

Privileged Identity Management (PIM)

La soluzione

La soluzione **Privileged Identity Management (PIM)** permette di controllare, monitorare e mettere in sicurezza le utenze privilegiate.

Il servizio permette di automatizzare e generare password aggiornate dopo ogni accesso, controllando l'effettiva autorizzazione degli utenti.

Consente inoltre di ricostruire lo storico di ogni utilizzo delle utenze privilegiate, attraverso funzionalità di auditing, registrando puntualmente l'attività eseguita.

Prevede infine che gli utenti si colleghino attraverso un "proxy", evitando di creare un accesso diretto tra la workstation e il servizio.

A chi è rivolto?

La soluzione è rivolta alle aziende e organizzazioni che hanno sistemi, dati "sensibili", personale che opera con utenze di alto privilegio, come ad esempio **"Root"** o **"Administrator"**. PIM supporta una strategia di protezione degli account privilegiati, fondamentale per la sicurezza e l'accesso sicuro ai dati.



Come erogiamo il servizio

Cybertech offre 2 modalità di servizio:

1. Servizio di installazione, configurazione e messa in opera della piattaforma e successiva gestione in modalità SaaS (Software as a Service) o On Premise.
2. Servizio di gestione della piattaforma esistente del cliente, mettendo a disposizione le nostre competenze attraverso i servizi erogati dalla **Control Room Cybertech** o il supporto dei nostri esperti On Premise (presso le strutture del cliente).



Perché PIM

- Per accedere alle applicazioni e ai dati "sensibili" attraverso accessi e utenze privilegiate;
- Per proteggere da attacchi e furti informatici sia esterni che interni;
- Per mettere in sicurezza gli accessi privilegiati.



Punti di forza

I servizi PIM consentono di:

- Monitorare le attività eseguite da utenze privilegiate;
- Gestire il processo di rilascio e blocco delle credenziali;
- Identificare account non gestiti.



Vantaggi

- Soluzione chiavi in mano (SaaS);
- Gestione remota della piattaforma;
- Disponibilità del centro di competenze Cybertech.



Opzioni del servizio	Bronze	Silver	Gold
List of integrated Systems			
Number of Users	Up to 100	Up to 300	More than 300
Number of shared credentials	Up to 20	Up to 50	More than 50
Target System type integrated: Active Directory	✓	✓	✓
Target System type integrated: Linux	✓	✓	✓
Target System type integrated: Local Windows or Custom system target	✗	✓	✓
Custom Launcher	✗	✓ (n°1)	✓ (n°2)

Features			
Production Environment	✓	✓	✓
Secret Policy	✓ (n°5)	✓ (n°10)	✓ (n°15)
Approval workflow	✓ (n°1)	✓ (n°2)	✓ (n°4)
AD as Repository	✗	✓	✓
AD Discovery	✗	✓	✓
Session Recording	✗	✓	✓
Linux Discovery	✗	✗	✓
VMWare Discovery	✗	✗	✓
SSH WhiteList	✗	✗	✓
Proxy Feature	✗	✓	✓

Corrective Maintenance (1 year starting from production delivery)			
Support on delivered features	✓	✓	✓
Platform Monitoring	✓	✓	✓
Tickets per year	25	60	120



IBM Secret Server



IBM Security Secret Server offre diversi vantaggi e permette di:

- Scoprire tutti gli account utente e applicativi privilegiati in tutta l'azienda.
 - Memorizzare le credenziali privilegiate in un caveau (non un caveau fisico ma un server 'blindato'), con funzioni di check-in e check-out
 - Richiedere l'aggiornamento automatico delle password, ad es. dopo ogni utilizzo, a intervalli regolari o quando i dipendenti lasciano l'azienda, etc.
 - Controllare cosa effettivamente possono fare gli Amministratori di sistema privilegiati.
 - Prevenire l'uso non autorizzato di account privilegiati limitando nel caso ci siano troppi utenti privilegiati.
 - Registrare e monitorare le attività di sessione privilegiata per audit e forense.
 - Creare report di conformità.
- Controllare l'escalation dei privilegi delle applicazioni, revocando o limitando i privilegi tra gli amministratori IT e gli utenti aziendali.
 - Arrestare prontamente il malware ove fosse rilevato.

Endpoint



Per saperne di più visita il sito
www.cybertech.eu

