KOMRAD Enterprise SIEM 4.5 · FAQ НОУ ДПО «УЦБИ "МАСКОМ"»

FAQ для слушателей

Нужно ли знать KOMRAD заранее?

Нет. Нужно понимать базовую администрирование ОС, сеть VM и смысл журналов событий. На занятии KOMRAD рассматривается как практический представитель класса SIEM.

Что делать, если установка не успевает завершиться?

Переходите на вариант 1 или помогайте группе, у которой стенд уже поднялся. Отчет можно сдать по теоретическому варианту, если вы честно указали ограничение среды.

Почему очистка журнала Windows включена в задание?

Потому что это типовой пример события, которое важно для ИБ: злоумышленник или нарушитель может пытаться скрыть следы. Выполнять очистку можно только в учебной VM.

Почему событие не сразу появилось в KOMRAD?

Проверьте сеть, время на VM, состояние агента/службы, выбранный журнал, сертификаты, IP-адрес KOMRAD и включен ли сбор в интерфейсе.

Какой сетевой режим VirtualBox выбрать?

Главное требование: VM с KOMRAD, Windows 10 и Linux/Astra должны видеть друг друга по IP. Обычно для лаборатории удобны `Сетевой мост` или `Внутренняя сеть`; NAT без проброса портов часто мешает входящим соединениям между VM.

У меня Astra 1.7, а в примере файл для Astra 1.8. Что делать?

Используйте фактический установщик, который вы получили от вендора или преподавателя. Для Astra 1.7 в документации показан пример `komrad_v4.5.22_astra_1.7_amd64.run`; для локального учебного комплекта есть пример `komrad_v4.5.22-demo_astra_1.8_amd64.run`.

Нужно ли ставить Extension Pack?

Да, если это указал преподаватель. Проверьте, что версия Extension Pack совпадает с версией VirtualBox.

Если Windows 10 не пингуется с KOMRAD?

Сначала исправьте сеть VirtualBox. До установки WMI-агента убедитесь, что Windows 10 и KOMRAD находятся в одном сетевом сегменте и `ping KOMRAD_IP` проходит.

Что важнее: установить всё или понять логику?

Для зачета важнее показать понимание: источник события, доставка, отображение в SIEM, вывод. Установка нужна как практический способ это увидеть.