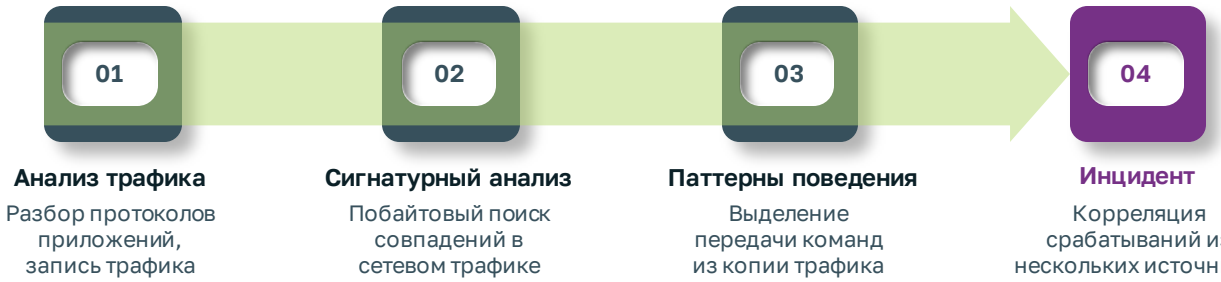
UDV NTA (Network Traffic Analyzer)

Система анализа сетевого трафика

Технология, используемая для обеспечения безопасности сетевого трафика, играет важную роль в защите сетевых ресурсов и данных от киберугроз. Основываясь на анализе сетевого трафика в реальном времени, UDV NTA позволяет выявлять подозрительную активность и предотвращать атаки до их завершения, минимизируя или полностью устраняя реальный нанесенный 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.

ИНДИКАЦИЯ КОМПРОМЕТАЦИИ И АТАК



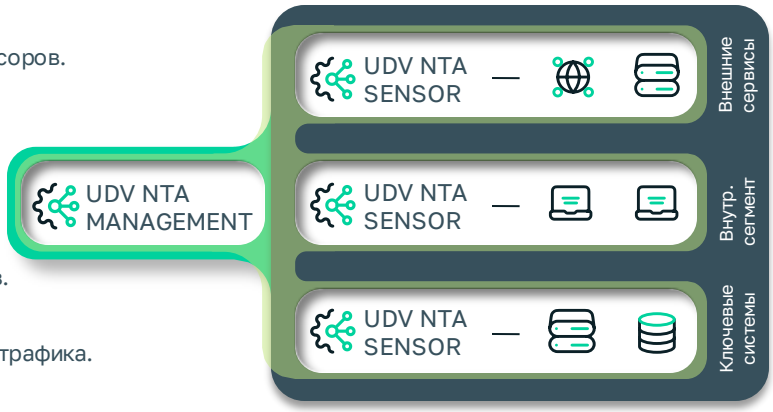
ВОЗМОЖНОСТИ

UDV NTA MANAGEMENT

- Централизованное управление сетью сенсоров.
- Нормализация и корреляция событий.
- Формирование инцидентов, отображение панелей мониторинга.

UDV NTA SENSOR

- Обнаружение сетевых соединений.
- Глубокий разбор протоколов приложений и промышленных протоколов.
- Индикаторы атаки и компрометации, индикаторы туннелирования протоколов.
- Запись, хранение, анализ копии сетевого трафика.
- Сигнатурное обнаружение вторжений.
- Хранение полученных файлов из сети.
- Проверка файлов на вредоносное ПО



ПРЕИМУЩЕСТВА И ВЫГОДЫ

Контроль сетевых соединений

Применение UDV NTA предоставляет возможность обнаружения несанкционированного доступа удаленного управления.

Выявление теневой инфраструктуры

UDV NTA определяет сетевые узлы, что позволяет обнаружить неавторизованные активы функционирующие в сети предприятия.

Ретроспективный анализ

Хранение метаданных сетевого трафика и его сырой копии позволяют проводить исследования причин инцидента и выявление сложных угроз.

Работа с инцидентами

UDV NTA использует механизмы корреляции, что позволяет агрегировать события из сети в инциденты по экспертным правилам.