監測、檢測與分析用戶的威脅

漏洞越來越多的內部威脅 Insider Threats

對企業資料的內部攻擊與對企業造成的損失的數量持續呈指數級增長。 復原困難造成受害企業的負面影響，並影響深遠。在 2016 年近 70%的受訪企業遭受了內部的的敏感資料的竊取破壞。這些內部威脅包含了 員工與第三方承包商對公司基礎設施的存取、使用關鍵資料的用戶、本地與遠端管理員。 ** The State of Cybersecurity and Digital Trust, HfS research, 2016*

解決方案

Ekran 系統是用於公司資訊安全監控的高級軟體解決方案，可以支援 Windows、Mac、Linux、X Winodw 與 UNIX 平台以與虛擬化環境（如 Citrix），記錄並分析企業伺服器、終端機與 本地 PC 上的每個用戶的連線。

基於索引的錄影記錄格式，Ekran 系統捕獲任何用戶對企業端點的操作，從伺服器設定的更改到敏感資料的存取，為您提供探索和記錄任何事件所需的所有細節。

捕獲螢幕上的活動並透過多層日誌的詳細訊息建立索引，如應用程式名稱、Windows Title、輸入的 Linux 指令、URL 地址、鍵盤輸入與 連接的 USB 設備等詳細資訊，提供更快速的搜尋與深入的調查。

目標事件的即時警報與 rule-based 的 USB 設備管理可以即時地進行威脅檢測來幫助您的團隊因應事件。各種報告提高稽核能力，並允許交叉檢查。

如何運行

Ekran Client 安裝在伺服器或個人電腦上，記錄所有登錄用戶連線的影像與附帶的 metadata，如 應用程式名稱、Windows Title、輸入的 Linux 指令、URL 地址、鍵盤輸入與 連接的 USB 設備等詳細資訊。Ekran 可輕鬆搜尋 metadata 為所有連線記錄提供全功能播放。透過 Web 操作面板、即時警告，直接鏈接到對應的錄影並可主動阻斷使用 USB 設備。其他存取管理選項可為關鍵端點建立一個防線，並實現連線與個人用戶之間的單一連接。

具成本效益的任何部署

Ekran 系統是依照受監控的端點數量授權計費、並支援浮動授權 Floating licensing :點擊即可將端點之間授權轉移並支援商業的 MS SQL Server 與免費的 PostgreSQL 資料庫，是極具備成本效益部署。

協助遵循各種標準與法規的要求

使用 Ekran System® 可以協助您遵循如 HIPAA、NERC、FFIEC、FISMA、FERPA、PCI-DSS、SOX、SWIFT CSP 與 NYDFS(23 NYCRR Part 500)等標準與法規要求。

Ekran System

使用客戶遍及世界各地

特權用戶監控
Privileged user monitoring

錄影檔與資料庫使用 RSA 憑證的加密保護

支援 一次性密碼、二次登入身份認證與 雙因子認證 確認登入者為本人

發現、調查與預防所有可能的違規行為

透過可搜尋的錄影記錄監控用戶活動

使用 Ekran 系統您可以控制企業網路用戶的工作，包括本地與遠端系統管理員。Ekran 系統建立所有 本地、遠端與終端機連線的完整影像記錄。 使用 Ekran 系統沒有任何東西可以隱藏，每個用戶的螢幕將與活動細節將一起被捕獲。 該產品適用於任何網路協定、應用程式與架構。

特權帳號與連線管理 Privilege Account and Session Management (PASM)

當使用 Ekran System 企業版管理伺服器、Windows 跳板機 (Jump Box) Agent、Server Agent 並透過 Ekran System 遠端連線軟體連線時，可自動產生特權帳號密碼自動登入後方被保護的主機，並在設定時間後取消密碼。

分析監控結果 – 發現可疑的用戶行為

Ekran 系統使用易於分析的影像記錄（即使是用於 Linux 的 SSH 與 Telnet）的組合，也可搜尋代表活動細節的文本 text metadata。 在所有記錄中進行進階搜尋，是您執行追溯用戶操作分析和事件調查的有效工具。

能夠快速響應事件

Ekran 系統提供了一個 rule-based 的警報系統，在發生潛在的危險行為時通知您的安全人員。 發送包含與相關錄影檔的直接鏈接通知，可以進行快速事件調查。可選擇查看目前運行中的用戶連線、即時稽核用戶活動，當檢測到惡意行為時手動或自動可阻止用戶。

使用報告稽核用戶活動

使用 Ekran 系統，您可以產生各種報告，讓您可以在一段時間內分析用戶不同方面的活動。定期報告選項可確保所有必要的統計訊息直接傳遞到您的信箱。解決方案包括舉證 forensic 匯出能力，產生用戶連線相關的保護日誌，包括連線側錄影像、metadata 與嵌入的播放控制功能。

Deloitte. · UKRSIBBANK BNP PARIBAS GROUP · cfcapital · FERRERO · BANCO POPULAR · Bankia · cash converters · ups · Banco Santander · nationale nederlanden · Ubezpieczenia · renfe · BBVA · bankinter · REPUBLIC OF SLOVENIA STATISTICAL OFFICE · CHRISTIE'S

進一步 Ekran 產品資訊請洽 台灣地區代理商 商丞科技股份有限公司 (02) 2914-8001

Ekran System

可支援 單台 Ekran Server 的小型或多台 Ekran Server Cluster 的大型佈署

可透過關鍵字搜索直接播放資料庫內或歸檔的錄影檔

即時警報與行動可以自動啟動阻斷應用程式或強迫登出用戶之保護行動