Minacce comuni

Sommario

Traccia esercizio principale

Quanti e quali sono i livelli su cui è basato il sistema di valutazione di ThreatConnect?

Analizza la lista di best practice ThreatConnect:
https://knowledge.threatconnect.com/docs/best-practices-indicator-threat-and-confidence-ratings

Compila una lista spiegando, per ogni livello, le caratteristiche.

Traccia esercizio facoltativo

Creare un elenco di minacce comuni che possono colpire un'azienda, ad esempio phishing, malware, attacchi DDoS, furto di dati.

- Inizia raccogliendo informazioni sulle minacce alla sicurezza informatica, utilizzando fonti aperte, i siti web di sicurezza informatica e i forum di discussione.
- Analizza ciascuna minaccia in dettaglio, cercando di comprendere il modo in cui può essere utilizzata per compromettere la sicurezza informatica e i danni che può causare.
- Utilizza queste informazioni per creare un elenco delle minacce più comuni, tra cui malware, attacchi di phishing e attacchi DDoS aggiungendo tutte le informazioni raccolte dall'analisi.

Suggerimento: dare una breve lettura al rapporto Clusit https://clusit.it/rapporto-clusit/

Svolgimento esercizio

Il sistema di valutazione di ThreatConnect si basa su due dimensioni principali: il **Threat Rating** e il **Confidence Rating**. Ciascuno di questi parametri è strutturato in livelli che rappresentano la gravità della minaccia e il livello di fiducia nell'accuratezza della valutazione.

Threat Rating

Il **Threat Rating** è un indicatore della pericolosità della minaccia associata, suddiviso in sei livelli (da 0 a 5):

1. Unknown
    a. Caratteristiche: Mancanza di informazioni sufficienti per valutare la minaccia.
    b. Esempio: Indicatori in fase di analisi iniziale, senza dettagli sufficienti.
2. Suspicious
    a. Caratteristiche: Attività sospetta, ma senza conferma di dannosità.
    b. Esempio: Accesso frequente a un URL da parte degli utenti, senza apparenti minacce immediate.
3. Low Threat
    a. Caratteristiche: Adversario poco sofisticato, potenzialmente opportunistico e con breve durata.
    b. Esempio: Scansioni su una porta specifica da un netblock conosciuto.
4. Moderate Threat
    a. Caratteristiche: Adversario con competenze di base; attività mirata ma non persistente.
    b. Esempio: Documento che simula un memo aziendale e prende di mira un dipartimento specifico.
5. High Threat
    a. Caratteristiche: Adversario avanzato e determinato; attività persistente e mirata.
    b. Esempio: Log di accesso multipli legati a un documento malevolo diffuso.
6. Critical Threat
    a. Caratteristiche: Adversario altamente qualificato e con risorse illimitate, capace di attacchi in qualsiasi fase di intrusione.
    b. Esempio: Esfiltrazione di dati sensibili a un host man-in-the-middle, richiede una risposta immediata.

Confidence Rating

Il Confidence Rating rappresenta la fiducia nell'accuratezza della valutazione dell'indicatore, suddiviso in sette livelli:

1. Unknown (0)
    - Caratteristiche: Valutazione non effettuata o non assegnata.
2. Discredited (1)
    - Caratteristiche: La valutazione è stata confermata come inaccurata.
    - Esempio: File innocuo erroneamente identificato come malware.
3. Improbable (2–29)
    - Caratteristiche: Valutazione non confermata e illogica o non plausibile.
    - Esempio: Host C2 smantellato; l'indicatore potrebbe essere obsoleto.
4. Doubtful (30–49)
    - Caratteristiche: Valutazione possibile ma non logica, senza altre informazioni di supporto.
    - Esempio: IP di scansione da provider VPS, necessità di ulteriori verifiche.
5. Possible (50–69)
    - Caratteristiche: Valutazione non confermata, ma con alcune prove logiche o parzialmente consistenti.
    - Esempio: Indirizzo email simile a quello usato in un malware ma comune.
2. Probable (70–89)
    - Caratteristiche: Valutazione logica e plausibile, compatibile con altre informazioni disponibili.
    - Esempio: URL con caratteristiche simili a URL dannosi conosciuti su un host diverso.
3. Confirmed (90–100)
    - Caratteristiche: Valutazione confermata da analisi indipendenti o dirette.
    - Esempio: File eseguibile che distribuisce una variante di malware nota.

Best Practice per l'utilizzo di Threat Rating e Confidence Rating

1. Definire Standard di Valutazione
   Standardizzare i significati di ciascun livello di Threat Rating e Confidence Rating garantisce che gli analisti e i team abbiano una comprensione uniforme delle minacce.
2. Automatizzare la Deprecazione del Confidence Rating
   Configurare un sistema per ridurre automaticamente il Confidence Rating degli indicatori non aggiornati permette di eliminare gradualmente quelli obsoleti, garantendo un database rilevante.
3. Utilizzare Combinazioni di Rating per Attività Automate
   Configurare applicazioni per avviare azioni automatiche, come scansioni di rete o blocchi, basate su specifiche combinazioni di Threat Rating e Confidence Rating.
4. Aggiornare e Verificare Costantemente i Ratings
   Verificare regolarmente la precisione dei Confidence Ratings, soprattutto per indicatori con alti livelli di minaccia, per garantire che rimangano attuali e pertinenti.
5. Collaborare con la Community
   Contribuire a comunità di intelligence condividendo indicatori valutati accuratamente può migliorare le difese collettive contro le minacce.

Questi livelli e le best practice forniscono un quadro completo per gestire in modo efficace gli indicatori di minaccia all'interno di un'organizzazione.

Svolgimento esercizio facoltativo

1. Phishing

Descrizione: Il phishing è un attacco di ingegneria sociale in cui i criminali inviano email o messaggi fraudolenti progettati per ingannare gli individui e farli rivelare informazioni sensibili come password, numeri di carte di credito o altri dati personali.

Impatto:

- **Perdite Finanziarie:** Accesso non autorizzato ai conti finanziari può causare perdite dirette.
- **Violazione dei Dati:** Credenziali compromesse possono essere utilizzate per accedere illegalmente alle reti aziendali.
- **Danno alla Reputazione:** La divulgazione pubblica di un attacco di phishing può danneggiare la reputazione dell'azienda.

2. Malware

Descrizione: Il malware è un termine generico per software dannoso progettato per interrompere, danneggiare o ottenere accesso non autorizzato a un sistema informatico. Questo include virus, worm, cavalli di Troia, ransomware, spyware e adware.

Impatto:

- **Perdita dei Dati:** Il malware può eliminare o crittografare dati importanti.
- **Interruzione del Sistema:** Il malware può causare crash o rallentamenti del sistema, interrompendo le operazioni aziendali.
- **Furto dei Dati:** Alcuni tipi di malware sono progettati per rubare dati sensibili.
- **Perdite Finanziarie:** Il ransomware richiede un pagamento in cambio delle chiavi di decrittazione.

3. Attacchi DDoS

Descrizione: Gli attacchi DDoS (Distributed Denial of Service) coinvolgono l'inondazione di un bersaglio con traffico per renderlo inaccessibile agli utenti legittimi.

Impatto:

- **Tempo di Inattività del Servizio:** Il sito web o il servizio target diventano inaccessibili, causando interruzioni nelle operazioni aziendali.
- **Perdite Finanziarie:** Il tempo di inattività può causare perdite di ricavi e costi aggiuntivi per mitigare l'attacco.
- **Danno alla Reputazione:** Interruzioni prolungate possono danneggiare la reputazione dell'azienda.

4. Violazione dei Dati

Descrizione: Una violazione dei dati si verifica quando dati sensibili, confidenziali o protetti vengono accessi o divulgati senza autorizzazione.

Impatto:

- **Perdite Finanziarie:** Sanzioni e multe per non conformità alle normative sulla protezione dei dati.
- **Danno alla Reputazione:** Perdita di fiducia dei clienti e possibili azioni legali.
- **Interruzione Operativa:** Tempo e risorse spesi per la risposta agli incidenti e il recupero.

5. Minacce Interne

Descrizione: Le minacce interne provengono da all'interno dell'organizzazione, come dipendenti, consulenti o partner che hanno accesso a informazioni sensibili.

Impatto:

- **Furto dei Dati:** Gli insider possono esfiltrare dati sensibili per guadagno personale o per venderli a concorrenti.
- **Sabotaggio del Sistema:** Gli insider possono intenzionalmente interrompere i sistemi o i processi.
- **Danno alla Reputazione:** Le azioni degli insider possono portare a pubblicità negativa.

6. Password Deboli o Rubate

Descrizione: Password deboli o rubate possono essere sfruttate da attaccanti per ottenere accesso non autorizzato a sistemi e dati.

Impatto:

- **Violazione dei Dati:** Accesso non autorizzato a dati sensibili.
- **Compromissione del Sistema:** Gli attaccanti possono installare malware o eseguire altre attività dannose.
- **Perdite Finanziarie:** Credenziali rubate possono essere utilizzate per frodi finanziarie.

7. Vulnerabilità Non Corrette

Descrizione: Vulnerabilità del software che non vengono corrette possono essere sfruttate dagli attaccanti.

Impatto:

- **Violazione dei Dati:** Accesso non autorizzato a dati sensibili.
- **Compromissione del Sistema:** Gli attaccanti possono ottenere il controllo sui sistemi.
- **Interruzione Operativa:** Vulnerabilità sfruttate possono causare il fallimento del sistema.

8. Attacchi Man-in-the-Middle (MitM)

Descrizione: Gli attacchi MitM avvengono quando un attaccante intercetta la comunicazione tra due parti per spiare o manipolare i dati.

Impatto:

- **Furto dei Dati:** Dati intercettati possono includere informazioni sensibili.
- **Manipolazione dei Dati:** Gli attaccanti possono modificare i dati in transito.
- **Danno alla Reputazione:** Comunicazione compromessa può portare alla perdita di fiducia.

9. Minacce Persistenti Avanzate (APT)

Descrizione: Gli APT sono attacchi prolungati e mirati in cui un utente non autorizzato ottiene accesso a una rete e rimane indetectato per un periodo esteso.

Impatto:

- **Furto dei Dati:** Esfiltrazione furtiva di dati sensibili.
- **Compromissione del Sistema:** Controllo a lungo termine sui sistemi.
- **Interruzione Operativa:** Degradazione graduale delle operazioni.