Иннотех (холдинговая компания Т1): миграция SIEM системы

Безопасность | Финансы

Клиент

ИТ-Холдинг, поставщик комплексных ИТ-услуг и заказной разработки программного обеспечения для компаний финансового сектора со штатом более 10 000 сотрудников, 160 городов присутствия.

Цели

Миграция с западного SIEM-решения на Smart Monitor

Перенос функциональных и контентных наработок с текущей SIEM системы в рамках программы импортозамещения. Повышение гибкости и масштабируемости SIEM.

> *"Среди ключевых преимуществ хочется отметить поиск событий: в нём много функций и он работает быстро*
>
> Ирина Изотова, Руководитель службы поиска и анализа угроз ИБ Т1

Задачи

- интеграция с SOAR, BI, TIP
- построение отказоустойчивый, масштабируемой системы
- реализация гибкой системы разграничения прав доступа
- приведение к разработанной для текущей SIEM модели данных

Результаты

гибкость+скорость
в части функциональных доработок, гибкость при миграции, универсальность применения

25K
EPS средний поток событий

400+
активных правил корреляции

78
справочников с данными

Материалы

смотреть — видео с VB-Trend 2024: Опыт миграции SIEM-системы

читать — заметка корпоративного блога прошедшей конференции VB-Trend 2024