Pratica W19D1(2)

EPICODE

Esercizio
Threat Intelligence & IOC

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.

Soluzione:

ThreatConnect è una piattaforma di intelligence sulle minacce che aiuta le organizzazioni a raccogliere, analizzare e rispondere a informazioni sulle minacce informatiche. La sua metodologia di valutazione può variare nel tempo con l'evoluzione del prodotto e delle pratiche di sicurezza. Al momento del mio ultimo aggiornamento (aprile 2023), non esiste un "sistema di valutazione" di ThreatConnect universalmente riconosciuto come tale. Tuttavia, possiamo parlare in termini generali di come le piattaforme di intelligence sulle minacce, simili a ThreatConnect, valutano e gestiscono le informazioni sulle minacce attraverso diversi livelli di analisi e valutazione.

Le piattaforme di threat intelligence lavorano tipicamente su più livelli di informazione e analisi per fornire alle organizzazioni una comprensione profonda delle minacce. Questi livelli possono variare da dettagli tecnici specifici a valutazioni strategiche ampie. Di seguito, una possibile interpretazione dei livelli su cui una piattaforma di intelligence sulle minacce potrebbe basare il suo sistema di valutazione, tenendo presente che la specifica metodologia di ThreatConnect potrebbe differire:

1. Indicatori Tecnici (Indicatori di Compromissione - IoC)

- **Caratteristiche**: Questo livello include dati specifici e osservabili come indirizzi IP malevoli, URL, hash di file, e-mail sospette ecc., che possono indicare una potenziale compromissione della sicurezza.
- **Utilizzo**: Gli IoC sono utilizzati per rilevamenti automatici e risposte in tempo reale, facilitando il blocco o la mitigazione delle minacce conosciute.

2. Tattiche, Tecniche e Procedure (TTP)

- **Caratteristiche**: Questo livello analizza e descrive le modalità operative degli attaccanti, ovvero come tendono a operare e quali strumenti utilizzano. Le TTP aiutano a comprendere il "come" dietro agli attacchi, oltre ai semplici indicatori di compromissione.
- **Utilizzo**: La conoscenza delle TTP supporta lo sviluppo di strategie di difesa più sofisticate, consentendo alle organizzazioni di anticipare e mitigare attacchi futuri.

3. Campagne

- **Caratteristiche**: Una campagna è un insieme di attacchi coordinati che perseguono un obiettivo specifico. Questo livello collega insieme IoC e TTP per identificare e analizzare campagne malevoli.
- **Utilizzo**: Comprendere le campagne aiuta a identificare gli attori delle minacce e le loro motivazioni, migliorando così la preparazione e la risposta agli attacchi.

4. Attori delle Minacce

- **Caratteristiche**: Questo livello si concentra sull'identificazione e l'analisi degli attori delle minacce, come gruppi di hacking, organizzazioni criminali o stati-nazione, inclusi i loro obiettivi, capacità e intenti.
- **Utilizzo**: Analizzare gli attori delle minacce fornisce intuizioni strategiche che aiutano a prevedere minacce future e a sviluppare difese a lungo termine.

5. Intelligence Strategica

- **Caratteristiche**: Al più alto livello, l'intelligence strategica riguarda l'analisi delle tendenze globali delle minacce, delle politiche di sicurezza e delle strategie di mitigazione a livello macroscopico.
- **Utilizzo**: Queste informazioni sono cruciali per i decision-maker per sviluppare politiche di sicurezza, allocare risorse e pianificare in modo proattivo la difesa contro le minacce emergenti.

È importante notare che la specifica implementazione e il dettaglio di questi livelli possono variare notevolmente tra le diverse piattaforme di intelligence sulle minacce e possono evolvere nel tempo in risposta all'evoluzione del paesaggio delle minacce informatiche. La collaborazione e la condivisione di informazioni all'interno e tra le organizzazioni rimangono fondamentali per una difesa efficace contro le minacce informatiche.