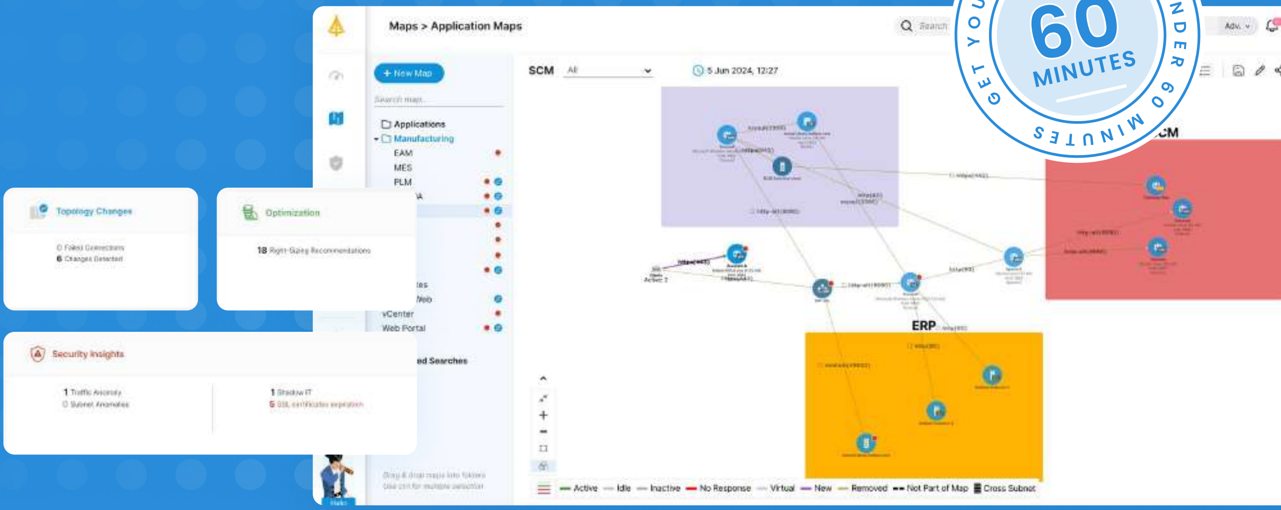
Strengthening Digital Resilience: Unpacking DORA & NIS2

Navigating the Future of Cybersecurity

A FADDOM WHITEPAPER

Table of contents

GET YOUR FIRST MAP IN UNDER 60 MINUTES



Introduction

In the ever-evolving landscape of digital threats, the European Union has taken a proactive stance to fortify the resilience of its financial and critical sectors, introducing the Digital Operational Resilience Act (DORA) and the updated Network and Information Systems Directive (NIS2) - regulations that are set to redefine cyber defense standards within the EU and beyond.

As the enforcement of NIS2 in October 2024 and DORA in January 2025 looms near, many entities are finding themselves unprepared to meet the mandatory requirements. Faddom's research highlights common pitfalls, ranging from tardy compliance realization to the adoption of overly complex and costly solutions.

The mandatory requirements are broad and require the implementation of several processes that are mostly, but not only, supported by advanced and diverse cyber technologies. There is no single solution that provides a complete answer to NIS2 and DORA.

Navigating the intricate web of NIS2 and DORA prerequisites is undoubtedly a resource-consuming challenge, though Faddom offers a beacon of hope with its agentless IT infrastructure discovery and real-time application dependency mapping platform. With over 100 satisfied customers around the globe, Faddom's Israeli-based cyber company provides a cost-effective answer to the directives' fundamental building blocks, making the fundamental compliance requirements easy to complete in one week or less.

Say goodbye to complicated approaches and embrace Faddom's simple yet comprehensive solution, tailored to meet the core demands of NIS2 and DORA. By partnering with us, organizations can fortify their cyber defenses, ensure seamless incident reporting, and achieve operational resilience - all while staying ahead of EU regulatory standards.

Navigate Your Future Cyber Resilience with DORA & NIS2!

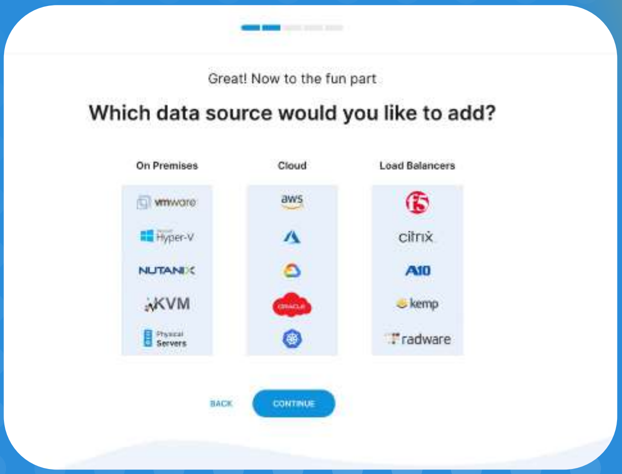
The intricate nature of cyber threats in Europe, fueled by geopolitical complexities and rapid technological progress, necessitates decisive regulatory action. The Global Cybersecurity Outlook 2024 report from the World Economic Forum sheds light on the stark contrast of resilience between large enterprises and small to medium-sized enterprises (SMEs), **emphasizing the vulnerability of the latter due to limited resources.**

The Digital Operational Resilience Act (DORA) stands at the forefront of EU legislation, offering a comprehensive framework to bolster the operational resilience of the financial sector in the face of digital disruptions. From meticulous ICT risk management to robust incident reporting and stringent oversight of third-party ICT service providers, DORA sets a high standard for financial entities like banks, insurance companies, and investment firms.

Embracing the key functions of DORA such as ICT risk management, financial entities are tasked with establishing resilient ICT systems and protocols to effectively mitigate risks. Faddom emerges as a crucial ally in this journey, with cutting-edge technology for real-time asset discovery and dependency mapping. By providing unparalleled visibility into hybrid environments, Faddom empowers financial entities to proactively manage ICT risks and fortify their cybersecurity posture.

> Faddom is helping us with detection of common vulnerabilities (CVE's), tracking of SSL certificates to include status and expiration dates, and Identify abnormal traffic behavior on servers. Overall, a clean approach to everything pulled together on one pane of glass.

Troy Clavel, CTO,
First National Bank of Sioux Falls.



Great! Now to the fun part

Which data source would you like to add?

Prioritize Critical Operations for ICT Risk Management

Requirement:

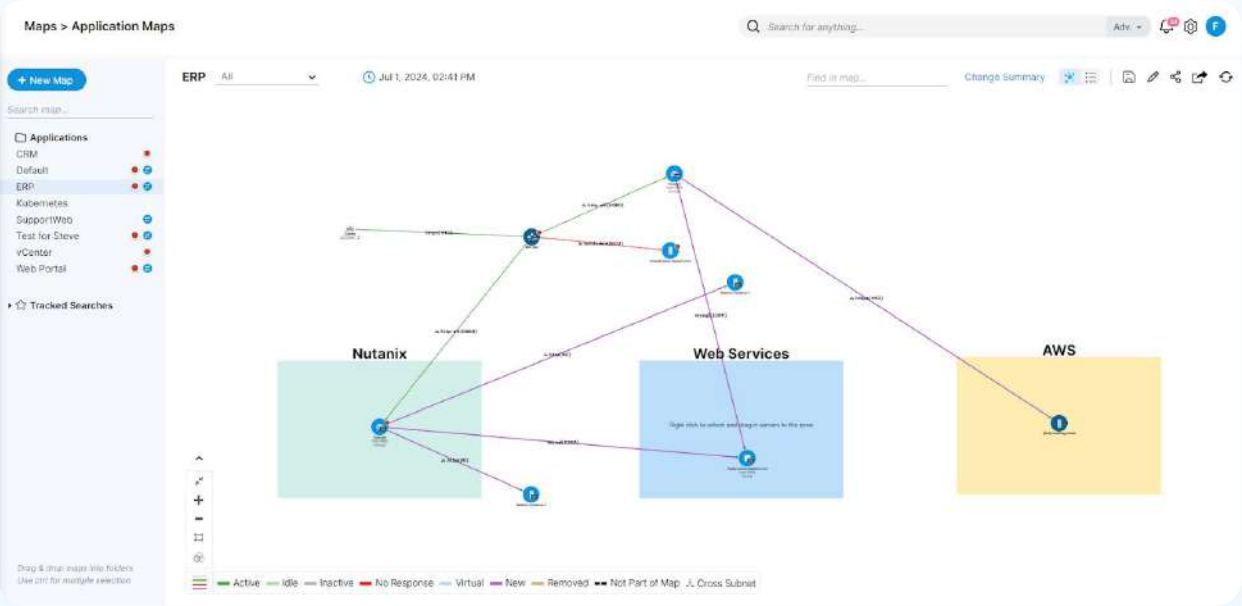
Within the framework of the Digital Operational Resilience Act (DORA), the cornerstone of operational resilience lies in effective ICT risk management. Financial entities face the vital task of establishing and upholding resilient ICT systems and protocols to navigate the ever-evolving threatful landscape. To fulfill this requirement, it is crucial to first prioritize your attention and resources towards your organization’s most critical business process.

Faddom's Contribution:

Faddom takes ICT risk management to the next level with real-time, agentless asset discovery and dependency mapping. Our cutting-edge technology offers unparalleled visibility into your hybrid environment, empowering financial entities to proactively identify and mitigate ICT risks. By leveraging Faddom's solutions, organizations can bolster their cybersecurity posture and ensure robust visibility across their IT infrastructure.

With Faddom's comprehensive visibility capabilities, financial entities can streamline their risk management processes through continuous automated procedures. This proactive approach not only meets the strict requirements set forth by DORA but also forms the foundation for a resilient and secure operational environment. Trust Faddom to be your partner in fortifying your ICT risk management practices and staying ahead of cyber threats in today's digital landscape.

At Faddom, we endorse the adoption of methodologies favored by mature organizations, ensuring seamless implementation. By visualizing your critical business processes - often referred to as your 'Crown Jewels'- on your IT infrastructure map, we empower you to prioritize these assets.
From optimizing network availability to mitigating cyber vulnerabilities, this approach allows you to effectively manage IT risks aligned with your entity's business objectives.



Immediate and Complete Incident Reporting

Requirement:

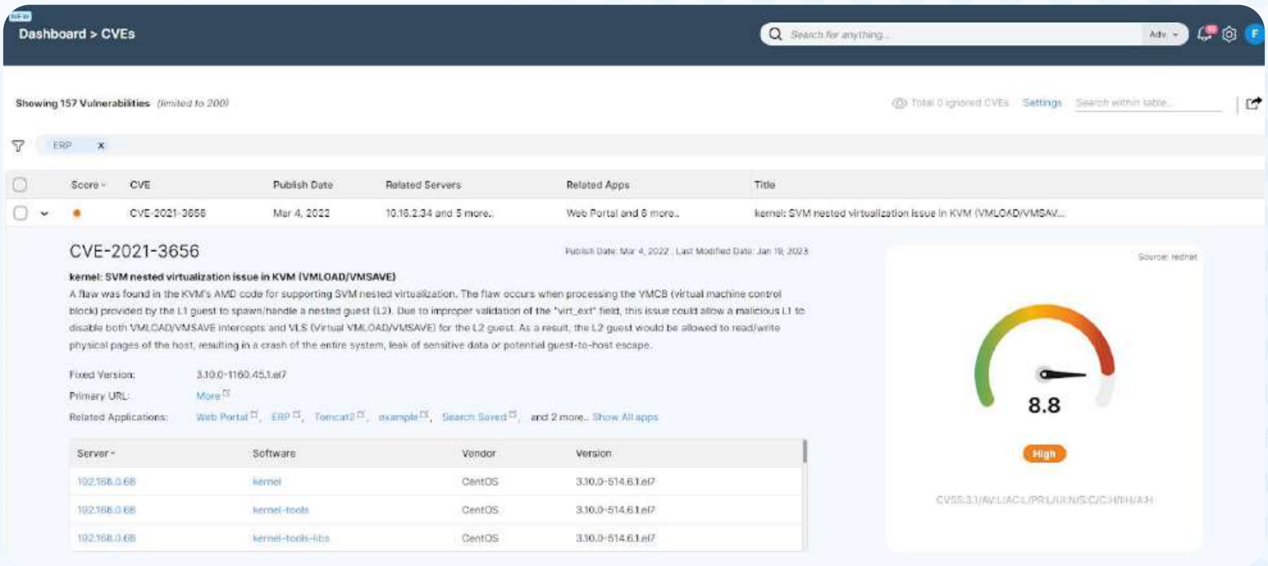
In today's fast-evolving digital realm governed by DORA standards, every moment counts in safeguarding your ICT infrastructure. Enter Faddom, your trusted partner at the forefront of incident reporting excellence.
Why Incident Reporting Matters: In the era of DORA, timely reporting of ICT-related incidents isn't just a requirement; it's the basis of transparency and resilience across sectors. Faddom understands the urgency and importance of swift action when it comes to identifying and addressing vulnerabilities, as well as preparing for the realization of a cyber incident, in which case Faddom would materialize and contain it in the shortest possible time while minimizing the damage.

Faddom's Contribution:

Faddom's advanced capabilities in CVE detection and user access tracking set the standard for proactive incident management. Our robust platform ensures rapid incident identification and reporting, empowering you to stay ahead of threats.
Unveiling Critical Insights: In the face of an incident, Faddom provides unparalleled visibility into user-server interactions. Our comprehensive insights offer vital context on potential vulnerabilities, equipping your team with the knowledge needed to safeguard your business applications effectively.
In the event of a cyber incident, Faddom's solution provides real-time insights into the affected areas, their connections, and their impact on your organization's critical business assets. This capability enables IT operations and cybersecurity professionals to effectively communicate with business leaders across the board by using clear, unified, business-centric language to explain the incident's impact. Simultaneously, our solution offers feedback to the incident response teams, ensuring the effectiveness of their containment efforts.

Beyond Compliance:

Compliance with DORA's stringent standards is non-negotiable, and Faddom exceeds these requirements. Our proactive approach not only ensures adherence to regulations but also enhances your organization's overall risk mitigation strategy.



Showing 157 Vulnerabilities *(limited to 200)*

□		Score	CVE	Publish Date	Related Servers	Related Apps	Title
□	⌄	●	CVE-2021-3656	Mar 4, 2022	10.16.2.34 and 5 more..	Web Portal and 6 more..	kernel: SVM nested virtualization issue in KVM (VMLOAD/VMSAV...

CVE-2021-3656

Publish Date: Mar 4, 2022 | Last Modified Date: Jan 19, 2023

kernel: SVM nested virtualization issue in KVM (VMLOAD/VMSAVE)

A flaw was found in the KVM's AMD code for supporting SVM nested virtualization. The flaw occurs when processing the VMCB (virtual machine control block) provided by the L1 guest to spawn/handle a nested guest (L2). Due to improper validation of the "virt_ext" field, this issue could allow a malicious L1 to disable both VMLOAD/VMSAVE intercepts and VLS (Virtual VMLOAD/VMSAVE) for the L2 guest. As a result, the L2 guest would be allowed to read/write physical pages of the host, resulting in a crash of the entire system, leak of sensitive data or potential guest-to-host escape.

Fixed Version: 3.10.0-1160.45.1.el7
Primary URL: More
Related Applications: Web Portal, ERP, Tomcat2, example, Search Saved, and 2 more.. Show All apps

Server	Software	Vendor	Version
192.168.0.68	kernel	CentOS	3.10.0-514.6.1.el7
192.168.0.68	kernel-tools	CentOS	3.10.0-514.6.1.el7
192.168.0.68	kernel-tools-libs	CentOS	3.10.0-514.6.1.el7

Source: redhat

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Elevate Your Operational Resilience and Third-Party Risk Management:

Operational Resilience Testing

Requirement:

In today's volatile and unpredictable landscape, financial entities must ensure seamless operational resilience even during severe disruptions, as continuity is not just a goal but a necessity. In today's unpredictable financial landscape, continuity is not just a goal but a necessity.

Faddom's Contribution:

Faddom introduces a paradigm shift in operational resilience testing with state-of-the-art, real-time detection capabilities. Our platform goes beyond traditional methods by dynamically visualizing dependencies across both cloud and on-premises environments. Navigate disruptions seamlessly with Faddom as your strategic partner. From change management to risk mitigation, our intuitive visualization tools empower your organization to maintain robust, uninterrupted operations in any scenario.

Third-Party Risk Monitoring

Requirement:

As reliance on third-party service providers grows, mitigating associated risks becomes paramount of most significant importance. As reliance on third-party service providers grows, so does the need for vigilant risk management.

Faddom's Contribution:

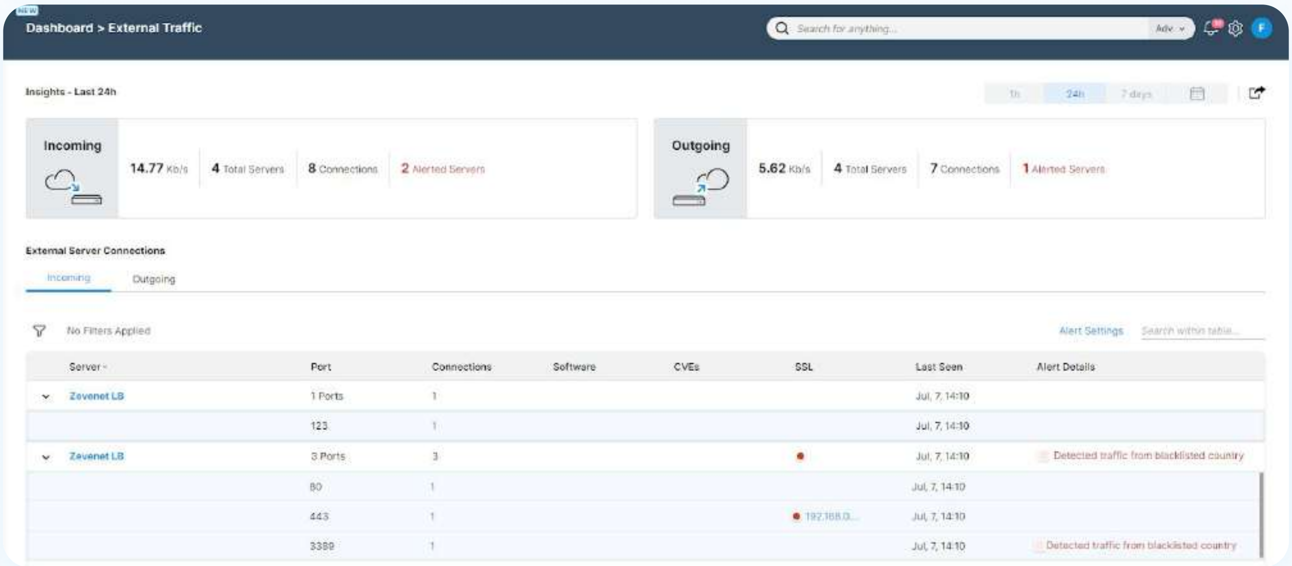
Faddom leads the charge in mitigating risks associated with shadow IT and external service providers. Our advanced detection capabilities provide unprecedented visibility into third-party interactions, offering crucial insights through comprehensive SSL analysis and North-South external traffic monitoring. Stay ahead of threats with Faddom's proactive approach to risk management and compliance, setting new standards for secure engagements in today's interconnected world.

Partner with Faddom Today:

Transform your operational resilience and third-party risk management strategies with Faddom's innovative solutions.

Contact us now to discover how our cutting-edge technologies can safeguard your business continuity and enhance your operational efficiency in the face of evolving challenges.

Embrace resilience. Embrace Faddom.



Insights - Last 24h

Incoming: 14.77 Kb/s | 4 Total Servers | 8 Connections | 2 Alerted Servers

Outgoing: 5.62 Kb/s | 4 Total Servers | 7 Connections | 1 Alerted Servers

External Server Connections

No Filters Applied

Server	Port	Connections	Software	CVEs	SSL	Last Seen	Alert Details
Zevenet LB	1 Ports	1				Jul, 7, 14:10	
	123	1				Jul, 7, 14:10	
Zevenet LB	3 Ports	3			●	Jul, 7, 14:10	Detected traffic from blacklisted country
	80	1				Jul, 7, 14:10	
	443	1			● 192.168.0...	Jul, 7, 14:10	
	3389	1				Jul, 7, 14:10	Detected traffic from blacklisted country

Main Differences Between NIS2 and DORA

Network and Information Security Directive or NIS2 (Directive (EU) 2022/2555) is a directive, whereas the Digital Operational Resilience Act or DORA (EU Regulation No. 2022/2554) is a sector-specific regulation.
While NIS2 sets out cybersecurity standardization goals that organizations based in all EU countries must achieve, it's up to each EU country to "transpose" (a.k.a. "translate") the NIS2 directive into actual national laws. This will happen at different times in different countries and throughout a variety of legislation.
All the same, many parts of NIS2, such as the maximum fine of €10 million for breaches (or % of the global annual revenue, whichever is higher), will be similar everywhere.

DORA on the other hand, is a finance sector-specific EU-wide regulation. It has a list of EU-wide compliance obligations that organizations within the scope will share regardless of where they are based. It also comes into force for every affected organization at the same time (January 17, 2025)
Under DORA, a bank in one country - say Italy - and an investment firm in another country - for example, Belgium - will need to meet the same compliance requirements. The only difference will be who their competent authority is going to be.
In this regard, local regulators are responsible for defining which organizations are critical, and therefore subjected to advanced testing requirements. The selection criteria they use however will be written within the DORA regulation, and not an arbitrary choice.

For the financial services industry, DORA Supersedes NIS2

If your organization could be described as a financial services firm, the most critical thing you need to understand when it comes to NIS2 versus DORA is a legal term called “lex specialis”, which means that if two laws cover the same thing, a law governing a specific subject matter is more important than a law governing only general matters. So if DORA and NIS2 both apply to your organization (which can happen), lex specialis prevails, and the sector-specific law (DORA) takes precedence over the more general regulation (NIS2) when it comes to any specific requirement.

Therefore, if you are a:

- Bank
- Investment firm
- Insurance company
- Reinsurance company
- Payment institution
- Electronic money institution
- Crypto-asset service provider
- Credit rating agency
- Statutory auditor
- Audit firm
- Administrator of critical benchmark
- ICT third-party service provider
- Or any other financial entity covered by DORA and NIS2

Then you need to focus on complying with DORA above any national-level transposition of NIS2. For FSI cybersecurity risk management and reporting obligations, DORA is what counts.

DORA Is Stricter Than NIS2

DORA and NIS2 overlap a lot. For example, NIS2 has reporting timelines like DORA (24 and 72 hours) and equally large fines. The two pieces of legislation are also designed to be systematically linked in terms of information sharing. However, in almost every case, complying with DORA will require more work from your organization than complying with NIS2.

DORA vs NIS2 Comparison Table

Aspect	NIS2	DORA
Scope	Applies broadly to various businesses and sectors across the EU.	Specifically targets businesses in the financial sector and their critical third-party ICT providers.
Two Primary Focus	Harmonise overall cybersecurity across the EU. focusing on operators of essential services (OES) and digital service providers (DSPs) across various critical sectors.	Building digital operational resilience in the financial sector.
Applicable Entities	Organisations in a wide range of sectors, including transport, energy, and health, that have a minimum of 50 employees and/or at least an annual turnover (and/or an annual balance sheet total) ono million euros.	Financial institutions and their critical ICT service providers, except for some micro businesses such as small insurance intermediaries: employing fewer than 10 persons with an annual turnover or balance sheet that does not exceed 2 milion euros.
Regulatory Overlap Handling	Part of the broader cybersecurity regulatory framework.	In case of overlap with other regulations like NIS2 and DORA takes precedence (lex specialis exemption).
Testing Requirement	Varies depending on the country.	A range of assessments and tests every year and advanced threat-led penetration testing every three years.
Reporting Obligations	An initial report within 24 hours, a detailed report within 72 hours, and a final report within 1 month.	An initial report within 24 hours, a detailed report within 72 hours, and a final report within 1 month.

Charting the Waters of NIS2 Compliance?

Keep reading!

Strengthening Cybersecurity Across Critical Sectors:

As the digital landscape expands, so do the threats facing essential sectors like energy, transport, health, and digital infrastructure. NIS2 emerges as a pivotal framework, enhancing cybersecurity.
GDPR, CRA, NIS, DORA, NIS2… Read enough cyber acronyms, and your eyes will start getting heavy. Although you might have acronym fatigue, DORA and NIS2 are on track to become two of the most important security legislative instruments in history, and they do not mean the same thing.
If both DORA and NIS2 intersect with what your organization does, understanding DORA vs NIS2 will be one of the most critical compliance questions you will face in the medium-term future.

Network and Information Systems Directive (NIS2)

Expanding Cybersecurity Frameworks:

NIS2 strengthens cybersecurity across essential sectors like energy, transport, health, and digital infrastructure, acknowledging the interconnected nature of modern threats.

Core Elements of NIS2

Proactive Risk Management:

Requirements: Entities must adopt proactive measures against evolving cyber risks.

Faddom's Contribution: Faddom's CVE detection and user access tracking enable rapid incident identification and reporting, aligning seamlessly with NIS2's stringent requirements.

Swift Incident Response:

Requirements: NIS2 mandates swift, comprehensive incident reporting to bolster response strategies.

Faddom's Contribution: Faddom's CVE detection and user access tracking enable rapid incident identification and reporting, aligning seamlessly with NIS2's stringent requirements.

Enhanced Security Standards:

Requirements: Higher security standards safeguard essential services against sophisticated cyber threats.

Faddom's Contribution: Real-time external traffic analysis and lateral movement detection by Faddom fortify the security posture of essential services, ensuring resilience in the face of adversity.

Supply Chain Resilience:

Requirements: NIS2 mandates rigorous supply chain security assessments to protect interconnected digital services.

Faddom's Contribution: Faddom enhances visibility into supply chain interactions with shadow IT detection and SSL insights, empowering organizations to manage risks effectively.

Accelerate Your Compliance Journey with Faddom:

Ready for NIS2 and DORA

At Faddom, we're committed to ensuring your organization stays ahead in the race to comply with NIS2 by October 2024 and DORA by January 2025. Recognizing the urgency and complexity of these regulatory landscapes, we've streamlined our efforts to offer swift and comprehensive support.

Rapid Implementation, Intuitive Platform:

Our self-service approach means you can deploy our agentless platform in less than one day, empowering you with advanced capabilities tailored for hybrid environments. From real-time, agentless dependency mapping to offline functionality, Faddom ensures seamless integration into your existing infrastructure.

Holistic Security Measures:

Faddom doesn't stop at asset discovery and dependency mapping. We equip you with crucial tools like CVE detection, North-South external traffic analysis, SSL Certificate Insights, User Access & Lateral Movement Detection, and Shadow IT Detection. These features fortify your cybersecurity posture, safeguarding your operations against evolving threats.

Your Trusted Partner in Compliance:

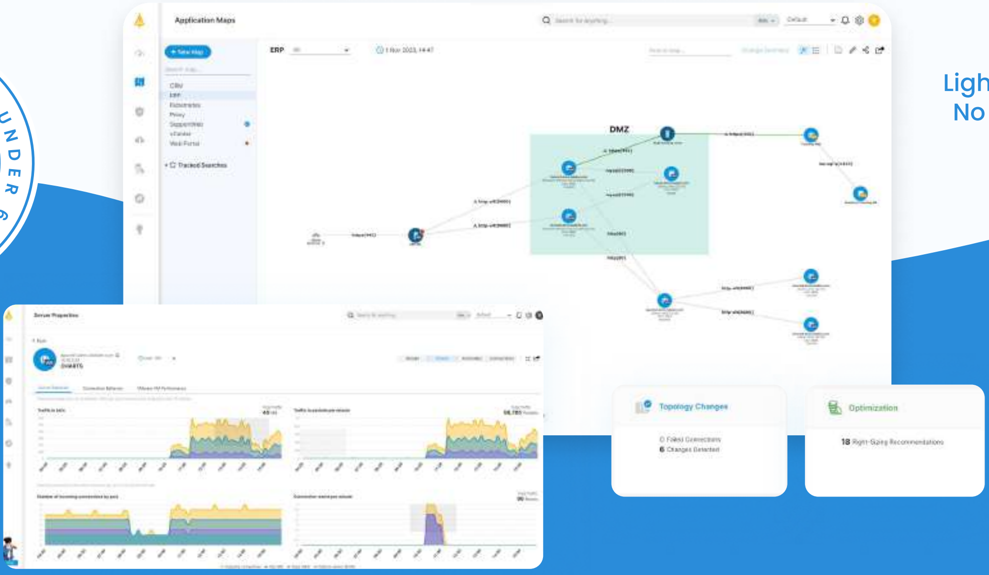
With Faddom by your side, compliance with NIS2 and DORA isn't just a checkbox—it's a strategic advantage. Trust us to deliver rapid implementation, robust security solutions, and unwavering support to keep your organization resilient and compliant in today's dynamic regulatory environment.

Get Ahead with Faddom

Contact us today and discover how Faddom can accelerate your compliance journey, ensuring you meet NIS2 and DORA requirements seamlessly. Let's navigate the future of cybersecurity together with confidence and innovation at every step.

GET YOUR FIRST MAP IN UNDER 60 MINUTES

60 MINUTES



Lightweight. No agents. No credentials. Works offline

Map all your dependencies within your network

About Faddom.com

Faddom is the fastest solution to discover all your IT infrastructure dependencies and map your business applications. Visualize your on-premises and cloud infrastructure in as little as one hour without agents. Instantly document all your servers and business applications, highlighting their interdependencies for an enhanced visibility posture. Our platform operates in real-time, automatically and continuously, with an offline mode as well. Faddom ensures unparalleled security and regulatory compliance for organizations worldwide, regardless of their size, budget, available resources, and manpower.