PREVENTING.

Le soluzioni di Dectar sono in grado di prevedere e prevenire i cyber attacchi alla infrastruttura IT. La tua azienda sarà in grado di anticipare le intenzioni dei cybercriminali e di respingere gli aggressori.

DEFENDING.

La tecnologia di Dectar agisce in tempo reale, difendendo gli asset della tua azienda tramite azioni pienamente automatizzate.

REACTING.

I prodotti Dectar reagiscono rapidamente a minacce concrete. ACSIA XDR Plus è di facile gestione, libera risorse e ottimizza il tuo budget IT.

Sviluppato e realizzato in Europa

L'obiettivo primario di Dectar è quello di impedire ai criminali di avvicinarsi ad infrastrutture ed asset digitali.

CONTATTI

Dectar

Prevent. Defend. React.

PREVENTING.
DEFENDING.
REACTING.

Dectar sviluppa soluzioni di cybersecurity uniche per la tua azienda.

I prodotti ACSIA di Dectar forniscono alla tua azienda una prevenzione automatizzata delle minacce informatiche

- Mantengono l'azienda al sicuro
- Riducono i costi
- Bloccano la ricognizione criminale
- Rivelano il rischio informatico
- Prevengono gli attacchi
- Riducono il numero di avvisi
- Correlano gli eventi

ACSIA XDR Plus

XDR: Extended Detection & Response

ACSIA XDR Plus™ offre una difesa predittiva e proattiva, facile e veloce da implementare, che automatizza sia la fase di protezione che di riparazione.

Threat Intelligence Predittiva

- Blocca le reti anonime
- Blocca i programmi dannosi
- Blocca gli URL dannosi
- Blocca gli indirizzi IP dannosi
- Blocca "command & control"
- Informa concretamente sulle minacce

Anti Sorveglianza Proattiva

- Identifica e blocca le tecniche di pre-attacco
- Blocca la raccolta delle informazioni
- Impedisce la scansione degli accessi
- Blocca la scansione delle vulnerabilità

Risposta Reattiva ad Eventi Cyber

- EDR, IDS, IPS e SIEM centralizzati
- Correlazione in tempo reale di tutti i log
- Playbook e soc automatizzati
- Rileva i comportamenti anomali
- Account Compromise e User Profiler

ACSIA CRA

Valutazione del Rischio Informatico

ACSIA CRA esegue un'analisi completa della situazione informatica dell'azienda, concentrandosi sull'esposizione di servizi e informazioni potenzialmente vulnerabili agli attacchi informatici.

Comprensione del Rischio Informatico

- Pensa come il nemico
- Scopre potenziali vulnerabilità
- Evidenzia eventuali problemi
- Mantengono l'azienda al sicuro
- Esamina le aree soggette a un attacco

Valutazioni Automatizzate della Sicurezza

- Esegue ricognizione passiva delle risorse
- Misura centinaia di variabili
- Analizza la situazione di cybersecurity
- Riassume i risultati in un punteggio di rischio
- Fornisce rapporto sui rischi