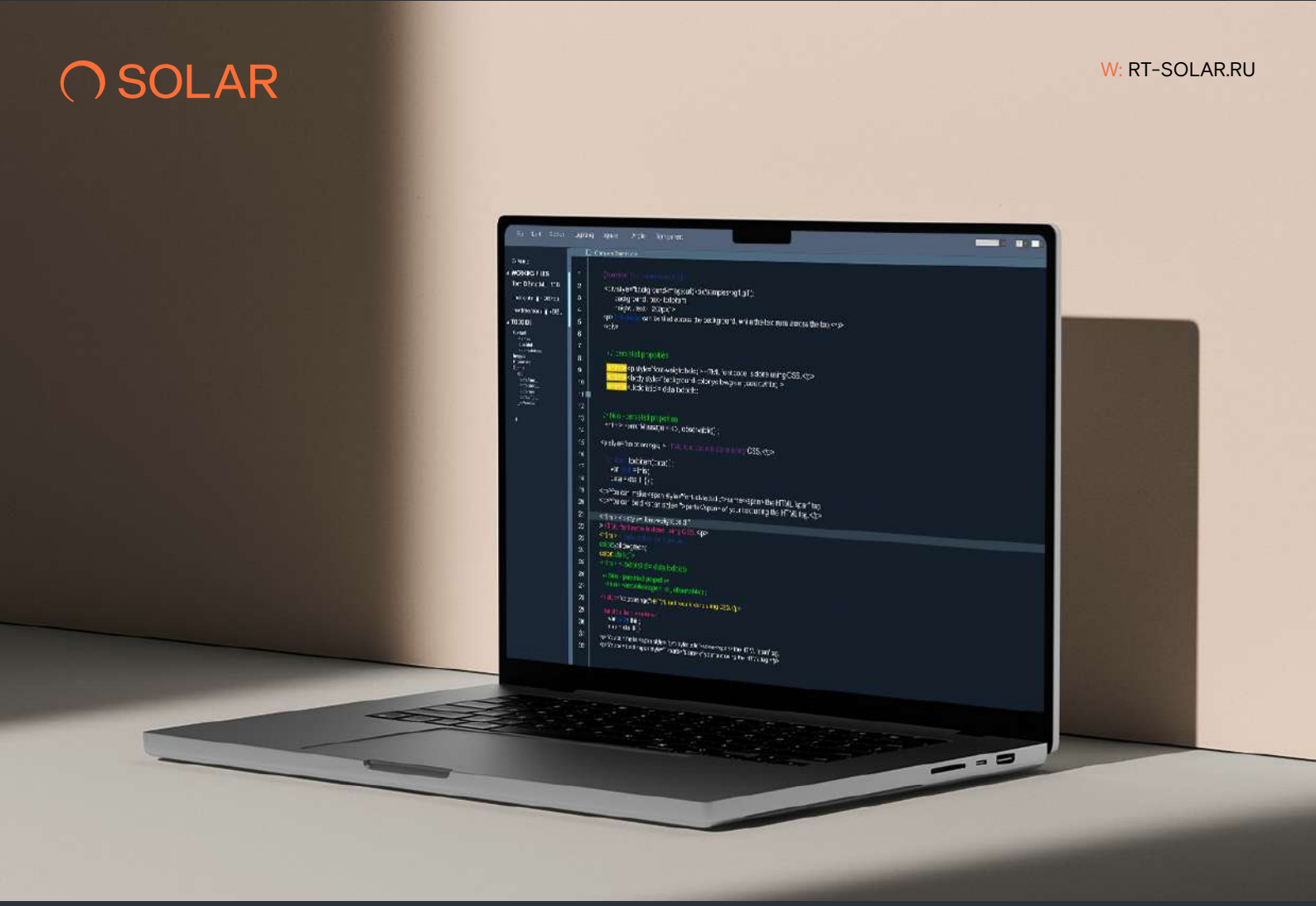
SOLAR

W: RT-SOLAR.RU



5 ШАГОВ

КОТОРЫЕ ПОЗВОЛЯТ СЭКОНОМИТЬ НА УСТРАНЕНИИ УЯЗВИМОСТЕЙ ДО РЕЛИЗА ПО

на 80%

уменьшается количество уязвимостей в коде при внедрении подхода SSDLC

Представьте, вы загорелись идеей внедрить безопасную разработку в вашей компании. И неудивительно — по словам экспертов, это самый эффективный метод создания защищенных приложений и защиты от угроз, связанных с уязвимостями и недостатками кода.

Как это сделать?
Многих останавливает то, что внедрение безопасной разработки — непростой и длительный процесс.

Если вы только в начале пути, рекомендуем вам пройти пять шагов и сэкономить на исправлении уязвимостей до релиза ПО. Ниже расскажем подробнее про каждый шаг на пути внедрения безопасной разработки.

1 шаг
Подготовительный

1. Убедитесь, что руководство вас полностью поддерживает в стремлении сделать разработку безопасной.

   Часто можно столкнуться с возражениями в духе «зачем нам тратить на это деньги» и «нормально же сейчас разрабатываем».
   С таким настроем руководства внедрять новые процессы будет тяжело, поэтому рекомендуем все же заручиться его поддержкой.

2. Выберите методологию безопасной разработки, которой вы будете придерживаться на всем пути.

   Обычно при выборе лидируют OWASP SAMM, BSIMM, Microsoft SDL, но это может быть любая другая методология, которая вам подходит.

3. Определитесь с масштабом внедрения.

   Сразу броситься в омут с головой и внедрять безопасную разработку во всей компании или пока ограничиться конкретным проектом или приложением? Примите решение на этом этапе.

4. Соберите команду.

   - Создайте рабочую группу и определитесь, кто за что отвечает. В ней могут быть разработчики, ИБ-специалисты и представители других команд, вовлеченных в процесс разработки ПО.
   - Выберите в команде разработки Security Champion — человека, который поможет вам смотреть на процесс разработки изнутри проекта и, конечно, будет драйвить использование практик безопасности в своей команде.

2 шаг
Оценочный

1. Составьте полное представление о разрабатываемых приложениях.

   Чтобы правильно выбрать инструменты для проверки безопасности ПО, надо больше узнать о приложении, которое вы разрабатываете: на каких языках оно написано, какие технологии и фреймворки использует, каково его внутреннее устройство — какие функции оно выполняет, какие пользователи с ним работают, какие данные в нем обрабатываются.

2. Оцените, как происходит разработка ПО сейчас.

   На этом этапе оцените вашу точку «до» — как устроены процессы и какие практики безопасности используются в проектах сейчас. Для этого как нельзя лучше подойдет грамотно составленный опросник, несколько часов в запасе и группа сотрудников разработки и ИБ, которые не против пообщаться.

3 шаг
Установочный

Выберите основные цели — чего вы хотите достичь при внедрении безопасной разработки.

Например, целью может быть внедрение инструментов автоматического анализа безопасности кода для определенного процента компонентов проекта в течение полугода или доведение выполнения требований комплаенса до 100%. Конкретные цели будут зависеть от многих факторов и проблем, стоящих перед компанией.

4 шаг
Тактический

Составьте план внедрения безопасной разработки.

Опираясь на данные интервью и предварительную оценку, можно составить роадмап внедрения практик безопасной разработки — подробное описание процесса со всеми этапами, дедлайнами и ответственными лицами.

5 шаг
Практический

1. Начните использовать основные инструменты безопасности приложений.

   Лучше всего начать с внедрения инструментов автоматизации проверок безопасности — статического анализа (SAST) и анализа состава ПО (SCA). Так вы решите первостепенные задачи по обеспечению безопасности кода и получите значительный прирост в качестве продукта:

   Статический анализ (SAST) поможет найти уязвимости на первых этапах разработки, сократить риски безопасности и сэкономить на исправлении проблем в коде перед релизом.

   Анализ состава ПО (SCA) поможет обезопасить разработку от заведомо уязвимых сторонних компонентов, в том числе с открытым исходным кодом.

2. Не молчите о предстоящих изменениях в процессах разработки.

   Если рассказывать коллегам обо всех планируемых нововведениях, это сильно упростит внедрение безопасной разработки и сделает его понятным и прозрачным.

3. Измеряйте эффективность внедренных процессов.

4. Помните, что безопасная разработка — это не разовая акция, а непрерывный процесс, который нужно выстраивать и поддерживать.

По мере развития и повышения уровня зрелости процессов защищенной разработки нужно будет внедрять и другие инструменты, но на первых порах этих методов будет достаточно.

ЧТО ДЕЛАТЬ ДАЛЬШЕ

Следующие действия зависят от вашего роадмапа, целей, которые вы ставили, и результатов.

В любом случае применение только вышеперечисленных рекомендаций и инструментов анализа защищенности уже поможет вам сделать большой шаг вперед в обеспечении безопасности вашего ПО и сохранить деньги компании в будущем.

ГДЕ УЗНАТЬ БОЛЬШЕ

Получите больше информации о первых шагах к построению безопасной разработки и внедрении решения для контроля безопасности кода Solar appScreener

Узнать больше