# W19D1 – Pratica

## Epic Education Srl

### ThreatConnect
### Analisi e catalogazione delle principali minacce cyber per le aziende
### OWASP Top 10 - MITRE ATT&CK

**Simone Giordano**

15/11/2025


**Contatti:**

Tel: 3280063044
Email: mynameisimone@gmail.com
Linkedin: https://www.linkedin.com/in/simone-giordano-91290652/

# Sommario

# **ThreatConnect -** Esercizio1

## 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-confidenc e-ratings
Compila una lista spiegando, per ogni livello, le caratteristiche.

## Esercizio

Il li velli su cui è basato ThreatConnect sono 6.

| Livello | Etichetta | Caratteristiche |
|---|---|---|
| **0 – Unknown** | 0 teschi | Non ci sono abbastanza informazioni per valutare la minaccia. Esempio: “sto ancora analizzando l’header di un’email, non so ancora nulla sul server SMTP”. |
| **1 – Suspicious** | 1 teschio | Non è confermata attività malevola; solo attività dubbia o osservazioni sospette da una minaccia non identificata. Esempio: “non capisco perché i laptop degli utenti visitino quell’URL, ma per ora non appare nulla palesemente malevolo”. |
| **2 – Low Threat** | 2 teschi | Rappresenta un avversario poco sofisticato, opportunistico e temporaneo. Esempio: “vediamo scansioni su quella porta da indirizzi IP in quel blocco tutto il giorno”. |
| **3 – Moderate Threat** | 3 teschi | Avversario con capacità e risorse di base, attività diretta ma non necessariamente persistente; l’indicatore corrisponde ad esempio alla fase di delivery/exploitation. Esempio: “quel file hash rappresenta un documento che finge di essere un promemoria aziendale diretto al dipartimento HR”. |
| **4 – High Threat** | 4 teschi | L'indicatore può essere attribuito a un avversario avanzato e indica che si è già verificata un'attività mirata e persistente. |
| **5 – Critical Threat** | 5 teschi | l'indicatore rappresenta un avversario altamente qualificato e dotato di risorse. Questo livello di minaccia dovrebbe essere riservato agli indicatori di avversari con capacità illimitate e che risultano critici in qualsiasi fase dell'intrusione. |

# **Analisi e catalogazione delle principali minacce cyber per le aziende**

## Esercizio facoltativo

## Traccia

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/

## Esercizio

**1. Malware (software malevolo)**

**Descrizione / modalità di attacco**
Il termine "malware" (malicious software) comprende virus, worm, trojan horse, spyware, keylogger, botnet. Il malware può essere installato su dispositivi aziendali tramite: email con allegati malevoli, link compromessi, exploit di vulnerabilità, download da siti non sicuri.
Una volta attivo può: installare back-door, rubare credenziali, esfiltrare dati, partecipare a botnet, crittografare file (ransomware).

**Danni possibili per l'azienda**

- perdita o furto di dati sensibili (clienti, proprietà intellettuale, finanze)
- interruzione di servizi, degrado delle performance o controllo remoto dei dispositivi
- compromissione della reputazione aziendale
- costi di recupero elevati (ripristino, investigazione, eventuali sanzioni/regolamentazioni)
- nel caso ransomware: pagamento del riscatto, perdita di produttività, rischio che backup/recupero risultino inefficienti

**Rilevanza/contesto italiano**
Il rapporto Clusit segnala che il malware rimane una minaccia prevalente. In Italia, settori critici come manifatturiero, trasporti, sanità hanno visto incrementi importanti degli incidenti gravi.
Conclusione: un'azienda deve considerare il malware come rischio "base" ma sempre attuale.

---

**2. Phishing e ingegneria sociale**

**Descrizione / modalità di attacco**
Il phishing consiste nell'inviare email, messaggi o usare canali digitali per indurre un utente a compiere un'azione: cliccare su un link malevolo, aprire un allegato, inserire credenziali su un sito contraffatto. Spesso è combinato con tecniche di ingegneria sociale (es. sfruttamento di fiducia, urgenza, autorità).

**Danni possibili per l'azienda**

- compromissione di credenziali (utente, amministratore) che può permettere accesso non autorizzato ai sistemi
- esfiltrazione di dati, frodi finanziarie (es. cambi di coordinate bancarie)
- propagazione di malware
- perdita di fiducia da parte dei clienti/partner, sanzioni per data breach
- aumento della superficie di attacco interno (l'errore umano diventa punto di ingresso)

**Rilevanza/contesto italiano**
Il rapporto Clusit segnala che in Italia l'ingegneria sociale e il phishing sono in forte crescita: ad esempio, gli

attacchi di phishing e di ingegneria sociale registrano un +87% in Italia. Il “fattore umano” continua a rappresentare un punto debole.
Conclusione: la formazione sulla consapevolezza del rischio e controlli tecnici adeguati sono fondamentali.

---

**3. Attacchi DDoS / Denial-of-Service (inclusi DoS)**

**Descrizione / modalità di attacco**
Un attacco di tipo DoS (Denial of Service) o distribuito DDoS (Distributed Denial of Service) mira a saturare le risorse (reti, server, link) di un’organizzazione, rendendo i servizi non disponibili o gravemente compromessi. Questo può avvenire tramite botnet che generano traffico massivo, richieste simultanee o sfruttamento di vulnerabilità di protocolli/servizi.
Spesso è usato anche come diversione o come parte di un attacco combinato, mentre l’attaccante esegue un’altra intrusione.

**Danni possibili per l’azienda**

- interruzione di servizio verso clienti / utenti / partner → perdita di fatturato, danno reputazionale
- costi per mitigazione (soluzioni anti-DDoS, aumento banda, ripristino infrastruttura)
- se parte di attacco più ampio: può servire a distrarre o facilitare furto di dati o altri attacchi
- potenziale responsabilità regolamentare se i servizi erogati rientrano in ambiti critici (ad es. infrastrutture, sanità)

**Rilevanza/contesto italiano**
Secondo Clusit, in Italia nel 2023 gli attacchi DDoS hanno registrato un incremento significativo e hanno superato il malware come tecnica predominante. Questo indica che anche nelle imprese italiane la resilienza alla disponibilità (availability) è oggi molto critica.
Conclusione: le aziende, anche quelle non “pubbliche”, devono considerare misure contro DDoS come parte della strategia di continuità operativa.

---

**4. Ransomware**

**Descrizione / modalità di attacco**
Il ransomware è un tipo di malware che, una volta installato, cifra o blocca l’accesso ai dati o ai sistemi dell’organizzazione, richiedendo un riscatto (in criptovaluta o altro) per la decrittazione o rilascio. Spesso combinato con esfiltrazione preliminare di dati dove l’attaccante minaccia di pubblicarli se il riscatto non viene pagato.
Modalità frequenti: phishing/email, exploit di vulnerabilità, credenziali rubate.

**Danni possibili per l’azienda**

- perdita permanente di dati o accesso ai sistemi
- pagamento del riscatto (senza garanzia di recupero)
- interruzione dell’attività operativa
- danno reputazionale e perdita di fiducia

- possibili sanzioni normative (es. GDPR) se ci sono esfiltrazioni di dati personali
- costi di ripristino enormi (backup, forense, consulenza, comunicazioni)

**Rilevanza/contesto italiano**
Il Rapporto Clusit segnala che il ransomware rimane una minaccia significativa e che la redditività per gli aggressori lo mantiene molto attivo. Le aziende italiane devono attribuire a questa minaccia un alto livello di rischio.

---

**5. Furto di dati / Esfiltrazione di informazioni sensibili**

**Descrizione / modalità di attacco**
L'attacco punta non tanto alla distruzione o all'interruzione, ma all'accesso, copia e sottrazione di dati sensibili: cliente, finanziari, proprietà intellettuale, segreti industriali, oppure dati personali che possono generare un data breach. Può avvenire tramite malware, phishing, insider threat, vulnerabilità. Spesso è parte di un attacco più ampio (es. prima installazione di malware → movimenti laterali → esfiltrazione).

**Danni possibili per l'azienda**

- violazione della privacy e obblighi normativi (GDPR, DORA, NIS2)
- sanzioni amministrative e cause legali
- perdita di vantaggio competitivo (es. proprietà intellettuale condivisa con concorrenti)
- danno reputazionale per perdita fiduciaria da parte di clienti/partner
- possibili ricatti (dati pubblicati) o estorsioni
- costi di risposta all'incidente: indagine, notifica, mitigazione, assicurazione cyber

**Rilevanza/contesto italiano**
Clusit segnala che circa il 17% degli attacchi gravi in Italia usa tecniche finora sconosciute, il che complica l'identificazione preventiva degli scenari di furto di dati. In un contesto dove le imprese italiane stanno aumentando la digitalizzazione, il rischio di esfiltrazione cresce.

---

**6. Attacchi alla Supply Chain / Fornitore terze parti**

**Descrizione / modalità di attacco**
Gli attaccanti prendono di mira i fornitori, partner, software o hardware di terze parti che hanno accesso ai sistemi aziendali. Una volta compromessa la "catena" (supply chain), possono risalire fino all'azienda target. Questo include attacchi a componenti software, librerie, servizi cloud, provider di sicurezza, hardware, ecc. Spesso più difficili da individuare perché l'ingresso non avviene direttamente dall'azienda target ma tramite un fornitore.

**Danni possibili per l'azienda**

- compromissione di sistemi critici via "backdoor" fornita dal fornitore
- perdita di controllo su ambienti e infrastrutture esterne
- interruzione dei servizi erogati tramite fornitore compromesso

- responsabilità condivisa o diretta se l'attack vector è il fornitore
- danni reputazionali e costo elevato per mitigare vulnerabilità in cascata

**Rilevanza/contesto italiano**
Nel panorama europeo la ENISA (Agenzia dell'Unione Europea per la sicurezza delle reti e dell'informazione) identifica "supply chain attacks" come una delle principali minacce. Per le aziende italiane, data la forte interdipendenza con partner europei/esterni, è un vettore di rischio crescente.

---

**7. Insider Threat (minaccia interna)**

**Descrizione / modalità di attacco**
La minaccia "insider" può venire da dipendenti, collaboratori, ex collaboratori o partner che hanno accesso ai sistemi o dati aziendali. Può essere volontaria (es. furto di dati) oppure involontaria (es. errore umano, phishing che coinvolge un utente interno). È più difficile da rilevare perché sfrutta credenziali legittime e accessi autorizzati.

**Danni possibili per l'azienda**

- esfiltrazione o distruzione di dati dall'interno
- privilege escalation per ottenere accesso a sistemi sensibili
- problemi di fiducia interna e reputazione aziendale
- difficoltà nella rilevazione e risposta (audit, monitoraggio)
- possibili implicazioni legali e normative se coinvolgono dati sensibili

**Rilevanza/contesto italiano**
Anche se i report italiani si focalizzano più su attacchi esterni, l'interazione tra attacchi esterni che sfruttano insider (ad es. phishing verso utenti interni) rende questa categoria rilevante. Il fattore umano è identificato come punto debole.

---

**8. Attacchi a Identità / Credential Theft & Access Abuse**

**Descrizione / modalità di attacco**
Gli attaccanti rubano credenziali (nome utente/password, token, sessioni) o utilizzano tecniche come credential-stuffing, password spraying, attacchi al protocollo di autenticazione (es. Kerberos), takeover di account. Con le credenziali possono accedere a sistemi, effettuare movimenti laterali, esfiltrare dati o installare malware.
Spesso combinati con phishing o botnet di stealer.

**Danni possibili per l'azienda**

- accesso non autorizzato ai sistemi aziendali
- uso delle credenziali rubate per attacchi interni (movimenti laterali)
- esfiltrazione, frode, sabotaggio
- aumento della superficie di attacco e difficoltà di tracciamento

- potenziale compromissione della fiducia verso l'azienda se i clienti risultano coinvolti

**Rilevanza/contesto italiano**
L'importanza di questo vettore è in crescita, come indicato da fonti internazionali e italiane: il furto di credenziali fornisce spesso la "porta d'ingresso" per gli attaccanti. I report generali (ad es. IBM) indicano che gli attacchi basati su credenziali sono fra i più frequenti oggi.

---

**9. Attacchi "Zero-day", vulnerabilità e exploit di software/hardware**

**Descrizione / modalità di attacco**
Gli attaccanti sfruttano vulnerabilità software o hardware non ancora note (zero-day) oppure note ma non ancora patchate nell'organizzazione target. Le vulnerabilità possono essere in sistemi operativi, applicazioni web, firmware, IoT, servizi cloud. Una volta sfruttata la vulnerabilità, l'attaccante può ottenere esecuzione di codice, elevazione di privilegi, accesso remoto, movimenti laterali.

**Danni possibili per l'azienda**

- compromissione dell'infrastruttura in modo rapido e spesso indiretto
- attacco "silente" che può rimanere nascosto fino a quando l'accesso è consolidato
- esposizione di sistemi critici e perdita di fiducia
- costi elevati se l'attacco si traduce in compromissione completa dell'ambiente operativo

**Rilevanza/contesto italiano**
Il Rapporto Clusit segnala che in Italia circa il 17% degli attacchi gravi nel 2023/24 ha usato tecniche "sconosciute" o zero-day. Per le aziende questo significa che mantenere aggiornata la gestione delle patch e l'asset inventory è essenziale.

---

**10. Manipolazione delle informazioni / disinformazione / interferenza (specialmente nei contesti critici)**

**Descrizione / modalità di attacco**
Quest'area riguarda attacchi alla **confidenza e integrità** delle informazioni: uso di deep-fake, campagne di disinformazione, interferenza nella supply chain informativa, alterazione di dati, attacchi che mirano alla fiducia più che alla disponibilità o riservatezza.
In ambito aziendale può manifestarsi come alterazione di processi decisionali, uso di identità compromesse per diffondere false comunicazioni, attacchi reputazionali.

**Danni possibili per l'azienda**

- perdita di fiducia da parte di clienti, stakeholder, mercato
- falsi comandi o manipolazione di processi aziendali
- danni reputazionali o legali se dati alterati vengono usati come base decisionale
- comportamenti illegali inavvertitamente attivati (es. invio errato di comunicazioni, uso improprio di risorse)

**Rilevanza/contesto italiano**
L'ENISA e altre fonti europee indicano che la manipolazione delle informazioni è tra le prime minacce

emergenti. Per le aziende italiane, in contesti dove l'influenza esterna (politica, economica) è forte, il rischio può essere significativo anche se meno "tradizionale".

# OWASP Top 10 - MITRE ATT&CK

## Pratica extra

### Traccia

Per ogni scenario proposto identifica:

- OWASP Top 10 (se presente);
- MITRE ATT&CK Enterprise (tecnica principale);
- Mitigazione suggerita da MITRE ATT&CK.

### Esercizio

**SCENARIO 1**

*Un'azienda ha ricevuto segnalazioni da utenti che hanno subito attacchi XSS. Gli utenti hanno inserito dati in un form online che eseguiva script dannosi nel loro browser. Questo ha permesso agli attaccanti di rubare i cookie di sessione e impersonare altri utenti.*

**OWASP Top 10**: A03:2021 - Injection (Cross-Site Scripting)
**MITRE ATT&CK**
**Tattica**: Initial Access (TA0001)
**Tecnica**: T1659 - Content Injection
**Mitigazione:**

| Mitigazione: **ID** | **Mitigation** | **Description** |
|---|---|---|
| M1041 | Encrypt Sensitive Information | Where possible, ensure that online traffic is appropriately encrypted through services such as trusted VPNs. |
| M1021 | Restrict Web-Based Content | Consider blocking download/transfer and execution of potentially uncommon file types known to be used in adversary campaigns. |

**SCENARIO 2**

*Un attaccante è riuscito a ottenere accesso non autorizzato ai dati aziendali sfruttando una vulnerabilità SQL Injection nell'interfaccia di login di un'applicazione. L'attaccante ha manipolato l'input per eseguire comandi SQL non autorizzati, estraendo dati sensibili dal database.*

**OWASP Top 10**: A01:2021 - Broken Access Control (SQL Injection)
**MITRE ATT&CK**
**Tattica**: Initial Access (TA0001)
**Tecnica**: T1190 - Exploit Public-Facing Application
**Mitigazione:**

| ID | Mitigation | Description |
|---|---|---|
| M1048 | Application Isolation and Sandboxing | Application isolation will limit what other processes and system features the exploited target can access. |
| M1050 | Exploit Protection | Web Application Firewalls may be used to limit exposure of applications to prevent exploit traffic from reaching the application. |
| M1037 | Filter Network Traffic | Restrict outbound network traffic from public-facing servers to prevent unauthorized connections from initiating communications with attacker-controlled infrastructure. While this may not prevent the initial exploitation, it limits the attacker's ability to verify and control the compromised server post-exploit, reducing the overall impact of the attack. |
| M1035 | Limit Access to Resource Over Network | Ensure that all publicly exposed services are actually intended to be so, and restrict access to any that should only be available internally. |
| M1030 | Network Segmentation | Segment externally facing servers and services from the rest of the network with a DMZ or on separate hosting infrastructure. |
| M1026 | Privileged Account Management | Use least privilege for service accounts will limit what permissions the exploited process gets on the rest of the system. |
| M1051 | Update Software | Update software regularly by employing patch management for externally exposed applications. |
| M1016 | Vulnerability Scanning | Regularly scan externally facing systems for vulnerabilities and establish procedures to rapidly patch systems when critical vulnerabilities are discovered through scanning and through public disclosure.[10] |

**SCENARIO 3**

*Un attaccante è riuscito a eseguire codice arbitrario sul server sfruttando una vulnerabilità di deserializzazione non sicura del client in una funzione che accetta oggetti serializzati dall'utente. Manipolando l'oggetto inviato, l'attaccante ha ottenuto l'esecuzione remota di codice sul server.*

**OWASP Top 10**: A08:2021 - Software and Data Integrity Failures
**MITRE ATT&CK**
**Tattica**: Execution (TA0002)
**Tecnica**: T1203 - Exploitation for Client Execution
**Mitigazione:**

| ID | Mitigation | Description |
|---|---|---|
| M1048 | Application Isolation | Browser sandboxes can be used to mitigate some of the impact of exploitation, but sandbox escapes may still exist. [104] [105] |

| ID | Mitigation | Description |
| --- | --- | --- |
| | and Sandboxing | Other types of virtualization and application microsegmentation may also mitigate the impact of client-side exploitation. Risks of additional exploits and weaknesses in those systems may still exist. [105] |
| M1050 | Exploit Protection | Security applications that look for behavior used during exploitation such as Windows Defender Exploit Guard (WDEG) and the Enhanced Mitigation Experience Toolkit (EMET) can be used to mitigate some exploitation behavior. [106] Control flow integrity checking is another way to potentially identify and stop a software exploit from occurring. [107] Many of these protections depend on the architecture and target application binary for compatibility. |
| M1051 | Update Software | Perform regular software updates to mitigate exploitation risk. Keeping software up-to-date with the latest security patches helps prevent adversaries from exploiting known vulnerabilities in client software, reducing the risk of successful attacks. |