1- Come funziona

ThreatConnect è una piattaforma di intelligence che aiuta le organizzazioni a gestire, analizzare e rispondere alle minacce alla sicurezza informatica. Il sistema di valutazione di ThreatConnect si basa su una serie di caratteristiche che sono organizzate in diversi livelli:

Livello 1: **Raccolta delle informazioni**

In questo livello, ThreatConnect si concentra sulla raccolta di informazioni di base legate alle minacce. Le caratteristiche principali includono:

Aggregazione dei dati: ThreatConnect raccoglie dati da diverse fonti, come feed di intelligence, report degli analisti e dati interni dell'organizzazione.

Normalizzazione: i dati raccolti vengono normalizzati e resi uniformi in modo che possano essere facilmente analizzati e correlati.

Classificazione: le informazioni vengono categorizzate in base al tipo di minaccia, come malware, phishing, attacchi DDoS, etc.

Identificazione dell'attore: vengono identificati gli attori responsabili delle minacce, come gruppi di hacker noti o entità sponsorizzate dallo Stato.

Livello 2: **Analisi delle informazioni**

In questo livello, l'attenzione di ThreatConnect si sposta sull'analisi delle informazioni raccolte durante la fase 1, per ottenere una comprensione più approfondita delle minacce. Le caratteristiche principali includono:

Analisi delle relazioni: le informazioni vengono analizzate per identificare le relazioni (ed eventuali correlazioni) tra diverse entità e attività.

Ricerca di indicatori di compromissione: vengono individuati gli indicatori che possono segnalare una possibile compromissione dei sistemi o delle reti.

Analisi del contesto: le informazioni vengono valutate nel contesto più ampio delle minacce esistenti per identificare potenziali tendenze o *pattern*.

Individuazione di campagne: viene identificata la presenza di campagne di attacco mirate o correlate.

Livello 3: **Condivisione e collaborazione**

Questo livello riguarda la condivisione delle informazioni e la collaborazione tra diverse organizzazioni per affrontare le minacce in modo collettivo. Le caratteristiche principali includono:

Scambio di intelligence: le informazioni vengono condivise con altre organizzazioni di fiducia per fornire una visione più completa delle minacce.

Piattaforma di collaborazione: ThreatConnect fornisce strumenti per la collaborazione in tempo reale tra analisti e team di sicurezza.

Conformità alle norme: le informazioni vengono condivise in conformità con le leggi e le politiche di condivisione dell'intelligence.

Accesso controllato: l'accesso alle informazioni condivise è gestito in modo sicuro e controllato per garantire la riservatezza.

Livello 4: **Risposta e mitigazione delle minacce**

In questo livello, ThreatConnect supporta la risposta e la mitigazione delle minacce attraverso la gestione delle informazioni e la collaborazione. Le caratteristiche principali includono:

Automazione delle risposte: le azioni di risposta automatica vengono attivate in base alle informazioni e alle regole definite.

Creazione di playbook: vengono sviluppati playbook per guidare le risposte agli attacchi noti e alle minacce comuni.

Monitoraggio della mitigazione: viene monitorata l'efficacia delle misure di mitigazione adottate per valutare l'impatto delle azioni intraprese.

Feedback del sistema: le informazioni sulle minacce e le azioni di mitigazione vengono utilizzate per migliorare continuamente la capacità di risposta e la difesa contro futuri attacchi.

Questi sono i principali livelli e le relative caratteristiche del sistema di valutazione di ThreatConnect. La piattaforma offre una serie di funzionalità avanzate che aiutano le organizzazioni a comprendere, rispondere e mitigare le minacce alla sicurezza informatica in modo efficace.

2- Valutazione delle informazioni

ThreatConnect utilizza un sistema di valutazione delle informazioni per assegnare un livello di affidabilità e di rilevanza a ciascuna fonte di intelligence o a ciascun indicatore di minaccia. Questo sistema di valutazione aiuta gli utenti a determinare l'attendibilità delle informazioni e a prendere decisioni informate sulla base di tali valutazioni. Il sistema di valutazione delle informazioni di ThreatConnect si basa sui seguenti parametri:

Fiducia:

Affidabilità della fonte: viene valutata l'affidabilità storica e l'accuratezza delle informazioni fornite dalla fonte. Ad esempio, una fonte di intelligence ben nota e affidabile potrebbe avere una valutazione di fiducia più alta rispetto a una fonte meno conosciuta o dubbia.

Accuratezza dei dati: viene valutata l'accuratezza e la coerenza delle informazioni fornite dalla fonte. Gli indicatori di minaccia provenienti da fonti che hanno dimostrato una maggiore precisione nel passato potrebbero ricevere una valutazione di fiducia più alta.

Rilevanza:

Pertinenza al contesto: viene valutata la pertinenza delle informazioni rispetto alle minacce e alle operazioni dell'organizzazione. Le informazioni che sono direttamente rilevanti per l'ambiente e le tecnologie utilizzate dall'organizzazione possono ricevere una valutazione di rilevanza più alta.

Specificità delle informazioni: viene valutata la specificità delle informazioni fornite. Le informazioni che sono dettagliate e forniscono un contesto più completo sulle minacce possono ricevere una valutazione di rilevanza più alta rispetto a informazioni generiche o vaghe.

In base a questi criteri, ogni fonte di intelligence o indicatore di minaccia viene assegnato un punteggio di fiducia e un punteggio di rilevanza. Questi punteggi possono variare da una scala di valutazione, ad esempio da 1 a 10, o essere espressi tramite termini qualitativi come "bassa", "media" o "alta".

Gli utenti di ThreatConnect possono utilizzare questi punteggi di fiducia e rilevanza per filtrare e prioritizzare le informazioni. Ad esempio, possono concentrarsi sulle fonti con un alto punteggio di fiducia o dare maggiore attenzione agli indicatori di minaccia con un punteggio di rilevanza elevato per prendere decisioni informate sulla base delle informazioni disponibili.

È importante sottolineare che il sistema di valutazione delle informazioni può essere personalizzato e configurato secondo le esigenze specifiche dell'organizzazione, consentendo di adattare i criteri di fiducia e rilevanza in base alle proprie politiche e requisiti di sicurezza.

La scala di punteggi assegnati per la valutazione delle informazioni in ThreatConnect può variare a seconda delle preferenze e delle configurazioni specifiche dell'organizzazione. Tuttavia, posso fornirti un esempio generale di come potrebbe essere strutturata la scala di valutazione:

Fiducia:

Basso: 1-3 - Indica una fonte di intelligence o un indicatore di minaccia poco affidabile o con una storia di scarsa accuratezza.

Medio: 4-7 - Indica una fonte di intelligence o un indicatore di minaccia relativamente affidabile con una moderata accuratezza.

Alto: 8-10 - Indica una fonte di intelligence o un indicatore di minaccia altamente affidabile con una comprovata accuratezza e coerenza.

Rilevanza:

Basso: 1-3 - Indica informazioni poco pertinenti o di scarsa specificità per l'ambiente o le operazioni dell'organizzazione.

Medio: 4-7 - Indica informazioni abbastanza pertinenti e specifiche per l'ambiente o le operazioni dell'organizzazione.

Alto: 8-10 - Indica informazioni altamente pertinenti e specifiche che forniscono un contesto approfondito sulle minacce rilevanti per l'organizzazione.

La personalizzazione della scala di punteggi consente di adattare il sistema di valutazione alle esigenze specifiche dell'organizzazione e di riflettere meglio i criteri di fiducia e rilevanza ritenuti più importanti.

3- Confidence Level

Il "*confidence level*" (livello di fiducia) in ThreatConnect rappresenta una misura dell'affidabilità o della certezza associata a una determinata fonte di intelligence, un'analisi o un'indicazione di minaccia. Questo livello di fiducia viene assegnato a ogni elemento per indicare quanto l'organizzazione può fare affidamento su di esso nelle decisioni di sicurezza.

Il "*confidence level*" di ThreatConnect si basa su una scala da 0 a 100, dove valori più alti indicano una maggiore fiducia nelle informazioni. Ecco alcuni punti chiave per comprendere come funziona il "confidence level":

Fonti e indicatori di fiducia: I livelli di fiducia sono assegnati a diverse fonti di intelligence, come feed di informazioni, report di analisti o dati interni, nonché agli indicatori di minaccia derivati da tali fonti.

Valutazione oggettiva: La valutazione del "confidence level" è basata su criteri oggettivi e su un'analisi approfondita delle informazioni disponibili. Viene considerata l'affidabilità storica della fonte, l'accuratezza delle informazioni fornite e la coerenza delle segnalazioni nel tempo.

Scenari di valutazione: Il livello di fiducia viene valutato per ciascuna fonte o indicatore in diversi scenari, ad esempio, per la fonte stessa o per l'indicatore in base alle specifiche circostanze o all'entità a cui si riferisce.

Personalizzazione: Le organizzazioni possono personalizzare le categorie o i livelli di fiducia per rispecchiare le proprie esigenze e priorità specifiche. Ciò consente loro di adattare il sistema di valutazione alle politiche e alle considerazioni di sicurezza dell'organizzazione.

Supporto decisionale: I livelli di fiducia assegnati alle informazioni aiutano gli analisti e i team di sicurezza a valutare la credibilità delle fonti, l'attendibilità degli indicatori di minaccia e la base su cui prendere decisioni informate.

È importante sottolineare che il "confidence level" è uno strumento di supporto decisionale e non rappresenta una valutazione assoluta dell'accuratezza o della veridicità delle informazioni. Gli analisti e i team di sicurezza devono considerare anche altre fonti di informazione, il contesto e la situazione specifica prima di trarre conclusioni definitive o intraprendere azioni.