kaspersky АКТИВИРУЙ БУДУЩЕЕ

Kaspersky Industrial CyberSecurity for Networks 3.0: новые возможности

Недавнее исследование «Лаборатории Касперского» показало, что 44% промышленных предприятий работают над инициативами кибербезопасности в рамках цифровой трансформации операционных технологий (OT)[1]. Это крайне важно, так как в 2020 году кибератакам подверглись 39% автоматизированных систем управления технологическим процессом (АСУ ТП)[2]. Угрозы не должны затрагивать критически важные промышленные процессы. Чтобы не допустить этого, нужно решение, которое защищает все устройства и системы гетерогенной промышленной инфраструктуры. Также необходимо отслеживать уязвимости в программном обеспечении АСУ ТП и не допускать их использования для проведения продвинутых атак, а также максимально снизить возможные последствия инцидентов кибербезопасности.

Расширенная функциональность и управление уязвимостями

Новая версия Kaspersky Industrial CyberSecurity for Networks отмечает уязвимости оборудования и дает рекомендации по снижению возможного ущерба от них, а также отслеживает трафик технологических процессов для выявления подозрительной активности. Теперь решение поддерживает протокол BACnet и может надежно защищать системы, функционирующие в «умных зданиях». Мониторинг трафика с режимом автоматизированного обучения, удобное обновление протоколов и новая веб-консоль упрощают управление и повышают эффективность борьбы с угрозами для промышленных систем.

Благодаря функциям управления уязвимостями клиенты получают данные о новых рисках по мере их возникновения и могут вовремя устранить или минимизировать их. Клиент может использовать консоль управления для доступа к базам данных, содержащим полную и точную информацию об уязвимостях (в том числе CVE-ID), уровне критичности, условиях и возможных последствиях использования уязвимостей, а также для получения рекомендаций по минимизации рисков. Благодаря этой возможности не нужно изучать специализированные отчеты, опубликованные на многочисленных сторонних ресурсах, где не всегда есть полная информация или практические рекомендации. Данные для Kaspersky Industrial CyberSecurity for Networks предоставляет команда экспертов «Лаборатории Касперского» ICS CERT – это глобальный проект, направленный на выявление действующих и потенциальных угроз, нацеленных на промышленные системы автоматизации и промышленный интернет вещей (IIoT).

[1] The State of Industrial Cybersecurity 2020 («Информационная безопасность систем промышленной автоматизации в 2020 году»), сентябрь 2020 года, ARC Advisory Group

[2] Ландшафт угроз для систем промышленной автоматизации. Статистика за второе полугодие 2020 г., 25 марта 2021 г., Kaspersky ICS CERT

Новые возможности

1. Полнофункциональная веб-консоль для взаимодействия с продуктом

- ✓ Информационная панель
  - Возможность персонализации информационной панели
  - Мониторинг потребления ресурсов на серверах и сенсорах (потребление ресурсов)
- ✓ Развертывание из веб-консоли: добавление сенсоров и управление ими
- ✓ Темная тема
- ✓ Карта сети
  - Поддержка до 100 000 узлов
  - Визуализация инцидентов безопасности на карте сети
  - Возможность автоматической группировки объектов на карте (по подсетям, поставщикам или категориям)

2. Управление уязвимостями

- ✓ Обновляемая база данных об уязвимостях промышленных систем (информацию предоставляет команда специалистов ICS CERT «Лаборатории Касперского»)

3. Поддержка новых протоколов (в том числе DPI)

- ✓ Регулярное обновление алгоритмов DPI. Добавление поддержки новых протоколов с ближайшим обновлением баз данных о продукте
- ✓ Поддержка новых промышленных протоколов: MICOM, PROFINET, TASE.2, DirectLOGIC, BACnet
- ✓ Улучшенное распознавание используемых протоколов: IEC104, Rockwell Ethernet/IP, MOXA
- ✓ Мониторинг значений параметров процессов (тегов) в режиме реального времени. Все теги, идентифицированные во время парсинга протоколов, можно просмотреть в едином представлении
- ✓ Обнаружение проблем в зашифрованном трафике (некриптостойкий шифр, самоподписанные сертификаты и сертификаты с истекшим сроком действия)

4. Управление активами

- ✓ Поддержка большого количества активов (до 100 000)
- ✓ Возможность указывать подсеть активов и фильтрация по подсетям
- ✓ Импорт проектов из системы SCADA. Обновляемая база данных систем SCADA, из которых возможен импорт

5. Улучшенный режим обучения

- ✓ Автоматизированная генерация правил для процесса. В процессе обучения выполняется анализ сетевого трафика, и на основе выявленных связей генерируются правила для процесса

6. Списки разрешенных событий

- ✓ Возможность внести любое событие в список разрешенных
- ✓ Возможность просмотреть свойства актива при создании правила
- ✓ Шаблоны распространенных правил
- ✓ Создание адаптированных событий для IT-сетей (меньше оповещений от сетевых плат)

7. Новый REST API для автоматизации операций

- ✓ Расширенная поддержка операций с активами
- ✓ Расширенная информация о тегах
- ✓ Получение данных об обнаруженных уязвимостях через API

8. Возможность создания образов, в состав которых входит продукт (для устройств)

9. Новые возможности управления внешними коннекторами (потребителями API)

- ✓ Расширяемый список поддерживаемых типов без перевыпуска продукта
- ✓ Возможность сохранения настроек коннектора
- ✓ Возможность отображения логотипов для коннекторов

10. Возможность экспорта и импорта конфигурации продукта и списка активов

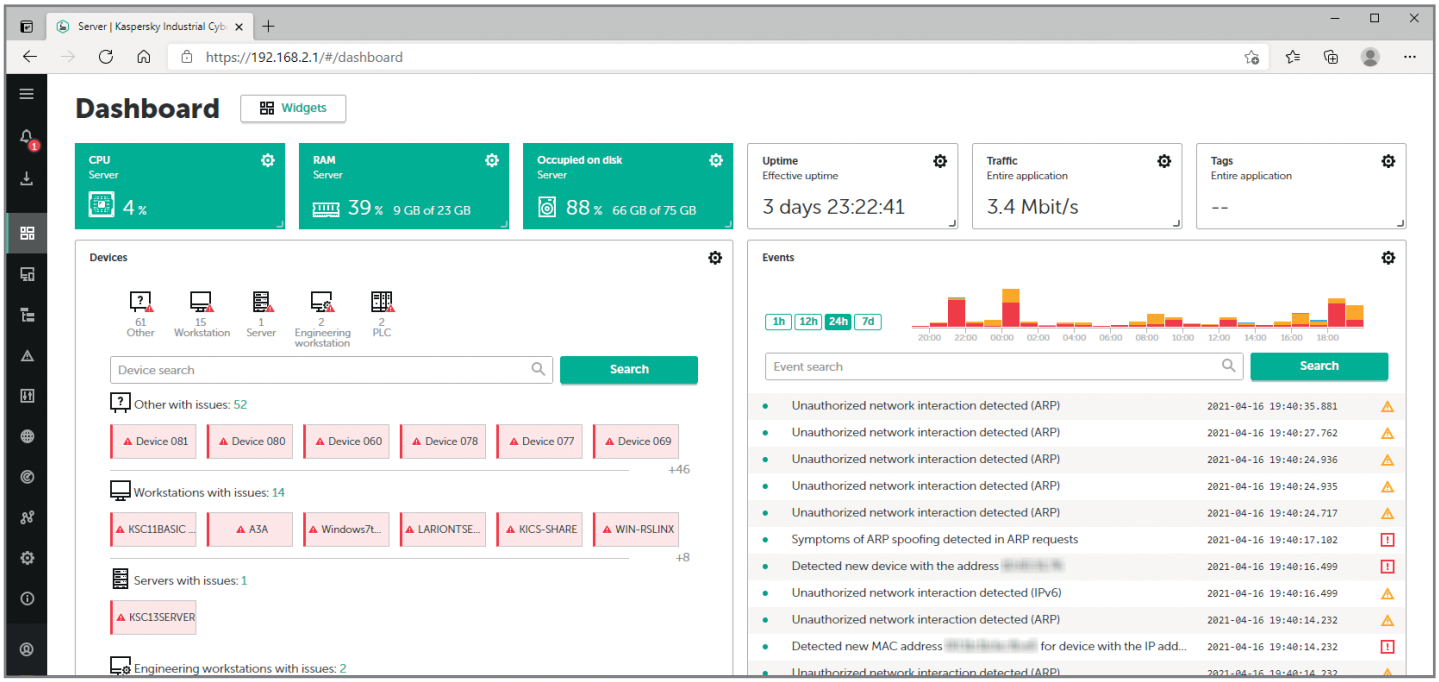
Как это работает

Мы расширили поддержку протоколов и добавили новые – MICOM, PROFINET, TASE.2, DirectLOGIC и BACnet, благодаря чему Kaspersky Industrial CyberSecurity for Networks теперь защищает не только разнообразные промышленные среды и устройства, но и системы автоматизации «умных зданий». Новые протоколы и алгоритмы DPI (технология глубокой проверки пакетов — Deep Packet Inspection) будут установлены во время автоматического обновления баз данных.

Обновленный продукт значительно упрощает создание правил определения отклонений в трафике технологических процессов, которые используются для предотвращения инцидентов безопасности. В новом режиме обучения Kaspersky Industrial CyberSecurity for Networks анализирует изменение параметров производственных процессов (теги) и автоматически создает правила нормального функционирования оборудования, поэтому ИБ-специалисту не нужно создавать их вручную.

В Kaspersky Industrial CyberSecurity значительно улучшены интерфейс и управление. Новая веб-консоль обеспечивает расширенную визуализацию инцидентов для более глубокого анализа угроз. Информация об обнаруженных атаках на АСУ ТП, методах и приемах злоумышленников передается в базу данных MITRE ATT&CK и в дальнейшем может использоваться экспертами по безопасности для анализа и расследования инцидентов. Используя веб-консоль, администратор может быстро развернуть платформу на новом промышленном оборудовании и добавить коннекторы для сторонних систем, например SIEM, сетевых экранов или систем SCADA, через REST API.

Интерфейс Kaspersky Industrial CyberSecurity for Networks



www.kaspersky.ru

Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity – это набор технологий и сервисов, призванный защитить промышленные процессы и узлы всех уровней (включая серверы SCADA, панели HMI, инженерные рабочие станции, ПЛК, сетевые соединения и персональное оборудование), сохраняя при этом стабильность и непрерывность технологических процессов.

Подробнее — на сайте ics.kaspersky.ru