deiteriy compliance

SSF. Как делать безопасную разработку безопасных приложений

ВЛАДИМИР КОВАЛЕВ | Deiteriy | Конференция АБИСС, Москва 2022

Владимир Ковалев

QSA, SSF Assessor

Deiteriy

vladimir.kovalev@deiteriy.com

т. +7 (812) 361-61-55

м. +7 (911) 779-14-69

PCI SSF

PCI SSF (Payment Card Industry Software Security Framework) – собирательное название стандартов безопасности в рамках разработки ПО и руководств, связанных с этими стандартами.

Стандартам из PCI SSF свойственен Objective based подход к выполнению требований. При таком подходе компании-разработчику необходима особая зрелость с точки зрения информационной безопасности, а также грамотный и тщательный анализ угроз.

Стандарты PCI SSF

- PCI SSF Secure Software Standard (SSS) – стандарт безопасности, применимый к платежному ПО и процессу их разработки.
- PCI SSF Secure SLC Standard (SSLCS, SSLC, SLC, Secure SLC) – стандарт безопасности, применимый к компании и регламентирующий безопасный жизненный цикл разрабатываемых приложений.

Стандарт Secure SLC

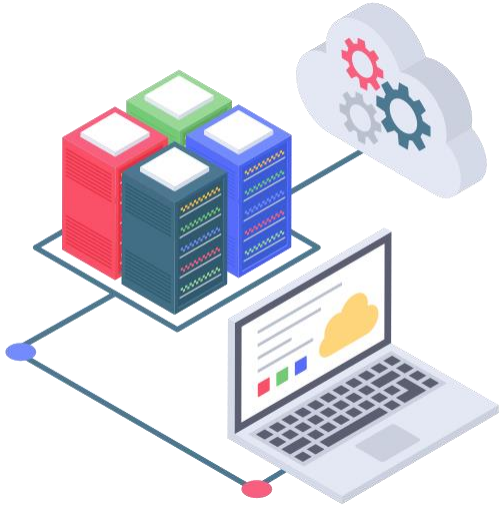
Жизненный цикл ПО

- Проектирование
- Написание кода
- Анализ кода
- Сборка кода
- Тестирование ПО
- Доставка ПО клиентам
- Поддержка ПО

Главная цель Secure SLC – обеспечить безопасность на всём жизненном цикле ПО

Скоуп Secure SLC

Одно из требований для компаний-разработчиков – контроль целостности ПО на всем его жизненном цикле.



Скоуп Secure SLC

- Должна быть определена защищаемая зона (скоуп Secure SLC), позволяющая гарантировать и контролировать целостность разрабатываемого ПО.
- Скоуп Secure SLC рекомендуется уменьшать, применяя дополнительные контрмеры для этого.
- Должна быть обеспечена безопасность в том числе информационной инфраструктуры, которая поддерживает жизненный цикл разрабатываемого ПО.

Требования Secure SLC

- Безопасно управлять жизненным циклом ПО;
- Безопасно проектировать ПО или изменения в нем.
- Обеспечить безопасность самого ПО и критичных активов, которые обрабатывает, передает, хранит или использует ПО.
- Выстроить коммуникацию со всеми заинтересованными сторонами.

Управление жизненным циклом ПО

- Возложить ответственность за безопасность ПО в целом на руководство Компании.
- Распределить ответственность за безопасность ПО в рамках всего его жизненного цикла.
- Обучать работников в соответствии с должностными обязанностями.
- Учитывать требования безопасности отраслевых регуляторов, применимые к ПО.
- Формально задокументировать, внедрить, анализировать процесс обеспечения безопасности ПО на всем его жизненном цикле, а также повышать эффективность этого процесса в случае необходимости.

Проектирование ПО

- Внедрить процесс инвентаризации критичных активов, которые обрабатывает, передает, хранит или использует ПО.
- Внедрить процесс анализа угроз, применимых к ПО.
- Для актуальных угроз, применимых к ПО, должны проектироваться и внедряться контрмеры.
- Эффективность внедренных контрмер требуется анализировать и в случае необходимости дорабатывать их.

Безопасность ПО и критичных активов

- Внедрить процесс управления уязвимостями.
- Внедрить процесс управления изменениями в ПО.
- Внедрить методологию версионности ПО.
- Внедрить контрмеры для контроля целостности ПО на всем его жизненном цикле.
- Внедрить процесс управления критичными активами, полученными из производственной среды.

Каналы коммуникации с клиентами

- Разработать и поддерживать в актуальном состоянии руководства по безопасному внедрению ПО.
- Внедрить процесс взаимодействия с заинтересованными сторонами.

Стандарт Secure Software

Критерий применимости SSS

- Приложение разрабатывается, как коробочное решение для участников PCI.
- Приложение непосредственно участвует или поддерживает проведение платежных транзакций.
- Приложение обрабатывает, хранит или передает ДПК.
- Приложение предназначено для работы с PCI-approved PTS POI устройствами.

Требования SSS

- Минимизировать поверхность атаки.
- Внедрить механизмы защиты ПО.
- Внедрить функции безопасности ПО.
- Управление безопасным жизненным циклом ПО.
- Module A – безопасность ДПК.
- Module B – Требования к терминальному ПО.

Минимизация поверхности атаки

- Инвентаризация критичных активов.
- Безопасные настройки ПО по-умолчанию.
- Условия хранения и отображения критичных активов.

Механизм защиты ПО

- Внедрить процесс анализа угроз, применимых к разрабатываемому ПО.
- Для всех актуальных и критичных угроз, применимых к ПО должны быть спроектированы и внедрены контрмеры.
- Должны быть внедрены механизмы защиты критичных активов.

Функции безопасности ПО

- Внедрить логирование событий информационной безопасности.
- Внедрить механизмы обнаружения потенциальных атак на ПО.
- Внедрены механизмы защиты критичных активов.

Управление жизненным циклом ПО

- Внедрить непрерывный процесс управления уязвимостями.
- Внедрить процесс доставки обновлений ПО.
- Разработать и поддерживать в актуальном состоянии инструкции по безопасному внедрению ПО.

Module A – безопасность ДПК

- Безопасно обрабатывать критичные аутентификационные данные.
- Безопасно обрабатывать и хранить PAN.

Module B – требования к терминальному ПО

- Руководствоваться документацией вендора сертифицированных по PTS устройств.
- Проектировать безопасную архитектуру терминального ПО.
- Внедрить контрмеры для предотвращения потенциальных атак на терминальное ПО.
- Тестировать терминальное ПО с точки зрения безопасности.
- Разработать и поддерживать в актуальном состоянии инструкции по безопасному внедрению терминального ПО.

Спасибо за внимание!