Nuove applicazioni dell'IA e di altre tecnologie abilitanti per i centri operativi di sicurezza

Novel applications of AI and other enabling technologies for security operation centres

TOPIC ID:
DIGITAL-ECCC-2024-DEPLOY-CYBER-06-ENABLINGTECH

Ente finanziatore:
Commissione europea
Programma Europa digitale (DIGITAL)

Obiettivi ed impatto attesi:
Questo tema affronta le tecnologie abilitanti (come l'IA) per i SOC, compresi i SOC nazionali che forniscono una capacità operativa centrale e supportano altri SOC a livello nazionale e svolgono un ruolo centrale come hub all'interno di un contesto di SOC, e anche le piattaforme SOC transfrontaliere in cui tali tecnologie possono rafforzare le capacità di analisi, rilevamento e prevenzione delle minacce e degli incidenti informatici e sostenere la produzione di intelligence di alta qualità sulle minacce informatiche. Queste tecnologie abilitanti dovrebbero consentire una creazione e un'analisi più efficace delle informazioni sulle minacce informatiche (Cyber Threat Intelligence, CTI), nonché un'elaborazione più rapida e scalabile delle CTI e l'identificazione di modelli che consentano un rilevamento e un processo decisionale rapidi.
Ambito di applicazione:
Le azioni in questo ambito dovrebbero sviluppare e distribuire sistemi e strumenti per la sicurezza informatica basati su tecnologie abilitanti (come l'IA), affrontando aspetti quali il rilevamento delle minacce, il rilevamento delle vulnerabilità, l'attenuazione delle minacce, il recupero degli incidenti attraverso l'auto-guarigione, l'analisi e la condivisione dei dati. Le attività devono includere almeno uno dei seguenti aspetti:
• Rilevamento continuo di schemi e identificazione di anomalie che indicano potenziali minacce, riconoscendo nuovi vettori di attacco e consentendo un rilevamento avanzato in un panorama di minacce in continua evoluzione.
• Creazione di CTI basate su nuove capacità di rilevamento delle minacce.
• Migliorare la velocità di risposta agli incidenti attraverso il monitoraggio in tempo reale delle reti per identificare gli incidenti di sicurezza e generare avvisi o attivare risposte automatiche.
• Mitigare le minacce di malware analizzando il comportamento del codice, il traffico di rete e le caratteristiche dei file, riducendo la finestra di opportunità per gli aggressori di sfruttare il malware.
• Identificazione e gestione delle vulnerabilità.
• Recupero dagli incidenti attraverso le capacità di auto-guarigione.
• Ridurre le possibilità di attacco e identificare preventivamente i punti deboli attraverso la scansione automatica delle vulnerabilità e i test di penetrazione.
• Protezione dei dati sensibili attraverso l'analisi dei modelli di accesso e il rilevamento di comportamenti anomali.
• Consentire alle organizzazioni di sfruttare e condividere le CTI e altre informazioni utilizzabili per analisi

e approfondimenti senza compromettere la sicurezza e la privacy dei dati, attraverso l'anonimizzazione e la de-identificazione. I fornitori di strumenti e servizi sono invitati a candidarsi a questo tema, anche se in consorzio con i SOC nazionali. Ove opportuno, si dovranno creare collegamenti con le parti interessate nel settore dell'High-Performance Computing, nonché attività volte a promuovere il networking con tali parti interessate.
I fornitori di strumenti e servizi sono invitati a candidarsi a questo tema, anche se in consorzio con i SOC nazionali. Ove opportuno, si dovranno creare collegamenti con le parti interessate nel settore del calcolo ad alte prestazioni. In casi ben giustificati, potrebbero essere concesse richieste di accesso all'infrastruttura di calcolo ad alte prestazioni di EuroHPC.
I sistemi, gli strumenti e i servizi sviluppati nell'ambito di questo tema saranno resi disponibili per la concessione di licenze a piattaforme SOC nazionali e/o transfrontaliere a condizioni di mercato favorevoli. Queste azioni mirano a creare o rafforzare i SOC nazionali e/o transfrontalieri, che occupano un ruolo centrale nel garantire la sicurezza (informatica) delle autorità nazionali, dei fornitori di infrastrutture critiche e di servizi essenziali. I SOC hanno il compito di monitorare, comprendere e gestire in modo proattivo le minacce alla sicurezza informatica. Alla luce del ruolo operativo cruciale dei SOC per garantire la sicurezza informatica nell'Unione, della natura delle tecnologie coinvolte e della sensibilità delle informazioni trattate, i SOC devono essere protetti da possibili dipendenze e vulnerabilità nella sicurezza informatica per prevenire l'influenza e il controllo stranieri. Come già sottolineato 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 una legislazione o a 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, sulla base delle ragioni di sicurezza esposte, le azioni relative ai SOC sono soggette all'articolo 12(5) del Regolamento (UE) 2021/694, in coerenza con il WP 2021/2022.

Prodotti da consegnare
• L'impiego dell'intelligenza artificiale e delle tecnologie chiave avanzate come fattori abilitanti per i SOC
• Strumenti per la creazione, l'analisi e l'elaborazione di CTI che consentono operazioni SOC più rapide e scalabili
• Alimentazioni o servizi CTI originali europei

Criteri di eleggibilità:
Le domande saranno considerate ammissibili solo se il loro contenuto corrisponde interamente (o almeno in parte) alla descrizione del tema per cui sono state presentate. Partecipanti ammissibili (Paesi ammissibili)
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 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 richiesto loro di caricare documenti che dimostrino lo status giuridico e l'origine.
Altre entità possono partecipare in altri ruoli del consorzio, come partner associati, subappaltatori, terze parti che forniscono contributi in natura, ecc.
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. Tutti i soggetti5 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 alle entità dei paesi ammissibili
- le attività del progetto (compreso il lavoro in subappalto) devono svolgersi nei paesi ammissibili
- la Convenzione di sovvenzione può prevedere restrizioni sui DPI
Composizione del consorzio - nessuna restrizione

Contributo finanziario:
I parametri della sovvenzione (importo massimo della sovvenzione, tasso di finanziamento, costi totali ammissibili, ecc.) saranno stabiliti nella Convenzione di sovvenzione (Scheda tecnica, punto 3 e art. 5).
Budget del progetto (importo massimo della sovvenzione): - Per il tema DIGITAL-ECCC-2024-DEPLOY-CYBER-06-ENABLINGTECH Novel applications of AI and Other Enabling Technologies for Security Operation Centres: indicativamente tra i 3 e i 5 milioni per progetto, ma non sono esclusi altri importi.
Tipo di azione e tasso di finanziamento Sovvenzione semplice - tasso di finanziamento del 50%.

Scadenza:
26 marzo 2024 17:00:00 ora di Bruxelles

Ulteriori informazioni:
call-fiche_digital-eccc-2024-deploy-cyber-06_en.pdf (europa.eu)