opentext™ | Cybersecurity

資料表

ArcSight Logger

整合機器資料的收集、儲存與分析，提供安全情報。ArcSight Logger 是領先業界的資料收集解決方案，能隨著企業一同成長，解決網路安全性、合規以及 IT 營運記錄管理的需求。

產品焦點

在這個充斥網路安全威脅的時代，集中型的機器資料記錄檔也迅速成為重要的情報來源。如今，有效的記錄管理在取得精確資安分析中扮演重要角色。

ArcSight Logger by OpenText™ 是一套全方位的記錄管理解決方案，能整合並儲存整體企業的機器資料記錄，並協助快速搜尋和報告這些資料，進而減輕合規負擔，並加速安全專家的鑑識調查。ArcSight Logger 在 ArcSight 產品線的任務中扮演重要角色，提供強力的多層式分析功能，奠定安全作業的基礎。

ArcSight Logger 讓企業可收集逾 480 種來源的資料記錄檔，並以驚人且具成本效益的壓縮比將記錄長期儲存於整齊的正規化格式。ArcSight Logger 不僅能夠每天擷取並儲存百萬件 (甚至達數十億件) 的事件，更能幫助安全專家以高效率運用這些資料發掘異常狀況，並透過簡化的搜尋功能和自訂儀表板來迅速完成鑑識調查。

ArcSight Logger 內建各式內容、儀表板和報告功能，協助確保安全性合規不中斷。另外也提供內容套件，確保遵循 PCI、SOX、HIPAA 等法規。如此即可減輕稽核負擔，並且縮短為了證明符合特定法令規定而花費的時間。

整體而言，ArcSight Logger 提供企業一套解決方案來簡化資料收集、儲存、合規及搜尋。

主要優勢

全方位資料收集

ArcSight Logger 每日能從任何來源收集 TB 規模的機器資料，包括記錄檔、點擊記錄、感應器、網路串流流量、安全裝置、Web 伺服器、自訂應用程式、社群媒體和雲端服務等等。它讓您能搜尋、監控並分析這些資料，掌握整個公司的寶貴安全情報。

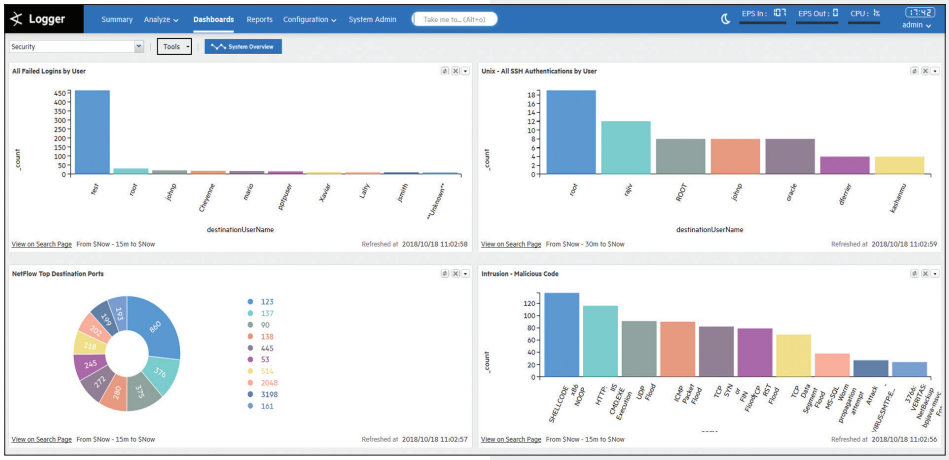

圖 1. ArcSight Logger 儀表板

ArcSight Logger 概覽

- 擷取偵測安全性漏洞所需的多樣、大量且高速流動的資料
- 按幾下滑鼠即可輕鬆架設、升級和維護系統
- 以符合成本效益的方式儲存並搜尋 TB 規模的資料，並提供快速的分散式同儕搜尋

彈性部署架構
ArcSight Logger 可叢集化架設，提供負載平衡的收集功能，並將搜尋查詢作業分散在整個平台上。它可以安裝於 Linux 系統和 VMware 虛擬機器 (VM)，可以裝置化，也能雲端架設 (AWS 和 Azure)。ArcSight Logger 可利用本地磁碟機或既有的 SAN 設備作為主要資料儲存。無論儲存裝置為內建或外接，都能有效壓縮資料以降低儲存和維護成本。

它採用的是 Common Event Format (CEF) 格式，一種可延伸的高效能文字格式，讓資料能輕易收集彙總供企業管理系統分析，如 ArcSight ESM by OpenText™、ArcSight Investigate by OpenText™ 和 ArcSght Interest UEBA by OpenText™，或是其他提供事件協調化、自動化、關連分析、優先順序安排、安全性事件分析或以上所有功能的第三方應用程式。

安全且可靠的資料收集
ArcSight Logger 軟體可提供加密並壓縮的記錄檔，保護資料預防攔截、修改和刪除，不論是靜態或傳送中的資料。ArcSight Logger 透過 Voltage SecureData Enterprise by OpenText™ 支援以下功能：

- 在 ArcSight Logger 裝置提供安全加密，讓機密的靜態資料 (儲存中的資料) 確實加密。同時也支援 TLS 和 SSL 加密協定以保護傳送中的資料。
- 安全性管理和使用者/群組角色定義。管理員可根據使用者角色和群組權限來設定報告及報告類別的存取權限。同時也能加密特定的資料欄，並可選擇性地授予解密權限。
- Voltage Format Preserving Encryption (FPE) by OpenText™ 能防止資料未經授權遭揭露。如此可保護靜態、傳送中及使用中的資料。
- 聯邦資訊處理標準 140-2 (FIPS 140-2)。

超快速調查與鑑識作業
攻擊成敗僅在數秒之間，因此能否及時取得正確的資訊相當關鍵。ArcSight Logger 提供簡單的搜尋介面能以超快速調查經編製索引的資料。有用的搜尋比對條件可輕易轉換為即時警示。

ArcSight Logger 還能利用機器學習的資料科學內容來加速調查作業。使用預先製作的內容，或使用 python 程序檔來開發專用的資料科學演算法。

ArcSight Logger 僅需不到 10 秒鐘就能搜尋累積多年達數十億筆事件的資料，讓您辨識侵害事件並執行詳細的入侵分析。

合規不中斷
ArcSight Logger 內建的內容可用於網路安全性、合規、應用程式安全性以及 IT 營運監控。同時並提供額外的合規內容套件，適用於 PCI、ITGOV、HIPAA、NERC 與沙賓法案 (Sarbanes-Oxley，SOX) 等規定，以附加產品選項的方式對應多種知名標準，包括美國國家標準技術局 (National Institute of Standards and Technology，NIST) 的 800-53 標準、ISO-17799 和 SANS。

容易部署與管理
ArcSight Logger 可透過 ArcSight 的集中式管理主控台 Management Center 進行設定、管理和監控作業，只要按幾下滑鼠就能輕易連結到資料。即使是大規模部署，也能輕鬆設定、管理和升級，讓您專心開發使用案例而不必煩惱操作工具。

主要功能

- 全方位資料收集
- 彈性部署架構
- 安全可靠
- 超快速搜尋與調查
- 合規不中斷
- 容易部署與管理
- 機器學習資料科學內容

為何選擇 ArcSight 產品線？
ArcSight SIEM by OpenText™ 平台不僅可擴充，更具強大功能。這是一套由安全專家為安全專家人員所開發的全方位解決方案。它採用全面性的安全情報思維，以獨特的方式整合巨量資料的收集、網路、使用者及末端監控與鑑識，搭配進階的安全性分析技術，包括搜尋、調查與 ArcSight Interset UEBA 解決方案。它提供即時威脅偵測與回應、合規自動化與保證以及 IT 營運情報，提供強大的多層式分析方法，實現企業自我防衛。

「ArcSight Logger 讓我們快速實現 PCI 合規，還幫助我們監控網路上的異常狀態，隨時掌握新興威脅。」

安全長
財星 500 大金融服務公司

與我們交流
www.opentext.com

市面上雖有多家廠商宣稱能提供可靠的 SIEM 解決方案，但是少有能與 ArcSight SIEM 團隊比擬的安全專業、經驗和領導地位。

我們的新一代解決方案、經實證的方法及逾 18 年來服務全球多家最大、最複雜 SOC 所累積的豐富經驗，讓 OpenText™ 別具一格，最能協助您提升公司安全狀態與營運品質。

若要進一步瞭解記錄管理，請造訪 **www.microfocus.com/arcsightlogger**

opentext™ | Cybersecurity

OpenText Cybersecurity 為所有規模的公司和合作夥伴提供全方位的安全性解決方案。從預防、偵測和回應，到復原、調查和合規，我們的整合式端對端平台透過全方位安全性產品組合，來協助客戶建立網路韌性。OpenText Cybersecurity 客戶獲得我們即時關聯式威脅情報之可行動深入解析的支援，受惠於高效率產品、合規體驗，以及有助於管理業務風險的簡化安全性。

760-TW0047-002 | O | 12/23 |