Курс PCSCAN 1 Основы безопасного программирования с использованием инструментальных средств анализа программного кода

В NTT Security полагают, что качественный, настроенный и ориентированный на безопасность жизненный цикл разработки программного обеспечения (ЦРПО) это ключ к успеху приложений. Наши эксперты по безопасности помогут Вашей команде разработчиков создавать безопасные приложения, встраивая требования безопасности в процесс разработки, начиная с самой первой фазы.

Что такое ЦРПО?

Проблемы безопасности в приложениях часто являются следствием недоработок на уровне проектирования, недостаточно высоких стандартов программирования и ошибок программистов. К сожалению, устаревший взгляд, что проверка безопасности должна проводиться только на завершающей стадии, и важна только перед выпуском приложения, все еще очень распространен. Безопасность приложения зависит от успешной интеграции и включения мер обеспечения и требований безопасности в
течение всего цикла разработки программного обеспечения (ЦРПО).

Целью курса является Введение в проблему безопасного программирования; Обучение работы с инструментальными средствами анализа кода Splint.

Целевая аудитория

Специалисты служб ИТ и/или ИБ, ответственные за внедрение программных продуктов, разработчики, тестировщики, программисты.

Пакет слушателя

- Фирменное учебное пособие в электронном виде.
- Организационно-распорядительные и методические материалы, на основе которых
- ведется обучение, дополнительная и справочная информация по тематике курса в
- электронном виде.

- **Статус:** Авторский курс учебного центра ТОО «ПАЦИФИКА»
- **Длительность обучения** – 3 дня (24 академических часа)
- **Форма обучения** – аудиторные занятия
- **Стоимость курса:** с одного слушателя 300 000 тг. с учетом НДС
- **На базе центра повышения квалификации:** ТОО «ПАЦИФИКА»
- **Место проведения** – г. Астана либо г.Алматы

Программа курса

	Описание курса	Время
День 1	• Понятие уязвимости • Теоретические сведения и практические примеры уязвимостей в программном коде. • Основы формирования хакерских атак • Причины возникновения уязвимостей в программном коде. • Введение в цикл разработки ПО. • Особенности современной разработки и описание типовых сценариев появления уязвимостей в программном коде. • Введение в SDLC (secure development lifecycle).	С 10 час. 00 мин. До 18 час. 00 мин.
День 2	• Принципы работы статических анализаторов кода. Чем анализаторы отличаются и как они работают. • Правила для описания новых уязвимостей. • Повышение качества работы статического анализатора. • Статический анализ реальных проектов. • Ложные срабатывания (False positive) – теоретическая составляющая: причины возникновения ложных срабатываний. • Фильтрация ложных срабатываний. • Полнота анализа и пропущенные ошибки (False negative). • Настройка HP Fortify с точки зрения различных ролей: разработчик, технический лидер, офицер ИБ.	С 10 час. 00 мин. До 18 час. 00 мин.
День 3	• Ошибки, которые статический анализатор не находит. • Динамический анализ и анализ времени выполнения. • Почему нужен Dynamic analysis, если есть static analysis • Принцип работы динамического анализатора. • Демонстрация работы динамического модуля и модуля времени выполнения. • Настройка модуля динамического анализа. • Интеграция инструментальных средств анализа кода с другими инструментальными системами, участвующими в разработке ПО.	С 10 час. 00 мин. До 18 час. 00 мин.

Дополнительная информация по телефону: +7 (727) 334-15-74
al@pacifica.kz
Менеджер ТОО «ПАЦИФИКА», Леонтьева Анастасия