ESERCIZIO W19D1 - Minacce Comuni

RICHIESTA

In relazione allo studio del capitolo sulla Threat Intelligence, allo studente è richiesto di evidenziare quali e quanti sono i livelli su cui è basato il sistema di valutazione di ThreatConnect e, per ognuno di questi, descriverne le caratteristiche.

~~~

SOLUZIONE

Prima di analizzare il sistema di valutazione di ThreatConnect, è utile fare una panoramica sulla piattaforma. ThreatConnect è una **piattaforma di Cyber Threat Intelligence (CTI)**, progettata per aiutare le organizzazioni a gestire in modo più efficace le minacce informatiche.

Fra i suoi punti di forza, spiccano la capacità di raccogliere, analizzare e contestualizzare un gran numero di informazioni sulle minacce, il supporto ai team di sicurezza nelle attività quotidiane e l'aiuto nel quantificare il rischio per ogni azienda, in relazione alle minacce informatiche.

Con il suo sistema di valutazione, ThreatConnect considera una vasta serie di aspetti, come ad esempio:

- Indicatori di Compromissione (IoC)
- Tattiche, Tecniche e Procedure (TTP) degli avversari
- Attori delle minacce
- Campagne di attacco
- Vulnerabilità
- Rischio ed efficacia delle difese

Volendo sintetizzare in poche righe, la forza di ThreatConnect risiede nel trasformare un flusso spesso caotico di dati sulle minacce in informazioni strategiche, dando così la possibilità alle organizzazioni di prepararsi nel migliore dei modi alle possibili minacce informatiche.

~~~

ANNOTAZIONI TECNICHE E CLASSIFICAZIONI

Il sistema di classificazione di ThreatConnect si basa su due parametri fondamentali e distinti per valutare ogni elemento di minaccia, la **Confidence** (Valutazione della Fiducia) e il **Rating** (Valutazione della Minaccia):

- **La Confidence**, detta anche Valutazione della Fiducia, indica quanto la piattaforma è sicura dell'accuratezza e dell'affidabilità dell'informazione sulla minaccia.
- **Il Rating**, detto anche Valutazione della Minaccia, esprime invece la gravità o pericolosità intrinseca di quella minaccia.

Come evidenziato, i due parametri sono completamente indipendenti l'uno dall'altro: una minaccia può avere un'altissima pericolosità, ma le informazioni su di essa sono scarse o di bassa qualità.

ThreatConnect valuta la Confidence sulla minaccia con **un valore numerico da 0 a 100**, con le informazione che ricadono, a seconda del loro valore numerico, in una di queste sei categorie:

- Al valore 0 corrisponde il grado **Screditato/Inesistente**: è stato confermato che l'informazione è inaccurata o che comunque l'informazione stessa non gode di nessuna fiducia
- Ai valori compresi fra 1 e 29 corrisponde il grado **Dubbioso/Scarsa Fiducia**: in questo caso il grado di accuratezza dell'informazione è molto basso
- Ai valori compresi fra 30 e 49 corrisponde il grado **Possibile/Bassa-Media Fiducia**: in questo caso il grado di accuratezza dell'informazione è medio, e potrebbe dunque essere plausibile. Mancano però conferme significative
- Ai valori compresi fra 50 e 69 corrisponde il grado **Probabile/Media Fiducia**: in questo caso c'è una buona probabilità che l'informazione sia accurata
- Ai valori compresi fra 70 e 89 corrisponde il grado **Molto Probabile/Alta Fiducia**: La fiducia nell'accuratezza dell'informazione è alta, con il supporto di diverse fonti o un importante lavoro di fact-checking interno
- A valori superiori all'89 (da 90 a 100) corrisponde il grado **Confermato/Altissima Fiducia**: in questo caso l'informazione è stata confermata come accurata da fonti indipendenti o da un'analisi approfondita e diretta. È il grado di Confidence più alto.

L'uso di un valore numerico per la Confidence in ThreatConnect permette una gestione molto più precisa, dinamica e automatica della threat intelligence. Questo dà la possibilità alle organizzazioni di reagire in modo proporzionato all'affidabilità delle informazioni sulle minacce.

Type	Value	Confirmation	Plausibility	Consistency
Unknown	0	Unknown; has not been assessed		
Discredited	1	Confirmed as inaccurate		
Improbable	2–29	Unconfirmed	Not logical or plausible	Contradicted by other information
Doubtful	30–49	Unconfirmed	Possible, but not logical	No additional information on subject
Possible	50–69	Unconfirmed	Reasonably logical	Some consistencies with other information
Probable	70–89	Unconfirmed	Logical and plausible	Consistent with other information on the subject
Confirmed	90–100	Confirmed to be accurate by independent sources and analysis		

A differenza della Confidence, il Rating delle minacce non utilizza valori numerici ma **una scala predefinita composta da sei possibili valori**. Alla base della scala c'è il grado Undetermined, al vertice c'è il grado Very High. La scala è composta in questo modo:

- **Undetermined (Non Determinato)**: È il grado più basso della scala e indica l'impossibilità di assegnare un Rating a causa della mancanza di informazioni. Questo non implica il fatto che non esista la minaccia, e che non possa essere pericolosa
- **Suspicious (Sospetto)**: il secondo grado della scala è assegnato quando una minaccia, pur senza prove dirette della sua pericolosità, mette in atto comportamenti ambigui e comunque sospetti
- **Low (Basso)**: il terzo grado della scala è assegnato a minacce di basso impatto o con funzionalità limitate. Ricadono in questa categoria tutti gli attacchi poco sofisticati
- **Medium (Medio)**: il quarto grado della scala è assegnato a minacce con un potenziale di impatto moderato. A questo livello, potrebbe già essere necessario prendere provvedimenti
- **High (Alto)**: il quinto grado della scala è assegnato a minacce significativa, con un alto potenziale di impatto per l'organizzazione. Ricadono in questa categoria diversi tipi di malware, ed è necessario intervenire in maniera tempestiva
- **Very High (Molto Alto)**: è il vertice della scala, ed è assegnato alle minacce dal grado di pericolosità massimo. Fra questi si possono citare i ransomware o gli exploit zero-day. La risposta dev'essere immediata e robusta

Level	Label	Capability	Determination	Progression
0	Unknown	Not enough information to assess threat		
1	Suspicious	Unknown		No confirmed malicious activity (some suspicious activity has been observed)
2	Low	Unsophisticated	Purely opportunistic and short lived	Pre-attack activity or attempt (potential to turn into a large threat)
3	Moderate	Basic skills and resources	Directed, but not persistent	Active intrusion (delivery, exploitation, installation)
4	High	Advanced skills and resources	Targeted and persistent	Post-compromise (C2, actions on objective)
5	Critical	Unlimited skill and resources	Wholly focused and determined	Any phase of progression

In conclusione, la Confidence esprime quanto ci si può fidare di un'informazione, il Threat Rating esprime quanto quella minaccia sia grave e quale sia il suo potenziale impatto. L'analisi fatta combinando entrambi i parametri rende ThreatConnect potente e molto utile nella pratica.