Threat Connect utilizza un sistema di valutazione a doppio livello per misurare la gravità delle minacce (Threat Rating) e la fiducia nell'accuratezza di tale valutazione (Confidence Rating).

- 1. Threat Rating (0 a 5 teschi)

Questa valutazione rappresenta il livello di pericolosità di un determinato indicatore (ad esempio, una firma malware o un indirizzo IP):

➔ 0 teschi (Sconosciuto): non ci sono abbastanza informazioni per valutare il livello di minaccia;
➔ 1 teschio (Sospetto): non è stata confermata attività malevola, ma ci sono segni sospetti;
➔ 2 teschi (Bassa minaccia): l'indicatore è associato a un avversario poco sofisticato, probabilmente opportunistico;
➔ 3 teschi (Minaccia moderata): l'indicatore rappresenta un avversario capace, impegnato in attività dirette ma non necessariamente persistenti (es. sfruttamento attivo);
➔ 4 teschi (Alta minaccia): l'indicatore è collegato a una minaccia avanzata e persistente che ha probabilmente già compromesso il bersaglio;
➔ 5 teschi (Minaccia critica): l'indicatore rappresenta un avversario altamente sofisticato e ben finanziato, tipicamente osservato in fasi critiche di un attacco (es. esfiltrazione di dati).

- 2. Confidence Rating (0 a 100)

Questa valutazione misura il livello di fiducia dell'analista o del sistema sull'accuratezza della valutazione della minaccia:

➔ 90-100 (Confermato): analisi indipendenti o più fonti confermano l'accuratezza dell'indicatore;

- ➔ 70-89 (Probabile): logico e coerente con le informazioni disponibili, ma manca una conferma diretta;
- ➔ 50-69 (Possibile): in parte logico, con informazioni parzialmente a supporto;
- ➔ 30-49 (Dubbioso): plausibile, ma privo di solide evidenze;
- ➔ 2-29 (Improbabile): le prove dirette contraddicono la valutazione iniziale, rendendo l'indicatore improbabile;
- ➔ 1 (Screditato): dimostrato essere incorretto;
- ➔ 0 (Non valutato): nessuna valutazione di fiducia è stata assegnata.

FACOLTATIVO

Analisi dettagliata delle minacce

1. Phishing

- ➔ **Descrizione**: il phishing è una delle forme più comuni di attacchi di ingegneria sociale. Gli attaccanti fingono di essere entità affidabili (banche, colleghi di lavoro o aziende famose) per convincere le vittime a divulgare informazioni sensibili come password, numeri di carte di credito o credenziali aziendali;
- ➔ **Come funziona**: l'attaccante invia email, messaggi o persino telefonate che appaiono legittime, ma contengono link malevoli o allegati infetti. Quando la vittima interagisce con il contenuto, fornisce involontariamente accesso a informazioni critiche o permette l'installazione di malware nel sistema;
- ➔ **Tecniche più comuni**:
  - ◆ **Spear phishing**: attacchi mirati contro individui specifici all'interno di un'organizzazione, come dirigenti o amministratori IT;

- ◆ **Whaling**: un sottoinsieme del spear phishing, specificamente rivolto a persone di alto profilo come i CEO;

➔ **Danni potenziali**: furto di credenziali, accesso non autorizzato a sistemi aziendali, furto di dati sensibili, potenziale compromissione dell'intera rete aziendale.

2. Malware

➔ **Descrizione**: il malware è un software dannoso progettato per infiltrarsi in sistemi informatici per vari scopi malevoli, come il furto di dati, il controllo del sistema o la distruzione di file;

➔ **Tipologie di malware**:

- ◆ **Virus**: codice dannoso che si replica nei file legittimi e si diffonde in tutto il sistema;
- ◆ **Trojan**: si presenta come software legittimo, ma una volta installato, concede all'attaccante accesso remoto al sistema;
- ◆ **Spyware**: raccoglie informazioni personali senza il consenso dell'utente;
- ◆ **Worms**: si diffonde autonomamente attraverso le reti, sfruttando vulnerabilità senza bisogno di interazione dell'utente;
- ◆ **Keylogger**: raccoglie le battute digitate dall'utente per rubare informazioni sensibili come password e numeri di carte di credito;

➔ **Meccanismi di distribuzione**: il malware può essere distribuito tramite allegati di email, siti web compromessi, chiavette USB infette o download di software illegale;

➔ **Danni potenziali**: blocco dei sistemi aziendali, furto di dati, compromissione della privacy, perdita di controllo sui dispositivi e, in alcuni casi, richieste di riscatto (come nel caso del ransomware).

3. Attacchi DDoS (Distributed Denial of Service)

- ➔ **Descrizione**: un attacco DDoS cerca di rendere un servizio o una rete inaccessibile inondando di richieste di accesso false. Questo sovraccarica il server o la rete, impedendo agli utenti legittimi di accedervi;
- ➔ **Come funziona**: gli attaccanti utilizzano una rete di dispositivi infetti (spesso chiamati **botnet**) per generare traffico massiccio verso il server target. I dispositivi della botnet possono includere computer, smartphone o persino dispositivi IoT (come telecamere di sicurezza e router);
- ➔ **Obiettivi tipici**: spesso vengono attaccati i siti web di e-commerce, istituti bancari, piattaforme di gaming o anche infrastrutture governative;
- ➔ **Danni potenziali**: interruzione dei servizi, perdita di vendite (soprattutto per i siti di e-commerce), danni alla reputazione e costi elevati per la mitigazione.

4. Furto di dati

- ➔ **Descrizione**: il furto di dati si verifica quando un attaccante riesce ad accedere illegalmente a dati sensibili o personali, come informazioni finanziarie, segreti industriali, o dati sanitari;
- ➔ **Meccanismi di attacco**:
  - ◆ **Sfruttamento di vulnerabilità**: gli attaccanti sfruttano falle nei software o nei sistemi di sicurezza;
  - ◆ **Credential stuffing**: usano credenziali rubate per accedere a più sistemi;
  - ◆ **Attacchi interni**: dipendenti insoddisfatti o ex dipendenti possono rubare dati per vendetta o guadagno;
- ➔ **Danni potenziali**: violazioni della privacy, perdita di proprietà intellettuale, multe e sanzioni legali, danni alla reputazione e perdite finanziarie.

5. Ransomware

- ➔ **Descrizione**: il ransomware è una forma di malware che cripta i dati dell'utente o dell'azienda, bloccando l'accesso ai sistemi fino a quando non viene pagato un riscatto, di solito in criptovaluta;
- ➔ **Come funziona**: di solito diffuso tramite email phishing o download infetti. Una volta che il ransomware è installato, cripta i file critici e visualizza una richiesta di riscatto per sbloccarli;
- ➔ **Esempi celebri**: il ransomware **WannaCry** ha colpito numerose organizzazioni in tutto il mondo nel 2017, compresi ospedali, bloccando l'accesso a dati critici fino al pagamento del riscatto;
- ➔ **Danni potenziali**: perdita permanente dei dati, interruzione dei servizi essenziali, costi finanziari per la decrittazione e potenziale perdita di fiducia da parte dei clienti e partner.

6. Attacchi interni (insider threats)

- ➔ **Descrizione**: le minacce interne sono attacchi che provengono da persone che hanno già accesso privilegiato all'interno dell'azienda, come dipendenti, contractor o partner;
- ➔ **Tipi di insider threats**:
  - ◆ **Malicious insiders**: dipendenti che agiscono con l'intenzione di danneggiare l'azienda;
  - ◆ **Negligent insiders**: dipendenti che, involontariamente, compromettono la sicurezza attraverso pratiche negligenti;
- ➔ **Esempio:** copia di dati sensibili su supporti esterni, invio di email contenenti informazioni confidenziali a indirizzi non autorizzati, installazione di software non autorizzato;
- ➔ **Danni potenziali**: furto di proprietà intellettuale, compromissione di dati sensibili, perdite finanziarie, cause legali e danni alla reputazione aziendale.

7. Attacchi di forza bruta

- ➔ **Descrizione**: gli attacchi di forza bruta sono una tecnica in cui un attaccante tenta ripetutamente di accedere a un sistema indovinando password o credenziali attraverso tentativi sistematici;
- ➔ **Tecniche comuni**: gli attaccanti utilizzano software automatizzati per provare ogni possibile combinazione di password fino a trovare quella corretta;
- ➔ **Danni potenziali**: accesso non autorizzato ai sistemi aziendali, furto di credenziali, compromissione della sicurezza aziendale, con conseguenti furti di dati o installazione di malware.