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:

IS5.3 Защита инфраструктуры сетей

- **Домен знаний:** Информационная безопасность (IS)
- **Сертификация:** Certified IS Specialist IS5
- **Связанные сертификации**: CCNA, CCNP,
- **Статус тренинга:** Авторский курс INTELLA
- **Длительность обучения** – 3 (три) дня (30 ак.часов)
- **Форма обучения** – аудиторные занятия
- **Тренер:** Ведущий преподаватель INTELLA
- **Место и даты проведения:** На базе центра повышения квалификации ТОО «INTELLA» (ведется набор)

г. Алматы, ул. Ауэзова, 60, БЦ «Almaty Resdense» 6 этаж. Оф 17а
г. Астана р-н Есиль ул. Д. Кунаева, 29/1, оф.1903

- **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

Курс посвящён одному из защитных механизмов, который относится к категории превентивных - мониторингу защищённости. В курсе детально рассматриваются основные типы уязвимостей компьютерных систем и сетей, причины их возникновения и методы выявления. Рассматриваются приёмы и инструменты как удалённого, так и локального анализа систем, приводятся примеры использования современных систем управления уязвимостями, представлена информация по методологии анализа защищённости.

Цель тренинга:

Ознакомление руководителей и специалистов департаментов и отделов информационной безопасности, защиты информации, информационных технологий, кадровых и юридических служб с актуальными вопросами обеспечения информационной безопасности в организации в соответствии с требованиями законодательства, а также приобретение практических навыков защиты информационных систем.

Тренинг ориентирован на:

системных администраторов и инженеров, имеющих опыт установки и использования решений на базе Microsoft Windows Server и UNIX, и желающих повысить свою квалификацию в области проектирования и настройки системы безопасности. Пройдя

обучение, слушатели научатся планировать, настраивать и обеспечивать требуемый уровень безопасности в сетях Microsoft Windows Server и UNIX.

Предварительная подготовка

Знания в объеме учебного курса IS2 Комплексное обеспечение информационной безопасности в организации, а также знание технического английского языка.

Практическая значимость

По окончанию курса слушатели смогут:

- Настраивать безопасность компьютеров под управлением SuSe Linux Server
- Настраивать безопасность компьютеров под управлением Windows Server
- Использовать техники хакерских атак
- Исследовать защищенность Web-серверов
- Защищать серверы DNS и Web
- Выполнять анализ рисков
- Создавать политики безопасности
- Анализировать сигнатуры пакетов

Пакет слушателя

- Раздаточные материалы в электронном виде

По окончании тренинга выдается сертификат INTELLA Certified IS Specialist IS5

Контакты:

Диана Фролова df@intella.kz (Алматы) +7 (777) 552 74 22
(Астана) + 7 (7172) 28-00-82
Татьяна Бережная tb@intella.kz (Алматы) +7 (727) 355 02 34

Программа

IS5.3 Защита инфраструктуры сетей

	Описание курса	Время
День 1	• Требования к защите инфраструктуры сетей • Обмен закрытыми ключами. Обмен открытыми ключами. • Аутентификация. • Создание и защита скриптов для Linux. Средства безопасности Linux. • Настройка аудита и ведение журналов в Windows. • Настройка шифрующей файловой системы (EFS). • Защита инфраструктуры в Windows Server. Основы аутентификации в Windows.	С 10 час. 00 мин. До 18 час. 00 мин.   
День 2	• Рекогносцировка и создание карты сети. • Определение рабочих станций сети. • Сканирование сети. Сканирование уязвимостей. • Социальная инженерия. Получение несанкционированного доступа. • Сокрытие атаки. Проведение DoS атаки. • Идентификация техник Web-атак. Методы атак на пользователей Интернет. • Анализа рисков. Концепции и методы. Процесс анализа рисков	С 10 час. 00 мин. До 18 час. 00 мин.   
День 3	• Реагирование на инциденты и эскалация. • Создание политики безопасности компании • Концепции основных сигнатур злонамеренного трафика. • Сигнатуры нормального трафика. • Сигнатуры не нормального трафика. • Исследование сигнатур пакетов Snort.	С 10 час. 00 мин. До 18 час. 00 мин.   

Требования для прохождения практического курса:

Наличие Ноутбука желательно.

1. На ноутбуке должен быть установлен VMwareWorkstation 9 или более поздняя версия.
2. На VMwareWorkstation должен быть развернут 64-разрядный WindowsServer 2008 (с установленным пакетом обновлений 2 или более поздним) или WindowsServer 2012.

Требования к виртуальному серверу:

***a. Процессор*:** 64-разрядный процессор IntelPentium D или выше, с частотой 2,66 ГГц или выше;

b. Оперативная память: Не менее 2 Гб доступной оперативной памяти (рекомендуется не менее 4 Гб);

c. Жесткий диск: Не менее 100 Гб доступного дискового пространства.

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

В стоимость включено:

- Раздаточный материал (в электронном и печатном виде)
- Кофе-брейки, обеды

Последующее обучение

- IS6 Управление рисками информационной безопасности в информационных системах организации. Практические аспекты
- IS-DLPBASE Технологии обнаружения и оповещения об утечках информации и угрозах информационной безопасности и основы конфигурирования DLP-систем
- IS-VULMAN Построение комплексной системы управления уязвимостями