Kafka et ksqlDB pour aider à la détection d'intrusion

Ribera, Maxime, maxime.ribera@zenika.com, Zenika, Bordeaux (Orateur)
Dugé de Bernonville, Géraud, geraud.dugedebernonville@zenika.com, Zenika, Bordeaux (Orateur)

Résumé : *Apache Kafka est une plateforme de traitement temps réel distribuée qui permet d'ingérer des volumes astronomiques de données. ksqlDB fait partie de l'écosystème Kafka et propose un langage inspiré de SQL pour requêter et analyser les flux de données en temps réel efficacement. ksqlDB permet d'adresser de nombreux cas d'utilisation comme l'enrichissement de données, le change data capture, la détection de fraudes, le monitoring temps réel… Cette présentation montre la mise en oeuvre de ksqlDB dans le cadre de la détection d'intrusion.*

Mots clés : *Kafka, Big Data, SQL, ETL*

Thématique : Thème 2: Structuration des données

1. Introduction

Kafka et ksqlDB sont des outils permettant le traitement de données massives en temps réel. L'objectif de cette présentation est de montrer un exemple de cas d'utilisation dans le domaine de la détection d'intrusion sur un réseau d'entreprise.

2. Méthodologie

La mise en oeuvre de ce cas d'utilisation se déroule selon les étapes suivantes:

- Collecte des trames réseau vers Kafka à l'aide de Kafka Connect
- Structuration des données à l'aide de ksqlDB pour aider aux analyses suivantes
- Utilisation de ksqlDB pour effectuer des agrégations et lever des alertes en cas de détection d'intrusion

3. Originalité / perspective

La détection d'intrusion (et de manière plus étendue la détection d'anomalie) est un des cas fréquemment cités dans le cadre de l'utilisation de ksqlDB. L'originalité de notre présentation est d'aller plus loin que les exemples référencés en montrant de manière intéractive différentes type d'attaques et la façon de les détecter avec ksqlDB.

La présentation alterne entre les aspects théorique autour de ksqlDB et les aspects pratiques avec démonstration de l'outil.

Si besoin, indiquer des références en dessous :

- Conférence donnée à BDX I/O 2019 : https://youtu.be/41qRQmRKq1Q