Безопасная разработка: ключевые аспекты.

2021

Деев Сергей
Менеджер продукта appScreener

Rostelecom
Solar

Предпосылки к широкому распространению мер безопасной разработки

Повышение роли компьютерных технологий в бизнес-процессах компаний и государственных структур с каждым годом;

Рост количества проводимых на них успешных компьютерных атак;

Недостаточность применяемых ранее мер по обеспечению ИБ;

Экспертное сообщество сформировало «best practice»;

Обязательные требования регуляторов.

Rostelecom
Solar

Ключевые мотивы внедрения практик безопасной разработки в организациях

Улучшение качества и безопасности разрабатываемого ПО:

- Необходимость сохранения лидирующей позиции на рынке;
- Прямая связь прибыли с безопасностью ПО.

e-commerce

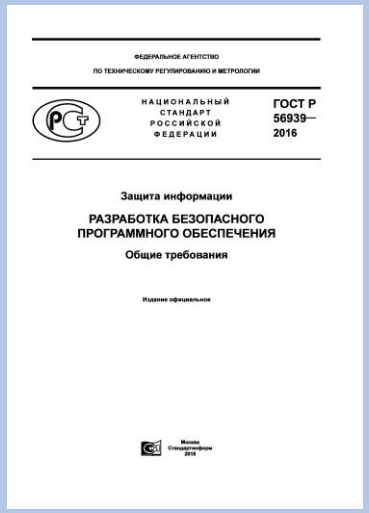
FinTech

Соответствие требованиям регуляторов и отраслевых стандартов:

- Приказы ФСТЭК России:239,76,55.
- Положения БР: 683П, 684П.

Банк России

Примеры практик безопасной разработки



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 56939— 2016

Защита информации

РАЗРАБОТКА БЕЗОПАСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Общие требования

Издание официальное

Москва
Стандартинформ
2016

Какие бывают практики и с чего начать?

Организационные	• Определение ответственного; • Подготовка плана внедрения практик и его ключевых этапов; • Согласование плана с высшим руководством.
Безопасность инфраструктуры	• Аудит и улучшение процессов эксплуатации ИС; • Аудит и повышение уровня защищенности ИС.
Безопасность продукта	• Анализ архитектуры безопасности, включая поиск уязвимостей в сторонних компонентах на основе данных из из открытых источников; • **Анализ исходного кода**;

Rostelecom
Solar

Rostelecom
Solar

appScreener – отечественное решение

Внесен в Единый реестр отечественного ПО (№ 6119) и сертифицирован ФСТЭК России на соответствие требованиям по 4-му уровню контроля отсутствия НДВ (сертификат № 4007) и ТУ.

appScreener поддерживает 35 языков и с каждым релизом их количество растет

Встраивание appScreenr в инфраструктуру

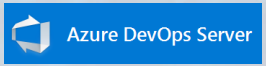
Репозитории

VCS хостинги

Средства разработки

Средства сборки

Серверы CI/CD



Отслеживание задач

Анализ кода

Открытый API предоставляет широкие возможности по дополнительной интеграции и автоматизации. Включает в себя JSON API и CLI

Rostelecom
Solar

Какие бывают практики и с чего начать? (продолжение)

Безопасность продукта	• Динамический анализ; • Фаззинг-тестировние; • Тестирование на проникновение ПО (проверка применимости выявленных уязвимостей) • Мониторинг информации о выявлении новых уязвимостей в сторонних компонентах и собственном коде ПО из известных источников для возможности оперативного реагирования на выявленные проблемы.

Rostelecom
Solar

Rostelecom
Solar

Спасибо за внимание!
Вопросы?

Контактные данные:

Деев Сергей, Менеджер продукта appScreener.

телефон : +79104585944 (мобильный, telegram, whatsapp)

email: s.deev@rt-solar.ru