Защита корпоративного сегмента

UDV NTA

Ключевой элемент сетевой видимости и раннего обнаружения кибератак

Основываясь на анализе сетевого трафика в реальном времени, UDV NTA позволяет выявлять подозрительную активность и предотвращать атаки, минимизировать или полностью исключить потенциальный ущерб. UDV NTA позволяет проводить комплексный анализ данных из различных источников, что помогает выявлять сложные и целенаправленные атаки, которые могли бы остаться незамеченными другими средствами защиты.

ВОЗМОЖНОСТИ

01 Регистрация сетевой активности при обходе периметровых средств защиты

02 Выявление неавторизованных устройств в сети

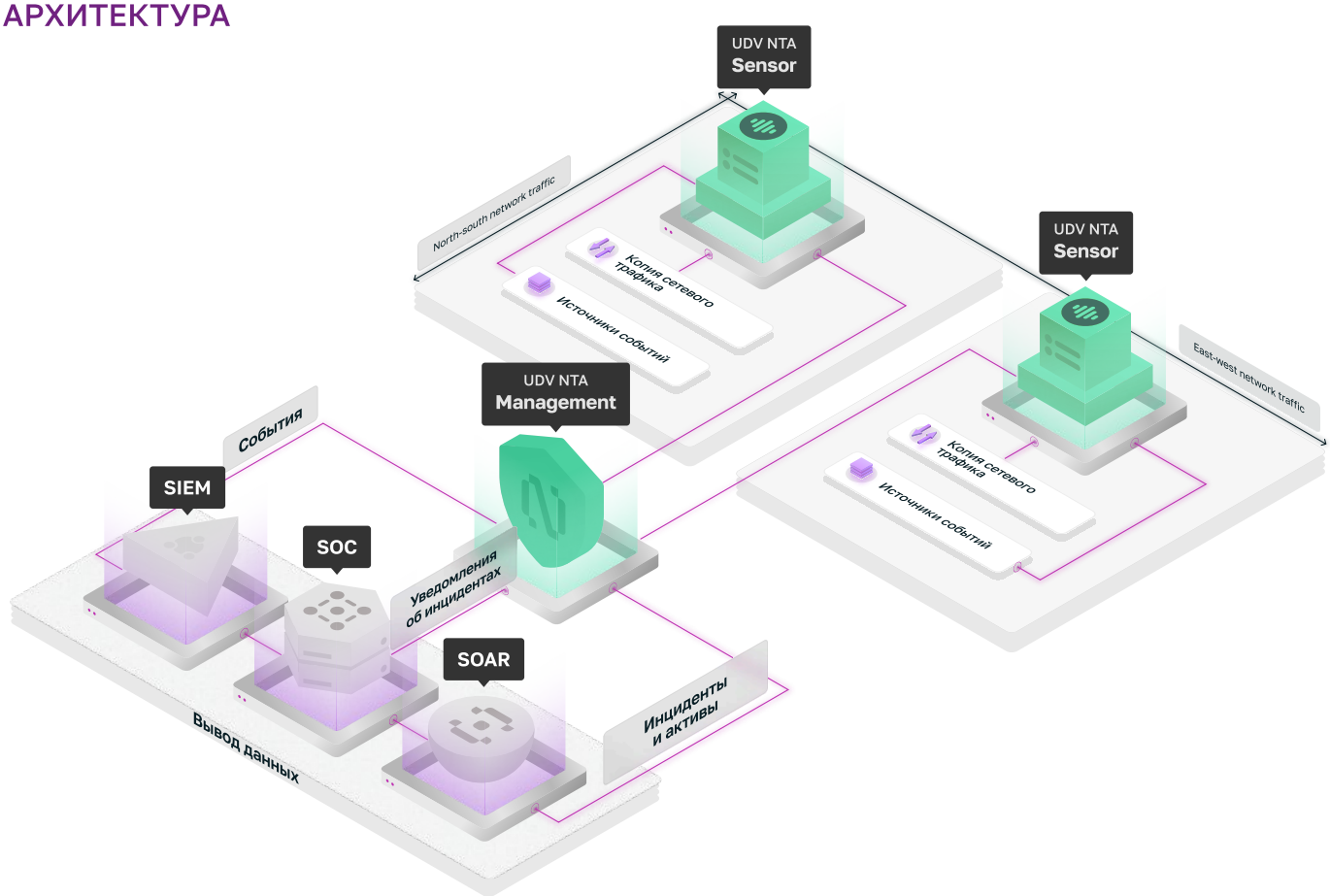
03 Обнаружение скрытых угроз с применением методов машинного обучения

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



АРХИТЕКТУРА

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

РЕШАЕМЫЕ ЗАДАЧИ

Определение поверхности потенциальной атаки

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

Проверка векторов атаки

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

Раннее обнаружение и локализация угроз ИБ в реальном времени

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

Снижение рисков ИБ при работе с поставщиками услуг

- Улучшается видимость работ в цепочке поставок

Выявление скрытых угроз

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

Соответствие законодательным требованиям и регулятивным нормам

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

ПРЕИМУЩЕСТВА

Оптимальный баланс ресурсов и стоимости

UDV NTA эффективно использует вычислительные ресурсы и требует на ~50% меньше по сравнению с аналогичными решениями

Объединение данных для точного обнаружения угроз

Максимальное покрытие за счет обработки и корреляции с сетевой активностью событий ИБ от устройств в сети

Максимальный контекст

Позволяет в пару кликов перейти к деталям сетевого события и исследовать специфичные поля протоколов приложений для проактивного поиска угроз

Объектный подход к анализу сети

Автоматически определяет устройства и связывает их с сетевыми действиями

Запишитесь на тест-драйв или закажите персональную демонстрацию UDV NTA

commercial@udv.group