PENTESTERRA

ATTACK CHAIN ANALYSIS

# I Tuoi Finding Isolati Nascondono un Percorso d'Attacco?

Non una lista di CVE - un grafo di come un attaccante entra davvero, correlando finding da rete, web, codice e OSINT in percorsi di attacco verificati.

**COS'È, IN BREVE**

È la correlazione di finding di sicurezza individuali in percorsi di attacco multi-step - rete, web/API, codice, OSINT in un unico grafo - invece di trattare ogni finding come un ticket isolato. Ogni nodo è mappato a una tattica e tecnica MITRE ATT&CK.

**5 Fonti**

Rete, web, API, codice, OSINT in un solo grafo

**ATT&CK**

Ogni nodo mappato a tattica e tecnica

**Verificato**

Catene costruite da step provati, non teorici

## LA SITUAZIONE OGGI

**CHI SEI**

Sei il CISO o il responsabile sicurezza di un'azienda che vuole sapere non solo quali vulnerabilità esistono, ma come si combinano in un percorso reale verso i tuoi dati critici.

**COSA È SUCCESSO**

Tre team diversi hanno chiuso ciascuno il proprio ticket di severità media l'ultimo trimestre - nessuno sapeva che i tre insieme formavano un percorso critico.

**PERCHÉ FA MALE**

Un report di vulnerabilità valuta i finding in isolamento. Un attaccante no - li concatena. Quel divario è esattamente dove inizia una violazione.

## DOVE VUOI ARRIVARE

**STATO DESIDERATO**

Vuoi vedere, con prova concreta, come i tuoi finding isolati si concatenano in un percorso di attacco reale verso i tuoi asset critici - non solo una lista ordinata per CVSS.

**LA SOLUZIONE**

Un servizio di Attack Chain Analysis: correlazione cross-dominio di finding da rete, web/API, codice e OSINT in un grafo, con mappatura MITRE ATT&CK e scoring di business impact e compliance per ogni percorso.

**PERCHÉ È DIVERSO**

Non stai comprando l'ennesimo report di vulnerabilità in ordine di CVSS. Stai lavorando con [NOME AZIENDA] - fornitore certificato, italiano, con quasi 20 anni di storia nel settore della sicurezza informatica. Probabilmente ci conosci già, o conosci qualcuno che è già stato nostro cliente. E fino a 20 catene di attacco vengono calcolate per ciclo, a profondità fino a 5 - ogni catena è ricostruita da finding verificati con exploit reali, non da ipotesi CVSS: dopo una correzione, l'intera catena viene ri-eseguita per confermare che sia davvero interrotta.

**PROVA CONCRETA**

Il risultato è un report PDF completo, pronto da consegnare, con ogni percorso critico mappato su MITRE ATT&CK e la singola correzione a maggiore leva evidenziata. Se emergono gap più ampi, ti proponiamo le misure aggiuntive: penetration test, vulnerability assessment, revisione DevGuard del codice.

| Fino a 20 | Profondità 5 | Re-verifica |
|---|---|---|
| Catene di attacco calcolate per ciclo | Percorsi multi-step, non singoli finding | Ogni catena ri-eseguita dopo una correzione |

## COSA INCLUDE DAVVERO

Non una lista di CVE ordinata per punteggio - un grafo reale di come i finding si combinano.

### Correlazione cross-dominio

Il motore estrae finding da ogni fonte e costruisce un grafo di come si collegano.

- Finding di rete + web + API + codice + OSINT in un solo grafo
- L'artefatto del passo uno è l'input del passo due
- Non una lista di vulnerabilità - percorsi di sfruttamento realistici
- Ricalcolato a ogni ciclo di valutazione

### Mappatura MITRE ATT&CK

Ogni nodo di una catena è mappato a una tattica e tecnica ATT&CK.

- Mappatura tattica e tecnica per nodo
- Vista per fase, dall'accesso iniziale all'impatto di business
- Diff della catena tra cicli: nuove, chiuse, modificate

### Impatto di business e contesto compliance

Una catena che termina su un database di pagamenti conta più di una che termina su un microsito marketing.

- Scoring per processo di business e criticità dell'asset
- Mappatura compliance: OWASP, PCI-DSS, GDPR, NIST, ISO
- Executive summary più la singola correzione a maggiore leva

### Verifica reale, non ipotesi

Le catene sono costruite da finding verificati, non da ipotesi CVSS.

- Ogni step della catena supportato da verifica exploit
- Rilevamento di regressione se uno step corretto si riapre
- Separazione confermato/potenziale, chiara sull'esistenza reale del finding

PENTESTERRA

ATTACK CHAIN ANALYSIS

## COSA RICEVI

- ✓ Un report PDF completo con ogni percorso critico mappato su MITRE ATT&CK
- ✓ Correlazione cross-dominio di finding da rete, web, codice e OSINT
- ✓ Scoring di business impact e mappatura compliance per ogni catena
- ✓ La singola correzione a maggiore leva evidenziata per ogni percorso
- ✓ Re-verifica automatica delle catene dopo ogni correzione

## COME FUNZIONA

**1**

**Definiamo il perimetro**

Le fonti di finding da correlare - rete, web, codice, OSINT.

**2**

**Costruiamo il grafo**

Correliamo i finding esistenti in percorsi di attacco realistici.

**3**

**Mappiamo su ATT&CK**

Ogni nodo con tattica, tecnica, e impatto di business.

**4**

**Ti consegniamo il report**

Un PDF completo con i percorsi critici e la correzione a maggiore leva.

## Scopri i percorsi d'attacco nascosti nei tuoi finding

Un report completo, pronto da presentare a clienti, auditor o al tuo consiglio di amministrazione.

**Richiedi la tua Attack Chain Analysis →**

info@pentesterra.com · pentesterra.com/attack-chain-analysis