imperva中央集中管理及報表軟體

功能與特性

- 提供統一介面，集中管理所有iMPERVA之系統軟體。
- 提供 CLI (Command Line Interface)、SSH命令列管理介面與 Web管理介面。
- 支援多重管理者機制，可以依據不同的管理者角色給予不同的權限及管理設備範圍。
- 須提供事件管理中心介面，讓管理者查詢即時監控之訊息，並提供篩選功能，定義呈現之範圍及條件。
- 提供告警事件收斂彙整管理技術，將類似之事件集中為一項，以減少管理者之負擔。
- 系統告警(Alert)資訊可透過email、SNMP、OS Command及Syslog等機制通知相關管理者或第三方系統。
- Web管理介面需以HTTPS方式加密連線。
- 可集中管理所有被監控目標之設定、政策、報表，並可自動派送至各個iMPERVA監控防禦系統。
- 須提供管理者作業之工作稽核記錄(System Event)，包括管理者登入/登出、修改設定、產製/修改報表等工作記錄，且管理者本身無法對此記錄做任何修改。為安全考量，須提供密碼強度限制的相關設定，如密碼長度、是否需大小寫混合、有效期限…等。
- 所有log及稽核資料須能備份匯出，並可支援多種匯出方式：SAN、FTP、HTTP file transfer、NFS、Mount file system、SCP…etc.。匯出的資料須提供加密或驗證技術。
- 需提供NTP校時功能，可與上層時間伺服器對時，確保事件時間準確性。
- 具備特徵碼更新機制，可立即生效不影響系統運作，並可派送至各個iMPERVA監控防禦系統。
- 具備自動隱藏或移除告警、報表中敏感性資料之功能，使用者可自訂敏感性資料欄位或物件。
- 系統需具備服務探勘功能，以使管理者知道目前於單位網路環境中有多少網站及資料庫在提供服務，掃描結果須包括IP、Port、作業系統等資訊。
- 需提供原廠更新（可設定排程每日、每週或每月執行）特徵碼機制，無需手動介入操作即可自動更新。
- 需可提供手動更新機制，以免因內部資安政策考量無法連網時，可手動更新特徵碼。
- 原廠提供更新之內容，包括政策定義、特徵碼、報表範本、資料庫弱點掃描項目。
- 須內建報表系統，所有報表產出都可在設備內獨立完成，不需另行匯出資料至其他的報表模組以產生報表。
- 可依使用者需求自行調整報表格式（可自行新增或刪除顯示於報表之欄位及設定報表產出之條件），可調整欄位顯示順序，並可設定第一排序(sorting)欄位及第二排序欄位，以產出符合使用者需求之報表。

加值經銷商

iMPERVA台灣區代理商
CipherTech
TRUST&SECURITY
亞利安科技有限公司
台北市內湖區11449港華街85巷15號1樓
TEL: +886-2-2799-2800
FAX: +886-2-2799-8196
http://www.ciphertech.com.tw