Analisi avanzata dei dati in tempo reale per la resilienza delle infrastrutture

Advanced real-time data analysis used for infrastructure resilience

TOPIC ID:
HORIZON-CL3-2024-INFRA-01-03

Ente finanziatore:
Commissione europea
Programma
Programma quadro Horizon Europe (HORIZON)

Obiettivi ed impatto attesi:
I risultati dei progetti dovrebbero contribuire ad alcuni o a tutti i seguenti risultati:
· Migliori capacità di identificazione dei rischi e degli eventi difettosi nelle reti infrastrutturali e nelle città intelligenti attraverso l'analisi in tempo reale (compresi i big data) da parte di attori pubblici e privati tramite piattaforme sicure e affidabili e sistemi interconnessi in cui la collaborazione segue quadri giuridici e politici chiari;
· Strumenti e processi per facilitare gli sforzi degli stakeholder nell'identificare, analizzare, valutare e monitorare continuamente i rischi e aumentare la capacità di adattamento agli eventi inattesi in anticipo, consentendo l'analisi di varie fonti di dati (ad esempio audio, video, social media, contenuti web, informazioni spaziali, dati generati da sensori o macchine);
· Identificazione, classificazione e tracciamento rapidi e continui in tempo reale di agenti pericolosi, contaminanti o anomalie nelle reti infrastrutturali e nelle catene di fornitura;
· Interfacce interoperabili e una migliore collaborazione tra i sistemi di rilevamento delle operazioni infrastrutturali e di risposta, i centri di gestione/coordinamento del rischio nazionali/UE e le attrezzature di primo soccorso, al fine di consentire operazioni a distanza sulla scena, tenendo conto delle conoscenze dei cittadini;
· Aumento della cyber-resilienza delle reti industriali xG e dei dati cloud che coprono domini infrastrutturali specifici
· Migliore capacità di mappare in tempo reale la fonte (o le fonti) dei fattori di rischio che potrebbero mettere in pericolo l'infrastruttura di rete supportata dall'osservazione della Terra e dai dati di geolocalizzazione. Se l'analisi comprende l'elaborazione di dati personali, si dovrebbe considerare di includere una valutazione del rischio o dell'impatto sulla privacy degli individui e della società.
Ambito di applicazione:
La società odierna è più interconnessa che mai. Le reti di telecomunicazione, le reti di trasporto, l'aviazione, l'energia, le reti idriche e la finanza sono la spina dorsale della società odierna. A causa della loro eccezionale complessità e dimensione, le reti infrastrutturali rappresentano una sfida specifica quando si tratta di identificare i diversi rischi, sia informatici che fisici. Soprattutto nel dominio cibernetico, molte intrusioni o attacchi rimangono inosservati o vengono rilevati relativamente tardi. Gli sviluppi

tecnologici in aree come l'apprendimento automatico per l'analisi, le interfacce utente e le applicazioni di archiviazione hanno il potenziale per migliorare le relative capacità.
I moderni ambienti urbani e le infrastrutture interconnesse creano costantemente grandi quantità di dati. Inoltre, altre fonti possono essere sfruttate per supportare l'identificazione e l'analisi dei rischi per le infrastrutture. Pertanto, la ricerca sul miglioramento dell'anticipazione dei rischi attraverso l'analisi dei dati in tempo reale può potenzialmente portare a strumenti utili per migliorare la preparazione (piani di emergenza, esercitazioni basate su scenari, allocazione delle risorse, ecc.)
La resilienza delle città intelligenti è caratterizzata da una serie di requisiti specifici che tengono conto soprattutto degli aspetti dell'integrazione, considerando gli approcci incentrati sull'utente e gli aspetti sociali ed etici dell'Industrial Internet of Things (IIoT), gli approcci di AI/Machine Learning per l'analisi dei dati in tempo reale, la garanzia di trasparenza, la conoscenza sufficiente e le sfide operative in questo settore.
Se da un lato la disponibilità di grandi quantità di dati provenienti da fonti diverse offre il potenziale per migliorare l'identificazione dei possibili rischi per le infrastrutture, dall'altro aumenta la richiesta di strumenti analitici veloci e resistenti. È necessario filtrare le informazioni per identificare i dati rilevanti come indicatori di rischio e, dato l'elevato numero di forme diverse di attacchi o intrusioni informatiche, anche stabilire un ordine di priorità e decidere in base al grado di pericolo che presentano. Ciò implica la necessità di abbinare i dati al contesto appropriato e di verificarne la fonte, al fine di garantire che vengano analizzati solo i dati pertinenti, evitando così falsi risultati. Una più rapida identificazione e localizzazione di agenti pericolosi e contaminanti all'interno delle reti infrastrutturali è fondamentale per consentire una risposta rapida, informare e coinvolgere i cittadini e i residenti ed evitare danni su larga scala in caso di incidente. Tali capacità di identificazione possono essere implementate come parte dell'infrastruttura e integrarsi con i sistemi utilizzati dalle autorità pubbliche per garantire che le informazioni siano disponibili il prima possibile. Inoltre, è fondamentale sviluppare metodi per una migliore cooperazione tra i diversi attori, per garantire una comprensione e un'interpretazione comune dei dati e per fornire strumenti interattivi per lo scambio e la visualizzazione a supporto delle decisioni. A questo proposito è essenziale la cooperazione tra i diversi attori pubblici e privati.
Questo tema richiede il contributo efficace delle discipline SSH e il coinvolgimento di esperti SSH, delle istituzioni e l'inclusione di competenze SSH rilevanti, al fine di produrre effetti significativi e significativi che rafforzino l'impatto sociale delle relative attività di innovazione.
Condizioni specifiche dell'argomento:
Si prevede che le attività raggiungano il TRL 5-6 entro la fine del progetto – si veda l'Allegato generale B.

Criteri di eleggibilità:
Qualsiasi soggetto giuridico, indipendentemente dal suo luogo di stabilimento, compresi i soggetti giuridici di Paesi terzi non associati o di organizzazioni internazionali (comprese le organizzazioni internazionali di ricerca europee) può partecipare (indipendentemente dal fatto che sia idoneo o meno al finanziamento), a condizione che siano state soddisfatte le condizioni stabilite dal regolamento Horizon Europe e qualsiasi altra condizione stabilita nel tema specifico del bando. Per "soggetto giuridico" si intende qualsiasi persona fisica o giuridica costituita e riconosciuta come tale ai sensi del diritto nazionale, del diritto dell'UE o del diritto internazionale, dotata di personalità giuridica e che può, agendo in nome proprio, esercitare diritti

ed essere soggetta a obblighi, oppure un soggetto privo di personalità giuridica.
I beneficiari e gli enti affiliati devono registrarsi nel Registro dei Partecipanti prima di presentare la domanda, per ottenere un codice di identificazione del partecipante (PIC) ed essere convalidati dal Servizio Centrale di Convalida prima di firmare la convenzione di sovvenzione. Per la convalida, durante la fase di preparazione della sovvenzione, verrà chiesto loro di caricare i documenti necessari che dimostrino il loro status giuridico e la loro origine. Un PIC convalidato non è un prerequisito per presentare una domanda.

Questo tema richiede il coinvolgimento attivo, in qualità di beneficiari, di almeno 2 autorità governative locali o regionali di 2 diversi Stati membri dell'UE o Paesi associati. Per questi partecipanti, i richiedenti devono compilare la tabella "Informazioni sugli operatori della sicurezza" nel modulo di domanda con tutte le informazioni richieste, seguendo il modello fornito nello strumento informatico di presentazione. Se i progetti utilizzano dati e servizi di osservazione della terra, posizionamento, navigazione e/o tempistica correlati basati su satelliti, i beneficiari devono utilizzare Copernicus e/o Galileo/EGNOS (possono essere utilizzati anche altri dati e servizi).

Contributo finanziario:
Contributo UE previsto per progetto La Commissione ritiene che un contributo UE di circa 5 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 5,00 milioni di euro. Tipo di azione Azioni di ricerca e innovazione

Scadenza:
20 novembre 2024 17:00:00 ora di Bruxelles

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