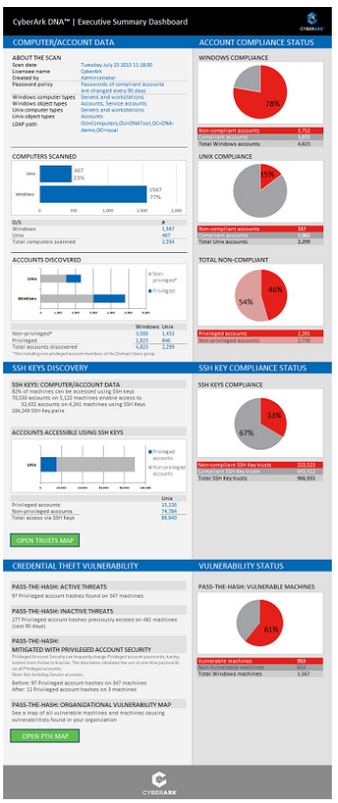
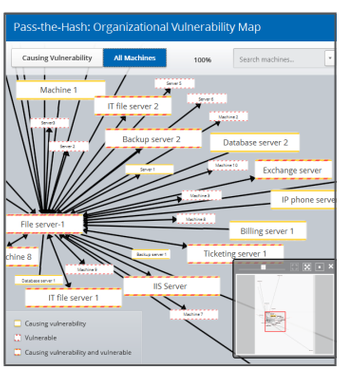
發現與稽核
(CyberArk DNA™)

用CyberArk DNA™掃描你的網路:

- 發現特權帳號在哪裡
- 明確評估特權帳號安全風險
- 辨識所有特權密碼、SSH金鑰、和密碼散列
- 蒐集可靠和全面的稽核資訊



綜合管理儀表板(Dashboard)樣本



密碼散列和SSH金鑰信任關係以視覺化分佈圖強化可見度

挑戰

特權帳號是通往公司最重要數據資料的途徑，因此會受到大多數先進的和來自內部的攻擊。管理特權帳號並確保其安全的第一步，是要獲得相關風險的可見度，包括：

特權帳號數量 — 通常特權帳號的數量是組織員工數量的三到四倍之多。
這些帳號存在於組織的每一個硬體和軟體之中，如資訊系統管理員或超級用戶帳號、腳本和應用程式帳號、特定商業用戶帳號、和企業社群網路帳號。特權帳號的可觀數量代表組織有嚴重的安全弱點。

特權憑證狀態 — 特權帳號的安全與否取決於可存取這些強大帳號的特權憑證狀態(強度、帳齡等)。 為了實施安全措施，組織經常設定憑證管理政策，諸如每90天輪調密碼。過期、靜態且不符合此政策的憑證會有較大的被攻擊風險。特權憑證具有不同的形式，包括：

- **密碼** — 老舊和靜態的密碼會導致嚴重的憑證風險。特別是針對組織中最具關鍵性的帳號，許多合規性規定建議經常性的輪調密碼。
- **SSH金鑰** — 這些金鑰儲存於網路各處，對資安團隊構成重大挑戰，因為這些特權憑證能夠很容易被建立卻沒有任何紀錄，所以很難追蹤、管理或控制。
- **密碼散列** — 密碼經常被作業系統雜湊處理成散列，並儲存於本機電腦以方便使用，但駭客攻擊，例如傳遞雜湊，會大量利用這些密碼散列的弱點以便執行憑證竊取攻擊、假扮員工帳號、以及存取重要資產和數據資料。

發現、積核並了解網路中特權帳號及憑證的弱點有助於處理下列特定的難題：

安全及風險管理:
對風險沒有全面性的了解，資安和資訊團隊就沒有足夠的資訊以減輕特權帳號的相關風險。

稽核與合規性:
當組織對其特權帳號環境缺乏清晰可見度時，因為缺乏符合規定所需的可靠資訊，就可能不知不覺地違反內部政策而造成無法通過定期稽核審查的結果。

專案策劃:
組織一旦專注於確保特權帳號安全，若缺乏清晰檢視問題點的能力，則難以規劃用於執行解決方案的相關預算評估和所需資源。

解決方案

CyberArk Discovery & Audit™正在申請專利，這是獨立且容易使用的工具，可揭露特權帳號全挑戰的嚴重性。此解決方案針對組織特權帳安號環境，提供全面性的檢視，包括：

- 在網路中的所有特權帳號
- 特權密碼及其目前狀態
- 整個組織的SSH金鑰組和單獨金鑰，及其相關狀態，包括帳齡、加密特性、合規狀態、和信任關係
- 特權帳號對傳遞雜湊攻擊的弱點、它們在網路中的位置、以及所有可能的攻擊途徑。

發現與稽核

執行DNA掃描是直接了當的自動化作業，無需在本機或目標系統安裝任何代理伺服器，且消耗非常低的頻寬。有了此一快速，方便的評估工具，IT和資安管理員可針對每一個特權帳號，獲取詳細的數量、狀態和弱點的詳細資訊，全部都顯示在直覺式的使用者介面上。

CyberArk DNA回應了下列問題:

- 特權帳號存在於哪些網路伺服器上?
- 哪些帳號有特權升級?
- 環境中存有多少SSH金鑰和單獨金鑰?
- 網路上的哪些機器和帳號可用SSH金鑰存取? 是從哪裡存取?
- 哪些特權帳號不符合公司的政策? (如: 超過90天未變更密碼)
- 是否有外部承包商或第三方在伺服器上增加特權帳號?
- 是否有已除役的產品存有"後門"帳號?
- 網路上有多少設備和哪些設備易受到傳遞雜湊的攻擊?

特點

CyberArk DNA 所提供的主要功能包括:

- **易於使用，非侵入式的掃描** — 直接了當的三步驟程序，掃描工作站和伺服器上整個目錄的特權、共用和一般帳號，且無需在網路上安裝任何東西。
- **詳細的報告** — 針對所有的特權帳號、密碼、SSH金鑰和傳遞雜湊弱點，及其各項狀態，以單一版本提供詳細的報告。
- **以圖形顯示結果** — 以綜合管理儀表板清晰、簡潔地顯示特權帳號風險及合規性狀態。
- **傳遞雜湊弱點分佈圖** — 以清晰圖表顯示儲存特權密碼散列的網路設備，顯示攻擊者如何利用傳遞雜湊攻擊在網路中流竄並到達目標設備。
- **SSH金鑰信任分佈圖** — 以視覺化顯示所有的SSH金鑰(包括單獨的SSH金鑰)，說明提供對特權帳號作存取的信任關係。
- **針對性警報** — 具標記與警示的稽核報告，顯示特權帳號的不當管理、不符政策的密碼 、單獨SSH金鑰、以及傳遞雜湊弱點等相關問題。
- **對運作方面影響最小的強大掃描能力** — 多線程(執行緒)應用的設計，加速掃描，低消耗網路頻寬，且在活動目錄(Active Directory)網域控制站和目標設備上使用非主要的網路和CPU資源。所有的掃描都在唯讀模式下執行，不會在環境中造成任何變動。

優點

發現每一個特權帳號及其狀態以辨識風險程度
快速精確的報告，顯示特權帳號的數量和狀態，使組織能夠立即指認出未知的或不當管理的特權帳號，並快速採取行動以處理相關問題。

了解面對特定網路安全威脅的弱點
特權密碼散列的辨識可提供對傳遞雜湊弱點的深入觀察，並改進其降低風險計畫和執行。

節省珍貴的稽核準備時間和成本
針對特權帳號的狀態，稽核人員可獲得可靠、密切相關的全面性檢視，以祛除複雜的配圖和人工作業去檢視這些通常難以蒐集且費時的相關資訊。

獲得對特權帳戶的問題和解決方案的可見度
獲取對特權帳號的清晰可靠檢視，可以更瞭解問題點所在，並得以針對解決方案的規劃、預算編制和佈署，進行更佳的操作。

實施全面的解決方案
CyberArk為業界領先的特權帳號安全解決方案，針對特權帳號的管制、監控、管理和情資，提供全面的解決方案。這個點對點的解決方案以關鍵性稽核功能為出發點，可找出在網路上所有的特權帳號。

規格

CyberArk DNA™ 可於下列平台執行:

- Windows 7

針對所有的作業平台，提供32位元和64位元版本。

支援下列目標系統

Windows工作站:
- Windows 2000
- Windows XP
- Windows Vista
- Windows 7
- Windows 8

Windows 伺服器:
- Windows 2000
- Windows 2003
- Windows 2008
- Windows 2012

Unix:
- RHEL 4-6
- Solaris Intel 10
- SUSE
- Fedora
- Oracle
- CentOS

網路協定

Windows:
- Windows File and Print Sharing
- Windows (WMI)

Unix:
- SSH
- SFTP

掃描的樣本資料
- Windows 和 Unix 帳號
- 網域帳號
- 本地帳號
- Windows 服務帳號:
- Windows 服務
- 已排程的任務