
# Splunk Getting Started

***Авторский курс RRC Security, официального дистрибьютора Splunk***

## Описание курса

Курс проходит полный рабочий день с перерывами на обед и кофе и состоит из презентационных материалов и лабораторных работ, выполняемых слушателями на своих компьютерах. Для эффективного прохождения программы всем участникам передается комплект документов, примеры данных для заданий и дистрибутивы ПО.

## Программа

- задачи, для которых целесообразно использовать Splunk;
- архитектура решения и базовые принципы масштабирования решения ;
- архитектура агентов и структура попадания данных в Splunk ;
- хранение данных в Splunk;
- использование функционала поиска в Splunk;
- приложение Splunk for Windows Infrastructure;

(отдельная лабораторная посвящена установке и настройке данного приложения на компьютерах слушателей. Эта лабораторная возможна только на ноутбуках с ОС Windows);

- использование функционала тревог и предупреждений в Splunk;
- использование базовых статистических команд Splunk и базовых команд для аналитики;
- корреляция данных с помощью Splunk на примере объединения в транзакции множества событий;
- использование справочников для обогащения данных, полученных в Splunk ;
- нанесение данных на карту и обогащение их гео информацией;
- модели данных и Pivot в Splunk;
- извлечение полей и работа с текстом в контексте работы Splunk;
- приложения в Splunk;
- расширенные аналитические функции Splunk и функционал машинного обучения.

Обучение проходит на ноутбуках слушателей.

**Требования к ПО:** Windows, Mac OS, возможен Linux, одна из лабораторных может быть выполнена только на платформе Windows. Необходимо заранее установить последнюю версию Splunk Enterprise (Trial), которую можно скачать с сайта из раздела «Free Splunk» — *https://www.splunk.com/en_us/download/splunk-enterprise.html*. Ноутбуки для обучения должны иметь RAM >4 Гб и как минимум 6 Гб свободного места на жестком диске, куда устанавливается Splunk.

Обучение бесплатное. Количество мест ограниченно.
При регистрации обязательно указать название компании и корпоративный электронный адрес.

Более подробно узнать о курсе и ближайших датах обучения можно у Евгении Огай, менеджера по продукту Splunk компании RRC jane@rrc.kz

Ждем Вас на наших тренингах!

Обучение будет проходить по адресу: г. Алматы, ул. Гоголя 127/1, гостиница КАЗЖОЛ