Cyber Security Report

W19D1

15/11/2025

Autore :
Pace Massimiliano
email : *efmpas@gmail.com*

Indice :

INTRODUZIONE LIVELLO DI VALUTAZIONE THREATCONNECT

Livelli del sistema di valutazione di ThreatConnect:
ThreatConnect utilizza due scale di valutazione per gli indicatori:
•Threat Rating (Valutazione della minaccia): Indica quanto l'indicatore rappresenta una minaccia.
•Confidence Rating (Livello di confidenza): Esprime quanto è affidabile l'assegnazione della valutazione della minaccia.

Livello	Nome	Caratteristiche principali
0	Unknown	Informazioni insufficienti per valutare la minaccia
1	Suspicious	Attività sospetta, nessuna conferma di attività malevola
2	Low	Minaccia poco sofisticata, opportunistica e di breve durata; potenziale pre-attacco
3	Moderate	Avversario con capacità basilari, azione moderatamente mirata; fase di intrusione attiva (delivery, exploit, installazione)
4	High	Minaccia avanzata, attività mirata e persistente; post-compromissione (C2, obiettivi)
5	Critical	Avversario altamente qualificato e con risorse illimitate; fase critica in qualunque momento dell'intrusione

Threat Rating
(Skulls scale: 0-5)

Valore	Nome	Caratteristiche principali
0	Unknown	Nessuna valutazione, manca conferma
1	Discredited	Provato che sia inaccurato
2–29	Improbable	Non confermato; poco plausibile, contraddetto da altre informazioni
30–49	Doubtful	Non confermato; possibile, ma poco logico; mancano altre informazioni
50–69	Possible	Non confermato; ragionevolmente logico; alcune consistenze con altre informazioni
70–89	Probable	Non confermato direttamente; logico e plausibile; consistente con altre informazioni
90–100	Confirmed	Confermato tramite fonti indipendenti o analisi diretta; coerente con altre informazioni sul soggetto

Confidence Rating (Scala percentuale 0-100)

Queste scale sono utilizzate insieme per assegnare un contesto e una priorità agli indicatori raccolti su ThreatConnect.

Facoltativo
Elenco minacce comuni

Esempi di minacce che possono colpire un'azienda includono:

•Phishing: Email o messaggi apparentemente legittimi che cercano di indurre gli utenti a rivelare credenziali o dati sensibili.
•Malware: Software dannoso che compromette la sicurezza di sistemi e dati aziendali. Può includere virus, ransomware, trojan.
•Attacchi DDoS: Sovraccarico di servizi online tramite traffico distribuito per renderli inaccessibili agli utenti.
•Furto di dati: Esfiltrazione non autorizzata di informazioni aziendali o personali tramite exploit tecnici o social engineering.

Metodo di analisi

•Raccogli informazioni da fonti aperte come siti di sicurezza e report di settore.
•Analizza ogni minaccia valutando come compromette la sicurezza e quali danni causa.
•Inserisci le informazioni più importanti nell'elenco finale per ciascuna tipologia.

Esercizio EXTRA

Analizzo scenari uno per uno come richiesto, indicando l'OWASP Top 10, la tecnica MITRE ATT&CK principale e la mitigazione suggerita.

Scenario 1: Attacco XSS in un form online

OWASP Top 10:
A7:2017 Cross-Site Scripting (XSS), ora incluso nella voce Injection nelle versioni più recenti della Top 10.

MITRE ATT&CK:
Tecnica principale: T1059.007 - Command and Scripting Interpreter: JavaScript. Lo scenario si connette anche a T1189: Drive-By Compromise, dove uno script viene eseguito nel browser della vittima visitando una pagina malevola o vulnerabile.

Mitigazione MITRE ATT&CK:
Sanitizzazione e validazione rigorosa degli input utente.
Uso di output encoding per tutti i dati utente che vengono visualizzati come HTML.
Implementazione di Content Security Policy (CSP) e settaggio dell'attributo HttpOnly sui cookie sensibili.

Scenario 2: Attacco SQL Injection sull'interfaccia di login

OWASP Top 10:

A1:2017 Injection (SQL Injection è il riferimento più classico di questa categoria, ancora rilevante nella Top 10).

MITRE ATT&CK:
Tecnica principale: T1505.002 - Server Software Component: SQL Stored Procedures, oppure genericamente T1190 - Exploit Public-Facing Application (l'attaccante sfrutta una vulnerabilità di una web app pubblica).

Mitigazione MITRE ATT&CK:
- Utilizzo di query parametrizzate/preparate.
- Validazione e sanitizzazione dell'input utente.
- Limitare i privilegi degli account DB collegati all'applicazione.
- Implementare logging e alerting in caso di anomalie sull'input.

Scenario 3: Esecuzione remota codice via deserializzazione insicura

OWASP Top 10:

A8:2017 Insecure Deserialization (presente nelle Top 10, ancora oggi una delle vulnerabilità più gravi nelle applicazioni enterprise).

MITRE ATT&CK:

Tecnica principale: T1059 - Command and Scripting Interpreter (esecuzione di comandi su server) e/o T1210 - Exploitation of Remote Services (vettore: oggetto malizioso deserializzato dalla funzione vulnerabile).

Mitigazione MITRE ATT&CK:

•Non accettare mai oggetti serializzati da fonti non affidabili.
•Implementare controlli rigorosi sull'integrità e il tipo degli oggetti deserializzati.
•Aggiornare e patchare costantemente le librerie che gestiscono la serializzazione/deserializzazione.

Tabella comparativa riassuntiva

Scenario	OWASP Top 10	MITRE ATT&CK	Mitigazione suggerita
1. XSS	A7:2017 Injection/XSS	T1059.007 / T1189	Validazione input, encoding output, CSP, HttpOnly
2. SQLi	A1:2017 Injection	T1505.002 / T1190	Query parametrizzate, validazione input, least privilege
3. Deserializ.	A8:2017 Deserialization	T1059 / T1210	Evita oggetti insicuri, controlli integrità, patching