udv|group

софтлайн РЕШЕНИЯ

Найти и обезвредить

Анализ трафика с помощью UDV NTA для проактивной защиты от атак

UDV Group — ведущий разработчик в области кибербезопасности

UDV Group предоставляет единый портфель решений для защиты технологических сетей, корпоративного сегмента и автоматизации в области объектовой безопасности:

- **защита АСУ ТП и объектов КИИ**
- **мониторинг инфраструктуры**
- **реагирование на инциденты ИБ**
- **автоматизация работы SOC**
- **выполнение требований регуляторов**

12+
лет на рынке ИБ и ИТ

Подтвержденный опыт интеграции в нефтегазовой отрасли, энергетике, металлургии

10+
патентов

Собственный исследовательский центр в области кибербезопасности

200+
разработчиков

Распределенная команда со штаб-квартирой в Екатеринбурге

1500+
инсталляций

Внедренные проекты по защите АСУ ТП и корпоративных сетей

О спикере

Михаил Пырьев

Менеджер продукта UDV NTA

Кратко

Экспертиза

Сетевая безопасность, исследование кибератак, создание продуктов

7+ лет опыта

в проектировании и разработке систем обеспечения сетевой безопасности для компаний-субъектов КИИ

3+ лет исследований

рынка решений класса NTA/NDR

Автор статей по анализу сети

с 2019 года

Программа

Что внутри?

01

Драйверы анализа трафика

Класс NTA как ключевой элемент защиты

02

Причины возникновения драйверов

Статистика прошлого года
и прогноз развития киберугроз

03

Обзор решения UDV NTA

Возможности, архитектура

04

Применение UDV NTA

Практические кейсы

05

Live demo UDV NTA

Обзор интерфейса и расследование инцидента ИБ

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

Причины

Статистика за 2025 год

Рост APT-атак на 27%

Основная цель - остановка бизнес-процессов, а не выкуп

Источник: Информзащита, RED Security

Каждая четвертая атака через цепочки поставок

Годом ранее доля таких атак не превышала 10%

Источник: Коммерсантъ на основе исследования «Бастион»

47% доля новой техники ClickFix на замену фишинга

Классическая модель «укрепили периметр — и все защищены» не работает

Источник: Информзащита

Общий тренд - удешевление атак за счет ИИ

ИИ-помощники проводят 80–90 % планирования, разведки и разработки методов вторжения

Причины

Прогноз на 2026 год

01

Эволюция ИИ киберугроз

Более опасные и в то же время более простые для реализации

02

Компрометация подрядчиков – среди главных трендов

Сохранение тенденции последних лет из-за низкой зрелости ИБ и бюджетов на борьбу с угрозами в цепочке поставок

03

Уязвимости в популярном софте

Прекращение поддержки Windows 10, отсутствие тщательного исследования отечественного ПО на предмет ошибок безопасности

04

Больше проактивности и превентивности

За счет киберустойчивости – быстрого и беспроблемного восстановления

Источник: Anti-malware

Решение

UDV NTA

UDV NTA — система анализа сетевого трафика для обнаружения кибератак, которая позволяет видеть активность как на периметре, так и внутри сети.

Продукт помогает специалистам по ИБ выявлять подозрительную активность и предотвращать атаки до их завершения, минимизируя или полностью исключая потенциальный ущерб и повышая уровень безопасности сети.

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

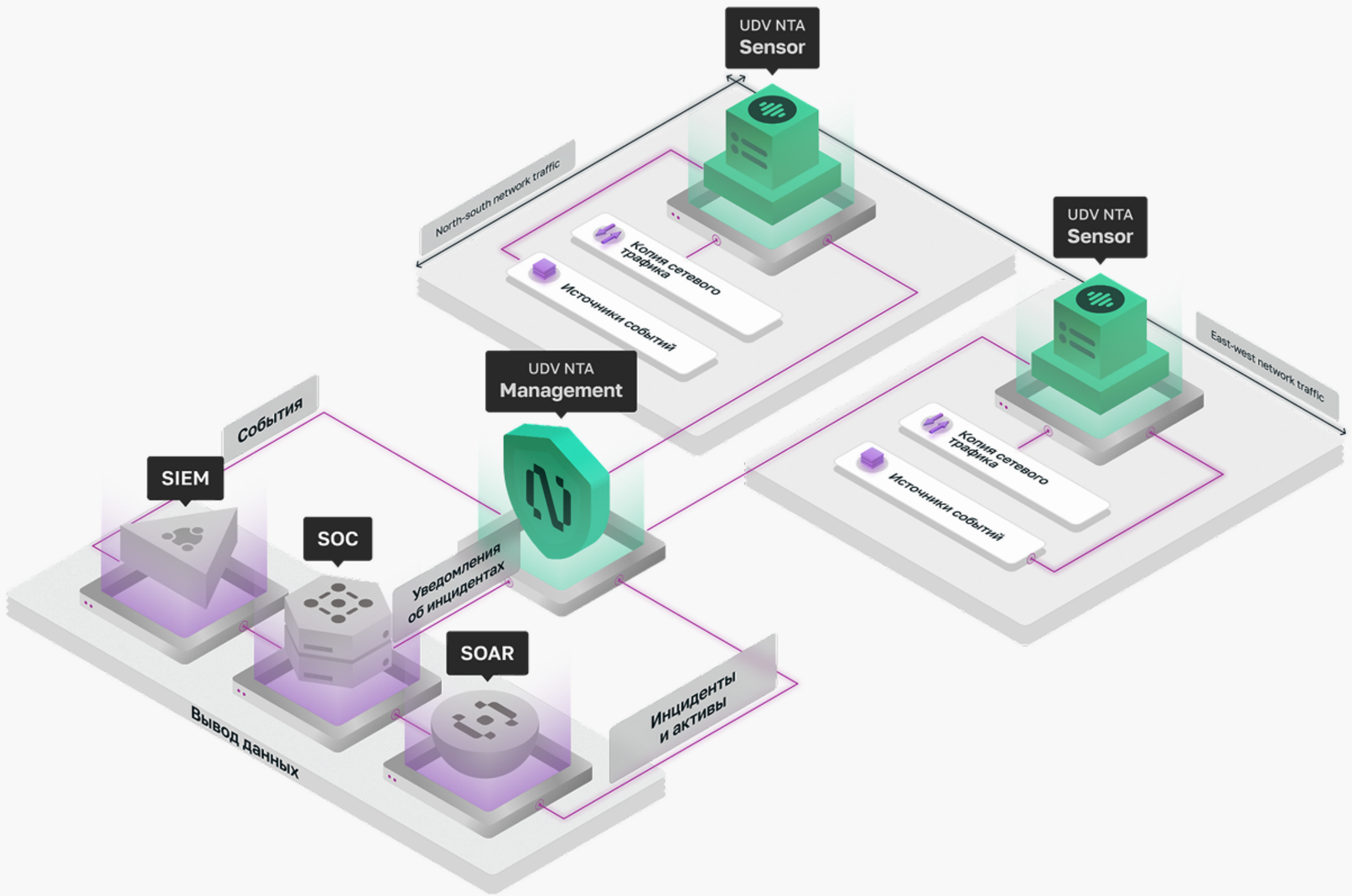
Компоненты UDV NTA

MANAGEMENT

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

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



Преимущества

Почему UDV NTA?

01

Доступные современные технологии

UDV NTA эффективно использует вычислительные ресурсы и требует на ~50% меньше по сравнению с аналогичными решениями при сопоставимом уровне анализа трафика

02

Глубокое понимание состояния сетевого узла

UDV NTA формирует комплексное представление статуса информационной безопасности за счет приема событий ИБ от рабочих станций, серверов, сетевого оборудования и сопоставления их с сетевой активностью

03

Расширенная поддержка прикладных протоколов

UDV NTA - единственное на рынке РФ решение для анализа сетевого трафика с возможностью глубокой инспекции пакетов любого протокола уровня приложения

04

Максимальный контекст

UDV NTA позволяет в пару кликов перейти к деталям сетевого события, информации о владельце и характеристиках сетевого узла, а также найти связи на карте сети

Live demo

UDV NTA 1.1

Сценарий демонстрации

Обзор интерфейса

Рассмотрим панель мониторинга и раздел управления инцидентами

Расследование инцидента

Проведем погружение в детали инцидента, а также обзор карты сети

Проактивный поиск угроз

Выдвинем гипотезы и проверим их на основе данных

Ретроспективный анализ

Анализируя экземпляр сетевого трафика, получим знания на основе экспертных правил

udv|group софтлайн решения

udv.group

Закажите пилотный проект
или персональную демонстрацию
наших решений

Контакты

Анастасия Зырянова
Пресейл-менеджер
по сетевой безопасности

anastasiya.zyryanova@softline.com
Электронная почта