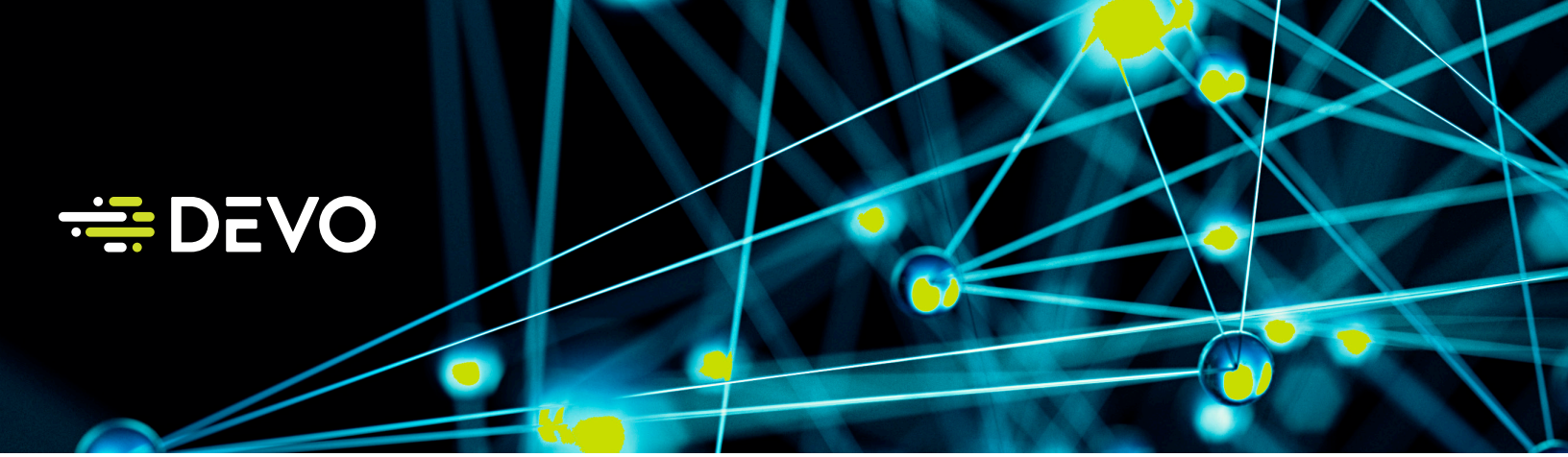

Leading European Bank turns to Devo for SIEM Enhancement

A customer case study

A leading banking and insurance group turned to Devo as part of their security transformation. They saw machine data at scale as a means of brokering information across the business and delivering a better and more secure customer experience.

Why SIEM enhancement

As with any modern banking environment, data growth was a given – the bank projected data ingest rates of 11TB of data per day coming from a multitude of devices, systems, and applications. The challenge was adding new data sources, particularly data sources from a growing number of non-standard technologies across new business areas, while also keeping costs in check. The bank originally ran their SOC on IBM's QRadar solution. IBM QRada r was unable to scale or perform to meet the needs of the security team – limiting performance to 16 queries per cluster or less. Licensing and hardware costs were getting out of control and there were a number of compliance concerns as data had to be extracted separately for audit teams – inadvertently exposing sensitive data via email. Lastly, the existing SIEM solution lacked the real-time capabilities critical for tackling the modern threat landscape.

In spite of these challenges, it wasn't possible for the bank to pursue a complete replacement of QRadar. The bank had implemented hundreds of customized rules and workflows that were deeply embedded in their security and incident management processes. In addition, they had users across multiple divisions who were trained in the current solution.

What the bank really needed was an approach that would allow them to continue operations with their SIEM, while standing up a complementary solution that would address the speed, scale, and performance needs of the SOC. This bank took an evolutionary approach by augmenting their SIEM with the Devo Data Analytics Platform – reducing risk, delivering immediate cost savings, and increasing the value of their technology investment.

INDUSTRY: FINANCIAL SERVICES

LOCATION: EUROPE

CHALLENGE

The bank needed to improve its SOC's security analytics capabilities in order to scale, safeguard new areas of an expanding business, and protect their brand.

SOLUTION

The Devo Data Analytics Platform coexists with a legacy SIEM solution allowing the bank to cost effectively collect all security-relevant data. Devo extends the traditional SIEM by enabling security analysts to conduct threat hunting, detection, and investigation at greater speed and scale.

RESULTS

- Ingest 100% of all security-relevant data, available for query in real time
- Reduce query times by 98%
- Achieved millisecond time-to-alerts
- Retained 5 years of historical data vs. 1 week
- Reduced licensing and hardware costs

Security becomes the hub for all data

The biggest challenge for the bank was collecting all data in a centralized location – even disregarding critical data sources due to high costs. The bank lacked a holistic view across all security point solutions and terabytes of dispersed data. Devo now stores all security-related and non-security information enabling analysts to analyze, visualize, and extract insight in real time, resulting in better processes for security:

- Standard mechanism for collecting logs from all applications and systems – no more data silos or lost security events
- Consistent approach to tracing all applications and performance logging from development, pre-production, and production environments
- Common alert system for applications errors, and early detection of errors and issues
- Complete visibility for threat detection and investigation processes across cloud and on-premises applications

Historical data is king for security and compliance

Historical data is just as critical as real-time data for security, not just to identify trends but to quickly analyze when an attack began and to find command & control indicators, even years back. With QRadar, the bank could only store one week of historical data. In addition, the long delays in accessing and querying cold data left analysts frustrated and lengthened detection and resolution times. Now the bank can store data for 5 years using Devo – all data is hot and instantly available for analysis and investigation.

Long retention times also benefit the bank from a regulatory and compliance perspective. In the past, audit teams waited for the security team to extract data and reports via email – which in itself is a huge data security red flag! With Devo, the audit teams can directly access the data they need, freeing the security team to focus on threat identification and response.

Real-time visibility for a strong security posture

Today's financial services environments contain multiple critical systems requiring real-time monitoring to protect against the possibility of a breach. In the past, the SOC team was hampered by query max-limits and micro-batching of alerting, delaying responses by hours. The deployment of Devo side by side with the traditional SIEM meant that Devo could manage, filter, and forward key events to the SIEM, and the SIEM still handled the routine correlations and false-positive noise reduction. The bank's SOC team also applied Devo's advanced, real-time data visualization to detect complex threats in less time – as well as gain a better understanding of the impact of these threats on their infrastructure. Using Devo, real-time streaming data for aggregation and dashboards load in seconds instead of hours. Multiple aggregation tasks in real time enabled the SOC to gain more immediate and detailed insight through dashboarding.

What's happening now

Staying ahead of the threat landscape comes down to identifying, understanding, and responding to new and complex threats – and for a modern security team, that means remaining in a state of constant evolution. The bank has continued to ingest higher and higher data volumes with Devo, with daily volumes ranging from 11 to 20TB per day, which has allowed the team to improve security operations. Devo is an integral and growing part of the bank's SOC cybersecurity program as it advances.