

AC SIA CRA

un **monitoraggio completo** dell'esposizione del tuo studio professionale o della tua azienda al **rischio Cyber**



ACSIA CRA analizza il livello di sicurezza della tua organizzazione, identifica le sue potenziali vulnerabilità e calcola il tuo livello di cybersicurezza, in modo da avere una chiara comprensione del tuo rischio informatico.

ACSIA CRA esegue un'analisi completa della situazione informatica di un'azienda o di uno studio professionale, concentrandosi sull'esposizione dei servizi e delle informazioni che possono essere vulnerabili agli attacchi informatici.

Perché scegliere ACSIA CRA?



Identifica rapidamente i rischi esterni

ACSIA CRA verifica tempestivamente la situazione della tua azienda in termini di sicurezza informatica, esaminando la tua superficie di attacco esterna ed evidenziando come e dove la tua azienda possa essere a rischio.



Identifica rapidamente i rischi esterni

ACSIA CRA verifica tempestivamente la situazione della tua azienda in termini di sicurezza informatica, esaminando la tua superficie di attacco esterna ed evidenziando come e dove la tua azienda possa essere a rischio.



Totale visibilità della superficie di attacco

ACSIA CRA utilizza diverse fonti per analizzare la superficie di attacco. L'analisi di ACSIA CRA non si limita al perimetro esterno, ma include anche le identità digitali.



Costantemente aggiornato

Se vengono scoperte nuove vulnerabilità, l'indice ACSIA CRA si aggiorna automaticamente consentendo all'organizzazione di monitorare attivamente il perimetro.



Facile da usare

ACSIA CRA ha bisogno solo di informazioni facili da reperire per identificare la tua azienda (partita IVA e domini web).



Aiuta a migliorare

ACSIA CRA identifica le configurazioni errate, aiutando il tuo team a migliorare le politiche di sicurezza sull'utilizzo di account e dispositivi.



Informazioni chiare

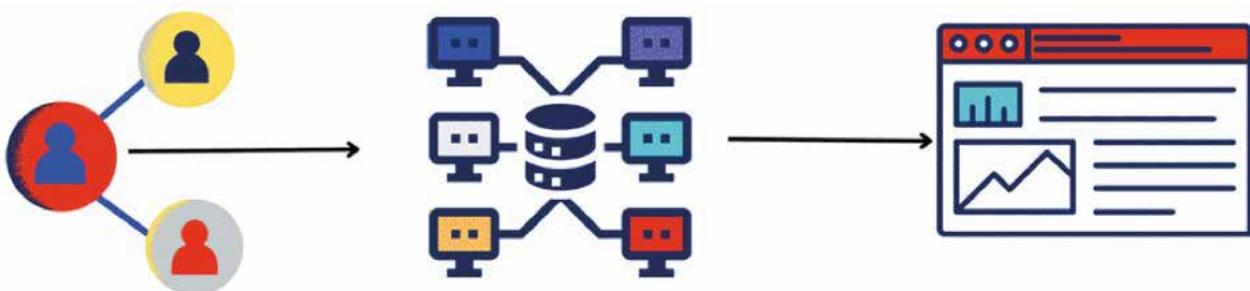
L'interfaccia di ACSIA CRA è di facile comprensione, con analisi e report informativi adatti anche al personale non tecnico.

ACSIA CRA al lavoro

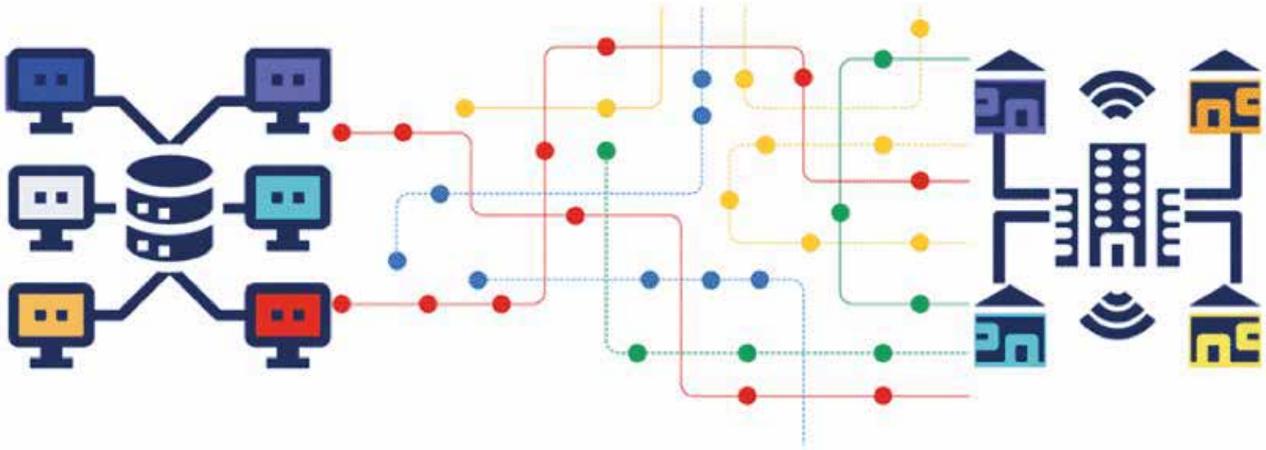
Controlla l'esposizione dell'azienda

ACSIA CRA valuta la sicurezza informatica dei tuoi asset disponibili al pubblico, analizzando i rischi e documentando lo stato della tua sicurezza informatica aziendale.

ACSIA CRA effettua scansioni passive per mappare ed elencare le vulnerabilità. La nostra valutazione del rischio fornisce alla tua azienda un quadro chiaro dei problemi, dell'esposizione e delle debolezze in termini di sicurezza.



Scopri e traccia il tuo livello di sicurezza
Scan Thousands Of Assets



Scansiona migliaia di attività



È possibile individuare rapidamente qualsiasi potenziale esposizione delle risorse aziendali. ACSIA CRA scansiona la superficie di attacco eseguendo migliaia di test. Si comporta in modo simile al software maligno nelle fasi di ricognizione e analisi che precedono gli attacchi informatici a un determinato bersaglio. La valutazione del rischio eseguita da ACSIA CRA è riassunta in un indice che considera sei livelli di analisi. Questa analisi produce un punteggio da 0 (non sicuro) a 100 (più sicuro).

Traccia i progressi nel tempo



Valuta il livello di rischio



Il punteggio assegnato da ACSIA CRA rappresenta un indicatore complessivo del livello di rischio. I nostri risultati derivano da un'analisi della potenziale esposizione delle risorse dell'azienda agli attacchi informatici.

I rapporti di ACSIA CRA forniscono informazioni su una serie di problemi e vulnerabilità che i criminali informatici possono individuare e sfruttare per effettuare attacchi informatici contro la tua azienda. Il tuo team potrà essere in grado di affrontare e risolvere le vulnerabilità della superficie di attacco, degli asset e dell'infrastruttura della tua organizzazione.

Identifica le vulnerabilità



Documenta i progressi

Le scansioni regolari documentano il miglioramento del punteggio assegnato da ACSIA CRA nel tempo. Potrai dimostrare che l'azienda è proattiva per quanto riguarda audit, assicurazione informatica, legislazione, GDPR e certificazione. Prova quindi che il tuo team sta lavorando attivamente per migliorare la sicurezza informatica.



In che modo ACSIA CRA può aiutare la tua azienda o il tuo studio professionale?

Fase 1

Basta inserire i dati

Identifica quindi l'azienda da testare con alcuni parametri facili da trovare.

- 1•** Inserisci il numero di partita IVA (obbligatorio).
- 2•** Inserisci uno dei seguenti elementi: dominio web, URL, e-mail o IP.

Fase 2

ACSIA CRA raccoglie informazioni

ACSIA CRA comincia a misurare centinaia di variabili da fonti OSINT, HUMINT e CLOSINT. Il sistema si avvale di motori di ricerca e social media e verifica un'ampia gamma di potenziali vulnerabilità.

Fase 3

ACSIA CRA analizza

ACSIA CRA esegue una valutazione e fornisce una panoramica del rischio potenziale di attacchi informatici.

Il sistema ti mostrerà lo stato di sicurezza degli asset IT, delle identità digitali e un'analisi della situazione complessiva della sicurezza informatica.

Fase 4

Reports di ACSIA CRA

ACSIA CRA fornisce un rapporto dettagliato e un punteggio/indice di rischio informatico.

Verranno presentati risultati approfonditi sulla tua situazione in termini di sicurezza e il livello di rischio verrà aggiornato automaticamente quando verranno scoperte nuove vulnerabilità.

ACSIA CRA è quanto di più efficace e semplice possa esserci per la sicurezza informatica

L'analisi da parte di ACSIA CRA viene eseguita da un sistema automatico che cerca vulnerabilità, falle, configurazioni errate di server, infrastrutture e altro ancora.

ACSIA CRA si comporta in modo simile al software maligno nella fase di analisi dell'obiettivo dell'attacco.

Il sistema di ricerca di ACSIA CRA garantisce una copertura completa e un punto di vista imparziale sulle reti e le configurazioni locali.

Tutte le variabili raccolte vengono analizzate e confrontate con i dati già presenti nel database di migliaia di aziende di ACSIA CRA.

La situazione informatica di ogni asset viene analizzata e correlata alle possibili minacce.

Facilissimo da usare e da avviare

ACSIA CRA è semplice da usare e facile da implementare. Richiede manutenzione e interventi minimi e ha un elevato grado di automazione. Questo ti faciliterà la vita