sosafe

Breaking down the NIS2 Directive: What it means for your company

Discover how the NIS2 Directive aims to counteract increasingly sophisticated cyberthreats

NIS2

The Network and Information Security Directive is a piece of legislation that aims to set a common level of cyber security within Member States of the European Union. Its goal is to protect critical sectors by setting stricter cyber security standards, but it also focuses on rapid incident reporting and greater cooperation between EU members on cyber security.

Contents

What is NIS2?

The NIS2 Directive, the successor of the initial Network and Information Security Directive, serves as a pivotal piece of legislation designed to **bolster cyber security and safeguard critical infrastructure throughout the European Union** (EU). By addressing the shortcomings of its predecessor and broadening its reach, the NIS2 Directive amplifies security stipulations, strengthens reporting mandates, and enhances crisis management capabilities.

Understanding the necessity and relevance of the NIS2 Directive calls for a comprehensive grasp of our increasingly interconnected digital ecosystem. Europe's digital infrastructure, sprawling and complex, supports almost every facet of contemporary life and commerce. This interconnectedness offers exceptional opportunities for growth and efficiency but also opens the door to a multitude of potential cyber threats and vulnerabilities.

By shoring up the digital defenses initiated by the original 2016 NIS Directive and extending its protective cover, the NIS2 Directive represents a fortified stronghold in our cyber landscape. Introduced in 2022, **the new NIS2 Directive responds to the rise of increasingly sophisticated and damaging cyber threats**, establishing a solid, all-encompassing, and adaptable defense strategy.

Current situation of the European threat landscape – why NIS2?

Recently, the threat landscape has taken a dire turn as hackers continue to evolve and innovate. Technological advancements, especially AI tools, play a pivotal role by enabling cybercriminals to devise more sophisticated and seamlessly executed threats. Coupled with the growing professionalization of the cybercrime industry, it's now simpler than ever to launch attacks. This industry even provides platforms for cybercriminals that operate similarly to conventional SaaS offerings.

Adding another layer to this complex web are global tensions and national conflicts, which are increasingly manifesting in the digital space. State-sponsored hacking, cyber espionage, and cyber warfare are emerging as potent tools, complicating the threat landscape further. Additionally, the surge in remote work has inadivertently expanded opportunities for cybercriminals, who exploit vulnerabilities like unsecured personal devices and unreliable connections.

Our Human Risk Review 2023 confirmed these trends: **3 in 4 cybersecurity professionals believe their organization's cyber risk has heightened due to the intertwining of geopolitics, the rise of AI, and the shift to remote work.** Also, one out of every two organizations have fallen prey to a cyberattack. What's more alarming is that a third of these professionals anticipate another breach in the foreseeable future.

This surge in cyber threats particularly imperils essential and important industries. These sectors are attractive targets for cybercriminals, mainly because any service disruption they face demands immediate rectification. This urgency makes them susceptible to blackmail, with malicious actors seeking financial gain. To emphasize this vulnerability, Statista's 2022 data highlighted energy, education, healthcare, government, transportation, and media and telecom as being among the industries most frequently targeted by cyberattacks.

Recognizing the magnitude of this cyber onslaught, regulatory measures like the NIS2 Directive and DORA have been introduced. These legislative efforts act as beacons, guiding European organizations amid these turbulent waters. Their primary aim is to foster a coordinated response, ensuring that entities are better equipped to counteract the ever-evolving cyber threats.

What are the objectives of NIS2?

NIS2 goes a step further in the realm of digital resilience and threat management. Moving beyond just ramping up cyber security, it serves as a roadmap for uninterrupted business performance, enhancing collaborations, and nurturing a workforce well-versed in secure behaviors. Here's what NIS2 aspires to achieve:

Implement asset management practices to identify and protect critical information systems and assets.

Put into action supply chain security measures to review and guarantee the safety of third-party providers.

Report to relevant authorities and maintain incident response capabilities.

Provide training and heighten awareness among employees about optimal cyber security protocols.

Formulate and put into action cyber security strategies along with risk management protocols.

Ensure incidents are reported to the appropriate bodies and uphold the capability to respond to incidents.

Establish protocols for handling incidents, mandates for reporting, and response plans.

Eliminate inconsistencies and improve communication and cooperation between Member States.

Devise a strategy to **guarantee the consistent delivery of critical services** during cyber incidents.

From NIS to NIS2: What are the key changes?

The initial NIS Directive was introduced as a response to the increased digitalization that brought about new, more serious cyber security risks for both organizations and the broader public. These risks had to be addressed to protect critical services, sensitive information, and the well-being of individuals and economies. However, after its establishment in 2018, the implementation of the NIS Directive varied between Member States, leading to a fragmented system where organizations didn't or only partially implemented the requirements. One of the key reasons was that the definition of an essential service provider differed between States, highlighting the need for new, more detailed, and improved legislation.

Following the required revision of the NIS Directive, the European Commission defined a new NIS2 Directive that adapts to the current needs of the market and addresses the deficiencies of the previous one. More specifically, **the NIS2 has an expanded scope** of what is considered an essential service provider, a new crisis liaison organization, stricter reporting obligations for organizations, a focus on supply chain security, cyber hygiene requirements, introducing peer reviews for improved collaboration among Member States, and expanding on personal liabilities for management bodies. Continue reading to find out more about these changes.

NIS → NIS2

Additional entities and sectors

The purview of NIS2 extends to include additional entities, encompassing sectors like chemical production, medical device manufacturing, food processing, and social networking services, all of which fell outside the jurisdiction of its predecessor, NIS. Article 3 of NIS2 refines the classifications, supplanting the terms "operator of essential services" and "digital service provider" with "essential entities" and "important entities," determined by their scale and sector. Although these classifications share similar obligations, essential entities will be subjected to more stringent regulatory scrutiny and enforcement actions. You can find the full list of entities in the scope of NIS2 further below.

European Cyber Crisis Liaison Organisation Network (EU-CyCLONe)

According to Article 16, the Commission will form an EU-CyCLONe organization made up of representatives from EU countries in charge of managing cyber crises and, if needed, representatives from the European Commission. This organization's main goal is to coordinate how different countries deal with major cyber security issues through the following:

- Ensuring countries are well-prepared to handle big cyber security incidents and crises.
- Developing a shared understanding of what's happening during these incidents and crises.
- Assessing the impact of these incidents and suggesting ways to make things better.
- Coordinating how countries manage these incidents and help political leaders make decisions about them.
- Talking about and helping with each country's response plans for cyber security incidents.

The NIS2 Directive also establishes a Cooperation Group to facilitate the seamless exchange of information and cooperation between Member States. EU-CyCLONe will regularly report to the Cooperation Group about the big cyber security incidents and trends, especially the ones affecting essential organizations and services. By July 17, 2024, and every 18 months after that, the organization will submit a report to the European Parliament and the Council, explaining their recent activities.

Supply chain security

Article 22 of NIS2 requires organizations to address security in their respective supply chain, including **risks created by supplier relationships**. This is crucial because many cyberattacks happen due to vulnerabilities in third-party suppliers, so organizations have to evaluate the quality and resilience of the products and services they are using to ensure they won't be a weakness for essential service providers. It's also important for organizations to evaluate how their third-party suppliers handle cyber security and if their current measures are robust enough to protect the entire supply chain.

Entities that provide important services to Member States – such as DNS service, a TLD name registry, domain name registration, cloud computing, data center, content delivery network, managed service, managed security, or provider of an online marketplace, search engine, or social networking – but reside outside of the Union need to appoint a representative inside Europe. The representative will be responsible for the organization's NIS2 compliance obligations and reporting security incidents.

To ensure a common level of cyber security with all suppliers and reduce the chances of cyber incidents, essential service providers must include the required measures in the contracts with third-party suppliers.

Stricter reporting

To ensure a swift response, Article 23 of NIS2 requires affected organizations to send an early notification to the Computer Security Incident Response Team (CSIRT) or a national competent authority, where applicable, within 24 hours of experiencing a significant cyber incident, which is one that causes severe disruption of processes or financial loss to the organization or causes considerable material or non-material damage to another person. If needed, organizations can also seek assistance for implementing possible mitigation measures. The authorities will respond to the notification, offer guidance on how to handle the incident, and inform other affected countries if necessary.

Within 72 hours of becoming aware of the incident, the affected organization should provide details about the incident and an initial assessment of the significant incident. Finally, within a month after the submission of the incident notification, the affected organization should provide a report with a detailed description of the incident's severity, impact, and root cause and the applied mitigation measures by the organization.

Cyber hygiene

With cyber threats becoming more complex and sophisticated, it's crucial for organizations to maintain a basic level of cyber hygiene practices. As the foundation for protecting essential infrastructures, organizations should implement a common baseline of safety practices, including regular software and hardware updates, periodic password changes, management of new installs, limitations of administrator-level access accounts, and the backing-up of data.

Furthermore, as many attacks happen through connected devices, employee training and user awareness of common cyber threats are crucial for creating a proactive framework of preparedness, enhancing the overall safety and security of essential service providers in the EU.

Peer reviews

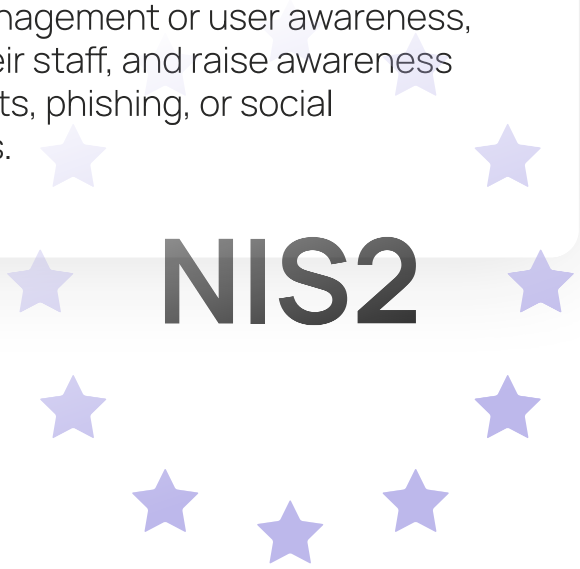
As regulated in Article 19 of the NIS2 Directive, the Cooperation Group will create a system of voluntary peer reviews so that Member States can learn from shared experiences and improve cyber security. The reviews will cover topics like how well countries implement cyber security risk-management measures and reporting obligations, the capabilities of their competent authorities, and the level of mutual assistance and information sharing.

The peer reviews may be on-site or virtual, following a pre-set code of conduct and with full cooperation between the parties. Once the review is completed, the cyber security experts will create a draft report with findings and recommendations to improve cyber security. These reports will be submitted to the Cooperation Group and the relevant cyber security network and can be made public if the reviewed organization chooses.

Personal liabilities for the management bodies

Member States should define the fines and penalties for organizations that fail to implement the required measures defined in NIS2. They have until 2025 to inform the Commission of those rules and measures. Aside from the organizations, Article 20 of NIS2 also mandates personal liability for management bodies like company boards and executives of organizations to enforce cyber security requirements. Any failure to comply can result in various enforcement orders and substantial fines for non-compliance.

> **Introduction (89)** Essential and important entities should adopt a wide range of basic cyber hygiene practices, such as zero-trust principles, software updates, device configuration, network segmentation, identity and access management or user awareness, organize training for their staff, and raise awareness concerning cyber threats, phishing, or social engineering techniques.



Which entities come under NIS2?

As stated before, the current NIS2 applies to more organizations than its previous version NIS. In general terms, the focus falls primarily on enterprises that provide essential and important services, specifically those with a minimum of 50 employees or generate an annual revenue of €10 million.

To address the issue of divergences between Member States about what qualifies as operators of essential and important services and ensure uniformity, **NIS2 divides organizations in scope into two groups: essential entities and important entities.** It also expands the scope of NIS by including, among other sectors, manufacturers of certain products and digital services.

With the new changes, NIS2 sets the threshold for **essential entities** at organizations with at least 250 employees, €50 million annual turnover, and €43 million balance that work in energy, transport, banking, finance markets, health, drinking water, wastewater, digital infrastructure, ICT service management, public administration, and space. **Important entities** are those with fewer than 250 employees, whose annual turnover is more than €10 but not exceeding €50 million, and an annual balance not exceeding €43 million, and operate in postal and courier services, waste management, chemicals, food, manufacturing, digital providers, and research organizations.

Please note that an entity that exceeds the ceiling for the important sector but does not qualify as an essential entity is required to comply with this law as an important enterprise.

The same cyber security measures and reporting requirements apply to both essential and important entities. However, the two categories are subject to different supervisory and penalty regimes. Essential entities are subject to supervision upon implementation, while important entities will be investigated only if evidence of non-compliance is received.

Even if an organization doesn't meet the criteria for essential or important entities, it can still choose to comply with NIS2 to improve its cyber security system. To register, entities will need to provide their name, address, and registration number, which sector they fall under in NIS2, their State, contact details, and a list of assigned IP addresses.

Essential sector	Important sector
Threshold ≥ 250 employees › €50 million turnover › €43 million balance	Threshold 50 – 249 employees €10 - €50 million turnover €10 - €43 million balance
Energy	Postal and courier services
Transport	Waste management
Banking	Chemicals
Financial markets	Food
Health	Manufacturing
Drinking water	Digital providers
Wastewater	Research organizations
Digital infrastructure	
ICT service management	
Public administration	
Space	

DORA and NIS2: A comparative overview

To address the growing challenges of cyberattacks and safeguard Europe's essential systems and digital infrastructure, the European Commission has recently rolled out two key legislative measures: the NIS2 – discussed in this article – and the Digital Operational Resilience Act (DORA). Both share similar timelines: DORA was initially proposed in 2020 and finalized in 2023, and NIS2 was introduced and published in 2022 and came into effect in January 2023.

Both regulations aim to improve the cyber resilience of organizations in Europe, but they target different sectors. NIS2 expands on the previous NIS Directive and aims to standardize cyber security and governance for operators of essential and important services like transport, telecoms, water and waste management, data centers, banking, public administration, research organizations, postal and courier services, and others. On the other hand, **DORA is a new regulation designed to improve the integrity of digital systems in financial entities** across Europe and harmonize how organizations detect, handle, and report ICT-related risks.

Despite their different scope, both NIS2 and DORA have a common goal to unify the cyber security efforts of organizations across Europe, protect information integrity, and mitigate the ever-growing risk of breaches.

Timeline for meeting NIS2 requirements

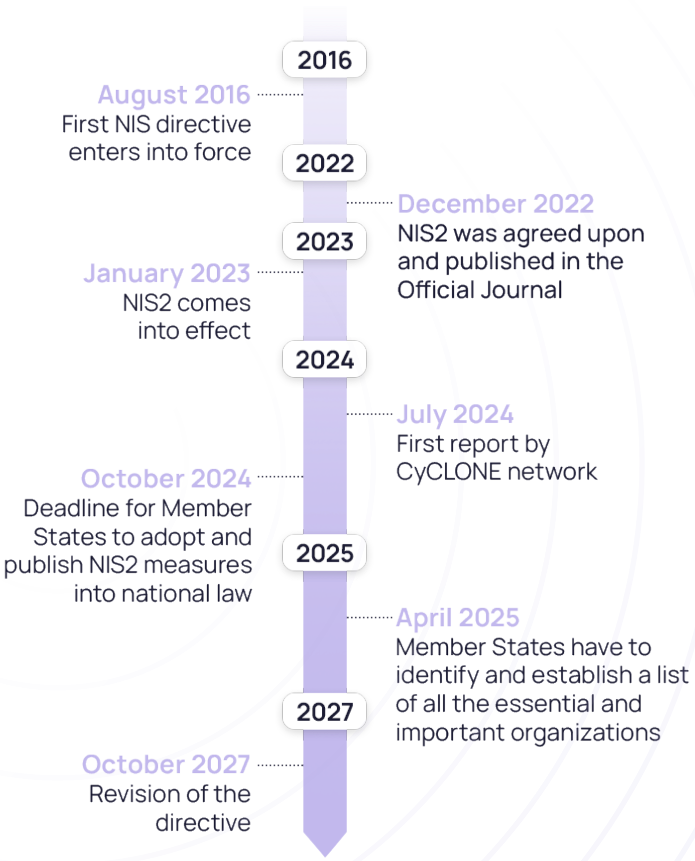
In July 2016, The European Parliament and the Council of the European Union adopted the NIS Directive to increase the overall level of cyber security within the EU and improve the resilience of critical infrastructure. It entered into force in August 2016, with a 21-month period for Member States to transpose it into national law – by May 2018. By this date, essential service and digital service providers had to be fully compliant with the cyber security regulations and reporting obligations laid out in NIS.

However, with the growing digitalization and repeated cyberattacks, it became evident by 2020 that there was a need for more robust legislation that would protect the systems and information of critical service providers and expand the scope to some important sectors. In December 2020, the European Commission proposed an updated version of the NIS Directive, called the NIS2 Directive, to address these challenges. After a one-year revision and negotiation, the NIS2 Directive was agreed upon in 2022 and published in the Official Journal on December 27, 2022.

NIS2 officially went into effect on January 16, 2023. Member States have until October 17, 2024 to adopt and publish the NIS2 measures into national law to ensure compliance. Failure to comply with NIS2 by the set deadline can result in various fines and fees, both on a personal level and for the organization as a whole.

On July 17, 2024, and every 18 months thereafter, the EU-CyCLONE network should submit a report assessing its work. The CSIRT network should also provide a report by January 17, 2025 that will assess the progress Member States have made relating to operational cooperation and draw up conclusions and recommendations on peer reviews – efforts to mutual experience sharing, learning, and help with compliance. By April 17, 2025, Member States must identify and establish a list of all the essential and important organizations within the scope of NIS2.

The current NIS2 is set for revision in October 2027, three years after its adoption.


2016
August 2016
First NIS directive enters into force
2022
December 2022
NIS2 was agreed upon and published in the Official Journal
2023
January 2023
NIS2 comes into effect
2024
July 2024
First report by CyCLONE network
October 2024
Deadline for Member States to adopt and publish NIS2 measures into national law
2025
April 2025
Member States have to identify and establish a list of all the essential and important organizations
2027
October 2027
Revision of the directive

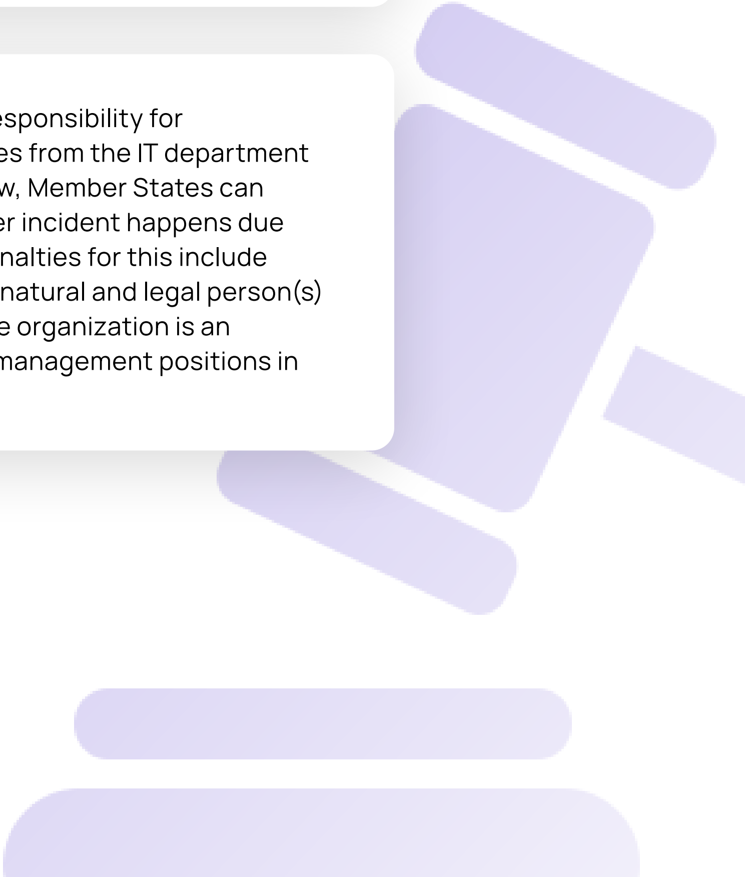
Understanding the consequences of non-compliance

The NIS2 Directive establishes a foundational set of sanctions for breaches related to cyber security risk management and reporting duties. These penalties for organizations not adhering to the stipulated deadlines come in various forms, including non-monetary remedies, administrative fines, and criminal sanctions. However, the exact fines vary, taking into account the organization and the difference between their intended and actual implementation.

National supervisory authorities can impose **non-monetary** remedies, including compliance orders, binding instructions, security audit implementation orders, and threat notification orders to entities' customers.

Administrative fines are distinguished between essential and important entities within NIS2. The new regulation requires national authorities to impose maximum fine of at least €10,000,000 or 2% of the global annual revenue to essential entities, whichever is higher. Important entities can be subject to a maximum fine of at least €7,000,000 or 1.4% of the global annual revenue, whichever is higher.

Moving away from its predecessor, NIS2 shifts the responsibility for implementing and upholding cyber security measures from the IT department and **now includes top management personnel.** Now, Member States can also hold C-level managers personally liable if a cyber incident happens due to gross negligence of the company. Some of the penalties for this include making compliance violations public, publishing the natural and legal person(s) responsible for the violation and its nature, and if the organization is an essential entity, banning an individual from holding management positions in case of repeated violations.



Next steps: How to become NIS2-compliant

While there is a lengthy 24-month timeline to implement NIS2 fully, timely preparation is key to becoming fully compliant. Planning out a strategy, coordinating with third-party suppliers, and budget forecasting takes time, so it's a smart move for organizations to take some early steps to have a timely, stress-free implementation process.

During the implementation period, entities can follow these steps to reach compliance:

1

Meet with management and stakeholders to discuss the implementation strategy and assess how NIS2 will impact everyday work.

2

Ensure all board members, managers, the IT team, and employees conducting the essential services understand the NIS2 requirements.

3

Identify critical elements and processes that provide essential services and conduct a gap analysis to reveal the areas where cyber security measures fall short of NIS2 requirements.

4

Identify third-party suppliers that provide essential services and their potential vulnerabilities.

5

Construct a cyber security awareness plan involving all levels in the organization to ensure both employees and board members are on track with current and upcoming work changes, reporting expectations, and other cyber security topics.

6

Find compliance partners that can provide support or guidance to become compliant.

7

Allocate the necessary budget to implement the requirements of NIS2.

8

When all NIS2 measures are implemented, perform a second gap analysis to ensure you have achieved full compliance.

How SoSafe can help with NIS2 compliance

NIS2 is designed to expand and improve the previous NIS Directive so that providers of essential and important services can meet the ever-growing threat of cyberattacks. To do this, organizations must take a holistic approach that considers risk management requirements, reporting obligations, and response plans defined in NIS2.

Effective risk management lies at the core of NIS2, with Articles 7, 9, 20, and 21 highlighting the importance of training both management bodies and employees to give them sufficient knowledge and skills to identify risks and assess cyber security risk-management practices.

To aid with this, SoSafe's gamified awareness training includes a variety of learning modules that cover a range of threats and best security practices, enabling your employees to recognize threats and effectively battle them. With content available in over 30 languages, our platform covers diverse linguistic backgrounds and complies with native language training requirements in various countries. Besides, SoSafe's Content Management Solution provides a consolidated unit where employees can access all training modules and security policies at once – including your own -, boosting employee engagement and aiding compliance. But awareness training goes beyond training modules: It needs to be integrated in daily life and communications. Our chatbot, Sofie, can be integrated into Microsoft Teams, allowing you to instantly connect with your employees to address urgent alerts and send training nudges within minutes.

Article 11 of NIS2 requires the CSIRTs to provide dynamic risk and incident analysis and situational awareness regarding cyber security. By putting the human factor at the center of our analysis and metrics, SoSafe's ISO 27001-compliant Risk and Reporting Cockpit Tool focuses on systematic analysis with the human factor in mind and allows you to track the progress of awareness programs and access detailed analyses, metrics, and KPIs regarding human risk within your organization. Furthermore, to ensure timely incident reporting, our Reporting Button, Phish Assist, empowers employees to report security incidents swiftly, expediting early threat detection and reporting.

Aligning with NIS2 and having the proper resources and training in place will not only ensure compliance but will also significantly **strengthen your company's defenses** against cyber threats, preventing business disruptions and contributing to the success of your business.

Scale your security culture with ease

With its awareness platform, SoSafe empowers organizations to strengthen their security culture and mitigate human risk. The platform delivers engaging learning experiences and smart attack simulations that help employees become active defenders against online threats – all powered by behavioral science to make the learning journey fun and effective. Comprehensive analytics measure the behavioral change impact and tell organizations exactly where vulnerabilities lie so that they can proactively respond to cyberthreats. The SoSafe platform is easy to deploy and scale, effortlessly fostering secure habits in every employee.

TEACH — Engaging Micro-Learning

A behavioral science-based learning platform employees love. Strengthen your resilience to cyberthreats and fulfill compliance obligations with dynamic and impactful learning experiences across channels to easily build long-lasting, secure habits.

- → Story-driven, gamified learning content designed to engage and stick
- → Curated and guided content library readily scalable for growth
- → Low-effort customization and content management to fit every organization

TRANSFER — Smart Attack Simulations

User-centric phishing simulations that foster secure habits. Train your employees on how to recognize cyberattacks with our regular automated spear phishing simulations that create lasting security awareness in their everyday work – to effectively reduce risk and crucial threat detection time.

- → Personalized and realistic cyberattack simulations
- → Context-based learning walkthroughs to reinforce secure employee behavior
- → Easy reporting of threats with a one-click Phishing Report Button

ACT — Strategic Risk Monitoring

Protect your organization from costly incidents by using our comprehensive human risk assessment solution. Receive a complete overview of your human layer security so that you can stay ahead of potential vulnerabilities. Monitor and interpret the impact of your awareness programs, analyze behavior, and make informed data-driven decisions.

- → Contextual insights, including technical and behavioral KPIs
- → Industry benchmarking and actionable guidelines
- → Built for ISO/IEC-27001 requirements, and on a privacy-by-design approach

CONNECT — Sofie Rapid Awareness

Cyber criminals are moving faster than ever, but so can you. Rapid Awareness enables you to rapidly connect with your employees in MS Teams. Enable rapid micro-learning to address emerging threats, empower your team with instant alerts, and transform them into your strongest defense.

- → Connect directly with your staff in MS Teams
- → Save time and communicate with ease
- → Send bite-sized security alerts that employees can easily digest
- → Track and monitor the number of employees who read the alert

sosafe

SoSafe GmbH
Lichtstrasse 25a
50825 Cologne, Germany

info@sosafe.de
www.sosafe-awareness.com
+49 221 65083800