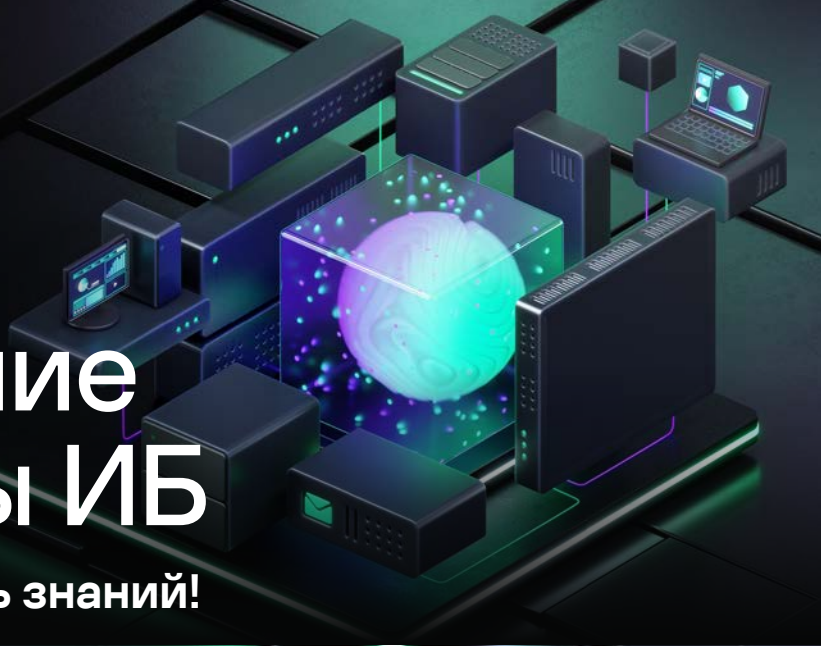
Технические курсы
«Лаборатории Касперского»



Поиск угроз и реагирование на инциденты ИБ

Разблокируйте новый уровень знаний!

Погрузитесь в новые знания с **Авторизованными Учебными Центрами «Лаборатории Касперского».** Тренинги по продукту для бизнеса от лидера решений в сфере IT-безопасности повысят ваш профессиональный уровень и расширят перспективы.

KL 034. Kaspersky Unified Monitoring and Analysis Platform. Administration

Kaspersky Unified Monitoring and Analysis Platform (KUMA) является решением класса SIEM, для сбора, хранения обработки, корреляции и визуализации разрозненных данных. Курс знакомит с архитектурой и возможностями решения, рассказывает и показывает, как выполнить установку и настройку решения на многочисленных примерах. Материалы курса включают слайды с описанием принципов работы и настройки, а также лабораторные работы для закрепления практических навыков настройки.

По окончании курса слушатели смогут:

- Развернуть Kaspersky Unified Monitoring and Analysis Platform для демонстрации решения;
- Настроить получение событий из разных источников и в разных форматах;
- Настроить взаимодействие с внешними системами с целью обогащения событий и реагирования на инциденты;
- Отслеживать состояние источников и компонентов системы.

KL 051. Kaspersky Unified Monitoring and Analysis Platform. Investigation

Kaspersky Unified Monitoring and Analysis Platform (KUMA) является решением класса SIEM для сбора, хранения, обработки, корреляции и визуализации разрозненных данных. Теоретический материал и лабораторные работы дают необходимые знания и навыки, благодаря которым слушатель сможет выполнять задачи по детектированию и обнаружению угроз, используя **Kaspersky Unified Monitoring and Analysis Platform**.

По окончании курса слушатели смогут:

- Настраивать обработку событий (нормализация, агрегация, обогащение);
- Создавать правила корреляции и анализа данных для выявления угроз;
- Создавать различные правила реагирования на угрозы;
- Использовать ресурсы и функции KUMA для анализа и выявления угроз (активные списки, словари, переменные, API);
- Выявить угрозы, анализируя полученные события.

kaspersky

KL 048. Kaspersky XDR Expert. Administration

XDR Expert — надёжное решение для кибербезопасности для защиты корпоративной ИТ-инфраструктуры от сложных киберугроз.

XDR Expert позволяет:

- Собирать телеметрию и хранить её в виде удобном для анализа.
- Вручную и автоматически анализировать собранные данные и выявлять угрозы.
- Опираясь на отчеты и панель мониторинга комплексно оценивать уровень корпоративной безопасности.
- Анализировать этапы развития киберугроз, используя граф расследования.
- Автоматически и вручную реагировать на угрозы, что в комбинации с интеграционными возможностями продукта позволяет реализовывать сложные сценарии защиты.
- Эффективно работать с собранными данными. Интерфейс предоставляет пользователю удобные методы взаимодействия, включая контекстные действия по поиску и реагированию, отображению данных, построение графа расследования.

Слушатель сможет спланировать и выполнить развертывание и настройку решения, будет понимать принципы использования решения и сможет выполнять задачи по его обслуживанию.

KL 059. Kaspersky XDR Expert. Investigation

Теоретический материал и лабораторные работы курса дают необходимые знания и навыки, благодаря которым слушатель сможет понять принципы использования решения и сможет выполнять задачи по детектированию и обнаружению угроз, используя XDR Expert.

В ходе практических лабораторных работ слушатель сможет смоделировать различные угрозы и выполнить их детектирование и анализ, используя возможности XDR Expert, среди которых:

- Анализ полученной телеметрии с конечных узлов;
- Выявление комплексных атак и реагирование на них;
- Возможности по построению графа расследования;
- Автоматизация реагирования с использованием плейбуков.