САВРУС

СРЕДА АНАЛИЗА И ВИЗУАЛИЗАЦИИ РИСКОВ
В УПРАВЛЕНЧЕСКИХ СИСТЕМАХ

Описание курса для администраторов 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: Администратор 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 администрирования и сопровождения SIEM системы САВРУС. В курсе затрагиваются комплексные вопросы грамотного развёртывания SIEM системы САВРУС с нуля и доработки системы в части вопросов администрирования, подключения новых источников и основ troubleshooting.

Описание аудитории курса:

Курс предназначен для:

- специалистов конечных пользователей SIEM системы САВРУС, которые выполняют функции администрирования и сопровождения SIEM системы САВРУС;
- специалистов интеграторов, которые производят внедрение или сопровождение SIEM системы САВРУС;
- специалистов, желающих закрепить свои знания по продукту SIEM системы САВРУС в части администрирования системы.

Количество обучающихся в группе:

Размер группы для обучения составляет от 3 до 7 обучающихся.

Приобретаемые навыки:

После прослушивания курса обучающиеся приобретают навыки развёртывания системы с нуля, навыки решения нестандартных ситуация в ходе внедрения, администрирования и сопровождения системы, навыки работы с базовыми компонентами и ресурсами Консоли SIEM системы САВРУС, приобретаются базовые знания принципов сбора и получения событий от источников, навыки формирования технических требований на этапе подготовки источников к подключению к системе.

Продолжительность курса:

Курс рассчитан на 7 академических часов.

Рекомендации по расписанию:

Курс рассчитан на 1 день с 10:00 до 19:00 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 серверных подсистемах и основах виртуализации, базовые навыки администрирования серверных платформ на базе ОС Windows и RHEL (CentOS), базовые знания построения информационных сетей.

Программа курса:

- вводная презентация к курсу;
- вводная презентация по SIEM системе САВРУС;
- архитектура программно-аппаратного комплекса, компоненты ПАК;
- жизненный цикл события в системе;
- настройка аудита в источниках событий;
- практическая работа по развёртыванию SIEM системы САВРУС с нуля;
- обзор консоли САВРУС;
- компоненты и инструменты консоли;
- практическая работа по созданию, настройке и управлению объектами в консоли САВРУС;
- управление пользователями в системе;
- поиск и устранение неисправностей (Troubleshooting);
- разбор практических примеров и практическая работа в группах.