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

Шаблон отчета по практической работе

ФИО:
Группа:
Дата: 14.05
Вариант ПЗ: 1 / 2 / 3

1. Цель

Кратко напишите, что вы проверяли: изучение SIEM, установка KOMRAD, подключение Windows, подключение Linux.

2. Состав стенда

Узел	ОС	IP-адрес	Роль
KOMRAD			SIEM
Windows			Источник событий
Linux			Источник событий

3. Выполненные действия

№	Действие	Команда/операция	Результат
1			
2			
3			

4. События в KOMRAD

Источник	Событие	Где найдено в KOMRAD	Почему важно
Windows			
Windows			
Linux			

5. Выводы

1. Какие события были рутинными?

2. Какие события можно считать подозрительными?
3. Что дала нормализация событий?
4. Какие ГОСТы связаны с регистрацией событий и реагированием?
5. Что бы вы настроили дополнительно в промышленном стенде?