Организационные задачи, с которыми сталкиваются компании при внедрении и использовании процессов SDL

Константин Саматов, член Правления Ассоциации руководителей служб информационной безопасности

Задача 1. Что такое SDL?

- Security development lifecycle - SDL
- Разработка безопасного программного обеспечения
- Процесс, затрагивающий все стадии жизненного цикла программного обеспечения и направленный на минимизацию угроз и уязвимостей связанных с программным обеспечением

Задача 2. Кому нужен SDL?

1. Разработчики ПО
2. Субъект КИИ имеющий ЗОКИИ (с 01.01.2023)
3. Владелец ИСПДн с «внешними» пользователями
4. Владелец ГИС и МИС
5. Финансовые организации

Задача 3. Методология SDL

ГОСТ Р ИСО/МЭК 15408-1-2012 Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий (1-3 части)

ГОСТ Р 58412-2019 Разработка безопасного программного обеспечения. угрозы безопасности информации при разработке программного обеспечения

ГОСТ Р ИСО/МЭК 18045-2013 Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий

ГОСТ Р 56545-2015 Защита информации. Уязвимости информационных систем. Правила описания уязвимостей

ГОСТ Р 58143-2018 Тестирование проникновения

ГОСТ Р 56546-2015 Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем

ГОСТ Р 56939-2016 Разработка безопасного программного обеспечения. общие требования

МЕТОДИЧЕСКИЕ ДОКУМЕНТЫ ФСТЭК РОССИИ

Практики SDL: Microsoft, CISCO, Infotecs, Yandex, Сбер и т.п.

Задача 4. Кто будет реализовывать SDL?

1. Менеджер по ИБ
2. Специалист по SDL
3. Security Champion
4. Внешний подрядчик
5. Смешанный вариант

Задача 5. Основные вехи SDL

Формирование потребности

Формирование основных требований по ИБ

Проектирование

- Формирование перечня рисков
- Разработка модели угроз
- Формирование требований на основе рисков и модели угроз
- Включение требований в техническое задание
- Отражение требований в рамках технического проекта

Разработка

- Анализ уязвимостей архитектуры
- SAST
- DAST
- Fuzzing

Ввод в эксплуатацию

- Анализ уязвимостей ПО
- Тестирование на проникновение

Сопровождение

- Тестирование ПО на наличие уязвимостей
- Мониторинг уязвимостей в используемых библиотеках
- Устранение уязвимостей

Вывод из эксплуатации |модернизация\ доработка\ модификация

Контроль вывода из эксплуатации | начало цикла

Будущее SDL или на что обратить внимание

1

Требования Банка России: 382-П, 683-П, 684-П, 719-П:

- Анализ и устранение уязвимостей ПО
- Соответствие ОУД или сертификация

2

Требования к владельцам ЗОКИИ. С 01.01.2023 дополняются п. 29.2 - 29.4 (Приказ ФСТЭК России от 20.02.2020 № 35):

- 29.3. Прикладное программное обеспечение, планируемое к внедрению в рамках создания (модернизации или реконструкции, ремонта) ЗОКИИ должно соответствовать требованиям по безопасной разработке (наличие руководства по безопасной разработке программного обеспечения, проведение анализа угроз безопасности информации программного обеспечения, наличие описания структуры программного обеспечения на уровне подсистем), требования к испытаниям по выявлению уязвимостей в программном обеспечении: SAST, DAST, Fuzzing
- 29.4. Выполнение требований 29.3 оценивается лицом, выполняющим работы по созданию (модернизации, реконструкции, ремонту) или обеспечению безопасности ЗОКИИ, на этапе проектирования на основе документации разработчика ПО.

Спасибо за внимание!

Константин Саматов, член Правления Ассоциации руководителей служб информационной безопасности