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
www.intella.pro
info@intella.kz

ПРИГЛАШЕНИЕ

На обучающий тренинг:

ISPT1 Развертывание и администрирование MaxPatrol Enterprise Edition

- **Домен знаний:** Технологии СУИБ
- **Сертификат:** INTELLA
- **Тренинг предназначен для:** Специалистов ИБ и администраторов ИТ
- **Тренер:** Кирилл Мурзин
- **Статус тренинга:** авторский
- **Длительность обучения**: 2 (два) дня (18 ак.час)
- **Форма обучения**: аудиторные занятия
- **На базе центра повышения квалификации:** «INTELLA»
- **Место и даты проведения –** г.Алматы, ул.Ауэзова, 60, оф.17А, 6 этаж или Астана 2 и 4 квартал 2019гг
- **Расписание –** с 10.00 до 18.00, обед с 13.00 до 14.00.

СПЕЦИФИКАЦИЯ

№	Наименование тренинга	Примечание	Стоимость, тенге без НДС
1	**ISPT1 Развертывание и администрирование MaxPatrol Enterprise Edition**	Цена за одного чел.	200 000

Аннотация тренинга

Тренинг даст полное теоретическое и практическое понимание **функционала и отличительные особенности системы мониторинга информационной безопасности MaxPatrol.**

В основу тренинга положена нехватка информации и практических навыков в области развертывания и администрирования системы MaxPatrol.

Тренинг разработан по новейшей методике, основой которой является оптимизация возврата инвестиций 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 схему IP адресов для большого предприятия и решить задачи маскирования переменной длины на уровне эксперта.

В тренинге предлагаются оригинальные задания, которые максимально приближены к реальным условиям работы. Сложность и комплексность заданий даёт высочайший уровень подготовки, который не доступен после прослушивания любых других авторизированных тренингов.

Основные преимущества:

1) Материал подается в нескучном формате без лишней теории
2) В тренинге половина времени отводится на практику

3) Тренинг вмещает весь материал, который необходим как часть других программ обучения
4) Основной задачей тренинга поставлено понимание материала, а не зазубривание

Требование к слушателю

Базовые знания о структуре сети

По окончанию обучения

Вы приобретете знания по:
Методологии оценки защищённости
Функционалу MaxPatrol.
Особенностям администрирования системы мониторинга информационной безопасности
Развертыванию, архитектуре и компонентам системы MaxPatrol
Базовыми приёмами работы с MaxPatrol.
Сценариям использования MaxPatrol
Инвентаризация информационных активов
Выявление уязвимостей и анализ результатов сканирования

Пакет слушателя

Оптимизированные конспект

В стоимость включено:

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

Последующее обучение

Основы сетей, все тренинги домена сетевых технологий, Microsoft и информационной безопасности

Исполнительный директор УЦ INTELLA Диана Фролова

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

День 1

Развертывание и администрирование MaxPatrol Enterprise Edition

Модуль 1. Введение. Контроль состояния защищённости как механизм защиты. Основные задачи, возникающие в ходе контроля защищённости систем, возможности их автоматизации. Функционал и отличительные особенности системы мониторинга информационной безопасности MaxPatrol. Архитектура MaxPatrol. Схема лицензирования.

Модуль 2. Развертывание MaxPatrol. Компоненты системы. Взаимодействие компонентов системы. Варианты размещения компонентов, критерии выбора и выбор наиболее приемлемого компонента. Решения для различных сетей, возможности по масштабированию системы MaxPatrol. Системные требования и рекомендации. *Практическая работа 1. Развертывание MaxPatrol.*

Модуль 3. Обновление MaxPatrol. Структура системы обновлений. Обновление через Интернет и локальный сервер обновлений. *Практическая работа 2. Обновление MaxPatrol.*

Модуль 4. Основные возможности и элементы интерфейса консоли. Базовые приёмы работы с MaxPatrol. Простейший сценарий использования MaxPatrol. *Практическая работа 3. Базовые приёмы работы с MaxPatrol.*

Модуль 5. Разграничение доступа и защита данных в системе MaxPatrol. Пользователи и роли пользователей. Назначение прав на объекты системы. *Практическая работа 4. Разграничение доступа в MaxPatrol.*

Модуль 6. Инвентаризация информационных активов. Объекты инвентаризации. Инвентаризация с помощью сетевого сканера (принципы, методы, результаты). *Практическая работа 5. Инвентаризация сетевых ресурсов.* Инвентаризация с использованием системных проверок. Использование в ходе инвентаризации модулей анализа СУБД и приложений. Анализ результатов инвентаризации. Отслеживание изменений в инвентаризационной информации. *Практическая работа 6. Инвентаризация с использованием системных проверок.*

День 2

Модуль 7. Уязвимости и способы их выявления. Понятие уязвимости. Базы уязвимостей. Тесты и эксплойты. Выявление уязвимостей по косвенным признакам. Тестирование с возможностью выведения из строя (DoS). База проверок, входящая в состав MaxPatrol. Категории проверок. Объекты сканирования. *Практическая работа 7. Оценка защищенности сетевых ресурсов.*

Модуль 8. Оценка защищённости распространенных сетевых приложений (электронная почта, FTP, DNS и другие). *Практическая работа 8. Оценка защищенности сетевых приложений.*

Модуль 9. Особенности оценки защищённости Windows-систем. Требования к сетевой инфраструктуре. Используемые транспорты. Привилегии пользователей. Анализ возможных ошибок. *Практическая работа 9. Сканирование Windows.*

Модуль 10. Особенности оценки защищённости Unix-систем и сетевого оборудования. Требования к сетевой инфраструктуре. Используемые транспорты. Привилегии пользователей. Анализ возможных ошибок. *Практическая работа 10. Сканирование Unix и сетевого оборудования.*

Модуль 11. Оценка защищенности СУБД. Требования к сетевой инфраструктуре. Используемые транспорты. Привилегии пользователей. Анализ возможных ошибок. *Практическая работа 11. Сканирование СУБД.*

Модуль 12. Оценка соответствия требованиям стандартов. Адаптация MaxPatrol под корпоративные требования. Управление стандартами и проверками. *Практическая работа 12. Оценка соответствия требованиям стандартов.*

Модуль 13. Анализ результатов сканирования. Отчёты. Оценка степени риска уязвимостей. CVSS. Проверка действительного существования уязвимости. Принятие решения по устранению уязвимостей. *Практическая работа 13. Работа с отчетами.*

Модуль 14. Оценка стойкости паролей. Методы проверки стойкости паролей. Поддерживаемые протоколы и приложения. Настройки профиля. *Практическая работа 14. Оценка стойкости паролей.*

Модуль 15. Методологии оценки защищённости. Использование MaxPatrol в ходе тестирования на проникновение. Анализ Web-приложений. *Практическая работа 15. Тестирование на проникновение и анализ Web-приложений.*

Модуль 16. Управление процессом сканирования в MaxPatrol, способы запуска сканирования, основные параметры, влияющие на ход сканирования и на производительность. Сканирование по расписанию. *Практическая работа 16. Управление MaxPatrol.*

Модуль 17. Обслуживание системы, выявление причин сбоев. Управление лог-файлами. Обслуживание базы, хранение результатов сканирования. Резервное копирование и восстановление системы после сбоев.