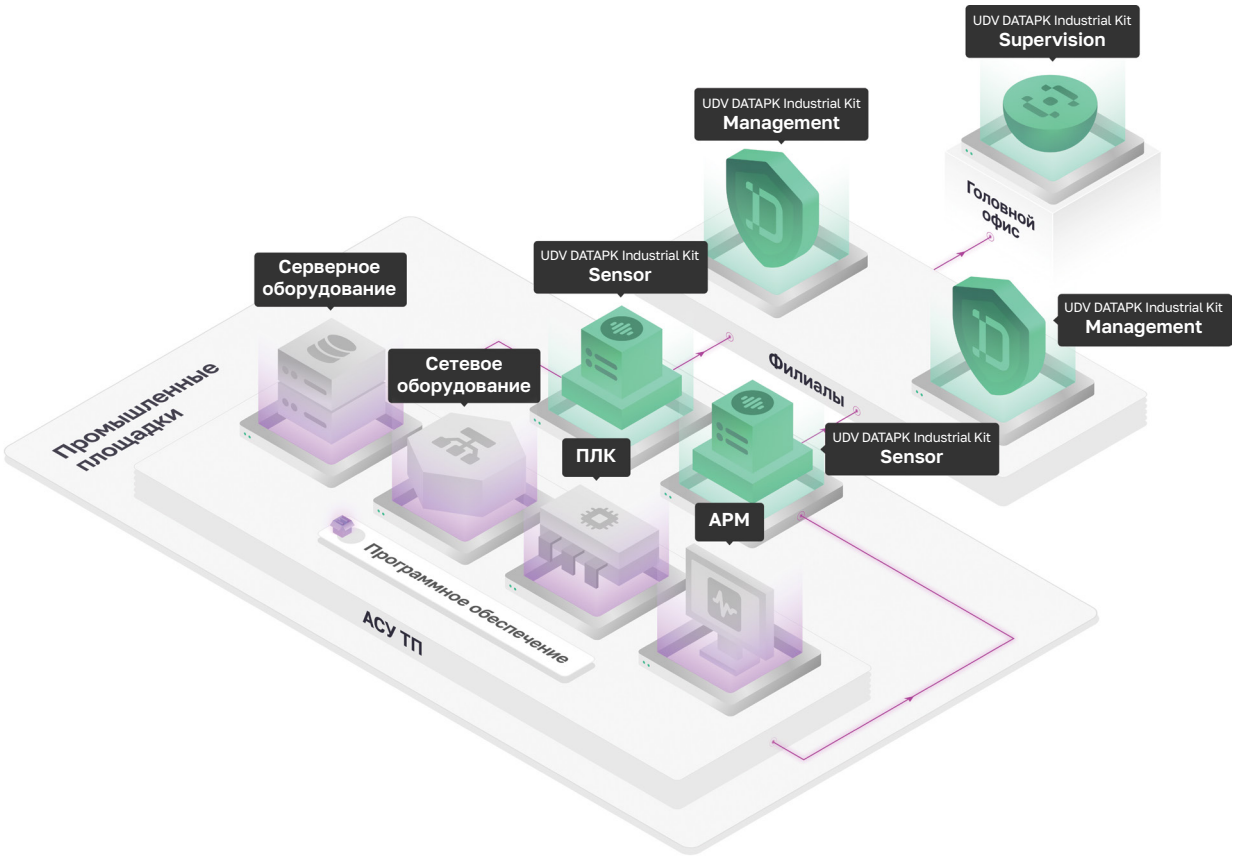
udv|group

UDV DATAPK Industrial Kit 3.0

Комплексная киберзащита АСУ ТП с полной видимостью атак, угроз и соответствием законодательству

UDV DATAPK Industrial Kit помогает экспертам по ИБ и АСУ ТП справляться с современными вызовами кибербезопасности и не беспокоиться о негативном влиянии на технологические процессы. Благодаря полной видимости ландшафта, комплексного подхода к выявлению атак и скрытых угроз до момента их реализации и возможности закрыть требования законодательства, с UDV DATAPK Industrial Kit промышленные предприятия могут быть уверены в киберустойчивости своего производства.



КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

Анализ промышленного сетевого трафика (Industrial NTA)

Находит устройства внутри сети, быстро выявляет атаки и проводит расследования, контролирует параметры технологических процессов

Управление конфигурациями (Configuration Management)

Контролирует соответствие необходимым значениям конфигураций любых ИТ и АСУ ТП устройств

Управление уязвимостями (Vulnerability Management)

Проводит неинвазивный аудит защищенности АСУ ТП методом White Box, выявляет и позволяет устранить угрозы, проверяет соответствие требованиям ИБ

Управление внешними событиями (External Events Management)

Собирает и обрабатывает события ИБ из различных внешних источников, визуализирует данные, позволяет отправлять нормализованные события в сторонние системы

Контроль версий проектов ПЛК (Version Control)

Обеспечивает централизованное хранение проектов ПЛК, мониторит изменения и позволяет восстановить версии проектов, отслеживает неизменность программ на ПЛК

Обнаружение и реагирование для ПЛК (EDR for PLC)

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

ПРЕИМУЩЕСТВА

- Отсутствие негативного влияния на АСУ ТП и технологические процессы
- Сочетает функции нескольких классов решений ИБ (Приказ N 235 ФСТЭК России)
- Адаптивность под индивидуальные потребности пользователей
- Совместимость с компонентами АСУ ТП российских и зарубежных производителей
- Неинвазивный безагентный подход к анализу защищенности
- Сертифицирован ФСТЭК России по профилю защиты систем обнаружения вторжений

Реализация мер приказов №239 и №31 ФСТЭК России

АУД.1	Инвентаризация информационных ресурсов
АУД.2	Анализ уязвимостей и их устранение
АУД.4	Регистрация событий безопасности
АУД.5	Контроль и анализ сетевого трафика
АУД.6	Защита информации о событиях безопасности
АУД.7	Мониторинг безопасности
АУД.8	Реагирование на сбои при регистрации событий безопасности
АУД.9	Анализ действий отдельных пользователей
АУД.10	Проведение внутренних аудитов
ЗИС.6	Управление сетевыми потоками
ЗИС.31	Защита от скрытых каналов передачи информации
ЗНИ.7	Контроль подключения машинных носителей информации
ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов
ИАФ.2	Идентификация и аутентификация устройств
ИАФ.3	Управление идентификаторами
ИАФ.4	Управление средствами аутентификации
ИНЦ.1	Выявление компьютерных инцидентов
ИНЦ.2	Информирование о компьютерных инцидентах
ИНЦ.6	Хранение и защита информации о компьютерных инцидентах
ОДТ.4	Резервное копирование информации
ОДТ.3	Контроль безотказного функционирования средств и систем
ОПО.4	Установка обновлений программного обеспечения
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения
ОЦЛ.1	Контроль целостности программного обеспечения
ОЦЛ.2	Контроль целостности информации
ПЛН.2	Контроль выполнения мероприятий по обеспечению защиты информации
СОВ.1	Обнаружение и предотвращение компьютерных атак
СОВ.2	Обновление базы решающих правил
УКФ.1	Идентификация объектов управления конфигурацией
УКФ.2	Управление изменениями
УКФ.4	Контроль действий по внесению изменений
УКФ.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения
УПД.1	Управление учетными записями пользователей
УПД.4	Разделение полномочий (ролей) пользователей
УПД.5	Назначение минимально необходимых прав и привилегий
УПД.6	Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему
УПД.9	Ограничение числа параллельных сеансов доступа
УПД.10	Блокирование сеанса доступа пользователя при неактивности
УПД.12	Управление атрибутами безопасности
УПД.14	

ЛИЦЕНЗИРОВАНИЕ

UDV DATAPK Industrial Kit лицензируется по количеству компонентов различных уровней и модулям в составе каждого из компонентов. Необходимое количество компонентов каждого уровня зависит от потребностей, особенностей целевого окружения и используемых функциональных возможностей. В наличии бессрочные и срочные лицензии, а также срочные сертификаты технической поддержки двух типов.

Контакты
commercial@udv.group
8-800-511-65-51

Сайт
udv.group

Телеграм
@udv_group

udv | group