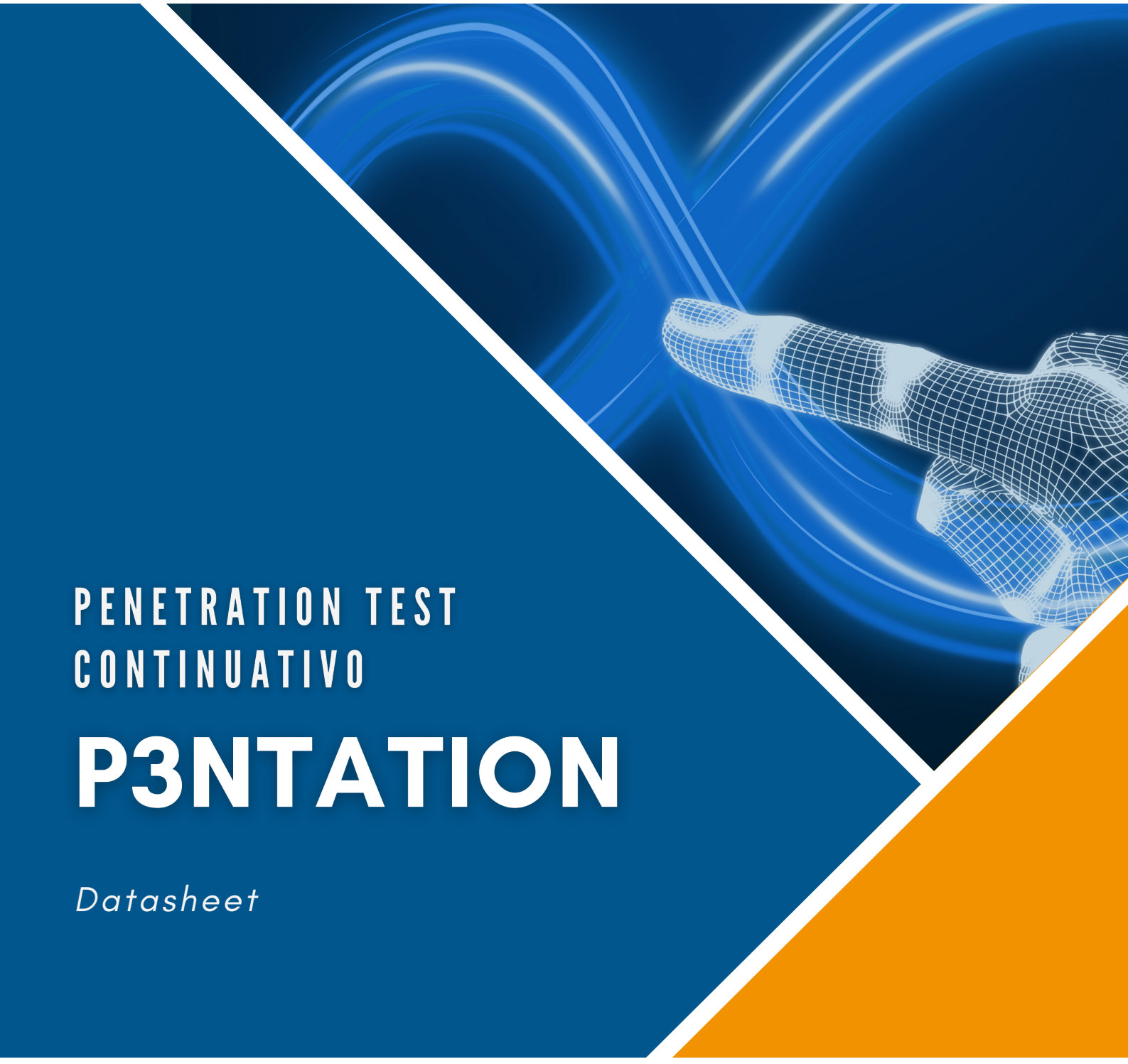

PENETRATION TEST CONTINUATIVO

P3NTATION

Datasheet

Le aziende del Gruppo MEET IT

Via di Corticella, 89/2
40128 Bologna BO

+39 05 14070383
www.3cime.com | info@3cime.com

Viale Alcide De Gasperi, 37
33100 Udine UD

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

TESTA. RILEVA. CORREGGI.

Il servizio pensa e attacca come un "hacker buono" per individuare tutte le vulnerabilità.

P3ntatioN è il servizio MEET IT dedicato al Penetration Test Continuativo che si basa su una **piattaforma agentless** utilizzata per la **vigilanza continua** e la **convalida proattiva della sicurezza** di tutto il sistema informatico aziendale.

Il testing avviene tramite una sorta di hacker virtuale che attacca costantemente l'infrastruttura IT del Cliente, alla ricerca di **eventuali vulnerabilità con lo scopo di fornire indicazioni sulle misure correttive da adottare**.

I comuni servizi di Penetration Test offrono una fotografia di un istante, che può variare nel tempo, e che non rappresenta il real time, in quanto le informazioni appena raccolte potrebbero già essere obsolete poco dopo il termine del test.

Il PenTest Continuativo, invece, simulando degli attacchi hacker reali, anche fra i più avanzati e recenti, testa continuamente ed in tempo reale il perimetro della sicurezza aziendale, in cerca di eventuali vulnerabilità da sanare. Il test, infatti, individua se ci sono punti deboli in cui un hacker potrebbe sferrare un attacco e a quale profondità potrebbe arrivare, allertando il team IT e **suggerendo azioni correttive immediate** per porre rimedio all'eventuale falla di sistema, senza interrompere o rallentare l'operatività e preservando l'integrità dei dati.

I suggerimenti per la remedation vengono forniti con una **roadmap** che tiene conto delle priorità a seconda dei rischi più importanti su cui è necessario concentrarsi.
Il servizio non rileva falsi positivi, ma solo minacce reali.

NECESSITÀ

Il servizio risponde alle domande più importanti per i Clienti:

- Quanto è sicura e conforme la nostra azienda in questo momento?
- Dove siamo più vulnerabili?
- Siamo protetti dalle minacce più recenti?
- In quanto tempo possiamo ripristinare la nostra compliance?
- Come possiamo prioritizzare le risorse della nostra azienda?
- Come possiamo comunicare meglio il livello di rischio alla direzione?

VISITA IL SITO *MEETIT.CLOUD*

ELEMENTI DI TEST

Pre-Exploitation

- Email Gateway
- Web Gateway
- Web Application Firewall

Exploitation

- Endpoint Security
- Phishing Awareness

Post-Exploitation

- Lateral Movement
- Data Exfiltration

VANTAGGI

Monitoring in tempo reale

Analisi puntuale delle vulnerabilità

Roadmap automatica per correzioni

Massimi livelli di sicurezza informatica

GDPR compliance

Scalabilità semplice

Facilità di utilizzo

Resilienza continua

Operatività continua 24/7 e on demand

VISITA IL SITO *MEETIT.CLOUD*

TIPI DI PENETRATION TEST

Penetration Testing (Black Box)

PenTest automatizzati full stack che includono tutte le funzionalità del prodotto. Non sono necessarie credenziali iniziali per eseguire questo test.

Test mirati

vengono utilizzati scenari di test predefiniti per preformare facilmente Penetration Test mirati o creare scenari di destinazione personalizzati utilizzando le opzioni avanzate

What-if (Gray Box)

si eseguono scenari di Penetration Test granulari con punto di partenza identificato e con la definizione dell'obiettivo finale. Serve per valutare il percorso che viene eseguito durante tutto il processo.

Valutazione delle vulnerabilità

valuta e identifica le vulnerabilità nella rete in base al punteggio CVSS.

FASI DI ATTACCO, SFRUTTAMENTO DELLE VULNERABILITÀ

All'interno di ogni Penetration Test, il servizio **esegue più fasi di attacco dinamico** contro i segmenti di rete di destinazione. Il test inizia con **Reconnaissance** (Scanning, Enumeration, Vulnerability Scan), mappando la superficie di attacco.

Sulla base dei risultati inizierà a sfruttare dinamicamente la rete con particolare attenzione alle vulnerabilità identificate. Ogni fase di attacco viene analizzata e i risultati possono essere utilizzati per continuare il test attraverso la rete, espandendo la superficie di attacco. Il servizio effettuerà lo **sniffing delle credenziali** per tentare di decifrare le password ed utilizzarle per accedere ai sistemi aziendali.

Continuerà poi con il **discovery** attraverso la rete per indirizzare il test. Inizierà il movimento laterale e seguirà azioni di **exploitation e post-exploitation**, cercherà di **bypassare le soluzioni EDR / NGAV** per convalidarne l'efficacia.

La fase finale è la **piena pulizia e sanificazione della rete** target.

Scansione

Il servizio sonda una rete identificando indirizzi IP attivi, porte e dettagli della topologia, individuando tutti gli host, i server e i relativi dispositivi.

Enumerazione

Estrae i dati utente, i dati del computer, i nomi host, le risorse/condivisioni di rete, il file system e altri servizi, creando una connessione attiva a un determinato sistema.

Valutazione delle vulnerabilità

Analizza degli host attivi alla ricerca di vulnerabilità note.

Credenziali di sniffing

Intercetta il traffico di rete e dei dati relativi all'host per estrarre le credenziali degli utenti con maggiore attenzione agli utenti con particolari privilegi, inclusi account di dominio Active Directory.

Cracking delle password

Utilizza più misure per recuperare le password in chiaro di utenti, host e server, decifrando gli hash delle password dai dati memorizzati o trasportati da un sistema, utilizzando una combinazione di tecniche di brute force e dizionario.

Relay

Intercetta le comunicazioni tra due parti e inoltra i dati a un altro dispositivo (di terze parti), comprese le tecniche basate sulla rete attraverso MITM.

Esecuzione di codice in modalità remota (RCE)

Utilizza più metodi per l'esecuzione di codice remoto su un determinato sistema, utilizzando le funzionalità di evasione della difesa per bypassare i meccanismi di rilevamento AV/EDR e aprire un canale C&C per controllare l'attacco al dispositivo di destinazione.

Raccolta dati

Raccoglie dati aggiuntivi dall'endpoint, inclusi prodotti di sicurezza, dettagli di accesso alla rete, credenziali di dominio/locali, credenziali/cronologia del browser, file SAM (Security Account Manager) e accesso a servizi e app critici cloud/locali.

Movimento laterale

Gestisce una procedura di estrazione del materiale di autenticazione per poter ruotare lateralmente verso nuovi endpoint in tutta la rete.

Escalation dei privilegi
Funzionalità remote e locali per testare in escalation utenti con accessi standard e privilegiati.

Esfiltrazione dati
Trasferisce i dati da un endpoint di destinazione innescato dall'acquisizione di un dispositivo.

Pulizia
Pulisce i sistemi dall'attacco nel caso in cui abbia inserito paylod.

Relazione dettagliata
Il rapporto dettagliato visualizza una ricca varietà di informazioni sulle attività e sui risultati del test. Tutti questi elementi sono inclusi per impostazione predefinita nel report dettagliato esportabile.

Relazione esecutiva
Il rapporto esecutivo mostra una panoramica dettagliata della situazione di sicurezza dell'organizzazione per quanto riguarda i segmenti di rete testati.

PERCHÉ SCEGLIERE IL SERVIZIO MEET IT?

Agentless
Il servizio non richiede l'installazione, la configurazione, la manutenzione o l'aggiornamento degli agenti, a differenza degli altri servizi sul mercato.

Full Attack Emulation - Exploit reali
Il servizio sfida la sicurezza degli endpoint con ethical exploit del payload per emulare scenari di attacco reali end-to-end. Tutti gli altri strumenti non sfruttano il punto finale, ma piuttosto deducono che può essere fatto anche se una Kill Chain completa è bloccata, quindi producono molti falsi allarmi.

Test dinamico basato sulla superficie di attacco
Il servizio esegue test dinamici su tutta la rete in base alla superficie di attacco, eseguendo exploit completi e attacchi post-exploitation per mostrare l'impatto completo della rete, non solo l'host.

Copertura completa dei segmenti di rete
Il servizio testa l'intera rete con scenari di test dinamici basati sulla superficie di attacco senza agenti. Il servizio trova tutte le vulnerabilità di rete in tutti gli host, Active Directory, Database, web hosting, dispositivi di rete, ecc.