EPICODE

ESERCIZIO W19D1

MINACCE COMUNI

Mungiovì Fabio

TASK

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.

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/

ESECUZIONE

Il sistema di valutazione di ThreatConnect si basa su due pilastri principali, ognuno con i propri livelli per aiutarci a capire meglio le minacce.
Possiamo immaginare questi due pilastri come due termometri che misurano cose diverse: uno misura quanto è "cattiva" una minaccia, l'altro quanto siamo "sicuri" di quella valutazione.

Valutazione della Minaccia (Threat Rating)

Questa valutazione ci dice quanto è pericoloso un "Indicatore", che potremmo pensare come un segnale di allarme. È misurata su una scala da 0 a 5, rappresentata da teschi 💀, dove più teschi ci sono, più la minaccia è grave.

- **Sconosciuta**: Quando vediamo questo livello, significa che non abbiamo abbastanza informazioni per capire quanto sia pericolosa la minaccia.
- **Sospetta** 💀 **:** In questo caso, non c'è ancora una conferma che la minaccia sia realmente "cattiva", ma ci sono delle attività che non tornano, che ci fanno pensare che qualcosa non vada.
- **Minaccia Bassa** 💀💀: Qui parliamo di un avversario non molto sofisticato, che agisce in modo un po' casuale e le cui azioni sono spesso di breve durata. Oppure, potrebbe indicare attività che precedono un attacco, come un "avvicinamento" prima di entrare in casa.
- **Minaccia Moderata** 💀💀💀: A questo livello, l'avversario è più capace, agisce in modo più mirato e determinato.
  È il momento in cui l'attacco è in corso, magari quando si cerca di "entrare" nel sistema o di "installare" qualcosa di indesiderato.
- **Minaccia Alta** 💀💀💀💀: Questa minaccia è attribuita a un avversario molto avanzato, e significa che un'attività mirata e persistente è già avvenuta.
- **Minaccia Critica** 💀💀💀💀💀: Questo è il livello più grave, riservato agli indicatori che provengono da avversari estremamente abili e con molte risorse.
  Si tratta di minacce critiche in qualsiasi fase dell'intrusione.

Valutazione della Fiducia (Confidence Rating)

Questa valutazione è un numero tra 0 e 100 e ci dice quanto siamo sicuri che la nostra valutazione della minaccia (quella con i teschi) sia corretta. È come la nostra sensazione di quanto è affidabile il "termometro della minaccia".

- **Non Valutata (0):** Non è stata ancora assegnata una valutazione di fiducia.
- **Screditata (1):** Questo significa che la valutazione precedente si è dimostrata sbagliata.
- **Improbabile (2–29):** La valutazione è possibile, ma non molto logica, e ci sono altre informazioni che la smentiscono direttamente.
- **Dubbiosa (30–49):** La valutazione è possibile, ma non è la conclusione più logica, e non ci sono altre informazioni che la confermano o la smentiscono.
- **Possibile (50–69):** La valutazione non è confermata, è abbastanza logica e si accorda solo con alcune delle informazioni che abbiamo.
- **Probabile (70–89):** La valutazione non è confermata direttamente, ma è logica e coerente con tutte le altre informazioni che abbiamo.
- **Confermata (90–100):** Questa valutazione è stata confermata da fonti indipendenti o da un'analisi diretta, ed è perfettamente logica e coerente.

Entrambe queste valutazioni sono fondamentali per aiutare le organizzazioni a prendere decisioni rapide e precise sull'impatto degli Indicatori, permettendo agli analisti, ai sistemi di difesa e ai leader di comunicare in modo chiaro e standardizzato.

FACOLTATIVO

Minacce Informatiche Comuni per le Aziende

Nel panorama digitale odierno, le aziende devono fare i conti con una serie di minacce informatiche che possono causare danni significativi, sia economici che reputazionali. È fondamentale conoscere queste minacce per potersi difendere in modo efficace. Possiamo immaginare il mondo digitale come una città, e queste minacce come diverse forme di criminalità che cercano di entrare o danneggiare i nostri "edifici" (le nostre aziende).

Malware

Il **malware** è un termine generico che raggruppa tutti i software malevoli, progettati per infiltrarsi o danneggiare un sistema informatico senza il consenso dell'utente.
È come un virus che infetta un organismo, ma in questo caso infetta i computer.
Ne esistono diverse tipologie, ognuna con un suo modo di agire:

Virus: Si attaccano a programmi legittimi e si diffondono quando questi vengono eseguiti, replicandosi.

Worm: Sono programmi autonomi che si replicano e si diffondono attraverso la rete senza bisogno di attaccarsi a un altro programma.

Trojan (Cavallo di Troia): Si mascherano da software legittimi o utili per ingannare gli utenti e farsi installare. Una volta dentro, possono aprire delle "porte" per altri attacchi o rubare dati.

Ransomware: Questo tipo di malware blocca l'accesso ai file o all'intero sistema di un utente, chiedendo un riscatto (in inglese "ransom") per ripristinare l'accesso. Il danno principale è la perdita di accesso ai dati cruciali e il pagamento di somme elevate per recuperarli, ma spesso senza garanzie.

Spyware: Come suggerisce il nome, questi software spiano le attività dell'utente, raccogliendo informazioni personali o aziendali senza il suo consenso, per poi inviarle a terzi.

I danni causati dal malware possono variare dalla corruzione dei dati alla perdita di produttività, fino al furto di informazioni sensibili e all'interruzione delle operazioni aziendali.

Attacchi di Phishing

Il phishing è una tecnica di frode online in cui i criminali cercano di ingannare le vittime per ottenere informazioni sensibili, come password, numeri di carte di credito o dati bancari. Lo fanno mascherandosi da entità affidabili (banche, aziende note, servizi online) tramite email, messaggi o siti web falsi. È come un pescatore (da cui "phishing", che suona come "fishing" in inglese) che getta l'amo sperando che qualcuno abbocchi.

Esistono diverse varianti:

Spear Phishing: È un attacco di phishing mirato a una persona o a un'azienda specifica, spesso con informazioni personalizzate per renderlo più credibile.

Whaling: Un tipo di spear phishing rivolto a figure di alto profilo all'interno di un'azienda, come CEO o dirigenti, per ottenere accessi privilegiati. Qui si va a caccia di balene, i "pezzi grossi".

Smishing: Phishing condotto tramite SMS.

Vishing: Phishing condotto tramite chiamate vocali.

I danni possono includere il furto di credenziali, accessi non autorizzati a sistemi aziendali, frodi finanziarie e compromissioni della reputazione.

Attacchi DDoS (Distributed Denial of Service)

Un attacco **DDoS** mira a rendere un servizio online (come un sito web o un'applicazione) non disponibile, sovraccaricandolo con un'enorme quantità di traffico proveniente da più fonti contemporaneamente. È come se migliaia di persone cercassero di entrare contemporaneamente in un negozio molto piccolo, bloccando l'ingresso e impedendo ai clienti legittimi di accedere.

Questi attacchi utilizzano spesso reti di computer compromessi, chiamati "botnet", che vengono controllati a distanza dal cybercriminale. I danni principali sono l'interruzione dei servizi online, la perdita di entrate durante il blocco e un potenziale danno alla reputazione dell'azienda, dato che i clienti non possono accedere ai servizi.

Furto di Dati

Il **furto di dati** è l'atto di rubare informazioni sensibili, personali o aziendali, senza autorizzazione. Questo può avvenire tramite una serie di metodi, non solo attraverso malware o phishing.
Ad esempio, può capitare tramite l'accesso non autorizzato a database, la compromissione di sistemi poco protetti, o anche tramite dipendenti interni malintenzionati.

- Le informazioni rubate possono includere:
- Dati personali dei clienti (nomi, indirizzi, numeri di previdenza sociale, dati sanitari).
- Informazioni finanziarie (numeri di carte di credito, dettagli bancari).
- Segreti commerciali, proprietà intellettuale, piani aziendali.
- Credenziali di accesso.

Le conseguenze sono gravi: multe salate per violazione della privacy (come quelle previste dal GDPR), perdita di fiducia da parte dei clienti, danni reputazionali, calo delle vendite e svantaggio competitivo.

Queste sono solo alcune delle minacce più comuni, ma il panorama della sicurezza informatica è in continua evoluzione.

Rimanere informati e adottare misure preventive adeguate è fondamentale per proteggere qualsiasi attività.

Rapporti come quello di **Clusit,** che analizza lo stato della sicurezza in Italia, sono strumenti preziosi per comprendere l'entità e le tendenze di queste minacce.