Системный подход к разработке безопасного ПО

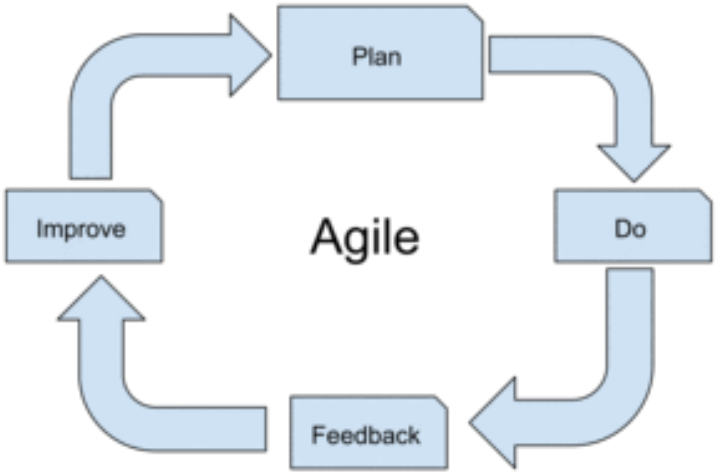
Минко В.С.

Кратко об SDL

- Набор дополнительных практик на каждом этапе разработки
- Используется при разработке всех продуктов Microsoft с 2004 года
- После внедрения SDL количество выявленных уязвимостей сократилось на 50-70%
- Всю информацию можно найти: http://www.microsoft.com/security/sdl

Зачем еще один процесс?

У нас все хорошо, ведь у нас Ag;)e



И мы создаем надежное ПО

- Разрабатываем требования и проектируем архитектуру
- Проводим ревью кода
- Проверяем код статическими анализаторами
- Настроены Check-In Policy
- Используем unit-тесты
- Развернуты сервера непрерывной интеграции
- Исходный код проходит проверку в рамках сертификации

Но...

Юный хакер «Василий Пупкин»™ ничего о ваших серьезных процессах не знает, поэтому прислал вам описание свеже-выявленной уязвимости в вашем продукте.

Безопасность асимметрична

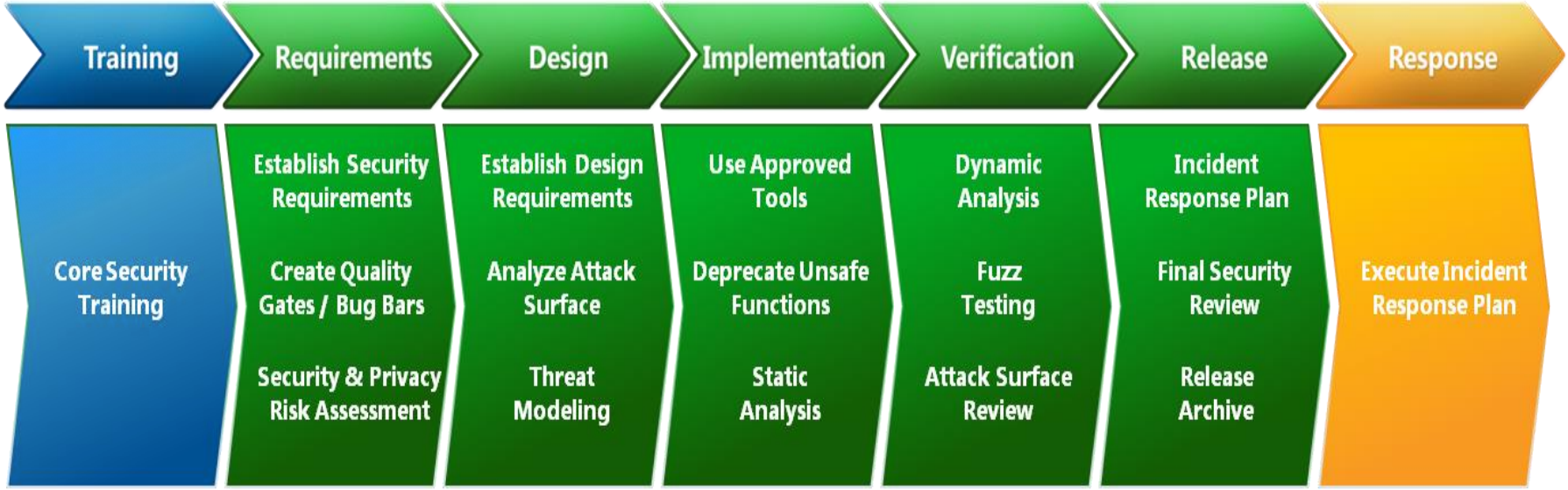
- Усилия защищающего и атакующего не пропорциональны
- Разработчик должен защищать все компоненты
- Хакеру достаточно найти наиболее уязвимый компонент и успешно атаковать только его
- Последствия даже маленькой уязвимости, обнаруженной злоумышленниками, могут быть катастрофичными

Что делать?

- Все компоненты системы должны иметь одинаковый уровень безопасности
- Лучше проводить внутренний аудит системы, чем получать «весточки» из вне
- Без систематизации затраты на защиту будут не эффективны
- SDL предлагает систематизированный набор практик для безопасной разработки

Практики SDL

Что предлагает SDL



iSDL - SDL в InfoTeCS

- iSDL – модифицированный вариант SDL.
- Смещен в сторону ФСТЭК сертификации.

Участники процесса

Фазы внедрения практик

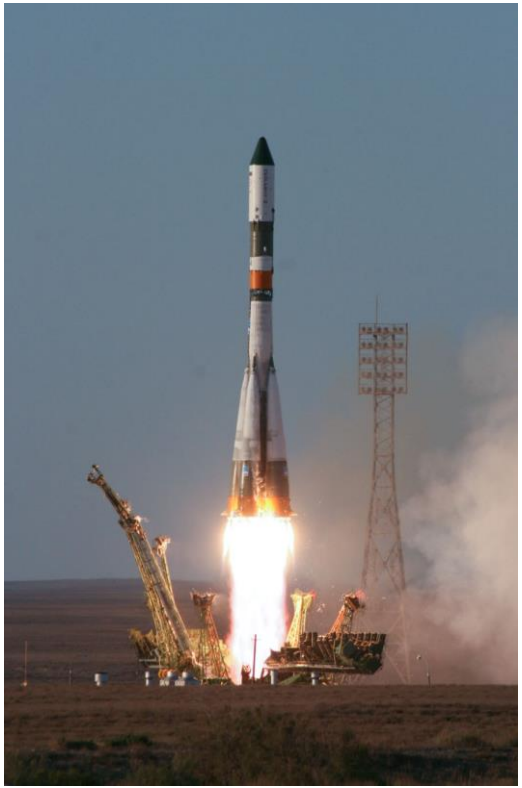
От простых практик к сложным:

Фаза Preparation

- ДОЛЖЕН быть определен уровень качества продукта.
- В проекте ДОЛЖНА быть выделена роль ответственного за безопасность.
- В проекте ДОЛЖНО выделяться время на решение технологических задач.
- В проекте ДОЛЖНЫ учитываться затраты на безопасную разработку.

Фаза Initiation

- В проекте ДОЛЖЕН быть определен план по безопасной разработке ПО.
- Для команды проекта проведена вводная презентация по практикам SDL.
- ДОЛЖНЫ быть определены требования регуляторов и нормативных документов.
- ДОЛЖНО быть подготовлено высокоуровневое описание системы.
- ДОЛЖЕН проводиться одноранговый code-review (peer-review).



Фаза Beginner

Работа с уязвимостями

Все уязвимости в продукте ДОЛЖНЫ фиксироваться, анализироваться и исправляться.

- Отдельный бэклог уязвимостей с ограниченным доступом.
- Система оценки тех. рисков.
- Регламент по работе с уязвимостями.

Модель угроз

ДОЛЖНА быть построена и поддерживаться в актуальном состоянии модель угроз.

- Spoofing. Нарушение аутентичности
- Tampering. Модификация данных
- Repudiation. Отказ от собственных действий
- Information Disclosure. Раскрытие информации
- Denial of Service. Отказ в обслуживании
- Elevation of Privilege. Эскалация привилегий

Security review

РЕКОМЕНДУЕТСЯ проводить security-review проектируемых решений.

- В форме ревью сторонними архитекторами.
- Проектная документация корректируется по замечаниям.

Анализ технологий

Используемые технологии и/или библиотеки ДОЛЖНЫ проходить анализ на безопасность.

- Учёт сторонних компонентов.
- Регламент по работе со сторонними компонентами.
- Привлечение Перспективного Мониторинга.
- Разбор отчётов.

Предупреждения компилятора

Количество предупреждений компилятора ДОЛЖНО не увеличиваться.

- Контроль числа предупреждений при сборке.
- Нарушение сборки при увеличении количества предупреждений.

SAST

ДОЛЖНЫ быть устранены все критические предупреждения статического анализатора.

- В качестве анализаторов C/C++ рекомендуется использовать PVS-Studio, CppCheck.
- Итеративный процесс настройки SAST.

Penetration testing

РЕКОМЕНДУЕТСЯ проводить тестирование на проникновение.

- Привлечение Перспективного Мониторинга.
- При серьёзном изменении функциональности или архитектуры.

Фаза Intermediate

Фаза Intermediate

- В проекте выделено время на самообучение сотрудников.
- ДОЛЖНЫ быть зафиксированы дополнительные требования безопасности.
- ДОЛЖНЫ использоваться средства защиты, встроенные в компилятор.
- РЕКОМЕНДУЕТСЯ настроить сборку продукта без предупреждений.
- ДОЛЖНО проводиться тестирование продукта на соответствие требованиям безопасности.

Что дальше?

- SDL – это процесс.
- Итеративный контроль состояния практик.


infotecs
Спасибо. Вопросы?
30.03.2018
vitaly.minko@infotecs.ru