NetDescribe

NetDescribe Use Case

SIEM Migration | Effizientes Event Pipelining beim Umzug in die Cloud

mit Cribl

www.**netdescribe**.com

1. Die Ausgangssituation

Der Kunde hat aktuell Splunk und Splunk Enterprise Security als SIEM erfolgreich im Einsatz. Es besteht eine über Jahre “gewachsene” Splunk Umgebung mit zahlreichen Custom AddOns wie z.B. SAP. Ebenso sind viele verschiedene Datenquellen angebunden. Nicht zu vergessen, die ausgebildeten Splunk User und Admins sowie die vielen etablierte Prozesse.

Aufgrund eines Herstellerwechsels zu Azure Sentinel sollte die bestehende Lösung ausgetauscht werden. Die Migration musste vor einem sehr knappen Zeithorizont von ca. drei Monaten erfolgen.

Wie können Datenströme störungsfrei erfasst und weitergeleitet werden?

Cribl ist eine herstellerunabhängige Plattform, die Kunden die Flexibilität bietet, Daten von jeder Quelle zu jedem Ziel zu leiten, zu formen, umzustrukturieren und anzureichern, ohne neue Agenten hinzuzufügen. Cribl verarbeitet Daten, indem es Störfaktoren eliminiert und im Gegenzug dazu beiträgt, wertvolle Daten länger zu erhalten, ohne das Infrastruktur-Budget des Kunden zu sprengen. Mit Cribl ist es möglich eine original-getreue Kopie der Rohdaten an einen kosten-günstigen Speicherort zu leiten, um sie für Compliance- und Audit-Zwecke langfristig aufzubewahren, und sie an Analysetools weiterzuleiten.

Der Schlüssel: Vollständige Kontrolle über Ihre Observability-, Security- und Telemetriedaten!

Viele Unternehmen kämpfen damit, wachsende Datenmengen zu analysieren, ohne eine neue Infrastruktur aufbauen zu müssen.

Die Komplexität der Tools und die Bindung an einen bestimmten Anbieter erschweren das Senden von Daten an Analyseplattformen von Drittanbietern.

Security Teams werden mit Daten aus verschiedenen Quellen und Formaten überschwemmt. Das macht es schwierig, Events zu korrelieren und somit Sicherheitslücken zu erkennen und darauf zu reagieren. Hinzu kommt die Einhaltung von Datenschutz- und Compliance Richtlinien.

Die dabei entstehende Herausforderung für Unternehmen ist ein stetig steigender Ressourcen-verbrauch, immer höhere Anforderungen an das Datenmanagement und die Datenanalyse sowie ein erheblicher finanzieller Aufwand.

Cribl - Feature Highlights + Easy Handling

Quickconnect - Streamen Sie Quellen zu Zielen durch einfaches Drag-and-Drop. Einfachere und schnellere Datenübernahme und Weiterleitung von Punkt A nach Punkt B.

Flex-Deploy - Vor Ort, in der Cloud oder hybrid. Wählen Sie das Modell, das Ihren Anforderungen am besten entspricht.

Nutzen Sie das **Release-, Versions- und Archive-Management** zum Tracking von Konfigurationsänderungen zur Sicherstellung der **Auditierbarkeit**.

Synthetisches Testen (Replay) - Nach einer Änderung können Data Samples aus einer Low Cost Storage nochmal durchgespielt werden, um Fragen zu beantworten, die Sie nicht im Voraus vorhergesehen haben.

2. Der Use Case

Das Unternehmen aus der Medienbranche ist einer der führenden Entertainment- und E-Commerce-Anbieter im deutschsprachigen Raum. Ergänzt wird das Entertainment-Portfolio durch digitale Verbrauchermarken in den Segmenten Commerce & Ventures sowie Dating & Video.

Die Vorgabe der Geschäftsführung lautete: “Die SIEM Lösung muss durch Microsoft Azure Sentinel ersetzt werden und zwar innerhalb von drei Monaten.”

Die Lösung von NetDescribe

Cribl und NetDescribe zeigen Ihnen, wie Sie Ihr Datenmanagement sofort vereinfachen können und der Umzug in die Cloud zum Erfolg wird.

Die Daten-Engine von Cribl unterstützt Sie bei der Analyse, Erfassung, Verarbeitung und Weiterleitung Ihrer Daten in jeder Größenordnung. Erfahren Sie auf den folgenden Seiten, wie NetDescribe und das Cribl-Portfolio Ihnen die Auswahl, Kontrolle und Flexibilität bieten, um Ihre IT- und Sicherheits-abläufe jetzt und in Zukunft zu unterstützen.

Die Cribl-Familie

Cribl Stream™ - unterstützt Sie bei der Verarbeitung von Maschinendaten – Protokollen, Messdaten, Anwendungsdaten, Metriken usw. – in Echtzeit und übermittelt sie an die Analyseplattform Ihrer Wahl.

Cribl Edge™ - hilft Ihnen bei der Erfassung und Verarbeitung von Observability-Daten. Sie können Protokolle, Metriken, Anwendungsdaten usw. in Echtzeit von Ihren Linux- und Windows-Rechnern, Apps, Microservices etc. an Cribl Stream oder ein beliebiges unterstütztes Ziel liefern.

Mit **Cribl Search™** können Sie Maschinendaten – Protokolle, Instrumentierungsdaten, Anwendungsdaten, Metriken usw. – suchen, untersuchen und analysieren, ohne sie vorher in einen speziellen Speicher zu verschieben. Dies kann mit Daten geschehen, die sich auf Cribl Edge oder in einem Data Lake wie Amazon S3 befinden.

Die Timeline

13. Juli 2023
Cribl PoC

August 2023
Installation
Cribl Cluster
(4 Worker + 1 Leader)

August-Oktober 2023
Cribl Packs,
Routes, ND-Snap

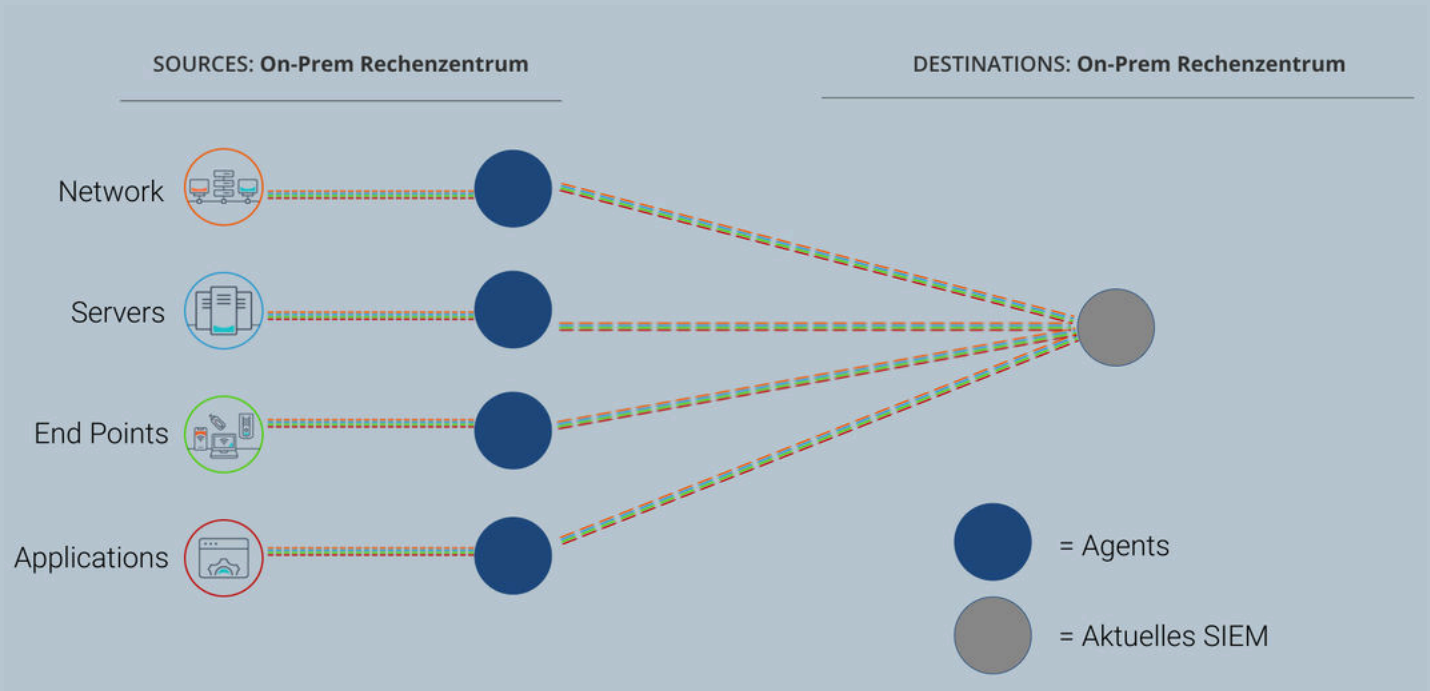
31. Oktober 2023
GO LIVE

3. Anforderungsanalyse und Umsetzung

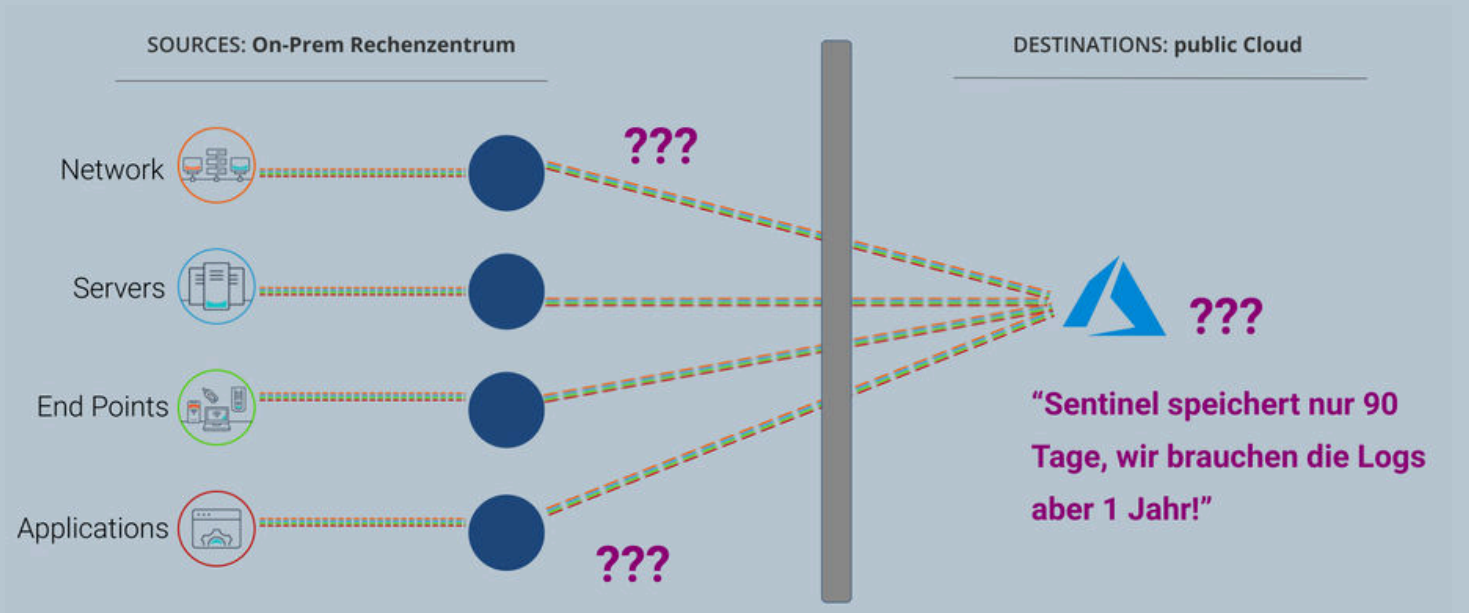
Der SIEM Wechsel von Splunk auf Azure Sentinel innerhalb von drei Monaten stellte das Team von NetDescribe vor eine interessante Herausforderung. Nach einer ersten Anforderungsanalyse wurde Cribl als “Datendrehscheibe” vorgestellt. Daraufhin entschied sich der Kunde sofort für einen Proof of Concept. Innerhalb kürzester Zeit wurde Cribl on prem installiert und die vorhandene Splunk Umgebung wurde so angepasst, dass aktuelle Daten zusätzlich an Cribl geschickt und von dort optimiert an das neue SIEM System weitergeleitet werden.

Technische Parameter:	**Anzuschliessende Datenquellen:**
• 500 GB Log Volumen pro Tag • über 1500 Splunk Forwarder (Agents) im Einsatz • über 200 Security Use-Cases aktiviert	• diverse Server Logs (Linux, Windows...) • Firewall Logs • Cloud Daten • Applikationen

In der **Ausgangssituation** waren alle Sources (Network, Services, End Points und Applications) ebenso wie die Destination im On-Prem Rechenzentrum verortet und wurden über Splunk gesammelt und weitergeleitet.

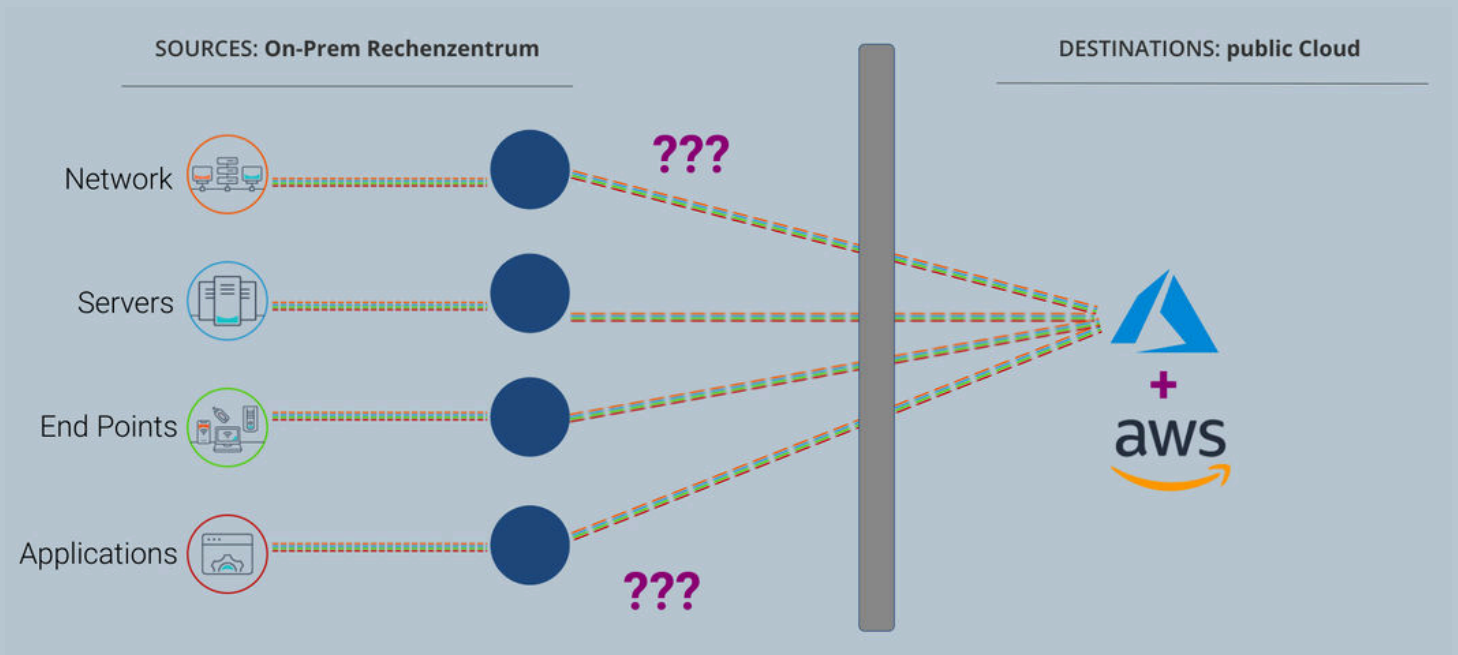


Die Frage: Wie sollte die **neue Zielumgebung,** die Destination, aussehen? Fest stand, sie würde sich in einer Public Cloud befinden. Aber wie konnten die Daten dorthin migriert werden?

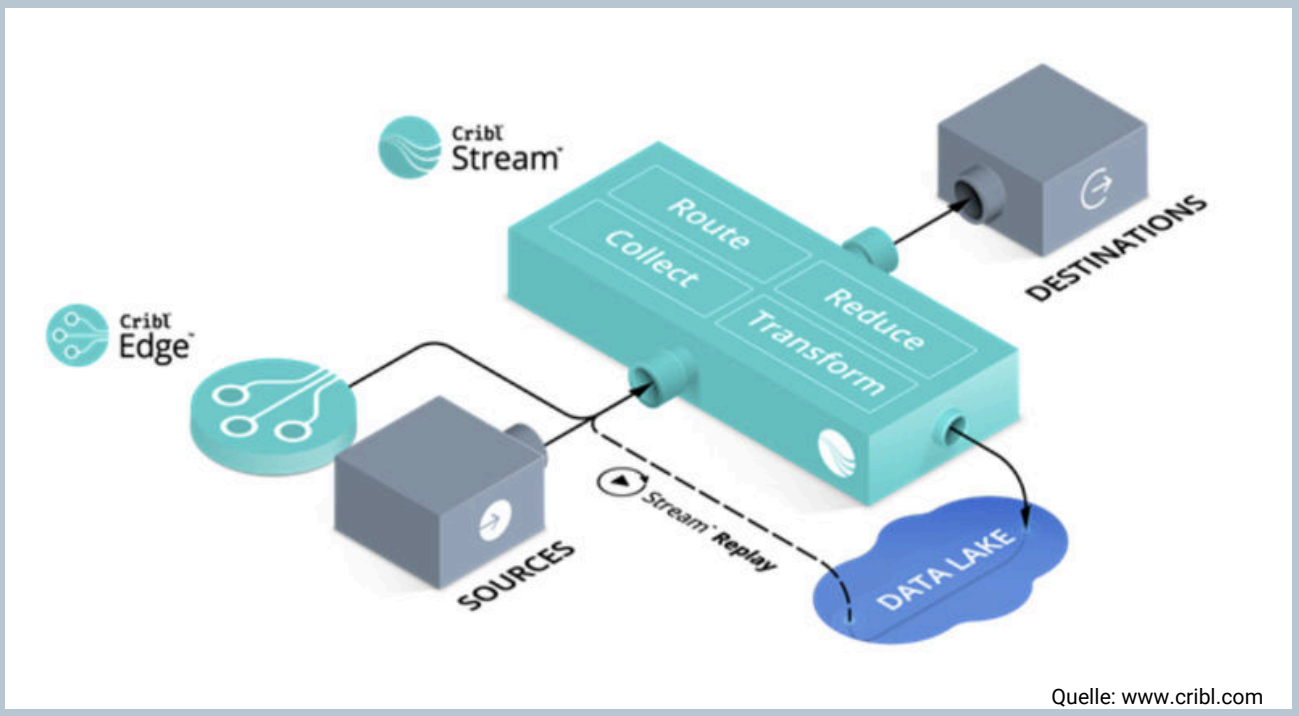


Eine weitere Herausforderung waren die **Richtlinien zur Datenspeicherung**. Azure Sentinel speichert nur 90 Tage, die Logs wurden aber ein Jahr lang benötigt.

Die **Lösung:** Eine zusätzliche Anbindung der S3 Speicher (Data Lake) über Cribl nach aws.

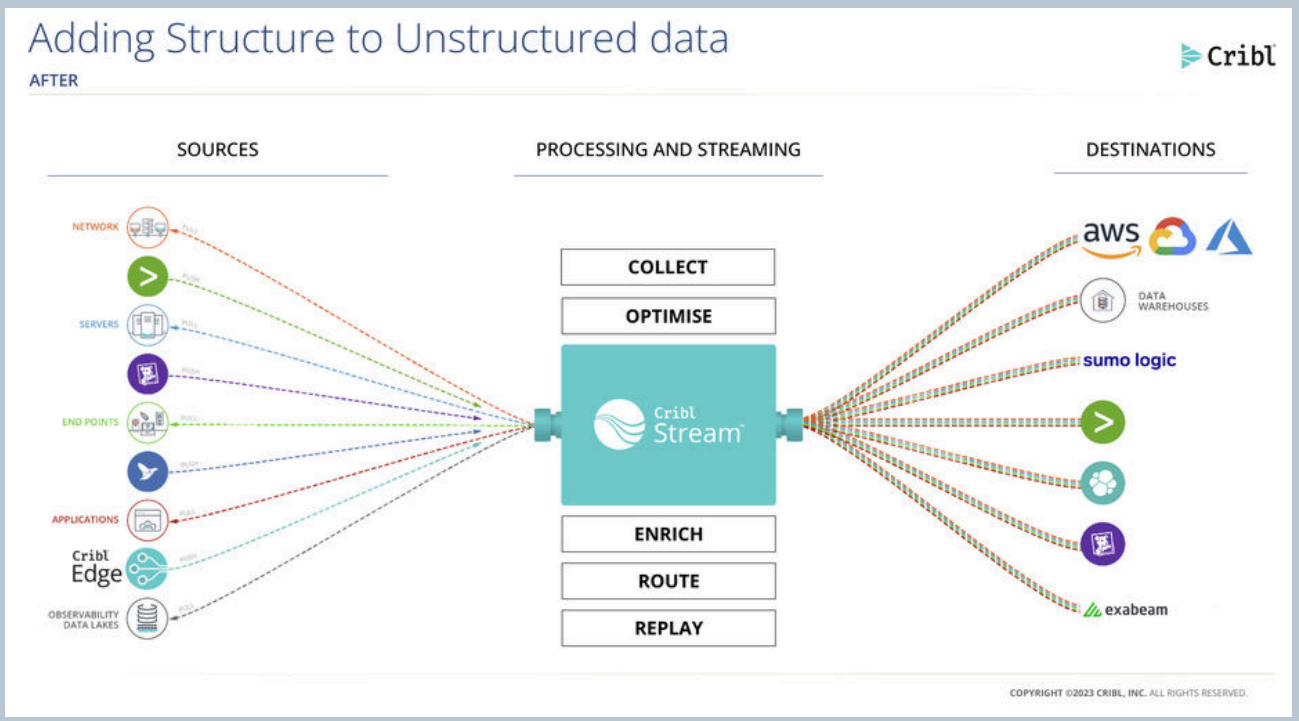


Und an dieser Stelle kommt Cribl Stream ins Spiel und sorgt für die effiziente Verarbeitung von Protokollen, Metriken, Traces, IT- und sicherheitsrelevanten Daten in Echtzeit. Es bietet Teams die Flexibilität, die gewünschten Daten zu sammeln, sie in die gewünschten Formate zu bringen, sie genau dorthin zu senden, wo sie benötigt werden, und die Daten bei Bedarf wiederzugeben (Replay).

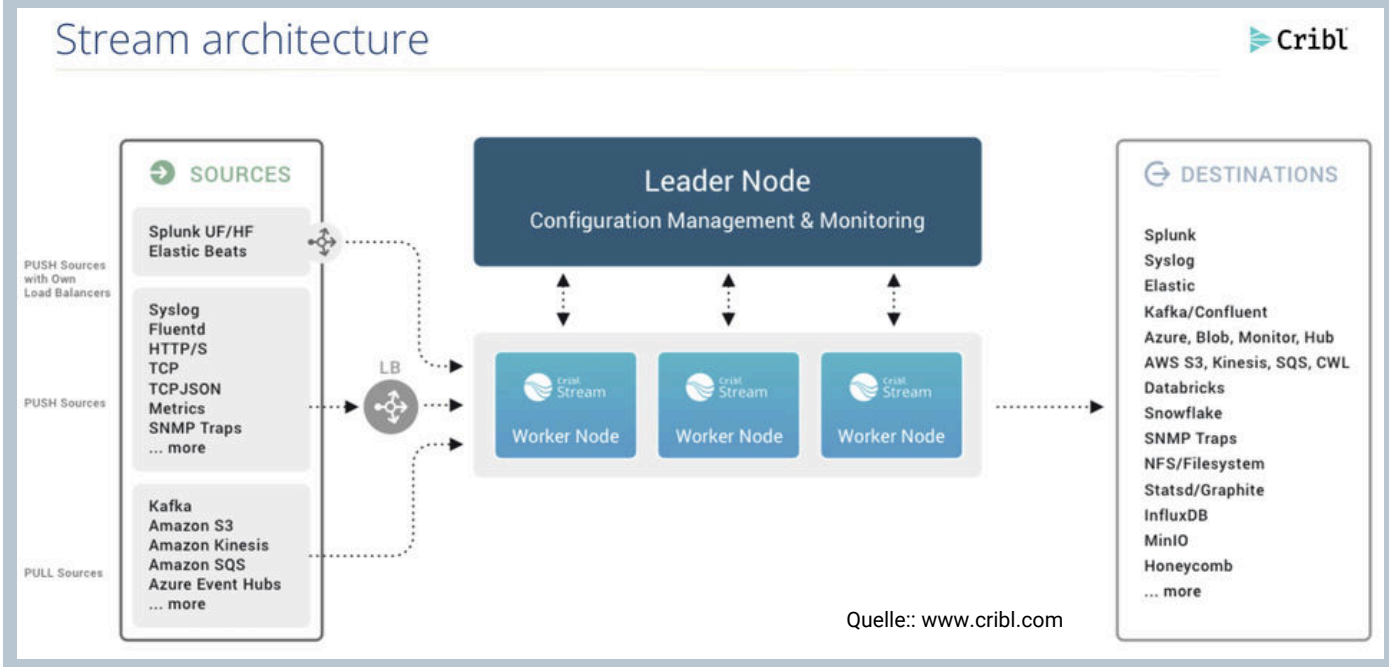


Quelle: www.cribl.com

Cribl Stream im Detail zeigt den großen Vorteil des Produkts. Es “versteht” von Haus aus bereits viele Sources und kann diese ansteuern, was einen geringeren Konfigurationsaufwand und damit Zeit- und Kostenersparnis bedeutet.

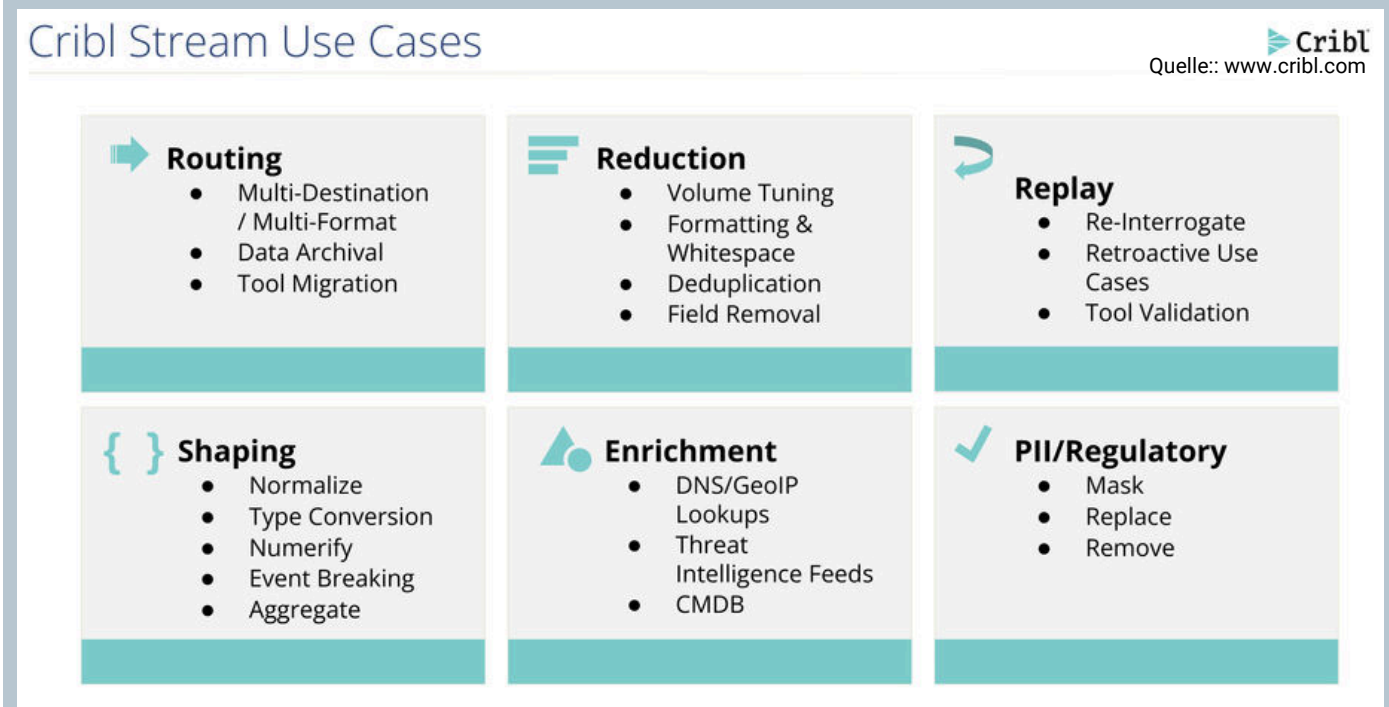


Und für alle Technikfans gehen wir hier noch einen Schritt weiter in die hochskalierbare Architektur.
Stream kann Push-Daten von Quellen wie Splunk, HTTP, Elastic Beats, etc. empfangen und Daten von Kafka, Kinesis Streams, S3, etc. oder sogar externen Inputs wie Wetterdaten, Luftqualität und allem anderen abrufen. Streamen Sie Daten an Splunk, AWS Kinesis Streams, etc., sowie an Ziele, die Batch- oder Non-Streaming-Ausgaben unterstützen, wie S3-kompatible Speicher, Dateisystem/NFS, MinIO, Google Cloud Storage und Azure Blob Storage.



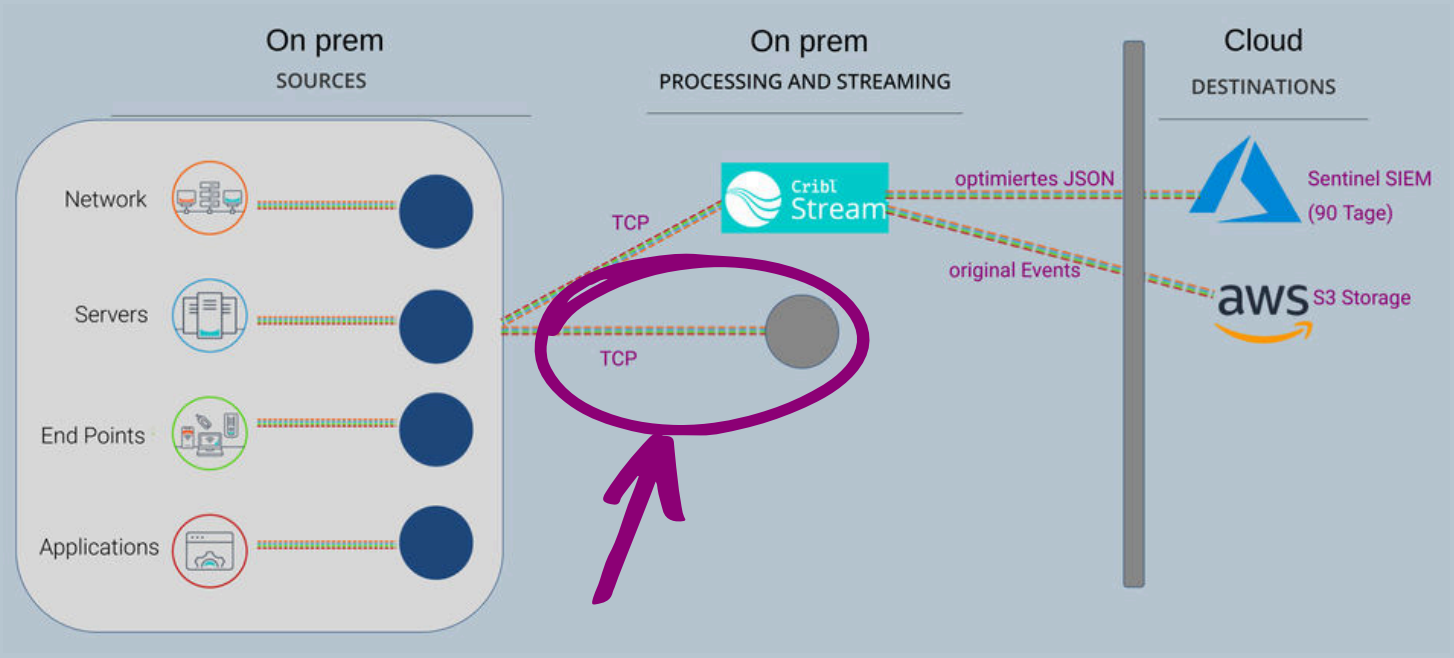
Quelle:: www.cribl.com

Cribl Stream maximiert den Wert Ihrer Observability-Daten, indem es Daten aus anderen Quellen in Echtzeit umwandelt und mit Kontext versieht und so den Wert Ihrer Analysetools steigert.
Ganz nach Ihren Bedürfnissen!

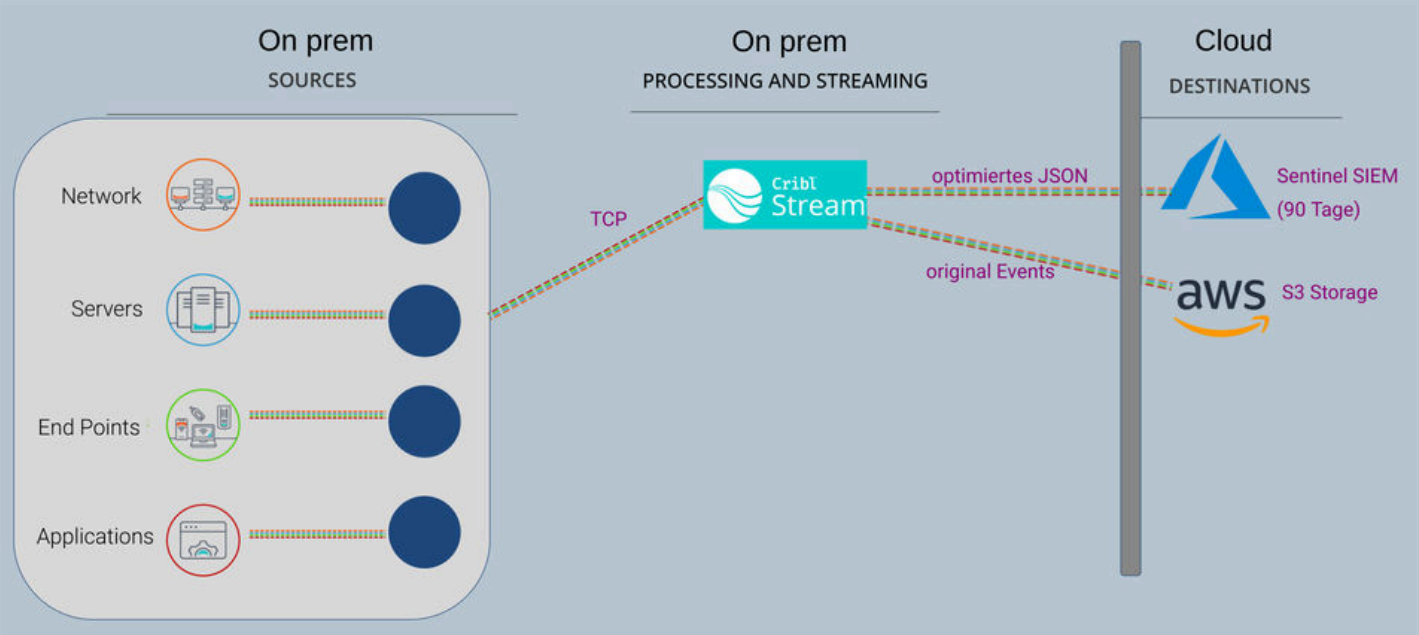


Quelle:: www.cribl.com

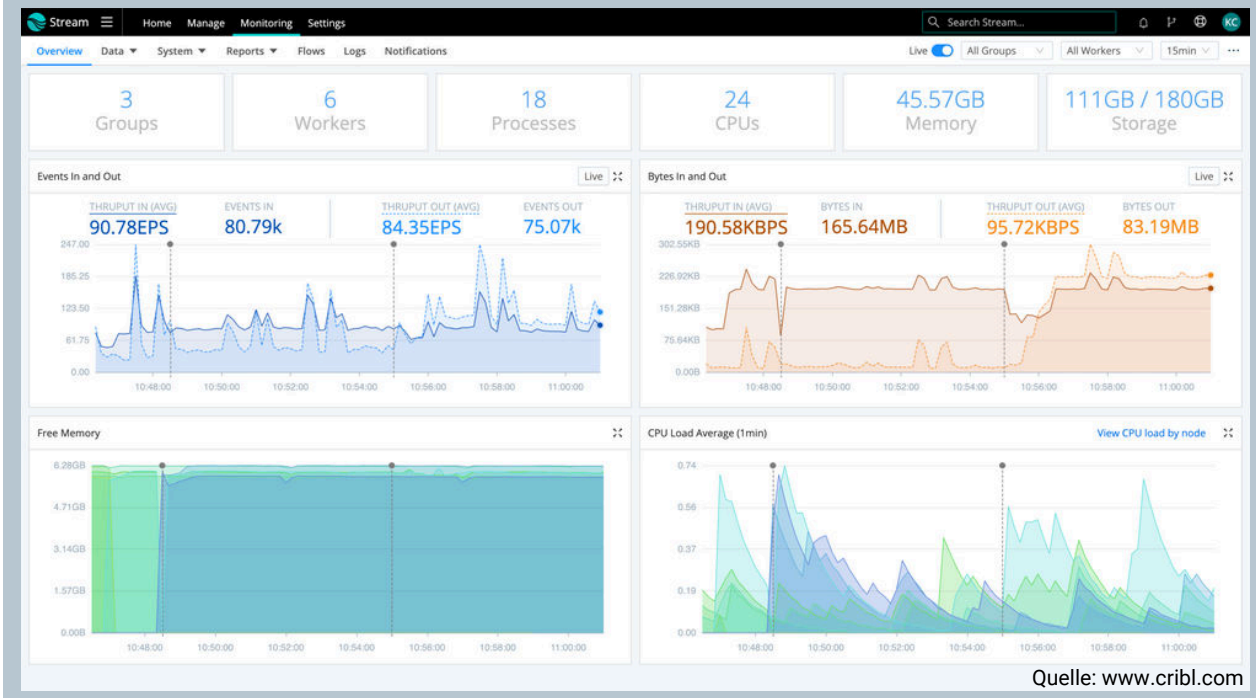
In der **Migrationsphase** wurden die Daten dupliziert und parallel an zwei Destinations geschickt:
ALT: Splunk und NEU: Azure Sentinel + S3 Storage



Ergebnis: Die alte Splunk Lösung wurde dekommissioniert und alle Events über Cribl in die Cloud-Platform gestreamt. Damit war das Ziel des Umzugs auf die neue SIEM-Lösung in der Cloud vollzogen.

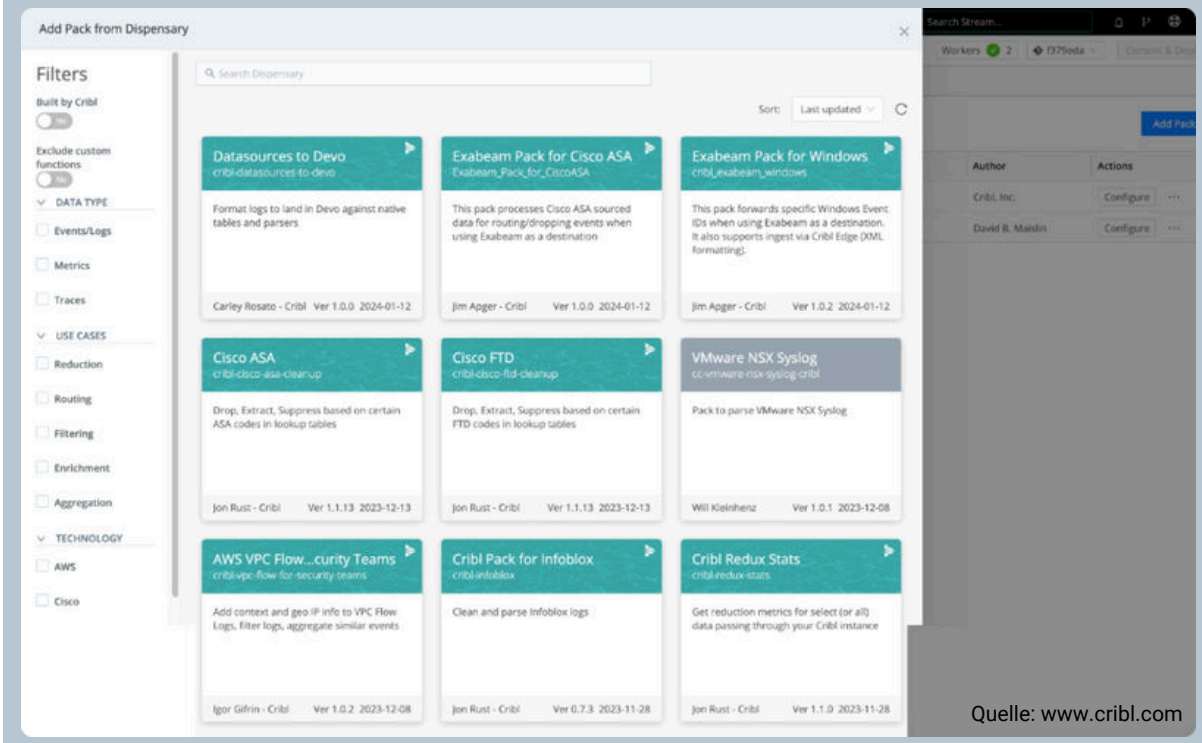


Das **Monitoring-Dashboard** ist eine einzige Quelle der Wahrheit für alle IT- und Sicherheitsdaten, die durch Stream fließen. Cribl Stream bietet Benutzern eine Vogelperspektive auf ihre Daten - von der Quelle bis zum Ziel. Mit wenigen Klicks können Benutzer detaillierte Dashboards aufrufen, die Datenverkehr, Erfassungsaufträge, Aufgaben und allgemeine Systemmetriken anzeigen.



Quelle: www.cribl.com

Cribl Packs bieten Stream-Benutzern mit vorgefertigten Routen, Pipelines, Beispielen, Lookups und Knowledge Objects einen sofortigen Mehrwert. Sehen Sie sofort die Einsparungen, ohne einen einzigen Ausdruck, eine Regex oder ein Lookup zu schreiben.

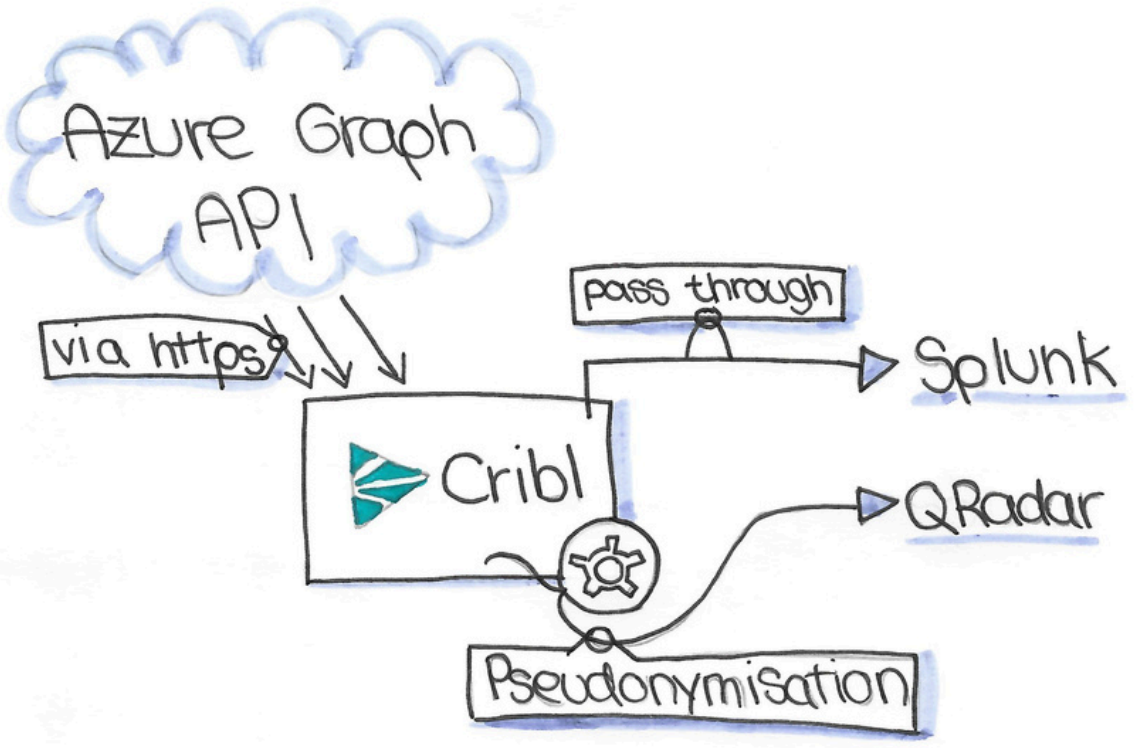


Quelle: www.cribl.com

4. Die Ergebnisse

- Alle jahrelang in Splunk konfigurierten, kontinuierlich angepassten und optimierten Regeln zur Datenaufbereitung konnten sehr einfach in Cribl übernommen werden.
- Datenanreicherungen wurden von Splunk nach Cribl problemlos portiert.
- Maximale Zeitersparnis bei der Anbindung der Datenquelle. Ohne Cribl wäre der Aufwand wesentlich höher gewesen und hätte, statt weniger Tage, mehrere Monaten in Anspruch genommen.
- Einziger Aufwand für den Kunden war die Übertragung der SIEM Regeln aus Splunk zu Azure Sentinel. Durch gleiche Feldzuordnungen in Splunk und Azure Sentinel war mit Cribl ein effizienter und schneller Umstieg möglich.
- Die gewonnene Unabhängigkeit von einem bestimmten Hersteller eröffnet nun flexible Möglichkeiten, um zukünftige Herausforderungen zu meistern.

Der Einsatz von Cribl “kinderleicht” erklärt:



Quelle: Matilda Barth - Tochter unseres Mitarbeiters Martin Barth

Cribl - Business Benefits

Mit Cribl erhalten Sie die vollständige Kontrolle über alle Observability-Daten und eine nie dagewesene Flexibilität bei der Verwendung beliebiger Tools ohne den Einsatz neuer Agenten.

Keine Agentenüberlastung Sie müssen keine zusätzlichen Agenten laden
Keine Datenüberlastung Sie können große Datenmengen bewältigen
Keine Bandbreitenbeschränkungen Sie reduzieren Ihre Übertragungskosten
Langfristige Aufbewahrung Definieren Sie die Aufbewahrung nach Ihren Anforderungen
Onboarding unbekannter Datensätze Schnelles Onboarding von neuen Datenquellen mit visuellen Tools

„Überprüfen Sie Ihre Observability Daten in Echtzeit und ohne Limit."
Alexander Hauptner, Cribl-Experte bei NetDescribe

Die Cribl Stream™ Funktionen auf einen Blick

Cribl Stream fungiert als universeller Empfänger und Sammler von Protokoll- und Metrikdaten. Mit Stream können Sie Daten aus jeder beliebigen Quelle abrufen, umwandeln, analysieren und korrelieren und sie an jedes beliebige Ziel oder sogar an mehrere Ziele senden, ohne dass zusätzliche Tools erforderlich sind.

Stream kann Push-Daten von Quellen wie Splunk, HTTP, Elastic Beats, Kinesis, Kafka, TCP JSON empfangen und Daten von Kafka, Kinesis Streams, Azure Event Hubs, SQS, S3, Microsoft Office 365 oder sogar externen Inputs wie Wetterdaten, Luftqualität und allem anderen, was Ihr Unternehmen für bessere Entscheidungen benötigt, abrufen.

Streamen Sie Daten an Splunk, AWS Kinesis Streams, SQS und CloudWatch Logs, Elasticsearch, Honeycomb, TCP JSON, Syslog, Kafka Azure Event Hubs und Monitor Logs, StatsD und StatsD Extended, Graphite, InfluxDB, Wavefront, SignalFx und mehr, sowie an Ziele, die Batch- oder Non-Streaming-Ausgaben unterstützen, wie S3-kompatible Speicher, Dateisystem/NFS, MinIO, Google Cloud Storage und Azure Blob Storage.

Cribl Stream maximiert den Wert von Observability-Daten, indem es Daten aus anderen Quellen in Echtzeit umwandelt und mit Kontext versieht und so den Wert Ihrer Analysetools steigert.

Collect – Senden Sie Daten von jedem Ort an jeden Ort.
Reduce – Eliminieren Sie nutzlose Daten, um Kosten zu kontrollieren. Sie können eine originalgetreue Kopie an einem kostengünstigen Zielort aufbewahren und sie bei Bedarf wieder aufspielen.
Shape – Gewinnen Sie aussagekräftige Erkenntnisse aus Ihren Daten.
Route – Nutzen Sie Ihre Daten da, wo sie den größten Wert haben und senden Sie die richtigen Daten an die richtigen Ziele.
Replay – Speichern Sie Ihre Daten für den Tag X an einem kostengünstigen Speicherort und rufen Sie sie bei Bedarf ab, um die Sicherheit zu erhöhen, sowie Betriebsstörungen und -ausfälle zu vermeiden.