SICUREZZA CONTINUA
DELL'ACTIVE DIRECTORY

P3NTATION AD

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

CONTROLLA E PROTEGGI CONTINUAMENTE IL TUO AD

Il servizio P3ntatioN AD ti permette di controllare la sicurezza dell'Active Directory, il cuore del tuo sistema informativo, di evidenziarne i rischi e di suggerire le remediation necessarie per ritornare periodicamente a livelli di sicurezza migliori.

Con il **Penetration Test per AD** riduci al minimo i percorsi di attacco e proteggi *Active Directory* e *Azure* da ogni angolazione.
La **gestione dei percorsi** di attacco è una componente fondamentale per difendere gli ambienti AD e Microsoft 365 dalle minacce informatiche.
Se si considera che Microsoft ha segnalato più di 25 miliardi di tentativi di attacco agli account aziendali solo nel 2021, la protezione dei percorsi di attacco risulta essenziale. *P3ntatioN AD* semplifica enormemente questo processo, **classificando e quantificando i punti critici dei percorsi di attacco**, fornendo le informazioni necessarie per identificare ed eliminare i percorsi con maggiore esposizione e rischio.

Tradizionalmente, la gestione dei percorsi di attacco è stata una sfida. Questo perché chi si occupa di sicurezza è spesso condizionato a pensare in termini di elenchi, controllando migliaia di problemi generici di configurazione. Gli attaccanti, invece, pensano in termini di grafici.
Questa prospettiva rende più facile per loro trovare percorsi di attacco efficaci. *P3ntatioN AD* ti aiuta a **ridurre il rischio di attacchi** in modo significativo, fornendoti una **mappatura grafica** di tutti i percorsi di attacco AD e Azure, che ti consente di identificare facilmente, dare priorità ed eliminare le vie più vitali che gli aggressori possono sfruttare.

USE CASE

Un progetto di questo genere è indicato in particolar modo quando le organizzazioni hanno **molti utenti da gestire**. Questo è vero anche nel caso di più Active Directory o di acquisizioni e fusioni di organizzazioni.

VISITA IL SITO *MEETIT.CLOUD*

Mappatura continua dei percorsi di attacco

Visualizzazione di ogni relazione e connessione in AD e Azure, per semplificare l'identificazione di percorsi di attacco nuovi ed esistenti.

Priorità dei punti di blocco

Misurazione dell'impatto di qualsiasi punto in un percorso di attacco e identificazione delle posizioni ottimali per bloccare il maggior numero di percorsi.

Protezione delle risorse critiche

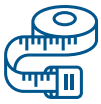
Identificazione delle risorse critiche di livello zero e monitoraggio automatico delle stesse al fine di rilevare eventuali attività sospette che indichino la loro compromissione.

Guida pratica alla remediation

Il Cliente ottiene una guida pratica alla correzione dei buchi, con istruzioni chiare, senza dover apportare modifiche drastiche all'AD.

Analisi completa della remediation

Si sfrutta la cronologia dettagliata delle attività degli utenti per ispezionare i confini del percorso di attacco prima di rimuovere l'accesso al percorso, assicurando che non vi siano conseguenze inaspettate nella bonifica.



Misurazione della postura di sicurezza AD

Si stabilisce una linea di base continua di AD e Azure, per monitorare e misurare la riduzione del rischio man mano che vengono rimossi i percorsi di attacco.

Visibilità senza precedenti su Azure AD

Azure utilizza tecnologie diverse per gestire le identità e gli accessi, ma è vulnerabile agli stessi tipi di attacchi alle identità di AD.

OUTPUT DEL SERVIZIO

Il servizio è **continuativo** e utilizzabile in fase di POC, visto in logica one-shot. AD infatti è in continua riconfigurazione e va monitorato permanentemente.

Il servizio include il **supporto sistemistico esperto** del Gruppo MEET IT, erogato via email all'indirizzo che verrà comunicato in sede di attivazione.

PREREQUISITI

Il Cliente deve avere o dotarsi di:

- Un **dominio AD Active Directory** o un **dominio Azure AD**
- Possibilità di installazione di un **agent** su di una **macchina Windows**
- Possibilità di far accedere tale macchina al **servizio SAAS** del Gruppo MEET IT (P3ntatioN AD)

VANTAGGI

Previene

I buchi trovati sono falle effettive nella sicurezza, non sono una statistica. Questo consente di prevenire rischi reali.

Ottimizza

Fornisce le soluzioni per ottimizzare il proprio sistema AD e renderlo più efficace e sicuro.

VISITA IL SITO *MEETIT.CLOUD*