opentext™ | Cybersecurity

資料表

ArcSight Enterprise Security Manager

借助功能強大、可調整的 SIEM 解決方案，即時偵測及回應威脅。ArcSight ESM 提供大規模的事件收集、原生威脅情報、領先業界的關連引擎，以及原生 ArcSight SOAR。

談到威脅偵測和回應，每一秒都舉足輕重。OpenText 所提供的 ArcSight Enterprise Security Manager (ESM) 大幅縮短即時和大規模偵測、回應和分類網路安全威脅的時間。ArcSight ESM 是一套功能強大的智慧型 SIEM (安全資訊與事件管理) 解決方案，利用即時事件關連分析，協助安全團隊偵測並回應內部與外部威脅。有了 OpenText 所提供的原生 ArcSight SOAR，它能將回應時間從數小時或數天縮短至數分鐘，並透過簡化的安全作業中心 (SOC) 工作流程，以及 ArcSight Marketplace 提供的持續更新威脅套件，讓 SOC 無需額外人力即可因應更多威脅。

主要優點

透過營運效率即時偵測威脅

ArcSight Enterprise Security Manager 是一套功能全面的即時威脅偵測、分析、工作流程及法規遵循管理平台，具有資料加強能力。ArcSight ESM 能夠即時偵測網路安全威脅並引導分析師進行應變，協助安全作業團隊迅速應對各種威脅指標。程式會自動辨識威脅並排定優先順序，讓團隊可避免因誤判所導致的大部分成本、複雜性及額外作業。ESM 提供集中檢視功能，讓 SecOps 團隊能掌握環境的現況，讓精簡化程序的工作流程更有效率。SOC 團隊可透過經提升的偵測能力、即時關連、工作流程自動化，以及原生 ArcSight SOAR，迅速且準確地解決事件。

整個企業的事件可見度

ArcSight ESM 運用 OpenText ArcSight Security Open Data Platform (SODP) 的進階事件收集技術，強化來自 450 種以上不同安全事件來源類型的資料並加以分析。ArcSight SODP 的 SmartConnector 支援所有常見的事件格式 (原生 Windows 事件、API、防火牆記錄檔、系統記錄、Netflow、直接的資料庫連線能力等)。ArcSight ESM 也會從雲端擷取資料。除此之外，我們的 FlexConnector 架構也支援開發自訂連接器，以利擷取和關連其他來源。事件來源越多意味著有更高的可見度，並可針對貴組織的需求開發更複雜的安全使用案例。

利用 GTAP 威脅情報防範最新威脅

Galaxy Threat Acceleration Programme (GTAP) Basic 是所有 ArcSight ESM 使

ArcSight ESM 概覽

即時偵測威脅
領先業界的事件關連可擴充至超過 100,000 EPS，將事件記錄分析集中化，以在出現威脅時進行偵測。

原生威脅情報
透過 ArcSight ESM 的原生 TI 摘要 GTAP，確保 ArcSight ESM 隨時掌握最新威脅。

內容與報告
預設內容提供 MITRE ATT&CK 對應、模組化儀表板、數百種可調整的關連規則，以及其他項目。

MSP/MSSP 就緒
支援分散式安全環境中的多方租用實作。

原生 SOAR
現成可用的 ArcSight SOAR 可讓您的團隊使用自動化、教戰手冊、事件管理、SOC 分析等功能。

用者均可使用的原生威脅情報摘要。它會自動將威脅監控內容整合至以開放原始碼威脅情報資料為基礎的 ArcSight ESM，透過提高產業威脅可見度，提供更全面的涵蓋範圍，對抗現代威脅與行銷活動。ArcSight ESM 也整合許多第三方和開放原始碼威脅情報摘要，並透過我們的進階威脅情報解決方案 GTAP Plus 提供精選的威脅情報防護 *(請參閱「附加元件」)*。

具備原生 SOAR 的自動化回應

ArcSight SOAR 被認為是現代安全分析的核心部分，因此將其提供作為輔助的原生解決方案。透過內建教戰手冊和逾 120 個整合外掛程式，ArcSight SOAR 能有效且有效率地自動化並協調管理分類、調查與回應活動。它支援視覺化的工作流程教戰手冊與詳細的 KPI 報告，並透過詳細的案件時間軸支援更佳的團隊協同作業。

透過整合與內容最大化投資報酬率

ArcSight ESM 整合了 ArcSight 產品組合的其他部分和大量的第三方安全工具 (EDR、票證系統、身分識別儲存庫等)，協助您最大化投資報酬。這些可在由 OpenText 提供的 ArcSight Marketplace 上檢視。ArcSight ESM 也隨附數百種現成可用的關連規則與儀表板。您也可以建立自訂內容 (規則、趨勢、儀表板和報告)，以因應幾乎所有的安全使用案例，然後可以輕鬆地封裝並部署在其他系統上，或是分享給其他事業體或 OpenText 社群。分層架構中可設定多個 ArcSight ESM，以動態方式自動同步內容系統。ArcSight Marketplace 和 ArcSight ESM 預設內容套件會持續更新新的安全使用案例、規則和支援的產品，這些內容可輕鬆進行部署，

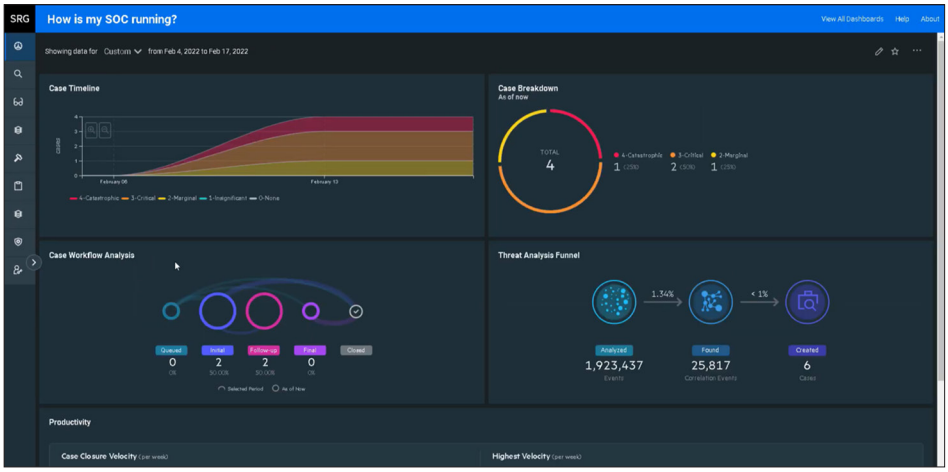

圖 1. SOC 指標儀表板

以協助您針對相關威脅提出警示並分類防禦機制，同時讓您的投資獲得更大報酬。

主要功能

功能強大的即時關連

ArcSight ESM 對事件與警示進行關連，找出環境中的高優先程度威脅。強大的關連引擎可即時分析大量事件資料 (每秒超過 100,000 筆事件)，以準確地呈報違反平台內部規則的威脅。

智慧型動態事件風險評分及優先順序排定

ArcSight ESM 獨特的優先順序公式包含用於評估每個事件的準則，以判斷其對您網路的相對重要性或優先順序。計算程序會納入許多資料點，例如定義的網路與資產模型、開放的連接埠，以及從第三方解決方案匯入的弱點掃描結果。例如，一個已知的攻擊可能會利用特定弱點入侵。如果遭鎖定的系統暴露出該弱點，且資產上受攻擊的連接埠處於開放狀態，則 ArcSight ESM 可假定此攻擊極可能成功並給予高優先程度。

分類與常態化

分類與常態化會將收集來的原始事件記錄轉換成通用格式，以在整個 ArcSight 平台使用。我們採用常見活動格式 (CEF)，這是 ArcSight 透過在數十年間於數十種安全與網路技術類別中累積的 300 多種連接器專業經驗，所開發的業界標準。經過分類和常態化處理的資料可協助您迅速辨識需要調查或立即採取行動的狀況，讓您將注意力放在最急迫的高風險威脅上。

工作流程自動化

建立案例時，ArcSight ESM 會自動從偵測到的事件擷取工件、建立案例範圍、分類案例、整合案例，將其對應至 MITRE ATT&CK 架構，並指派給分析師或分析師群組。自動化分類會優先處理警示，並自動關閉誤判。教戰手冊可設定為自動觸發或手動執行。ArcSight ESM 的內建案例管

理系統能讓分類作業有效率地進行，並在個案時間軸上有效追蹤所有活動。透過追蹤 SLA 與分析師回應時間指標，SOC 團隊可以縮短平均回應時間，並將事件呈報給合適的人員以解決問題。ArcSight ESM 也整合了許多第三方票證系統。

多方租用

ArcSight ESM 讓分散的事業體共用一個簡單的 SecOps 檢視。有了多方租用的功能及可精細設定至事件層級的存取控制權限，企業即可使用一組集中管理功能，包括以規則為基礎的限定值和統一的權限角色、權限及職責矩陣。單一部署的租戶會被指派唯一的租戶識別碼，且租戶的資料一律隔離 (安全資料區隔)。可自訂獨特的規則、報告與儀表板，讓目標系統擁有者與利益相關者存取。

整合 ArcSight Intelligence

由 OpenText 提供的 ArcSight Intelligence 具有強大的行為分析，並以無人監督的機器學習為後盾，協助您偵測內部威脅、零時差攻擊和進階持續威脅 (APT)。透過將 ArcSight Intelligence 與 ArcSight ESM 整合，您將獲得可偵測已知和未知威脅的多層式分析方法，為組織提供更全面的安全防護。此外，整合還能以更深入的威脅脈絡強化每個解決方案。舉例來說，ArcSight ESM 警示的風險分數會考量與這些警示相關的任何實體行為風險分數，以達到最佳化。使用者也可以根據 Intelligence 偵測到的異常行為建立關連規則。

整合 ArcSight Recon

ArcSight ESM 整合了由 OpenText 提供的 ArcSight Recon，在安全作業環境中支援極為快速且直覺式的搜尋與資料視覺化。ArcSight Recon 是新一代的記錄管理、合規、搜尋與調查解決方案，以進階分析平台為基礎打造，滿足安全團隊不斷演變的需求。ArcSight ESM 與 ArcSight Recon 的組合讓 SOC 人員可透過智慧型視覺化功能偵測並瞭解公司內部未知的安全威脅，以快速修補安全威脅所帶來的任何衝擊，或在安全威脅造成損失之前預先緩解。

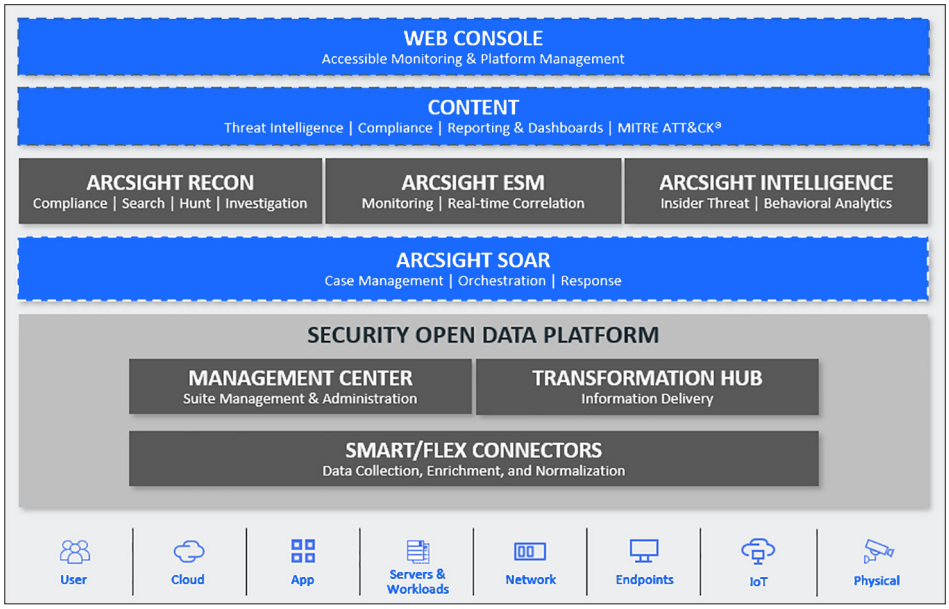

圖 2. ArcSight 產品組合

其他 ESM 功能

其他功能

- **活動式清單**—動態記憶清單能夠保存數百萬筆記錄，作為監控可疑流量或行為的監看清單。活動式清單可於任何關連規則中使用。
- **排程報告**—並且將結果自動傳送給重要的利益相關者。
- **API**—使用以 OpenText 為基礎的 API 和 Swagger 整合的 ArcSight REST，共用來自 ArcSight ESM 的事件和案例資料。
- **OpenText 儀表板的 ArcSight Fusion**—ArcSight 的 Web 式 Fusion使用者介面連接 ArcSight 平台的所有元件，並支援可自訂的小工具儀表板，以視覺化方式呈現 SOC 指標。
- **MITRE ATT&CK 儀表板**—即時檢視環境中發生的所有 MITRE ATT&CK 相關事件，面對 SOC 的頂級威脅技術，以及貴組織偵測個別技巧能力的清楚影像。
- **資料安全**—使用無法變更的資料儲存來保護資料完整性。
- **Active Directory 整合**—透過 AD 使用者和群組管理 ArcSight ESM 使用者和群組成員資格。
- **分散式關連**—此模式可讓使用者部署多個關連和彙總的執行個體，以提高處理速度，並透過更多內容相關事件分析改善關連精確度。

附加元件

GTAP Plus

GTAP Plus 是 ArcSight ESM 的進階威脅情報摘要，整合來自 OpenText™ Cybersecurity Galaxy 威脅研究網路的深入見解，為 ArcSight 使用者提供主動防禦。它能提供更高的可見度、減少誤報，並

「ArcSight 讓我們不只是迅速偵測到真正的攻擊，還能以近乎即時的速度將協調回應自動化。ArcSight 的彈性協助我們以智慧方式因應未來需求。」

Dmitriy Ryzhkov
資深資訊安全分析師
NPC Ukrenergo

與我們交流
www.opentext.com

強化威脅回應，以擴大防護現代威脅與威脅活動。GTAP Plus 致力於消除盲點，並提供 ATT&CK 和 D3FEND 對策的進階實作能力，以協助在侵害發生前先行阻止。

高可用性 (HA)
透過多個 ArcSight ESM 系統最佳化效能環境，具備自動容錯移轉功能，以防主系統發生任何通訊或操作問題。

合規見解程序套件 (CIP)
使用 ArcSight CIP 減輕稽核與合規的負擔。這些套件透過一系列規則、儀表板、資料監控、現用通道、自動化、報告等，為合規提供必要基礎。套件適用於 GDPR、NERC、HIPAA、ITGOV、FISMA、PCI 和 SOX。

Voltage SecureData Enterprise 附加元件
ArcSight 利用 OpenText 技術的 Voltage SecureData Enterprise，套用 Format Preserving Encryption (FPE)，藉此在不將社會安全號碼或信用卡號碼等敏感資料洩漏給分析師或 ArcSight 使用者的情況下，保留關連功能。

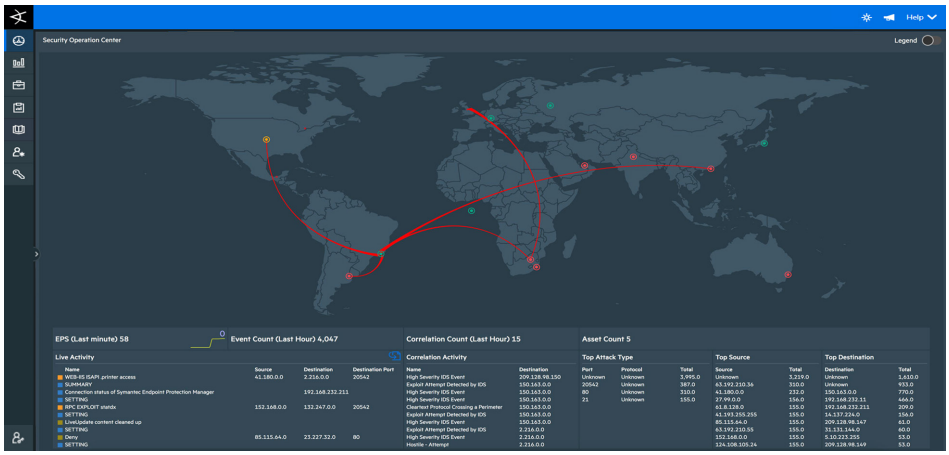

圖 3. 具有世界地圖的 SOC 儀表板

ArcSight Marketplace
透過 ArcSight Marketplace，使用者可以從我們的合作夥伴、社群和安全專家取得數百種支援內容套件。這包括免費和付費內容，使用 ArcSight 認證的應用程式、規則集，儀表板、整合、還有連接器等更多功能，進一步強化您的 ArcSight 使用率。

如需更多資訊，請瀏覽
www.microfocus.com/arcsightesm

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，我們的統一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 客戶自我們即時的關聯式威脅情報獲得可據以行動的深入見解，享有可協助管理業務風險的高效率產品、合規體驗以及簡化的安全性。