Optimierung von Security Information & Event Management (SIEM) Lösungen

NetDescribe und die Confluent Platform holen zusammen mit Ihnen das meiste aus Ihrer SIEM-Lösung heraus:

CYBER SECURITY ANALYTICS PLATFORM

> Höhere Qualität
> Mehr Flexibilität
> Erhebliche Kostenreduzierung

So können NetDescribe und die Confluent Platform (basierend auf Apache Kafka®) bei der Modernisierung von SIEM / CIP-Lösungen helfen:

Hintergrund
Die Vielfalt der Cyber Bedrohungen wächst. Dazu gehören Angriffe oder Versuche, die Datenbestände einer Organisation aufzudecken, zu verändern, zu deaktivieren, zu zerstören, zu stehlen oder sich unbefugten Zugang zu beschaffen.

Security Information & Event Management (SIEM), manchmal auch **Cyber Security Analytics Platform (CSAP)** genannt, sind entstanden, um diese Bedrohungen aufzudecken und ihnen vorzubeugen.

SIEM / CSAP-Lösungen sammeln und aggregieren Log-Daten, die über das Netzwerk und die technologische Infrastruktur generiert werden, um Analysen und Einblicke zu ermöglichen.

- ★ Viele alte SIEM-Lösungen, die heute noch in Unternehmen eingesetzt werden, können mit dem Tempo und der Komplexität aktueller Bedrohungen nicht mehr Schritt halten.
- ★ Darüber hinaus werden neuere SIEM-Lösungen oft nach einem Pay-per-Ingest Modell berechnet, was zu explodierenden und unvorhersehbaren Kosten führen kann.

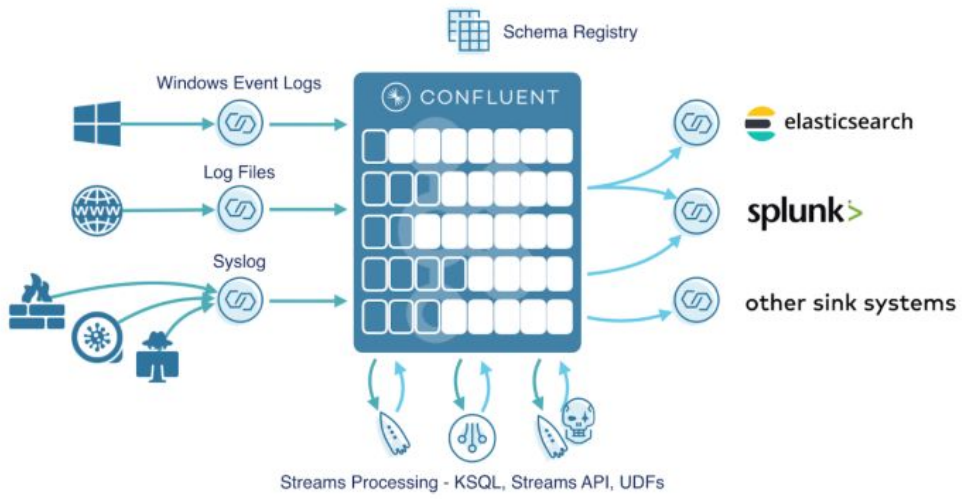
Die Nutzung von Confluent Platform (basierend auf Apache Kafka®) in Kombination mit den Professional Services und dem Training von Confluent, sowie der Expertise von NetDescribe bietet klare Vorteile:

Qualität: Aufnahme, Aggregation und Speicherung einer vielseitigen und wachsenden Anzahl von Security Events / Sensordaten in einer einzigen verteilten, skalierbaren und beständigen Plattform; kombiniert mit der Transformation, Verarbeitung und Filterung von Daten in geordnete Ströme zur umfassenderen Erkennung, Untersuchung und Echtzeitanalyse von Bedrohungen.

Flexibilität: Aggregierte Daten können an jede verbunde Quelle gesendet und damit geteilt werden, einschließlich SIEM-Indizes, Suchanwendungen, benutzerdefinierte Anwendungen oder ML/AI-Modelle.

Kostensenkung: Der Datenverkehr wird erheblich reduziert und neue Consumer können effizienter und schneller als je zuvor integriert werden.

Funktionalität von Confluent Platform in SIEM



Abwehr von Cyber Bedrohungen auf höchstem Level:

> Erfassung von Netzwerk-Event(s)

> Daten werden angereichert, normalisiert & konvertiert

> Daten werden ins System zur Erkennung von Bedrohungen geladen

> Bedrohungssuche führt zur Entdeckung von Mustern

> Analyse-Dashboarding

> Automatische Erkennung von Bedrohungen mit Entscheidungsfindung / automatische Aktionen in Echtzeit

Höhere Qualität: Die Datenerfassung erfolgt in Leitungsgeschwindigkeit und ermöglicht die Erkennung von Bedrohungen, die zuvor nicht identifiziert wurden, da herkömmliche Ingest-Ansätze mit den ständig wachsenden Datenmengen nicht mehr Schritt halten können.

Mit der Zeit werden Unternehmen mit neuen Bedrohungen konfrontiert. Confluent Platform unterstützt die Analyse historischer Daten.

Neue Anwendungen können Daten direkt nutzen. Es besteht keine Notwendigkeit, weitere Silos hinzuzufügen, die Daten für individuelle Anwendungsanforderungen enthalten.

Mehr Flexibilität: Die Normalisierung von Daten ist schneller und effizienter. Filter können, einmal an einer Stelle gesetzt, für die gesamte Datenerfassung angewendet werden. Dadurch wird der Betrieb der SIEM-Plattform vereinfacht.

Neue Use Cases, Anwendungen und Dienste können viel schneller bereitgestellt werden.

Kosten- und Time-to-Market-Reduzierung: Das Onboarding neuer Systeme in SIEM wird erheblich reduziert, da die Confluent-Lösung eine schnellere Anbindung neuer Systeme ermöglicht.

Erhebliches Reduktionspotential für die Aufnahme in bestehende SIEM-Lösungen, wodurch die Lizenzkosten für Pay-per-Ingest verringert werden. Häufig macht sich die damit verbundene Kostenreduzierung für die gesamte Plattform-Modernisierung mehr als bezahlt.

Zusammenfassung aus Business-Sicht

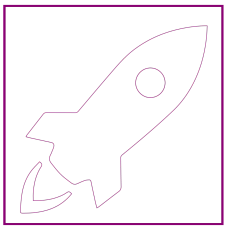
Dank der Vorteile von Confluent Platform können Unternehmen ihre Ausfallsicherheit (Cyber Resilience) erhöhen und gleichzeitig unter anhaltenden Bedrohungen und perfiden Angriffen kosteneffizient arbeiten.

In Anbetracht der verbesserten Qualität, der erhöhten Flexibilität und der reduzierten Kosten von SIEM / CSAP, werden die wahren Geschäftsvorteile an der Risikovermeidung gemessen - die schwer zu quantifizieren sein kann, ähnlich wie die Ausgaben für Versicherungsprämien.

Außerdem können Kunden durch die Verbesserung der SIEM-Plattform die von der BAFIN, dem BSI und anderen Organisationen vorgegebenen Compliance Vorschriften einhalten.

Die nächsten Schritte hin zu Ihrer SIEM-Modernisierung

Schritt 1: Innovations-Workshop (Präsentation + Demo) > 0,5 Tage
Schritt 2: Technischer Check-Up SIEM & Scoping > ½ - 1 Tage
Schritt 3: Business Value Workshop zur Quantifizierung des erwarteten Nutzens für das Unternehmen



Zielsetzung	Detail	Wertschöpfung & Ergebnis
> Kennenlernen der Business-Technologie-Treiber und des Use Cases, um eine Lösungsarchitektur und einen Implementierungsentwurf vorzuschlagen	> Geführte Diskussionen und Workshop > Teilnehmer aus Infrastrukturbetrieb und Anwendungsentwicklung	> Optimierter Entwurf der SIEM-Plattform > High-Level Architektur > High-Level Empfehlungen und Maßnahmen > Maßgeschneiderter Implementierungsplan

CONFLUENT

Confluent wurde von den ursprünglichen Entwicklern von Apache Kafka® gegründet und bietet mit Confluent Platform die vollständigste Version von Kafka. Confluent Platform verbessert Kafka mit zusätzlichen Open-Source- und kommerziellen Funktionen, die entwickelt wurden, um das Streamen von Daten in Produktion für Betreiber und Entwickler optimal zu gestalten.
Apache Kafka® ist eine verteilte Event-Streaming-Plattform, die mehrere Billionen Events pro Tag verarbeiten kann.