udv|group

UDV DATAPK Industrial Kit 2.1

ЧТО НОВОГО?

СОДЕРЖАНИЕ

UDV DATAPK Industrial Kit

Комплекс решений для мониторинга состояния защищенности и оперативного обнаружения инцидентов информационной безопасности в промышленных сетях.

Выпущенная в конце 2023 года версия UDV Industrial Kit 2.0 вывела на рынок масштабные функциональные возможности: переработанную архитектуру взаимодействия компонентов, новый механизм поиска уязвимостей, расширение возможностей анализа сетевого трафика, улучшения пользовательского интерфейса, улучшения быстродействия системы, были расширены списки поддерживаемых операционных систем, промышленных протоколов, источников событий ИБ.

Новый выпуск 2.1 расширяет существующие возможности комплекса, позволяя организациям, использующим UDV DATAPK Industrial Kit еще более эффективно защищать промышленные периметры.

Ниже вы можете ознакомиться со списком ключевых новых возможностей и улучшений, доступных в UDV DATAPK Industrial Kit 2.1, выпущенном в феврале 2024 года.

Панель мониторинга общего состояния ИБ

С выходом версии 2.1, специалисты по ИБ АСУ ТП могут централизованно отслеживать общее состояние безопасности АСУ ТП используя перенастроенную панель мониторинга и оперативно реагировать на инциденты ИБ в режиме реального времени. Новая панель может быть адаптирована для отображении информации по определенным сенсорам UDV DATAPK Industrial Kit, отображает аналитическую информацию за настраиваемые промежутки времени, а также предоставляет возможности для быстрого перехода к детальной информации по активам, инцидентам, вторжениям и сетевым соединениям, что сокращает количество действий, которое аналитикам по ИБ необходимо выполнять для реагирования на выявленные проблемы ИБ.

Улучшения механизма поиска уязвимостей

UDV DATAPK Industrial Kit 2.1 расширяет возможности нового механизма поиска уязвимостей посредством каталога CVE (Common Vulnerabilities and Exposures), добавленного ранее в версии 2.0, позволяя инженерам ИБ АСУ ТП эффективно находить уязвимости в ПЛК и SCADA-системах. Дополнительно, данный выпуск призван повысить точность выявления уязвимостей путем сокращения количества ложных срабатываний (false-positives) и повысить скорость при анализе, а также упростить сам процесс оценки защищенности целевых систем АСУ ТП.

Поддержка БДУ ФСТЭК России

Теперь специалисты по ИБ АСУ ТП помимо каталога CVE и стандарта OVAL имеют возможность выявлять уязвимости в соответствии с Банком данных угроз безопасности ФСТЭК России, что позволяет обеспечивать соответствие требованиям регулятора и обеспечивать актуальную защиту АСУ ТП.

Мониторинг состояния сенсоров DATAPK

UDV DATAPK Industrial Kit 2.1 расширяет возможности мониторинга собственных сервисов и теперь позволяет администраторам системы отслеживать ключевые показатели компонентов комплекса, обеспечивающих сбор данных с целевых АСУ ТП: доступность, потребление вычислительных ресурсов и быстродействие. Данные функциональные возможности позволяют оперативно выявлять узкие места в системе и устранять их.

ДРУГИЕ УЛУЧШЕНИЯ

Контроль параметров технологического процесса

С помощью версии 2.1, специалисты по ИБ АСУ ТП и администраторы АСУ ТП имеют возможность контролировать критические параметры технологического процесса АСУ ТП, изменения которых может привести к катастрофическим последствиям. Данная возможность реализуется благодаря регулярно выпускаемым пакетам экспертизы DATAPK Industrial Kit, которые могут быть адаптированы под потребности того или иного окружения АСУ ТП.

Улучшения страниц событий и инцидентов

Теперь специалисты по ИБ АСУ ТП могут быстрее осуществлять поиск по событиям и инцидентам благодаря наличию преднастроенных быстрых фильтров, дополнительным операторам в поисковой строке и интеллектуальным подсказкам.

ДРУГИЕ УЛУЧШЕНИЯ

Улучшения страницы карты сети

Интерактивная карта сети в UDV DATAPK Industrial Kit 2.1 стала ещё быстрее и удобнее. Добавлена боковая панель, отображающая детальную информацию по каждому сетевому соединению и объекту защиты. На ней можно найти источника и получателя трафика, сетевой протокол, и другие сетевые и инфраструктурные атрибуты. Сделанные улучшения позволяет специалистам по ИБ АСУ ТП оперативнее производить анализ обнаруженных сетевых соединений и определять, какие узлы АСУ ТП участвуют в сетевом взаимодействии.

Поддержка ПЛК Haiwell (Modbus TCP)

Специалисты ИБ АСУ ТП теперь могут анализировать сетевой трафик, собранный с ПЛК Haiwell, использующими протокол Modbus TCP. Версия 2.1 позволяет обнаруживать потенциально опасные сетевые соединения по данному протоколу и управлять ими, что позволяет повысить защищенность окружений АСУ ТП, имеющих в своем составе ПЛК этого производителя.

Поддержка ПЛК ОВЕН (PLC-Browser)

В версии 2.1 добавлена возможность анализа сетевого трафика ПЛК отечественного производителя «Овен», использующего протокол PLC-Browser. Данное улучшение позволяет специалистам по ИБ АСУ ТП анализировать события от ПЛК данного производителя 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 новых версиях".*

udv|group

UDV DATAPK Industrial Kit 2.1

ЗАКАЖИТЕ ПЕРСОНАЛЬНУЮ ДЕМОНСТРАЦИЮ
ИЛИ ПИЛОТНЫЙ ПРОЕКТ

ЗАКАЗАТЬ

КОНТАКТЫ

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

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

support@udv.group
+7 (343) 286-12-03