PENTESTERRA

BREACH & ATTACK SIMULATION

I Tuoi Controlli Fermerebbero Davvero un Attacco?

Simulazioni scenario-based mappate su MITRE ATT&CK - dimostra se i controlli che hai già comprato bloccano davvero un attacco reale, non solo se esiste una vulnerabilità.

COS'È, IN BREVE

È l'esecuzione di scenari di attacco realistici - accesso iniziale, esecuzione, escalation di privilegi, movimento laterale, impatto - usando template di adversary reali (APT29, APT28, Lazarus e altri) mappati su MITRE ATT&CK, per verificare se i tuoi controlli esistenti li fermano davvero.

MITRE ATT&CK

Ogni step dello scenario mappato a tattica e tecnica

Ricorrente

Esegue su schedulazione o on-demand, non una volta l'anno

Verificato

Un exploit funzionante dietro ogni controllo fallito

LA SITUAZIONE OGGI

CHI SEI

Sei il CISO o il responsabile sicurezza di un'azienda che ha investito in EDR, SIEM, firewall - e deve sapere se questi controlli fermano davvero un attacco reale, non solo se sono configurati correttamente sulla carta.

COSA È SUCCESSO

Avete comprato EDR, un SIEM e un upgrade firewall quest'anno - nessuno ha davvero testato se fermano un attacco reale.

PERCHÉ FA MALE

Un controllo che sembra configurato correttamente sulla carta e un controllo che blocca davvero una tecnica reale non sono la stessa cosa - e un incidente è un pessimo momento per scoprire la differenza.

DOVE VUOI ARRIVARE

STATO DESIDERATO

Vuoi sapere, con prova concreta, quali dei tuoi controlli di sicurezza fermano davvero un attacco reale e quali hanno solo l'aspetto di funzionare.

LA SOLUZIONE

Un servizio di Breach & Attack Simulation: scenari di attacco scenario-driven con template di adversary reali, validazione dei controlli di sicurezza esistenti, e un exploit funzionante verificato dietro ogni controllo fallito.

PERCHÉ È DIVERSO

Non stai comprando l'ennesimo tool di simulazione isolato. 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 i risultati diventano immediatamente parte di Attack Chain Analysis e Vulnerability Management, non un report separato da riconciliare a mano - la maggior parte dei fornitori vende questi come prodotti separati, con agenti separati e report separati.

PROVA CONCRETA

Il risultato è un report PDF completo, pronto da consegnare, con ogni controllo testato, quali hanno tenuto, quali hanno fallito, e l'exploit verificato dietro ogni fallimento. Se emergono gap più ampi, ti proponiamo le misure aggiuntive: penetration test, vulnerability assessment, formazione anti-phishing.

APT29 · APT28 · Lazarus

Template di adversary reali da MITRE ATT&CK

Non Distruttivo

Verifica exploit sicura per staging e produzione

Drift

Misurato tra una valutazione e l'altra

COSA INCLUDE DAVVERO

Scenari di attacco reali, non solo teorici - con un exploit funzionante dietro ogni controllo fallito.

Kill chain scenario-driven

Ogni simulazione esegue uno scenario di attacco completo, come si svolgerebbe un'intrusione reale.

- Template di adversary reali: APT29, APT28, Lazarus Group e altri, da MITRE ATT&CK e CVE curate
- Cicli di simulazione ricorrenti o on-demand
- Scenari interni, esterni e ibridi

Validazione dei controlli di sicurezza

Il punto non è il finding - è la risposta a 'il controllo lo ha fermato?'

- Copertura dei controlli preventivi e detective per scenario
- Drift dei controlli misurato tra le valutazioni
- Gap classificati per esposizione, non per numero di scenari

Un controllo fallito arriva con un exploit funzionante

Gli strumenti di sola simulazione dicono solo che un controllo non è scattato.

- Verifica exploit non distruttiva dietro ogni controllo fallito
- Passi di riproduzione ed evidenza allegati al finding
- Scope isolati staging/produzione, opzione human-in-the-loop

Integrato con scansione e pentest

BAS non è isolato - i risultati diventano subito parte di Attack Chain e Vulnerability Management.

- Condivide scope, asset e finding con gli altri moduli
- Nessuna flotta di agenti separata da distribuire
- Alimenta l'Attack Chain Analysis come step di percorso verificati

PENTESTERRA

BREACH & ATTACK SIMULATION

COSA RICEVI

- ✓ Un report PDF completo con ogni controllo testato e il relativo esito
- ✓ Simulazioni con template di adversary reali (APT29, APT28, Lazarus)
- ✓ Un exploit verificato dietro ogni controllo fallito
- ✓ Drift dei controlli misurato rispetto alla valutazione precedente
- ✓ Risultati integrati in Attack Chain Analysis e Vulnerability Management

COME FUNZIONA

1

Definiamo lo scenario

Adversary, tecniche e perimetro - stabiliamo insieme lo scope.

2

Eseguiamo la simulazione

In modo sicuro e non distruttivo, su staging o produzione.

3

Verifichiamo i controlli

Quali hanno tenuto, quali hanno fallito, con exploit a supporto.

4

Ti consegniamo il report

Un PDF completo con i gap prioritizzati per esposizione.

Scopri se i tuoi controlli fermano davvero un attacco

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

Richiedi la tua Breach & Attack Simulation →

info@pentesterra.com · pentesterra.com/breach-attack-simulation