技術中立日誌串流與最佳化技術
(Agnostic Log Streaming and Optimization Technology)

目錄

目錄

1. 日誌管理與合規性挑戰 3
2. 為什麼選擇 Cribl？ 4
2.1 資料減量與節省成本 4
2.2 供應商中立技術 (Vendor-Neutral Technology) 5
2.3 集中式可觀測性 (Centralized Observability) 5
2.4 平台架構與擴展性 6
2.5 法規與合規性 6
3. 架構（僅限地端 ON PREMISE ONLY） 7
3.2 韌性 (Resiliency) 8
4. Cribl 策略優勢與投資回報率 (ROI) 9
5. 為何選擇 Cribl 而非其他競品？ 9
6. Cribl 教育訓練與最新資源 10
6.1 Cribl 免費教育訓練 10
6.2 Cribl 最新資源與社群支援 10

1. 日誌管理與合規性挑戰

企業在處理資安資料、分析與合規性方面正面臨日益增加的挑戰。

資料的增長、複雜性與多樣性，正對預算以及資安團隊的效率與時間帶來龐大壓力。

造成此現象的原因有多種:

- 數位活動的增加。
- 越來越多資安工具需要來自相同系統的相同資料，或同一系統的不同資料。
- 監管機構對日誌記錄的要求不斷增加。

然而，預算的增長速度卻無法跟上，導致風險增加與效率低落：

- 我們該如何收集所需的所有資料？
- 我們該如何儲存這一切？
- **我們該如何在保持可視性與合規性的同時，以最佳、最具成本效益的解決方案來路由 (route) 與儲存資料？**
- 我們該如何將資料從一個分析解決方案轉移到另一個，而不需要從頭來過，並將風險降至最低？

基於這些原因，**企業需要一項與供應商無關（Agnostic）的技術，讓他們能夠自由選擇並掌握資料的控制權**。這正是現今企業開始採用中立的資安管道 (Security Pipeline) 技術的原因，這些技術將資料的收集、轉換與路由層從現有的 SIEM (資安資訊與事件管理) 或 XDR 系統中脫鉤。

圖 1 - 日誌遙測管道的採用 (Log Telemetry Pipeline Adoption)

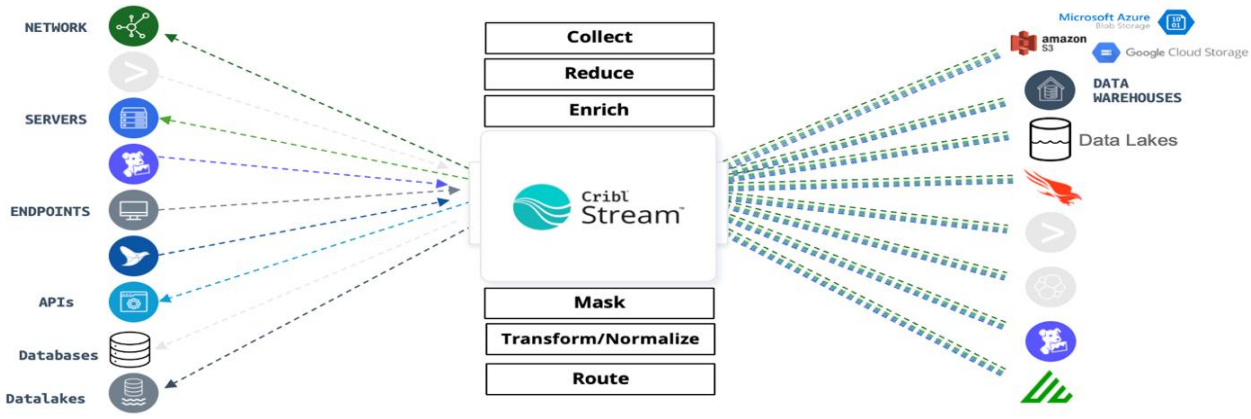
Source: Predicts 2023: Observing and Optimizing the Adaptive Organization

2. 為什麼選擇 Cribl？

Cribl Stream 是一個與供應商無關的「可觀測性管道 (Observability Pipeline)」技術，賦予您極大的彈性，能從任何來源收集、縮減、豐富化、正規化並路由資料到您現有資料架構中的任何目的地。

這是一款專門為解決管理大量且複雜資安資料挑戰所打造的解決方案。

圖 2 - Cribl 可觀測性管道

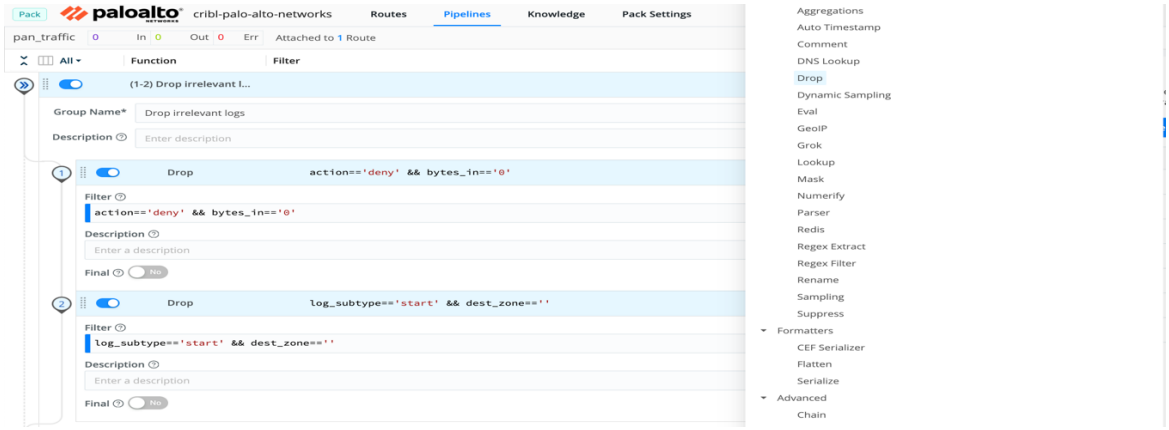


企業使用 Cribl 來解決以下網路安全挑戰：

2.1 資料減量與節省成本

- Cribl 可過濾、解析並將與資安相關的資料路由至 SIEM 或 XDR，從而降低 EPS (每秒事件數) / 資料量以及資料寫入 (ingestion) 成本。
- Cribl 會丟棄不必要的日誌。如果因合規性需要保留這些日誌，Cribl 可以將它們路由至低成本的儲存空間（例如：地端儲存或雲端 S3）。
- 該解決方案為資安管理員提供了一個易於使用的圖形化介面，無需撰寫任何腳本或冗長的正則表達式 (Regex)，即可選擇性地丟棄不需要的資料。

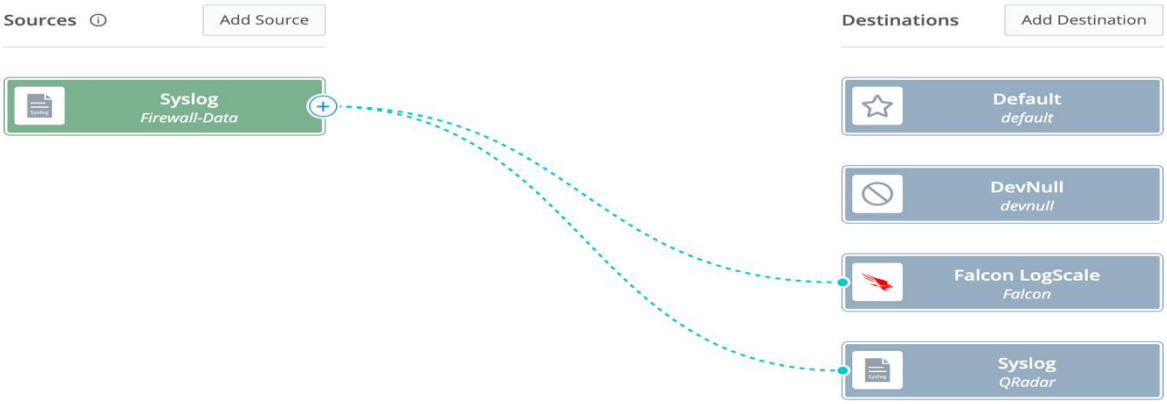
圖 3 - 資料控制



2.2 供應商中立技術 (Vendor-Neutral Technology)

- Cribl 可以將資料無縫地寫入任何 SIEM 或 XDR 系統。
  當您導入新的資安技術時，**Cribl 能以接收端技術預期的格式，輕鬆地將另一份資料副本路由過去，免去更新解析器 (Parser) 的麻煩**。
- Cribl 的核心理念允許企業平順地轉移至新的資安分析平台，進而降低在移轉階段發生資料遺失或出現監控盲區的風險。

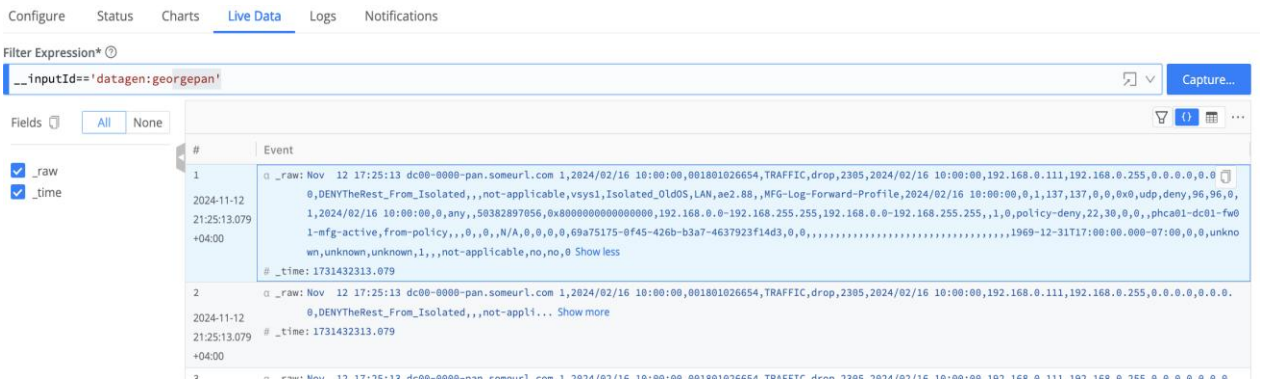
圖 4 - 多重目的地路由



2.3 集中式可觀測性 (Centralized Observability)

Cribl 提供單一管理介面 (Single pane of glass) 來管理和路由來自所有資安產品的日誌，大幅提升營運效率。它消除了資訊孤島 (Silos)，確保資安團隊能即時接收具有可操作性的資料。
資安工程師在排解資料問題時經常缺乏可視性。Cribl 提供了從資料收集、轉換，直到寫入資安平台的端到端 (End-to-End) 資料視角。

圖 5 - 資料可視性



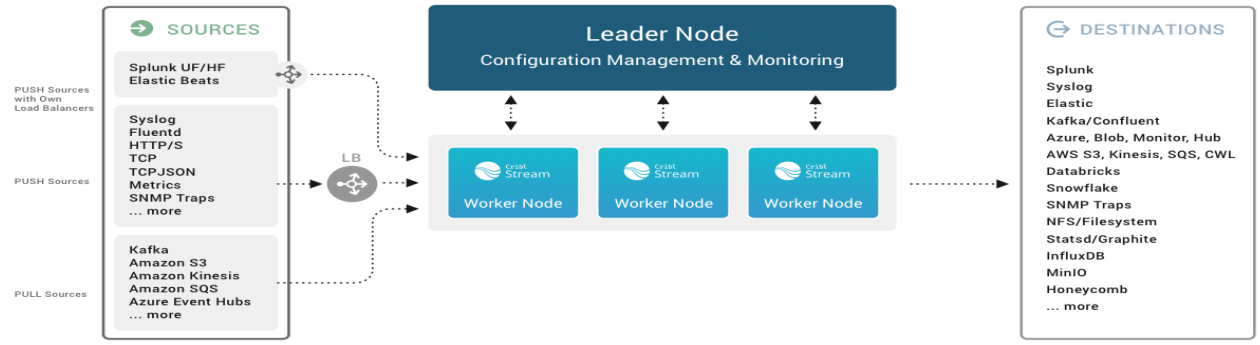
2.4 平台架構與擴展性

Cribl 的架構僅包含兩個元件：管理層 (Management Plane) 與資料層 (Data Plane)。
該技術基於「無共享架構 (Shared-Nothing Architecture)」理念所打造，使其在使用相對較低運算資源的情況下，依然能保持簡單且高效。

它僅運行最基礎的服務與相依性，因此具備極高的速度與韌性。任何元件或伺服器發生故障，都不會影響資料流。

該平台後端不使用資料庫，這使得它可以無上限地水平擴展。

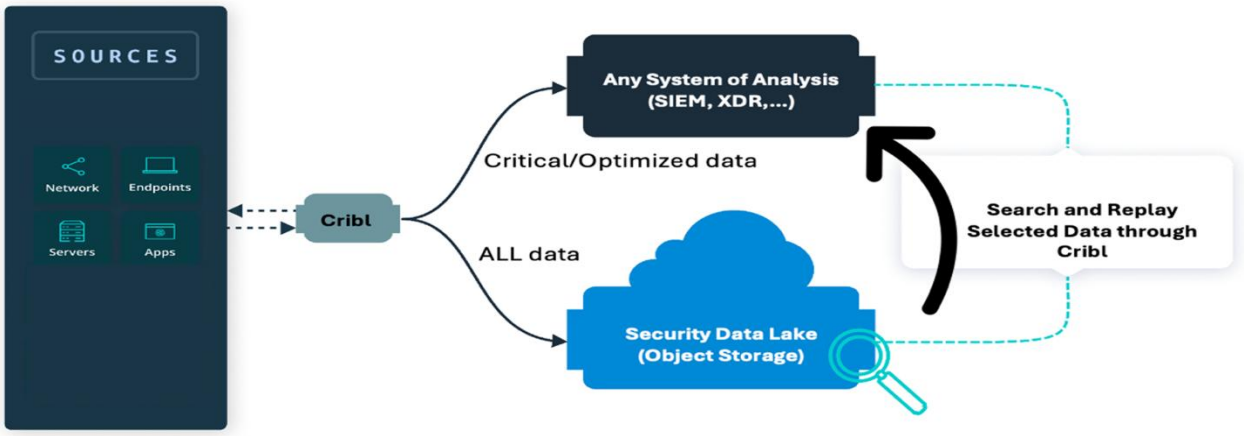
圖 6 - Cribl 精簡架構



2.5 法規與合規性

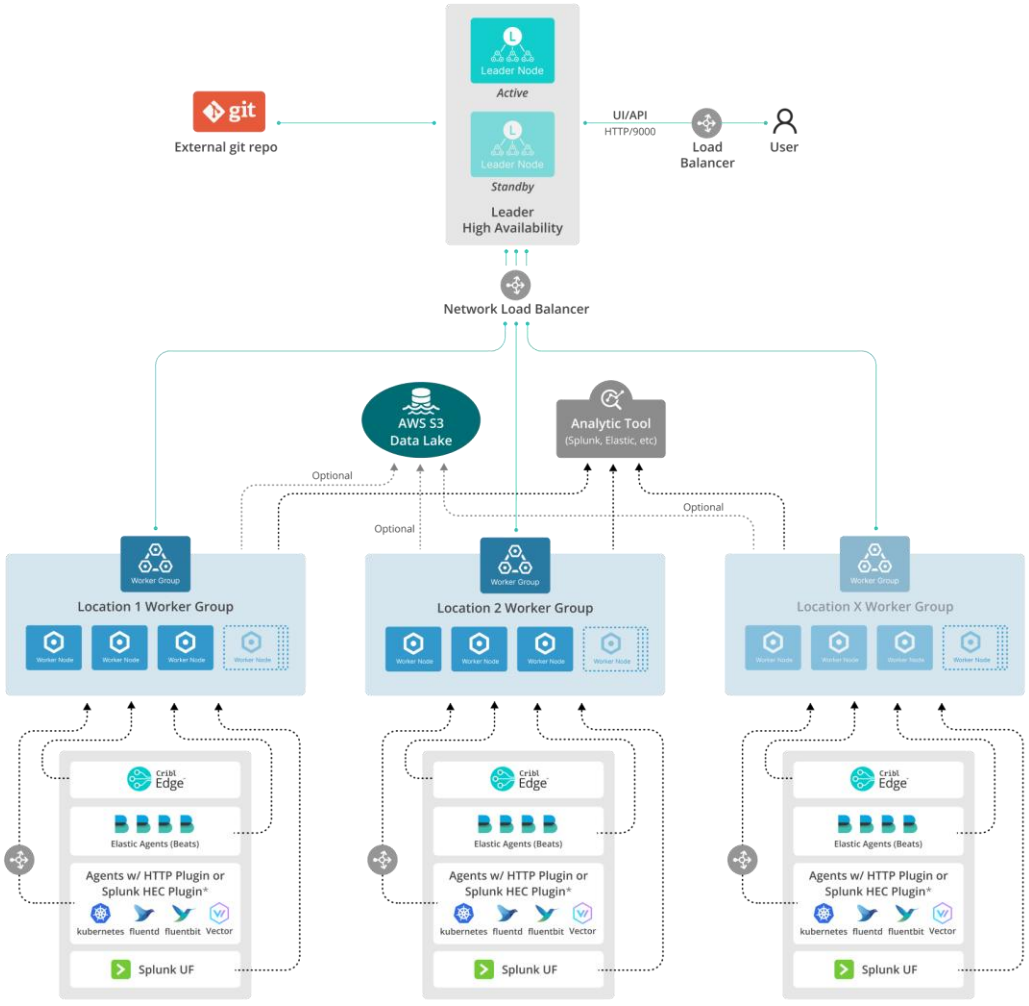
Cribl 能以低成本幫助企業跟上嚴苛的合規性要求。它提供了一種選項，**可以將所有原始日誌保留在具備成本效益的儲存層中，同時僅將經過整理、符合合規重點的日誌傳送到 SIEM**。資料以開放格式儲存，不受任何 SIEM 或 XDR 綁定。
如果需要調閱資料，可以透過 Cribl 進行搜尋，並將其重新水化 (Rehydrate，即回放/還原) 到 SIEM 平台中。
這滿足了法規要求（例如：GDPR、ISO 27001）及內部稽核的需求。

圖 7 - 資安資料湖 (Security Data Lake)



3. 架構（僅限地端 ON PREMISE ONLY）

圖 9 - Cribl 架構



Cribl 提供了高度強韌的架構。這個架構可以簡化為三個關鍵層級：資料收集層、處理層與控制層。

1. **資料收集層 (Data Collection Tier)：** Cribl Stream 可持續接收來自各種來源的資料輸入，包含 Splunk、HTTP、Elastic Beats、Kinesis、Kafka、TCP JSON 等等。

2. **處理層 (Processing Tier)：** 處理層的運作發生在工作群組 (Worker Groups) 中。工作群組是共用相同設定的工作節點 (Worker Nodes) 集合。在工作群組內，可設定資料流，包含每個群組的路由、管道、來源與目的地。

- **控制層 (Control Tier)：** Cribl 領導節點 (Leaders) 提供單一設定管理入口網站，以及監控各工作群組效能的控制台。

3.2 韌性 (Resiliency)

關鍵韌性功能（工作群組 Worker Groups）：

- **無共享架構 (Share-Nothing Architecture)：** 群組中的每個工作節點都是獨立運作的，即使與領導節點斷線，仍可處理並緩衝資料。這意味著如果領導節點或網路連線發生故障，工作節點會繼續收集並緩衝資料，確保不會發生立即的資料遺失。
- **持久化佇列 (Persistent Queues)：** 工作節點可以設定持久化佇列，讓它們在下游服務中斷或流量激增時緩衝資料。這可防止資料遺失，並為系統從故障中復原爭取時間。
- **最低節點建議：** 為了實現高可用性 (HA)，建議每個群組至少部署三個工作節點。這使得系統在單一節點進行計畫性維護或發生非預期停機時，能夠容許故障且不會中斷服務。

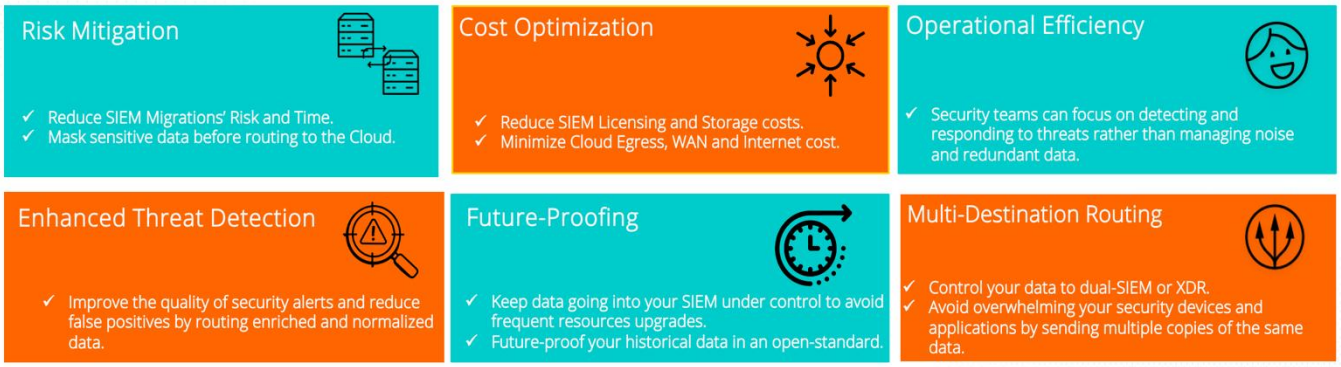
關鍵韌性功能（領導節點 Leaders）：
在客戶自行管理的高可用性 (HA) 架構中，任何時間都只有一個領導節點處於活動狀態 (Active)，而第二個領導節點則處於待機狀態 (Standby)。

- **狀態一致性 (State Consistency)：** 主要與待機領導節點使用共享的 NFS 備份磁碟區來維持狀態與設定的一致性。這確保了待機節點在容錯移轉 (Failover) 時，能立即獲得最新的設定。
- **無縫容錯移轉 (Seamless Failover)：** 若主要領導節點發生故障，待機領導節點會自動接管。這種無縫轉換是透過放置在領導節點前方的負載平衡器 (Load Balancer) 來實現的，負載平衡器會主動輪詢 /health 端點。負載平衡器可確保工作/邊緣節點 (Worker/Edge Nodes) 以及其他用戶端始終被路由到活躍且健康的領導節點，使得切換過程對 Cribl 環境的其他部分而言幾乎是無縫的。

4. Cribl 策略優勢與投資回報率 (ROI)

透過將 Cribl 嵌入資安分析架構中，客戶可獲得許多策略性優勢，總結如下表：

圖 10 - Cribl 策略優勢



5. 為何選擇 Cribl 而非其他競品？

雖然市場上出現了一些新興技術，但 Cribl 仍因以下諸多原因保持領先地位：

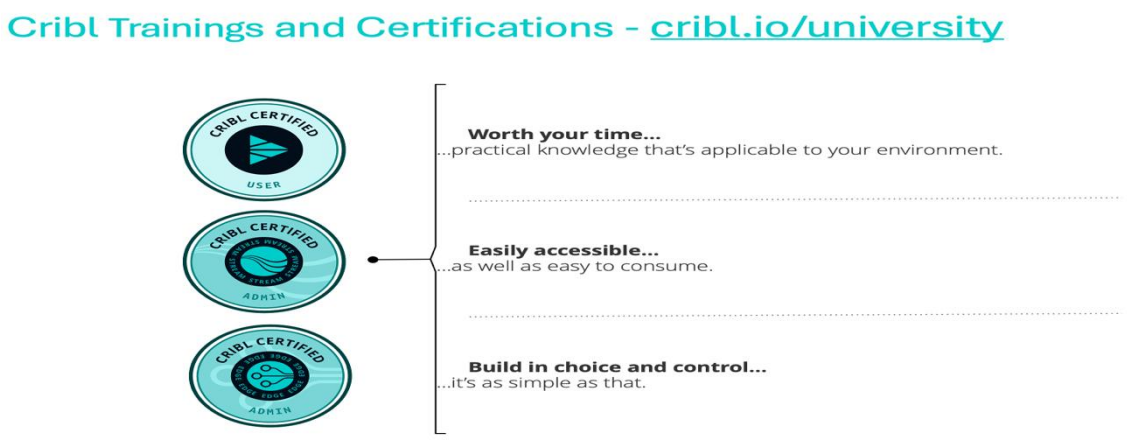
- **Cribl 支援數量最多的 SIEM 與分析解決方案**。
- **Cribl 是一項經過驗證且具備高度擴展性的技術，最大的客戶每天寫入超過 1PB 的資料**。
- 該技術基於無共享架構，提供了極高的韌性、簡便性與效能。
- 這是一個專門建構的資料管道技術，從第一天起就是為了處理資安與可觀測性的日誌及事件資料而設計。
- **獲得技術供應商聯盟的信任：** Cribl 已與 CrowdStrike、Microsoft 和 Elastic 等技術供應商簽署了合作夥伴關係。
- **Cribl 社群成長非常快速：** 截至 2024 年 11 月，已經有超過 8000 名社群成員在公開的 Slack 頻道上互相支援。（備註：社群擁有超過 10000 名活躍使用者）
- Cribl 是一項經過驗證的技術，擁有跨越所有產業的數百名客戶。
- 它是矽谷成長第 4 快的新創公司（年營收從 100 萬美元成長至 1 億美元）。
- 獲得超過 6 億美元的資金挹注。
- 擁有 Sequoia、Greylock、CRV 和 Google Ventures 等知名投資者背書。

6. Cribl 教育訓練與最新資源

6.1 Cribl 免費教育訓練

Cribl 提供全球認可的免費教育課程與認證。我們持續更新教材內容，並根據需求增加額外的學習資料。

圖 11 - Cribl 教育訓練



6.2 Cribl 最新資源與社群支援

雖然 Cribl 為企業客戶提供 24x7 全天候支援，但您也可以善加利用社群的經驗與資源，以獲取額外價值並分享經驗。
Cribl 及其社群（包含客戶、合作夥伴與使用者）開發了多種管道套件 (Packs)，為最常見的資料來源提供開箱即用 (Out of the box) 的內容資源。
Cribl 社群擁有超過 10,000 名活躍使用者，他們分享經驗、互相支援，還能透過 Slack 獲得 Cribl 工程師的即時協助。

圖 12 - Cribl 資源與社群支援