

# Security Data Lake for Federal-Level Financial Regulator

cybersecurity

finance

## Customer

A federal financial regulator responsible for monetary policy, financial stability, and the supervision of financial markets and institutions. It regulates monetary policy, manages foreign exchange and gold reserves, supervises financial markets and institutions, and ensures the smooth functioning of the payment system.

## Goals

building a disaster-resilient, geographically distributed platform for collecting and analyzing information security events across various segments of the computing infrastructure. Implementing a unified Security Data Lake for prompt detection and response to information security incidents.

## Tasks

centralized search across disparate data storages

implementation of a technical platform for the detection and response to information security incidents

functional refinement of the platform according to the specialized requirements of the client

training of Bank specialists for independent administration and system development

building a geographically distributed infrastructure for collecting, storing, and analyzing information security events

## Results

**>15K**  
assets

**4 TB/d**  
indexing data

**300+**  
data sources

monitoring the  
computing  
infrastructure of the  
**digital  
currency**

**150+**  
active users

*specialized training courses for employees*