Transforming NIS2 Challenges into Strategic Opportunities

A Cisco Perspective

Preface

This report provides guidance on secure digitalisation under the new NIS2 Directive for decision-makers. It covers:

1. EU's digitalisation potential and value
2. Risks to Member States, sectors, and organisations
3. NIS2 Directive's impact on the European market, development, and competitiveness

The report emphasises the complexity of building holistic resilience in Europe, discussing digital maturity, external cyber threats, and the collective maturity of organisations. It concludes with a practical guide for implementing the NIS2 Directive, offering examples of activities and capabilities to achieve and maintain compliance.

Developed collaboratively by Cisco and Radar Group, the report analyses European-specific and open data, drawing on extensive expertise in the IT landscape.

Executive summary

As the European Union's digital landscape undergoes pivotal changes, the introduction of the NIS2 Directive is a testament to the EU's commitment to fortifying its digital infrastructure and competitive position in the global market. This report aims to mitigate the intricacy and increased complexity, as well as the substantial effort required for successful implementation of NIS2. NIS2 concerns Member States, as well as countries dependent on the European market.

The background and purpose of the NIS2 Directive is to secure digital development within the Union, which is estimated to be worth around EUR 3 trillion (approx. 20 percent of the EU's total GDP). Digitalisation has enormous potential and a significant impact on organisations' competitiveness and welfare. Increased resilience and robustness are prerequisites for ensuring digital transformation as more sophisticated threat actors emerge and attack surfaces are constantly increasing.

The Essence Of The NIS2 Directive

- Extending the scope
- Imposition of sanctions
- Increased security requirements
- Increased demands on management
- Supply chain security
- Increased collaboration and information sharing

An estimated 350,000 organisations across the EU will be affected by the NIS2 Directive

Impact on organisations

The NIS2 Directive is extending the scope to a broader array of sectors and operations and includes an elevated degree of accountability for the supply chain. Organisations, especially those engaging with NIS for the first time, will need to invest significant resources in understanding their responsibilities and ensuring compliance.

Navigating complexity

The global security situation is expected to continue to deteriorate in 2024, with authorities and the public sector exposed to the most cyber attacks – everything from state-sponsored hacktivists and groups to criminals. This impacts both trust and confidence, and can result in actual infrastructural and monetary damage implementation of the NIS2 Directive. The European Commission estimates that businesses that previously managed NIS1 may see an approximate cost increase of 12 percent, while those not covered by NIS1 may see an increase of approximately 22 percent after implementationof the NIS2 directive.

The cost of security

Cybersecurity has profound economic implications. As threats escalate, so do associated costs, with some incidents incurring expenditures exceeding EUR 500,000. Raising the level of cybersecurity maturity across the union will require significant investments and increased budgets. The European Commission estimates that a business that previously complied with NIS can expect an approximate increase in the ICT budget of 12 percent, while those who are not may see an increase of about 22 percent for NIS2.

Most sectors are facing increased threats

It is imperative to note that no sector is immune in today's interconnected digital economy, and the inherent risks require a comprehensive cybersecurity approach. Some of the sectors facing amplified risks include:

- The manufacturing industry's capacity for large-scale disruptions makes it an alluring target for cyber threats. Vulnerabilities stemming from legacy systems and highly critical OT environments require particular attention.
- The healthcare sector is facing increased threats that not only risk inflicting economic damage and jeopardising sensitive data and patient safety, but also severe reputational damage.
- Energy and critical infrastructure are undergoing rapid transformation propelled by digital and sustainable innovations. The sector has a pivotal role in Europe and a complex supply chain demanding proactive and robust cybersecurity measures.

A Vision for the Future

The NIS2 Directive is not just regulatory – it is visionary. It sketches a blueprint for a harmonised and secure digital future in the EU. By viewing it as a strategic tool, organisations can pave the way for a future where security and innovation are cornerstones.

Guidance is indispensable for organisations charting their path in this new NIS2 era. It's not just about navigating regulatory waters, but about steering towards a secure, innovative, and prosperous digital future in the European Union.

Table of contents

1. EU strengthens the single market through regulations

Compared to the rest of the world, it is evident that the EU has a stronger focus on regulation with the aim of strengthening the single market14. Regulatory requirements are seen as a proactive enabler for strengthened competitiveness, economic growth, and effective cooperation between Member States, as well as with other global operators offering their services in the single European market9. The foundations of the current legislative landscape began to be laid by the EU several years ago and include several general and specific regulatory frameworks. In 2020, the EU launched a new cybersecurity strategy that aims to increase Europe's resilience to cyber threats, protect vital societal functions, and ensure that everyone can benefit from trustworthy digital tools and services9. The new EU regulatory framework NIS2 is among the first at multilateral level to affect not only EU Member States, but also other countries dependent on the European market.

With increased digitalisation comes increased cyber threats that disregard borders, which means that it becomes important for countries to cooperate and develop common standards for cybersecurity. It is evident that businesses and society have not been able to increase their cybersecurity capabilities to meet new threats with the same speed and scope as digitalisation, and the introduction of the NIS2 Directive is a political response to this development14. The digitalised society is constituted by a closely interconnected infrastructure on which all Member States depend4. A chain is only as strong as its weakest link, and it is this reasoning that form the basis of the broad regulatory requirements now being introduced. It is important that socially critical operations jointly increase their computer and network defence capability, not only to protect their own operations, but to contribute to strengthening the entire chain and thus Europe's resilience.

1.1 The value of digitalisation

The total theoretical potential of secure digitalisation in Europe, in both the private and public sectors, is estimated at approximately EUR 3 trillion from 2025 onwards11,19. This corresponds to about 20 percent of Europe's total Gross Domestic Product (GDP) and can be compared to the value of Europe's largest economy Germany (with a GDP equivalent to approx. EUR 3.6 trillion) and the second largest economy France (with a GDP equivalent to approx. EUR 2.6 trillion). This huge digital potential means that the future prosperity of the EU depends on successful, secure, and robust digital transformation within the Union. The potential of digitalisation is so vast and transformative that Europe needs to focus on it to ensure its continued competitiveness, prosperity, and a better and more robust Union. This is largely the reason for the growing importance of the regulatory landscape and the purpose of the upcoming NIS2 Directive.

Continuous digitalisation has also proven to be an important tool for strengthening resilience and flexibility of the Member States during crisis. It is estimated that the global pandemic accelerated the pace of digitalisation by 3–4 years and, since then, it has continued to increase17. Operators that have historically focused on digitalisation during crises fared better or even emerged stronger from the crises by using digitalisation as a tool for increased resilience and flexibility. The businesses that were most successful had the ability to maintain their digital initiatives or start new ones during the crises.

Performance of digitally leading companies in comparison to the industry average[17]

x1.9	x1.5
Increased growth after 10 years (factor)	Increased profitability after 3 years (factor)

2. The Accelerating Threat

The potential of digitalisation is enormous, but neglected or poorly implemented digitalisation can result in significant value losses. Cybersecurity has thus become a critical issue for both businesses and entire nations to ensure competitiveness and protect valuable assets and rights. Increased threat levels result in higher costs and increasingly burdensome consequences for businesses. When analysing the most recent major incident, 40 percent of respondents stated that the cost for their operations exceeded EUR 250,000. According to the EU's security agency, ENISA, the median cost of an IT incident in the EU reached EUR 200,000 in 2022, – doubling within just a year[5].

Industry leaders are confirming this, with four out of five believing that cybersecurity incidents and related costs are likely to disrupt their business over the next 12 to 24 months[2].

The costs of cyberattacks and incidents are increasing, but the potential indirect cost of uncertain digitalisation, which can undermine trust in public and business services, is even greater7. A lack of digitalisation in the EU could lead to an estimated annual GDP loss of EUR 200 billion[20]. It is therefore crucial to manage cybersecurity effectively to avoid these risks that adversely affect society, our GDP, and our welfare through, for example loss of efficiency, tax revenue losses, distrust and loss of competitiveness.

Top 5 emerging cybersecurity threats for 2023[6]

Emerging threats	Possible threat actors	Probable impacts
Supply chain compromise of software dependencies	State-sponsored groups, criminal organisations	Disruption, Malfunction, Data Loss, Data Leakage
Advanced disinformation campaigns	State-sponsored groups, criminal organisations, hacktivists	Distrust, disinformation, financial damage
Rise of digital surveillance authoritarianism	State-sponsored groups, criminal organisations	Privacy breaches, human rights abuses
Human error and exploited legacy systems within cyber-physical ecosystems	State-sponsored groups, cyber criminals, hacktivists	Malfunction, Failures and Outages, Physical Damage
Targeted attacks enhanced by smart device data	Cybercrime actors, hackers-for-hire	Financial Damage, Privacy Breaches

2.1 The New Threat Landscape

The geopolitical situation is affecting global developments and has a clear impact on the entire European IT ecosystem. In 2024, the uncertain global situation is expected to continue, with one of the major issues being the increased tensions between major powers as well as changing alliances[21]. Trade wars, the quest for technological dominance, and territorial claims will continue to affect the international arena. Digital technologies are at the centre of these geopolitical tensions, where speed and scale play a significant role in winning and maintaining leadership positions in the future global economy.

Cyberattacks are growing rapidly under the current circumstances and are becoming increasingly complex and costly to protect against[7]. In addition, cyber threat actors' capabilities and interest in attacks on digital supply chains have increased, which has major effects throughout the IT ecosystem. Digital acceleration creates new challenges and threats that businesses need to protect themselves against through systematic security work and robust security intelligence. Below are some of the biggest threats to businesses and society in the coming years, according to the EU's cybersecurity agency ENISA[6].

2.2 Potential Exposure of EU member states based on digital maturity

Taking advantage of the opportunities offered by digital technology requires knowledge and structure. Digital maturity is therefore important for understanding how well a country has managed the adoption of digital technology and how well-positioned it is for realising the potential value offered by digitalisation. In addition, digital maturity can provide a basis for understanding how digital threats differ between Member States and their ability to counteract them.

The adoption of advanced digital technologies shows significant variation among EU countries. Radar's Digital Maturity Index is a combination of the Digital Economy and Society Index (DESI)[10], the Digital Intensity level in Businesses, and Radar's own security maturity index, which specifies EU Member States' progress on their digital performance and development. Highest maturity is found in the Nordic countries and Ireland, followed by the Netherlands. While there are impressive digital success stories in Europe, numerous countries still lag in the widespread adoption of digital infrastructure and technology, particularly in the uptake of emerging digital technologies such as AI and IoT[11]. The adoption of advanced technologies in many Member States is also uneven, with large organisations showing the highest level of digital intensity over small and medium-sized enterprises (SMEs)[11].

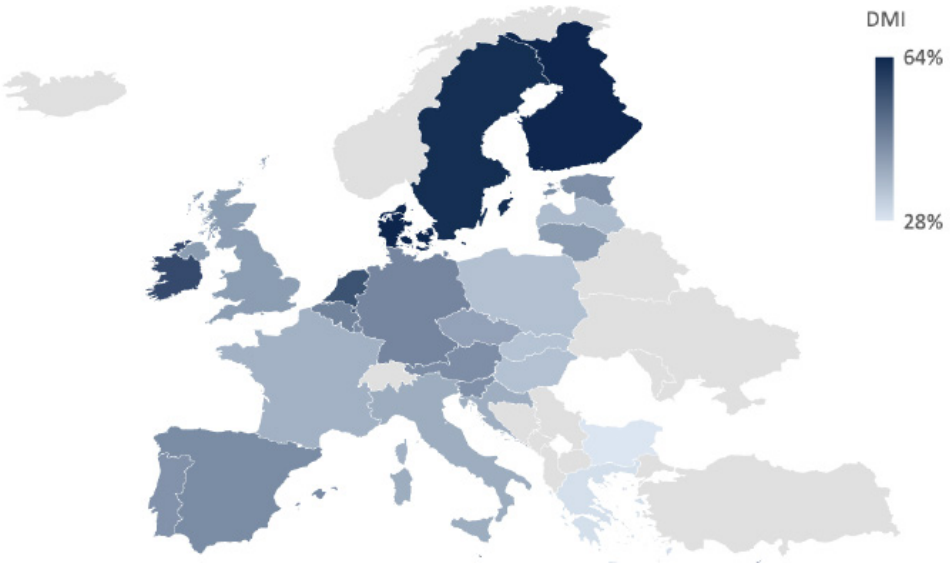


Figure 1. Digital maturity Index

2.3 Most targeted EU member states based on monitored attacks

Cyberattacks continue to increase, and the graphical representation shows the incidence of cyber attacks within the European market, spotlighting the United Kingdom, Germany, France, and Italy as the nations most severely afflicted. Notably, a correlation exists between the frequency of cyber attacks and the respective countries' GDP. Consequently, while Germany experiences a high volume of cyber attacks, when considered in proportion to its GDP, these incidents are essentially equal per economic activity level to those observed elsewhere in Europe. This observation underscores the cyber actors strategic preference for targeting regions with the highest potential for economic and political gain.

Interestingly, the most digitally developed countries are not always the ones with the highest resilience or the most advanced cybersecurity evfforts. According to Cisco's Cybersecurity Readiness Index, less developed nations like Indonesia, the Philippines, Thailand, and Brazil exhibit organisations with a higher degree of cybersecurity preparedness in comparison to more mature markets. This is partly due to these emerging economies starting their digital transformation more recently, allowing them to build digital enterprises from scratch without the burden of legacy systems. This clean slate approach enables them to integrate the latest cybersecurity technologies, frameworks, and architectures in an agile and incremental manner, adapting efficiently to the evolving cyber threat landscape.

The cybersecurity readiness levels of organisations in Europe indicates that nearly all countries lag behind the global cybersecurity readiness average. A mere ten percent of European companies can be categorised as adequately mature to effectively address the current cybersecurity challenges2. That means that we have a situation within the EU where 9 organisations out of 10 still are not on a sufficient maturity level to meet the threat levels of today. This, if nothing else, should be an immediate call for action and indicates the EU's reasoning behind the introduction of a strengthened NIS Directive. The more digitally mature organisations and society become, the more important the resilience and maintenance of the technology stack and organisation skillset will be.

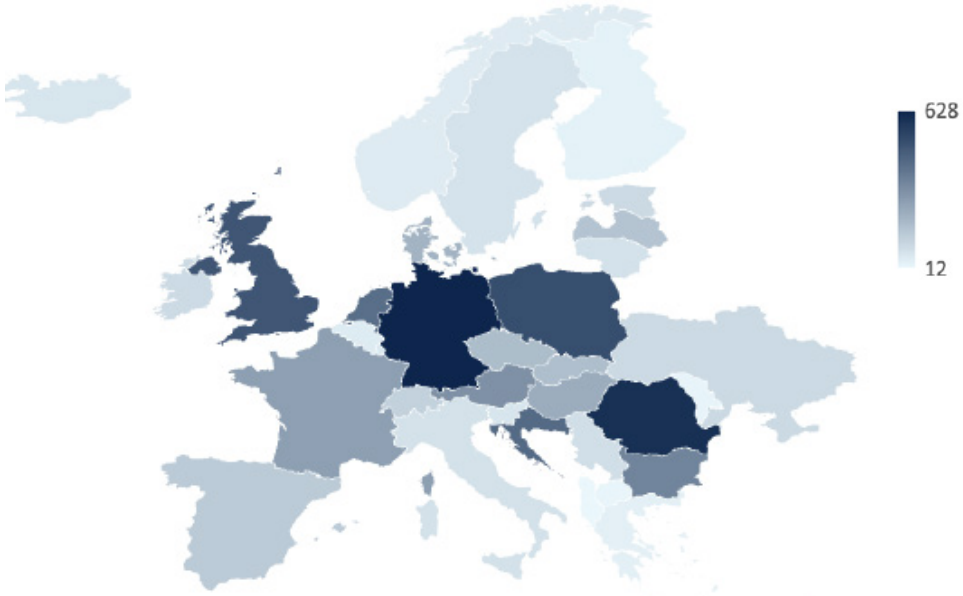


Figure 2. Cyber attacks per day in 2023, average, thousands[22] (2023).

Cyberattacks 2023 in millitons[23]

2.4 Most targeted sectors and organisations

When examining individual sectors prone to cybersecurity incidents, the public administration and government sector appears as the most significantly impacted, closely followed by digital service providers and the general public[7]. Notably, these sectors facing the highest frequency of cyber attacks are also those obligated to adhere to the NIS2 legislation. These statistics underscore the critical need to elevate cybersecurity measures, emphasising the imperative to encompass public administration and digital service providers within the scope of the revised directive[12]. This alignment highlights the urgency of integrating these key sectors into comprehensive cybersecurity strategies, ensuring their resilience against evolving cyber threats, and regulatory compliance with NIS2 legislation.

2.5 Industrial Systems Further Adding Complexity

It is crucial to recognise that all sectors are increasingly at risk in today's complex economic and geopolitical landscape. While we often focus on IT for cybersecurity, the often-forgotten OT (Operational Technology) that deals with control of physical processes and machinery within industrial operations in control systems, industrial networks are crucial for our digital resilience. OT systems have historically operated autonomously and often lack the security protocols that we take for granted in IT. By converging the IT and OT-environments organisations can yield benefits such as automated processes and real-time visibility into operations. However, as OT-systems become integrated with business networks and the Internet it imposes greater risks on OT as well as IT, since cyber attacks might move laterally between the OT and IT-environments.

Attacks against OT-environments are on the rise, and organisations must be aware of, and manage this risk as a part of a holistic cybersecurity strategy. Securing both legacy and OT environments can present challenges, necessitating specific skill sets and potentially leading to a siloed approach in managing cybersecurity for IT/OT-environments.

A potential ICS (Industrial Control System) attack targeting for example a manufacturer can inflict serious damage for the manufacturer or company in charge of the OT-system, as well as cause widespread damage for the economy, infrastructure, and public safety. Consequences of ICS attacks include, but are not limited to the following:

- Disruption of production
- Damage of equipment
- Safety risks
- Disruptions of the supply chain
- Can cause reputational damage
- Widespread economic problems, even nation-wide
- Fines and penalties for the organisation, by regulatory bodies

Addressing weaknesses or flaws in industrial control systems is essential to be one step ahead of hackers, state sponsored criminal organisations, or hacktivists. Identifying possible vulnerabilities is crucial to avoid unauthorised access, exploits or other situations that can compromise confidentiality, integrity, or availability. To keep ICS secure and reliable, and to stay ahead of emerging threats in the ICS landscape, it is essential to ensure that a combination of technical measures and best practices are used.

2.6 Deep dive into selected industries

All industries are subject to increased threats and need greater robustness and a higher level of cybersecurity. However, organisations in different sectors may struggle with different challenges and vulnerabilities due to specific preconditions, the nature of their business, or their level of digital and technical maturity. In this report, we take a closer look at three different industries: the manufacturing, healthcare, and energy and critical infrastructure sectors.

2.6.1 Manufacturing

The European manufacturing sector is large and represents 15 percent of the EU's total GDP. The German manufacturing sector is the largest based on economical metrics. However, in terms of the number of manufacturing organisations, Spain has the most followed by Italy. In the Cisco Cybersecurity Readiness Index Report, manufacturing is ranked in the top three of the most mature sectors together with Technical Services and Financial Services[2].

Europe's manufacturing sector comprises predominately small and medium-sized businesses, which is the group reporting the lowest cybersecurity maturity readiness in the Cisco index[2]. Even if the NIS2 Directive by design filters out small businesses as a direct target group obligated to comply with the directive, the manufacturing sector will still see a high degree of small businesses voluntarily adopting the principles of NIS2 to become qualified to deliver to larger manufacturing organisations in the scope of the directive, since they are often a part of an integrated supply chain.

Digitalisation in the manufacturing sector is in full swing with a high focus on implementing advanced technologies in their production facilities and operations, commonly referred to as Industry 4.0. The digital transformation addresses both the digitalisation of customer relations, internal processes, new digital relations with vendors and the transformation of physical products into service value propositions with digital content. All this will dramatically change the digital vulnerability, along with necessary efforts to ensure resilience, readiness, and NIS2 compliance. The integration of operational technology (OT) with business processes and networks, aimed at attaining business advantages, has substantially escalated the risk of exposure to cyber attacks. While these digital advancements have undeniably optimised manufacturing processes, they have also created vulnerabilities that cyber criminals can exploit[7].

In this context, the manufacturing sector's attractiveness to malicious actors goes beyond the conventional risk of data theft for ransom. The industry's capacity for large-scale disruptions, coupled with its potential for significant geopolitical ramifications, makes it an alluring target for cyber threats. As businesses continue to leverage technology for operational efficiency, it is paramount to address these vulnerabilities comprehensively to ensure the resilience of critical manufacturing processes against evolving cyber threats.

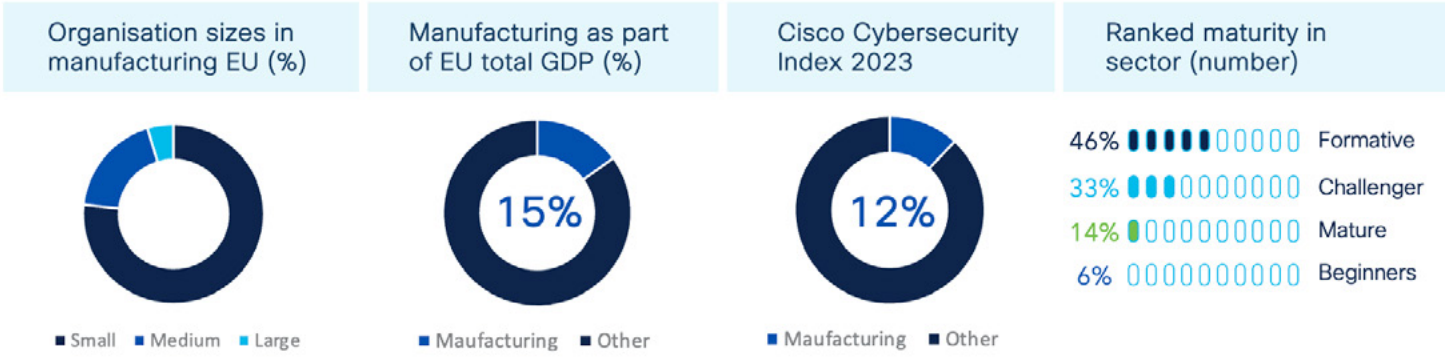


Figure 5. Manufacturing dashboard (2023).

2.6.2 Healthcare

The healthcare sector has a high level of maturity and experience in compliance with other policies and regulations covering medical and privacy requirements. However, with the high pace of digitalisation in this sector and the benefit of becoming more data-centric, becoming NIS2 compliant will be a challenge.

The European healthcare sector represent approximately 10 percent of the European total GDP. Medical and technological innovations are driving an increasing rate of digitalisation in this sector, but people working in organisations in these sectors are not predominately technical or digital specialists. Working to raise the overall knowledge and awareness around cybersecurity risks and risk management measures will be crucial for building resilience.

The healthcare sector has witnessed a concerning rise in cyber attacks[23], marking a trend that has far-reaching implications beyond mere financial losses and privacy breaches[7]. A noteworthy incident illustrates the gravity of the situation, where a threat group strategically targeted political figures in Ukraine and healthcare organisations in the United States assisting Ukrainian refugees. Their objective was to obtain geopolitical intelligence, which emphasises the potential for cyber incidents to yield ramifications that transcend traditional cyber crime boundaries[18].

This escalating threat landscape underscores the need for heightened vigilance within the healthcare sector and public administration bodies. Cyber attacks in these domains not only jeopardise sensitive data, but also inflict severe reputational damage. Additionally, the repercussions of cyber incidents in the healthcare sector are not confined to financial implications alone. Patient safety, confidentiality, and overall public health can be compromised, which amplifies the urgency for robust cybersecurity measures. As these attacks become more sophisticated and targeted, the stakes are higher than ever before. Healthcare institutions and public administration entities must invest in comprehensive cybersecurity strategies, focusing not only on preventing breaches, but also on proactive threat intelligence, incident response plans, and continuous staff training.

Investment in the proactive strenghening of the cybersecurity posture of healthcare organisations can have very tangible benefits as demonstrated by a recent Talos IR case study.

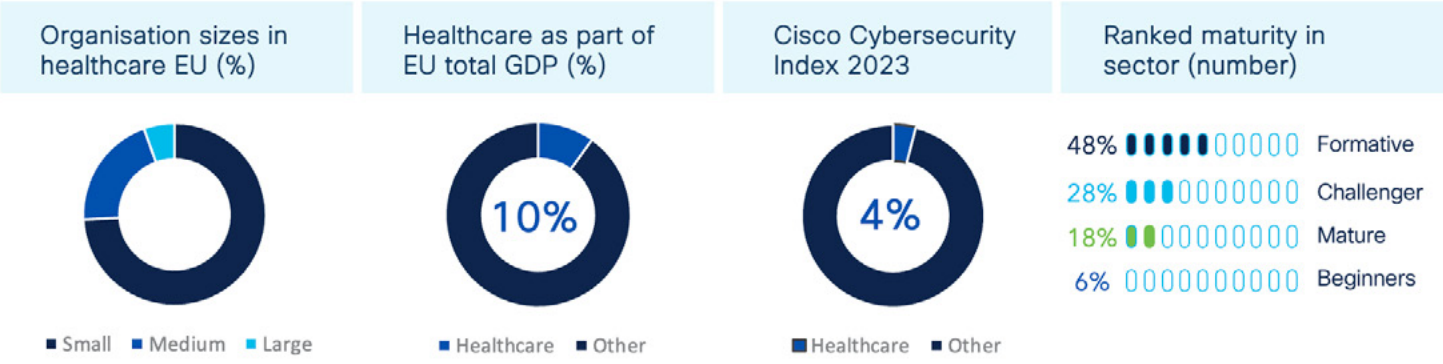


Figure 6. Healthcare dashboard (2023).

2.6.3 Energy

In Europe, the energy sector and critical infrastructure stand out as prominent targets, facing cyberattacks and physical disruptions in the supply chain[7]. The energy sector is undergoing transformation and digitalisation propelled by new digital technologies, sustainability demands, and regulations, which places high demands on securing the critical infrastructure and coordinating the IT and OT environments[3]. Some of the new challenges faced by the energy sector include[3]:

- Grids must handle more sustainable, distributed, and variable energy sources
- Environmental impacts such as fires and extreme weather conditions
- Evolving business models
- Expansion of grid capacity as the economy electrifies
- Cybersecurity risks
- Skills and resource gaps

The vulnerability of the energy systems is accentuated by the prevalence of smaller enterprises with lower cybersecurity maturity and capacity. A significant ongoing effort by NATO in Europe focuses on defending renewable energy systems, recognising their heightened vulnerability16. The renewable energy sector, in particular, is intricately linked to a complex supply chain, predominantly reliant on China – a nation known for leveraging trade for geopolitical objectives16. This reliance has amplified the sector's susceptibility to potential disruptions and cyber threats, demanding a proactive and comprehensive security approach.

Actors in the energy ecosystem must be prepared for a wider subset of actors to face new security requirements from the NIS2 Directive across electricity, oil, gas, district heating and cooling, and hydrogen, as well as vendors in their supply chain. To comply with NIS2 upon its implementation in each respective Member State, energy firms will need to enhance their cybersecurity capabilities accordingly.

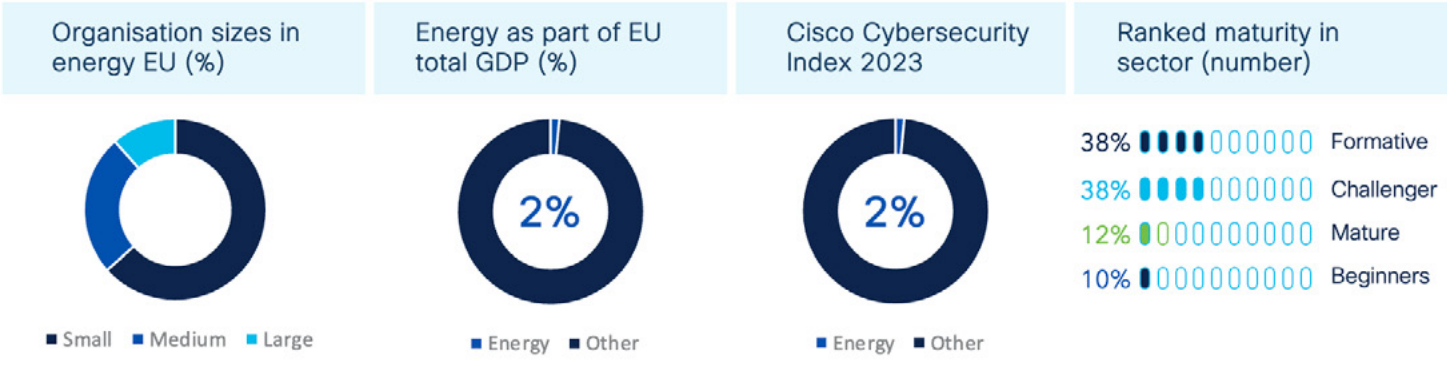


Figure 7. Energy dashboard (2023).

3. Going From NIS to NIS2

The new EU cybersecurity Strategy includes a decision to revise the previous NIS Directive (Security of Network and Information Systems)[9] to better meet current and future challenges and risks in our digitalised society[14]. The NIS2 Directive aims to harmonise the cybersecurity efforts of the Member States and must be implemented in national legislation by 17 October 2024[14].

3.1 Larger scope and tougher requirements

More sectors are covered in the NIS2 Directive, and a size rule is introduced to simplify and harmonise application across Member States. Medium and large-sized organisations with more than 50 employees and more than EUR 10 million in revenue are in scope of the Directive[8]. In addition, each country may decide on the inclusion of smaller entities carrying out activities that are of critical importance for society, the economy, or the sectors subject to the Directive[15]. The sectors are classified in the NIS2 Directive as essential or important entities, where essential ones face more stringent supervisory requirements[15].

Essential Entity	Important Entity
Energy	Postal and courier services
Transport	Waste management
Digital infrastructure	Digital providers • Providers of online marketplaces • Providers of online search engines • Providers of social networking services platform
Banking	
Financial market infrastructure	
Health	Food production, processing and distribution
Drinking water	Production and distribution of chemicals
Public administration	Manufacturing • Medical devices • Compute, electronics and optical products • Electrical equipment • Machinery • Motor vehicles, trailers, semi-trailers • Other transport equipment
Waste water	
Space	

Some of the biggest and most important differences in the NIS2 Directive include[15]:

- The imposition of sanctions up to EUR 10 million or 2 percent of global annual turnover
- The management bodies are responsible for approving the security measures and monitoring their implementation and can also be held accountable in case of non-compliance
- Stricter requirements for incident reporting, with early warnings to be provided within 24 hours and a notification report within 72 hours
- Entities in scope must assess resilience and address cybersecurity risks in their supply chains
- Increased cooperation and information sharing across organisations and Member States
- Harmonisation of security requirements and the connection to EU certifications
- The requirements for covered entitites to register themselves
- A diagram of security and safety
- Description automatically generatedThe Directive establishes a minimum standard including security measures to implement:

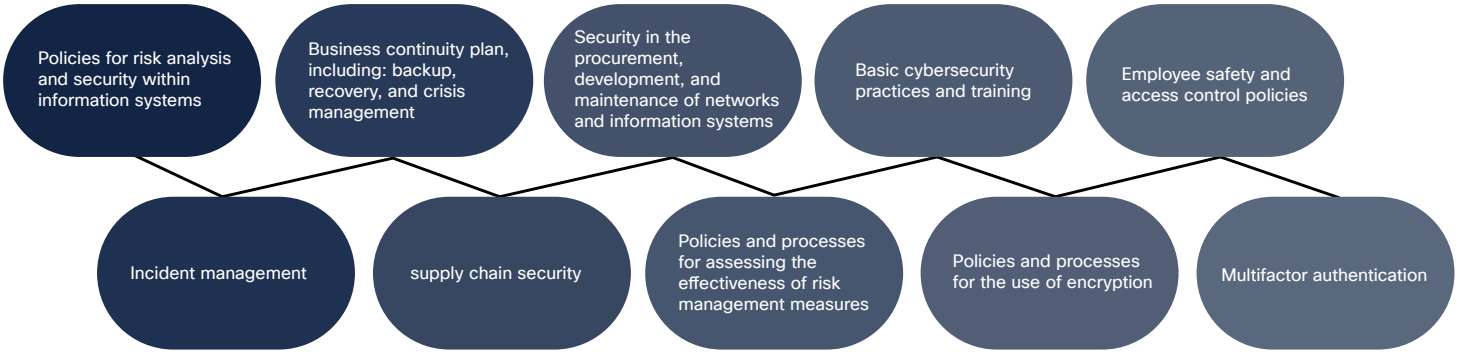


Figure 8. Security measures specified in the NIS2 Directive (2022)

An essential or critical entity becoming aware of a significant incident must provide an early warning without undue delay, and at the latest within 24 hours. The early warning should be followed by an incident notificationto the competent authorities within 72 hours containing an assessment of the incident, the severity and indicators of compromise. A final report is then to be submitted within 1 month of the incident notification. The member states should ensure that the notification requirement does not divert resources from activities related to incident handling.

3.2 Increased impact across the union

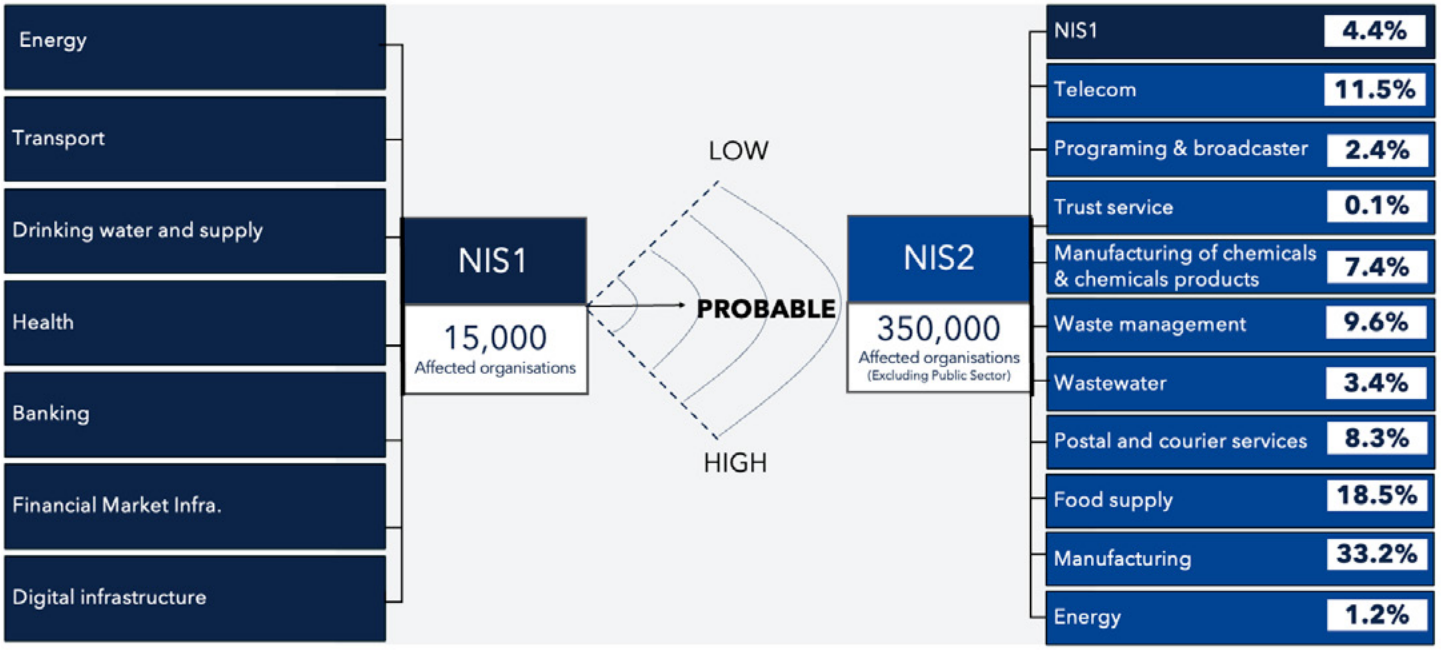


Figure 9. Expected impact across the union (2023)

NIS2 is expected to impact around 350,000 organisations in the European union. Expert estimates suggest that NIS2 will include between 7 and up to 40 times as many organisations as its predecessor. Radar's estimates suggest that at least 350,000 organisations will be impacted by the Directive. This is approximately double the previous estimates of around ten times as many organisations impacted than NIS. The analysis is partly based on a calculation of how many medium and large-sized organisations exist in the affected sectors, as well as an estimate of strategic adoption of the Directive by organisations to supply products or services to the sectors in scope or to mitigate risks and vulnerabilities. The analysis is partly based on a calculation of how many medium and large-sized organisations exist in the affected sectors, as well as an estimate of organisations needing to comply to the directive to be able to supply products or services to the sectors in scope.

3.3 COSTS TO IMPLEMENT NIS2

Implementing the NIS2 Directive will require investments. The size of these investments will depend on how complex and extensive the work will be for the business and the approach they choose. It is important that this cost is factored in early in the relevant budgets so as not to risk slowing down the work. The European Commission presents the following key figures, which clearly indicate that accelerated efforts will be needed by organisations to comply to the Directive:

Estimated costs for implementing NIS2[12]

Existing NIS operators	Not affected by NIS1
+12%	+22%
Increased costs within the information security budget over the next 3 years.	Increased costs in the information security budget over the next 3 years.

4. The role of service providers in building resilience

Service Providers (SPs) and Managed Service Providers (MSPs) will be in sbeS2 Directive, especially the large. The nuanced determination of their obligations rests upon considerations of the criticality of the services they supply to the society and economy. Their importance is twofold:

Mitigating risks: Serve many organisations and operators of essential services, breach in one MSP can have cascading effects throughout the ecosystem. Supply chain risks can result in smaller organisations being faced with disproportionately high cybersecurity risks, and this needs to be managed effectively.

Building cyber resilience: Access to specialised resources, security expertise, and infrastructure and will play a crucial role in building and enhancing national resilience across different sectors. Providing more cost-effective and scalable cybersecurity solutions that make advanced cybersecurity measures accessible to a wider range of organisations, like SMEs, which otherwise might be left behind.

In recent years, we have seen industrialisation of the IT landscape with extensive consolidation and the emergence of major global players. Much knowledge and capabilities that previously existed in-house have now moved to external suppliers, allowing organisations to focus on their core business. Effective implementation of the Directive requires collaboration to mitigate threats, and will forge closer relationships between customers and suppliers, as well as between organisations in the public and private sectors. SPs and MSPs can support in strengthening security for their customers in multiple ways:

Expertise	SPs and MSP's have knowledge and skills and an understanding of technology, cybersecurity threats, and – often – experience in disaster recovery. Providing access to specialised resources and enhancing overall resilience.
Scalability	Resiliency provided at scale through a common base and infrastructure and scalable services that can be adapted to the specific needs of organisations in different sectors.
Cybersecurity	SPs and MSPs can collaborate with the national authorities to establish comprehensive cybersecurity strategies and ensure the protection of critical data and infrastructure. Implementing robust security protocols, conducting regular security assessments, and providing rapid response in case of cyberattacks.
Business Continuity	Service providers can draw from vast experience in disaster recovery and business continuity planning to support in developing and implementing strategies that enable rapid recovery and minimise downtime for essential services.
Resource Optimization	MSPs can ensure that organisations with limited budgets can afford high-quality IT services through scalable and cost-efficient solutions. By staying adaptable, MSPs contribute to the continuous improvement of resiliency strategies, thereby ensuring that organisations are prepared for emerging challenges.
Regulatory Compliance	MSPs are well-versed in industry regulations and compliance standards and can assist organisations in adhering to these regulations. In a unified approach, service providers can work with national authorities to develop and enforce compliance standards consistently across nations.

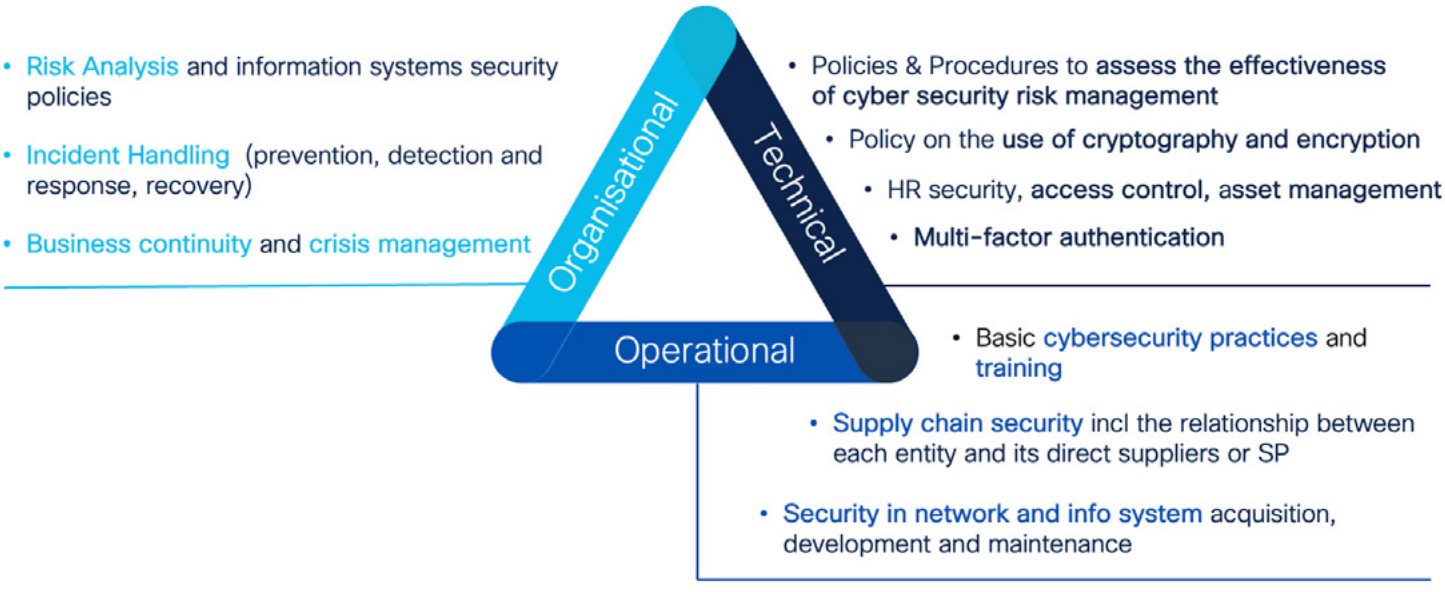
It is important to note that a high level of dependency on a single or a few SPs or MSPs can present a risk if one of them fails or experiences a major security breach, as that could have cascading effects. It is critical for SPs and MSPs to maintain a high ability to protect themselves against cybersecurity threats in order not to compromise other actors within the supply chain. It is also important for organisations to realise that it is not entirely possible to outsource compliance, since it is their responsibility in the end. Finding balance between outsourcing services and maintaining strategic control over decision-making processes, especially during crises, can be a challenging task. Leading service providers will play an equally important role to that of national authorities in building resilience within nations and organisations. The basis of the revised NIS-directive is that we exist in an ecosystem, where actors need to work together to increase security and strengthen the entire chain. Effective implementation of the directive requires collaboration to mitigate threats, and will forge closer relationships between customers and suppliers, as well as between organisations in public and private sector. SPs and MSPs can support in strengthening security for their customers via solutions and services, but another important contribution is that they will be key in proactively driving and developing the next stage of cybersecurity resilience across sectors.

5. What Should Be Done Now?

Unlike many other regulatory frameworks, NIS2 focuses on building broad resilience across society. It will therefore be important to have a holistic perspective on the implementation of NIS2. While the first iteration of NIS largely focused on technology, the spotlight is now on the human, business, and technology aspects alike.

5.1 The holistic perspective

The directive clearly stipulates that compliance is not just a matter of implementing technical solutions. The span of measures and undertakings needs to cover both organisational, operational, and technical aspects and be of both strategic (managerial responsibility) as well as operational (manage responsibility) interest. Consequently, all aspects need to be integrated in one strategic process and architecture. The following illustration shows the appropriate measures entities must undertake for the purpose of risk management, pertaining to the three dimensions.



5.2 Approach to implementing NIS2

Many businesses are already actively working with regulations such as GDPR and standards such as ISO 27001, and the experience and knowledge from working with these can help accelerate efforts to achieve compliance with NIS2. However, it is important to remember that specific measures must still be implemented to meet all the requirements of NIS2.

For the sectors that are affected by the Critical Entities Resilience (CER) Directive in addition to NIS2, it is a good idea to coordinate the work to implement both directives which follow the same timeline. In the extensive regulatory landscape, it can be challenging to understand how different regulations relate to each other, particularly between the broad NIS2 Directive and certain industry-specific regulations. One such example is DORA (Digital Operational Resilience Act), which applies to entities in the financial services sector and cover topics related to enhancing digital resilience against cyber threats. For organisations covered by DORA, NIS2 still applies, but any overlaps are avoided due to a provision that gives the specialised framework DORA precedence over the general NIS2 Directive. Still, many elements can be coordinated between different regulations to streamline the work, such as risk analysis, trainings, and establishing internal processes for management and governance.

6. How Cisco Can Help

NIS2 puts regulations on both an organisations technical and organisational structure and capabilities. Organisations must undertake critical efforts to ensure that they are secure. Regardless of whether they are public or private, SMEs or large organisations, beginner or mature in reliability and resilience levels. The following risk-management measures are included in the NIS2 Directive.

- Policies on risk analysis and information system security
- Incident handling
- Business continuity, such as backup management and disaster recovery, and crisis management
- Supply chain security, including security related aspects concerning the relationships between each entity and its direct suppliers or service providers
- Security in network and information systems acquisition, development, and maintenance, including vulnerability handling and disclosure
- Policies and procedures to assess the effectiveness of cybersecurity risk-management measures
- Basic cyber hygiene practices and cybersecurity training
- Policies and procedures regarding the use of cryptography and where appropriate, encryption
- Human resources security, access control policies and asset management
- The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems with the entity, where appropriate

Cisco is an acknowledged industry thought leader in cybersecurity and a trusted advisor in the regulatory landscape with extensive experience fulfilling compliance across the globe and in all industry sectors. Cisco can assist with each of these NIS2 measures with expertise, insights, recommendations, advisory capacity, services, and industry leading products. Cisco has the products and services to effectively manage evolving cyber risks and enhance an organisations cybersecurity strategy to adapt, evolve and improve resilience capabilities.

The three critical requirements derived from the NIS2 Directive measures that need to be immediately addressed are as follows:

1. Detection and Response
   - Incident Reporting
   - Incident Handling
   - Business Continuity and Crisis Management
2. Cybersecurity Strategy and Governance
   - Awareness and Training
   - Information Security Management
   - Cyber Risk Management and Compliance
3. Infrastructure Security and Application Security
   - Secure Development Practices
   - Identity and Access Control
   - Infrastructure/Network Security

The following sections go into detail on how Cisco sees our roles in helping organisations address both the NIS2 measures and these three critical requirements.

6.1 Cisco as a Supplier

Trust used to come down to a handshake. A promise from one person to another. But business has become too complex to base trust solely on personal relationships. Customer trust has come to depend on the security and transparency of the whole organisation—your products, services, personnel, processes, ethics and values, internal systems, suppliers, and contractors. Whether customers can trust you depends not only on your policies, but also on your suppliers—and your suppliers' suppliers. Not only on your cybersecurity, but also what you do when a breach does occur. Not only on how you store customers' private data, but also how you respond to a request from foreign law enforcement on a Friday afternoon.

In today's digital economy, an objective benchmark for assessing trust is vital. It requires full transparency. Data flowing over the internet—sometimes into a provider's cloud—includes sensitive data like login credentials, government ID numbers, financial information, trade secrets, business plans, and critical infrastructure details. If sensitive information gets into the wrong hands, consequences can include privacy breaches, loss of intellectual property, interruptions to operations and revenue, the lights going out, and even threats to national security.

The time has come for a New Trust Standard.

It's a compilation of what we've heard in conversations with thousands of customers around the world, over years. The New Trust Standard is a framework for expectations and accountability—where businesses and their customers can agree on new rules for trusted digital relationships.

Trust isn't about one thing, like encryption, certification, or supply chain oversight. It's about a combination of things. What those are will surely change over time in response to evolving customer expectations, technology, cyber threats, and international data governance. Read on for key elements of the New Trust Standard today.

Relevant links:

Summary of Cisco Security & Trust Principles

Cisco Trust Portal

6.2 Building on our experience with NIS

Actors in the entire ecosystem must contribute to building profound resilience and robustness. Service providers (SPs) and managed service providers (MSPs) have, together with Cisco, become a critical part of the digital landscape and infrastructure. Cisco has an extensive proportion of the most critical and risk-sensitive clients in the world. Therefore, Cisco is investing extensively into research and development in best-practices for compliance in organisational, operational, and technical frameworks and architectures.

6.2.1 Practicing Secure-by-Design

To ensure that organisations' networks and workloads remain secure, NIS2 encourages organisations to integrate security already from the moment the architecture is first conceived. Cisco's approach to Secure-by-Design can be seen in it's development of the Cisco Secure Development Lifecycle (CSDL).

6.2.2 Cybersecurity Strategy and Governance

The Cisco Secure portfolio provides advanced threat detection and prevention capabilities. Identifying and blocking malicious activities and intrusions, thereby helping protect critical infrastructure from cyber threats (which is a fundamental requirement of NIS2). Staying informed about emerging threats is a key aspect of

NIS2 compliance.

6.2.3 Enhancing the Security of our Cloud Infrastructure

Cisco leverages its Cloud Controls Framework (CCF) to centralise Cisco cloud compliance and certification efforts, using a “build-once-use-many” approach. As such, in preparation for the earlier NIS1, Cisco has fully mapped NIS1 Controls to Cisco Cloud Control Framework (CCF). Cisco intends to use CCF to map NIS2 controls once they are published by ENISA.

6.2.4 Efficient Management of Threats

When considering the threat landscape, Cisco leverages the MITRE ATT&CK framework to map out adversary behaviour and describe our protect and response capabiliies. Indeed, Cisco is an active contributor and considers threat-informed defence to be a critical aspect of effective risk management. Cisco Talos Intelligence Group provides threat intelligence services and tools to help our teams stay updated on the latest cyber threats and vulnerabilities.

6.3 Cisco as an Enabler

6.3.1 The Cisco Engagement Model

Based on its extensive experience of working with compliance in the regulatory landscape, Cisco has developed an engagement model to be used together with Cisco partners and clients in the compliance process. All organisations have unique and specific conditions with different maturity in different dimensions – with the Cisco engagement model, quality and assurance are ensured, which facilitates collaboration with high efficiency and visibility for all parties involved.

Figure 15. Cisco engagement model.

6.3.2 How the Cisco Secure Portfolio Can Simplify Your NIS2 Journey

Cybersecurity has historically been a messy array of independent technologies. This approach may have been adequate ten years ago, but today it presents many operational, policy enforcement, and monitoring challenges. Many organisations use dozens of cybersecurity solutions (if not more) from just as many vendors. In many cases, their security teams can investigate only a fraction of the security alerts that are received on a given day.

The Cisco Secure portfolio provides a holistic security architecture to meet the current and future security requirements for the enterprise and missions. Cisco's wide range of integrated cybersecurity solutions play a critical role in the support of the NIS2 journey. The Cisco Secure Architecture is integrated with management, threat intelligence, and the ability to integrate with other vendor security products and solutions using open-industry standards.

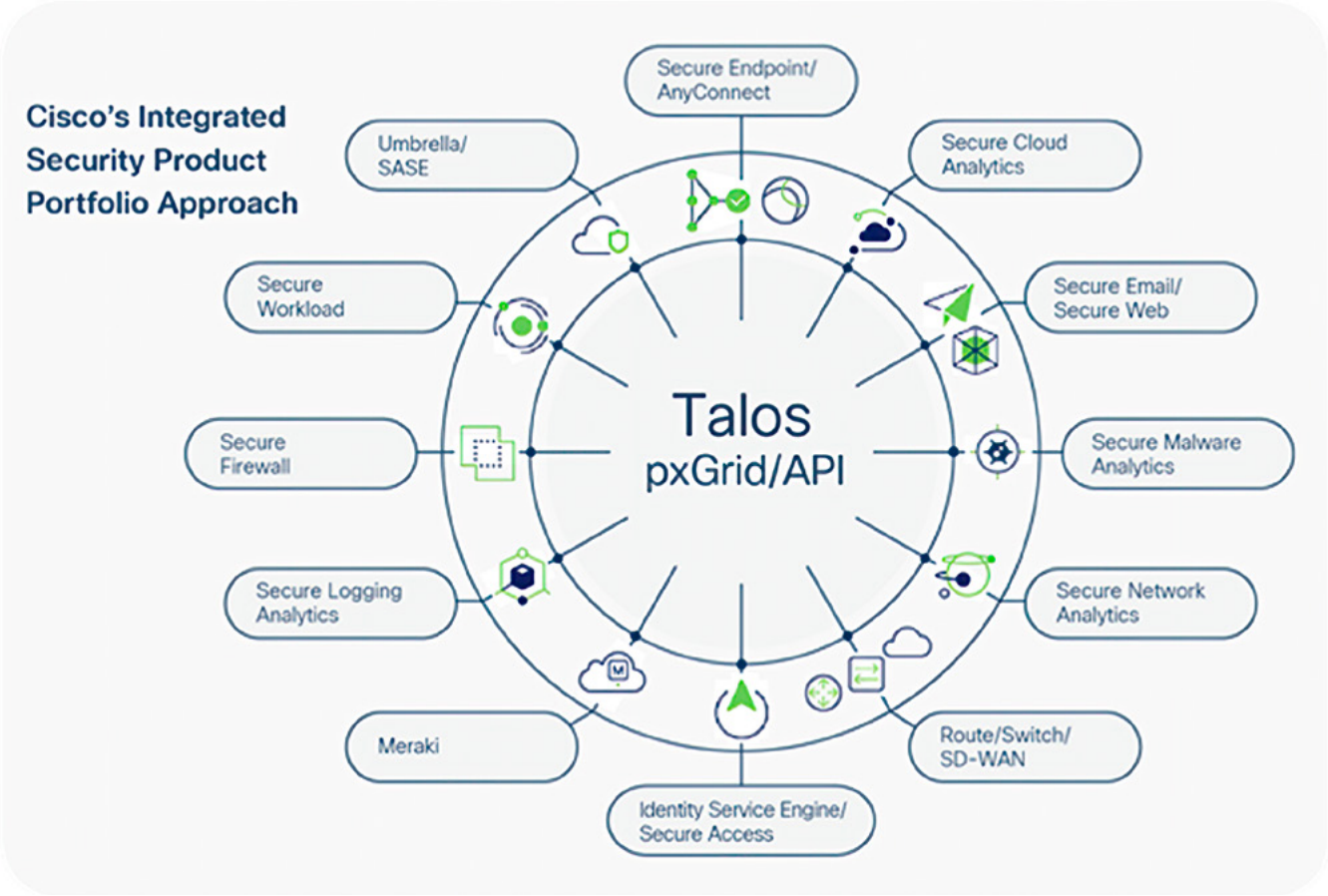


Figure 13. Cisco's Integrated Security Product Portfolio Approach (2023).

6.3.2.1 Cisco Talos

Cisco Talos is the threat intelligence organisation at the centre of the Cisco Secure portfolio. Talos is an elite group of security experts devoted to providing superior protection to customers with our products and services. Every decision point within the security matrix receives common data and can come to a common conclusion about how to deal with any threat. A common operating environment is critical when there is a need to provide security and insight to meet NIS2 requirements.

6.3.2.2 Infrastructure Security and Application Security

NIS2 emphasises the importance of secure access control and identity management. The Cisco Secure portfolio includes both experience engineering and operational experts from Cisco's global Professional Services organisation as well as a wider variety of product-based solutions to help assess and then secure clouds, applications, and workloads.

Historically, customers have solved these problems by using many vendors that provide point solutions, offering partial protection and creating silos. This results in poor outcomes, spiralling costs and complexity. Cisco's approach with the Cisco Security Suites, offers unified protection across platforms, secure users from any location and any device, and offer telemetry and insights that help early detection and resolution.

The suites (User Protection, Breach Protection, and Cloud Protection) help organisations improve efficacy, experiences, and economics with a rich portfolio of security solutions that help improve their security posture. These new suites are built with zero trust principles, leveraging the power of AI and are delivered through the Cisco Security Cloud. Lastly, customers can expect predictable and simple pricing, that helps lower costs, consolidate vendors and allocate resources to taheir most strategic priorities.

"There is no single product 'Silver Bullet' solution on the market that can solve all the requirements of NIS2. The Cisco Secure Portfolio includes all the necessary capabilities in one holistic, integrated architecture."

-Cisco Security & Compliance Advisor

The five supportive Cisco services related to NIS2 compliance:
Operational Maturity Assessment, Operational Maturity Assessment
Security Architecture Framework
Security Strategy, Risk and Compliance Services
Technical Security Assessment Services
Incident Response Services

6.3.2.3 Cisco Operational Technology (OT)

With Operational Technology (OT) no longer operating in a silo and starting to incorporate many of the same technologies that IT uses, such as remote access, data collection and analytics, artificial intelligence, and machine language, and various applications in the data center and cloud, Cisco's industrial cyber security solutions provide these types of environments with support and security along the NIS2 journey.

6.3.2.4 Detection and Response

The Cisco Secure Portfolio includes features that facilitate compliance reporting. This is crucial for organisations subject to NIS2, as they need to provide evidence of their cybersecurity measures and compliance efforts. Cisco Talos Incident Response (Talos IR) provides a full suite of proactive and emergency services to help customers prepare, respond, and recover from breaches. Talos IR enables 24-hour emergency response capabilities and direct access to Cisco Talos cybersecurity analysts.

Extended Detection and Response (XDR) solutions are essential for monitoring and reporting security events. Cisco XDR provides built-in automation, orchestration and guided remediation recommendations to help analysts automate repetitive tasks and mitigate threats more effectively, thereby helping to comply with the NIS2 requirement for continuous monitoring and reporting of security incidents.

6.3.2.2 Cisco pxGrid

Cisco pxGrid (Platform Exchange Grid), multiple security products can now share data and work together. This open, scalable, and Intenet Engineering Task Force (IETF) standards driven platform helps you automate security. Use one API for simple integration, open and automated for data sharing and control. Cisco pxGrid helps an entire ecosystem of dissimilar, IETF standards track technologies work together and manage your security technologies through a single interface. Check out all the Cisco Secure Technical Alliance Partners where multivendor product integrations improve security effectiveness. And enable data sharing to make multivendor technologies function as one.

NIS2 encourages collaboration and information sharing among organisations to improve overall cybersecurity. The Cisco Secure Portfolio supports secure communication and information sharing among entities.

6.3.3. Leveraging Cisco's Professional Services Experience in Building Transformational Programmes

Whilst the Cisco Secure Portfolio includes all the necessary capabilities in one holistic integrated architecture, it's important to recognise that people, policies, and processes will also need to ch,,ange to meet the NIS2 requirements. Cisco's Professional Services teams can help you adapt, optimise and where necessary modernise your organisation's governance and operational models as you begin your NIS2 journey, no matter what challenges you face.

Challenge	How Cisco's professional services can help
Understand requirements	Conduct scoping to understand organisational impact and requirements of regulations
Measure current capability and maturity	Baseline critical systems, security architecture, controls and capabilities
Develop a secure-by-design approach	Define a roadmap and establish priority areas, e.g. implementation and operation of controls, expansion of response capabilities, team training
Invest in people and processes	Develop operational capability and maturity of teams and supporting processes
Respond to changing business and threat landscape	Compare your security posture against the requirements of the specific NIS2 legislation

6.3.4 Benefitting from Cisco's Partner Network

Cisco and its partner network can advise on security issues, provide support in assessing and designing future-proof security architectures, as well as support in implementing the critical incident reporting requirements. Additionally, Cisco can use and share its specific global survey data to comprehensively evaluate, guide, and advise in maturity assessments. This includes IT infrastructure and application landscape designs to provide solid and tailored recommendations.

Based on the extensive experience of working with compliancy in the regulatory landscape Cisco has developed an engagement model to be used together with Cisco partners and clients in the compliance process. All organisations have unique and specific conditions with different maturity in different dimensions – with Cisco engagement model the quality and assurance is secured, an ease to collaborate and with high efficiency and visibility for all parties involved.

The incremental Cisco engagement model in the journey to NIS2 Compliancy:

To build a profound resilience and robustness actors in the entire ecosystem must contribute. Service providers (SP) and managed service providers (MSP) has together with Cisco become a critical part of the digital landscape and infrastructure. In addition, Cisco has an extensive part of the most critical and risk sensitive clients in the world. Therefore, Cisco is investing extensive efforts and research in best-practices for compliance – both in organisational, operational, and technical frameworks and architectures.

Cisco uses the best-practices attached to the Cloud Controls Framework (CCF) to centralize Cisco cloud compliance and certification efforts, using a "build-once-use-many" approach. As such, in preparation for the earlier NIS1, Cisco has fully mapped NIS1 Controls to Cisco Cloud Control Framework (CCF). Cisco will continue to use CCF for the assessments going forward, into full NIS2 compliance.

The Cisco Cloud Controls Framework (CCF) is a comprehensive set of international and national security compliance and certification requirements, aggregated into a single framework. The CCF is continuously updated as security compliance frameworks and regulations evolve. To benefit from this framework, the best-practice is to review, evaluate, and tailor it to reach the specific organisations conditions and compliance goals.

7. Conclusion

Europe has come a long way in digital development, and, in all sectors of society, digitalisation is seen as a strategically important component for the future. There is widespread understanding of the value of digitalisation, but despite this, there is a lack of knowledge and ability in many places about how digitalisation can be developed securely.

There is a collective potential in digitalising the EU that amounts to around EUR 3 trillion. This space is in our collective interest to capitalise on – and secure – for a more robust Europe.

As society becomes increasingly digital and connected, the threat and risk of cyber attacks increase. Incidents have increased in both number and cost, and vulnerability has reached a level that is not only a burden for the entity affected but for society as a whole. The EU's broad regulatory framework, NIS2, is a political response to this development, creating a common platform for increased collaboration and increased cybersecurity capabilities.

Cybersecurity has become a strategic operational issue, but the overall cybersecurity capability is linked to Europe's security and economic well-being. Secure digitalisation has become essential - for everyone.

8. Next steps

Cisco Cybersecurity Readiness
Cisco developed the Cisco Cybersecurity Readiness Index, which categorises companies into four stages of readiness: from Beginner, to Formative, Progressive, and finally Mature. This is based on their preparedness across five key pillars and the state of deployment of security solutions.

Cisco Supply Chain Security
Cisco recognises the importance role of supply chain security in a comprehensive Cisco cybersecurity strategy. Cisco deploys a capability that continually assesses, monitors, and improves the security of the Cisco supply chain throughout the entire lifecycle of our solutions.

Cisco Secure Architecture
A zero-trust network is based on a security model that establishes trust through continuous authentication and monitoring of each network access attempt. Zero trust helps enable secure access for users and devices and within apps, across networks, and clouds. Embed zero trust across the fabric of your multi-environment IT without compromising user experience

Cisco Zero Trust
A zero-trust network is based on a security model that establishes trust through continuous authentication and monitoring of each network access attempt. Zero trust helps enable secure access for users and devices and within apps, across networks, and clouds. Embed zero trust across the fabric of your multi-environment IT without compromising user experience..

Cisco's Professional Services
Cisco's services, aligned to NIST CSF's pillars are intended to enable a proactive approach to threat-informed defence, enabling you to assess and optimise the capabilities that keep your business secure.

In particular, Talos IR provides a full suite of proactive and emergency services to help you prepare, respond and recover from a breach. Talos IR enables 24-hour emergency response capabilities and direct access to Cisco Talos, the world's largest threat intelligence research group.

Incident Response:	Emergency Response
Threat Intelligence:	Intel on Demand, Threat Modelling
Preparing:	Security Architecture Assessment, IR Readiness Assessment, IR Plans, IR Playbooks, Log Architecture Assessmentv
Implementation and Optimisation:	Solution Design, Security Engineering, Industry leading products/controls such Cisco Secure portfolio
Operations:	Managed Detection & Response
Training:	Tabletop Exercises, Cyber Range Training
Hunting:	Compromise Assessment, Threat Hunting, Security Operations Assessment
Simulating:	Purple Team, Red Team, Penetration Testing

9. Reference list

1. Centre for Cyber Security Belgium (CCB) (2023). NIS2: Where are you? https://ccb.belgium.be/en/news/nis-2-where-are-you
2. Cisco (2023:1). Cybersecurity Readiness Index. Resilience in a hybrid world. Cisco_cybersecurity-readiness-index-report_2023.pdf
3. Cisco (2023:2). Digitalizing Europe's energy system to power the green energy revolution. https://www.cisco.com/c/dam/en_us/about/csr/environmental-sustainability/digitalizing-energy-system.pdf
4. DNV AS (2023). NIS2 Directive: Compliance risk or cyber security opportunity? https://www.dnv.com/Publications/nis2-directive-compliance-risk-or-cyber-security-opportunity--238994
5. ENISA (2022:1). NIS investments 2022. https://www.enisa.europa.eu/publications/nis-investments-2022
6. ENISA (2022:2). Threats fast forward 2023. https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030
7. ENISA (2022:3). Threat Landscape 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022
8. European Commission (2020). Annexes 1-3 to the Proposal for a Directive on Measures for a High Common Level of Cybersecurity Across the Union, repealing Directive 2016/1148. https://eur-lex.europa.eu/resource.html?uri=cellar:be0b5038-3fa8-11eb-b27b-01aa75ed71a1.0001.02/DOC_2&format=PDF
9. European Commission (2023). New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient. https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391
10. European Commission (2023). The Digital Economy and society index (DESI) 2022. https://digital-strategy.ec.europa.eu/en/policies/desi
11. European Commission (2023). 2023 Report on the state of the Digital Decade. https://digital-strategy.ec.europa.eu/en/library/2023-report-state-digital-decade
12. EUR-Lex (2023). Commission Staff Working Document Impact Assessment Report. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020SC0345
13. European Investment Bank (2023). Digitalisation in Europe 2022–2023. https://www.eib.org/attachments/lucalli/20230112_digitalisation_in_europe_2022_2023_en.pdf
14. European Parliamentary Research Service (EPRS) (2023). The NIS2 Directive: A high common level of cybersecurity in the EU. The 'EU Legislation in Progress' briefing 2023-02-08. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf
15. European Union (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555&qid=1684142672664

16. Impact loop (2023). Kan förnybar energi ta fart inom försvaret? https://www.impactloop.se/artikel/nya-affarsmojligheten-for-fornybar-energi-forsvar

17. McKinsey (2020). How COVID-19 has pushed companies over the technology tipping point – and transformed business forever. https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Strategy%20and%20Corporate%20Finance/Our%20Insights/How%20COVID%2019%20has%20pushed%20companies%20over%20the%20technology%20tipping%20point%20and%20transformed%20business%20forever/How-COVID-19-has-pushed-companies-over-the%20technology%20tipping-point-final.pdf

18. Picus (2023). Regions and industries at risk. https://www.picussecurity.com/resource/blog/regions-and-industries-at-risk-august-2023

19. McKinsey (2017). Möjligheter för Sverige i digitaliseringens spår. sverige-i-digitaliseringens-spar.ashx

20. Radar (2021). Från IT-säkerhet till digital affärsrisk. https://hub.radargrp.com/reports

21. Radar (2023:1). Cybersäkerhet 2023 – i ett alltmer osäkert och utsatt läge. https://hub.radargrp.com/content/svensk-cybersakerhet-2023

22. Shadowserver (2023). Cyberattacks dashboard. https://dashboard.shadowserver.org

23. Talos (2023). Incident response trends. https://blog.talosintelligence.com/talos-ir-q2-2023-quarterly-recap/

10. Footnotes

2. Centre for Cyber Security Belgium (CCB) (2023). NIS2: Where are you? https://ccb.belgium.be/en/news/nis-2-where-are-you

3. Cisco (2023:1). Cybersecurity Readiness Index. Resilience in a hybrid world. Cisco_cybersecurity-readiness-index-report_2023.pdf

4. Cisco (2023:2) . Digitalizing Europe's energy system to power the green energy revolution. https://www.cisco.com/c/dam/en_us/about/csr/environmental-sustainability/digitalizing-energy-system.pdf

5. DNV AS (2023). NIS2 Directive: Compliance risk or cyber security opportunity? https://www.dnv.com/Publications/nis2-directive-compliance-risk-or-cyber-security-opportunity--238994

6. ENISA (2022:1). NIS investments 2022. https://www.enisa.europa.eu/publications/nis-investments-2022

7. ENISA (2022:2). Threats fast forward 2023. https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030

8. ENISA (2022:3). Threat Landscape 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

9. European Commission (2020). Annexes 1-3 to the Proposal for a Directive on Measures for a High Common Level of Cybersecurity Across the Union, repealing Directive 2016/1148. https://eur-lex.europa.eu/resource.html?uri=cellar:be0b5038-3fa8-11eb-b27b-01aa75ed71a1.0001.02/DOC_2&format=PDF

10. European Commission (2023). New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient. https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391

11. European Commission (2023). The Digital Economy and society index (DESI) 2022. https://digital-strategy.ec.europa.eu/en/policies/desi

12. European Commission (2023). 2023 Report on the state of the Digital Decade. https://digital-strategy.ec.europa.eu/en/library/2023-report-state-digital-decade

13. EUR-Lex (2023). Commission Staff Working Document Impact Assessment Report. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020SC0345

14. European Investment Bank (2023). Digitalisation in Europe 2022–2023. https://www.eib.org/attachments/lucalli/20230112_digitalisation_in_europe_2022_2023_en.pdf

15. European Parliamentary Research Service (EPRS) (2023). The NIS2 Directive: A high common level of cybersecurity in the EU. The 'EU Legislation in Progress' briefing 2023-02-08. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf

16. European Union (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555&qid=1684142672664

17. Impact loop (2023). Kan förnybar energi ta fart inom

försvaret? https://www.impactloop.se/artikel/nya-affarsmojligheten-for-fornybar-energi-forsvar

18. McKinsey (2020). How COVID-19 has pushed companies over the technology tipping point – and transformed business forever. https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Strategy%20and%20Corporate%20Finance/Our%20Insights/How%20COVID%2019%20has%20pushed%20companies%20over%20the%20technology%20tipping%20point%20and%20transformed%20business%20forever/How-COVID-19-has-pushed-companies-over-the%20technology%20tipping-point-final.pdf
19. Picus (2023). Regions and industries at risk. https://www.picussecurity.com/resource/blog/regions-and-industries-at-risk-august-2023
20. McKinsey (2017). Möjligheter för Sverige i digitaliseringens spår. sverige-i-digitaliseringens-spar.ashx
21. Radar (2021). Från IT-säkerhet till digital affärsrisk. https://hub.radargrp.com/reports
22. Radar (2023:1). Cybersäkerhet 2023 – i ett alltmer osäkert och utsatt läge. https://hub.radargrp.com/content/svensk-cybersakerhet-2023
23. Shadowserver (2023). Cyberattacks dashboard. https://dashboard.shadowserver.org
24. Talos (2023). Incident response trends. https://blog.talosintelligence.com/talos-ir-q2-2023-quarterly-recap/