Sviluppo e diffusione di tecnologie chiave avanzate
Development and Deployment of Advanced Key Technologies

TOPIC ID:
DIGITAL-ECCC-2024-DEPLOY-CYBER-07-KEYTECH

Ente finanziatore:
Commissione europea
Programma Europa digitale (DIGITAL)

Obiettivi ed impatto attesi:
Risultato atteso:

- Implementazione di tecnologie all'avanguardia nel campo della cybersecurity.
- Strumenti per il rilevamento automatico delle minacce, il monitoraggio delle reti, la protezione dei dati e la risposta agli incidenti.

Obiettivo:
I progressi nelle tecnologie digitali fondamentali, come l'intelligenza artificiale (compresa l'IA generativa e l'IA avversaria), l'analisi dei Big Data, la tecnologia quantistica, la tecnologia blockchain, l'elaborazione ad alte prestazioni e il software-defined networking, creano nuove opportunità per il progresso della sicurezza informatica nelle aree di rilevamento delle vulnerabilità, rilevamento delle minacce e risposta rapida, riducendo la finestra di opportunità per gli aggressori di sfruttare tali vulnerabilità. Inoltre, possono offrire nuove possibilità di proteggere la sicurezza e la privacy dei dati.
L'obiettivo è quello di consentire agli operatori europei della sicurezza informatica di trarre vantaggio da queste nuove scoperte, migliorando le capacità di rilevamento e prevenzione, l'efficienza e la scalabilità e facilitando la condivisione dei dati e la conformità alle normative.
In particolare, le tecnologie innovative dovrebbero consentire l'elaborazione di grandi quantità di dati, automatizzando il riconoscimento dei modelli in tempo reale, l'analisi dei log e la scansione delle vulnerabilità, consentendo ai professionisti della sicurezza di concentrarsi sull'interpretazione dei dati e sulle decisioni di risposta di livello superiore. Dovrebbero consentire alle organizzazioni di distribuire soluzioni su scala più ampia e in ambienti sempre più complessi.
Una priorità è creare e rafforzare la capacità di fornire informazioni originali sulle minacce informatiche (CTI), ad esempio sotto forma di feed o servizi CTI.
Ambito di applicazione:
Le attività dovrebbero rafforzare le capacità di cybersecurity utilizzando tecnologie all'avanguardia, che comprendano vari aspetti della cybersecurity. Ciò comporta l'adozione e l'integrazione di nuovi strumenti, sistemi e servizi per il rilevamento delle minacce, la risposta agli incidenti, la difesa dalle minacce informatiche, la gestione delle vulnerabilità, la protezione dei dati e così via. Dovranno essere affrontati uno o più dei seguenti argomenti:

- Monitoraggio in tempo reale e risposta agli incidenti: garantire la rapida identificazione e risposta agli incidenti di sicurezza attraverso il monitoraggio continuo della rete, la generazione di avvisi e

meccanismi di risposta automatizzati.

- Difesa e analisi del malware: mitigazione delle minacce di malware attraverso l'analisi del comportamento del codice, l'esame del traffico di rete e la valutazione delle caratteristiche dei file, riducendo così le opportunità per gli aggressori di sfruttare le vulnerabilità.
- Gestione proattiva delle vulnerabilità: identificare e risolvere i punti deboli in modo proattivo attraverso la scansione automatizzata delle vulnerabilità e i test di penetrazione per affrontare le potenziali minacce prima che possano essere sfruttate.
- Protezione dei dati e rilevamento delle anomalie: salvaguardare i dati sensibili esaminando i modelli di accesso e identificando i comportamenti anomali per ridurre le violazioni dei dati e proteggere le informazioni critiche.
- Indagine sugli incidenti per aiutare a scoprire cause, portata e impatto degli incidenti o delle violazioni della sicurezza che si sono verificati.
- Utilizzo dei dati con privacy: consentire alle organizzazioni di sfruttare i dati per analisi e approfondimenti, preservando al contempo la sicurezza e la privacy dei dati attraverso tecniche quali l'anonimizzazione e la de-identificazione.

Affrontando tali questioni, la resilienza delle organizzazioni in materia di cybersicurezza dovrebbe essere potenziata, migliorando la postura complessiva della cybersicurezza, che comprende vari aspetti come il rilevamento delle minacce, la risposta agli incidenti e la gestione delle vulnerabilità.
In casi ben giustificati, le richieste di accesso all'infrastruttura di calcolo ad alte prestazioni di EuroHPC potrebbero essere accolte.
I sistemi, gli strumenti e i servizi sviluppati nell'ambito di questo tema, se pertinenti, saranno resi disponibili per la concessione di licenze a piattaforme SOC nazionali e/o transfrontaliere a condizioni di mercato favorevoli.
Questa azione mira alla diffusione di tecnologie chiave per la sicurezza informatica, in particolare nel contesto della sicurezza delle autorità nazionali, dei fornitori di infrastrutture critiche e di servizi essenziali. Poiché ciò comporta la gestione di incidenti informatici, malware e gestione delle vulnerabilità che potrebbero essere sfruttate da attori malintenzionati, la diffusione di tali tecnologie deve essere protetta da possibili dipendenze e vulnerabilità nella sicurezza informatica per prevenire l'influenza e il controllo stranieri. Come già osservato in precedenza, la partecipazione di entità non appartenenti all'UE comporta il rischio che informazioni altamente sensibili sulle infrastrutture di sicurezza, sui rischi e sugli incidenti siano soggette a legislazioni o pressioni che obbligano tali entità non appartenenti all'UE a divulgare tali informazioni a governi non appartenenti all'UE, con un rischio imprevedibile per la sicurezza. Pertanto, in base alle ragioni di sicurezza esposte, le azioni relative a queste tecnologie sono soggette all'articolo 12, paragrafo 5, del Regolamento (UE) 2021/694.

Criteri di eleggibilità:
Per essere ammissibili, i richiedenti (beneficiari ed enti affiliati) devono:
- essere persone giuridiche (enti pubblici o privati)
- essere stabilito in uno dei paesi ammissibili, ossia:
- Stati membri dell'UE (compresi i Paesi e territori d'oltremare (PTOM)) - Paesi SEE (Norvegia, Islanda, Liechtenstein) I beneficiari e le entità affiliate 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, verrà richiesto di caricare i documenti che dimostrano lo status giuridico e l'origine.
Si ricorda che tutti i temi di questo bando sono soggetti a restrizioni per motivi di sicurezza, pertanto i soggetti non devono essere controllati direttamente o indirettamente da un Paese che non sia un Paese ammissibile.
Tutte le entità dovranno compilare e presentare una dichiarazione sulla proprietà e sul controllo.
Inoltre:
- la partecipazione a qualsiasi titolo (come beneficiario, entità affiliata, partner associato, subappaltatore o destinatario di sostegno finanziario a terzi) è limitata a entità stabilite e controllate da Paesi ammissibili
- le attività del progetto (incluso il lavoro in subappalto) devono svolgersi in Paesi ammissibili (si veda la sezione localizzazione geografica e la sezione 10) - la Convenzione di sovvenzione può prevedere restrizioni sui diritti di proprietà intellettuale (si veda la sezione 10).

I soggetti interessati sono le aziende tecnologiche, in particolare le PMI, che lavorano per fornire e supportare altre organizzazioni private e pubbliche con il rilevamento delle minacce informatiche e i feed CTI. Le candidature dei consorzi, pur non essendo obbligatorie, contribuiranno positivamente all'impatto dell'azione.

Contributo finanziario:
Tipo di azione e tasso di finanziamento
Azioni di sostegno alle PMI - tasso di finanziamento del 50% e del 75% (per le PMI)

Scadenza:
21 gennaio 2025 17:00:00 ora di Bruxelles

Ulteriori informazioni:
call-fiche_digital-eccc-2024-deploy-cyber-07_en.pdf (europa.eu)