LogRhythm™

Security Intelligence and Analytics Platform
智慧型資安情資數據即時分析平台

從端點到網路，一氣呵成的威脅生命週期管理，自建SOC之最佳選擇！

LogRhythm 為技術獨步全球且備受各產業推崇的 Next-Gen SIEM，專事 Threat Lifecycle Management 威脅生命週期管理，連續九年蟬聯 Gartner SIEM Magic Quadrant Leaders 領導地位，連續四年榮獲 Gartner Peer Insights Customers' Choice 金質獎，極受各界專家及客戶青睞與高度肯定。LogRhythm擁有眾多專利技術，如: Machine Data Intelligence (MDI) Fabric、日誌內容正規化、威脅風險評級關聯式分析、時間正規化等。LogRhythm 內建且定期更新逾 1,000 種設備之標準分類及正規化及逾 1,650 項 AI 多維情境關聯式分析規則，具備3萬多種事件偵測能力，提供逾60萬條日誌正規化語法、百種以上法令遵循規範，以及逾800種預設報表與百種客製化報表範本，為全球公認自建SOC資安監控維運中心之不二選擇。

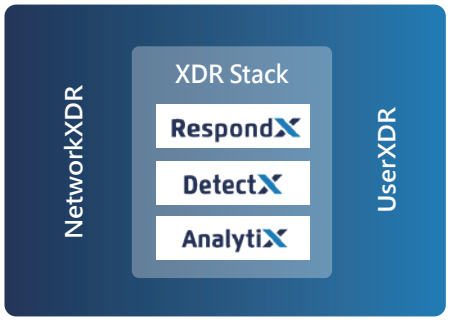
LogRhythm提供全方位的威脅生命週期管理，將資安威脅在不同階段所呈現之徵兆、樣態，及其所對應之監控、搜捕、偵測、調查、回應、復原、鑑識等程序所需要的人員、流程自動化與技術無縫整合，大幅縮短MTTD與MTTR，更可在有限的資安人力與資源下，提供即時有效的資安防護、情資交流與事件協同合作。LogRhythm Labs 近 500 位資安專家隨時研究最新情資及 MITRE ATT&CK 資安框架，並即時更新相關 AI 偵測分析規則套件，協助企業組織即時加強偵測與回應能力，迎戰各類詭譎多變的新興威脅。

LogRhythm XDR Stack

LogRhythm XDR Stack 是一套採用模組堆疊架構而成的 NextGen SIEM，其中包含採用專利MDI技術AnalyticX模組，專事收納各式設備日誌並進行非結構化日誌自動分類及正規化，大幅減少日誌整理之人力及時間，快速提升資料可用性及分析性，加速辨識資料內的潛在威脅及風險。

DetectX模組內建多種威脅偵測套件，針對入侵指標、攻擊策略、技術及程序(TTPs)進行威脅偵測及獵捕。採用機器學習關聯及建立基準線，有效辨識異常之行為。LogRhythm Labs 定期更新各類最新威脅偵測方式並提供套件，有效降低告警誤判率且大幅節省昂貴程式開發及維護。

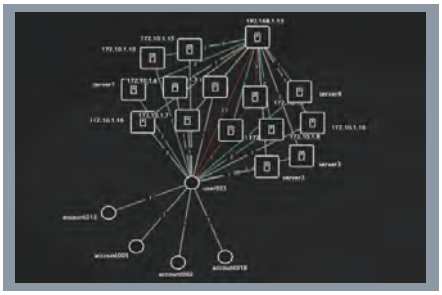
RespondX模組著重於資安事件協同及回應自動化 (Security Orchestration, Automation and Response, SOAR)。



內建十數種SmartResponse自動回應Plug-in套件，使資安事件自動化協同聯防機制更為完善。內建事件協同平台(Case Management)與近20套資安事件回應程序手冊(Case Playbook)，俾於資安事件發生時迅速提供跨單位、跨地理位置協同合作標準處理程序，XDR Stack 亦可整合 NetworkXDR 模組進行即時網路流量分析，快速偵測及辨識網路威脅，加強企業組織於遭受網路攻擊之及時防禦及回應能力。

LogRhythm v7.10 嶄新功能

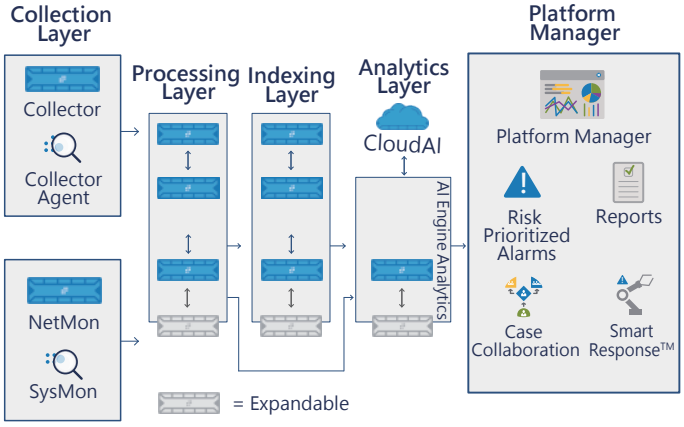
2022年第四季 LogRhythm 發布v7.10最新版本，提升Admin API Library功能，可整合既有流程及系統，加速事件回應以及降低維運時間。新增Alarm API，讓管理者無需連線資料庫也能存取告警內容。Metrics API 提供日誌流量及日誌統計數據。新增node-link widget 以利分析人員於Dashboard儀表板進行事件調查及分析時，以圖形節點方式進行關聯性分析。



全視覺化網路及系統節點圖示，使資安人員更容易辨識事故發生點與波及的熱點。

LogRhythm 端點到網路 一氣呵成的威脅生命週期管理平台

LogRhythm 系統元件

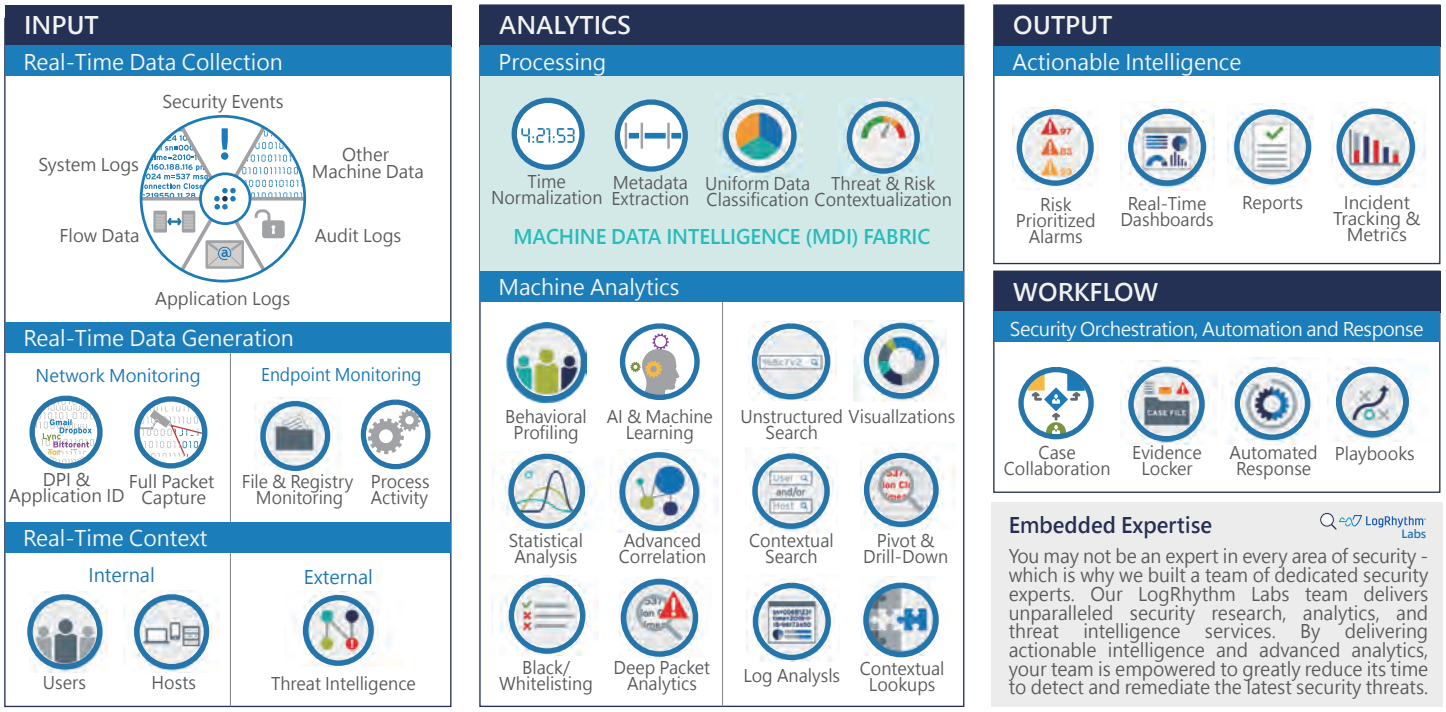


Collection Layer：無需安裝代理程式之資料收容器，可收納近端及遠端逾千種各項設備資料格式，提供集中管理機制，本身具備 TLS 加密能力以及 10 : 1 傳輸壓縮比，強化資料安全及傳輸效能。

- System Monitor：Lite Agent / Pro Agent 獨立產出具備深度可視性、即時、可供鑑識之主機活動資料，包含：機敏性之系統、應用系統、使用者活動資料，如：使用者授權、檔案異動、被使用之應用系統網路通訊內容以及端點不易監控到之底層活動等，且支援多種作業系統。
- **Network Monitor**：支援威脅偵測、事件回應所需之資料，包含：深度辨識應用系統 ID、Rich Session-Based Metadata 萃取、Layer 2~7 封包分析、Full Packet 截取等，用以支援分析外洩資料及重建惡意軟體、執行 RespondX 回應措施、產製儀表板所需之數據。

Data Processors：由 Data Collector、System Monitor、Network Monitor 傳送之資料予以正規化、萃取 Metadata，並提供管理者集中化資料正規化控管機制。

AI Engine：內建逾 1,650 項 AI 規則，採用多維情境關聯式分析，Trend 及 Baseline 機器學習機制，大幅提升已知及未知威脅之辨識能力。具備即時防禦功能，可透過 RespondX 加速協同聯防、審核與自動化回應。



Embedded Expertise

LogRhythm Labs

You may not be an expert in every area of security - which is why we built a team of dedicated security experts. Our LogRhythm Labs team delivers unparalleled security research, analytics, and threat intelligence services. By delivering actionable intelligence and advanced analytics, your team is empowered to greatly reduce its time to detect and remediate the latest security threats.

Platform Manager：依風險評級管理事件、發出訊息、告警及通知，啟動分散式搜查、鑑識分析、產製報告與即時儀表板。案件及資安事件流程管理依據事件性質、風險程度及人員職責，迅速提供跨單位、甚至跨地理位置進行協同合作之標準處理程序。

技術優勢

Data Collector：無需任何特殊程式語言學習，可即時完整地收集各種型式之資料來源，包含：System Logs、Security Events、Flow Data、Application Logs、Audit Logs 等，以及自行開發應用程式之日誌。

- 支援 UDP/TCP、Secure Syslog、SNMP、一般或壓縮文字檔案等日誌。
- 可支援 Flow Data，含 IPFIX、NetFlow、sFlow、JFlow 與 SmartFlow 等日誌。
- 可透過 UDLA Adapter 收集資料存放於資料庫如：Oracle、SQL Server、MySQL 等日誌。
- Windows 事件日誌 (遠端或本機收集)。
- 雲端服務：Amazon AWS、Salesforce、Dropbox、Cradlepoint、Office 365。
- 可透過 API 收集 Cisco SDEE、Checkpoint OPSEC/LEA、AS400 & iSeries、Sourcefire eStreamer、Tenanble Security Center 與 CradlePoint 等日誌。
- 弱點掃描工具之日誌：Qualys、Rapid7、Tenable Security Center。

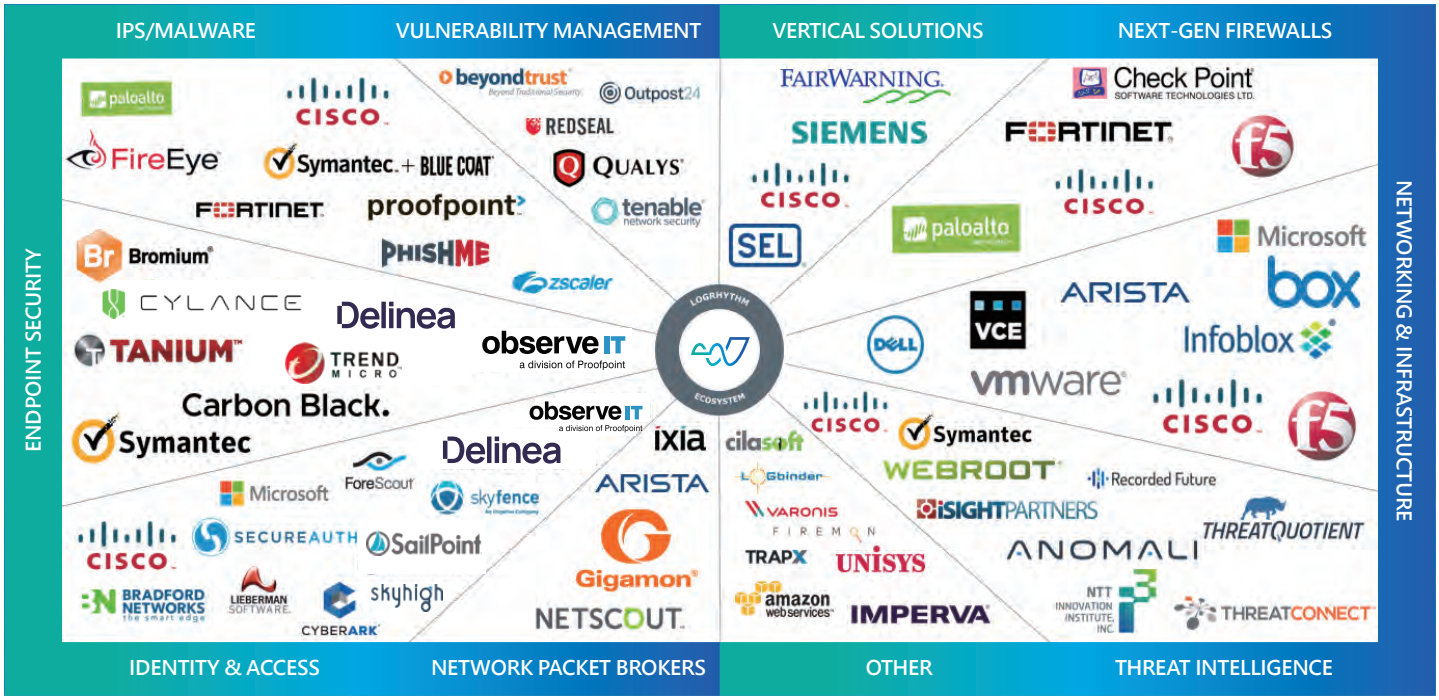
Machine Data Intelligence：專利的機器資料智慧分類篩濾技術 (MDI Fabric) 可針對逾千種各類裝置及設備資料，自動萃取 Metadata 並進行資安事件分類。

- 支援來自不同廠商及平台的數據收集並統一事件分類。
- 可針對個資機敏日誌進行遮罩。
- 每一情境處理皆為高度縝密的數據分析及計算結果。
- 日誌時間正規化以及進行誤差校正以利精確比對事件之關聯性。

Endpoint Monitoring and Forensic：結合 LogRhythm 智慧型資安情資數據即時分析平台，能掌握 IT 環境中的端點系統所有狀況。並透過 RespondX 對端點可能遇到的進階威脅、違反遵循與操作問題，提供主動的防護機制。

- **Independent Process Monitor：**偵測系統運行黑名單中的執行緒或重要系統執行緒異常時進行即時告警。可結合 RespondX 受影響之端點，直接進行中止或啟動特定執行緒。
- **Data Loss Defender：**可偵測端點上所使用的可攜式媒體，在資料即將進行傳輸前發出告警，並即時卸載該裝置，自動防止資料外洩。
- **Windows Registry Monitor：**可監控並偵測 Windows Registry 之變更，包含惡意軟體異常植入或竄改 Windows Registry 時，可結合 RespondX 即時修復及還原註冊表，防止惡意攻擊。
- **Network Connection Monitor：**可監控並記錄端點網路，包含 Listening Port、網路 Inbound / Outbound Traffic、連接埠以及執行緒。當偵測有可疑的網路連接時，可結合 RespondX 將未授權的連接埠 IP 於防火牆設備阻擋。
- **User Activity Monitor：**可監控並記錄端點使用者登入及登出帳號，並將使用者登入登出活動經由 AI 引擎進行進階關聯性分析。當有偵測異常登入行為時，可結合 RespondX 自動關閉本機或 AD 之對應帳戶。
- **File Integrity Monitoring (FIM)：**提供 Windows 及 Linux 檔案一致性監控，可針對指定之檔案、檔案類型或資料夾進行之變更、讀取、刪除、變更權限與變更檔案擁用者等事件進行記錄，亦同時計算檔案 Hash 值加以監控，可避免檔案遭惡意竄改。

TrueIdentity™：彙整同一使用者於不同系統、多個帳號及存取權限，建立精準的身份關聯性分析，提供單一且整合的視覺化管理，更準確判斷使用者潛在意圖，防範因「人」而引起之威脅。



Threat Intelligence Source：LogRhythm 可多元組合或獨立運用各方威脅情資來源，以利快速偵測並排序高風險性之威脅。並支援多種標準化資料交換格式，如：STIX、TAXII等，同時支援 ISAC、SOC 等重要情資交換應用，如：FS-ISAC、NH-ISAC。

ElasticSearch™：LogRhythm整合了ElasticSearch™ Lucene為基礎的索引技術，提供便捷強大的全文搜索能力，可在同一搜尋表示法結合上下文之內容標準與全文檢索標準，以獲得更精確的搜尋結果，進而加速威脅調查和事件回應。藉由ElasticSearch™分類服務與資料叢集，可建置於 active/active high-availability 架構，並可於單一介面快速交叉搜尋原始日誌之資料庫及事件日誌資料庫，以高達三倍的速度處理大量工作負載和索引數據。

Compliance Automation：預建20餘種法規遵循模組功能，如：GDPR、201CMR 17.00、BSI: IT-Grundschutz、CIS Critical Security Controls、DoDi 8500.2、FISMA、GLBA、GPG 13、HIPPA、HITECH & MU、ISO 27001、MAS-TRMG、NIST Cybersecurity Framework、NEI 08-09 Rev 6、NIST800-53、NERC CIP、PCI DSS、NRC Regulatory Guide 57.1、SOX、NYDFS Cybersecurity Compliance Regulation、SWIFT、UAE-NESA等。提供法規遵循自動化並確保落實執行，包括稽核機制、告警、查核及軌跡報告、已停用帳號之即時監控等。

LogRhythm Labs

由500名以上資安專家組成，擁有多項專利技術(持續增加中)用於 LogRhythm Next-Gen SIEM 平台上。定期提供之更新服務有：新增之設備日誌收納、地理資訊、AIE規則及清單、威脅情資、儀表板、SmartResponse™ Plug-in、Case Playbook、法令遵循及規範等。

關於 LogRhythm

LogRhythm 為資安威脅生命週期管理 (TLM) 技術先鋒，創立於 2003 年，總部位於美國科羅拉多州，逾 4 千多家各產業客戶橫跨 6 大洲，其原生且卓越的開發技術已取得多項專利。LogRhythm 完整且單一、End-to-End 的資安情資分析平台功能包括：日誌收納分析、威脅偵測、使用者與實體行為分析 (UEBA)，網路通信及行為分析 (NTBA)，以及資安事件協同及回應自動化 (SOAR)。LogRhythm 智慧型資安情資數據即時分析平台具備機器學習及人工智慧能力，為資安監控中心 (SOC) 重要基礎，可確保客戶實體、虛擬及雲端各類資訊資產之安全。

Gartner Magic Quadrant for SIEM Leader

Gartner Peer Insights Customers' Choice

CybersecAsia Readers' Choice Awards SIEM Awards Winner

Cybersecurity Breakthrough Award Best SIEM Solution Award Winner

Spring Expert Insights Top10 Best of SIEM Solutions Award Winner

Singapore Business Review Tech Excellence Award Winner

G2 Grid® Leader in SIEM System Security & Incident Response Fall

SIEM Best Product, Winner

Network Security and Management Best Product Winner

LogRhythm™ 漢領國際有限公司 JAS Lead

106414台北市大安區敦化南路二段77號8樓之2
電話：+886-2-2709-6983
傳真：+886-2-2707-6983
www.jas-solution.com sales@jas-solution.com