udv|group

UDV DATAPK Industrial Kit 2.2

Что нового?

Содержание

Введение

UDV DATAPK Industrial Kit – это комплексное решение для обеспечения кибербезопасности любых АСУ ТП, которое позволяет быстро начать реагировать на угрозы без негативного влияния на защищаемые системы.

Продукт обеспечивает видимость ландшафта АСУ ТП, позволяет выявлять инциденты на ранних этапах, реагировать на них и выполнить требования регуляторов. UDV DATAPK Industrial Kit использует целостный подход и обширные возможности адаптации под нужды предприятия в рамках единого решения, что позволяет оптимизировать расходы на построение устойчивой защиты АСУ ТП.

Новая версия 2.2 расширяет возможности заказчиков по выстраиванию целостного подхода к информационной безопасности АСУ ТП благодаря улучшениям инструментов для поиска уязвимостей, их устранения, повышению гибкости настройки правил обнаружения вторжений (IDS) и улучшенному пользовательскому интерфейсу.

Ниже вы можете ознакомиться со списком ключевых новых возможностей и улучшений, доступных в UDV DATAPK Industrial Kit 2.2, выпущенном в октябре 2024 года.

Новые возможности

Поддержка сетевого оборудования в модуле управления уязвимостями

Теперь инженеры по информационной безопасности имеют возможность выявлять угрозы ИБ в сетевом оборудовании окружений АСУ ТП с целью их дальнейшего оперативного устранения, что позволяет организациям сократить риски для промышленных ландшафтов.

Вывод рекомендаций по устранению найденных уязвимостей

С выходом версии 2.2 инженеры по ИБ и администраторы компонентов систем АСУ ТП, принимающие непосредственное участие в устранении уязвимостей и установке обновлений, могут опираться на рекомендации, предоставляемые в пользовательском интерфейсе UDV DATAPK Industrial Kit. Благодаря данному нововведению, промышленные организации могут сократить расходы на ИБ и повысить уровень защищенности своих систем.

Улучшения управления правилами обнаружения вторжений (IDS)

UDV DATAPK Industrial Kit 2.2 позволяет экспертам по ИБ сократить трудозатраты на адаптацию правил обнаружения вторжений (IDS) к внутренним политикам ИБ их организации. Теперь создание новых правил IDS может быть осуществлено на базе уже существующих, а уже созданные правила IDS могут быть применены или исключены из применения на индивидуальных сенсорах UDV DATAPK Industrial Kit. Помимо этого, переработаны связанные страницы: расширены возможности фильтрации и просмотра параметров правил IDS, упрощен механизм выполнения операций с множественными правилами, автоматизирован процесс синхронизации правил.

Другие улучшения

Расширение возможностей мониторинга состояния сенсоров UDV DATAPK Industrial Kit

Администраторы UDV DATAPK Industrial Kit теперь имеют больше инструментов для отслеживания быстродействия сенсоров. Добавлены дополнительные виджеты с метриками по событиям ИБ, передаваемым от сенсоров UDV DATAPK Industrial Kit на компонент менеджмент, обработанным сетевым пакетам и событиям ИБ от внешних источников, а также дата и время последнего сбора мониторинговых данных.

Улучшения страницы событий

Версия 2.2 позволяет аналитикам по ИБ сократить время на обработку событий ИБ благодаря расширенным возможностям преднастроенных поисковых фильтров, а также «быстрым» переходам к связанным сенсорам и сетевым потокам. Также, была улучшена структура атрибутов событий ИБ.

Состояние соответствия конфигураций эталонным на странице конфигураций

UDV DATAPK Industrial Kit 2.2 позволяет инженерам по ИБ сократить время на анализ активов, имеющих отклонения от эталонной конфигурации, благодаря отображению состояния соответствия конфигураций активов эталонным непосредственно на странице «Конфигурации».

Операции с множеством инцидентов

Аналитики по ИБ теперь могут более оперативно — в несколько кликов — решать свои задачи благодаря упрощенному механизму выполнения операций над множеством инцидентов.

Другие улучшения

Возможность настройки номера порта веб-сервера

Инженеры внедрения, осуществляющие развертывание версии 2.2, теперь могут настроить номер порта веб-сервера UDV DATAPK Industrial Kit, тем самым адаптировав установку под корпоративные стандарты по информационной безопасности.

Отказ от контейнеризации в пользу RPM-пакетов

С выходом UDV DATAPK Industrial Kit 2.2 администраторы системы могут не задумываться о необходимости развертывать и отслеживать контейнеры и их быстродействие в составе решения. Теперь фундаментом системы являются всем знакомые RPM-пакеты Linux.

Поддержка АСУ ТП и протоколов передачи данных

Поддержка ПЛК Regul (Regul)

В версии 2.2 добавлена возможность анализа сетевого трафика ПЛК Regul отечественного производителя «Прософт Системы», использующего одноименный протокол Regul, а также возможность контроля его конфигураций. Данное улучшение позволяет специалистам по ИБ АСУ ТП анализировать события, выявлять аномальные отклонения конфигурационных параметров и оперативно принимать меры по устранению связанных инцидентов ИБ.

С полным списком улучшений, изменений и исправлений Вы можете ознакомиться в Руководстве по эксплуатации, в разделах «Что нового?» и «Полный список изменений в версии 2.2».

Закажите пилотный проект
или персональную демонстрацию
наших решений

commercial@udv.group udv.group
+7 (800) 511-65-51 vk.com/udv.group

620100, г. Екатеринбург, ул. Сибирский тракт,
12, строение 7, этаж 4 udv.group