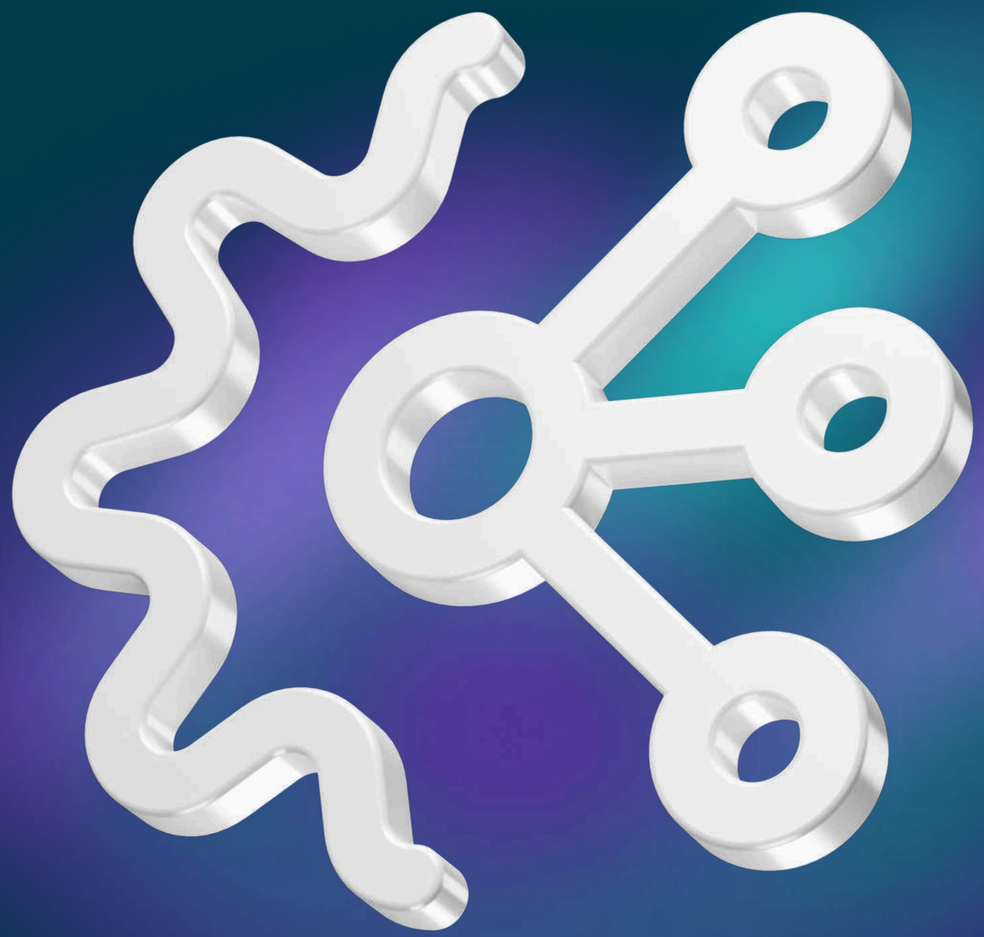
udv|group

UDV NTA

Система выявления угроз безопасности на основе анализа сетевого трафика



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

200+

Разработчиков в штате

Распределённая команда
со штаб-квартирой в Екатеринбурге

1000+

Инсталляций

Проекты по защите АСУ ТП
и корпоративных сетей

10+

Патентов

Собственный исследовательский
центр в области кибербезопасности

10

Лет на рынке

Подтвержденный опыт интеграции
в крупных предприятиях
нефтегазовой отрасли, энергетики,
металлургии и других

Текущие вызовы кибербезопасности

Каждая компания находится под перманентной угрозой от профессионалов

Число кибератак в России и в мире

Среднее время реагирования на угрозу более 270 дней

2/3 нарушений ИБ пропускается специалистами

IBM Security Report 2023

Время реагирования определяет ущерб

Реагирование спустя 200 дней после инцидента увеличивает стоимость восстановления более чем на $1 млн

IBM Security Report 2023

Защищать сеть снаружи уже недостаточно — необходимо видеть происходящее внутри, чтобы быстро и эффективно реагировать на угрозы

UDV NTA

UDV NTA — система выявления угроз безопасности на основе анализа сетевого трафика, которая позволяет видеть активность как на периметре, так и внутри сети.

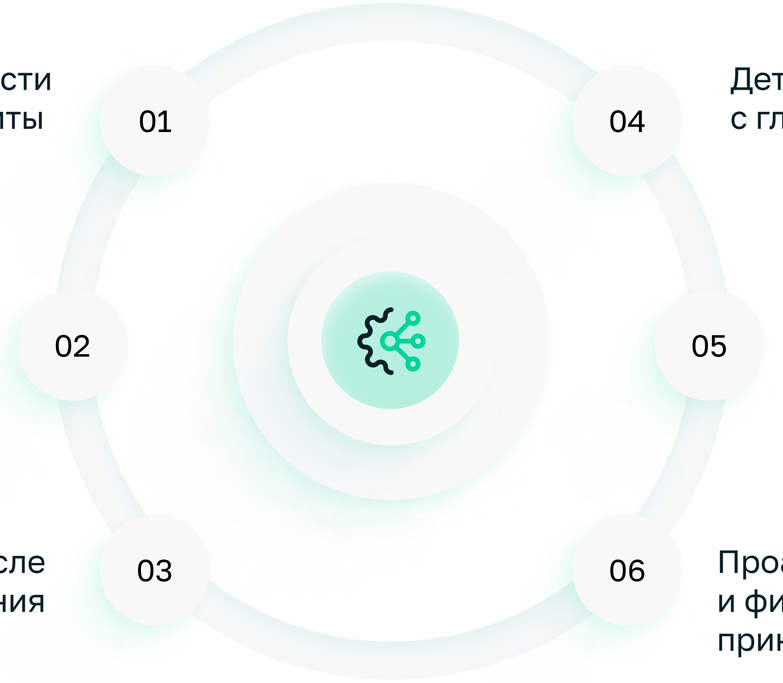
Продукт помогает командам SOC и специалистам по ИБ выявлять подозрительную активность и предотвращать атаки до их завершения, минимизируя или полностью устраняя реальный нанесенный ущерб и повышая уровень ее безопасности.

Возможности UDV NTA

01 Регистрация сетевой активности при обходе периметровых средств защиты

02 Выявление неавторизованных устройств в сети

03 Обнаружение скрытых угроз, в том числе с применением методов машинного обучения



04 Детализация сетевых событий ИБ за счет связи с глубоким разбором протоколов приложений

05 Запись доказательств для расследования инцидентов как в виде копии сетевого трафика, так и передаваемых по сети файлов

06 Проактивный поиск угроз за счет индексирования и фильтрации метаданных по специфичным для прикладных протоколов полям

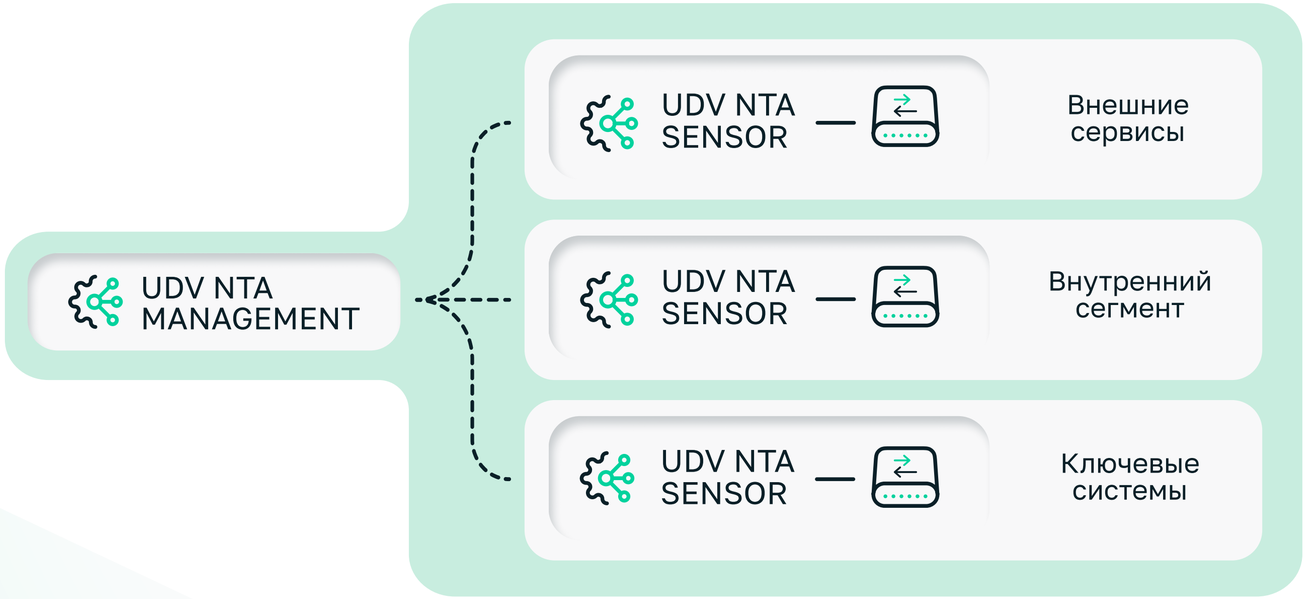
Архитектура UDV NTA

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



udv|group

Преимущества UDV NTA

Анализ логов

Снижение нагрузки на SIEM за счет возможности получения событий от конечных узлов или СрЗИ и корреляции данных событий с сетевой активностью

Гибкая настройка

- Снижение объема хранимой информации на UDV NTA уровня Management за счет выбора метаданных для хранения
- Снижение объема хранимой информации на UDV NTA уровня Sensor за счет фильтрации записываемого трафика

Представление протоколов приложений с индексацией

Быстрый поиск в контексте протокола приложений с помощью представлений и фильтров по специальным полям

Карточки сетевых устройств

Повышение осведомленности о наличии конечных узлов в сети и их активности в реальном времени

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

Сценарии использования

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

Спасибо!

Закажите пилотный проект или персональную демонстрацию наших решений

Контакты

commercial@udv.group
8-800-511-65-51

Адрес

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

Сайт

udv.group

Telegram

@udv_group