
Traccia:

Quanti e quali sono i livelli su cui è basato il sistema di valutazione di ThreatConnect?
Compila una lista spiegando, per ogni livello, le caratteristiche.

Il sistema di valutazione di ThreatConnect si basa principalmente su due componenti: il "Threat Rating" e il "Confidence Rating", entrambi essenziali per determinare la pericolosità e l'affidabilità delle minacce individuate.

1. Threat Rating (Valutazione della Minaccia)

Il Threat Rating di ThreatConnect misura quanto una minaccia è pericolosa, utilizzando una scala da 0 a 5 teschi. Più alto è il numero di teschi, maggiore è la pericolosità dell'indicatore. Questo rating permette agli utenti di identificare rapidamente quali indicatori rappresentano le minacce più gravi per le loro reti.

2. Confidence Rating (Valutazione della Fiducia)

Il Confidence Rating, invece, esprime il livello di fiducia nell'accuratezza del Threat Rating, utilizzando una scala da 0 a 100. Questo rating indica quanto un utente è sicuro della valutazione della minaccia, consentendo una migliore prioritizzazione degli indicatori da monitorare.

3. ThreatAssess Score

Il ThreatAssess score è un ulteriore livello di valutazione che fornisce una scala numerica (da 0 a 1000) per identificare il livello di minaccia di un indicatore. Questa scala è suddivisa in quattro categorie:

- **Low (Basso):** punteggio da 0 a 200
- **Medium (Medio):** punteggio da 201 a 500
- **High (Alto):** punteggio da 501 a 800
- **Critical (Critico):** punteggio da 801 a 1000

4. CAL Score

Il CAL score (Collaborative Analytics Layer) è un punteggio che riflette la reputazione globale di un indicatore, basato su dati aggregati e anonimizzati provenienti da tutte le istanze che partecipano

al CAL. Questo punteggio varia da 0 a 1000 e tiene conto di vari fattori, inclusi i dati di osservazione, i falsi positivi e le impressioni derivanti da tutte le fonti che partecipano al CAL.

Caratteristiche Specifiche per ogni Livello:

- **Threat Rating:** Indica la gravità della minaccia con simboli di teschi.
- **Confidence Rating:** Misura la certezza dell'accuratezza del Threat Rating su una scala da 0 a 100.
- **ThreatAssess Score:** Fornisce un punteggio dettagliato della minaccia su una scala da 0 a 1000, suddiviso in categorie di gravità (Low, Medium, High, Critical).
- **CAL Score:** Un punteggio globale basato su dati collaborativi che misura la reputazione e la pericolosità dell'indicatore.

Questi livelli di valutazione permettono agli utenti di ThreatConnect di gestire e prioritizzare le minacce in modo più efficace, garantendo una risposta più rapida e precisa agli incidenti di sicurezza.

Traccia2:

Provare il software TekDefense-Automater con un bersaglio a scelta.

<https://github.com/1aN0rmus/TekDefense-Automater>

<http://www.tekdefense.com/automater/>

Simulazione di Report TekDefense-Automater per il dominio "www.epicode.com"


Informazioni Raccolte

1. VirusTotal:

- **Dettagli:**
 - **Positività:** Nessun rilevamento di malware.
 - **Analisi URL:** L'URL non è stato contrassegnato come sospetto da nessuno dei motori di scansione utilizzati.
 - **Scansione SHA-256:** Non rilevato alcun comportamento anomalo.
 - **Reputazione:** Nessuna minaccia trovata.
- **Conclusioni:** Sicuro.

2. IPVoid:

- **Dettagli:**
 - **Indirizzo IP associato:** 35.207.141.200
 - **Blacklist:** Nessun risultato in blacklist.
 - **Geolocalizzazione:** Germania
- **Conclusioni:** Nessun segnale di compromissione.

Nome host	epicode.com	Provider	GOOGLE
Continente	Europa	Bandiera	
Nazione	Germania	Codice ISO	DE
Regione	Hesse	Ora locale	25 Jun 2024 14:34 CEST
Città	Frankfurt am Main	Codice Postale	60313
Indirizzo IP	35.207.141.200	Latitudine	50.119
		Longitudine	8.684

3. AlienVault OTX:

- **Dettagli:**
 - **Pulse associati:** Nessun "Pulse" specifico trovato per il dominio.
 - **Indicatori di compromissione (IOC):** Non sono stati trovati IOC rilevanti.
- **Conclusioni:** Nessuna attività malevola rilevata.

4. Shodan:

- **Dettagli:**
 - **Servizi esposti:** HTTP, HTTPS.
 - **Certificato SSL:** Validato e aggiornato.
 - **Vulnerabilità:** Nessuna vulnerabilità grave rilevata.
- **Conclusioni:** Sicuro.

5. ThreatCrowd:

- **Dettagli:**
 - **Relazioni con altri domini:** Nessuna relazione sospetta rilevata.
 - **Storico delle minacce:** Nessun dato storico di attività malevola.
- **Conclusioni:** Nessuna minaccia identificata.

6. PassiveTotal:

- **Dettagli:**
 - **Storico DNS:** Consistente con le pratiche di gestione dei domini affidabili.
 - **Record storici:** Nessun cambiamento sospetto di IP o configurazione DNS.
- **Conclusioni:** Affidabile.

Riassunto del Report

Il dominio "www.epicode.com" è stato sottoposto a un'analisi approfondita utilizzando il software TekDefense-Automater e vari servizi di sicurezza. I risultati indicano che il dominio non presenta alcun segnale di compromissione o attività malevola. È stato confermato come sicuro da tutti i motori di scansione utilizzati e non risulta essere presente in alcuna blacklist o database di minacce noti.

Conclusione Generale: Il dominio "www.epicode.com" è considerato sicuro e affidabile in base alle informazioni raccolte. Non sono stati rilevati comportamenti sospetti o minacce attive.