SOLUZIONI DI SICUREZZA
PER ACTIVE DIRECTORY

SECURE AD

On prem, Cloud & Hybrid

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

SICUREZZA. CONTROLLO. PROATTIVITÀ.

Il servizio Secure AD di MEET-IT permette di mettere in sicurezza le configurazioni dei Microsoft Active Directory, nonchè di Microsoft Entra ID

I sistemi informativi delle nostre organizzazioni stanno diventando sempre più complessi. L'**Active Directory** rimane il **cuore delle nostre infrastrutture** e, di conseguenza, **lo strumento più importante da proteggere**, sia in configurazione completamente on premise che ibrida, integrata con Microsoft Entra ID. Il servizio Secure AD di 3CiMENT - gruppo MeetIT prevede una durata minima contrattuale di **3 anni**, con fatturazione annuale anticipata.

PREMESSA

Il servizio parte dalla costatazione che l'Active Directory è, insieme ai dati, la cosa più importante da proteggere in azienda.
I pirati informatici cercano sempre di rubare delle credenziali, partendo da quelle utente per arrivare a quelle di amministrazione. Una volta ottenute colpiscono i dati. L'**AD è dunque il ponte fra l'esterno e l'interno**, lo strumento irrinunciabile per lavorare, ma, allo stesso tempo, il più difficile da difendere.
Scopo del servizio, supportato ovviamente da prodotti di mercato è quello di **aiutare gli amministratori nella gestione di un ambiente complesso, nel capire se ci sono attacchi**, anche potenziali in corso, e nell'**applicare le best practice di configurazione**.

VISITA IL SITO *MEETIT.CLOUD*

L'utilizzo di strumenti di auditing in tempo reale per Active Directory garantisce **analisi approfondite e monitoraggio delle minacce alla sicurezza** su tutte le modifiche chiave alla configurazione, agli utenti e agli amministratori nel vostro ambiente AD. Il servizio traccia le modifiche ad Active Directory e rileva gli indicatori di compromissione (**IOC**) in AD e Entra ID per **contrastare gli aggressori e i loro tentativi di distribuire ransomware**. Inoltre, tiene traccia dei movimenti laterali degli avversari nella rete e controlla le attività sospette degli utenti.
Rileva tempestivamente le minacce, tra cui la replica non autorizzata dei domini, l'estrazione offline del database AD e il collegamento GPO a livello di dominio, per mitigare ed evitare costosi attacchi ransomware.
Impedisce agli aggressori di apportare modifiche a gruppi critici, impostazioni GPO e collegamenti o di sottrarre il database AD per rubare credenziali, indipendentemente dai privilegi che hanno dirottato.
Tramite lo strumento di **Logon Activity**, è possibile promuovere una maggiore sicurezza, controllo e conformità nella propria organizzazione acquisendo, segnalando e generando report su tutte le attività di accesso/disconnessione AD e di accesso Entra ID. Logon Activity rileva gli exploit Kerberos più comuni, identifica le vulnerabilità NTLM e fornisce strumenti di analisi forense di facile utilizzo per determinare chi ha fatto cosa e quando.
Sfrutta l'intelligenza artificiale generativa e l'apprendimento automatico per **rilevare attività insolite in Active Directory ed Entra ID**, come picchi di blocchi degli account, accessi non riusciti, modifiche alle autorizzazioni e rinominazioni dei file. Monitora continuamente le TTP (tattiche, tecniche e procedure) degli hacker e controlla le modifiche. Con un solo clic, GenAI Intelligence traduce i dati in riepiloghi rilevanti per l'azienda, consentendo ai team di sicurezza di semplificare le indagini e comunicare efficacemente i rischi ai dirigenti e alle parti interessate.

Il servizio prevede la possibilità di gestire le configurazioni di Active Directory in modo sicuro, al fine di:

Monitorare AD ed Entra ID in tempo reale

Correggere le mis-configuration

Attivare una sorta di Penetration test continuo sull'AD

Proteggere gli oggetti più importanti di AD

VISITA IL SITO *MEETIT.CLOUD*

Ciò a livello tecnico è molto importante e **più efficace rispetto alle soluzioni MFA** su cui alcuni clienti si indirizzano, perché **protegge l'AD alla fonte**. In periodi di elevata minaccia informatica, sia che si tratti di informazioni che suggeriscono un attacco imminente o di segnali di una violazione in corso, le organizzazioni potrebbero dover applicare temporaneamente controlli più severi sui propri ambienti Active Directory. La funzione **Shields Up** del servizio Securing AD fornisce un meccanismo di **risposta rapida per bloccare gli oggetti Active Directory critici, impedendo modifiche non autorizzate o accidentali durante un incidente di sicurezza**.
Questa modalità di emergenza è progettata per essere di breve durata ma altamente restrittiva, offrendo un modello di protezione preconfigurato che può essere attivato istantaneamente. In questo modo, contribuisce a salvaguardare le risorse di livello zero e altri componenti vitali dell'infrastruttura Active Directory fino a quando la minaccia non si attenua. Sebbene sia destinato all'uso temporaneo in situazioni di emergenza, Shields Up può anche essere implementato in modo continuativo come misura di sicurezza proattiva. Shields Up protegge le risorse e le configurazioni critiche di livello zero impedendo la cancellazione, la modifica o le variazioni delle politiche non autorizzate, tra cui:

- Impedisce la cancellazione e la modifica di utenti, computer, gruppi e politiche di gruppo di livello zero.
- Impedisce la cancellazione e la modifica di entità di sicurezza esterne e entità di sicurezza note.
- Impedisce al responsabile del dominio di collegare e scollegare politiche di gruppo, modificare la sicurezza e modificare ms-DS-MachineAccountQuota.
- Impedisce il collegamento e lo scollegamento delle politiche di gruppo per l'unità organizzativa (OU) dei controller di dominio.
- Impedisce la creazione, la cancellazione e la modifica dei modelli di certificazione.
- Impedisce le modifiche di sicurezza e le modifiche all'attributo DsHeuristics degli oggetti del servizio directory.
- Impedisce la modifica del contenitore AdminSDHolder.

L'obiettivo è quello di contenere e bloccare gli incidenti in corso interrompendo i movimenti laterali e le tecniche di persistenza prima che si aggravino, in modo da poter proteggere i sistemi critici in tempo reale, non dopo che il danno è stato fatto, ottenendo report mirati sullo stato degli oggetti, oltre alla possibilità di ripristinare facilmente qualsiasi modifica indesiderata a uno stato precedente e affidabile.

OUTPUT

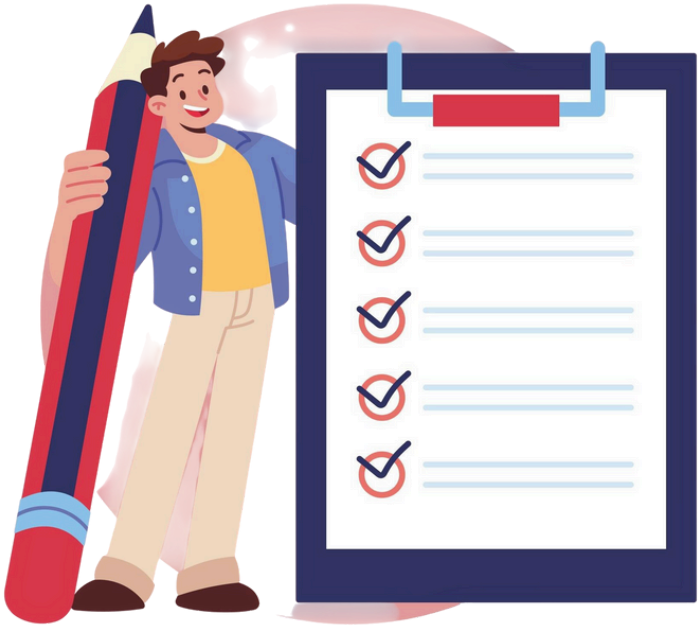
Il servizio prevede il supporto della configurazione dell'ambiente AD e Microsoft Entra ID : per l'attivazione è necessario "contare" gli utenti di AD della organizzazione.
La forza di output del servizio è quella di non rimandare semplicemente a documenti Microsoft che il cliente si deve leggere e decifrare in autonomia, ma nel **fornire la lista delle operazioni da seguire per le remediation di postura e di sicurezza** tramite l'utilizzo di un efficace motore di intelligenza artificiale.
Il servizio ha la durata di contratto ed include il supporto sistemistico di 3CiMENT - Gruppo MeetIT erogato dal team di assistenza.

PRE-REQUISITI

Ambiente Cloud e On-Premise

Fornire accesso all'AD del Cliente

Account Utente dedicato all'attivazione del servizio



LIMITI

Il servizio di supporto viene erogato nel normale orario di lavoro.

VISITA IL SITO ***MEETIT.CLOUD***