Leading European Bank turns to Devo for SIEM Enhancement

CUSTOMER SUCCESS STORY

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 QRadar 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 the Devo Platform, reducing risk, delivering immediate cost savings, and increasing the value of their technology investment.

INDUSTRY: Financial Services
HEADQUARTERS: 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 Platform coexists with a legacy SIEM solution allowing the bank to cost effectively collect all security-relevant data. Devo extends the capabilities of traditional SIEM by enabling security analysts to conduct threat hunting, detection, and investigation at greater speed and scale.

REQUIREMENTS

- 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.

WHY DEVO

This leading European bank chose Devo as its SIEM solution for the following reasons:

- Devo ingests 100% of the bank's necessary security data and cuts query times by 98% compared to the incumbent.
- The bank can now retain 5 years of historical data, as opposed to 1 week with QRadar, all with a lower TCO.
- Devo enables the team to maintain compliance by giving audit teams direct and quick access to the data they need.
- Devo Provides advanced threat hunting and detection capabilities to reduce MTTR and risk.

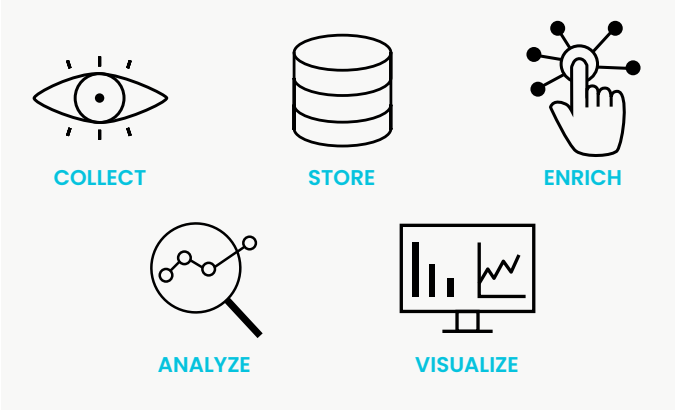
WHAT'S HAPPENING NOW

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.

THE DEVO PLATFORM: CLOUD-NATIVE SIEM, SOAR, UEBA & AI

The Devo Platform delivers a simplified, scalable, and high-performance SIEM solution with integrated behavior analytics, AI, and end-to-end SOAR capabilities. The Devo Platform arms your security team with unparalleled speed and scale, delivering full visibility of your data and risk posture.

• Zero infrastructure for seamless transfer - Zero central infrastructure required; quickly ingest any data source with wide ranging OOTB content on Devo Exchange.
• Outstanding time to value - We make migration painless and enable your team to start implementing critical security use cases quickly.
• Preeminent security analytics - No other SIEM on the market can match our speed and scale when searching across real-time and historical data.
• Upskill SOC teams - Devo reduces analyst burnout and improves productivity with our at-a-glance visualizations, attack-tracing AI, and response automation.
• Flexibility and customization - Devo provides the flexibility to customize your deployment and maximize your existing tools with pre-built integrations.



Learn more at devo.com

Devo
255 Main Street
Suite 702
Cambridge, MA 02142

Devo is the only cloud-native logging and security analytics platform that releases the full potential of your data to empower bold, confident action. With unrivaled scale to collect all of your data without compromise, speed to give you immediate access and answers, and clarity to focus on the signals that matter most, Devo is your ally in protecting your organization today and tomorrow. Devo is headquartered in Cambridge, Mass. Learn more at **www.devo.com**.