?????? ???????? ????????????? KICS for Nodes \ KICS for Linux Nodes

> В этой части статьи мы поговорим о рекомендациях по настройкам политик безопасности KICS for Nodes \ KICS for Linux Nodes.

Детальные и универсальных рекомендаций тут вряд ли возможны, потому что:

- технологические процессы бывают разные,
- архитектуры систем АСУ ТП бывают разные,
- функциональные роли, способы и режимы эксплуатации узлов, на которые устанавливается KICS for Nodes \ KICS for Linux Nodes тоже бывают разные.

Но, всё же, мы попробуем дать общие рекомендации и соображения, которые стоит учесть при настройках политик безопасности.

Первоначальное использование всех технологий детектирования рекомендуется в режиме информирования («Только сообщать», «Только статистика») во избежание негативного влияния ложных срабатываний на работу технологический процесс.

На дальнейших этапах при настройке политик следует учитывать два вида рисков:

- риски, обусловленные угрозами безопасности информации;
- риски негативного влияния на работу защищаемого узла, обусловленные некорректными настройками KICS for Nodes.

Если конкретнее, то нужно учитывать следующие факторы:

1) Функциональная роль узла. Чем важнее корректная работа узла для технологического процесса, тем больше нужно уделить внимания возможности ложного срабатывания технологий защиты, чтобы минимизировать влияние на технологический процесс. Для минимизации рисков ложных срабатываний рекомендуется использовать следующие методы:

- Работа технологий детектирования в режиме в режиме информирования (особенно это касается технологий, использующих обновляемые базы сигнатур: антивирусная защита, защита от эксплойтов, защита от сетевых угроз, защита шифрования сетевых файлов и папок. Потому что файлы и сетевые взаимодействия, которые до обновления баз не считались вредоносными, после обновления могут начать таковыми считаться.

- Испытания корректности функционирования узла с заданными/обновленными политиками, обновленными базами в тестовой среде: стенд производителя/поставщика системы АСУ ТП, виртуальные машины;

- Поэтапная установка/обновление баз KICS for Nodes в системе АСУ ТП. Например, в системе есть 10 узлов, на которые нужно установить KICS for Nodes. Если есть такая возможность, то лучше их устанавливать по частям, чтобы в случае каких-либо сложностей иметь эти сложности на минимальном количестве узлов в каждый отдельный момент времени.

- Если система АСУ ТП резервированная, то устанавливать/обновлять базы KICS for Nodes не на обоих каналах сразу, а сперва на одном канале, и в случае, если достаточно длительное время всё идёт хорошо, - на втором канале.

2) Подверженность узла угрозам безопасности информации. Если для узла обеспечивается эшелонированная защита от угроз безопасности информации (меры физической защиты, защита периметра, мониторинг сети, встроенные средства защиты и другие меры), то с учетом функциональной роли узла стоит рассмотреть возможность более длительного использования защитных технологий в режиме информирования. А если узел подвержен угрозам безопасности с высокой вероятностью, например:

- подключен к Интернету,

- находится на периметре сети и взаимодействует со смежными системами,

- не обеспечиваются достаточные меры физической защиты),

то с учетом функциональной роли узла рекомендуется более краткосрочное применение технологий обнаружения в режиме информирования, чтобы узел меньшее количество времени находился в состоянии без активной защиты.

С учетом этих двух основных факторов применим дифференцированный подход и поделим все защищаемые устройства на 4 группы:

Кто-то может ввести более детальную градацию с 6 (2x3), 9 (3x3) группами.

Название группы узлов	Зеленая группа	Желтая группа	Оранжевая группа	Красная группа
Риски ИБ	Низкие	Высокие	Низкие	Высокие
Важность для ТП	Низкая	Низкая	Высокая	Высокая

С учетом специфики каждой группы для них можно рассмотреть следующие наборы настроек:

Название группы узлов	Зеленая группа	Желтая группа	Оранжевая группа	Красная группа
Риски ИБ	**Низкие**	**Высокие**	**Низкие**	**Высокие**
Важность для ТП	**Низкая**	**Низкая**	**Высокая**	**Высокая**
Время применения защитных технологий в режиме информирования перед включением активного режима (для исключения влияния ложных срабатываний)	Короткое	Короткое	Постоянное или длительное	Длительное или постоянное
Настройки постоянной антивирусной защиты	Максимально глубокие настройки, насколько позволяет аппаратная конфигурация узла	Максимально глубокие настройки, насколько позволяет аппаратная конфигурация узла	Поверхностные настройки или отключение	Средние настройки
Применение периодической антивирусной проверки (проверка по требованию)	Максимально глубокие настройки проверки, насколько позволяет аппаратная конфигурация узла	Максимально глубокие настройки проверки, насколько позволяет аппаратная конфигурация узла	Средние настройки проверки по требованию; Использование портативного сканера.	Максимальное глубокие настройки проверки по требованию; Использование портативного сканера.
Частота запуска проверки по требованию	Часто, по расписанию	Часто, по расписанию	Вручную, в период «технологического окна» в фоновом режиме	Вручную, в период «технологического окна» в фоновом режиме
Действия, выполняемые над зараженными и возможно зараженными объектами	Карантин/Удалять	Карантин/Удалять	Только сообщать	Только сообщать
Настройки остальных технологий детектирования	Максимально глубокие настройки, насколько позволяет аппаратная конфигурация узла	Максимально глубокие настройки, насколько позволяет аппаратная конфигурация узла	Поверхностные настройки	Средние настройки

1) Необходимость использования отдельных технологий детектирования. Если какая-либо технология детектирования в контексте конкретного узла не даёт никакой дополнительной защиты от угроз безопасности и это подтверждено проектом и моделью угроз, то стоит рассмотреть возможность отключения этой технологии, чтобы они не потребляли ресурсы узла и не вызывали ложных срабатываний. В случае с KICS for Nodes для Windows отдельные функциональные модули можно даже не устанавливать, ведь

функциональный модуль не сможет оказать негативное влияние на работу узла, если он не установлен.

2) Одной из наиболее затратных в плане ресурсов задач является проверка по требованию, поэтому в случае наличия ограничений ресурсов на узле можно её оптимизировать следующими способами:

- выполнение задачи в фоновом режиме;
- снижение частоты периодического запуска задачи или запуск задачи вручную в период технологического окна;
- снижение глубины работы эвристического анализатора или его отключение;
- настройка объектов проверки;
- проверка только новых и измененных файлов;
- настройка параметров производительности

Revision #2
Created 20 November 2025 13:26:12 by Sergey Malyugin
Updated 25 November 2025 08:29:28 by Sergey Malyugin