Программа обучения
«Администрирование «СёрчИнформ Мониторинг безопасности» (СёрчИнформ SIEM)»

Цель: овладение слушателями навыками администрирования и использования «СёрчИнформ Мониторинг безопасности» (СёрчИнформ SIEM) в профессиональной деятельности в сфере информационной безопасности.

Формы проведения обучения: лекции и практика.

Категория слушателей: сотрудники службы системных администраторов и службы информационной безопасности предприятий и организаций.

День 1

10.00 – 11.20 **Общее описание и назначение систем класса «СёрчИнформ Мониторинг безопасности» (СёрчИнформ SIEM)** (лекция)

Описание класса систем управления инцидентами информационной безопасности (SIEM). Назначение, место в структуре безопасности, общие положения систем управления инцидентами информационной безопасности (SIEM).

11.20 – 11.40 **Перерыв**

11.40 – 13.00 **Описание состава «СёрчИнформ Мониторинг безопасности» (СёрчИнформ SIEM), способов разворачивания, необходимых элементов** (лекция)

Описание способов установки Центр администрирования (DataCenter) и «СёрчИнформ Мониторинг безопасности» (СёрчИнформ SIEM). Особенности разворачивания, установки систем. Раздача прав. Детали по установке и администрированию MongoDB. Возможности по использованию в сложной структуре.

13.00 – 14.00 **Обед**

14.00 – 16.00 **Общая настройка «СёрчИнформ Мониторинг безопасности» (СёрчИнформ SIEM)** (лекция)

Центр администрирования (DataCenter). Разделы «Меню» и «Администрирование».

Нюансы внутренних и внешних настроек «СёрчИнформ Мониторинг безопасности» (СёрчИнформ SIEM). Работа с коннекторами, подключение источников. Уведомление о бездействии источников. Детали архивного копирования.

День 2

10.00 – 12.00 **Работа с правилами и инцидентами. Способы создания пользовательских правил и подключения новых источников** (лекция)

Работа с разделами «Правила» и «Инциденты». Интерфейс закладок, их функционал. Способы работы с правилами, сортировка, фильтрация, экспорт и печать данных. Корректировка правил, создание пользовательских правил. Закладка «Инциденты» – настройка и применение.

12.00 – 13.00 **Обед**

13.00 – 15.00 **Панели графических представлений** (лекция)

Карта инцидентов, Карта подключений, Сканер сети и Дашборд.

Самостоятельная работа

1 день **Разворачивание Центра администрирования (DataCenter), Консоли аналитика и «СёрчИнформ Мониторинг безопасности» (СёрчИнформ SIEM)** (практика)

Разворачивание, подключение лицензий, настройка распределения лицензий, интеграция с Active Directory, настройка прав доступа. Практическая работа, которую учащиеся должны выполнить в своей сети (допустимо как разворачивание на отдельном стенде – тогда нужен тестовый контроллер домена, так и разворачивание в рабочей сети – тогда нужны права доступа к рабочему контроллеру домена).

Настройка Центра администрирования (DataCenter), Консоли аналитика и «СёрчИнформ Мониторинг безопасности» (СёрчИнформ SIEM) (практика)

Центр администрирования (DataCenter) – настройка подключения к Telegram (опционально, потребуется действующий аккаунт Telegram), настройка записи логов действий пользователя, настройка уведомлений об окончании места на сервере «СёрчИнформ Мониторинг безопасности» (СёрчИнформ SIEM).

«СёрчИнформ Мониторинг безопасности» (СёрчИнформ SIEM) – настройка архивного копирования. Скрытие коннекторов и правил, изменение уровня записи логов служб. Подключение удаленной консоли (нужна дополнительная отдельная АРМ). Создание белых и черных списков, изменение флагов. Подключение источников данных (как минимум 1 источник для Контроллера событий Windows (WinEventConnector), 1 источник для Контроллера Microsoft SQL (MSSqlConnector) – можно от Центра администрирования (DataCenter)), настройка уведомлений о бездействии источников данных. Направления потоков событий системных журналов (syslog) по нескольким коннекторам при помощи предоставляемой утилиты.

Тестирование

1 час (для каждого обучающегося)	**Тестирование в устной и практической форме** Осуществляется представителем вендора (зачет).