

*SIMULAZIONE
AUTONOMA DI INTRUSIONE*

3BAS (Breach & attack Simulation)

Datasheet

Le aziende del Gruppo MEET IT



Via di Corticella, 89/2
40128 Bologna BO

+39 051 4070383
www.3cime.com | info@3cime.com



Viale Alcide De Gasperi, 37
33100 Udine UD

+39 0432 524001
info@ntonline.it | www.ntonline.it



AI DRIVEN BREACH AND ATTACK SIMULATION

La finestra sul “vero” attacco esterno che mostra quanto è davvero solida la tua difesa mentre un intruso digitale tenta di farsi strada nei meccanismi di Active Directory.

IL SERVIZIO

3BAS è una piattaforma **Cloud di Breach & Attack Simulation** (BAS) che sfrutta Intelligenza Artificiale e ottimizzazione matematica per eseguire autonomamente operazioni avanzate di ethical hacking, come le **Ransomware Simulation** e i tentativi di **Lateral Movement**, simulando un'intrusione reale all'interno di ambienti **Microsoft Active Directory**.

A differenza di un classico Penetration Test interno, la simulazione parte dall'esterno, riproducendo tecniche di attacco realistiche e mettendo alla prova l'intera catena difensiva, dalla prevenzione dell'escalation dei privilegi fino alla protezione dall'esfiltrazione dei dati.

PUNTI DI FORZA



REALISTICO

L'attacco è condotto da remoto, senza generare traffico anomalo rilevabile né dover creare esclusioni nei sistemi di difesa



SAAS CLOUD

Ogni simulazione sfrutta aggiornamenti continui tramite la piattaforma centralizzata.



MSSP-READY

Permette la gestione multi-tenant e l'esecuzione simultanea di BAS su più siti.



AGENTLESS

Non richiede né sonde né agenti sugli endpoint: basta eseguire il First Stage nella rete target.



AI-DRIVEN

Il motore DPZR™ coordina le tecniche di attacco con approccio realistico e ottimizzato



REPORT CHIARO

Risultati mappati sul framework MITRE ATT&CK® con impatto, tecniche utilizzate e piano di remediation.



NO FALSE POSITIVES

Evidenzia solo vulnerabilità realmente sfruttabili, come un attaccante esperto.



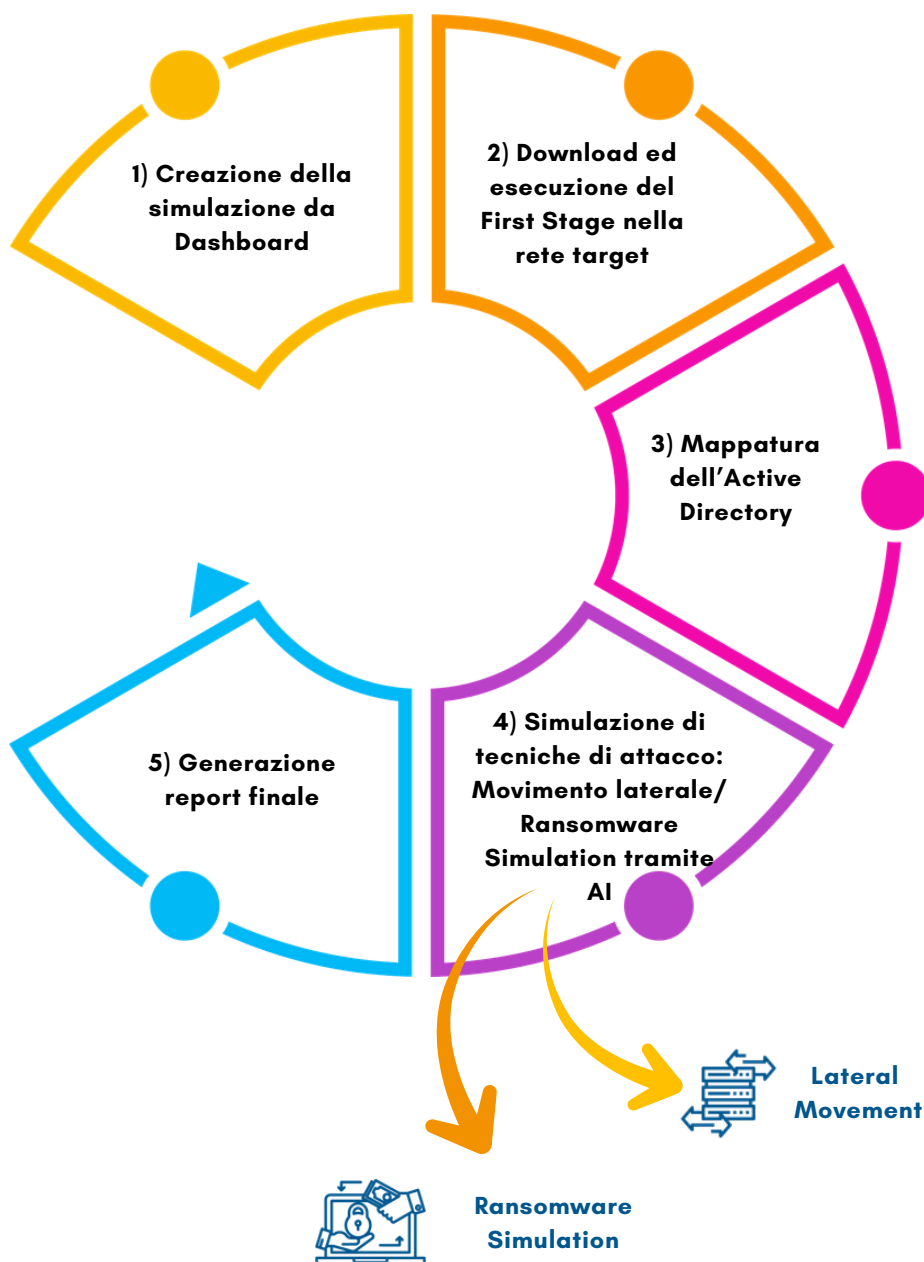
INTEGRABILE

API per l'integrazione con altre soluzioni di sicurezza e workflow automatizzati.

VISITA IL SITO **MEETIT.CLOUD**



COME FUNZIONA?



La piattaforma crea una **sandbox isolata** per ogni assessment e adotta tecniche stealth, replicando in modo fedele il comportamento di un vero **Red Team umano**. Questo include l'esecuzione di scenari di attacco complessi, come le **Ransomware Simulation** (simulazioni di attacchi ransomware completi). Tali capacità sono rese possibili da modelli di **Machine Learning** avanzati, in grado di imparare dinamicamente gli schemi comportamentali della rete e adattare di conseguenza le tecniche di attacco.

TECNICHE SIMULATE

3BAS è in grado di eseguire molteplici tecniche offensive avanzate, tra cui:

- **EDR/XDR evasion**
- **Comunicazione C2 via HTTPS + SMB pivoting**
- **Active Directory health check**
- **Simulazione ransomware**
- **Lateral movement**
- **Privilege escalation**
- **Esecuzione .NET/EXE/COFF in-process**
- **Sfruttamento misconfigurazioni AD**