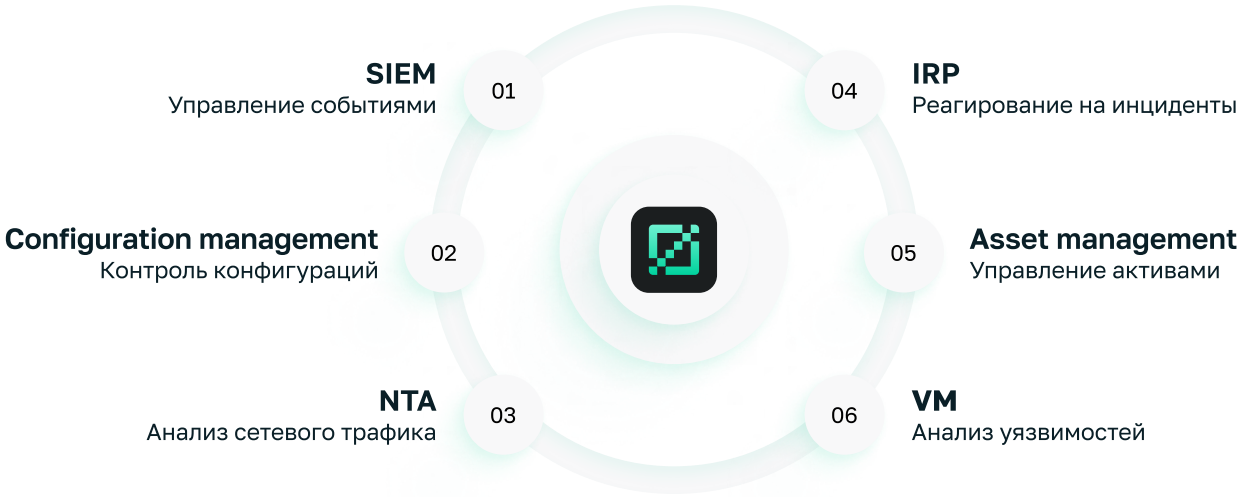
Защита корпоративных сетей

UDV MultiProtect

Комплексное решение для обеспечения кибербезопасности среднего бизнеса

UDV MultiProtect позволяет быстро и эффективно повысить уровень защищенности за счет комбинации функциональности нескольких классов продуктов в одном решении и доступных «из коробки» сценариев выявления и реагирования на инциденты ИБ от коммерческого SOC.



РЕШАЕМЫЕ ЗАДАЧИ

Выявление компьютерных атак

Анализ сетевого трафика, событий безопасности, выявление аномалий и действий злоумышленников.

Предотвращение инцидентов ИБ

Поиск уязвимостей в ПО и аудит изменений в эталонных настройках оборудования, которые могут стать точкой входа злоумышленника в сеть.

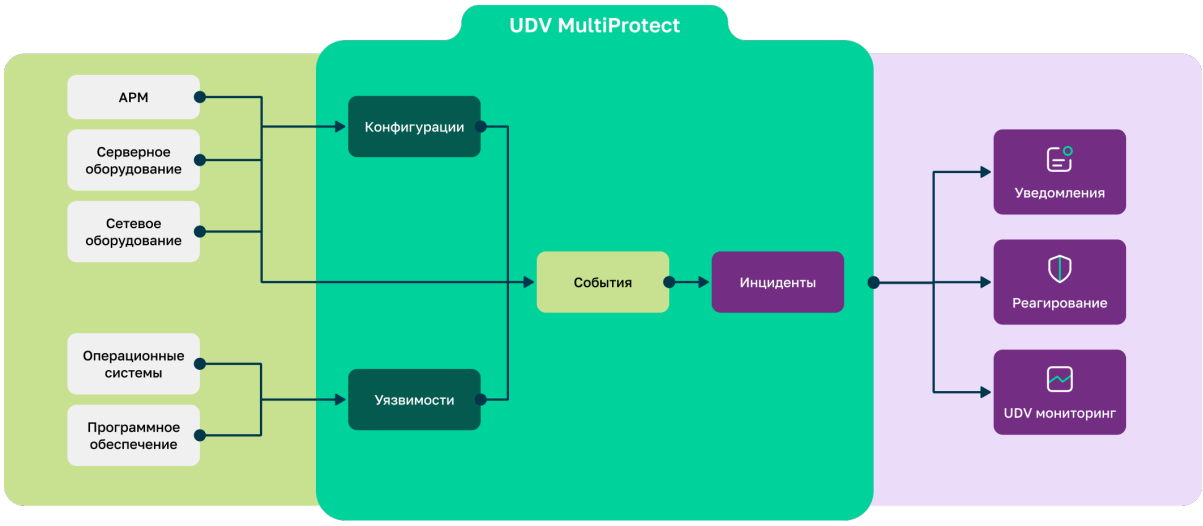
UDV MultiProtect

Сокращение ущерба от инцидентов ИБ

Сокращение времени простоя сервисов / недоступности сайта, репутационного вреда, финансовых потерь из-за выплат хакерам и т. д. за счет экспертных сценариев выявления инцидентов и реагирования.

Инвентаризация ИТ-инфраструктуры

Поддержание информации о корпоративной сети в актуальном состоянии за счет автоматической инвентаризации активов (технических средств и ПО). Выявление майнеров и теневых вычислительных средств.



ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

Управление активами

- Инвентаризация сети (технических средств и программного обеспечения)
- Классификация активов по типу, информационной системе и любым другим меткам

Управление конфигурациями

- Контроль безопасности настроек и их неизменности, аудит изменений

Реагирование на инциденты

- Готовый пошаговый алгоритм обработки и расследования инцидентов
- Автоматизированное обогащение информации по инцидентам и реагирование
- Определение техник реализации инцидентов по известным методологиям (ТТУ ФСТЭК и MITRE ATT&CK)
- Оповещения на электронную почту о регистрируемых инцидентах

Сканирование сетевого трафика и обнаружение вторжений

- Обнаружение несанкционированных сетевых потоков и соединений
- Выявление сетевых атак, «майнеров», удалённого администрирования
- Визуализация карты устройств в сети и сетевых соединений

Управление внешними событиями

- Получение событий ИБ с различных источников
- Корреляция событий ИБ, выявление инцидентов

Управление уязвимостями

- Поиск уязвимостей
- Проверка соответствия требованиям (Compliance)

ПРЕИМУЩЕСТВА

Комплексная защита

1 продукт - 6 необходимых мер защиты в едином интерфейсе

Экономия ресурсов

Стоимость ниже, чем у сета моно-продуктов, автоматизация процессов

Экспертиза

Механизмы выявления инцидентов от коммерческого Центра мониторинга ИБ, техническая поддержка, консультации

Подтвержденная эффективность

Использование технологий, применяемых для защиты промышленных объектов КИИ, проверенных на 150+ проектах в сегменте корпораций