Optimize Your SIEM with Cloudera

SOLUTION BRIEF

Early detection of cyber threats and reduction of overall enterprise risks are not simple tasks. As the data center continues to become software defined, and workloads continue to flow across hybrid environments to take advantage of low-cost infrastructure, it becomes increasingly difficult to understand enterprise risks. From compliance to cybersecurity, enterprises are leveraging Security Information Event Management (SIEM) software to figure out how they can avoid cyber breaches. But even with a SIEM deployed, there is still much to be desired.

Costly to Increase Enterprise Visibility

Unfortunately for enterprises that have deployed a SIEM, the underlying proprietary platform can't scale to the volume or variety of information that is required in this hyper-connected world without running into technology or cost constraints. As enterprises require more information to increase visibility, they must not only pay SIEMs licensing fees for ingest and indexing but also continue to scale storage infrastructure costs to meet SLAs. These pressures force organizations to limit data retention rates to months instead of years.

Limited Analytics Flexibility

SIEMs are fantastic for descriptive and diagnostic analytics across a subset of information for real-time dashboards, however, search-based analytics limit data scientists and analysts. Building, tuning, and deploying advanced analytics and machine learning across years' worth of data goes well beyond SIEM's capabilities. Without a way to leverage open source analytic innovation at scale, enterprises struggle to build custom analytics applications within a SIEM's rigid framework.

SIEM Lock-In

Proprietary software, like SIEMs, requires a proprietary data storage and a specific SIEM data format, which makes it extremely difficult to break away from. Once all of your data is put into this format, only SIEM-certified apps can access and analyze the data. As data volumes grow and use cases expand, having application and analytic flexibility is critical in order to meet the needs of your organization.

Cloudera has helped countless organizations optimize their SIEM deployments by off-loading data, enriching the events with new data streams, and exposing long-term data for advanced analytics. Cloudera's open platform offers:

Cost-Effectively Increased Enterprise Visibility

Off-loading data from SIEM to Cloudera allows organizations to reduce their SIEM storage and indexing costs while increasing the volume and variety of data accessible for analytics. Landing data on Cloudera's platform and structuring it in the Apache Spot community's defined open data model allows organizations to break vendor lock-in, store multiple years' worth of data at a lower cost, and open up data ingest for any type of data. This expands enterprise visibility for smarter analytics and faster response times for potential risks. Deploying Cloudera's scalable platform on commodity hardware, or in any cloud environment, allows for lower-cost infrastructure—further reducing spend without sacrificing SLAs.

Analytic Flexibility

Optimizing SIEM with Cloudera allows organizations to open up analytic flexibility—from simple search to SQL to statistical analysis to machine learning. Executing these analytic techniques across larger volumes of diverse information allows organizations to significantly reduce IT and cybersecurity risk through earlier detection, investigation, and response. Deploying open source analytic libraries (Python, Scala, R) or partner technologies on Cloudera allows enterprises to continue to expand their analytic scope without having to re-platform for future advance analytics use cases.

Deploying Cloudera's cybersecurity solution allows organizations to:

- Accelerate time to incident investigation and response with comprehensive enterprise visibility
- Detect advanced threats faster by applying machine learning and artificial intelligence to larger enriched data
- Change the economics of cybersecurity with an open source platform that supports multiple line of business workloads

cloudera®

Deployment Flexibility

While SIEM can only be deployed on-prem or on AWS, Cloudera's platform can be deployed on-prem or across multiple clouds. This enables organizations to have a multi-cloud strategy in order to avoid cloud lock-in, avoid potential downtime, and easily migrate workloads between clouds to take advantage of low-cost environments. Spinning up transient clusters for specific data processing—or analytic use cases while being able to scale storage or compute independently—allows organizations to experiment fast without having to invest in up-front infrastructure costs.

Cloudera has already empowered organizations as they begin their journey to optimize their SIEM deployments and open up machine learning and advanced analytic use cases. Significantly reducing the cost of storing and ingesting their data with open source technology has allowed these organizations to expand their enterprise visibility, break vendor lock-in, and provide the analytics their enterprise requires.

Learn more about how Cloudera can optimize your SIEM deployments at www.cloudera.com/cybersecurity

Challenges by Role

CISO – Future proofing a strategy while balancing overall cyber risk exposure with enterprise constraints is not a trivial task

Security Engineer – Adding new data streams while scaling and integrating applications causes technology constraints

Incident Responders – Contextual and historic data is inaccessible in order to reduce the mean time to incident response

Security Analytics – Can't execute ad-hoc queries and large scale machine learning against enriched data for anomaly detection

About Cloudera

Cloudera delivers the modern platform for machine learning and advanced analytics built on the latest open source technologies. The world's leading organizations trust Cloudera to help solve their most challenging business problems by efficiently capturing, storing, processing and analyzing vast amounts of data.

Learn more at cloudera.com