КУРС SPLUNK DEVELOPER

Длительность: 24 часа | Форма проведения: очная, 3 дня по 8 часов | **РЕГИСТРАЦИЯ**

Цель курса

Освоение платформы Splunk для самостоятельного решения практических задач. Получение навыков по анализу машинных данных, построению отчетности, пользовательской модификации интерфейса и разработке дополнительной функциональности. Формирование знаний об архитектуре решений на базе Splunk, языке поисковых запросов (SPL), способе построения специализированных приложений на платформе Splunk и наборе доступных средств разработчика.

Для кого предназначается курс?

— Специалисты, эксплуатирующие Splunk в своих организациях. Курс будет полезен для тех, кто хочет повысить эффективность использования Splunk и реализовать новые практические задачи.

— Специалисты, которые хотят повысить уровень знаний в области управления данными. Навыки работы с платформой Splunk будут востребованы при реализации проектов в области Big Data, информационной безопасности, ИТ-мониторинга и бизнес-аналитики.

Необходимая подготовка

Обязательно

— Базовые навыки работы с консолью Linux
— Базовые навыки работы с XML
— Наличие ноутбука, удовлетворяющего минимальным требованиям:
  - любая операционная система
  - установленный браузер (допустимы последние версии Firefox, Chrome, Safari, IE 11)
  - клиент SSH
  - клиент RDP
  - больше 1 Гб ОЗУ

Дополнительно

— Опыт работы с JS
— Опыт работы с Python

Содержание курса

Курс строится на материалах сертифицированных учебных программ Splunk и дополняется практическим внедрения Splunk в российский компаниях. Практические задания реализуются на лабораторном стенде со специально подготовленным набором тестовых данных. В качестве источников данных выступают как наиболее распространенные ИТ-решения, так и специализированные средства защиты информации.

ДЕНЬ #1. ОСНОВЫ ИСПОЛЬЗОВАНИЯ SPLUNK

1. Знакомство со Splunk
2. Изучение интерфейса Splunk
3. Введение в механизм поиска по данным
4. Применение поисковых механизмов
5. Дополнительная обработка результатов поиска
6. Создание отчетов и визуализация данных

новое 7. Практика применения SPL

ДЕНЬ #2. ПРОДВИНУТОЕ ИСПОЛЬЗОВАНИЕ SPLUNK

1. Создание дашбордов, использование Simple XML
2. Расширение функциональности дашбордов
3. Работа с объектами знаний (Knowledge Objects)
4. Работа с полями в Splunk
5. Построение отчетности, схемы оповещения и реагирования

новое 6. Введение в Data Model

ДЕНЬ #3. РАЗРАБОТКА И ИНТЕГРАЦИЯ РЕШЕНИЙ НА SPLUNK

1. Обзор архитектуры Splunk и лицензирование
2. Источники данных, индексирование данных и понятие индекса
3. Ролевая модель Splunk
4. Приложения и надстройки (Apps и Add-ons)
5. Интеграция со сторонними системами

новое 6. Создание пользовательских Alert Action и Modular Input

День #1. Основы использования Splunk

1. Знакомство со Splunk

— позиционирование Splunk
— области применения Splunk
— описание возможностей получения данных в Splunk
— описание этапов жизненного цикла обработки данных в Splunk
— описание основных компонентов платформы Splunk
— описание возможностей поиска и визуализации данных

2. Изучение интерфейса Splunk

— базовые термины и определения, используемые в курсе
— описание лабораторной среды и демонстрационного стенда
— введение в интерфейс Splunk, основная навигация
— обзор приложений на базе платформы Splunk

3. Введение в механизм поиска по данным

— выполнение базовых поисковых запросов
— работа с временными диапазонами поисковых запросов
— определение содержания результатов поиска
— детализация/уточнение результатов поиска
— использование временной шкалы
— работа с событиями
— управление поисковыми заданиями

4. Применение поисковых механизмов

— структура языка поисковых запросов (SPL)

- обзор основных команд поиска и методов поиска
- команды, трансформирующие данные: top, rare, stats

5. Дополнительная обработка результатов поиска

- работа с результатами поиска: фильтрация, детализация, группировка
- корреляция данных: формирование событий, работа с транзакциями, группировка полей

6. Создание отчетов и визуализация данных

- сохранение поиска в виде отчета (Reports)
- редактирование отчетов
- варианты визуализации данных (диаграммы, графики, таблицы и прочее)
- создание панелей инструментов (Dashboards)
- добавление отчетов на панель инструментов
- изменение панелей инструментов
- визуализация результатов работы статистических и трансформирующих команд
- обогащение визуализации, использование команд trendline, iplocation, geostats и аналогов

7. Практика применения SPL

Интерактивная лекция. Лектор подключается к Splunk и формирует поисковые запросы, используя полезные, но редко используемые команды, параллельно объясняя синтаксис и алгоритм их работы:

- механизм subsearch
- команды streamstats, eventstats
- команда autoregress
- dynamic eval
- способы построения транзакций: transaction, stats, join, append, map

День #2. Продвинутое использование Splunk

1. Создание дашбордов, использование Simple XML

- знакомство со способами создания дашбордов
- изучение внутренней структуры основанных на Simple XML дашбордов
- типы визуализации, расширенная настройка визуализации с помощью Simple XML
- автоматическое обновление дашбордов

2. Расширение функциональности дашбордов

- понятие токена, использование токенов для управления вводом пользователя
- использование механизма post-process search для ускорения работы дашбордов
- расширение функциональности дашбордов с помощью пользовательских JS-скриптов и стилей CSS

3. Работа с объектами знаний (Knowledge Objects)

- обзор типов источников событий и типов данных
- управление правами доступа к данным
- политика согласованного именования объектов знаний
- инструмент lookup и его применение для обработки данных
- создание, настройка lookup, размещение в файле, автоматизация
- создание и использование тегов (Tags)

- описание типов (Event Types) событий, их создание и использование
- использование макросов (Macros) с применением параметров
- применение сценариев реагирования (Workflow Actions): функции GET, POST и Search

4. Работа с полями в Splunk

- изучение механизма Field Extractor (FX)
- определение вариантов для извлечения полей с использованием FX
- обзор процесса извлечения полей вручную с использованием FX
- использование FX для изменения извлекаемых полей
- псевдонимы полей данных (Field Aliases) и вычисляемые поля (Calculated Fields)

5. Построение отчетности, схемы оповещения и реагирования

- создание и настройка отчетов по расписанию (Scheduled Reports)
- создание оповещений (Alerts), использование полей в оповещениях
- нестандартные действия оповещений (Alert Actions)

6. Введение в Data Model

- построение и акселерация Data Model
- практика применения Data Model в поисковых запросах
- описание общей информационной модели (CIM – Common Information Model)

День #3. Разработка и интеграция решений на Splunk

1. Обзор архитектуры Splunk и лицензирование

- описание основных компонентов платформы Splunk
- внутренняя архитектура платформы
- общие требования Splunk: права доступа, синхронизация времени, сетевые порты
- особенности использования в виртуальной среде
- варианты лицензирования и контроль использования лицензии

2. Источники данных, индексирование данных и понятие индекса

- варианты сбора данных
- применение Universal Forwarder
- индексирование данных, обзор индексов (Indexes)
- разделение информации на отдельные индексы

3. Ролевая модель Splunk

- описание механизмов ролевого доступа
- пользователи (Users), роли (Roles) и возможности (Capabilities)
- варианты аутентификации и интеграция ролевой модели с Microsoft Active Directory

4. Приложения и надстройки (Apps и Add-ons)

- структура каталогов Splunk
- приложения (Apps) и надстройки (Add-ons)
- структура приложений и конфигурационные файлы Splunk
- создание собственных приложений и надстроек
- установка приложений и технических надстроек из базы Splunkbase
- обзор премиальных приложений Splunk: Enterprise Security, UBA, ITSI

5. Интеграция со сторонними системами

— обзор методов интеграции
— использование Splunk REST API и SDK
— использование Splunk Web Framework для поиска и визуализации данных

6. Создание пользовательских Alert Action и Modular Input

— пользовательские источники данных и активные действия Splunk
— создание пользовательских источников данных
— создание пользовательских активных действий Splunk
— приложение Splunk Add-on Builder