資料庫監控暨紀錄軟體100M
資料庫防火牆軟體100M

功能與特性

- 可以網路方式收集資料庫活動資料或完全以agent收集資料庫活動資料。
- 不須取得資料庫帳號即可進行資料庫稽核，並產生連線稽核紀錄。
- 系統須支援異質資料庫環境，可同時監控分析不同類型之資料庫系統，並提供分析報表功能；系統須支援Oracle、Sybase、Microsoft SQL Server、IBM DB2、Informix、MySQL、PostgreSQL、Netezza、Progress、Teradata等資料庫系統。
- 需可紀錄資料庫傳回前台應用程式的資料(Response Data)。
- 具備資料庫使用行為自動學習功能，自動學習存取資料庫的帳號、存取之database、存取之資料表(table)、存取之操作(operations)、存取之來源IP(Source IP)、由何應用程式(Source Application)存取Database等，以建立資料庫正向使用行為模型。
- 資料庫稽核資訊須包括來源IP(Source IP)、目的IP(Destination IP)、存取DB的user帳號、該次事件發生之時間、被存取之物件(Object)、Sql Query、回應筆數、回應時間、被影響筆數等資訊，並可自訂顯示於稽核瀏覽頁面的欄位資訊。
- 需具備可記錄資料庫回應前台應用程式query的資料之回應資料，並可設定存取哪些資料表(table)或欄位(cloumn)時才需記錄回應資料。
- 須提供敏感資訊資料遮罩功能，以防止敏感資訊於本設備管理介面或本系統之輸出文件以完全明碼方式呈現降低資料外洩之機會。
- 可支援排程將稽核資料備份匯出(Archive)。
- 可支援SAN外部光纖儲存網路、NFS、Mount File System、FTP、SCP等方式，排程將稽核資料備份匯出(Archive)，並且須支援加密與簽章功能。
- 為監控資料庫本機行為，本系統需具備可安裝於database server之agent，agent支援的作業系統平台包括AIX, HP-UX, Solaris, Linux,Windows, Z/OS, AS/400等。
- 系統須具備資料庫(Database)攻擊或入侵特徵（Signature），當偵測出具有攻擊或入侵特徵時系統可以發出告警，告警功能提供異常行為及完整過程訊息分析功能，包含來源IP、發生時間、目的端IP、事件描述(Alert Description)、事件內容（Details)等資訊，並可進行條件過濾(filter)。
- 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。
- 可阻斷異常存取行為。(資料庫防火牆軟體獨有功能)
- 系統需具備資料庫服務探勘功能，以使管理者知道目前於單位網路環境中有多少資料庫在提供服務，掃描結果須包括IP、Port、作業系統等資訊。
- 系統需具備資料庫弱點掃描功能，並於結果中建議弱點修補方式，以使資料庫無致命弱點，降低資料庫安全事件發生之機會。
- 設備需提供原廠更新特徵碼機制，無需手動介入操作即可自動更新（可設定排程每日、每週或每月執行）。

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