udv|group

UDV DATAPK Industrial Kit

Комплексная система для киберзащиты АСУ ТП любого масштаба с полной видимостью атак, угроз и выполнением требований законодательства

- Отсутствие негативного влияния на АСУ ТП и технологические процессы
- Модульная архитектура позволяет сократить расходы
- Адаптивность под индивидуальные потребности пользователей
- Сертифицирован ФСТЭК России по 4 уровню доверия (сертификат № 4719) по профилю защиты систем обнаружения вторжений
- Сочетает функции нескольких классов решений ИБ для максимального покрытия мер приказов ФСТЭК России № 239 и № 31
- Совместимость с компонентами АСУ ТП российских и зарубежных производителей

Вызовы кибербезопасности промышленности

01 СЗИ не должны влиять на технологический процесс

Киберустойчивость без остановки производственного процесса

02 Обилие legacy-систем и уязвимых протоколов

- Не поддерживают установку агентов и/или обновления
- Отсутствие шифрования и слабая аутентификация промышленных протоколов

03 Слепые зоны в инфраструктуре

- Отсутствие точной карты сети/инвентаризации из-за долгого жизненного цикла оборудования
- Обилие теневых активов в технологическом сегменте

04 Требования регуляторов

Необходимо обеспечивать соответствие требованиям регуляторов, использовать доверенные средства защиты и подтверждать контролируемость технологического сегмента

Какие задачи решает?

01 Анализ промышленного сетевого трафика

На основе анализа копии сетевого трафика обнаруживает кибератаки, несанкционированные подключения и скрытые угрозы, включая сложные атаки, выявляемые с помощью алгоритмов ML

02 Управление внешними событиями

Собирает и обрабатывает события ИБ из различных внешних источников, визуализирует данные, позволяет отправлять нормализованные события в SIEM, IRP/SOAR, на OPC UA серверы

03 Управление уязвимостями

Проводит аудит защищенности АСУ ТП, не вмешиваясь в технологический процесс, выявляет и позволяет устранить угрозы, проверяет соответствие требованиям ИБ

04 Управление версиями проектов ПЛК

Обеспечивает централизованное хранение проектов ПЛК, отслеживание изменений в коде/конфигурациях, резервное копирование и восстановление версии

05 Обнаружение аномалий в работе ПЛК

Оперативно выявляет аномалии в поведении ПЛК посредством безагентного анализа, используя методы машинного обучения

06 Управление конфигурациями

Контролирует соответствие конфигураций любых ИТ и АСУ ТП устройств необходимым значениям

Архитектура решения

Sensor

- Получает и хранит копию сетевого трафика
- Получает с АСУ ТП данные о конфигурациях, установленном ПО, его версиях, принимает внешние события ИБ от сторонних источников
- Передает предобработанные данные на Management

Management

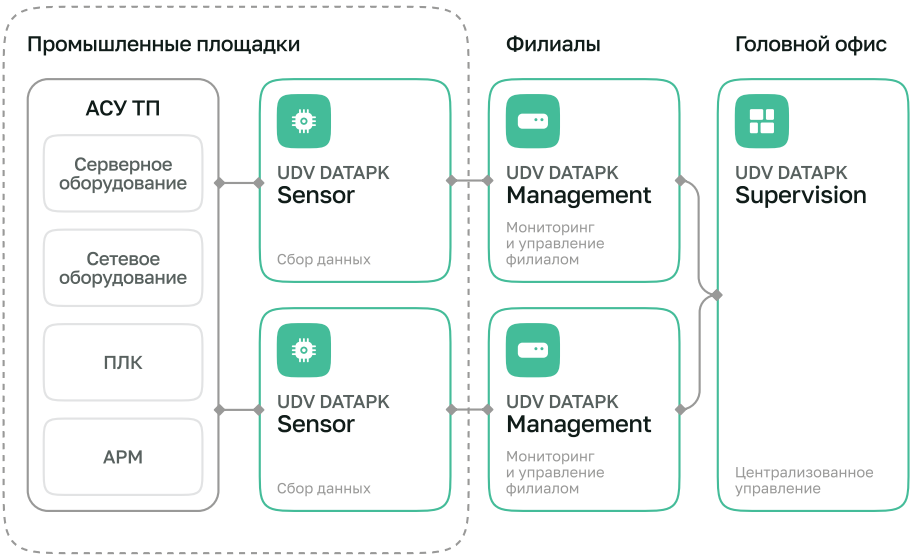
- Конфигурация и администрирование связки Management + Sensor
- Хранение обработанных данных и их передача на Supervision
- Базовые панели мониторинга

Supervision

- Централизованная аналитическая информация об общем состоянии защищенности АСУ ТП
- Управление учетными записями пользователей системы

Лицензирование

UDV DATAPK Industrial Kit лицензируется по количеству компонентов различных уровней (Sensor, Management, Supervision) и модулям в составе каждого из компонентов, что позволяет экономить бюджет, включая в поставку только необходимую функциональность



Хотите обсудить ваш проект или договориться о демонстрации?

www.udv.group