SECURE
Cyber Resilience for SMEs

SECURE Project
(Strengthening EU SMEs Cyber Resilience)

Webinar – Assolombarda

12 March 2026

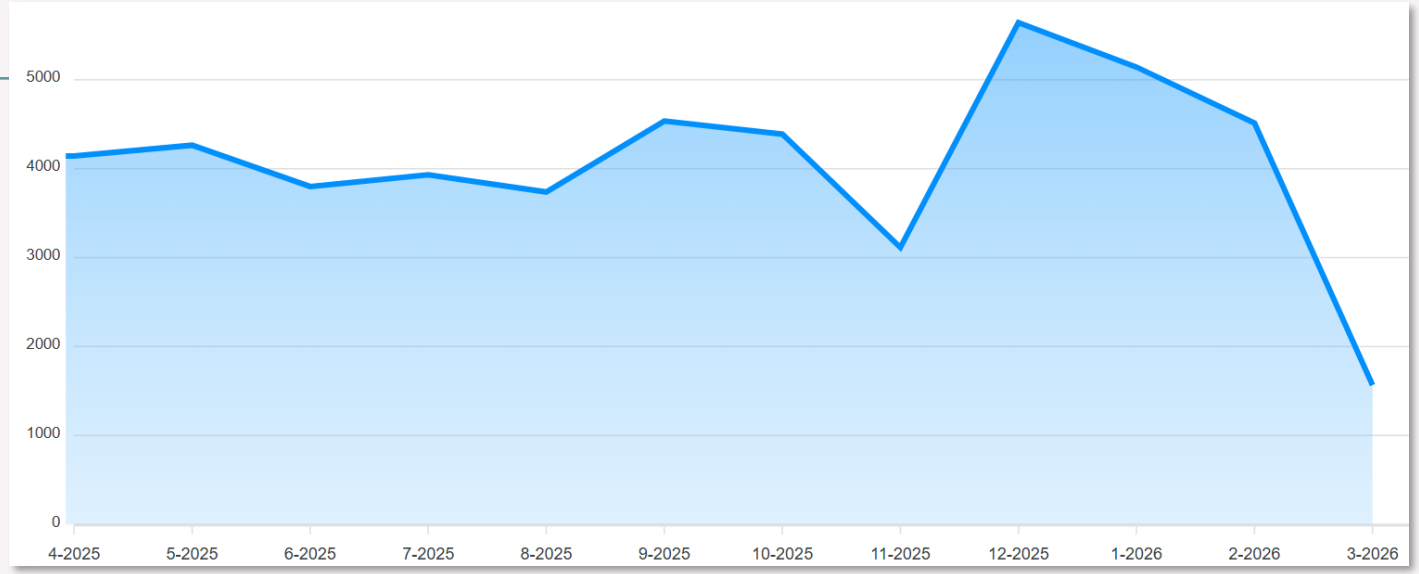
Danilo D'Elia, SECURE
project coordinator

Il contesto del CRA in termini di vulnerabilità ed esposizioni

Il CRA introduce obblighi stringenti per i produttori, tra cui la segnalazione degli incidenti legati alle vulnerabilità e la valutazione del loro impatto, al fine di analizzare i rischi in corso.

- **Aggiornamenti di sicurezza tempestivi** e **documentazione chiara**, in linea con i requisiti di conformità del CRA.
- **Classificazione dei prodotti in categorie di rischio**, con requisiti normativi più rigorosi per quelli a rischio più elevato.

CVE creati mensilmente (Common Vulnerabilities and Exposures) da aprile 2025 all'inizio di marzo 2026



Nel **febbraio 2026** sono stati creati **4.513 CVE**
Fonte: CVE FIND

PMI nel campo di applicazione

Produttori di prodotti con componenti digitali (ad es. produzione di componenti elettronici, computer e apparecchiature periferiche, apparecchiature di comunicazione ed elettronica di consumo)

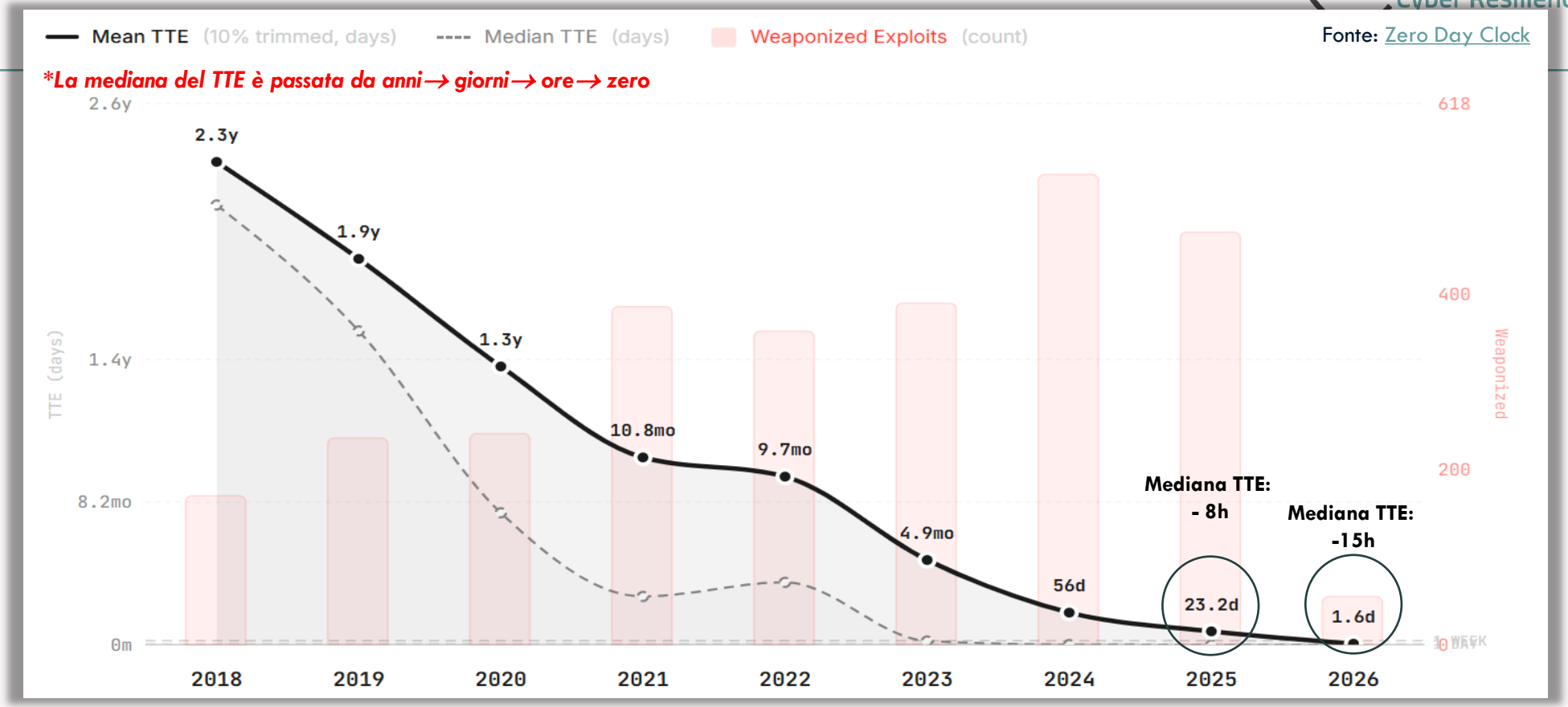
Fornitori di strumenti e soluzioni per la conformità al CRA (ad es. consulenza IT, servizi di cybersecurity, soluzioni software per la conformità, servizi di protezione dei dati e della privacy, e servizi di formazione)

Altre categorie adeguatamente giustificate in linea con il CRA (ad es. distribuzione e importazione di tecnologie, sviluppo di software open-source, servizi di consulenza normativa, organismi di standardizzazione in cybersecurity, servizi di infrastrutture digitali)

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Cronologia da vulnerabilità a sfruttamento (2018-2026)

SECURE
Cyber Resilience for SMEs



Secondo la metodologia Zero Day Clock, gli attacchi zero-day si verificano quando il Time-to-Exploit (TTE) è "zero" o negativo, **cioè quando lo sfruttamento avviene contestualmente o prima della divulgazione pubblica.**

La Mediana del TTE è crollata, con lo snapshot del 2025 che mostra: **– 8 ore di mediana TTE* e 471* exploit "weaponizzati" registrati**
→ Di conseguenza, gli exploit vengono sempre più spesso sviluppati automaticamente, non lasciando ai difensori quasi alcun tempo di reazione.

***Tutte le metriche si basano su fonti affidabili (CISA KEV, VulnCheck KEV, VulnCheck XDB) ed escludono exploit assegnati retroattivamente o corrotti, in linea con la metodologia.**

SECURE - Strengthening EU SMEs Cyber Resilience Project

SECURE
Cyber Resilience for SMEs

Coordinator:
- Agenzia per la Cybersicurezza Nazionale (ACN)

Partners:
- Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy (NASK, Poland)
- Instituto Nacional de Ciberseguridad de España – INCIBE (Spain),
- Centre for Cybersecurity Belgium – CCB (Belgium)
- Luxembourg House of Cybersecurity – LHC (Luxembourg),
- Associazione Cyber 4.0 (Italy)
- Autoritatea pentru Digitalizarea României – ADR (Romania),
- Industrie 4.0 Österreich – Plattform für Intelligente Produktion (PIA, Austria).

Project Scope

Reinforce the *cybersecurity resilience* of European micro, small and medium-sized enterprises (mSMEs) by helping them comply with the requirements of the ***Cyber Resilience Act (CRA) -*** *Regulation (EU) 2024/2847*, through the launch of Open Calls for financial support.

Project Total Budget

EUR 16,5 Million

Number of Open Calls in the next years

At least 2

Target Applicant

EU and EEA Micro, Small and Medium Enterprises

Funded by the European Union

1st Open Call General Information

SECURE
Cyber Resilience for SMEs

Financial support for mSMEs to **co-finance mini-projects** (activities, goods and services) aimed at strengthening cyber resilience and achieve the compliance with the Cyber Resilience Act.

Open Call Operational Information

Call Launch Date
28/01/2026

Call Deadline
29/03/2026

Language
ENGLISH

Grant Type
LUMP SUM Funding
(no mandatory financial reporting)

Budget and Cofinancing

Call Total Budget
EUR 5,000,000

Projects Cofinancing Rate
50%

Prefinancing (optional)
Max. 40% of the grant

Maximum Grant
EUR 30,000

The Ceiling applies also to projects with total eligible costs higher than EUR 60.000

All Relevant Call Documents will be shared today on the website

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Reporting Methods & Eligible Costs

SECURE
Cyber Resilience for SMEs

Lump Sum Funding Mechanism

Not Needed

Actual Cost Reporting at any stage of the project

Needed

- Breakdown of estimated eligible costs by budget category
- Evidences for the achieved objectives

The Cost esteem will be used during the Proposal Evaluation to assess the consistency of the project activities with the expected costs

Eligible Costs *(can be co-financed)*

Direct Costs

- **Personnel Costs** - *Employees; natural persons direct contracts; seconded persons; SME owner and natural person beneficiary.*
- **Subcontracting costs** - *service providers, consultancy etc. – Must be registered in EU or EFTA MS; not controlled by countries outside EU/EFTA.*
- **Equipment** - *max 80% of direct costs; only for the shared cost corresponding to the actual rate of use during project duration*
- **Purchase cost** - *consumable and supplies, promotion, dissemination, results protection, publications, certificates etc.*

Indirect Costs

Flat rate of 7% of the total eligible costs (included in the max. financing of EUR 30,000)

Ineligible costs *(cannot be cofinanced)*

Return on capital, debt and debt service charges, provisions for losses or debts, interest owed, currency exchange losses, excessive or reckless expenditure, costs already funded by another EU action, alcoholic beverages, gifts or entertainment expenses, travel costs

Call Eligibility Requirements

1. Company Eligibility Criteria

- The Applicant is an individual entity
- The Applicant is a mSME (*https://eur-lex.europa.eu/eli/reco/2003/361/oj/eng*)
- The Applicant is established in one of the eligible countries (EU + EEA)
- The applicant meets all the ethical and legal requirements (only self dec.)
- Absence of double funding (only self dec.)

2. CRA-Related Eligibility Criteria

Applicants CRA scope Requirements: Applicants must operate in a sector or have business activity that falls within the CRA scope and regulatory framework or demonstrate willingness to do so

Eligible Activities: only projects aimed at achieving compliance with CRA will be accepted

Who Can Apply? 1/3
Company Eligibility Criteria

SECURE
Cyber Resilience for SMEs

All eligibility criteria must be met to apply for the call

1

Individual Entities

Eligible Organizations

- Single organization with legal personality acting independently in its own name
- Self employed persons (i.e: sole traders)
- Associations and interest groupings with legal personality (only as sole beneficiaries)

Exclusions

- Consortia, business networks or joint applications
- Natural Persons (except for self-employed persons - i.e: sole traders)
- International Organizations
- Entities without a legal personality
- EU bodies
- Other special cases (see Annex 1)

2

mSMEs Definition

Enterprise category	Headcount: annual work unit (AWU)	Annual turnover	or	Annual balance sheet total
Medium-sized	< 250	≤ EUR 50 million	or	≤ EUR 43 million
Small	< 50	≤ EUR 10 million	or	≤ EUR 10 million
Micro	< 10	≤ EUR 2 million	or	≤ EUR 2 million

For Partner & Linked enterprise definition please visit: https://op.europa.eu/en/publication-detail/-/publication/79c0ce87-f4dc-11e6-8a35-01aa75ed71a1

3

Geographical Eligibility

Company HQ or Branch for which the financing is requested & UBO Nationality shall be EU + EEA

4

Legal and ethical Requirements

e.g: no conviction by final judgment for fraud, corruption; no guilt of professional misconduct …

5

No Double Funding

Submitted project must not be subject to double funding

Who Can Apply? (2/3)
Applicants CRA-Related requirements

SECURE
Cyber Resilience for SMEs

Economic operators under CRA Scope

Manufacturers

Importers

Distributors

Open-source software stewards

OF

Products with digital elements (PDEs) – Focus of CRA Category within the first Open Call

Category	Brief Meaning	Compliance Procedure	Example Products
Default Products	Low-risk PDEs (~90% of total), general consumer or office devices	Internal self-assessment leading to an EU declaration of conformity	Standard printers, USB drives, office productivity software, smart speakers, connected light bulbs, fitness trackers

Based on the adoption of implementing acts by European Commission specifying technical descriptions of categories of products with digital elements, the next Open Calls will be focused also on:

- Important Products (Class I and II)
- Critical Products

ADMISSIBLE COMPANIES: the Applicant Company falls, may fall or will fall under the CRA Scope based on the CRA Regulation (Regulation-EU 2024/2847)

Who Can Apply? (3/3)
Eligible Activities & Other EU Projects

SECURE
Cyber Resilience for SMEs

Category 2: *CRA Cybersecurity Governance, Risk Management and Compliance Assessment – Modules 1, 2 and 3*

Category 3: *CRA requirements training*

Category 4: *CRA-related cybersecurity trainings*

Category 5: *Expertise support in the CRA conformity project execution*

Category 6: *Vulnerability tests*

Category 7: *Laboratory tests*

Category 8: *Penetration tests*

Category 10: *CRA self-assessment tool*

Category 11: *Software Development – Security by Design for CRA Products*

Category 12: *Business Continuity, Incident and Response Planning for CRA Products and Processes*

Category 13: *Supply Chain Risk & Security Assessment*

Category 14: *Data Protection & Privacy Compliance*

Category 16: *Monitoring, protection and prevention services and tools*

SECURE is building **synergies with other CRA implementation DEP projects**.
Tools developed under these linked projects will be made available to mSMEs to support eligible activities under the cascade funding scheme.

Category 1: Accredited trusted third-party audit with the CRA certificate

Category 9: CRA third-party assessment service

Category 15: CRA Regulatory Obligations and Documentation Support

→ **Out of Call 1 Scope due to lack of CRA Certification Schemes**

Technical Evaluation Criteria

Individual Evaluation Parameters

SECURE
Cyber Resilience for SMEs

Evaluation Committee will assess the proposal scores by **individual evaluation** and though **Consensus Meetings.**

There will be at least 3 evaluators for each single proposal

Individual evaluations will refer to the following parameters.

CRITERIA	Focus
Excellence and Relevance	1. *Relevance to EU cybersecurity goals on CRA* 2. *Project objectives and methodology* 3. *Resources and capabilities*
Impact and Clarity	1. *Expected outcomes for the SME* 2. *Clarity of Description* 3. *Indicators and KPIs to measure success*
Implementation	1. *Work Packages (WP)* 2. *Deliverables, Evidences and cost consistency* 3. *References to other EU Projects*

Score	Evaluation
0 = N/A	Proposal fails to address the criterion or cannot be assessed due to missing or incomplete information.
1 = Poor	Criterion is inadequately addressed or there are serious inherent weaknesses.
2 = Fair	Proposal broadly addresses the criterion, but there are significant weaknesses.
3 = Good	Proposal addresses the criterion well, but shortcomings are present.
4 = Very good	Proposal addresses the criterion very well, with only minor shortcomings.
5 = Excellent	Proposal successfully addresses all relevant aspects of the criterion; shortcomings are negligible.

Funded by the European Union
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

*Related Call Official Document = **ANNEX 1 - Open Calls Application Guidelines***

Contacts and Other Information

- **WEBSITE**: https://www.secure4sme.eu/about-secure
- **FAQ**: https://www.secure4sme.eu/faq
- **For questions on Open Calls please contact**: submission-support@secure4sme.eu
- **For other questions** (CRA Regulation, SECURE project, Other EU Projects, Dissemination, Events, etc.) **please contact**: info@secure4sme.eu
- **Online Contact Form:** https://www.secure4sme.eu/contacts
- **Newsletter**: https://www.secure4sme.eu/newsletter
- **News and Events:** https://www.secure4sme.eu/news-events
- **National (Cybersecurity) Coordination Centres**: https://cybersecurity-centre.europa.eu/nccs_en

Funded by the European Union

SECURE
Cyber Resilience for SMEs

Thank you!

Website: www.secure4sme.eu

Contact Mail: info@secure4sme.eu

Linked In

Youtube

Funded by the European Union

EU Funding Statement: Funded by the European Union under GA No 101190325. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Cybersecurity Industrial, Technology and Research Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

ECCC disclaimer: The project is supported by the European Cybersecurity Competence Center and its members.