

UDV DATAPK Industrial Kit

Комплексное решение для обеспечения кибербезопасности АСУ ТП

UDV DATAPK Industrial Kit позволяет быстро начать реагировать на угрозы без влияния на защищаемые системы. Обеспечивает видимость ландшафта АСУ ТП, выявляет инциденты на ранних этапах и помогает выполнить требования регуляторов. UDV DATAPK Industrial Kit использует целостный подход в рамках единого решения, что позволяет оптимизировать расходы на защиту АСУ ТП.

КОМПЛЕКСНЫЙ ПОДХОД К ОБЕСПЕЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ АСУ ТП



ВОЗМОЖНОСТИ UDV DATAPK Industrial Kit

Анализ сетевого трафика и обнаружение вторжений

- Анализ копии сетевого трафика (SPAN)
- Выявление и инвентаризация активов
- Визуализация карты устройств в сети и сетевых соединений
- Обнаружение атак, нелегитимных узлов, несанкционированных сетевых соединений
- Более 20 000 правил обнаружения «из коробки»
- Обновление правил обнаружения без модификации программного кода
- Формирование инцидентов ИБ

Управление конфигурациями

- Контроль безопасных настроек и их неизменности, аудит изменений
- Анализ соответствия требованиям ИБ
- Работа без использования агентов
- Использование стандартных общедоступных протоколов компонентов АСУ ТП
- Формирование инцидентов ИБ

Управление уязвимостями

- Неинвазивный аудит безопасности без использования агентов
- Проверка соответствия требованиям (Compliance)
- Технологии OVAL и «CPE to CVE»
- Поддержка различных БДУ, включая ФСТЭК России
- Формирование инцидентов ИБ

Управление внешними событиями

- Получение событий ИБ с различных источников
- Нормализация и корреляция событий ИБ
- Возможность настройки правил корреляции событий ИБ
- Отправка инцидентов ИБ в сторонние системы (syslog)
- Формирование инцидентов ИБ



Реализация мер приказов №239 и №31 ФСТЭК России

UDV DATAPK Industrial Kit выполняет требования регулятора к организационным и техническим мерам проектирования и эксплуатации систем безопасности значимого объекта КИИ:

- Идентификация и аутентификация устройств
- Контроль доступа из внешних систем
- Управление инсталляцией компонентов ПО
- Инвентаризация информационных ресурсов
- Анализ и устранение уязвимостей
- Регистрация события безопасности
- Контроль и анализ сетевого трафика
- Выявление, оповещение и защита информации об инцидентах
- Управление и контроль изменений конфигурации объектов
- Мониторинг безопасности и проведение аудитов

ПРЕИМУЩЕСТВА UDV DATAPK Industrial Kit

-  Создан специально для АСУ ТП и учитывает особенности промышленных сетей
-  Может работать в полностью пассивном режиме: безагентный подход минимизирует дополнительную нагрузку на работу АСУ ТП
-  Входит в экосистему UDV Group, включающую решения для защиты АСУ ТП и КИИ, корпоративных сетей и физического периметра объекта
-  Совместим с Siemens, Schneider Electric, OBEH, CODESYS, Haiwell, InTouch, Honeywell, различными ОС – список постоянно пополняется
-  Техническая поддержка вендора 24/7, возможность кастомизации под заказчика и непрерывное развитие функциональности
-  Опыт применения для защиты значимых объектов КИИ РФ в металлургии, энергетике, нефтегазовом секторе, промышленности
-  Реализует все необходимые возможности класса промышленных СОВ, поддерживает базу данных решающих правил с учетом особенностей технологических сетей
-  Сертифицирован ФСТЭК России по требованиям профиля защиты СОВ уровня сети, по уровням доверия в соответствии с Приказом №76 от 2 июня 2020 г.
-  Выполняет функции нескольких классов решений: системы обнаружения вторжений, средства управления событиями и средства анализа защищенности (Приказ №235 ФСТЭК России)

45+ корпоративных заказчиков

150+ реализованных проектов

1500+ установленных комплексов

Закажите пилотный проект или персональную демонстрацию наших решений: commercial@udv.group