CYBERARK®

白皮書

CYBERARK 身份安全成功藍圖快速降低風險教戰手冊

www.cyberark.com

目錄表

總結

在現今的混合雲端及多雲世界裡，身份已成新邊界。實體和網路邊界消融瓦解，所有身份都可能成為攻擊途徑，侵害組織最寶貴的資產。企業必須加強身份安全來降低風險，但對於許多組織來說，實施有效的身份安全計劃（找出弱點、評估潛在風險、引入新的安全控制）可能是一項艱鉅的任務。

CyberArk 身份安全成功藍圖經專門設計，協助企業借助實證有效的措施有系統、高效率地改善其安全態勢並降低風險。CyberArk 藍圖快速降低風險教戰手冊可幫助組織快速實施 CyberArk 藍圖最關鍵的元素，以快速強化安全性並降低風險。本白皮書審視 CyberArk 藍圖並解釋快速降低風險教戰手冊如何幫助您快速啟動實施身份安全措施及加快降低風險。

CyberArk 藍圖協助降低身份安全風險

身份安全是現今資訊技術及安全主管的核心要務。外部攻擊者及惡意內部人員可擅自佔用存取特權帳號並橫行於網路，以竊取機密資訊、破壞關鍵系統和應用程式並損害業務。Verizon 的 2020 年資料外洩報告顯示，超過 80% 的資料外洩事件與強力破解或憑證遺失或被竊取有關。[1]

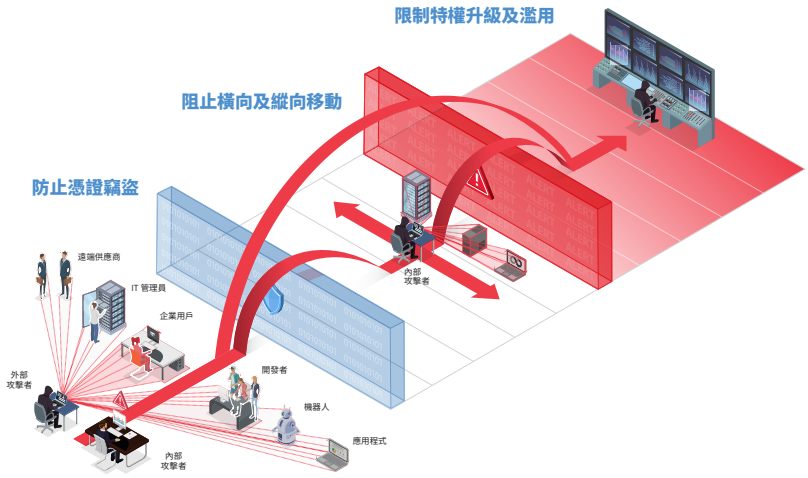
CyberArk 開發出一套指示性藍圖，可幫助企業建構及維護一個有效強化身份安全性的計劃。CyberArk 身份安全成功藍圖的設計專門針對滲透者竊取資料及破壞系統的三種常見手法進行防禦。遵循「像攻擊者一樣思考」的做法，制定按優先順序、分階段執行的計劃，其中所採取的行動均與可能降低的對應風險緊密相扣。

雖然每個組織的 IT 環境各有不同，但攻擊者可透過下列方式攻擊幾乎任何業務：1) 未經授權擅自獲取存取特權帳號憑證，2) 遍訪網路尋找高價值目標，以及 3) 使用升級的特權竊取機密資訊或干擾服務。

依此考量，CyberArk 藍圖以三項指導原則為主軸：

1. 防止憑證竊盜
2. 阻止橫向及縱向移動
3. 限制特權升級及濫用

[1] The Forrester Wave™：特權身份管理，2018 年第四季



CyberArk 藍圖的三項指導原則

CyberArk 藍圖快速降低風險教戰手冊瞄準最大風險

CyberArk 藍圖快速降低風險教戰手冊著重於 CyberArk 身份安全成功藍圖計劃的最高優先元素，協助您在最短的時間內解決最緊迫的需求。隨後，您可以針對較不迫切的用例實施 CyberArk 藍圖的更多元素。

本教戰手冊遵循 NIST 電腦安全事故處理指南內的美國國家標準暨技術研究院、ENISA 事故管理最佳實踐刊物內的歐盟網路與資訊安全局及 ACSC 網路安全事故減緩策略的澳洲網路安全中心等主要監管機構所推薦的最佳事故回應實踐程序。例如，此教戰手冊可對應 NIST 事故回應生命週期的準備、偵測與分析及遏制、根除與復原等階段，如下圖所示。

資料來源：NIST 特別刊物 800-61 修訂版 2

本教戰手冊透過主動保護最常受到攻擊的身份與特權帳號的存取權，協助您做好更周全的準備。此外，還可透過分析特權連線活動，幫助您識別被侵用的帳號、隔離攻擊者及制訂修正措施。舉個例子，假設現在有個特權帳號被用來發起攻擊。如果該帳號已被加密保管，您將可確定有權存取該帳號者以及他們存取的系統，並利用該資訊減緩攻擊。如果該帳號未獲保管，您可檢查整個企業內的相似帳號，以偵測及隔離潛在的安全漏洞。您還可以擴充身份安全計劃的範圍，保護面臨危險的帳號。

本教戰手冊可幫助您應對事件回應生命週期的遏制、根除與復原階段。一旦確定被侵用的帳號及/或特權之後，便可利用一次性密碼和專屬帳號選項將它們加密保管。這可防止憑證被攻擊者利用，使其進一步的企圖得逞。

您也可以移除攻擊者在事故中使用的組件，應對事件回應生命週期的遏制、根除與復原階段。例如您可停用或刪除遭受侵用的帳號、對關鍵系統採取代理伺服器式存取，以及將特權帳號監控擴大至整個企業。

CyberArk 藍圖提出一個按照優先順序執行的五階段式安全計劃框架，排出與降低風險潛能相對應的計劃里程碑。教戰手冊則側重於藍圖的前三個階段，針對最常成為目標、因此潛在風險最高的帳號，見下表所示。教戰手冊依循藍圖的指導原則，幫助防止憑證竊盜、阻止橫向及縱向移動並限制特權升級。

CyberArk 藍圖第 1-3 階段及教戰手冊目標

		身份安全控制工具及技術			
	目標	存取	最小特權	特權存取	金鑰管理
第 1 階段	保護擁有控制整個環境潛力的最高特權身份	金鑰管理	雲端管理員及影子管理員	雲端管理員、網域管理員、虛擬機器管理員及 Windows 本機管理員	第三方安全工具（透過 C3 聯盟）及 Windows 服務（網域管理員權限）
第 2 階段	集中於鎖定最通用的技術平台	PaaS 管理員、雲端特權實體及 CI/CD 主控台管理員	雲端特權實體	工作站本機管理員、特權 AD 用戶、*NIX 根目錄 + SSH 密鑰	第三方商業工具（透過 C3 聯盟）及第三方應用程式伺服器
第 3 階段	將身份安全整合至企業安全策略及應用程式流程的架構	Web 應用程式（任務關鍵）	IT 管理員工作站	*NIX 根目錄（類似）、頻外存取、資料庫內建管理員	CI/CD 工具鏈流程及動態應用程式（容器和微服務）

本教戰手冊旨在儘快實施最關鍵的安全控制。許多組織可在 30 至 60 天內執行教戰手冊。有些需要更長時間。在實務應用中，教戰手冊所需時間取決於組織的規模、複雜性、成熟度、文化及迫切感。往往在發生資料外洩之後或企業領導者迫切想要增強其安全系統的情況下，公司會將人事紛爭擱置一旁、拋開繁文縟節並加快推行安全計劃，一些後期階段的藍圖建議便可納入教戰手冊的目標中。

教戰手冊第一階段 – 保護高價值目標

教戰手冊的第一階段著重於保護企業中潛在風險最大的高價值目標。識別及保護任何可能被利用來控制整個環境的身份及其相關特權存取，例如網域管理員和雲端管理員帳號。透過隔離特權連線、加密保管及輪換密碼、採用自適應多重要素驗證及智慧化監控及分析特權連線活動，防止未經授權存取並降低風險。透過在地端及雲端環境內儲存和轉換密碼及隔離 Windows Server 本機管理員帳號，阻止橫向及縱向移動。對雲端 IaaS 管理員帳號應用自適應多重要素驗證及單一登入，並對這些 IaaS 管理員及影子管理員應用最小特權控制。

教戰手冊第二階段 – 鎖定最常用的技術平台

在第二階段內，鎖定最常部署的技術平台。透過加密保管及轉換密碼以及隔離特權連線，保護用來管理伺服器和工作站的特權地端、雲端代管及雲端聯合 Active Directory 帳號。

教戰手冊第三階段 – 將身份安全納入企業安全策略

在第三階段內，為工作站、筆記型電腦、桌上型電腦及虛擬桌面實例（VDI）實行作業系統層級的最小特權存取控制，以降低特權升級風險。終端特權管理解決方案藉由刪除終端上的本機管理權限及根據政策嚴密控制用戶和應用程式權限，協助您限制風險曝露。您可透過執行最小特權原則（授予用戶執行其工作所需的最小特權組合），防止縱向移動並改善您的安全態勢。設置應用程式控制來預防勒索軟體和其他惡意軟體及限制未經批准的應用程式運作，可降低風險及不確定因素。

確保成功

實施全企業、全面性的身份安全計劃必須長期奮戰，無法一蹴而就。教戰手冊是您整個身份安全旅程中至關重要的第一步。為確保成功，您必須為快速降低風險計劃準備妥當，並在執行教戰手冊之後繼續擴大您的防禦廣度及深度。

此外也應記住，CyberArk 藍圖是為了防禦對企業構成最高風險的最常見威脅而建構的。每個客戶都有各自不同的情況。如果您為了回應網路攻擊而執行教戰手冊，您可能需要調整及重新排定優先任務，以因應您的特定情況。例如，若您偵測到一個通用技術平台上的特權憑證（例如工作站上的本機管理員帳號）已被侵佔，您可能需要隔離、加密保管及輪換這些憑證，同時對所有本機管理工作站實行最小特權原則。

您需要逐步完整實施 CyberArk 藍圖的所有五個階段，以實現終極安全性。

執行教戰手冊之前

在執行教戰手冊之前應提前規劃，以確認利益相關者、專案團隊成員以及計劃所需的硬體和軟體資源。建立一個專案計劃，定義您計劃實施的特定身份安全控制及技術。定義成功的標準，以及您評估進度及衡量成果將使用的工具和方法。

完成教戰手冊時

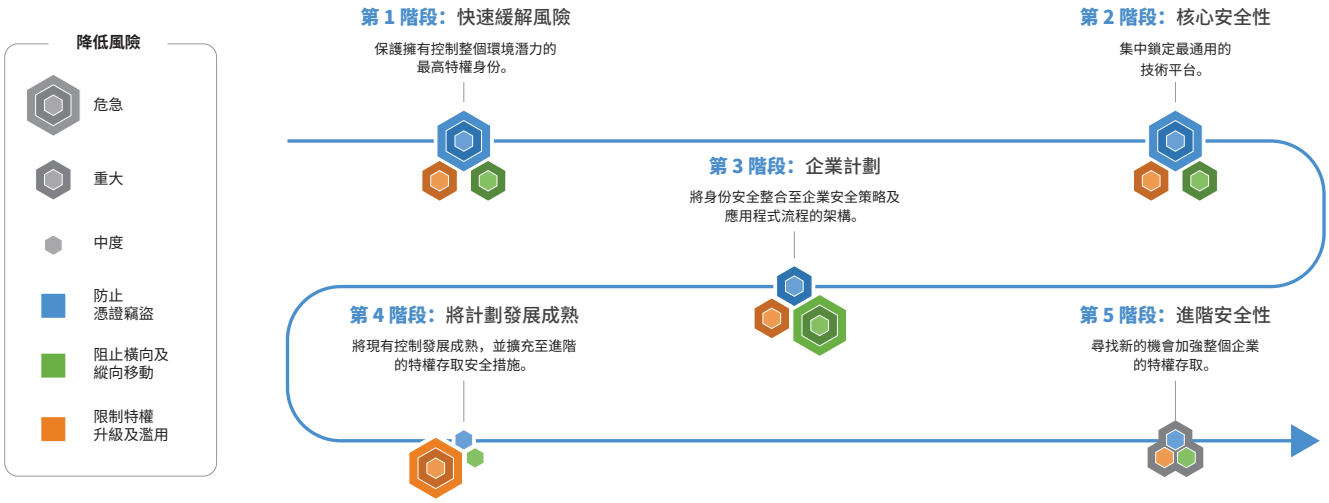
執行教戰手冊之後，應進行事後檢討。確認哪些環節順利進行，哪些流程日後需要改進。使用您的經驗心得，建立持續性的特權存取安全系統及實踐程序。制定一個定期執行身份安全增強的正式計劃，以提高防禦的深度及廣度。

為高階主管及企業領導者制定總結報告，解釋教戰手冊將如何幫助公司提高網路安全性並降低風險。描述進一步增強安全性所需的其他措施及投資。以具意義且相關的詞語說明風險，例如業務停擺、收益損失或監管機構罰款。

執行教戰手冊之後

鼓勵 CyberArk 客戶安排一次藍圖會議，在設計和建構在整個組織內擴展身份安全控制的路線圖方面獲取更多支援。在解決藍圖框架內最關鍵且時間最緊迫的問題後，您可以擴大身份安全計劃的範圍。首先，實施藍圖第 1-3 階段設定的控制及技術，如下表所示。如下圖所示，繼續逐步建立框架的第 4 階段和第 5 階段，強化您的安全態勢。

持續評估您的網路安全計劃之有效性，並在必要時進行調整。執行滲透測試或紅隊 - 藍隊練習，測試您的防禦力。利用網路掃描工具識別弱點並改善您的安全態勢。適當時修訂計劃並重新排定安全措施的優先順序。



教戰手冊後的活動

		身份安全控制工具及技術			
	目標	身份存取管理	最小特權管理	特權存取管理	應用程式金鑰管理
第 1 階段	保護擁有控制整個環境潛力的最高特權身份	自適應 MFA 及雲端管理員	雲端管理員及影子管理員	雲端管理員、網域管理員、虛擬機器管理員及 Windows 本機管理員	第三方安全工具（透過 C3 聯盟）及 Windows 服務（網域管理員權限）
第 2 階段	集中於鎖定最通用的技術平台	PaaS 管理員、雲端特權實體及 CI/CD 主控台管理員	雲端特權實體	工作站本機管理員、特權 AD 用戶、*NIX 根目錄 + SSH 密鑰	第三方商業工具（透過 C3 聯盟）及第三方應用程式伺服器
第 3 階段	將身份安全整合至企業安全策略及應用程式流程的架構	Web 應用程式（任務關鍵）	IT 管理員工作站	*NIX 根目錄（類似）、頻外存取、資料庫內建管理員	CI/CD 工具鏈流程及動態應用程式（容器和微服務）
第 4 階段	將現有控制發展成熟，並擴充至進階身份安全控制	Web 應用程式（核心）	工作團隊工作站及 Windows 伺服器	網路及基礎設施管理員、資料庫具名管理員、業務應用程式（任務關鍵）	靜態應用程式（自家舊版及作業系統為架構）
第 5 階段	尋找新的機會增強整個企業的特權存取。	Web 應用程式（所有）	*NIX 伺服器	大型主機管理員及業務應用程式（所有）	Windows 服務（所有嵌入式使用）

結論

實體和網路邊界消融瓦解，所有身份都可能成為攻擊途徑，侵害組織最寶貴的資產。CyberArk 藍圖快速降低風險教戰手冊可幫助您儘快識別及減輕對組織造成最大潛在風險的特權存取安全缺漏。依循 CyberArk 藍圖建議及指南的教戰手冊可協助您快速緩解惡意攻擊、資料外洩或其他緊急安全事件。

為何選擇 CyberArk?

CyberArk 藍圖展現出 CyberArk 在全球銷售、銷售工程、安全服務及客戶成功組織方面的全方位知識與經驗。作為特權存取管理領域無可置疑的領導者，CyberArk 具備獨有的優勢，為企業組織提供全面且有效的身份安全藍圖：

- CyberArk 解決方案深受金融服務、保險、製造、醫療及科技等眾多產業的 6,300 多家客戶信賴，其中包括半數以上的財星 500 大企業。
- CyberArk 的補救及紅隊服務始終扮演核心角色，協助企業從 21 世紀最重大資料外洩事件中復原。此外，CyberArk 還提供業界唯一的威脅研究與創新實驗室。
- CyberArk 安全服務、客戶成功及 PAS 計劃辦公室組織擁有數十年的實務操作及支援經驗，且切身瞭解身份安全風險及最佳實踐做法的各個方面。
- 領先的研究與顧問公司認可 CyberArk 為一家兼具願景規劃完整性與執行能力的身份安全領導者。

關於 CyberArk

CyberArk（NASDAQ: CYBR）是身份安全市場的全球領導者。CyberArk 以特權存取管理為核心，為商業應用、分散式工作、混合雲端負載以至整個開發維運流程中的人類和機器在內的任何身份，提供最為全面的安全產品。全球領先的企業組織信賴 CyberArk 協助保護其最重要的資產。欲瞭解有關 CyberArk 的更多資訊，請瀏覽 www.cyberark.com。