VIRTUSLAB

Success story

Building risk detection engine with Kafka and stream processing for top global retailer

Our client, a global retailer, aimed to enhance the security of their system since hackers carried out fraudulent activities on their E-commerce site. VirtusLab developed a risk engine platform for them using the Apache Kafka framework. This solution monitors, categorises, and prevents malicious attacks. On the very first day after implementation, it detected and prevented thousands of attempted frauds.

The Challenge

With the prevalence of cloud computing and the ease of access to computing power, attackers were building massive botnets to imitate real customers and carry out fraudulent activities. The ideal solution would be able to counter that threat. Our client needed a way to recognise and prevent account takeovers in real-time, at scale.

The solution

Having previously worked with Virtuslab, the client chose to outsource this task to them. VirtusLab built a reliable and scalable risk engine platform using Apache Kafka. The main responsibilities of the platform included:

- Categorising authentication attempts.
- Calculating statistics to observe malicious traffic patterns.
- Reacting proactively to prevent various types of attacks.

The platform offers several different types of analysis performed in parallel, using specific data pipelines. As the platform is event-driven, every new login event triggers each pipeline's execution. An event is just a statement of the fact – something that has happened in the real world.

The platform utilised Kafka Streams, a library that can be used with any JVM application, and ksqlDB for specific stream processors. Kafka Streams based applications do not have any specific requirements about the deployment platform, thus its infrastructure is built on top of Kubernetes. This allows for scaling up and down according to the traffic volume. Additionally, specific stream processors utilise ksqlDB while integrating with multiple third-party systems through Kafka Connect.

The results

After implementing the risk detection platform, the system blocked around 30,000 IP addresses, of which about a 1000 were unique, and locked approximately 500 fake user accounts within a single day.

These statistics demonstrate the effectiveness of the solution in preventing fraudulent activities and protecting user accounts. The platform is also recognises:

- Login attempts from unknown and untrusted devices for given user.
- Login attempts from new locations for a given user.
- Login attempts from botnet agents.
- Brute-force attacks.

The tech stack

Framework	Apache Kafka Kafka Streams ksqlDB:
Infrastructure	Kubernetes
Integration and Communication	Kafka Connect

About VirtusLab

At VirtusLab, we aim to lead in software technology, working consistently to enhance efficiency. Our profound commitment to research and development and a dedicated focus on emerging trends and inspirations fuels an innovative culture. This ethos precisely guides advancing our cutting-edge solutions, inviting collaboration to expand the boundaries of software technology collectively. We welcome you to be a part of this transformative journey.

Let’s connect

Contact Details

info@virtuslab.com

POLAND

Kraków Headquarters

Virtus Lab Sp. z o.o.
ul. Szlak 49
31-153 Kraków

GERMANY

Berlin Office

+49 30 52014256

VirtusLab GmbH
Potsdamer Platz 10
10785 Berlin

UNITED KINGDOM

London Office

+44 (0)20 4577 1051

Virtuslab Ltd.
40 Bank Street HQ3
London E14 5NR