

Бауманский учебный центр «Специалист»

Программа курса KL 034.4: Kaspersky Unified Monitoring and Analysis Platform. Administration (Поиск угроз и реагирование на инциденты ИБ для администраторов)

Код курса: КЛ034

Тема	Ак. часов
Модуль 1. Общие сведения	1
Модуль 2. Архитектура	1
Модуль 3. Установка	2
Модуль 4. Сбор и обработка событий	2
Модуль 5. Интеграции	2
Модуль 6. Хранение событий	1
Модуль 7. Корреляция	4
Модуль 8. Алерты	1
Модуль 9. Реагирование	4
Модуль 10. Мониторинг состояния источников и метрики	2
Модуль 11. Лабораторные работы • Лабораторная работа 1. Установить Kaspersky Unified Monitoring and Analysis Platform. • Лабораторная работа 2. Настроить получение событий с помощью агента Windows (WMI). • Лабораторная работа 3. Настроить получение событий из DNS. • Лабораторная работа 4. Настроить получение событий от Kaspersky Endpoint Security для Windows. • Лабораторная работа 5. Настроить получение событий Linux. • Лабораторная работа 6. Настроить получение событий Kaspersky Security Center. • Лабораторная работа 7. Настроить получение событий Kaspersky Anti Targeted Attack Platform. • Лабораторная работа 8. Настроить получение EDR-телеметрии из KATA. • Лабораторная работа 9. Импортировать информацию о компьютерах из Kaspersky Security Center. • Лабораторная работа 10. Настроить обогащение событий с помощью Active Directory. • Лабораторная работа 11. Настроить интеграцию с Kaspersky Endpoint Detection and Response. • Лабораторная работа 12. Настроить интеграцию с CyberTrace. • Лабораторная работа 13. Настроить холодное хранение событий в KUMA. • Лабораторная работа 14. Настроить мониторинг состояния источника. • Лабораторная работа 15. Выполнить резервное копирование ядра (дополнительно). • Лабораторная работа 16. Настроить получение событий с помощью агента Windows (WEC) (дополнительно). • Лабораторная работа 17. Настроить маршрутизацию событий (дополнительно). • Лабораторная работа 18. Настроить авторизацию через Active Directory. • Лабораторная работа 19. Настроить получение событий через rsyslog. • Лабораторная работа 20. Обеспечить отказоустойчивость ядра. • Лабораторная работа 21. Обеспечить отказоустойчивость коллектора.	
Аудиторная нагрузка в классе с преподавателем	20 ак.ч. + 20 ак.ч. самостоятельно

По окончании обучения на курсе проводится итоговая аттестация. Аттестация проводится в виде теста на последнем занятии или на основании оценок практических работ, выполняемых во время обучения на курсе.

Контакты центра

Для частных лиц
+7 (495) 232-32-16

Для организаций
+7 (495) 780-48-44

E-mail
info@specialist.ru