KL 032.1.1:

Kaspersky Symphony XDR Core

Описание курса

Kaspersky Symphony XDR Core — надежное решение для кибербезопасности для защиты корпоративной ИТ-инфраструктуры от сложных киберугроз.

Kaspersky Symphony XDR Core позволяет:

- Собирать данные из множества различных источников и хранить их в виде удобном для анализа. Службы-коллекторы способны получать и приводить к единому формату данные из множества различных источников. Данные хранятся в аналитической высокопроизводительной СУБД ClickHouse. Продукт поставляется с набором готовых к использованию нормализаторов.
- Вручную и автоматически анализировать собранные данные и выявлять угрозы. Корреляторы имеют гибкие возможности для реализации даже самой сложной логики детектирования. В комплект поставки включен набор разнообразных правил корреляции.
- Опираясь на отчеты и панель мониторинга комплексно оценивать уровень корпоративной безопасности.
- Анализировать этапы развития киберугроз используя граф расследования.
- Анализировать действия угрозы, используя собранную телеметрию, при интеграции с решением KEDR.
- Управлять конечными устройствами и надежно защищать их с помощью Kaspersky Endpoint Security.
- Автоматически и вручную реагировать на угрозы, что в комбинации интеграционными возможностями продукта позволяет реализовывать сложные кросс-продуктовые сценарии защиты.
- Эффективно работать с собранными данными. Веб-интерфейс предоставляет пользователю удобные методы взаимодействия, включая контекстные действия по поиску и реагированию, визуализации данных, построение графа расследования.

Теоретический материал и лабораторные работы дают необходимые знания и навыки, благодаря которым слушатель сможет спланировать и выполнить развертывание и настройку решения, будет понимать принципы использования решения и сможет выполнять задачи по его обслуживанию.

Длительность

1.5 дня (12 часов)

Требования к участникам

Чтобы успешно усвоить весь материал данного курса вам требуются знания и навыки работы с

Kaspersky Unified Monitoring and Analysis Platform (KUMA) и Kaspersky Security Center (KSC), которые вы можете получить пройдя следующие учебные курсы:

- Kaspersky Unified Monitoring and Analysis Platform (курс KL 034)
- Kaspersky Security Center (курс KL 002)

Содержание