udv|group

UDV NTA 2.0

Интеллектуальный анализ сетевого трафика для раннего обнаружения кибератак

udv|group

CyberLympha® тринидата

UDV Group — группа компаний российских разработчиков высокотехнологичных решений для обеспечения киберустойчивости промышленных, коммерческих и государственных предприятий.

Мы помогаем компаниям эффективно управлять состоянием их цифровой инфраструктуры, обеспечивая полную видимость технологического и ИТ — контура, контролировать состояние сети и устройств, своевременно нейтрализовать угрозы — до того, как они повлияют на бизнес.

- Защита АСУ ТП и объектов КИИ
- Мониторинг инфраструктуры
- Реагирование на инциденты ИБ
- Предиктивная аналитика киберугроз
- ИБ консалтинг и техническая поддержка
- Выполнение требований регуляторов

12+ лет

на рынке информационной безопасности

Подтвержденный опыт интеграции в нефтегазовой отрасли, энергетике, металлургии

1000+

инсталляций

Проекты по защите АСУ ТП и корпоративных сетей

Глубокая экспертиза в АСУ ТП и кибербезопасности в промышленности

Наличие сертификатов ФСТЭК по 4 уровню доверия

Сильная инженерная база, продукты высокого уровня зрелости

Гибкий подход, возможность кастомизации решений под запрос

Драйверы

Запрос рынка

Как не допустить остановку деятельности?

Как оптимизировать усилия текущей команды?

Как остановить злоумышленника?

Решение

Снижение риска простоя сервисов и ущерба от кибератак

- **полная видимость сети** для выявления слабых мест и проактивной защиты от внутренних угроз
- **обнаружение забытой или скрытой ИТ-инфраструктуры** и сервисов для повышения точности оценки рисков
- **мониторинг сетевой безопасности** в сегментах, где невозможно использование агентов (сетевое оборудование, IoT, устаревшее ПО)
- своевременное **обнаружение целевых кибератак**
- **контроль рисков** информационной безопасности при работе с подрядчиками

Драйверы

Запрос рынка

Как не допустить остановку деятельности?

Как оптимизировать усилия текущей команды?

Как остановить злоумышленника?

Решение

Повышение эффективности реагирования на инциденты ИБ без увеличения штата

- **своевременная локализация угроз ИБ** через сетевые соединения на карте сети
- **обогащение подозрительной сетевой активности информацией** о владельце, характеристиках и групповой принадлежности сетевого узла
- **дополнение событий ИБ в SOC сетевой связностью** для составления и подтверждения цепочек атак

Драйверы

Запрос рынка

Как не допустить остановку деятельности?

Как оптимизировать усилия текущей команды?

Как остановить злоумышленника?

Решение

Исключение повторения инцидентов ИБ

- **отображение взаимосвязи** между пораженным активом и скомпрометированными вплоть до точки входа злоумышленника
- **ретроспективный анализ** по метаданным или экземплярам копии сетевого трафика
- **глубокий разбор пакетов до прикладного уровня** для обнаружения причин возникновения инцидента ИБ

Решение

UDV NTA 2.0

UDV NTA 2.0 — интеллектуальная система анализа сетевого трафика для раннего выявления кибератак, расследования инцидентов и проактивного поиска угроз.

Объединяет полную видимость сети и контекст конкретного бизнеса, чтобы:

- находить угрозы до того, как злоумышленник нанесет ущерб
- быстро принимать решения по реагированию на основе данных

udv|group

Функционал

Возможности продукта

01

Регистрация обхода периметровых средств защиты

02

Выявление нелегитимного использования штатных утилит

03

Обнаружение скрытых угроз с применением методов машинного обучения

04

Детализация событий ИБ данными глубокого разбора трафика

05

Запись доказательств инцидента

06

Поиск угроз по полям прикладных протоколов

Функционал

Сценарии применения UDV NTA

Повседневные

Видимость сети

Задача:

Понять, что именно планируем защищать и какие сервисы сейчас активно используются, чтобы выявить слабые места и оценить имеющиеся риски

Как:

UDV NTA предоставляет:

- механизмы выявления активов из копии сетевого трафика
- визуализацию карты сети
- глубокий анализ сетевого трафика до уровня приложений

Результат:

- Снижается риск появления «слепых зон» в инфраструктуре
- Уменьшается поверхность атаки за счёт полной сетевой прозрачности

Функционал

Сценарии применения UDV NTA

Повседневные

Проверка векторов атаки

Задача:

Размышляя как нарушитель, проверить возможные варианты точек входа в инфраструктуру и дальнейших шагов

Как:

UDV NTA предоставляет информацию о незащищенных участках инфраструктуры (например, учетные данные в открытом виде или избыточный удаленный доступ)

Результат:

- Снижается количество или полностью исключаются уязвимые места, которые могут привести атакующего к ключевым системам

Функционал

Сценарии применения UDV NTA

Под атакой

Раннее обнаружение и локализация угроз ИБ в реальном времени

Задача:

Основная задача при реализации угрозы — понять поведение и замысел нарушителей на протяжении всей цепочки кибератак

Как:

UDV NTA объединяет обнаружение на основе IDS или внутренних механизмов с контекстом на основе глубокого анализа сети, чтобы быстро подтвердить или опровергнуть оповещение

Результат:

- Снижается среднее время реакции на атаку (MTTR)
- Предотвращается возможность повторного проникновения

Функционал

Сценарии применения UDV NTA

Под атакой

Выявление скрытых угроз

Задача:

Усилить проактивный поиск угроз и достоверно оценивать их

Как:

Благодаря встроенным модулям машинного обучения, UDV NTA производит статистический анализ, акцентируя внимание на подозрительных взаимодействиях

Результат:

- Выявляется туннелирование протоколов
- Выявляются устройства, использующие программное обеспечение для подключения сгенерированным доменам (DGA)

Функционал

Сценарии применения UDV NTA

Контроль

Снижение рисков ИБ при работе с поставщиками услуг

Задача:

Учесть риски ИБ при проведении работ подрядными организациями, на которые не распространяется политика ИБ компании

Как:

UDV NTA позволяет контролировать доверенные другим организациям доступы для проведения работ и сигнализировать при наличии кибератаки

Результат:

- Улучшается видимость работ в цепочке поставок

Функционал

Сценарии применения UDV NTA

Регулятор

Соответствие законодательным требованиям и регулятивным нормам

- 152 ФЗ
- 187 ФЗ
- NIST SP 80061 R2
- **ГОСТ Р 57580.1-2017**
  Безопасность финансовых (банковских) операций

Решение задачи импортозамещения:
UDV NTA включен в Реестр российского ПО
реестровая запись №27786 от 06.05.2025

Доверенное ПО:
UDV NTA в составе программного комплекса CL DATAPK имеет сертификат соответствия ФСТЭК России по профилю защиты СОВ (сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ) №4719 от 28.09.2023

Архитектура

Компоненты UDV NTA

UDV AI Platform
ИИ-ассистент

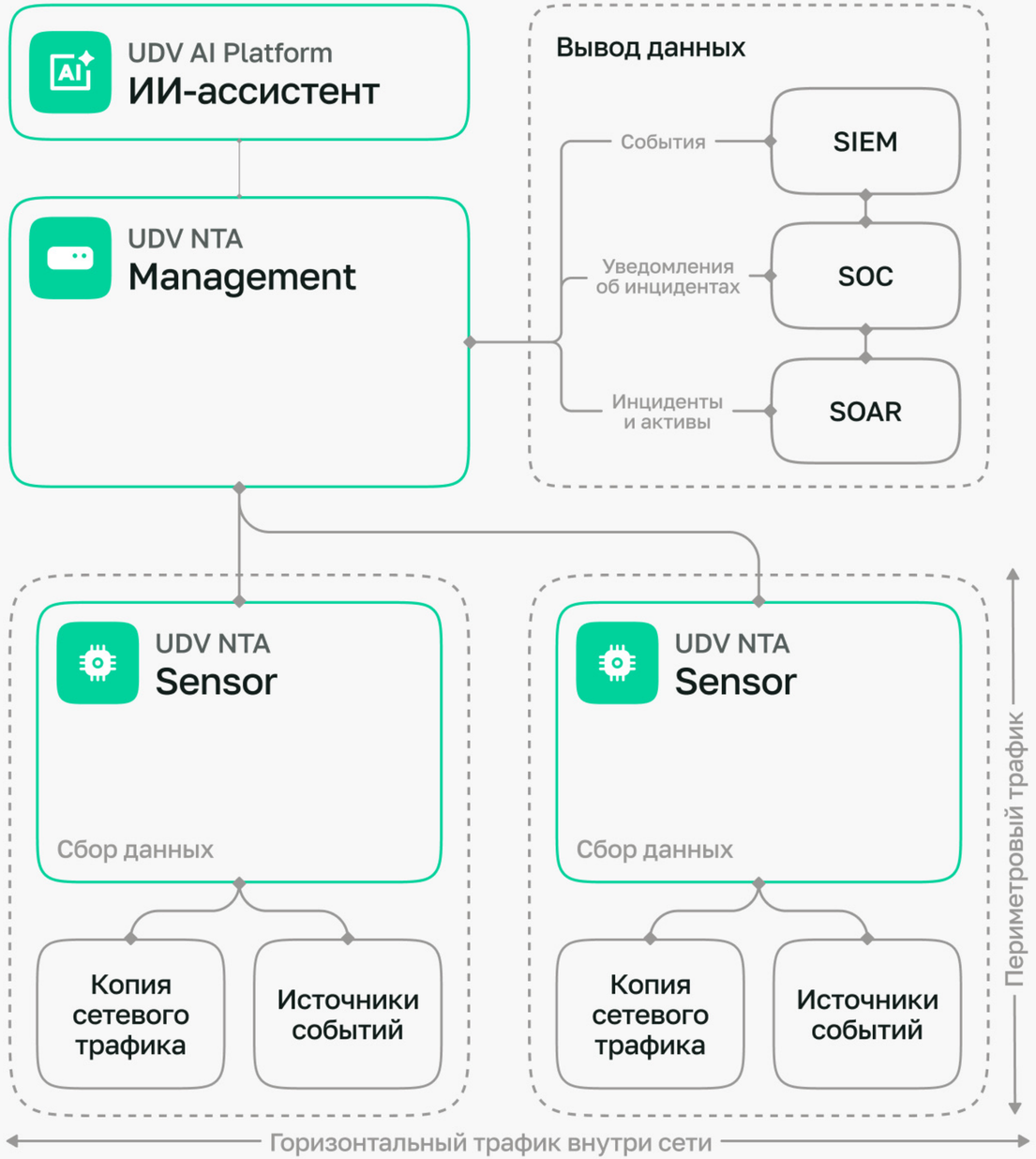
- Разбор инцидента и рекомендации по реагированию с учётом бизнес-процессов компании
- Отчёты по запросу — от сводки за смену до поиска закономерностей за месяц
- Работа с продуктом без глубокой экспертизы в NTA
- LLM-независимость: локальная модель или маскирование данных

UDV NTA
Management

- Нормализация и корреляция событий
- Формирование инцидентов и отображение панелей мониторинга
- Хранение метаданных сетевого трафика
- Централизованное управление сетью сенсоров

UDV NTA
Sensor

- Анализ сетевого трафика
- Разбор протоколов передачи данных
- Запись и хранение копии сетевого трафика
- Хранение полученных из сети файлов
- Прием событий ИБ от узлов сети



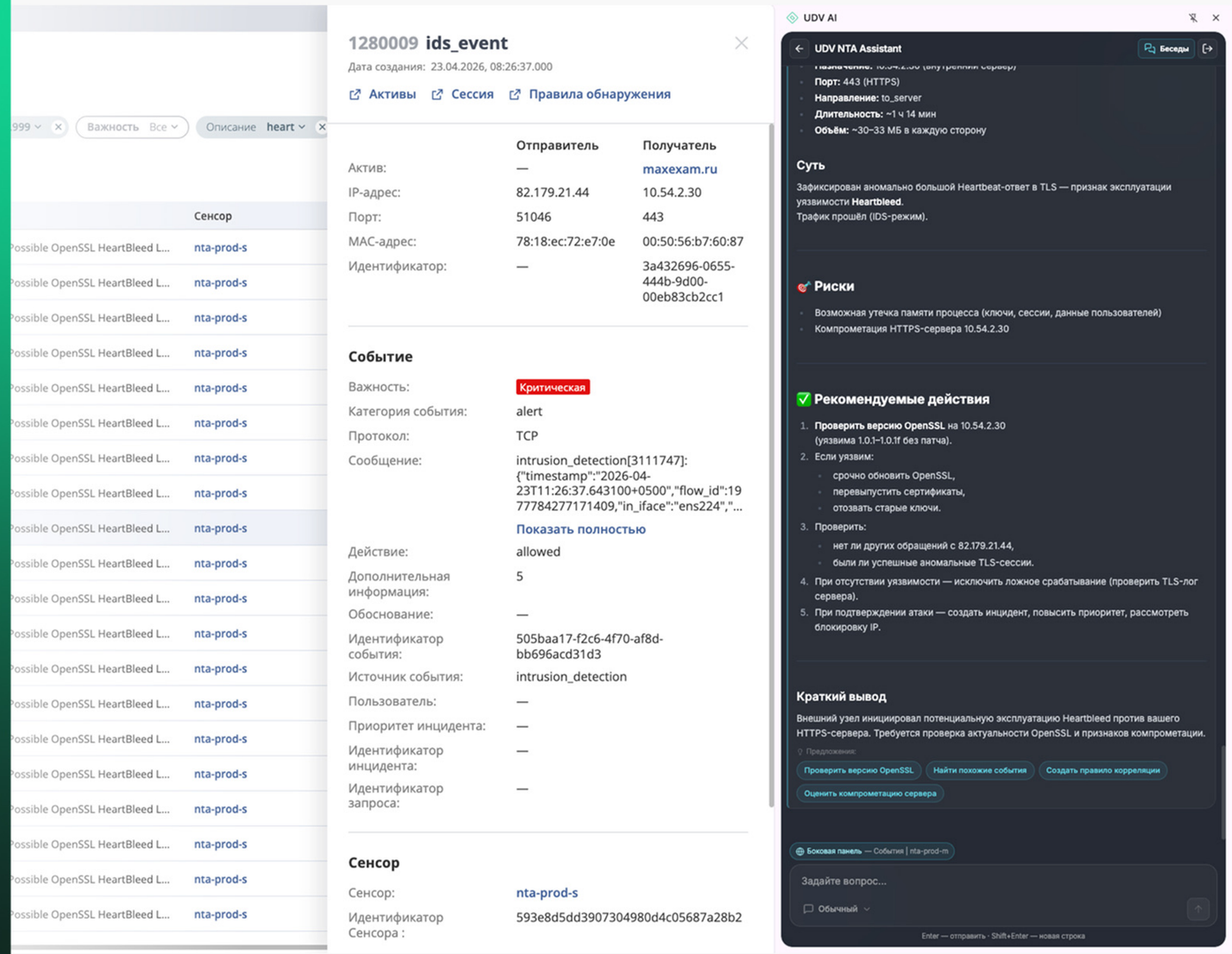
Функционал

ИИ-ассистент в UDV NTA

Быстрее реагируем на инциденты
ИИ-ассистент анализирует инцидент и мгновенно выдаёт рекомендации с учётом контекста компании: регламентов, активов и критичных бизнес-процессов

Растём в защищённости, не в ФОТ
Анализ трафика становится доступен специалистам с минимальным опытом — ИИ помогает разобраться в событиях без глубокой экспертизы

Меньше рутины для аналитиков
Аналитики перестают искать инструкции и настраивать правила вручную — нужные ответы приходят от ИИ-ассистента за секунды



Кейс

Заказчик

- Региональный оператор связи в республике Татарстан, предоставляющий услуги фиксированной и мобильной связи, широкополосного доступа в интернет и цифрового телевидения для населения и бизнеса.

Задачи

- Построить процесс выявления и реагирования на инциденты ИБ внутри компании на основе данных.
- Повысить экономическую эффективность используемых ИБ-продуктов.

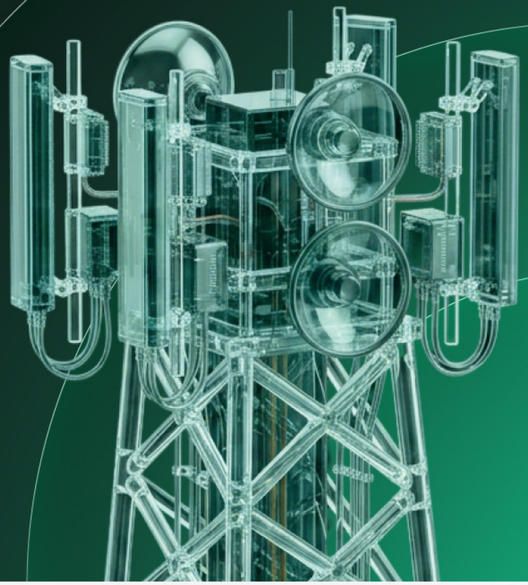
Решение UDV NTA было выбрано как оптимальное по соотношению стоимости владения и видимости сети

Выгода

Результат внедрения

Специалисты по ИБ в несколько кликов получают данные о скомпрометированных сетевых узлах и их взаимодействиях, что позволяет быстро принимать решения по реагированию

Оптимизирован бюджет за счет перехода на бессрочные лицензии в соответствии с политикой лицензирования, принятой в UDV Group — выполнены требования регулятора (UDV NTA сертифицирован ФСТЭК России)



Преимущества

Почему UDV NTA?

Меньше вычислительных ресурсов

До 50% меньше CPU и RAM по сравнению с аналогичными решениями при сопоставимом уровне анализа сетевого трафика

Учитывает контекст бизнеса

Помогает приоритизировать инциденты, дает рекомендации по реагированию, формирует персонализированные отчеты

Максимальная видимость сети

- Корреляция событий ИБ от хостов с их сетевой активностью «из коробки»
- Индикация любого протокола уровня приложения по запросу пользователя

Обнаружение актуальных угроз и локализация атак

- Автообновляемая экспертиза вендора UDV Threat Intelligence и подключение собственной базы IoC
- Переход в 2 клика от инцидента к карте сети с визуализацией затронутых узлов и их сетевых взаимодействий

Знакомство с продуктом

С чего начать?

Консультация

Напишите нам на commercial@udv.group. Мы свяжемся с вами, обсудим ваши задачи и требования

Персональная демонстрация

Проведем презентацию функционала и интерфейса продукта

Тест-драйв продукта

Дадим доступ к тестовой инфраструктуре и расскажем о возможных сценариях применения продукта

Пилотный проект

Развернем программное обеспечение в выделенном участке вашей сети, поможем с настройками и запуском

udv|group

Закажите пилотный проект или персональную демонстрацию наших решений

Контакты

8-800-511-65-51
Телефон для связи

zapros@udv.group
Электронная почта

udv.group
Сайт

@udv_group
Телеграм

620100, г. Екатеринбург, ул. Сибирский тракт, 12, строение 7, этаж 4
Адрес

udv.group