Комплексная система мониторинга событий ИБ для Банка России

Безопасность | Финансы

Клиент

Центральный банк Российской Федерации – главный регулятор денежно-кредитной системы Российской Федерации.

Банк России

Цели

Построение катастрофоустойчивой территориально-распределенной платформы сбора и анализа событий информационной безопасности для различных сегментов вычислительной инфраструктуры. Реализация единого Security Data Lake для оперативного выявления и реагирования на инциденты информационной безопасности.

Задачи

- централизованный поиск по разрозненным хранилищам данных
- реализация технической платформы для службы выявления и реагирования на инциденты ИБ
- функциональная доработка платформы под специализированные требования заказчика
- обучение специалистов Банка для самостоятельного администрирования и доработки системы
- построение геораспределенной инфраструктуры сбора, хранения и анализа событий ИБ

Результаты

4 ТВ/день
поток индексируемых событий

300+
источников данных

> 15 тысяч
объектов мониторинга

ИБ+ИТ
единый Data Lake для данных ИБ и ИТ

150+
активных пользователей платформы

специализированные курсы для сотрудников