

Impact of malicious use of Open-Source Intelligence on critical infrastructure business continuity

Horizon Europe

● IN ATTESA

Codice

HORIZON-CL3-2027-01-INFRA-02

Ambito

Internazionale

Località

Europa

Curatore

Marlene Faria

DETTAGLI FINANZIARI

Tipo di supporto

Fondo perduto

Intensità Massima di Aiuto

100%

Budget

7.7M€

Valore di Progetto Ammissibile

3.8M€ - 3.8M€

DATE E SCADENZE

Data di Pubblicazione

12 dicembre 2025

Data di Apertura

5 maggio 2027

Deadline

4 novembre 2027 alle ore 17:00 GMT+1

DESCRIZIONE

Objectives

This call aims to enhance the security and resilience of critical infrastructure in the EU by addressing the risks posed by the malicious use of Open-Source Intelligence (OSINT). The objective is to improve awareness among critical infrastructure operators and authorities about OSINT threats, develop advanced tools for OSINT mapping and risk analysis, and strengthen incident response and business continuity planning. The call also seeks to support the removal of harmful OSINT from the public domain and to develop awareness campaigns and training for employees of critical entities. Eligible applicants include consortia with at least three relevant practitioners from EU Member States or Associated Countries, representing critical infrastructure operators, authorities responsible for resilience, or law enforcement/private security companies. Entities established in China or controlled by Chinese entities are not eligible.

Funding

The support is provided as a non-refundable grant under the Horizon Innovation Actions (IA) scheme. The funding rate is up to 70% of eligible costs for most participants, and up to 100% for non-profit legal entities. The total budget for the topic is €7.67 million, with an expected EU contribution of €3.835 million per project and two grants anticipated. Eligible costs are reimbursed as a lump sum.

SPESE AMMISSIBILI

- Personnel Costs
- Travel costs
- Equipment costs
- Other goods, works and services costs
- Subcontracting
- Indirect Costs

BONUS E MAGGIORAZIONI

- Up to 100% funding rate for non-profit legal entities
- Mandatory involvement of at least 3 relevant practitioners from EU/Associated Countries
- Synergy-building and clustering with other relevant projects encouraged

IDONEITÀ

Modalità di Candidatura
Aggregata / Partenariato

Settori Idonei

- Energia e Ambiente
- ICT e Software
- Logistica
- Altro

Tipologie Aziendali

- Microimpresa
- PMI
- Small Mid-Cap
- Mid-Cap
- Grande impresa
- Enti privati non profit
- Enti pubblici

Tipi di Azione

- Development of OSINT mapping and risk analysis tools
- Analysis of publicly available information for hostile operations
- Development of awareness campaigns and training curricula
- Incident response and business continuity model improvement
- Removal of harmful OSINT from public domain
- Integration and optimisation of existing security tools
- Engagement with Europol Innovation Lab for validation
- Consideration of AI data processing implications for OSINT misuse
- Development of tools to counter hybrid and lone wolf threats

DETTAGLI PROGRAMMA UE

ID Bando

HORIZON-CL3-2027-01-INFRA-02

Cluster

Cluster 3: Civil Security for Society

Destinazione

D3. Resilient Infrastructure

Modalità di Presentazione

single-stage

Contributo UE

€3,835,000.00 per project

Progetti Previsti

2

Regola dell'Intensità di Aiuto

Up to 70% of eligible costs for Innovation Actions (IA); up to 100% for non-profit legal entities

LINK UFFICIALI

Regolamento Ufficiale

<https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/HORIZON-CL3-2027-01-INFRA-02>

Pagina Grantavia

<https://grantavia.com/it/incentives/impact-of-malicious-use-of-open-source-intelligence-on-critical-infrastructure-business-continuity>

Video Informativo

<https://www.youtube.com/shorts/46sBAgRpL5o>

Prenota un incontro

<https://bookings.cloud.microsoft/book/Prenotaunappuntamento@epsa.com/?ismsaljsauthenabed>