Continuum informatico sicuro (IoT, Edge, Cloud, spazi dati)

Secure Computing Continuum (IoT, Edge, Cloud, Dataspaces)

TOPIC ID: HORIZON-CL3-2023-CS-01-01

Ente finanziatore: Commissione europea. Programma Horizon Europe

Obiettivi ed impatto attesi: Risultati attesi:
- Strumenti per supportare la resilienza, la preparazione, la consapevolezza e il rilevamento della cybersecurity all'interno delle infrastrutture critiche e delle catene di fornitura;
- mitigazione delle vulnerabilità delle infrastrutture cloud;
- integrazione sicura dell'IoT non attendibile in ambienti attendibili; - utilizzo di architetture Zero-Trust;
- fiducia e sicurezza per ecosistemi IoT connessi di massa e gestione del ciclo di vita;
- interoperabilità e integrazione sicure dei sistemi; - strumenti di automazione basati sull'intelligenza artificiale per l'intelligence delle minacce informatiche;
- infrastrutture sicure, identità sicure e usabilità per una catena di sicurezza che copre la comunicazione, la raccolta dei dati, il trasporto dei dati e l'elaborazione dei dati.

Ambito di applicazione: L'evoluzione della nostra società interconnessa comporta molteplici livelli di piattaforme cloud, edge computing e IoT che interagiscono continuamente tra loro. Tuttavia, questo ecosistema sempre connesso e popolato da entità potenzialmente vulnerabili richiede meccanismi di protezione avanzati, intelligenti e agili per gestire la sicurezza e la privacy dei singoli componenti durante il loro ciclo di vita e dei sistemi complessivi.
La complessità di questi ambienti interconnessi sottolinea la necessità di rilevare, analizzare e mitigare in modo proattivo e automatizzato gli attacchi di cybersecurity nel cloud, nell'edge, nelle implementazioni OT, IoT e in domini applicativi come, ad esempio, le smart city.
L'integrazione della sicurezza end-to-end e della privacy incentrata sull'utente in piattaforme distribuite complesse richiede un lavoro per affrontare le minacce alla sicurezza e le vulnerabilità nell'intero ecosistema della piattaforma. È incoraggiata l'identificazione e l'analisi di potenziali aspetti normativi e barriere per le tecnologie/soluzioni sviluppate, se pertinenti.

Criteri di eleggibilità: Per essere ammissibili, i richiedenti (beneficiari ed enti affiliati) devono:
-essere soggetti giuridici (enti pubblici o privati) avere sede in uno dei Paesi ammissibili, ovvero Stati membri dell'UE (compresi i Paesi e territori d'oltremare (PTOM)) Paesi non UE:
– Paesi SEE elencati e Paesi associati o Paesi che hanno in corso negoziati per un accordo di associazione e in cui l'accordo entra in vigore prima della firma della sovvenzione (elenco dei Paesi partecipanti)
– Paesi in via di adesione,
I beneficiari e gli enti affiliati devono iscriversi al Registro dei partecipanti – prima di presentare la proposta – e dovranno essere convalidati dal Servizio centrale di convalida (REA Validation). Per la convalida, sarà loro richiesto di caricare documenti che dimostrino lo status giuridico e l'origine.

Alcune attività derivanti da questo argomento possono comportare l'utilizzo di informazioni classificate e/o la produzione di risultati sensibili dal punto di vista della sicurezza (EUCI e SEN). Si rimanda alle relative disposizioni della sezione B Sicurezza - Informazioni classificate e sensibili dell'UE degli allegati generali.

Contributo finanziario: La Commissione stima che un contributo UE compreso tra 4,00 e 6,00 milioni di euro consentirebbe di affrontare adeguatamente questi risultati. Tuttavia, ciò non preclude la presentazione e la selezione di una proposta che richieda importi diversi. Budget indicativo
Il budget totale indicativo per il tema è di 28,00 milioni di euro. Tipo di azione Azioni di innovazione (IA).

Scadenza: 23 Novembre 2023 17:00:00 Brussels time

Ulteriori informazioni:
wp-6-civil-security-for-society_horizon-2023-2024_en.pdf (europa.eu)
pag. 103