ТОО «INTELLA»
010000, г. Астана, р-н Есиль
ул. Д. Кунаева, 29/1, оф.1903
БИН 080840000052

+ 7(7172) 28 00 82
+7(727) 355 02 34
info@intella.kz
www.intella.pro

ПРИГЛАШЕНИЕ
На обучающий тренинг:

IS-DLPBASE Технологии обнаружения и оповещения об утечках информации и угрозах информационной безопасности и основы конфигурирования DLP-систем

- **Домен знаний:** технологии СУИБ
- **Сертификация:** Certified Specialist - DLP
- **Статус тренинга:** авторский INTELLA
- **Длительность:** 2 дня (20 ак.часа)
- **Тренер:** Алексей Зайончковский
- **Форма обучения** аудиторные занятия
- **Место проведения** На базе центра повышения квалификации: «INTELLA»
  г.Алматы, ул.Ауэзова, 60 БЦ “Almaty Residense” 6 этаж офис 17а
  тел. +7 (727) 355 02 34
  г.Астана, 010000, г. Астана, р-н Есиль ул. Д. Кунаева, 29/1, оф.1903
  тел. +7 (7172) 28 00 82
- **Даты проведения** ведется набор
- **Расписание** с 10.00 до 18.00, обед с 13.00 до 14.00.
- **В стоимость включено:** Раздаточный материал (в электронном и печатном виде) Кофе-брейки

Аннотация тренинга

Цель курса: Ознакомление слушателей с вопросами подготовки и внедрения систем обнаружения и оповещения об утечках информации и угрозах информационной безопасности (DLP-систем) в компании.

Сбалансированный тренинг по технологиям обнаружения и оповещения об утечках информации и угрозах информационной безопасности и основам конфигурирования DLP-систем, который даёт достаточно информации для построения целостной картины работы DLP-систем. Тренинг построен по модульной системе, которая облегчает понимание и значительно увеличивает процент усвоенной информации.
Тренинг написан по новейшей методике, основой которой является оптимизация возврата инвестиций Тренинга и оптимальное соотношение цена/время/качество.
Половина времени отводится на практические занятия.
По окончанию тренинга слушатель получает достаточно знаний и навыков для того, чтобы самостоятельно распланировать и внедрить систему защиты от утечек чувствительной информации.

Основные преимущества тренинга:

1) Материал подается в нескучном формате без лишней теории
2) В тренинге половина времени отводится на практику
3) Основной задачей тренинга поставлено понимание материала, а не зазубривание
4) Есть сертификационный экзамен для подтверждения знаний

Целевая аудитория:

Начальники служб ИТ и/или ИБ; специалисты, ответственные за защиту конфиденциальной информации.

По окончанию обучения

Вы приобретёте знания по:

- Правовым и организационным основам построения систем защиты от утечек информации
- Терминологии, основным технологиям и принципам работы DLP систем
- Функциональным особенностям DLP систем

Вы сможете:

- Произвести начальную настройку StaffCop Enterprise
- Настроить политики
- Настроить основные сервисы
- Сделать базовую настройку безопасности конфиденциальных данных

Пакет слушателя:

Ускоритель команд, Оптимизированный конспект

Контакты

Диана Фролова df@intella.kz (Алматы)
Асель Муханмеджанова asel@pacifica.kz (Астана) + 7 (7172) 28-00-82
Татьяна Бережная tb@intella.kz (Алматы) +7 (727) 355 02 34

День 1. Архитектура систем обнаружения и оповещения об утечках и угрозах ИБ (DLP систем)

1. Правовые основы защиты информации в РК
2. Организационные основы обеспечения безопасности конфиденциальной информации
   2.1.Идентификация бизнес-процессов обработки защищаемой информации
   2.2.Выделение и классификация информационных активов, содержащих защищаемую информацию
   2.3. Назначение владельцев информационных активов, их права и обязанности
   2.4. Идентификация и учет сотрудников, допущенных к обработке защищаемой информации
   2.5. Регулирование использования информации в трудовых и гражданско-правовых договорах
   2.6. Классификация и грифование документов, содержащих защищаемую информацию
3. Технологические решения для обеспечения безопасности информации ограниченного доступа
   Задачи, решаемые DLP
   Типовая архитектура построения, принцип работы DLP систем,
   Особенности организационной работы при эксплуатации DLP
   -система принципов классификации информации
   - ввод правил реагирования
   - выполнение системой DLP операций контроля
   - обработка инцидентов
4. Краткий обзор основных DLP решений
5 Процедура управления инцидентами
   5.1.Обнаружение и регистрация событий системой DLP
   5.2.Выявление инцидентов
   5.3.Оперативное реагирование на инцидент
   5.4.Расследование инцидента
   5.5. Политика реагирования на инцидент
   5.6.Анализ причин инцидента и «полученных уроков»

Лабораторная работа: Модель принятия решения по инциденту

День 2. Современные инструменты обнаружения и оповещения об утечках информации и угрозах информационной безопасности. DLP-системы

1. Функционал DLP систем
   - Контентный анализ файлов
   - Анализатор угроз
   - Система оповещений
   - Предустановленные словари
2. Особый контроль

3. Архитектура McAfee DLP (или аналогичные решения)
4. Лучшие практики создания политик DLP

Лабораторная работа: Тестирование DLP системы (на базе продуктов McAfee DLP или анналогичное решение).

5. Экзамен

Экзамен

- Экзамен проходит письменно с наличием лабораторных работ
- На экзамен запрещено приносить любые средства коммуникаций
- Экзамен предполагает наличие с собой только учебных материалов IS
- 40 вопросов на 1 час времени и лабораторная работа на 2 часа
- Среди вопросов есть как тестовые, так и открытые вопросы.

Дополнительно

- Для получения Сертификата об окончании курса требуется успешно пройти модули разделов и принять участие в опросе по курсу.
- Точное место и способ проведения тренинга уточняйте у менеджера по обучению
- При группах от 3 человек стоимость и место проведения тренинга по согласованию с Заказчиком
- Тренинги могут проводиться в г. Алматы, г. Астан, г. Москва или дистанционно