ESERCIZIO W19D1 PRATICA 1

1. **Phishing**: Questa minaccia coinvolge l'invio di comunicazioni fraudolente (come e-mail, messaggi di testo o telefonate) che fingono di provenire da fonti legittime per ottenere informazioni sensibili come password, dati finanziari o informazioni personali.
2. **Malware**: Questo termine generico indica un software dannoso progettato per infiltrarsi o danneggiare un sistema informatico. Alcuni esempi specifici includono:
    - **Ransomware**: Come il ransomware Medusa, che cripta i file sul computer della vittima e richiede un riscatto per ripristinare l'accesso ai file.
    - **Spyware**: Software che raccoglie informazioni sulle attività degli utenti senza il loro consenso.
    - **Trojan**: Un programma dannoso che si nasconde all'interno di software legittimo e può consentire agli attaccanti di accedere al sistema compromesso.
3. **Attacchi DDoS (Denial of Service)**: Questi attacchi mirano a sovraccaricare un servizio online con traffico in entrata, rendendolo inaccessibile agli utenti legittimi.
4. **Vulnerabilità 0-day**: Queste sono vulnerabilità di sicurezza sconosciute o non patchate che possono essere sfruttate dagli hacker prima che il produttore rilasci una correzione.
5. **Exploit come Oday Click iPhone e Spectre v2**: Questi si riferiscono a specifici exploit informatici che sfruttano vulnerabilità nei sistemi operativi o hardware, consentendo agli attaccanti di ottenere accesso non autorizzato o di compromettere i dati.
6. **Attacchi basati su password deboli o rubate**: L'uso di password deboli o compromesse può consentire agli attaccanti di accedere ai sistemi o alle informazioni sensibili.
7. **Attacchi basati sul social engineering**: Questi approcci mirano a manipolare gli individui per ottenere informazioni riservate o accesso non autorizzato, spesso tramite ingegneria sociale su e-mail, telefono o piattaforme social.
8. **Insider Threats**: Questa minaccia coinvolge dipendenti o altre persone interne all'organizzazione che sfruttano la loro posizione privilegiata per scopi dannosi.
9. **Attacchi di ingegneria inversa**: Questi coinvolgono lo studio e l'analisi di prodotti software o hardware per identificare e sfruttare vulnerabilità.

È importante che le aziende comprendano queste minacce e adottino misure di sicurezza appropriate per proteggere i loro sistemi e dati. La sensibilizzazione, la formazione degli utenti e l'implementazione di soluzioni di sicurezza informatica robuste sono essenziali per mitigare questi rischi.

TRACCIA 2

Il sistema di valutazione di ThreatConnect si basa su tre livelli principali che sono fondamentali per valutare le minacce informatiche. Ecco una lista che spiega ciascun livello:

1. **Livello di Triage (o livello di base)**:
    - **Caratteristiche**:
        - Questo è il livello iniziale di valutazione delle minacce.
        - Si concentra sulla raccolta e l'analisi delle informazioni di base relative alle minacce.
        - Include dati di intelligence di base, come indicatori di compromissione e informazioni di base sulle fonti delle minacce.
        - Obiettivo principale: determinare rapidamente se una minaccia potenziale richiede un'ulteriore indagine o azione.
2. **Livello di Valutazione (o livello intermedio)**:
    - **Caratteristiche**:
        - Questo livello amplia l'analisi delle minacce rispetto al livello di triage.
        - Coinvolge una valutazione più approfondita dei dati e delle informazioni relative alle minacce.
        - Include analisi più dettagliate dei modelli di attacco, delle tattiche e delle procedure utilizzate dai cybercriminali.
        - Integrato con dati di intelligence più sofisticati, come indicatori comportamentali (IOBs) e indicatori di attacco (IOAs).
        - Obiettivo principale: comprendere meglio la natura e l'origine delle minacce per supportare le decisioni tattiche e strategiche di sicurezza informatica.
3. **Livello di Intelligence (o livello avanzato)**:
    - **Caratteristiche**:
        - È il livello più avanzato del sistema di valutazione di ThreatConnect.
        - Coinvolge un'analisi approfondita delle minacce con un focus sulla proattività e sulla previsione delle tendenze delle minacce.

- Include dati di intelligence sofisticati e contestualizzati, come intelligence sulle minacce mirate (ad esempio, attacchi specifici a determinati settori o organizzazioni), analisi comportamentale avanzata e valutazione delle capacità e delle intenzioni degli attori delle minacce.
- Obiettivo principale: fornire informazioni strategiche e tattiche di alto livello per consentire agli analisti e ai team di sicurezza di prendere decisioni informate e preventive per mitigare le minacce.

Questi tre livelli insieme forniscono una struttura completa per valutare e gestire le minacce informatiche in modo efficace, consentendo agli esperti di sicurezza di ottenere una visione dettagliata delle minacce attuali e future e di adottare misure adeguate di protezione e risposta.