Система анализа трафика для регионального оператора связи

Региональный оператор связи в республике Татарстан, предоставляющий услуги фиксированной и мобильной связи, широкополосного доступа в интернет и цифрового телевидения для населения и бизнеса. Компания владеет и развивает современную телекоммуникационную инфраструктуру, включая волоконно-оптические сети, и играет ключевую роль в цифровизации региона.

udvlgroup

О проекте

Цель

Заказчик обратился в UDV Group с целью внедрить новое решение класса NTA для собственной внутрикорпоративной сети. Предыдущее решение не предоставляло специалистам по ИБ достаточного количества данных для изучения аномалий трафика и инцидентов и не позволяло оперативно реагировать на них. Еще одним приоритетом заказчика было повышение экономической эффективности закупаемых ИБ-продуктов, поэтому при выборе UDV NTA разница в цене сыграла решающую роль.

В качестве решения была внедрена система

UDV NTA

Обеспечивает полную видимость сети, позволяет обнаружить атаку до того, как бизнесу будет нанесен ущерб.

О проекте

Виктор Колюжняк

Исполнительный директор UDV Group

«Внедрение UDV NTA позволило заказчику не только выполнить строгие требования регуляторов, но и значительно повысить экономическую эффективность вложений в ИБ-инфраструктуру. Мы обеспечили его команду исчерпывающими данными для мгновенного реагирования на угрозы и перевели лицензии на выгодную бессрочную модель. Этот кейс подтверждает: наше сертифицированное решение — это стратегический шаг для тех, кто ценит независимость, скорость внедрения и полный контроль над безопасностью своей сети.»

Результаты внедрения

- Специалистам по ИБ теперь проще получать информацию о сетевых событиях и связанных с ними метаданных сетевого трафика для расследования инцидентов ИБ
- Удобный интерфейс позволяет в несколько кликов получить необходимые данные в реальном времени: активные сетевые узлы, карта их взаимодействий, детальный разбор сетевых сессий
- Выполнены требования регулятора за счет использования решения, сертифицированного ФСТЭК России
- Заказчик перераспределил бюджет благодаря переходу на бессрочные лицензии в соответствии с политикой лицензирования, принятой в UDV Group

Особенности проекта

01

Комплексный проект с интеграцией UDV SIEM и UDV SOAR

Проект внедрения включал в себя не только установку и настройку UDV NTA, но и интеграцию с SIEM- и SOAR-системами. За счет чего получилось создать единую инфраструктуру ИБ, в которой данные о сетевых событиях автоматически коррелируются с информацией из других источников, обеспечивая более полную картину угроз и автоматизацию процессов реагирования на инциденты, повышая эффективность работы службы ИБ.

02

Реализация проекта за 5 месяцев

Благодаря слаженной работе задействованных команд все этапы проекта — от анализа требований до пилотного проекта и введения в эксплуатацию — были выполнены менее чем за полгода. Это позволило заказчику быстро начать использовать решение с целью анализа сетевого трафика и усиления защиты корпоративной сети от потенциальных угроз.

03

Передача контроля над системой анализа трафика в руки штата ИБ заказчика

Ранее функция анализа инцидентов и реагирования была делегирована внешнему подрядчику. Внедрив более удобное и информативное решение UDV NTA, заказчик планирует обучать специалистов самостоятельно выявлять угрозы и оперативно реагировать на инциденты. Такой подход позволяет получить большую независимость, гибкость и контроль над своими средствами защиты.