

ESERCIZIO – ThreatConnect

1. Livelli del sistema di valutazione ThreatConnect

Il sistema di valutazione degli indicatori di ThreatConnect si basa su due dimensioni principali:

- **Threat Rating:** indica il livello di pericolosità dell'indicatore.
- **Confidence Rating:** indica quanto si è sicuri della valutazione assegnata.

Queste due metriche permettono di capire sia la gravità di una minaccia sia l'affidabilità delle informazioni disponibili.

2. Descrizione dei livelli di valutazione

Threat Rating (0–5)

- **0 – Unknown:** non ci sono abbastanza informazioni per valutare la minaccia.
- **1 – Suspicious:** attività sospetta ma non confermata come malevola.
- **2 – Low:** minaccia a basso impatto o poco sofisticata.
- **3 – Moderate:** minaccia concreta con attacco attivo o mirato.
- **4 – High:** minaccia avanzata e persistente, spesso già dentro il sistema.
- **5 – Critical:** minaccia critica con alto impatto e attaccante molto sofisticato.

Confidence Rating (0–100)

- **0:** non valutato.
 - **1:** informazione falsa o non attendibile.
 - **2–29:** improbabile, poche prove.
 - **30–49:** dubbio, possibile ma non confermato.
 - **50–69:** plausibile, alcune prove presenti.
 - **70–89:** probabile, informazioni coerenti.
 - **90–100:** confermato con alta certezza.
-

3. Minacce informatiche comuni (analisi sintetica)

Phishing

Tecnica di ingegneria sociale che utilizza email o siti falsi per rubare credenziali.

Impatto: furto account e accessi non autorizzati.

Malware

Software malevolo installato su un sistema (trojan, worm, spyware).

Impatto: controllo remoto, furto dati, danni al sistema.

Ransomware

Blocca o cifra i dati chiedendo un riscatto.

Impatto: perdita accesso ai dati e blocco operatività.

DDoS

Attacco che sovraccarica un servizio rendendolo irraggiungibile.

Impatto: indisponibilità dei servizi online.

Furto di dati (Data Breach)

Accesso non autorizzato a informazioni sensibili.

Impatto: perdita di privacy e possibili sanzioni.

Vulnerabilità software

Sfruttamento di bug o configurazioni errate.

Impatto: accesso non autorizzato o esecuzione codice.

Minacce interne (Insider)

Utenti interni che causano danni volontariamente o per errore.

Impatto: perdita dati o sabotaggio.

ESERCIZIO EXTRA – OWASP, MITRE ATT&CK e mitigazioni

Scenario 1 – XSS e furto cookie

Un attaccante inserisce uno script in una pagina web che ruba i cookie di sessione degli utenti.

- **OWASP Top 10:** A03:2021 Injection (Cross Site Scripting)
- **MITRE ATT&CK:** T1189 – Drive-by Compromise
- **Mitigazione:** isolamento applicazioni e browser sandboxing, controllo contenuti web e filtri di sicurezza.

Scenario 2 – SQL Injection

Un attaccante sfrutta il campo login per eseguire query SQL e accedere al database.

- **OWASP Top 10:** A03:2021 Injection (SQL Injection)
- **MITRE ATT&CK:** T1190 – Exploit Public-Facing Application

- **Mitigazione:** utilizzo di Web Application Firewall, validazione input e protezioni contro exploit.
-

Scenario 3 – Deserializzazione non sicura

Un server deserializza dati non controllati permettendo esecuzione di codice remoto.

- **OWASP Top 10:** A08:2021 Software and Data Integrity Failures
 - **MITRE ATT&CK:** T1190 – Exploit Public-Facing Application
 - **Mitigazione:** controlli sui dati in ingresso, WAF e protezioni contro exploit applicativi.
-

Conclusione

L'analisi degli indicatori di minaccia e l'utilizzo di framework come OWASP e MITRE ATT&CK permettono di classificare meglio gli attacchi informatici e adottare contromisure efficaci. Comprendere il livello di rischio e la probabilità di una minaccia è fondamentale per migliorare la sicurezza dei sistemi e prevenire incidenti.