Traccia:

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.

SVOLGIMENTO:
L'argomento di oggi di questo esercizio riguarda la threat intelligence che è fondamentale per valutare gli IOC ovvero degli indicatori di compromissione che sono prove che indicano un intrusione o un attacco informatico in corso o già avvenuto come malware credenziali rubate o sottrazione di dati sensibili.
Questo sistema si basa su due tabelle:
. Threat rating
. Confidence rating

THREAT RATING
scala da 0 a 5
0 = nessuna minaccia: non ci sono abbastanza informazioni per valutare la minaccia
1 = sospetta: minaccia bassa non sono confermate attività malevole ma alcune attività sospette sono state rilevate
2 = bassa: attività preliminare o tentativo che potrebbe crescere, un tentativo semplice molto spesso automatizzato
3 = moderata: competenze e risorse di base, mirato ma non insistente, attività di intrusione come ad esempio sfruttare una vulnerabilità, attacco reale ma non molto avanzato o persistente
4 = alto: competenze e risorse avanzate, mirato e persistente, dopo la compromissione controllo e comando e azioni sugli obiettivi, attacco ben chiaro con obiettivi chiari.
5 = critico: abilità e risorse illimitate, totalmente focalizzato e determinato, progressione qualsiasi fase dell'attacco, attacco di livello massimo condotto da un gruppo molto esperto.

CONFIDENCE RATING
questa scala va da 0 a 100 e viene utilizzata per capire quanto è credibile e accurata un'informazione di threat intelligence

1 = la valutazione ha confermato che la minaccia non è reale, falsi positivi
2 - 29 = improbabile: nessuna conferma ciò che sappiamo non è né logico né plausibile vi è la presenza di informazioni discordanti
30 - 49 = incerta: la valutazione dell'informazione è possibile ma non convincente sono necessarie altre informazioni per identificare la minaccia
50 - 69 = possibile: alcune informazioni indicano un grado di veridicità concreto possibile, mancano solo prove definitive per evidenziare la minaccia.

70 - 89 = probabile: la minaccia non è stata ancora confermata ma ci sono informazioni coerenti e molti segnali che indicano che la minaccia sia reale.
90 - 100 = confermata : l'informazione è stata confermata da diverse fonti si tratta di un dato affidabile al 100% la minaccia risulta reale a valle della valutazione.

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/

INTRODUZIONE ALL'ARGOMENTO
Principali minacce dal punto di vista informatico per le aziende:
Phishing:
descrizione: tecnica che mira ad ingannare l'utente inducendolo a fornire credenziali o dati sensibili spesso tramite email false o pagine web contraffatte molto simili alle originali
modalità di attacco: l'attaccante invia messaggi apparentemente credibili come colleghi, banca ecc.. con link o allegati malevoli
danni: furto di credenziali e dati, accesso ai sistemi dell'azienda non autorizzato, perdite economiche e anche di reputazione.
MALWARE:
descrizione: programmi creati per danneggiare o compromettere i sistemi informatici
modalità di attacco: diffusione tramite email, siti infetti, dispositivi usb o vulnerabilità di rete
danni: furto di informazioni riservate, distruzione di dati.
RANSOMWARE:
descrizione: tipo di malware che cifra i dati aziendali
modalità di attacco: email di phishing o vulnerabilità di sistemi non aggiornati
danni: costi elevati di riscatto per decriptare i dati, perdita definitiva di quei dati, interruzione dell'operatività dell'azienda
ATTACCHI DDOS:
descrizione: attacco che mira a saturare le risorse di una rete o di un server rendendolo inaccessibile
modalità di attacco: utilizzo di una rete di computer (botnet) infetti controllati dall'attaccante che generano traffico anomalo verso il bersaglio
danni: interruzione dei servizi on line, danno reputazionale, perdita di produttività quindi danno economici.

ATTACCHI DI INGEGNERIA SOCIALE:
descrizione: manipolazione psicologica dell'utente per ottenere informazioni esempi sono: persone che si fingono addetti della banca falsi tecnici telefonate di supporto false.
danni: accessi non autorizzati, furti di credenziali.

VULNERABILITÀ SOFTWARE PER MANCATI AGGIORNAMENTI:
descrizione: bug o falle di sicurezza nei sistemi operativi o nelle applicazioni che possono essere sfruttati per un attacco.
danni: accessi da remoto non autorizzati, esecuzioni di codici malevoli o diffusione di malware.

Il rapporto clusit aggiornato a ottobre del 2025 analizza l'evoluzione delle minacce informatiche che riguardano i dati fino al primo semestre del 2025, nel rapporto si evince che:
aumento di attacchi gravi +10% rispetto al 2024
maggiore complessità degli attacchi
target principali aziende e pubbliche amministrazioni che sono carenti nelle misure di difesa e anche nella formazione del personale.
Il rapporto evidenzia come motivazione principale di tali attacchi quello economico circa il 78% degli attacchi.
Le tecniche più utilizzate sono:
phishing e social engineering
ransomware una delle minacce ancora più dannosa
supply chain attack che sfruttano vulnerabilità nei sistemi anche nei fornitori o nei partner delle aziende
furti di dati e di identità digitali.

RANSOMWARE
Dal rapporto si evince come la minaccia più pericolosa sia ancora quella dei ransomware e dell'estorsione perché i cyber criminali non si limitano più a cifrare i dati ma minacciano anche di pubblicarli on line, colpendo anche a volte anche i dati dei clienti o dei partner dell'azienda.
Impatti: blocco totale della produzione o erogazione dei servizi, costi elevati per il ripristino, danni per la reputazione, rischio di violazione della GDPR per la diffusione dei dati personali.

Impatto dell'intelligenza artificiale
Il rapporto ha anche evidenziato come il ruolo dell'intelligenza artificiale impatta i cyber attacchi poiché viene sfruttata per automatizzare o perfezionare gli attacchi con la creazione di:
email di phishing più realistiche e personalizzate
generazione di codice malevolo
deep fake audio o video
analisi dei dati rubati per estrarre quante più informazioni utili.
A parti inverse l'intelligenza artificiale può essere utilizzata nella difesa per analizzare il comportamento delle minacce, rilevamento automatico delle anomalie e automazione delle risposte agli incidenti.

CONCLUSIONE

senza dilungarmi troppo il rapporto ha quindi evidenziato come la sicurezza informatica sta acquistando importanza e che le aziende italiane sono invitate ad investire sulla sicurezza informatica, implementare strategie di resilienza .

come viene citato nel rapporto la differenza tra le aziende che resistono e quelle che soccombono non sta nella fortuna ma nella preparazione.