 72 hours, which needs to include the assessment of the incident, severity and impact, and related IOCs.

The screenshot displays the Recorded Future interface for a malware analysis. At the top, the title "MALWARE" is visible. Below it, the specific malware is identified as "Gh0st RAT (Moudoor)".

**Notes:** 47 Insikt Group Notes. A link "Show recent events or cyber events" is provided.

**Malware Category:** Remote Access Trojan (RAT), Wiper Malware.

**References:** 100 000+.

**First Reference:** Mar 30, 2009.

**Latest Reference:** Oct 24, 2023.

**Curated:** ★.

**Recorded Future Community:** Malware ⓘ.

**Used in List:** RF - Hackers.

**Recorded Future AI Insights:** Generated based on 100 references | Aug 28, 2022 - Oct 2, 2023 | Analyst: Meghan McGowan.

**ANALYST NOTES FROM RECORDED FUTURE:** + Create Analyst Note.

**TECHNICAL LINKS:** 7 Days. Learn More ⓘ.

**Summary of technical links:** 2% of 5 635 total events between Oct 17, 2023 - Oct 24, 2023. Load More.

**Indicators & Detection Rules:**

Domain	Hash	IP Address
7003.aadaa1.cc ● 68	6bd98c534f856cc4450de4... ● 80	182.43.76.21 ● 77
luluge.e3.luyouxia.net ● 65	2db39121b9ff72da21002... ● 75	192.253.237.97 ● 76
yuankong12.e3.luyouxia... ● 26	312e995a1fb6ee2dd74bd... ● 75	103.142.8.158 ● 70
1 more	62+ more	24+ more

**URL:**

URL
tcp://107.163.43.161:1238... ● 25
tcp://149.210.60.137:443/ ● 25
tcp://211.23.219.226:443/ ● 25

**Malware Signature:**

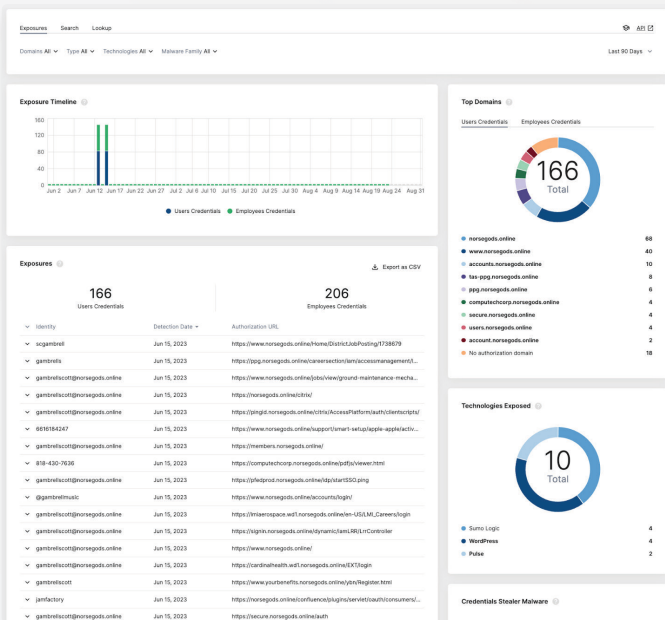
- Backdoor.Win32.Gh0st.CZ
- Backdoor.Win32.Gh0st.GC
- Backdoor.Win32.Inject
- 21+ more

**Actors, Tools & TTPs:**

MITRE ATT&CK Enterprise Identifier

- T1012 (Query Registry)
- T1018 (Remote System Di...)
- T1082 (System Informati...)
- 5 more

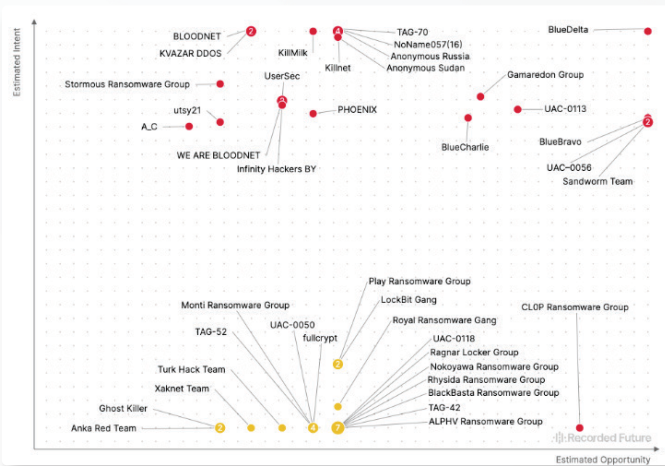
- Access valuable insights into potential incidents
- Equip users with essential information, updated in real time, on their threat landscape and accelerate research when potential incidents occur.



63% of confirmed data breaches involved weak, default, or stolen passwords. Recorded Future Identity Intelligence helps security and identity teams proactively prevent unauthorized access and takeover of accounts.

## Accountability of the management

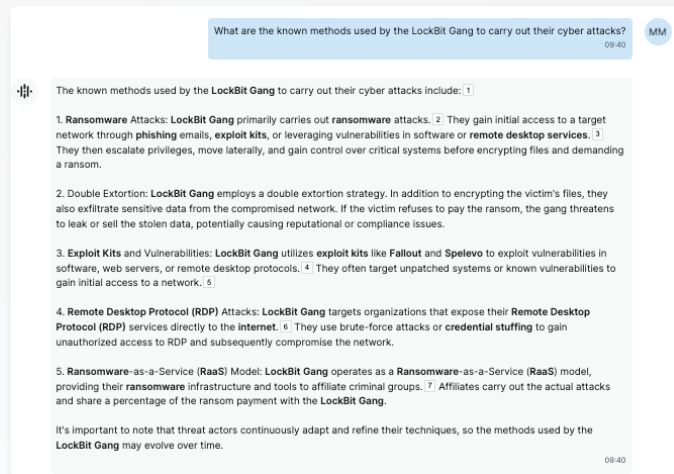
NIS2 outlines management's responsibility for the cybersecurity maturity of their organization. One way for management to take a more active role is by understanding the risk to your business through regular risk assessments.



- Recorded Future's Threat Maps provides automated analysis of threat actors targeting your enterprise. Visualize the most dangerous threats that have an opportunity to harm your organization
- Automatically track changes over time to better prioritize countermeasures

## Use of innovative technologies

The NIS2 Directive actively promotes the adoption of cutting-edge technologies, particularly artificial intelligence, within organizations. The Directive emphasizes the strategic utilization of innovative tools to enhance the identification and mitigation of cyber threats, while increasing efficiency and effectiveness of resources.



- Reduce time spent searching, summarizing, and writing reports by hours.
- Recorded Future AI answers your questions about threat patterns, implications, and intelligence sources
- Receive an AI Insights summary of your unique Threat Map, providing deeper visibility into threat intent and opportunities, along with recommended actions for faster response.

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

### ABOUT RECORDED FUTURE

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,700 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at [recordedfuture.com](https://recordedfuture.com)