FAQ

Данный раздел содержит список самых частых вопросов и ответов на них по продуктам KICS и MLAD

- FAQ

FAQ

Данная статья содержит список частых вопросов и ответов на них по продукту KICS и MLAD

Вопрос: Какие дистрибутивы в KICS for Networks сертифицированы, а какие текущие? На какие ОС устанавливаются дистрибутивы (текущие и сертифицированные)?

Ответ: Текущая версия KICS for Networks - 4.5 (релиз выйдет в октябре), устанавливается на CentOS Stream 9, сертифицированная версия - 4.3, устанавливается на Astra Linux Special Edition 1.7.

Вопрос: Какие дистрибутивы в KICS for Linux nodes сертифицированы, а какие текущие?

Ответ: Текущая версия KICS for Linux Nodes - 2.0 (релиз - конец сентября), сертифицированная версия - 1.5, **список поддерживаемых ОС**.

Вопрос: Какие отечественные дистрибутивы поддерживает KICS for Nodes для Linux версии 1.5?

Ответ: РЕД ОС 7.3, Гослинукс 7.17, 7.2, Альт Сервер 10, Альт Рабочая станция 10, Альт 8 СП Сервер, Альт 8 СП Рабочая Станция, Astra Linux Common 2.12, Astra Linux SE.

Вопрос: Как получать трафик из сети, построенной на неуправляемых коммутаторах?

Ответ: Неуправляемые коммутаторы не поддерживают функции мониторинга, такие как SPAN/RSPAN, и работают по принципу Plug-and-Play. Есть несколько способов получить трафик:

- Опросить устройства, которые есть в сети и на основании данного опроса сформировать карту сетевых взаимодействий.
- Для критических систем рекомендуется использовать TAP-устройства (Физическое устройство устанавливается между коммутатором и целевым узлом

(сервером, маршрутизатором). Копирует весь трафик (включая коллизии и ошибки) на отдельный порт).
- Установить KICS for Nodes на конечные точки и настроить интеграцию с KICS for Networks. KICS for Nodes будет передавать телеметрию в KICS for Networks.

Вопрос: С каким промышленным оборудованием и программным обеспечением платформа KICS имеет совместимость?

Ответ: С сертификатами совместимости можно ознакомиться по следующей ссылке: **сертификаты совместимости**.

Вопрос: Защищает ли KICS for Nodes от Руткитов и Буткитов?

Ответ: Да, проверка загрузочных секторов дисков и MBR предусмотрена в модуле "Постоянная защита файлов": https://support.kaspersky.com/KICS4Nodes/4.0/ru-RU/171457.htm.

«Включение защиты загрузочных секторов дисков и основных загрузочных записей.

Если флажок установлен, Kaspersky Industrial CyberSecurity for Nodes проверяет загрузочные секторы и основные загрузочные записи на жестких и съемных дисках защищаемого устройства.

По умолчанию флажок установлен».

Вопрос: Как выявить проблему и собрать диагностическую информацию по Kaspersky Industrial CyberSecurity for Nodes?

Ответ: Ответы на частые вопросы и как провести самодиагностику проблем можно получить по следующей ссылке: https://support.kaspersky.ru/corporate/kics-for-nodes-reminder.

Вопрос: При создании резервной копии Сенсора / Сервера KICS for Networks через скрипт kics4net-backup.sh выполняется остановка служб KICS for Networks. Что происходит с трафиком, поступающим на точки мониторинга, в момент остановки служб? Копится в буфер?

Ответ: Трафик не копится в буфер, теряется.

Вопрос: Может ли KEDR Expert работать в сегменте АСУ ТП?

Ответ: KEDR Expert изначально не спроектирован для работы в АСУ ТП, не проходит соответствие сертификаций и тестов совместимости, но в целом вы можете использовать на поддерживаемых ОС на свой страх и риск.

Может сильно влиять на загрузку хостов, промышленную сеть.

Вопрос: Может ли Kaspersky Endpoint Security работать в сегменте АСУ ТП?

Ответ: Нет, Kaspersky Endpoint Security разработан для защиты корпоративного сегмента. Решение KICS for Nodes специально разработан и заточен под специфику АСУ ТП:

- Минимальные аппаратные требования к защищаемым устройствам у KICS for Nodes ниже, чем у KES, что важно для маломощных устройств.
- При установке защитных решений на АРМ с установленным ПО АСУ ТП нужно соблюдать рекомендации производителя АСУ ТП по установке средств защиты (в рекомендация прописываются какие процессы, директории нужно добавлять в исключение, чтобы защитное решение их не блокировало). KICS for Nodes учитывает данный нюанс и при установке предлагает выбрать соответствующий профиль защиты, например, профиль исключения для ПО Simatic Step7, тем самым освобождает от ручной настройки данных рекомендаций. KES данную специфику не поддерживает и с большей вероятность может заблокировать легитимные процессы АСУ ТП, тем самым возникнет риск нарушения важного технологического процесса.
- Во всех защитных модулях KICS for Nodes поддерживается неблокирующий режим, благодаря которому вы можете корректно настроить защитное решение под специфику своей АСУ ТП. Тем самым нивелируется риск ложных сработок и блокировки важных и критических процессов (может заблокировать легитимное ПО АСУ ТП, воспринимая его как угрозу). Поскольку KES заточен под защиту корпоративного сегмента, то он работает преимущественно в блокирующем режиме и порой действует агрессивно. Поскольку корпоративная среда динамично меняется и разрастается, то и к защитным решениям предъявляются требования по ускоренному реагированию.
- Kaspersky Endpoint Security не проходит соответствие сертификаций и тестов совместимости.

Вопрос: Есть ли практика использования модуля мониторинга файловых операций для контроля целостности системных файлов? Если есть, то какие настройки необходимо использовать для этой задачи?

Ответ: Практика примерно такая же, как с другими папками:

- Выполнить запуск задачи в режиме информирования;
- Проанализировать ложные сработки и добавить их в исключения;
- Убедиться, что в процессе работы приложения длительное время нет ложных сработок;
- После того, как ложные сработки добавлены в исключение, при необходимости запускаете блокирующий режим.

Вопрос: Как осуществляется интеграция KICS for Networks с Kaspersky Security Center?

Ответ: При установке Сервера KICS for Networks нужно выбрать параметр **«Добавить функциональность взаимодействия программы с Kaspersky Security Center»**, после чего при установке программы устанавливается компонент Агент администрирования Kaspersky Security Center.

В Kaspersky Security Center нужно установить плагин управления KICS for Networks.

Вопрос: Как осуществляется интеграция Kaspersky Security Center с KICS for Nodes?

Ответ: Для реализации связи между Сервером администрирования Kaspersky Security Center и клиентами на клиентских станциях необходимо выполнить установку агента администрирования KSC. Инсталлятор агента администрирования KSC можно выгрузить из полного дистрибутива Kaspersky Security Center, который использовался для установки на Сервере администрирования. На клиенте запустить установку агента администрирования KSC, принять лицензионное соглашение. В диалоге указать IP-адрес Сервера администрирования. Так же необходимо проверить доступность указанных по умолчанию (TCP 13000; UDP 15000) портов между узлом и сервером администрирования KSC в обе стороны. Дальнейшие настройки оставить по умолчанию, запустить процесс установки и дождаться его завершения. Служба агента администрирования KSC запустится автоматически. После завершения установки требуется проверить, что службе агента администрирования KSC удалось успешно установить связь с Сервером. Для этого необходимо открыть командную строку от имени администратора, перейти в папку C:\Program Files (x86)\Kaspersky Lab\NetworkAgent и выполнить запуск утилиты klnagchk.exe. Убедиться, что утилита выводит сообщение «Попытка соединения с Сервером администрирования...OK».

Вопрос: На сколько примерно Сенсоры уменьшают поток трафика?

Ответ: Сенсоры могут уменьшить поток трафика до 50%.

Вопрос: Где можно ознакомиться с историями успеха?

Ответ: С историями успеха можно ознакомиться по ссылке: **Истории успеха**

Вопрос: Где посмотреть жизненный цикл продуктов?

Ответ: С жизненным циклом можно ознакомится по следующей ссылке: **Жизненный цикл приложений для бизнеса**

Переходим по ссылке и попадаем на страницу «Жизненный цикл приложений для бизнеса». Выбираем интересующее нас приложение и версию, далее сформируется диаграмма, которая отображает информацию о том, до какого времени осуществляется техническая поддержка.

image.png

Вопрос: Как собрать информацию для технической поддержки по продукту Kaspersky Industrial CyberSecurity for Networks?

Ответ: Для технической поддержки требуется предоставить журналы Kaspersky Industrial CyberSecurity for Networks. Для доступа к журналам нужно иметь root-права в операционной системе, где установлен Сервер.

Адреса директорий, где хранятся журналы, представлены в следящей статье:

Директории для хранения данных программы

Помимо журналов техническая поддержка может запросить дополнительные данные о компонентах программы. Требуемые данные можно получить с помощью скрипта централизованной установки компонентов программы *kics4net-deploy-<номер версии программы>.bundle.sh* или с помощью скрипта для локального запуска *kics4net-gather-artefacts.sh,* который находится на компьютере с установленным компонентом программы в директории /opt/kaspersky/kics4net/sbin/.

Чтобы получить данные о компонентах программы с помощью скрипта *kics4net-deploy-<номер версии программы>.bundle.sh:*

На компьютере, с которого выполнялась централизованная установка, перейдите в директорию с распакованными файлами скриптов и пакетов для установки, проверки и

удаления компонентов программы, входящих в комплект поставки. Файлы находятся во вложенной директории *kics4net-release_<номер версии программы>/linux-centos* (в случае использования Astra Linux файлы находятся во вложенной директории *kics4net-release_<номер версии программы>/linux-astra).* Введите команду: *bash kics4net-deploy-<номер версии программы>.bundle.sh --gather-artefacts -<параметр> <имя директории>*

где:

- *<параметр>* – определяет режим получения данных. Предусмотрены следующие параметры:
  - a – для получения всех данных;
  - c – для получения данных о сертификатах;
  - i – для получения данных о конфигурации обнаружения вторжений;
  - t – для получения файлов дампа трафика.
- <имя директории> – имя директории для копирования архивных файлов с данными.
- В приглашениях SSH password и BECOME password введите пароль учетной записи пользователя, от имени которого выполнялась установка компонентов программы.

Пример: *bash kics4net-deploy-<номер версии программы>.bundle.sh --gather-artefacts -a /tmp/data_for_support*

Дождитесь завершения работы скрипта kics4net-deploy-<номер версии программы>.bundle.sh. При успешном завершении файлы будут созданы в указанной директории.

Чтобы получить данные об установленном на компьютере компоненте программы с помощью скрипта *kics4net-gather-artefacts.sh:*

1. Выполните вход в систему с учетными данными пользователя с root-правами.
2. Перейдите в директорию /opt/kaspersky/kics4net/sbin/ и введите команду запуска скрипта для получения данных о компоненте программы: *bash kics4net-gather-artefacts.sh -<параметр> <имя директории>* где:

- <параметр> – определяет режим получения данных. Предусмотрены следующие параметры:
  - a – для получения всех данных;
  - c – для получения данных о сертификатах;
  - i – для получения данных о конфигурации обнаружения вторжений;
  - t – для получения файлов дампа трафика.
- <имя директории> – имя директории для копирования архивных файлов с данными

Пример: *bash kics4net-gather-artefacts.sh -a /tmp/data_for_support*

Дождитесь завершения работы скрипта *kics4net-gather-artefacts.sh.* При успешном завершении файлы будут созданы в указанной директории.

Вопрос: Для интеграции KICS for Nodes (Windows) с KICS for Networks требуется ли закупать отдельные лицензии для KEA?

Ответ: Всё в комплекте в лицензии KICS for Nodes, там есть ключ на KEA.