The background of the slide is a photograph of a businessman in a dark suit and tie, holding a large, metallic, 3D-rendered gear. The gear is semi-transparent, revealing a complex internal mechanism of smaller gears and shafts. The scene is set in a modern office environment with blurred computer monitors and desks in the background.

Системный подход к разработке безопасного ПО

Минко В.С.

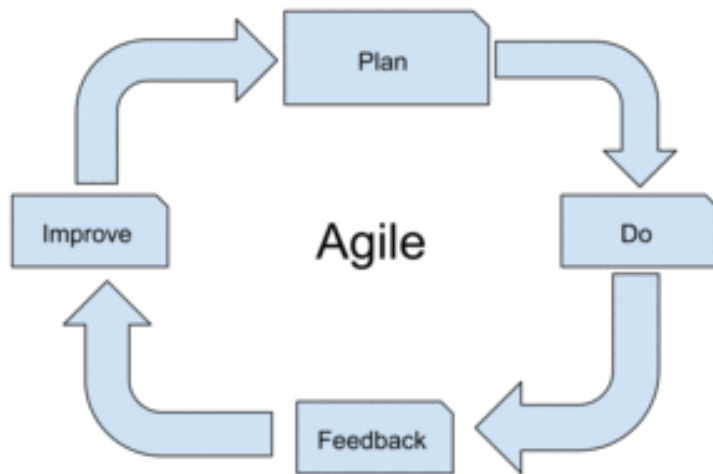
Кратко об SDL

- 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%
- Вся информация можно найти:
<http://www.microsoft.com/security/sdl>



Зачем еще один процесс?

У нас все хорошо, ведь у нас Ag;)е



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 катастрофическими



Что делать?

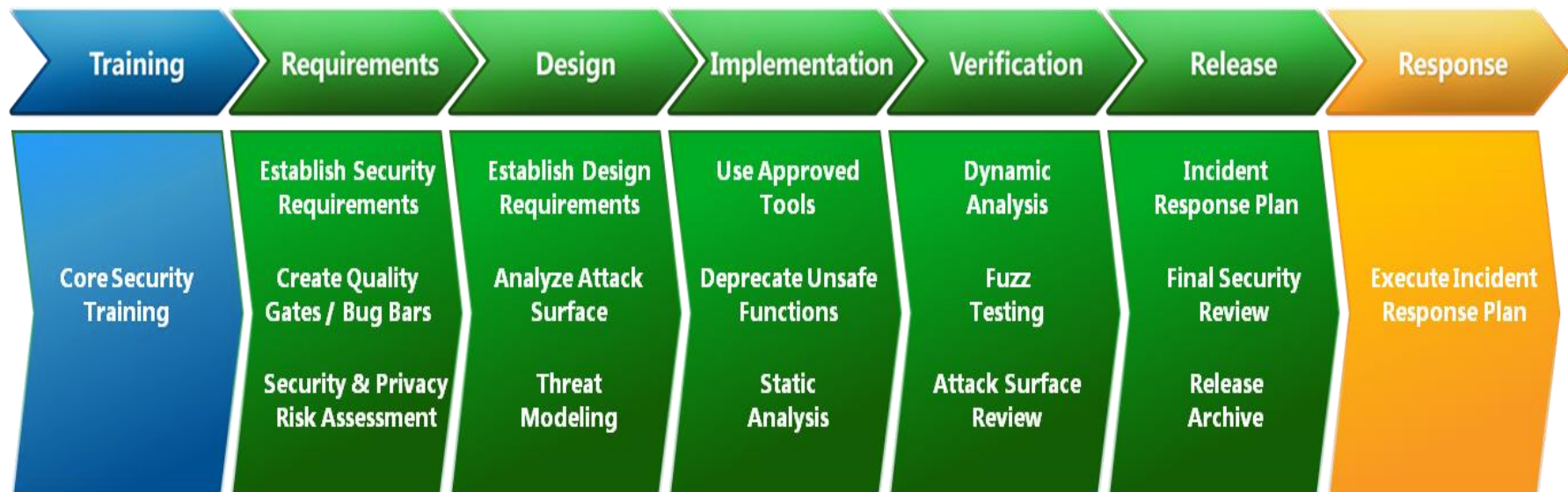
- Все компоненты системы должны иметь одинаковый уровень безопасности
- Лучше проводить внутренний аудит системы, чем получать «весточки» из вне
- Без систематизации затраты на защиту будут не эффективны
- SDL предлагает систематизированный набор практик для безопасной разработки



The background of the slide is a close-up photograph of a black smartphone lying on a black laptop keyboard. A large, light-colored wooden padlock is attached to the phone's screen. A set of keys, including a silver key and a circular metal token, is attached to the padlock's shackle. The lighting is dramatic, highlighting the textures of the wood, metal, and plastic.

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:



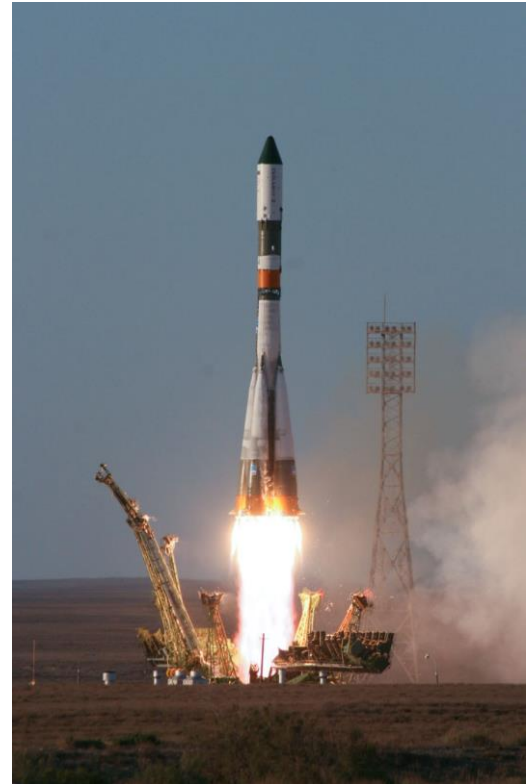
Фаза Preparation

- 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).



An overhead view of a business meeting around a large wooden table. Several people are seated around the table, each engaged with a different digital device. One person is using a laptop, another a tablet, and others are using smartphones. The scene is brightly lit, and the wood grain of the table is clearly visible.

Φαза 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.



A high-angle photograph of four people in a meeting. A woman on the left uses a tablet, a man on the right uses a smartphone, and another woman at the bottom left looks at a notebook. A laptop is open in the background. A semi-transparent white box with text is overlaid on the bottom right.

Φάση 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.



Спасибо. Вопросы?

30.03.2018

vitaly.minko@infotecs.ru