Авито: переезд SIEM с MS Sentinel на Smart Monitor за два месяца

Безопасность | Online сервисы

Клиент

крупнейший в России и входящий в Top-10 в мире интернет-сервис для размещения объявлений о товарах, вакансиях и резюме на рынке труда, а также услугах от частных лиц и компаний. Ежемесячная аудитория более 60 миллионов человек.

Цели

Миграция с западного SIEM-решения на Smart Monitor

За один квартал необходимо было мигрировать с облачной инсталляции SIEM на собственные вычислительные ресурсы, обеспечив перенос существующих наработок и логику работы с информационными источниками.

> *"Все критические правила из kill chain мы смогли перенести в Smart Monitor буквально в течение дня*
>
> Тимур Котов, Avito SOC Team Lead

Задачи

миграция с Cloud-native SIEM Solution Microsoft Sentinel

переезд SIEM в собственную On-premise инфраструктуру

реализация правил с собственной логикой силами клиента

перенос процессов SOC на Smart Monitor

Результаты

- применение workflow для построения процессов SOC
- поток обрабатываемых событий в инфраструктуре >2.5M EPS
- гибкая ролевая модель позволяет давать доступ всем и выходить за рамки SIEM
- использование CI/CD для управления конфигурациями
- объектами мониторинга являются 10K+ серверов
- *SIEM as a Code*

Материалы

смотреть — видео с VB-Trend 2024: Sentinel runaway. Тимур Котов, Avito SOC Team Lead

читать — заметка корпоративного блога прошедшей конференции VB-Trend 2024