CYBERARK®

Cyberview
力悅資訊

Magic Secrets Cloud

特權機器
雲端環境允許機器利用特權角色，因此使任何有權訪問該機器的用戶/攻擊者獲得特權角色。

圖例

雲端特權風險

公共魔法雲

程式碼存放區

IAM

資料庫

資料庫

2.

3.

食死人

竊取存取權和密鑰，並使用它來破壞魔法雲

創建新的後門帳號

資料破壞

雲端特權帳號

當連接到雲端控制台時，某些非特權Active Directory帳戶以聯合登入方式取得特權角色。

雲端控制台

控制台特權存取

針對雲端控制台的特權存取應該受到良好地保護與監控。對於將資料存儲在雲端中的組織來說，錯誤的代價非常高。

巫師

霍格華茲網路

1.

服務

應用

資料庫

SOC 團隊
不知道新創建的後門帳號

ACTIVE DIRECTORY

4.

資安維運

IAM 代理程式

API 金鑰和令牌

Cloud API金鑰嵌入在腳本中，存在開發人員的端點上，在程式原始碼中及公開在儲存庫裡或嵌入容器中。

特權金鑰混亂

在沒有適當可見性和控制的情況下使用短暫的令牌會造成金鑰混亂，因為它提供的資訊非常有限：誰在使用金鑰、用途，及其背後意圖。

IAM與聯合解決方案

IAM解決方案彌合了組織的網路身份基礎架構與雲端應用程式和服務的身份驗證需求之間的鴻溝。用於保護該橋接方式的憑證應受到保護和監控。此外，IAM解決方案與聯合解決方案擴展了組織的第0級資產。密碼和特權API金鑰是在IAM代理程式和設備上處理或儲存的，對它們的損害等同於對Active Directory或其他第0級資產的損害。

www.cyberview.com.tw