一、2026 年 3 月 3 日：首份《實施指南草案》深度解析

Prepared by Exein customer manager — NicolasHO

這份指南（Guidance）是歐盟委員會為了回應產業界對條文解讀不明的擔憂而發布的，目前正處於諮詢期。

1.「投放市場（**Placing on the Market**）」的數位化定義

過去 PDE 產品如何定義「首次進入歐盟市場」較為模糊。指南明確指出：

- 軟體下載即視為投放：只要軟體在歐盟境內可供下載，或透過雲端供用戶「遠端訪問」其核心功能，即視為投放市場。
- 更新版視為新產品：若軟體進行了「重大變更（Substantial Modification）」，則該更新版本需重新進行合規評估，不能沿用舊版的 CE 標誌。

2. 遠端數據處理（**Remote Data Processing**）的範疇

指南釐清了哪些「雲端服務」會被納入 CRA 監管：

- 功能不可分割性：如果 PDE 產品（如智慧攝影機）少了雲端 API 就無法運作，則該雲端服務必須符合 CRA 安全要求。
- 純代管服務豁免：若只是單純提供雲端儲存空間（如通用型 S3），則不屬於 CRA 的 PDE 範圍，而是適用 NIS2 指令。

3. 開源軟體管家（**OSS Stewards**）的減法管理

這對開源基金會（如 Apache, Linux Foundation）是重大更新：

- 責任減輕：指南確認「非營利」性質的開源開發者不承擔製造商責任，但「開源管家」須建立漏洞通報機制，並協助下游商業用戶。

二、(EU) 2025/2392 施行條例：精準的產品分類清單

這份於 2025 年 12 月 1 日發布的條例，將原本抽象的產品類別轉化為具體的技術定義。

1. 重要產品（**Important Products**）的細分

條例將 PDE 分為 Class I 與 Class II，這決定了廠商是否能「自我聲明」合規：

類別	技術定義範例	審核要求
Important Class I	瀏覽器、密碼管理員、防毒軟體、VPN 客戶端。	需遵循特定協調標準，或由第三方審核。

Important Class II	作業系統、管理程式（Hypervisors）、公鑰基礎設施（PKI）、路由器、防火牆。	強制第三方驗證。

2. 關鍵產品（Critical Products）的清單

這些產品由於具備「關鍵功能」且出問題會引發系統性風險，受到最高規格監管：

- 硬體安全模組（**HSM**）：包含支付終端機、加密金鑰儲存裝置。
- 智慧卡：用於身分認證或金融支付的晶片卡。
- 工業自動化系統：針對能源、交通等關鍵基礎設施所使用的 PLC 與控制軟體。

三、2026 年 9 月 11 日：迫在眉睫的「漏洞通報」大關

無論您的產品屬於哪一類，**2026** 年 **9** 月 **11** 日 是第一個「硬死線」。

強制通報流程細節：

1. **24** 小時內（早期預警）：一旦製造商察覺產品存在「已被積極利用」的漏洞，必須在 24 小時內通報至 單一報告平台（**SRP**）。
2. **72** 小時內（正式報告）：提供漏洞的詳細資訊、潛在影響以及初步緩解措施。
3. **14** 天內（最終報告）：說明修補程式（Patch）的可用性與修復細節。

專業提醒：即使您的產品是在 2027 年才需要貼 CE 標誌，只要該產品在 2026 年 9 月仍在市場上支援，您就必須履行這項漏洞通報義務。

四、給企業的行動建議

1. 審核 **SBOM** 機器可讀性：2026 年的指南強調 SBOM 必須符合 SPDX 或 CycloneDX 格式，建議現在就導入自動化生成工具。
2. 建立「**24** 小時通報」小組：2026 年 9 月的義務極其緊迫，企業需要預演如何在 24 小時內完成初步漏洞鑑定。
3. 重新檢視支援週期（**Support Period**）：指南要求製造商必須「顯著標示」支援終止日期。若產品支援少於 5 年，需準備好強大的合規理由（例如技術汰換過快）。

Cyber Resilience Act

The complete guide

exein

Index

1. The Cyber Resilience Act 3

2. The countdown has started 6

3. Navigating the CRA 7

4. Compliance made easy 14

1. The Cyber Resilience Act

What is the CRA

The EU's Cyber Resilience Act (CRA) is a legislative proposal that aims to revolutionize the security landscape.

By imposing robust cybersecurity standards, the CRA aims to strengthen the security of connected products and enable consumers to make informed choices about the security of the technology they use on a daily basis. This not only promotes a new playing field for EU and non-EU organizations, but ultimately paves the way for a safer digital marketplace for all.

The CRA has identified two main objectives to ensure the proper functioning of the internal market:

Creating conditions for the development of secure products

with digital elements by ensuring that hardware and software products are brought to market with fewer vulnerabilities, and ensuring that manufacturers take security seriously throughout the entire product lifecycle.

Creating conditions that enable users to consider cybersecurity

when selecting and using products with digital elements.

The need of being compliant

In response to this fast-evolving digital threat landscape, the European Union (EU) has identified that existing cybersecurity directives like NIS1/NIS2 and GDPR have limitations. While these regulations have been successful, they do not fully address the security needs of the increasingly large network of connected devices.

The Cyber Resilience Act (CRA) is a key measure to address these challenges. It specifically targets the security of connected devices, an area not adequately covered by previous legislation, thereby complementing the NIS2 Directive.

89%
of organizations
that operate and use IoT and connected products have faced cyber attacks in the past 12 months.

69%
of organizations
using or operating IoT devices have seen an increase in cyber attacks on their IoT devices over the past 36 months.

98%
of organizations
have experienced certificate outages in the last 12 months.

2.25
milion dollars
average cost to OEMs for outages on their production lines in the past 12 months.

Who is impacted by CRA

The Cyber Resilience Act (CRA) is a game-changer for cybersecurity in the EU market, with significant implications for businesses operating within the region.

This legislation primarily targets any devices with digital components. The aim is to establish a comprehensive set of requirements, ensuring these devices are built with security at the forefront from the very beginning.

Since the Act applies to all products sold within the EU market, regardless of the manufacturing location, it will also affect Original Equipment Manufacturers (OEMs) and their partners worldwide. This includes authorized representatives, resellers and distributors.
These entities will need to implement processes to verify that the products they handle comply with the CRA's regulations.

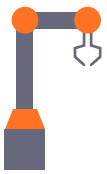
This collaborative approach across the entire supply chain will strengthen the overall security posture of the digital landscape within the EU.

Impacted markets

Smart Home

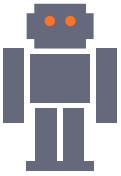
Automotive

Health Care



Manufacturers

Computer & Electronics



Robotics

Telco

Governance

IT Services

What happens if you don’t comply

If the company fails to meet CRA requirements the fine can reach 15 millions or an amount corresponding to 2.5% of the global annual turnover from the previous business year.
Furthermore, staggered measures from the competent authorities are also possible.

Level 1
An order may be issued to eliminate identified risks.

Level 2
Sale of product may be restricted or prohibited.

Level 3
Product recall.

2. The countdown has started

Deadline

September 2026
System in place to report issues

→

December 2027
Compliance with all requirements

September 2022
EU Commission pubblished the proposal for the CRA

December 2024
EU adopts the CRA

September 2026
Obligations to report incidents and disclose vulnerabilities are set to commence

December 2027
The new requirements will start to take effect

3. Navigating the CRA

Classifying your products under the CRA

The CRA employs a risk-based approach to classify Products with Digital Elements (PDEs) into categories with varying compliance requirements. Here's a breakdown of the classification system.

Important products with digital elements

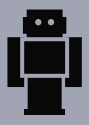
These products can fall into either Class I or Class II, depending on their function and associated risk.

Class I

Includes products that perform functions essential to the cybersecurity of other products or services, or pose a significant risk.

Examples:

Smart speakers



Internet connected toys

Smart home products with security features

Wearables

Network management systems

Router, modem & switches

Malware removal software

Operating systems

Standalone & embedded browsers

VPN servers & clients

Identity management systems

Password managers

Class II

Includes products that pose a higher risk, with the ability to adversely affect a large number of other products or the safety of users.

Examples:

Firewalls, intrusion detection & prevention systems

Tamper-resistant microprocessors & microcontrollers

Hypervisors & container runtime systems

Critical products with digital elements

These products typically belong to Class II, which represents the highest risk level.

Class II

Their compromise could have serious effects, such as the compromise of critical infrastructure or the breach of sensitive data.

Examples:

Hardware devices with safes

Smart meter gateway

Smart cards or similar devices

Meeting essential CRA security requirements

The CRA lists requirements in 3 main categories:

Essential security requirements

According to Article 5, products in scope of CRA must meet the essential requirements set out in Section 1 of Annex I.

Vulnerability handling requirements

According to Article 5 the processes put in place by the manufacturer must comply with the essential requirements set out in Section 2 of Annex I.

Reporting requirements

Manufacturers must report exploited vulnerabilities and incidents to national authorities via ENISA within 24 hours for early warnings and 72 hours for complete notifications when selecting and using products with digital elements.

Exein Platform: the go-to CRA Solution

Our platform goes beyond detection and response. Exein integrates a powerful Threat Intelligence module powered by generative AI.
This comprehensive resource provides readily accessible information and documentation related to your devices' security. By leveraging the latest threat intelligence, you can stay informed about emerging vulnerabilities and make proactive decisions to safeguard your devices throughout their lifecycle.
Exein provides a single, unified platform that empowers you to navigate the complexities of the CRA while ensuring the ongoing security of your connected devices. From pre-market assessments to real-time threat detection and response, Exein is your trusted partner in achieving and maintaining cyber resilience.

Essential security requirements

CRA	*Exein go-to solutions*
Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks;	*During development, Exein Analyzer builds a Software Bill of Materials (SBOM) to track components and identify vulnerabilities, while Runtime continuously monitors deployed devices for suspicious activity and has built-in incident response capabilities to automatically investigate and address potential threats.*
Products with digital elements shall be delivered without any known exploitable vulnerabilities;	*Exein Analyzer empowers manufacturers to proactively identify and eliminate potential security weaknesses throughout the entire product lifecycle.* *This includes pinpointing vulnerabilities within the product's firmware, ensuring a secure foundation from the very beginning.*
On the basis of the risk assessment referred to in Article 10(2) and where applicable, products with digital elements shall:	
be delivered with a secure by default configuration, including the possibility to reset the product to its original state;	*Analyzer manages the configurations that are delivered, and Runtime detects and responds when configurations are changed to make the system less secure.*
ensure protection from unauthorized access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems;	*Enhanced protection from unauthorized access can be obtained through Exein Runtime.* *Custom policies can be deployed to make sure only allowed users can perform any set of operations.*
protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms;	*Runtime can monitor and actively restrict access to both encrypted and plain files stored on the device (filesystem-monitor).*

protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorized by the user, as well as report on corruptions;	*Runtime can monitor and actively stop malicious or unauthorized programs from executing any action (process-monitor).*
protect the availability of essential functions, including the resilience against and mitigation of denial of service attacks;	*Exein Runtime is capable of detecting and effectively stopping in real time network-originated attacks such as DDoS or other brute force attacks (process-anomaly, network-anomaly).*
minimize their own negative impact on the availability of services provided by other devices or networks;	*By distributing an Exein Runtime detection and response agent on every product, we can effectively improve the security of the overall network and that of surrounding devices.*
be designed, developed and produced to limit attack surfaces, including external interfaces;	*Exein Analyzer can be used to outline the product software bill of materials and make sure that the attack surface is as reduced as possible.*
be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;	*Exein Runtime is designed specifically to act on the most granular level possible. When an incident is detected, a response action (threat-response) can be taken to prevent the specific malicious process from continuing its anomalous operations, leaving the rest of the system intact and fully operational.*
provide security related information by recording and/or monitoring relevant internal activity, including the access to or modification of data, services or functions;	*Exein Runtime collects and exports in real time all the activity related to security incidents.* *This includes all the logs that might be helpful to perform a post-mortem and forensic analysis.*

Vulnerability handling requirements

CRA	*Exein go-to solutions*
Identify and document vulnerabilities and components contained in the product, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the product;	*Exein Analyzer is designed specifically for this purpose, among other things. It automates various product security functions to support SBOMs and vulnerability lists via workflow automations to update SBOMs and generate reports to give greater context to a device's risk.*
In relation to the risks posed to the products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates;	*Exein Runtime allows manufacturers to immediately find out about new security breaches in their products, significantly shortening the time required to notify the authorities and the users and releasing a security update, lowering in this way the amount of damage caused by the attack*
Once a security update has been made available, publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and information helping users to remediate the vulnerabilities;	*Exein Runtime AI enables manufacturers to grasp the extent and origin of a security incident. However, the manufacturer is responsible for disclosing any vulnerabilities.*
Provide for mechanisms to securely distribute updates for products with digital elements to ensure that exploitable vulnerabilities are fixed or mitigated in a timely manner;	*Exein solutions allow you to immediately find out if any new vulnerability affects an existing product and mitigate its effect.*

Reporting requirements

CRA

The manufacturer is expected to report vulnerabilities to ENISA. There are no specific requirements as to the format or tool to use, as this may differ between EU member states

Exein go-to solutions

Exein reports are designed to meet the ENISA strict reporting requirements. This means you can report actively vulnerabilities and security incidents to the competent national authorities within the mandated timeframes: 24 hours for initial notification and 72 hours for the full report.

4. Compliance made easy

Our solutions in a nutshell

Exein Analyzer: Pre-Market security assessment
Exein Analyzer eliminates the guesswork from pre-market security assessments. This powerful tool utilizes advanced security technology to scan your devices and identify potential vulnerabilities. Unlike traditional methods, Exein Analyzer doesn't require access to firmware source code or installation of agents or SDKs, streamlining the process and minimizing disruption to your development workflow. With a comprehensive overview of your device's security landscape in hand, you can address vulnerabilities proactively, ensuring compliance with the CRA and fostering trust with your customers.

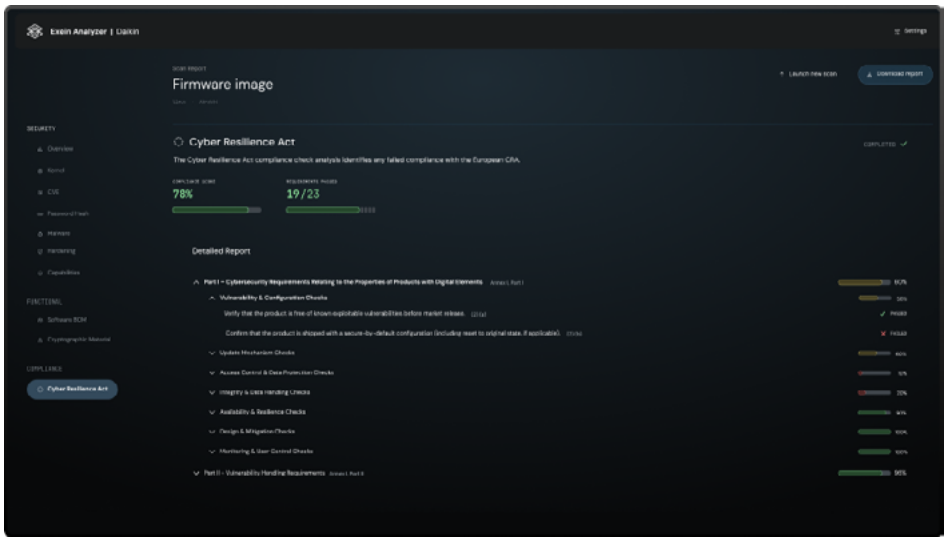
No Source Code Required
Analyze firmware directly, eliminating the need for source code access. This accelerates the vulnerability assessment process and streamlines the development workflow.

Effortless Deployment
With no agents or SDKs to install, Exein Analyzer ensures quick and seamless deployment, reducing time-to-market.

Broad Compatibility
Supports multiple systems, such as Linux, RTOS, UEFI, Docker, Android, and Uboot, ensuring security across various IoT environments.

Comprehensive Scanning
Exein Analyzer conducts extensive scans of IoT fleets to detect a wide array of threats, including weak passwords, potential exploitations, common vulnerabilities and exposures (CVEs), insecure compiler settings, and compromised cryptographic certificates.

Detailed Reporting
Generates clean, exportable reports that summarize key vulnerabilities and prioritize issues for efficient resolution, enabling focused and effective security management.



Exein Runtime: Real-Time threat detection
Exein goes beyond pre-market assessments, offering real-time protection for your deployed devices. Our flagship product, Exein Runtime, is a state-of-the-art solution specifically designed for Linux and RTOS systems.
This comprehensive suite provides a robust defense against cyberattacks, meeting the rigorous security standards outlined by the CRA.

Runtime Threat Detection & Response
Identifies and blocks external attacks in real-time, supporting any platform from Docker to RTOS.

Filesystem Activity Monitoring
Tracks and blocks suspicious filesystem activity with path-based rules, ensuring continuous oversight of critical file operations.

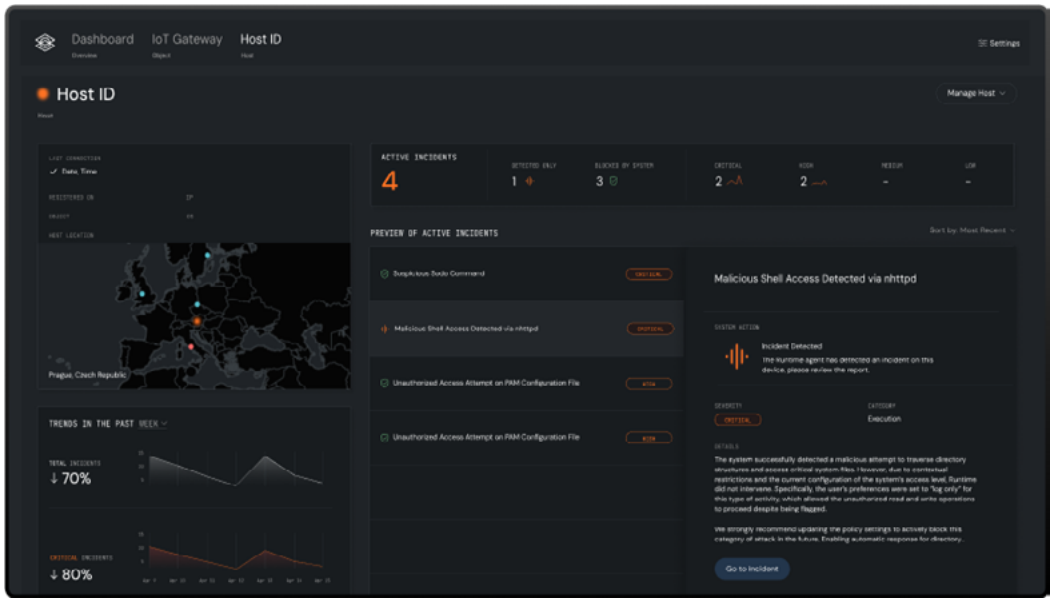
Network Threat Detection
Monitors network connections, socket operations, and DNS packet parsing to detect and immediately respond to network threats.

Process Activity Monitoring
Provides deep insights into running processes, including creation, execution, and termination, as well as behavioral changes.

Comprehensive Threat Intelligence
Aggregates threat intelligence from all devices, providing a global view of runtime security.

AI Enhanced Security
Utilizes advanced AI models to provide insights during security incidents, including potential scope, cause, and recommended mitigation actions.

Exportable Events
Allows the export of security events to any SIEM of choice, enabling flexible analysis and response within existing workflows and tools.



Exein's role in aligning solutions with the CRA

Exein's solution's play a pivotal role in ensuring compliance with the upcoming Cyber Resilience Act, an EU-wide legislation aimed at safeguarding consumers and businesses from digital products with inadequate security features.
The act mandates cybersecurity requirements for digital products throughout their lifecycle, emphasizing the security of connected devices and software across the EU.

Understanding Obligations

Exein's solutions are designed to meet the strict requirements outlined in the Cyber Resilience Act, providing companies with the confidence to fulfill each obligation effectively

Effortless Compliance Journey

With Exein, it's easy to effortlessly navigate the path to comliance, ensuring all necessary steps for reporting vulnerabilities and incidents are seamlessly integrated into operational processes.

Enhanced Product Security

Exein's advanced security features not only protect digital products but also enhance their overall security profile, aligning with the Act's goal of ensuring more secure digital products for EU consumers.

Our team of experts will work with you to understand your project requirements and provide a proof of concept (POC) that is entirely free of charge.

During the POC, we will discuss how our technology can help solve your security problems and provide an opportunity to see it in action.

Contact us at info@exein.io
Learn more at www.exein.io