МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
Минтранс России

Транспортный университет

ИЭФ | Мониторинг событий ИБ

Ожидаемые сроки исполнения:

Один семестр (Февраль 2025 - Июнь 2025)

Заказчик

Финансовая организация

2025

Контекст

В какой области решаем проблему?

МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
Минтранс России

Транспортный университет

Информационная безопасность, регистрация событий, мониторинг, анализ инцидентов, SIEM, кибербезопасность, управление событиями, интеграция систем.

Проблема

Что за проблема: кто пытается достичь какую цель и что мешает?

МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
Минтранс России

Транспортный университет

Кто?

Начальник отдела информационной безопасности финансовой организации

Что хочет?

Иметь возможность отслеживания и анализа событий инцидентов информационной безопасности из различных источников для оперативного реагирования

Что мешает?

При увеличении объема данных и числа источников событий текущие системы могут испытывать сложности с масштабированием и производительностью.

Какие есть способы решения и почему они не подходят?

Ручные методы регистрации событий не позволяют своевременно обнаруживать и реагировать на инциденты безопасности. Системы SIEM (MaxPatrol Security Information and Event Management) не всегда могут быть адаптированы под уникальные требования компании без существенных модификаций. Могут требовать мощного аппаратного обеспечения и высокой пропускной способности сети, что не всегда доступно.