САВРУС

СРЕДА АНАЛИЗА И ВИЗУАЛИЗАЦИИ РИСКОВ
В УПРАВЛЕНЧЕСКИХ СИСТЕМАХ

Описание курса для аналитиков
SIEM системы САВРУС

ООО «САВРУС»
125445, г. Москва, ул. Смольная, д. 24А, этаж 10, офис № 1029
ИНН/КПП 7743266740/774301001, ОГРН 1187746699546

ОПИСАНИЕ КУРСА

Наименование курса: Аналитик САВРУС**.**

Формат проведения:

Данный курс может быть проведён в двух форматах:

- очный формат обучения на территории заказчика;
- удалённый формат обучения с использование приложения для онлайн конференций.

Описание/цель курса:

Прослушивание данного курса даёт возможность познакомиться и освоить функционал аналитика SIEM системы САВРУС. В курсе затрагиваются вопросы по работе с функционалом SIEM системы САВРУС и основными компонентами/инструментами консоли САВРУС.

Описание аудитории курса:

Курс предназначен для:

- специалистов конечных пользователей SIEM системы САВРУС, которые выполняют функции по работе с SIEM системой САВРУС;
- специалистов интеграторов, которые производят внедрение или сопровождение SIEM системы САВРУС;
- специалистов, желающих закрепить свои знания по продукту SIEM системы САВРУС в части функционала системы.

Количество обучающихся в группе:

Размер группы для обучения составляет от 3 до 7 обучающихся.

Приобретаемые навыки:

После прослушивания курса обучающиеся приобретают навыки по работе с базовыми компонентами и ресурсами консоли SIEM системы САВРУС. Приобретаются базовые знания принципов сбора и получения событий от источников и способности проведения аналитических расследований инцидентов, а также вырабатываются навыки по работе с поиском событий, визуализацией и отчётностью в системе.

Продолжительность курса:

Курс рассчитан на 12 академических часов.

Рекомендации по расписанию:

Курс рассчитан на 2 дня с 10:00 до 17:00 с учётом перерывов.

Учебные материалы:

К курсу предоставляются презентации и практические материалы в электронном виде.

Материальное обеспечение курса:

При очном проведении курса на территории заказчика необходимо предоставление следующего оборудования:

- индивидуальные рабочие станции и/или виртуальные машины;
- проектор с экраном;
- флипчарт;
- сервер (удалённый сервер) со стендом.

При необходимости возможно предоставление с нашей стороны виртуальных машин и сервера со стендом.

При удалённом формате обучение происходит с использование приложения для онлайн конференций и на заранее развёрнутом исполнителем стенде и подготовленных виртуальных машинах для каждого обучающегося.

Предварительная подготовка к курсу:

Слушатель должен иметь представление о принципах проведения расследований инцидентов информационной безопасности (ИБ), должен иметь представление о принципах работы информационных систем в части аудита и регистрации событий ИБ, владеть базовыми навыками работы с серверными платформами ОС Windows, иметь базовые знания основ построения информационных сетей.

Программа курса:

День 1

1. Вводная презентация к курсу.
2. Вводная презентация по SIEM системе САВРУС.
3. Архитектура программно-аппаратного комплекса, компоненты ПАК.
4. Практическая работа по установке консоли САВРУС.
5. Обзор консоли САВРУС.
6. Обзор компонентов и инструментов консоли;
    - активные каналы;
    - визуализация событий;
    - дашборды;
    - правила корреляции;
    - активные листы;
    - контекстный поиск;
    - мониторинг;
    - отчётность.

День 2

1. Презентация по созданию, редактированию и работе правил корреляции и активных листов в SIEM системе САВРУС.
2. Практическая работа по созданию, настройке и управлению компонентов и инструментов в консоли САВРУС.
3. Практическая работа по работе с правилами и активными листами в SIEM системе САВРУС.
4. Практика работы с инцидентами.
5. Разбор практических примеров и практическая работа в группах.