



ACSIA CRA

CYBER RISK ASSESSMENT



Cos'è ACSIA CRA?

ACSIA Cyber Risk Assessment analizza la situazione di cyber sicurezza dell'azienda, concentrandosi sull'esposizione ed i conseguenti rischi legati ai suoi asset digitali, dati, informazioni e servizi.



Controlla in Quali Aree L'Azienda è Vulnerabile

Pensa Come il Nemico

ACSIA CRA agisce simulando l'evoluzione di un attacco informatico, che inizia con ricognizione e raccolta informazioni su di un possibile bersaglio.



Scopre Potenziali Vulnerabilità

L'analisi e la scansione automatizzate da parte di ACSIA CRA si concentrano su asset, informazioni, servizi esposti e disponibili esternamente.



Evidenzia Dove Possono Esserci Problemi

Puoi analizzare e documentare la superficie d'attacco dell'azienda con l'intervento di ACSIA CRA: avrai una visione oggettiva che anticiperà i cyber criminali.



Conosci il Livello di Esposizione e di Rischio

ACSIA CRA fornisce informazioni cruciali su come e dove il business è esposto, fornendo rapporti dettagliati sul suo livello di rischio.



Proteggi la Tua Azienda

ACSIA CRA rivela quindi quali strategie e contromisure adottare per mantenere al sicuro la tua azienda.



Analizza la Situazione Cyber dell'Azienda con ACSIA CRA

Scansiona la Superficie di Attacco

ACSIA CRA esegue una ricognizione passiva, analizzando gli asset disponibili ed esposti al pubblico.



Scopri Dove l'Azienda è Vulnerabile

ACSIA CRA analizza centinaia di variabili, valutando la situazione di cyber sicurezza e documentando potenziali problemi e vulnerabilità.



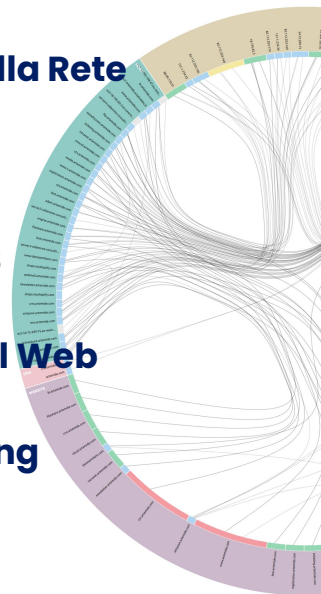
Il Tuo Team Può Agire Efficacemente

La nostra piattaforma fornisce un rapporto dettagliato del rischio, evidenziando l'esposizione dell'azienda, i pericoli e le strategie da attuare per limitarli.



ACSIA CRA Analizza

1. Sicurezza dei Domini
2. Sicurezza della Rete
3. Sicurezza IP
4. Sicurezza AS
5. Sicurezza del Web
6. Typosquatting



ACZIA CRA: Come Funziona?

Step 1 – Selezione Azienda

Identifica l'azienda da analizzare con pochi, facili parametri.

1. Inserisci:

Uno di questi parametri:

- Dominio Web
- URL
- E-mail aziendale
- IP

In aggiunta:

- Il numero di partita IVA

Step 2 – Raccolta Dati

ACZIA CRA misura centinaia di variabili, evidenziando dove la tua azienda può essere esposta.

2. Scansiona:

- Motori di ricerca
- Code Repositories
- Social Media
- Dati rubati
- Vulnerabilità
- Forum su Cyber crimini
- Paste Sites
- Mercato nero
- Database rubati
- Dark Web

Step 3 – Analisi

ACZIA CRA esegue una profonda analisi il cui risultato sarà una valutazione dettagliata dei potenziali e attuali rischi.

3. Risultato:

- Stato della sicurezza degli asset IT (incluse vulnerabilità)
- Stato della sicurezza delle identità digitali (inclusi malware & botnet)
- Analisi della situazione generale di cyber sicurezza

Step 4– Rapporto

L'indice numerico rappresenta un indicatore del livello di rischio.

ACZIA CRA lo aggiorna automaticamente in caso di nuove vulnerabilità.

4. Valutazione Asset:

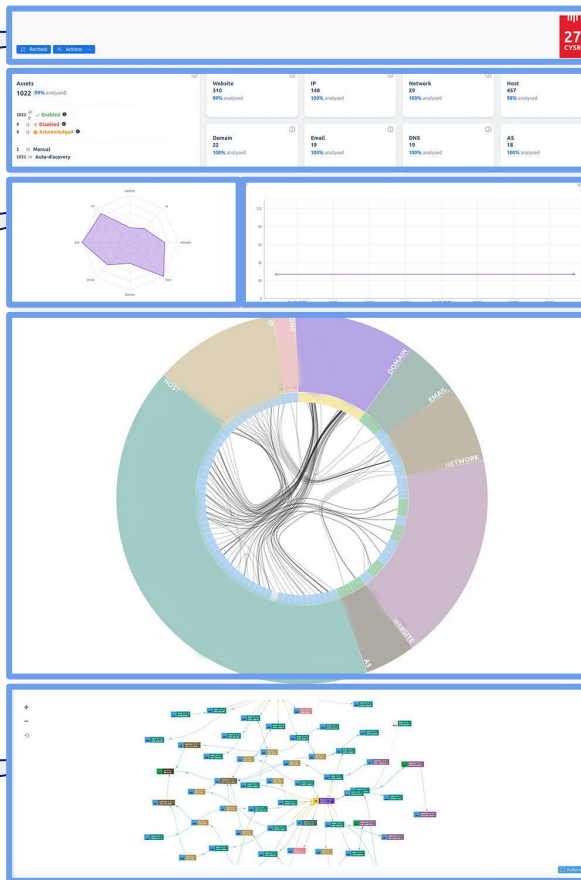
- Sicurezza domini
- Botnet
- Fughe/furti utenti
- Sicurezza Web
- Sicurezza IP
- Sicurezza della rete
- Sicurezza AS
- Typosquatting

ACSIA CRA: La Dashboard - una Visione d'Insieme

- Indice ACSIA CRA
- Informazioni sull'organizzazione

- Grafico della distribuzione delle risorse

- Rete pubblica dell'organizzazione analizzata



- Stato dell'analisi
- Asset analizzati

- Progresso dell'indice di rischio ACSIA CRA

- Superficie d'attacco dell'organizzazione

ACZIA CRA: Controllo del Livello di Rischio Continuo ed Automatizzato

Valutazione Automatica

La soluzione ACSIA CRA è completamente automatizzata: non necessita di interventi manuali. Offriamo poi dei pacchetti diversi per tali test, a seconda delle esigenze del cliente.

La soluzione invia raccomandazioni e avvertimenti quando sorgono nuove vulnerabilità, aggiornando automaticamente il punteggio di rischio.

Gli aggiornamenti permettono al cliente di avere piena visibilità sulla situazione dei suoi asset digitali (siti, server, reti, ecc.), permettendo di adottare strategie e contromisure efficaci ed efficienti.



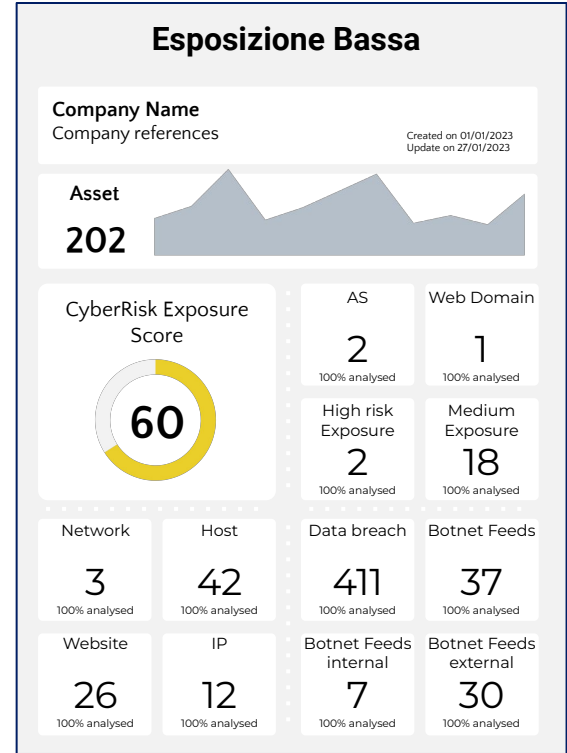
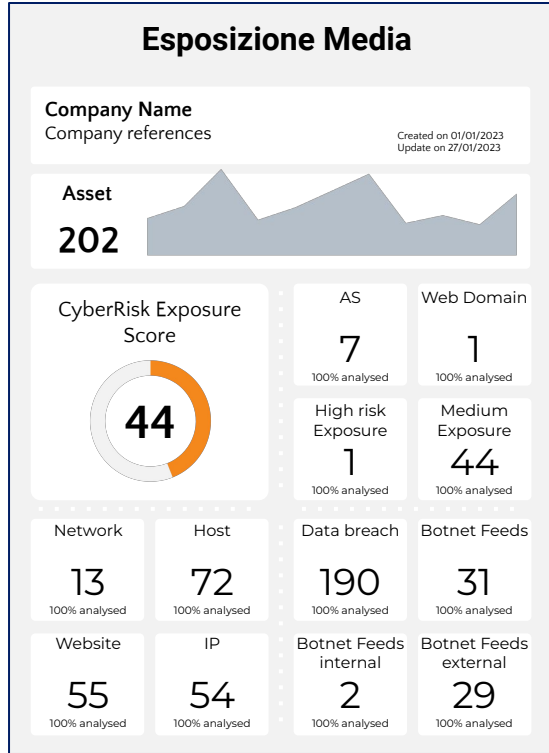
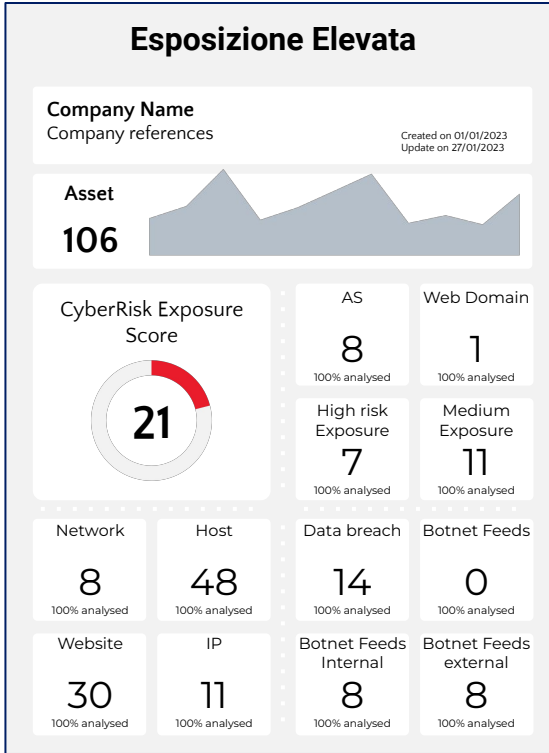
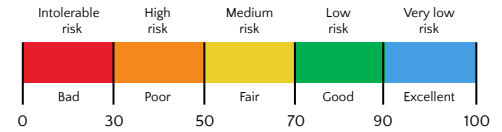
Metrics Scorecard

0-30	Bad - Intolerable Risk
30-50	Poor - High Risk
50-70	Fair - Medium Risk
70-90	Good - Low Risk
90-100	Excellent - Very Low Risk

Domini Ispezionati

- I domini ispezionati forniscono il punteggio di rischio
- Vulnerabilità dei siti e del set-up di hosting
- Situazione di sicurezza di domini e name server
- Situazione di sicurezza dei server di posta elettronica
- Situazione di sicurezza di IP, reti, BGP routes e ASN
- Presenza di malware all'interno dell'azienda
- Ricerca di fughe e furti di dati da/tra botnet e dark web

Esempio di ACSIA CRA: il Punteggio di Rischio



La valutazione del rischio è sintetizzata in un indice che considera sei fonti diverse di analisi dati e che produce un punteggio da 0 (rischio critico) a 100 (rischio minimo).

ACSIA CRA: Monitoraggio Proattivo di Fughe/Furti di Dati e Botnet



Oggetto dei Rapporti

Fughe/Furti di Dati: ricerca ed analisi di indirizzi email aziendali con prove di password utilizzate, password hashes e record di password vuote.

Darknet: analisi di coinvolgimento passato con darknet riguardante l'azienda in questione, con informazioni condivise in ambienti come forum criminali, chat, ecc.

Botnet: ricerca e analisi di terminali infettati da malware di tipo botnet, fornendo prove tangibili di file sottratti e messi a disposizione di cyber criminali.

Perché scegliere ACSIA CRA?



Identifica Rischi Esterni Rapidamente

ACSIA CRA valuta velocemente la situazione di cyber sicurezza della tua azienda, documentandone la superficie di attacco, mostrando come e dove è esposta a rischi.



Costantemente Aggiornato

Se vengono scoperte vulnerabilità, l'indice di rischio di ACSIA CRA si aggiorna automaticamente, permettendo di monitorare attivamente la situazione di cyber sicurezza.



Facilita i Progressi

ACSIA CRA identifica configurazioni fallaci, aiutando il tuo team a migliorare le politiche di sicurezza degli account e dei terminali in uso.



Completa Visibilità della Superficie d'Attacco

ACSIA CRA utilizza molteplici fonti per scansionare la superficie d'attacco. La sua analisi non è limitata al perimetro esterno ma include anche le identità digitali.



Facile da Usare

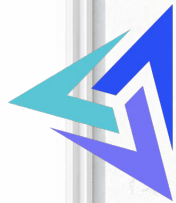
ACSIA CRA ha solo bisogno di informazioni e dati semplici e facili per te da trovare, per identificare la tua azienda (IVA e domini web).



Informazioni Chiare

La dashboard di ACSIA CRA è facile da capire, con rapporti esaustivi ed informazioni chiare, in linea quindi anche con le esigenze del personale non tecnico.

Grazie



ACSIA CRA
CYBER RISK ASSESSMENT