CISO VIEW

是 CYBERARK 贊助的一項業界計畫。

迅速降低風險：

進行 30 天全力衝刺以保護特殊權限憑證

全球 1000 名 CISO 共同撰稿：

Rob Bening
首席資訊安全長，
荷蘭商業銀行

David Bruyea
資深副總裁兼首席
資訊安全長，CIBC

Dawn Cappelli
副總裁兼首席資訊
安全長，羅克韋爾自動化公司

Jim Connelly
副總裁兼首席資訊
安全長，洛克希德馬丁公司

Dave Estlick
資深副總裁兼首席
資訊安全長，星巴克

Steve Glynn
首席資訊安全長，
澳新銀行集團有限公司

Mark Grant
首席資訊安全長，CSX

Gary Harbison
首席資訊安全長，
孟山都公司

Kathy Orner
副總裁兼首席資訊
安全長，嘉信力旅運公司

Chun Meng Tee
副總裁兼資訊安全主管，
SGX

Munawar Valiji
資訊安全主管，英國新聞集團

Mike Wilson
資深副總裁兼首席
資訊安全長，麥克森公司

在編寫本 CISO View 研究報告的過程中，我們借鑒一直在第一線修復漏洞並防範攻擊的安全專業人士及技術專家的寶貴經驗。這提供種內部觀點，有助於我們從備受矚目的資料外洩資料外洩事件中汲取教訓。本報告簡要介紹公認框架，可在約 30 天的時間內快速實作一組關鍵防護控制措施，全力保護特殊權限憑證。

目錄

贊助者寄語

CYBERARK® CISO View 系列報告由 CyberArk 贊助，並由獨立研究公司 Robinson Insight 編寫。CISO 在嘗試根據過去經驗就加強特殊權限存取控制做出明智決策時，借鑒其他安全專業人士得之不易的寶貴經驗。我們對各界人士能夠分享自己的見解深表感謝，專家小組成員及客座撰稿人將與更廣大的社群一起解決此問題。

感謝客座撰稿人投稿：

在資料外洩資料外洩之後與大型企業合作的技術專家及顧問：

John Gelinne
網路風險諮詢服務部門總經理，
德勤會計師事務所

Gerrit Lansing
首席架構師，CyberArk

大型企業中經歷過嚴重資料外洩事故的安全主管 *

* 由於法律限制，這些高階主管在為本研究報告撰稿時並未署名。

簡介

您如何避免資料外洩？最終，您需要知道攻擊者採用何種技術，採取哪些安全防護控制措施能夠阻止攻擊者。為了瞭解相關資訊，CISO 通常會求助於一些不值得羨慕的「專家」：那些已遭受資料外洩的企業。

在編寫本 CISO View 研究報告的過程中，我們借鑒一直在第一線修復漏洞並防範攻擊的安全專業人士及技術專家的寶貴經驗。這提供一種內部觀點，有助於我們從一些備受矚目的資料外洩事件中汲取教訓。

在過去兩年中，有許多成功的攻擊都能利用被劫持的特殊權限憑證。在我們研究的事故中，攻擊者能夠利用在大多數企業 IT 環境中發現的常見漏洞，獲得網域級別的 Windows 管理者憑證。

由於用於建立惡意軟體的工具套件大量存在，攻擊者可以相對輕鬆地應用這些攻擊技術。它們已被用於完全控制整個網路並竊取大量資料。

鑒於風險日益上升，保護特殊權限憑證已成為目前許多企業的當務之急。幸運的是，不需要太長時間就可顯著降低風險。如果具有足夠的緊迫意識，甚至可以在數周內實現此目標 - 就像在實際發生資料外洩後通常採取的行動。

本報告簡要介紹公認框架，用於在約 30 天的時間內快速強制執行一組關鍵防護控制措施，全力保護特殊權限憑證。我們與由全球 1000 名受人尊敬的 CISO 組成的專家小組合作，共同提出一些建議，可幫助資安團隊主動保護企業。

CISO 及安全團隊如何利用本研究報告？

- 應用從實際資料外洩中汲取的教訓
- 更深入瞭解對於利用 Windows 管理者憑證的攻擊技術
- 向股東介紹這些攻擊技術
- 評估您的風險：您所在企業易受攻擊的程度？
- 分析現有防護控制措施：根據建議做法，如何使現有防護控制措施符合標準？
- 排定新防護控制措施的優先次序：應首先實施哪些措施？
- 獲得高階主管的支持，讓 IT 管理者確認風險

> [透過分析 2,260 次資料外洩事故後發現]，約三分之二的洩露事故起因於使用安全性不高的預設密碼或密碼被盜。*

*Verizon 2016 年資料外洩調查報告

主要結論：攻擊者利用 Windows 管理者憑證漏洞

雖然長期以來，特殊權限憑證一直易於受到攻擊，但與在 Windows 環境中用於管理工作站、伺服器及網域控制站的管理憑證相關的漏洞已變得特別嚴重。攻擊者已瞭解 Windows 機器如何在記憶體中儲存特殊權限憑證，以及企業通常如何管理 Windows 環境中的特殊權限憑證，並且能夠同時利用上述儲存方式及管理方式。

在我們分析的事故中，攻擊者最初透過網路釣魚入侵後，就可以利用取得的憑證從網路入侵多台機器。根據 Mandiant M-Trends 2016 年報告，由於有大量工具套件可供使用，攻擊大多數 Windows 環境中的高特殊權限帳號並從記憶體中取得憑證已變得「幾乎毫不費力」。平均來說，在獲得環境的初始存取權限後，Mandiant 的 Red Team 可在三天內取得網域管理者憑證。

這些技術不僅可以快速產生作用，而且可以讓攻擊者獲得前所未有的控制權。其中最危險的攻擊為 Golden Ticket 攻擊，因為入侵者會攻破網域控制站，然後竊取用於加密 Kerberos 票證及簽名的金鑰。攻擊者可運用此組金鑰，悄悄取得存取任何所需資源的任何特殊權限 - 全面佔有公司網路，包括所有關鍵資產及加入網域的所有安全系統。

Microsoft 已確認與 Windows 環境相關的憑證盜竊帶來的風險，並著手強化 Windows 環境以防範搜集憑證的攻擊技術。但是，全面發佈所有更新並在企業內完成部署可能需要數年時間。

> 由於當前實施的許多 Active Directory 網域服務已運行數年時間，存在憑證盜竊風險，因此，企業應假定出現資料外洩，且網域或企業管理者憑證很有可能已被攻破而未偵測到。
>
> —Microsoft，「降低 PASS-THE-HASH 及其它憑證盜竊風險，第 2 版」2014 年

您所在企業的易受攻擊程度

使企業易於受到攻擊的習慣做法實例：

- 為終端使用者（如軟體開發人員或遠端銷售人員）提供他們工作站的本機管理者權限
- 允許 IT 技術支援員工在排除工作站及伺服器故障時使用網域管理者帳號
- 為 IT 管理者提供網域管理者帳號存取權限「以防萬一」
- 使用複製映像設置新工作站，導致工作站使用相同的本機管理者密碼
- 每隔 30-60 天才輪換一次管理者密碼
- 使用 AD 群組原則輪換一個管理密碼，並將相同密碼用於所有機器
- 允許應用程式使用的帳號具有網域管理者特殊權限

主要結論：攻擊者使用特殊權限路徑存取關鍵資產

在我們研究的事故中，攻擊者完成初步入侵的方式如下：利用惡意附件進行網路釣魚，等待使用者隨後下載惡意軟體到使用者的工作站。在 Windows 環境中，無論最初採用何種入侵手段，攻擊者都可以使用既有的特殊權限路徑擴大其攻擊範圍，從被攻破的工作站入侵包含重要資料的關鍵資產。

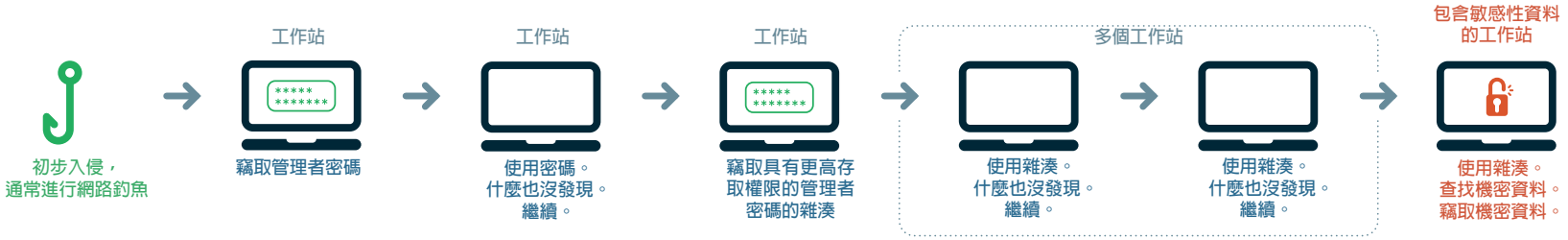
攻擊者的攻擊動機各異。攻擊者可能會探查整個環境，儘可能找到有用資訊，如敏感工作站上的財務資料，或資料庫伺服器中的信用卡號碼。或者，攻擊者可能野心更大，希望存取網域控制站，進而存取所有關鍵資產。

攻擊者如何從一個工作站暢行於多個工作站

攻擊者可在入侵的第一個工作站上，使用鍵盤側錄惡意軟體竊取工作站管理者密碼。如果其它機器使用相同的密碼，攻擊者就可以輕鬆登入另一工作站。

甚至攻擊者不需要知道密碼，攻擊者可利用其它更強大的憑證竊取技術更快速地從一台機器進入另一台機器。使用 pass-the-hash 技術，攻擊者可以取得儲存在電腦記憶體中、最近登入該機器的所有使用者（包括管理者）的密碼雜湊。攻擊者可使用竊取到的密碼雜湊輕易入侵其它工作站，最終登錄敏感工作站（圖 1）。

圖 1：進入包含敏感性資料的工作站



具體 pass-the-hash 攻擊實例：如果某技術支援人員最近協助過維修一台工作站，攻擊者就可以從該工作站竊取該技術人員的帳密雜湊，然後使用竊取的雜湊進入該技術人員有存取權的其它工作站。

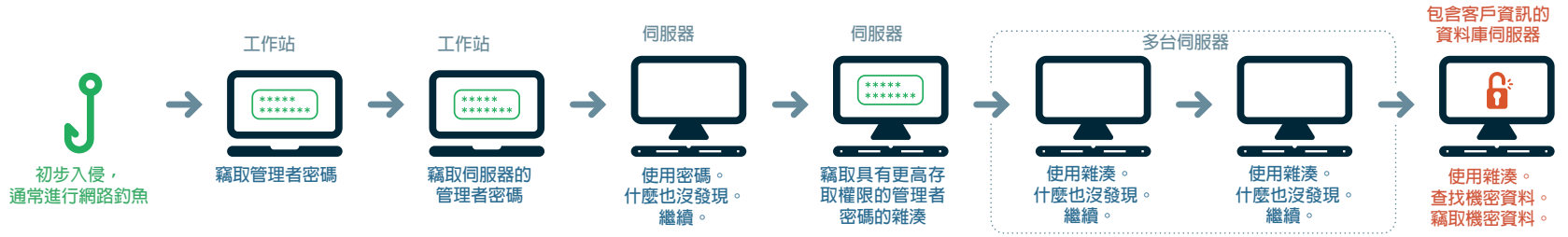
Pass-the-hash 是最有名的憑證取得技術。Pass-the-hash 是一種濫用 Kerberos 及 NTLM 身份驗證協定的方法。其它變化形式包括從被攻破的機器竊取 Kerberos 票證，將竊取的 Kerberos 票證部署到另一台機器上（pass-the-ticket），或者使用竊取的雜湊建立新的 Kerberos 票證（overpass-the-hash）。

攻擊者如何存取更高價值的資產

使用上文介紹的憑證竊取技術輕易入侵多台機器，攻擊者還可以提升其特殊權限，獲得更高價值帳號及機器的存取權限。例如，攻擊者可以使用竊取的憑證從入侵的第一個工作站進一步入侵進入另一工作站。如果使用者在第二台工作站上使用同一管理帳號存取某台伺服器，現在，攻擊者就可以存取該伺服器。接下來，攻擊者可以繼續進行憑證盜竊，入侵各伺服器。攻擊者可透過查找伺服器管理者密碼的雜湊，獲得更高的存取權限，進入多台伺服器，最終到達客戶資料庫（圖 2）。

> 一旦侵入您的網路，攻擊者首先會設法提升所擁有的特殊權限。如果未遵循最佳實踐，攻擊者就可以在彈指之間，非常輕鬆地在您的整個網路暢行無阻。
>
> —JIM CONNELLY，
> 副總裁兼 CISO，
> 洛克希德馬丁公司

圖 2：進入包含客戶資訊的資料庫

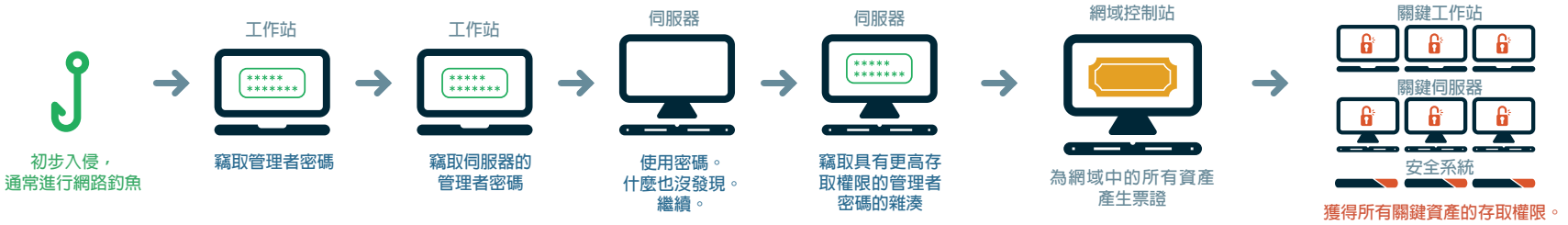


使用相同的技術，攻擊者還可以從伺服器進入網域控制站。一旦網域控制站被攻破，攻擊者就可以進行 Golden Ticket 攻擊，這樣，攻擊者就可以假冒成身份驗證機構，存取網路中的所有資產，包括安全系統及已與 Active Directory 整合的非 Windows 系統（圖 3）。

導致企業非常易於受到 pass-the-hash 及類似攻擊的習慣做法包括：

- 允許使用者在他們自己的工作站上使用具有管理特殊權限的帳號
- 所有本機管理者帳號使用相同的管理者密碼
- 未能一致地對 IT 管理者帳號強制執行密碼輪換或唯一性原則
- 設置網域管理者帳號，將其用於登入網域控制站以及伺服器及工作站
- 允許使用管理者帳號執行日常任務，如檢查電子郵件及瀏覽網際網路

圖 3：進入網域控制站



關閉特殊權限路徑

通常，安全團隊專注於在攻擊路徑的起始（防止網路釣魚）及結束（保護關鍵資產）階段採取防護控制措施。但是，採取防護控制措施以關閉特殊權限路徑才是關鍵。

雖然與以前相比，員工接受了更好的培訓，但網路釣魚的成功率仍然非常高。研究表明，有 30% 的員工會開啟網路釣魚訊息，約 13% 的人會按一下惡意附件或連結 *。毋庸置疑，在攻擊路線的另一端對關鍵資產採取保護措施非常重要。但是，攻擊者可透過使用特殊權限路徑，利用非關鍵資產避開或停用對關鍵資產採取的防護控制措施。

*Verizon 2016 年資料外洩調查報告

> 我們汲取到的其中一個教訓是，如果您的工作站及伺服器存在 pass-the-hash 類型的漏洞，攻擊者就能夠以非關鍵資產為支點，進而侵入關鍵資產。
>
> —GERRIT LANSING，
> 首席架構師，CYBERARK

建議措施

在攻擊者成功利用特殊權限路徑存取關鍵資產的事故中，「哪些措施有助於阻止攻擊呢？」已確定可以採取以下措施。這些策略奠定控制框架（第 10-12 頁）的基礎。

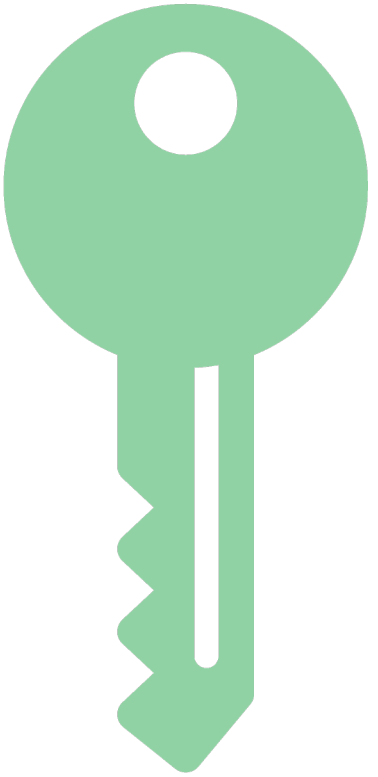
避免暴露特權憑證

限制管理憑證與攻擊者之間的接觸點至關重要。具體來說，如果工作站中安裝了惡意軟體，應確保惡意軟體無法控制本機管理者權限，蔓延到其它機器及 / 或發現伺服器或網域管理者帳號。

- 在您的身份認證結構內建立邊界以強制實行職責分離：
  - 網域管理者帳號應僅用於管理網域控制站，而不是伺服器或工作站
  - 伺服器管理者帳號應僅用於管理伺服器，而不是工作站
  - 工作站管理者帳號應僅用於管理工作站
- 管理者帳號僅用於執行管理任務，而不是日常活動
- 網域管理者帳號僅提供給絕對需要使用該帳號執行例行工作的人員
- 確保應用程式及服務使用的帳號只有最小權限：
  - 取消應用程式帳號的管理者特殊權限可能需要重構應用程式；一般來說，應用程式根本不需要這種級別的特殊權限，雖然有時為了方便開發人員，會以這種方式編寫或設定應用程式
- 禁止在連接網際網路的工作站上使用管理帳號存取敏感資產：
  - 請使用跳板機或未連接網際網路的專用管理工作站
- 禁止提供本機工作站管理者權限給員工（如軟體開發人員）：
  - 請從本機管理者群組中刪除他們的帳號，並使用工具提供暫時提升的特殊權限來執行需要管理者權限的臨時任務

建議措施一覽

- 避免暴露特權憑證
- 採用強密碼並將其儲存在加密金庫中
- 最大幅度減少管理者帳號數量
- 加強監控特權憑證盜竊事件



採用強密碼並將其儲存在加密金庫中

堅持採用以下這些做法有助於企業確保攻擊者無法竊取管理憑證或在其它機器上使用這些憑證：

- 需要使用具有嚴格規定長度及複雜性標準的唯一密碼
- 經常輪換密碼，最好是使用一次性密碼（或至少每天輪換一次）
- 自動選擇及輪換密碼
- 將密碼存放在加密儲存並防篡改的數位金庫中
- 使用者及應用程式需要透過多因子身份驗證才能存取金庫中的密碼

最大幅度減少管理者帳號數量

理想情況下，企業應建立最少數量的特殊權限帳號，以最大幅度減少受攻擊面並簡化憑證及帳密管理。

- 避免在 Active Directory 中為管理者設置單獨分配的特殊權限帳號。例如，以下一般流程有可能導致帳號增生的問題：
  - IT 服務台技術人員 Alice 擁有一個用於執行日常工作的帳號「Alice」，以及另一個具有所有工作站管理權限的帳號「Admin-Alice」
  - 伺服器管理者 Bob 擁有帳號「Bob」，以及另一個具有其工作站及伺服器管理權限的帳號「Admin-Bob」
  - 網域管理者 Charles 擁有帳號「Charles」，以及具有其工作站、伺服器及網域控制站管理權限的帳號「Admin-Charles」
- 將已經存在的內建本機管理者帳號用於所有工作站及伺服器：
  - 這些帳號可以共用，同時保留了各自的責任：保管憑證，並要求管理者在需要時，遵循程序從金庫中取出這些憑證。帳號的特權活動此時才有辦法可以受到控制及監管。（應刪除上述 Admin-Alice、Admin-Bob 及 Admin-Charles 帳號。）
  - 雖然可以使用內建帳號執行許多管理任務，但仍然可能需要設置個人管理者帳號，但這類帳號應盡可能地減少

30 天衝刺框架

這是一個快速行動框架，可幫助關閉 Windows 環境中的特殊權限路徑。旨在確保即使攻擊者攻破了某個工作站，仍然非常難以更進一步入侵，並且可以偵測攻擊者的進一步入侵 。

本框架致力於加快工作進度，在短期內（如 30 天）實施關鍵防護控制措施。保持衝刺思維（見側邊欄）的企業已實現此目標。完成衝刺所需的實際時間各不相同，具體取決於企業的規模、複雜性、成熟度及文化。

雖然本框架致力於對 Windows 管理帳號採取具體防護控制措施，保護 Windows 環境，但企業還應同時實施其它關鍵防護控制措施，如給作業系統及應用程式安裝修補程式，以及建立應用程式白名單。

建議的防護控制措施

下表列出了一組建議的防護控制措施，並說明應首先實施哪些防護控制措施以及後續步驟。

優先排序

建議的優先排序基於以下能盡力進行的項目：

- **快速確定帳號** – 確定 Windows 環境中的管理帳號
  - 對於快速行動計畫來說，前期分析不應花費太長時間，因為我們可以相當輕鬆地確定 Active Directory（AD）及本機管理者群組中的帳號。
- **優先考慮風險最高的帳號** – 首先控制最高權限帳號
  - 網域管理者帳號及有權存取大量機器（特別是伺服器）的管理者帳號，以及使用網域管理者特殊權限的應用程式帳號。
- **落實處理大量帳號** – 快速實施某些防護控制措施，然後逐步改進
  - 例如，理想情況下，工作站使用者的帳號不得具有管理特殊權限，但是，事故倖存者表示，考慮到工作站的絕對數量，落實並保持這種做法可能非常困難。

衝刺思維

如何快速在整個企業中部署一組新的安全防護控制措施？這取決於企業的緊迫意識。在遭遇資料外洩之後，企業內部達成一致，決策開始加速，立竿見影的效果戰勝了官僚主義，在短期內顯著提高安全保護成為可能。

當然，所有事故倖存者都希望他們及時完成衝刺，避免產生損失，這正是主動 30 天衝刺的目標。

> 即使 CISO 無法在 30 天內實施所有防護控制措施 – 但這樣做的意圖顯而易見。您必須排定優先次序。框架會進行細分 -「從這裡開始。首先落實這些措施」。這絕對有效，無論是 30 天、60 天還是 180 天。
>
> —STEVE GLYNN，CISCO，澳新銀行集團有限公司

30 天衝刺框架

建議的防護控制措施	**首先：首先處理這些帳號** *旨在於短期內（如 30 天）控制這些帳號。*	**然後：然後處理這些帳號** *實施這些防護控制措施可能需要更多時間，具體因企業而異。*
• 重新設定帳號以劃分職責	網域管理者帳號*（僅用於登入網域控制站）* 伺服器管理者帳號*（僅用於登入伺服器）* 工作站管理者帳號*（僅用於登入工作站）*	
• 將管理者密碼存放在金庫中 – 自動選擇及輪換密碼（如一次性密碼） – 監控密碼使用情況	網域管理者帳號 伺服器管理者帳號	工作站本機管理者帳號
• 需要通過多因子身份認證才能存取金庫中的密碼	所有密碼已存放到金庫中的帳號 *由於密碼已存放到金庫中，企業將在一段時間內繼續實施多因子身份認證。*	
• 隨機選擇管理帳號密碼，確保其唯一性	工作站本機管理者帳號	
• 禁止在連接網際網路的工作站上使用管理帳號存取敏感資產 – 使用跳板機或未連接網際網路的專用管理工作站 • 僅將管理者帳號用於執行管理任務 – 不用於執行日常活動	網域管理者帳號 伺服器管理者帳號 工作站管理者帳號	
• 盡可能避免使用個人的管理帳號（這會導致帳號增生） – 而是，應讓管理者使用內建帳號，並透過金庫存取密碼（參見第 9 頁瞭解詳情）	網域管理者帳號 伺服器管理者帳號 *對某些企業來說，在短期內刪除個人的管理者帳號並不實際。最初的解決辦法，是將個人的管理者帳號密碼存放到金庫中，然後逐步從使用個人的帳號改為使用內建帳號。*	工作站管理者帳號

接下一頁

30 天衝刺框架

接上一頁

建議的防護控制措施	**首先：首先處理這些帳號** *旨在於短期內（如 30 天）控制這些帳號。*	**然後：然後處理這些帳號** *實施這些防護控制措施可能需要更多時間，具體因企業而異。*
• 取消終端使用者的工作站管理者特殊權限 – 在需要時臨時提權		工作站本機管理者帳號 *應從本機管理者群組中刪除終端使用者帳號。如果使用者需要在工作站上執行需要管理者特殊權限的任務，則僅臨時提升特殊權限以執行特定的活動。*
• 使用偵測工具搜尋入侵或即時提權的跡象	網域管理者帳號 伺服器管理者帳號 工作站管理者帳號	
• 如果任何應用程式使用網域管理者特殊權限，如存取多台伺服器的管理者權限，則取消這些特殊權限	應用程式帳號 *對某些企業來說，在短期內處理所有這些應用程式並不實際，因此，將在一段時間內繼續重新設定或重新編寫應用程式。*	

表格備註：

- 網域管理者帳號：AD 中用於管理網域及網域控制站的帳號
  - 例如，企業管理者及網域管理者
- 伺服器管理者帳號：AD 中用於管理伺服器的帳號
  - 例如，資料中心員工用於維護多台伺服器的帳號
- 工作站管理者帳號：AD 中用於管理大量工作站的帳號
  - 例如，服務台及員工用於提供技術支援的帳號
- 工作站本機管理者帳號：每個工作站上的本機管理者群組中的帳號
  - 例如，用於在各個工作站上執行管理活動的帳號
- 應用程式帳號：應用程式用於運行系統或排程的非使用者帳號
  - 例如，用於執行備份或安裝軟體的帳號

衝刺之前

在開始衝刺之前，您需要選定用於保管密碼、多因子身份驗證以及進行偵測的技術，並成立團隊。成立小型團隊即可相當迅速地控制最重要的權帳號。例如，在發生資料外洩之後，僅有八位成員的團隊與一名安全顧問合作，在四周內保管 20 個網域及 6,500 台伺服器的管理者帳號。與在遭遇過資料外洩下全面實作控制握施相比，主動展開這項工作的進展會相對順利。

衝刺之後

通常，在開始衝刺之後，企業的待辦事項包括以下任務。

*控制更多帳號：*為了涵蓋 Windows 以外的帳號，請瞭解所有特殊權限帳號的範圍。有各種技術都會使用特殊權限帳號，如 Oracle 資料庫、Unix 及 Apple 電腦、NAS 及 SAN 存放裝置、任何具有 IP 位址的設備、虛擬環境中的系統管理程式及操作服務，以及雲端服務。

*增加控制的深度：*瞭解如何強化控制以監控帳號使用情況。例如，針對大多數敏感帳號，增加特殊權限連線側錄或使用者行為分析。

*繼續重構應用程式：*應用程式（特別是傳統應用程式）通常需要管理者特殊權限並使用會增加密碼輪換難度的嵌入式密碼。一般來說，應確保所有應用程式被授予了所需的最小特殊權限並安全使用密碼。要解決這些問題，通常需要重新設定或重新改寫應用程式。這不僅包括內部應用程式，也包括協力廠商應用程式。在這些情況下，企業必須與供應商合作，共同做出修改。

*使方案正式化：*制定流程來維護及支援新的防護控制措施，分析如何解決「可以採取什麼流程在系統中增加新資產及淘汰過時資產？」之類的問題。確保這些流程能夠滿足不斷變化的業務需求，並定期確認是否實現安全及業務目標。

CISO 及其安全團隊可以利用衝刺產生的動力轉型到更加全面的企業計畫 - 可能需要付出多年的努力。CISO View 報告《平衡法則：CISO 關於強化特殊權限存取控制的觀點》提供了以下三個關鍵領域的同行建議：

- CISO 及其團隊需要做出的策略決策
- CISO 需要在整個企業內發起的對話
- 成功計畫的基本組件

> 在受到網路攻擊期間強制執行安全保護措施，就好像在颶風來臨時給您的房子安裝防風窗一樣。與從資料外洩攻擊中復原後實施防護控制措施相比，現在就採取措施來保護高風險特殊權限憑證要容易得多。
>
> —JOHN GELINNE，總經理，
> 網路風險諮詢服務部門，
> 德勤會計師事務所

評估進度

有用的指標：

- 透過滲透測試來測量在實施防護控制措施之前與之後攻擊者攻破高價值帳號所需的時間。
- 使用自動工具掃描網路，確定需要更全面保護的帳號。在實施防護控制措施之後，再次掃描網路，瞭解易受攻擊的帳號的減少情況。

結論

攻擊者已提升了其技能，能夠利用 Windows 中的特殊權限路徑存取關鍵資產並竊取敏感性資料。如果不實施全面的防護控制措施來保護管理帳號，企業將因此面臨風險。本衝刺框架提供快速行動計畫，可協助實施一組防護控制措施來關閉特殊權限路徑。

要成功完成計畫，安全團隊需要整個企業的支援。說服 IT 管理者也至關重要。IT 管理者可能需要接受工作流程變更，或降低自己的特殊權限。但是，更有效的安全措施不僅可以保護整個企業，也可以保護管理者個人。這樣，即使由於攻擊者控制特權帳號而發生事故，管理者也可以快速洗清嫌疑。CISO View 報告《平衡法則》的「四段關鍵對話」一章提供了更多有關說服他人及處理異議的建議。

另外，還要贏得管理層這個關鍵團體的支持。管理層需要幫助確定組織的優先工作並增強緊迫感。有關如何與高階主管及 / 或董事會溝通的行為指南，請參閱下面附錄中的常見問題解答。

要存取其它 CISO View 報告，請瀏覽
www.cyberark.com/cisoview

> 您應表現得好像剛剛遭受過攻擊。如果受到攻擊，您將被迫設法解決問題。思維模式將從「這太難了，我們做不到」轉變為「我們必須做到！」，這是當務之急。
>
> —**客座撰稿人**

附錄 1：高階主管及董事會常見問題解答

此常見問題解答旨在幫助高階管理人員及董事會瞭解風險及相應的規避計畫。

1. 為什麼我們需要全力保護特權帳號？

如果未得到充分保護，我們將面臨資料外洩風險，如同新聞報導的情況，面臨影響許多大型企業的重大攻擊風險。在這些情況下，攻擊者利用 Windows 環境中的漏洞竊取特殊權限憑證，隱秘地在網路中執行操作，企圖全面控制企業的資訊系統。

這類攻擊的風險日益嚴峻。攻擊者可以廣泛使用各種工具套件，輕鬆開發自製工具來進行攻擊。Microsoft 本身也建議導入更有效的控制來降低風險。

透過研究分析這些嚴重資料外洩事故，我們可以瞭解需要對安全防護控制措施做出哪些改進。透過約 30 天的切實努力，我們將實施防護控制措施來加強保護，使攻擊者更難針對我們發動這些類型的攻擊。

2. 相比於其它安全目標，為什麼應優先保護特權帳號？

如果攻擊者竊取到特權帳號，將可以獲得非常高的權限來存取資訊系統。通常，特殊權限憑證是指員工（如 IT 管理者）用於操作及管理整個企業的運算資源的密碼。

使用特殊權限憑證，攻擊者可以存取智慧財產權、商業機密及客戶資訊。此外，攻擊者還可以停用任何安全技術，如企業已佈建的資料加密、防火牆以及偵測系統。

3. 攻擊者使用哪些技術來竊取特權帳號？

眾所周知，在大多數這類攻擊中，第一步是進行網路釣魚。使用者受到欺騙，按一下某個連結或開啟某個電子郵件附件，這會將惡意軟體下載到他們的工作站。研究表明，儘管付出了巨大努力對使用者進行反網路釣魚培訓，但網路釣魚的成功率實際上卻有所提高。

一旦惡意軟體下載到工作站上，攻擊者就可以侵入 Windows 環境，並利用 Windows 機器儲存憑證的方式。Windows 將所有最近登入該機器的使用者的密碼「雜湊」（即固定長度的密碼編碼）儲存在電腦記憶體中。透過竊取管理密碼的雜湊，攻擊者就可以存取多台機器。攻擊者會在每台機器的記憶體中搜尋其它密碼雜湊，這些雜湊繼而又可用於存取更有價值的機器（如資料庫伺服器），或者攻擊者達成存取網域控制站的最終目

標取得管理所有運算資源存取權限。一旦攻擊者存取網域控制站，就可以建立「票證」來登入網路上的任何關鍵資產，關閉安全系統，並完全控制資訊系統。

4. 您將如何加強對特權帳號的保護？

我們的原則是實施控制措施，例如：

- 為所有管理者帳號自動選擇並輪換唯一、複雜的密碼
  - 如果攻擊者得知一個密碼，尚可防止攻擊者能夠入侵多台機器
- 隔離用於管理網域控制站、伺服器及工作站的帳號
  - 使攻擊者無法使用竊取的憑證存取不同類型的機器
- 使用自動強制執行密碼原則並能夠監控管理活動以偵測憑證竊取行為的密碼金庫
  - 數位金庫具有防篡改能力，並且使用軍事級加密來儲存密碼
- 對存取金庫中密碼的授權使用者使用雙因子身份驗證

此策略與 Microsoft 就如何在企業 Windows 環境中防止憑證盜竊而提供的建議相一致。

5. 與其它企業採取的行動相比，本計畫如何採取行動？

許多在過去兩年中受到網路攻擊影響的企業都致力於採取補救措施，致力於更全面保護特權帳號。同時，全球其它企業也主動（而不是在受到攻擊之後）加強對特權帳號的安全保護。由全球 1000 名 CISO 組成的專家小組已發佈指導準則，說明如何制定全面的計畫來強化特殊權限存取控制，這些 CISO 分別來自荷蘭商業銀行、CIBC、羅克韋爾自動化公司、洛克希德馬丁公司、星巴克、澳新銀行、CSX、孟山都公司、嘉信力旅運公司、英國新聞集團及麥克森公司。請參閱《平衡法則：CISO 關於強化特殊權限存取控制的觀點》。

6. 您需要公司管理層提供哪些支持以成功實施本計畫？

獲得管理層的適當支持，您可以幫助確保：我們能夠迅速成功地在整個企業部署一組新的安全防護控制措施。雖然資安因素會驅動專案進展，但受影響的系統是業務單位所負責，因此這需要各個職能部門的支援。

要想快速降低風險，保持「衝刺思維」是最重要的因素之一。我們將嘗試保持與在遭受實際攻擊之後相同的緊迫感及進度 - 而不必承受阻止攻擊的可怕壓力。一些人必須於此作出變化，如：「放棄存取權限或採用新流程時猶豫不決。」，管理層制定的方針對於快速取得進展至關重要。

附錄 2：CISO VIEW 專家小組成員簡介

CISO View 專家小組 – 來自全球 1000 家公司的高階安全主管

Rob Bening

首席資訊安全長，荷蘭商業銀行（ING Bank）

Rob Bening 是荷蘭商業銀行的 CISO。他此前擔任首席技術架構師兼集團首席技術長，負責制定集團 IT 標準及一些全球標準化計劃。Rob 的上一項工作是建置運營及 IT 銀行板塊的架構功能、領導基礎設施架構及工程團隊。自 1985 年以來，Rob 在 ING 的 HR、稽核、安全、基礎設施及架構部門擔任了多項職務。

David Bruyea

資深副總裁兼首席資訊安全長，CIBC

David Bruyea 負責 CIBC 的資訊安全智慧、策略、政策、標準、風險評估、架構及專案管理。依據企業架構，David 的職責包括在制定及實施 IT 相關計畫時提供技術願景及領導能力。David 擁有超過 25 年的工作經驗，還在 CIBC 的技術與運營部門擔任過各種技術、諮詢及管理職位。

Dawn Cappelli

副總裁兼首席資訊安全長，羅克韋爾自動化公司（Rockwell Automation）

Dawn Cappelli 負責全球資訊安全專案，確保羅克韋爾產品及基礎設施的安全。Dawn 的團隊與各個業務部門、IT 及各事業主管密切合作，採用基於風險的方法來執行資訊安全性原則。此前，Dawn 是卡內基梅隆大學 CERT 內部威脅中心創始人兼董事，並且是 CERT 內部威脅指南的共同作者。Dawn 還曾在西屋公司負責開發軟體。Dawn 是 RSA 大會專案委員會及國內安全聯盟委員會（DSAC）的成員。

Jim Connelly

副總裁兼首席資訊安全長，洛克希德馬丁公司（Lockheed Martin）

Jim Connelly 負責洛克希德馬丁公司全球運算環境的整體資訊安全策略、政策、安全工程、運營以及網路威脅偵測及回應。Jim 擁有超過 25 年的工作經驗，負責監督洛克希德馬丁的智慧驅動防禦運營，並領導著業界知名網路安全專家團隊，該團隊負責管理公司的端到端安全基礎設施，防範 APT，並推動與洛克希德馬丁公司合作夥伴的開放式協作及資訊共用。

Dave Estlick - CISSP、CSSLP、CISA、CISM、CIPP

資深副總裁兼首席資訊安全長，星巴克

Dave Estlick 負責資訊保護及全球網路安全，包括運營、工程、架構、身份識別及存取管理，以及 IT 風險及合規。此前，Dave 負責管理星巴克的全球技術基礎設施。Dave 負責制定技術標準化、基礎設施聚合策略並實施相關專案，以及建立星巴克私有雲端。在星巴克任職之前，Dave 在 PetSmart 及亞馬遜擔任安全主管，管理 ePods 及 Icebox 的基礎設施服務，並曾在 Sun Microsystems 及波音公司（Boeing）擔任關鍵技術職務。

Steve Glynn

首席資訊安全長，澳新銀行集團有限公司

Steve Glynn 是澳新銀行的資訊安全及技術保證主管。Steve 負責制定關於人、支持、信任及社群的資訊安全策略，確保協助澳新銀行在全球 34 個市場中防範日新月異的網路威脅。Steve 擁有約 20 年的工作經驗。在來澳新銀行工作之前，Steve 在澳大利亞及新加坡的荷蘭銀行及蘇格蘭皇家銀行擔任過各種資深資訊安全、技術風險及技術領導職位。

CISO View 專家小組 – 來自全球 1000 家公司的高階安全主管（續）

Mark Grant 博士，CIPP

首席資訊安全長，CSX 公司

Mark Grant 負責確保 CSX 資訊資源的機密性、完整性及可用性。Mark 的職責包括整個 IT 環境的網路安全、存取控制、公司災難復原，以及制定企業架構的角色及願景。Mark 是鐵路資訊安全委員會的成員，也是眾多安全工作組的成員。自加入 CSX 以來，Mark 曾擔任過一些關鍵職位，負責 IT 服務規劃、交付及可靠性。

Gary Harbison

首席資訊安全長，孟山都公司（Monsanto Company ）

Gary Harbison 是孟山都的資訊安全辦公室主管，主要負責管理全球風險及網路威脅，為公司導入實用性安全解決方案。此前，Gary 主要在資訊安全領網域任職，負責技術、架構及策略制定，並在多家全球財富前 500 大公司及國防部擔任過領導職務。Gary 是華盛頓大學網路安全碩士課程的兼職教授。

Kathy Orner

副總裁兼首席資訊安全長，嘉信力旅運公司（Carlson Wagonlit Travel ）

Kathy Orner 負責資訊安全治理、風險與合規、安全運營與工程、實體安全，以及 IT 合規與審查。此前，Kathy 是嘉信力企業服務副總裁兼 CISO。她擁有豐富的 IT 管理經驗，包括在明尼蘇達州的聯合健康集團與藍十字與藍盾協會擔任 CISO 一職。當前，Kathy 是支付卡業（PCI）組織諮詢委員會成員。

Chun Meng Tee

副總裁兼資訊安全主管，新加坡證券交易所

作為新加坡證券交易所（SGX）的安全資訊主管，Chun Meng Tee 負責交易所資訊安全專案的功能與運營。來 SGX 任職之前，Chun Meng 在安永會計師事務所資訊安全部門工作，主要為金融機構及政府機關提供諮詢服務。此外，Chun Men 還曾在公共部門任職，擔任國防部及新加坡員警部隊資訊安全主管，負責資訊安全。

Munawar Valiji

資訊安全主管，英國新聞集團

Munawar Valiji 是新聞集團的地區 CISO，負責新聞集團、道鐘斯公司、華爾街日報及柯林斯出版集團在英國及 EMEA 的安全策略 ,包括設計、建構及維護高度安全且可輕鬆維護的安全平台。此前，Munawar 是金融時報的資訊安全主管。Munawar 擁有豐富的資訊安全從業經驗，包括在莫爾斯電腦、德勤、花旗銀行、摩根大通、澳大利亞國家銀行及 Sun Microsystems 擔任諮詢、技術及資深管理職位。

Mike Wilson

資深副總裁兼首席資訊安全長，麥克森公司（McKesson）

Mike Wilson 負責安全及 IT 風險管理。Mike 的 IT 及風險管理從業經驗跨越多個地理區網域及產業，包括金融服務、醫療保健、日用消費品及物流。來麥克森工作之前，Mike 在一家全球專業服務組織任職。當前，Mike 為思想領袖及產業組織提供支援，包括 NH-ISAC、雲端安

客座撰稿人簡歷

在資料外洩之後與大型企業合作的技術專家及顧問

John Gelinne

網路風險諮詢服務部門總經理， 德勤會計師事務所（Deloitte & Touche）

John Gelinne 負責德勤的彈性運營，協助各個部門預防、回應網路事故並從事故中復原。John 負責網路安全及實現技術彈性，協助各部門快速適應並回應動態變化、中斷及威脅。John 曾在美國海軍工作 30 年，退休之後，John 在保護海軍網路，防範複雜網路威脅方面發揮關鍵作用。John 擁有資訊系統管理及國家安全高等學位以及工程學本科學位。

Gerrit Lansing，CISSP

首席架構師，CyberArk

最近，Gerrit Lansing 成為 CyberArk 的首席架構師。此前，Gerrit 負責 CyberArk 的諮詢服務，包括策略指導、架構及大型專案服務團隊。Gerrit 曾為許多全球大型企業（包括幾家財富 10 強企業）提供諮詢服務。Gerrit 是安全防護控制措施設計領網域的專家，並會在發生嚴重資料外洩後與相關企業合作。來 CyberArk 工作之前，Gerrit 是一家大型保險公司的資訊安全分析師，負責系統安全、取證、事故回應及調查。

大型企業中經歷過嚴重資料外洩事故的安全主管

由於法律限制，這些高階主管在為本研究報告撰稿時並未署名。

關於 CISO VIEW 業界計畫

由於企業面臨的複雜網路威脅日益嚴峻，共用有關最佳安全實踐的資訊愈來愈重要。CyberArk 認為，如果安全團隊能夠從 CISO 社群的領導智慧中汲取靈感，這將有助於強化安全性原則，為企業提供更全面的保護。因此，CyberArk 委託獨立研究公司 Robinson Insight 推動一業界計畫，就如何加強特殊權限存取控制相關的主題徵詢 CISO 的意見。此項計畫彙聚眾多知名 CISO，他們就安全從業者當前面臨的問題分享自己的觀點。透過發佈 CISO 報告，展開研究以及召開圓桌會議，本計畫提供寶貴的同行指導，進行有益的對話。有關此計畫的詳細資訊，請瀏覽 www.cyberark.com/cisoview。

CyberArk（NASDAQ：CYBR）是一家提供特殊權限帳號安全解決方案的全球性公司。有關 CyberArk 的詳細資訊，請瀏覽 www.cyberark.com。

Robinson Insight 是一家致力於推進 CISO 計畫的行業分析公司。有關詳細資訊，請瀏覽：www.robinsoninsight.com。