



Cos'è e come funziona?

Kartos XTI Watchbots è la piattaforma di cyber sorveglianza sviluppata da Enthec per estendere il perimetro di sicurezza aziendale. Concepito con un approccio di strategia hacker, Kartos è costantemente in aggiornamento così da inglobare sempre categorie e capacità che anticipino l'evoluzione degli attacchi informatici.

Kartos XTI Watchbots: EASM + DRPS + SRS in un'unica piattaforma

External Attack Surface Management	Digital Risk Protection Services	Security Rating Services
Rilevamento delle superfici di attacco, delle risorse aziendali e delle informazioni di sistema, servizi e applicazioni cloud che sono disponibili e visibili a qualsiasi criminale informatico.	Rilevamento di informazioni contestuali sui potenziali attori dell'attacco, le loro tattiche e i loro processi per la realizzazione di attività dannose. Eliminazione delle attività avverse per conto dell'azienda.	Valutazione indipendente dei rischi propri e di terzi, per una visione completa della maturità sulla sicurezza informatica di qualsiasi azienda che utilizza un approccio esterno. Espansione e analisi delle informazioni fornite dai metodi tradizionali di valutazione del rischio.

Analisi di 9 categorie di minacce

- Web
- Salute del DNS / Phishing
- Gestione delle patch
- Reputazione IP
- Sicurezza web
- Sicurezza della posta elettronica
- Filtraggio dei documenti
- Filtraggio delle credenziali
- Social Networking



Strato AI. Consente un funzionamento automatizzato al 100% senza l'intervento umano in qualsiasi parte del processo.



Funzionamento continuo 365x24x7. Permette di individuare le nuove fughe di informazioni in tempo quasi reale.



Strumento rigorosamente non intrusivo. La ricerca è condotta su Internet, Deep Web e Dark Web e non attacca il perimetro IT delle aziende. Le informazioni ottenute rispettano scrupolosamente i limiti imposti dalla legislazione.



Massima facilità d'uso. Nessuna configurazione complessa. Tutto quello che è necessario fare è inserire il dominio nella piattaforma e tutto funziona in modo autonomo, senza la necessità di configurare i parametri di ricerca o qualsiasi altro criterio per individuare le informazioni.



L'unica piattaforma che analizza **conversazioni sui social media** dal punto di vista del rilevamento delle minacce e degli attacchi, al di là di quelli legati alla reputazione e al branding



Monitoraggio automatizzato, oggettivo e continuo dei rischi causati da terzi appartenenti all'Amministrazione o di superfici di attacco esterne ad essa

Company

Ogni azienda ha le sue esigenze e tutte, a prescindere dalle loro dimensioni, hanno bisogno di ridurre il loro livello di rischio. La vostra protezione è la protezione della vostra azienda, dei terzi e delle persone con cui lavorano e che servono.

Third Party

Sfruttano il funzionamento non intrusivo di Kartos per offrire alle aziende la possibilità di monitorare il livello di rischio nella loro catena del valore. Progettato per essere acquistato in pacchetti di licenze con diverse funzionalità, in modo che le aziende possano costruire il sistema di sorveglianza più adatto alle loro esigenze in termini di funzionalità e di prezzo.

LICENZE

LITE

Ogni azienda ha le sue esigenze e tutte, a prescindere dalle loro dimensioni, hanno bisogno di ridurre il loro livello di rischio. La vostra protezione è la protezione della vostra azienda, dei terzi e delle persone con cui lavorano e che servono

FUNZIONAMENTO

1



Acquisizione della licenza

Ogni licenza viene fornita con un numero di domini, che può aumentare in base alle esigenze.

2



Registrazione nella piattaforma

L'amministratore è registrato sulla piattaforma Kartos.

3



Introduzione dei domini:

L'amministratore inserisce nella piattaforma Kartos i domini che vuole monitorare e analizzare.

Kartos inizierà a operare da quel momento in poi, monitorando, analizzando e segnalando in tempo reale 24x7 le vulnerabilità in ciascuna delle 9 categorie dei domini introdotti.

4



Personalizzazione dello strumento

L'amministratore può configurare la ricezione di specifiche vulnerabilità, registrare altri utenti alla piattaforma, progettare il tipo di permessi, utilizzare che ciascun utente avrà e creare liste di domini per aree o dipartimenti aziendali.