Leading global solutions provider for communications and media	Location Global	Industry Cybersecurity	Size 25,000 employees

Deeper historical analytics with SQream DB

Speeding up HP ArcSight with a faster, easier to use GPU-powered analytics database

A global market-leader, providing customer experience software solutions and services deployed SQream DB alongside their existing HP ArcSight (SIEM) solution, to store more data and analyze historical data alongside live data at high speed.

This allows the vendor to continuously monitor incoming events, and detect anomalies as they happen, alert and respond to security threats.

The vendor was looking to increase data retention from a couple of months to a year, as well as improve event search capabilities.

- SQream Technologies created a custom connector for the HP ArcSight native format (CEF)
- The solution was implemented with a single 2U server, containing 40TB of raw data
- Deploying SQream DB allowed the vendor to avoid purchasing expensive hardware, saving hundreds of thousands of dollars while enhancing the performance of the HP ArcSight application
- SQream helped the vendor build a specialized visualization tool, which enables at-a-glance identification of anomalous events
- SQream DB is significantly faster than the existing solution – enabling the querying of trillions of events collected over a year in just a few seconds, compared with many minutes on a single months' data before SQream DB

CHALLENGE

HP ArcSight is a security analytics and intelligence software for Security Information Event Management, or SIEM. In a typical environment, various sources produce events and log events (e.g. endpoint users, security devices, databases, applications etc.).

Before deploying SQream DB, the vendor had extremely slow access to the insights, due to the design of the system. Additionally, these slow access times prevented query windows of over a couple of weeks, resulting in decisions being made only on short-term live data, instead of live data as well as historical data.

The system was ultimately not adequate for the requirements of near real-time response to issues, and was unable to meet the scalability requirement for the vendor's needs.

SOLUTION

The vendor chose to implement SQream DB for scale, speed and simplicity afforded by its market-leading GPU-based design. SQream DB is a high-performing, rapid, end-to-end analytics solution providing the vendor with the ability to identify anomalous events and issue alerts and warnings in a timely manner.

The new solution, built around SQream DB, pulls data directly from HP ArcSight using the SQream Technologies developed native HP Arc Sight connector. The solution retains HP ArcSight, adding SQream DB as a speed layer, which allows constant data flow between ArcSight and SQream DB.

The vendor is now able to avoid purchasing expensive hardware for improving the current system. With a leaner IT operation, there are now tangible savings on expenses while delivering new analytical capabilities. SQream DB ingests tens of billions of records per day, and can query both live and historical data at the same time, 10x faster than before.

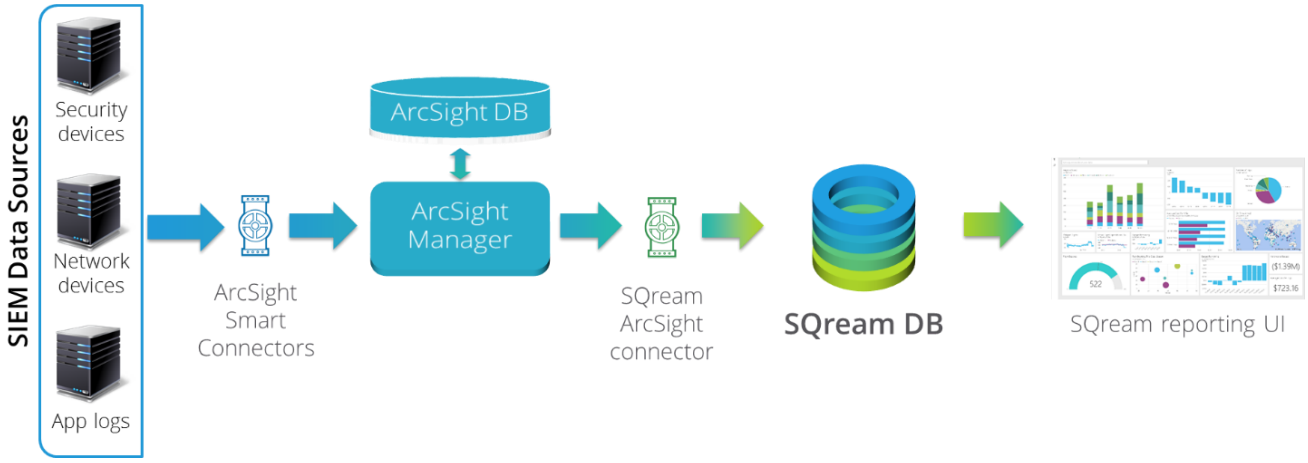

Figure 1 - New System Architecture, with SQream DB

RESULTS

SQream DB lets the vendor identify threats, abuse and attacks in near real-time, allowing them to act before damage is done. Deeper analysis of many billions of historical and recent events also enables the vendor to enhance the accuracy of anomaly detection, effectively **improving the ROC curve over a broader range of events – such as multi-stage breach patterns**.

With SQream DB, queries are now significantly faster, over a range of 6-12 months, compared to the previous 2-4 weeks, while saving hundreds of thousands of dollars with seamless integration – delivered and executed in under 5 days.

4 World Trade Center
150 Greenwich Street
New York, NY 10007

+1 646-931-1999
info@sqream.com
www.sqream.com
@SQreamtech