Керування потоками даних:

як Cribl допомагає IT і безпеці впоратися з лавиною телеметрії

Олексій Найда, Business Development Manager, iIT Distribution, — про «маршрутизатор», який сортує дані і відправляє командам безпеки саме ту інформацію, яка їм потрібна.

За даними IDC, щороку обсяг даних у корпоративних мережах зростає приблизно на 28%, тоді як IT-бюджети — лише на 7%. Цей дисбаланс створює постійний тиск на IT-відділи, команди безпеки та аналітики. Вони мусять обробляти дедалі більший потік телеметрії — логів, подій, метрик, — щоб забезпечити стабільність інфраструктури, кіберзахист і ефективність бізнес-процесів.

У результаті навіть досвідчені IT- та безпекові команди стикаються з ситуацією, коли даних надто багато, а часу, інструментів і ресурсів для їх ефективного використання — замало. Телеметрія надходить із десятків джерел: серверів, застосунків, мережевого обладнання, сенсорів безпеки — і швидко перетворюється з корисного ресурсу на інформаційний хаос.

Традиційна стратегія «збирай усе» у таких умовах більше не працює. Накопичення необроблених даних у SIEM або аналітичних системах призводить до зайвих витрат, затримок та інформаційного шуму. Тому все більше бізнесів замислюються не лише над тим, що збирати, а й як цим керувати.

Саме тут з'являється новий підхід — керування потоками даних або **data pipeline management**. Він дозволяє структурувати телеметрію, оптимізувати її маршрутизацію та відправляти потрібну інформацію саме туди, де вона дає найбільшу користь. Одним із лідерів цього напрямку є платформа Cribl, яка допомагає організаціям упорядкувати хаос даних і перетворити його на керований, прозорий потік інформації.

Коли даних забагато

Більшість організацій сьогодні працюють із десятками джерел телеметрії — від систем безпеки до корпоративних застосунків. Без централізованого керування це призводить до низки проблем.

- **Зростання витрат.** Неоптимізована маршрутизація даних перевантажує SIEM і системи зберігання.
- **Затримки в аналітиці.** Дані не потрапляють туди, де потрібні, у потрібний момент.
- **Безпекові ризики.** Відсутність єдиного контролю за потоком даних може створити вразливості.
- **Складність управління.** Велика кількість агентів і точок інтеграції ускладнює підтримку.
- **Дефіцит кадрів.** Постійна ручна обробка потоків даних вимагає значних людських ресурсів.

До цього додається ще один виклик — розмаїття джерел і форматів. Інформація надходить із систем моніторингу, SOC, мережевих сенсорів, застосунків, хмарних платформ, часто в різних форматах. Без єдиного прошарку обробки це перетворюється на хаос, який важко контролювати.

Архітектура розумного керування даними

Cribl створено саме для того, щоб упорядкувати хаос у потоках даних. Це гнучкий маршрутизатор і трансформатор телеметрії, який стоїть між джерелами даних і системами спостереження чи аналітики.

Його головна місія — не збирати все підряд, а дати змогу визначити, які дані куди мають іти, у якому вигляді та з якою цінністю.

Cribl об'єднує кілька ключових функцій:

- **збір даних** з будь-яких джерел (логи, телеметрія з агентів, API, мережеві потоки);
- **обробка і маршрутизація** в реальному часі — нормалізація, фільтрація, анонімізація, агрегування;
- **зберігання у CriblLake** — ефективному сховищі для «сирих» даних, доступних для подальшого відтворення чи аудиту;
- **доставка до систем аналітики** — Splunk, Elastic, Datadog, Sentinel, OpenSearch тощо.

Завдяки цьому компанія отримує контроль над усім життєвим циклом даних — від збору до аналізу.

Від «індексуй усе» до «керуй потоком»

У минулому компанії будували свої системи спостереження за принципом «збирай усе — аналізуй потім» (**рис. 1**). Але із зростанням обсягів даних цей підхід став надто дорогим і повільним.

Новий підхід, який реалізує Cribl, передбачає, що дані обробляються до того, як потрапляють у систему зберігання чи аналізу (**рис. 2**). Тобто компанія може контролювати

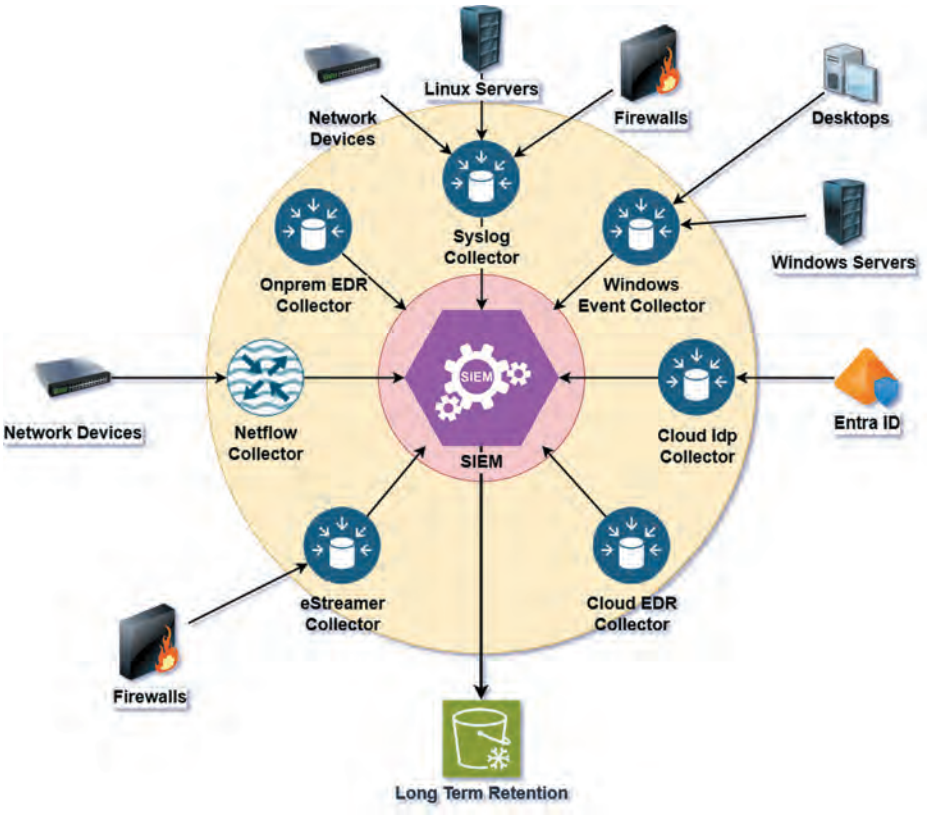

Рис. 1. До: класична архітектура SIEM. Усі джерела даних надсилають телеметрію безпосередньо до SIEM, створюючи навантаження, дублювання даних і високі витрати на зберігання

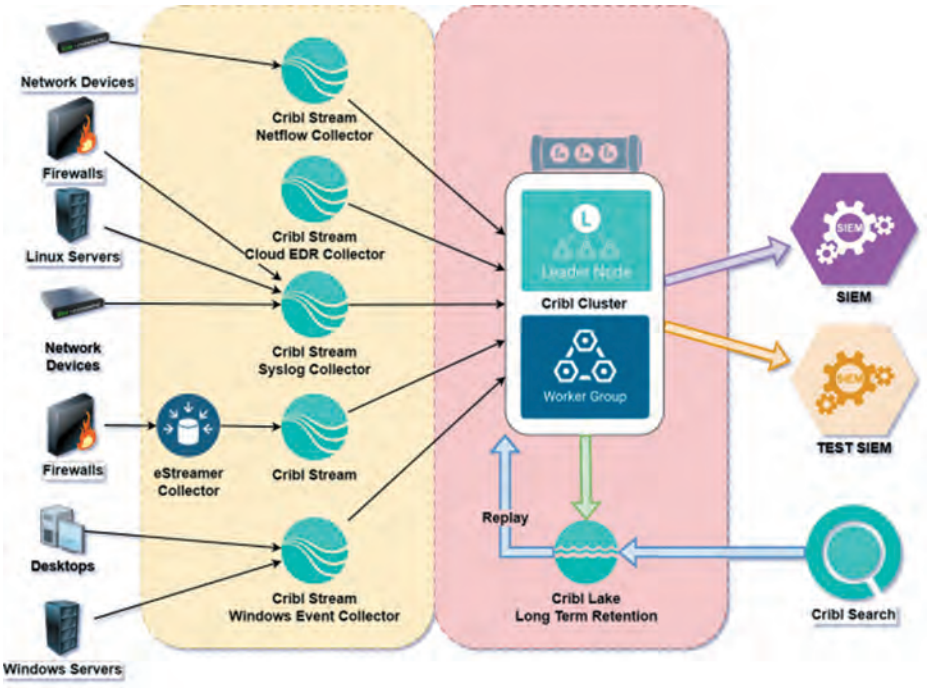

Рис. 2. Після: архітектура з Cribl. Cribl виступає інтелектуальним прошарком між джерелами даних і системами аналітики, забезпечуючи маршрутизацію, фільтрацію, зберігання та повторне використання телеметрії.

не лише те, що вона зберігає, а й як це впливає на витрати та ефективність. Таким чином, Cribl створює «розумний шар observability» — рівень, який забезпечує прозорість, гнучкість і масштабованість у роботі з телеметрією.

Cribl у службах безпеки та SOC

Для команд безпеки Cribl стає стратегічним елементом інфраструктури. Завдяки можливості фільтрувати і збагачувати події ще до надходження у SIEM SOC-команди отримують менше шуму і швидше реагують на інциденти.

Крім того, Cribl дозволяє маскувати або видаляти чутливі дані — це критично для організацій, що працюють у сфері фінансів чи охорони здоров'я або в державному секторі. Також платформа спрощує дотримання вимог GDPR, ISO 27001, PCI DSS, оскільки забезпечує прозоре керування даними та можливість відтворення історичних логів для аудиту.

Те, що працювало до 2025 року, не працюватиме у 2035-му

У найближчі роки ключовим трендом стане **smart observability** — підхід, за якого дані не просто збираються, а обробляються і маршрутизуються ближче до джерела свого виникнення. Це означає, що системи аналітики й безпеки отримуватимуть лише ті дані, які мають реальну цінність, а не терабайти «сирого шуму».

Для українських компаній цей тренд має особливе значення. Бізнес дедалі частіше переходить на гібридні та мультихмарні архітектури, де дані розподілені між датацентрами, хмарами та периферійними вузлами. У таких умовах важливо мати рішення, яке дозволяє зменшити залежність від дорогих сховищ, оптимізувати витрати на ліцензії та підтримку, але водночас не втратити контроль над безпекою і якістю даних, і Cribl чудово відповідає цим вимогам.

На ринку України рішення Cribl офіційно представляє iIT Distribution — компанія, яка має в своєму портфелі чимало інноваційних та всесвітньо визнаних виробників рішень у галузі кібербезпеки та побудови безпечної інфраструктури.

Як офіційний дистриб'ютор **Cribl**, **iIT Distribution** *надає комплексну підтримку на всіх етапах — від консалтингу й пілотного впровадження до розгортання проєктів.*

Для отримання детальної інформації звертайтеся за контактами:
+38 (044) 339 91 16,
sales.ua@iitd.ua
Офіційний сайт:
https://iitd.ua/