Titolo	Horizon Europe - Approaches and tools for security in software and hardware development and assessment
Ambito territoriale	Europa
Ente finanziatore	Commissione europea
Ente gestore	Commissione europea
Stato	Attivo
Beneficiari	Le domande devono essere presentate da consorzi costituiti da almeno 3 soggetti giuridici indipendenti, stabiliti in 3 Paesi diversi partecipanti al Programma Horizon Europe.
Obiettivi	Il software è alla base di tutte le tecnologie digitali e, come tale, al centro delle infrastrutture, dei servizi e dei prodotti IT. L'attuale sviluppo del software dà priorità alla rapida implementazione rispetto alla sicurezza, il che si traduce in vulnerabilità e applicazioni non sicure. L'ingegneria della sicurezza, sia a livello software che hardware, deve essere integrata nel loro sviluppo. Sebbene gran parte del software e dell'hardware utilizzati nell'UE sia sviluppato al di fuori dell'Unione Europea, dovrebbe essere conforme ai requisiti di sicurezza all'interno dell'UE. L'UE dovrebbe poter fare affidamento su software e hardware che possono essere verificati e controllati in termini di sicurezza. In particolare, dovrebbero essere ulteriormente esplorate le potenziali implicazioni sulla sicurezza derivanti dall'utilizzo di software e hardware open source e la verificabilità della sicurezza in tale contesto. Il software è soggetto ad aggiornamenti continui, pertanto il livello di sicurezza non può essere valutato una volta per tutte, pertanto sono necessari metodi e strumenti per eseguire valutazioni continue della sicurezza. Inoltre, anche le normative sulla sicurezza e sulla privacy si evolvono e devono essere prese in considerazione negli approcci di conformità. L'identificazione e l'analisi di potenziali aspetti normativi e barriere per le tecnologie/soluzioni sviluppate sono incoraggiate, ove pertinente.
Attività ammissibili	Si prevede che i risultati dei progetti contribuiranno ad alcuni o tutti i seguenti risultati: • miglioramento dell'ingegneria della sicurezza hardware e software; progettazione di sistemi resilienti; • migliore accesso ai test di hardware e software in ambienti virtuali, chiusi e sicuri; • studio sistematico e, ove possibile, automatizzato delle vulnerabilità, analisi del software, scoperta delle vulnerabilità e valutazione dinamica della sicurezza; • hardware e software certificabili affidabili; • servizi di sicurezza basati sull'intelligenza artificiale, ad es. sicurezza predittiva, rilevamento avanzato di anomalie e intrusioni, controlli sullo stato del sistema.
Spese ammissibili	Le proposte dovrebbero contribuire al raggiungimento di uno o più dei seguenti impatti: • rafforzamento delle capacità di cibersicurezza dell'UE e della sovranità dell'Unione europea nelle tecnologie digitali; • infrastrutture, sistemi e processi digitali più resilienti; • maggiore sicurezza del software, dell'hardware e della catena di fornitura; • tecnologie dirompenti protette; • garanzia e certificazione di sicurezza intelligenti e quantificabili condivise in tutta l'UE; • consapevolezza rafforzata e gestione e cultura comuni della sicurezza informatica.
Budget	Euro 37.000.000,00
Agevolazione	**IA – Innovation Actions**. Sovvenzione a fondo perduto fino al **70%** delle spese ammissibili.
Erogazione	Dopo la firma della sovvenzione, i progetti riceveranno un prefinanziamento per iniziare a lavorare sul progetto.

	Il prefinanziamento copre fino al 50% del cofinanziamento di progetto. Il prefinanziamento sarà pagato 30 giorni dall'entrata in vigore/10 giorni prima della data di inizio/garanzia finanziaria (se richiesta), a seconda di quale data sia più recente. Pagamento del saldo: alla fine del progetto, verrà calcolato l'importo finale della sovvenzione.
Data apertura	27-06-2024
Data chiusura	20-11-2024
Valutazione	Valutazione a graduatoria
Difficoltà	Difficile
Link al bando	Bando
Link informazioni	Informazioni
Contatto	imprese@eurosportello.eu