Optimizing Security Information & Event Management (SIEM) solutions

Learn how NetDescribe and Confluent Platform can help you get the most value out of your SIEM Solution:

CYBER SECURITY ANALYTICS PLATFORM

> Improving quality
> Increasing flexibility
> Significantly reducing costs

How Confluent Platform (based on Apache Kafka® can help modernize SIEM / CSAP solutions:

Background
The cyberthreat landscape is growing. This includes attacks or attempts to expose, alter, disable, destroy, steal or gain unauthorized access to an organization's data assets.

Security Information & Event Management (SIEM), sometimes referred to as **Cyber Security Analytics Platform (CSAP)**, have risen in order to detect and help prevent these threats.

SIEM / CSAP solutions collect and aggregate log data, generated across the network and technology infrastructure, to provide analysis and insights.

- ★ Many legacy SIEM solutions running in enterprises today are failing to keep pace with the rate and sophistication of modern-day threats.
- ★ Furthermore, the more modern SIEM solutions are often charged on a pay-per-ingest model, which can result in escalating and unpredictable costs.

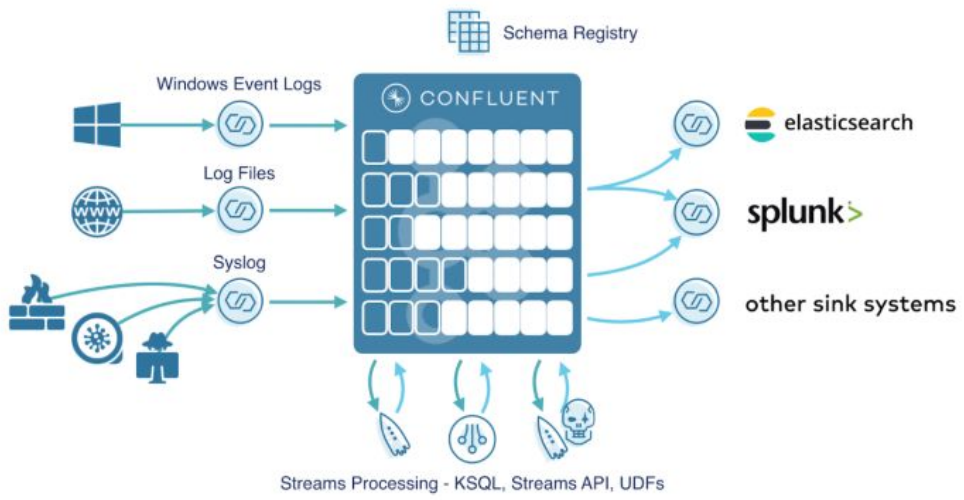
Inserting Confluent Platform (based on Apache Kafka®) combined with Confluent Professional Services (PS) & Training and NetDescribe's expertise delivers significant value:

Quality: Ingest, aggregate and store a diverse and growing set of security event/sensor data into a single distributed, scalable and persistent platform, combined with transform, process and filter data into curated streams for richer threat detection, investigation and real-time analysis.

Flexibility: Send and share aggregated data to any connected source, including SIEM indexes, search applications, custom applications or ML/AI models.

Cost Reduction: Data traffic will significantly be reduced and news consumers can be onboarded much faster than ever before.

How Confluent Platform works in SIEM



High-level cyber threat defense approach:

> Capturing of network events/event is captured

> Data enriched, normalized & transformed

> Data is loaded into the threat detection system

> Threat hunting leads to pattern discovery

> Analytics dashboarding

> Real-time automated threat detection, with decisioning / automated actions

Quality Improvement: Capture data at wire speed, enabling detection of threats that weren't previously detected, as conventional ingest approaches cannot keep up with ever-increasing data volumes.

Over time, organizations will experience new threats. Confluent Platform supports the analysis of historical data.

New applications can directly use data. There is no need to add more silos that host data for individual app requirements.

Flexibility: Normalization of data is faster and more efficient. Filters can be set once, in one place and applied for all data capture. This simplifies SIEM platform operations.

New use cases, applications and services can be provided much faster.

Cost & Time-to-Market Reduction: Onboarding of news systems into SIEM is significantly reduced because the Confluent solution offers to connect news systems more quickly.

Significant reduction potential for ingests into existing SIEM solutions - reducing the pay-per-ingest license costs. Often the cost reduction associated more than pays for the overall platform modernization.

Business Result Summary

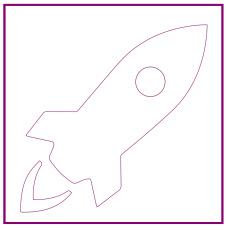
By leveraging the benefits of Confluent Platform, businesses can increase their cyber resilience, while operating under persistent threats and sophisticated attacks, in a cost-efficient manner.

Given the improved quality, increased flexibility and reduced costs of SIEM / CSAP, the true business benefits are measured in risk avoidance - which can be hard to quantify, much like spending on insurance premiums.

Also, by improving the SIEM platform, customers can achieve regulatory compliance given by BAFIN, BSI and other organizations.

Next steps with your SIEM modernization

Step 1: Innovator Workshop (Presentation + Demo) > 0,5 days
Step 2: SIEM technical discovery and scoping session > ½ - 1 day
Step 3: Business Value Workshop to quantify expected benefits for the business



Goal	Detail	Value / Outcome
> To understand the business-technology drivers and use case to propose a solution architecture and implementation blueprint	> Guided discussion and workshop > Attendees from infrastructure Operations and Application Development	> Optimized SIEM platform blueprint > High-level architecture > High-level recommendations and efforts > Tailored implementation plan

CONFLUENT

Confluent was founded by the original developers of Apache Kafka® and offers the most complete version of Kafka with Confluent Platform. Confluent Platform enhances Kafka with additional open source and commercial features designed to make streaming data in production optimal for operators and developers.

Apache Kafka® is a distributed event streaming platform that can handle trillions of events per day.