SecretTechnologies

Как мы реализовали безопасную разработку корпоративного файлообменника Secret Cloud Enterprise

ДАВАЙТЕ ЗНАКОМИТЬСЯ

Леонид Варламов

Заместитель генерального директора
Сикрет Технолоджис

О СИКРЕТ ТЕХНОЛОДЖИС

- **8 лет**
  на рынке ИБ
- **90+**
  технических специалистов
- **> 100**
  реализованных проектов
- **7 решений**
  в Реестре отечественного ПО
- **1 решение**
  сертифицировано ФСТЭК РФ

Семейство продуктов Secret Cloud

Система безопасного обмена файлами с сотрудниками и партнёрам сертифицирована ФСТЭК РФ

Trace Doc

Система создания уникальных копий документов

Screen Guard

Система снижения рисков утечки информации путем фотографирования

Data Mask

Система профилирования и обезличивания чувствительных данных

Printer Guard

Система контроля и экономии ресурсов печати

О ЧЁМ ПОГОВОРИМ

- Почему разработчики обычно не практикуют DevSecOps, и почему начали мы
- Получение первого сертификата ФСТЭК РФ – опыт Сикрет Технолоджис
- Внедрение безопасной разработки – что это для нас, какой фокус
- Планы развития безопасной разработки в Сикрет Технолоджис
- Почему важность безопасной разработки только растёт

ПОЧЕМУ ПОЯВЛЯЮТСЯ УЯЗВИМОСТИ

1

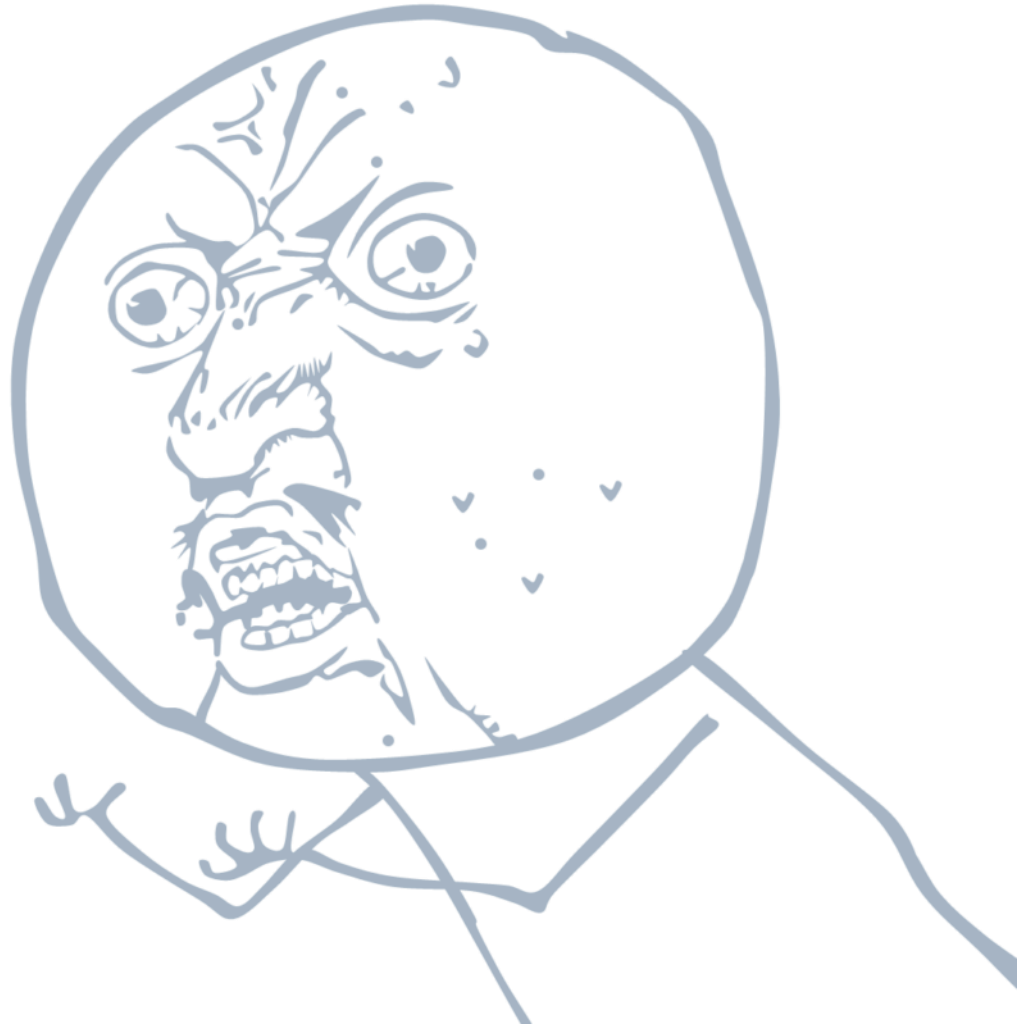
Разработчики не замотивированы следить за устранением уязвимостей и не видят в этом явных выгод

сложно долго дорого

2

Не все компании-разработчики осознают важность процесса выявления и устранения уязвимостей

внимание время бюджет



КОГДА НАЧИНАЮТ УСТРАНЯТЬ УЯЗВИМОСТИ

Конкурентное преимущество
на рынке ПО

Уменьшение финансовых
и репутационных рисков

Выполнение требований регуляторов
для работы в КИИ

ЗАЧЕМ МЫ ВНЕДРИЛИ DEVSECOPS

Риск взлома Заказчиков через наш продукт

Появились Заказчики, желающие купить наш продукт только при наличии сертификата ФСТЭК

КАК МЫ ПОЛУЧАЛИ СЕРТИФИКАТ ФСТЭК

11.2021
Поженили DevSecOps и требования ФСТЭК

Поняли, что ФСТЭК РФ требует примерно то же

Лаборатория: нужно внедрять безопасную разработку

Внедрили безопасную разработку

Импорто-заместили окружение

Подготовили вагон документов

Отправили продукт на проверку в лабораторию

Отправили продукт на проверку во ФСТЭК РФ

12.2022

ЧТО ИМЕННО ПРИШЛОСЬ ДЕЛАТЬ

- Написать очень много бумажек
- Детально описать архитектуру продукта
- Сформировать архитектуру безопасности
- Выделить поверхности атаки
- Написать фаззинг-тесты
- Переписать фаззинг-тесты
- Научиться писать фаззинг-тесты
- Написать юнит-тесты (очень много)
- Описать функциональные тесты
- Определить реализуемые функции безопасности
- Установить много ПО для проверки продукта
- Научиться пользоваться этим ПО
- Проверить, как реализуются функции безопасности
- Устранить сотни уязвимостей
- Проверить исходный код на секреты
- И ещё много всего...

КАК МЫ УЛУЧШАЛИ DEVSECOPS

Основной упор – максимальная автоматизация всего,
что делается вручную, и что можно автоматизировать

- Корректировка процесса движения задач в Jira (обязательный этап – проверка офицером ИБ)
- Встраивание в пайплайн разработки мониторинга SonarCube и Svacer и настройка Quality Gates
- Написание юнит-тестов на регулярной основе и повышение их покрытия
- Ручной контроль актуальных уязвимостей
- Повышение версий используемых библиотек

ЧТО ЕЩЁ МЫ ПЛАНИРУЕМ УЛУЧШАТЬ

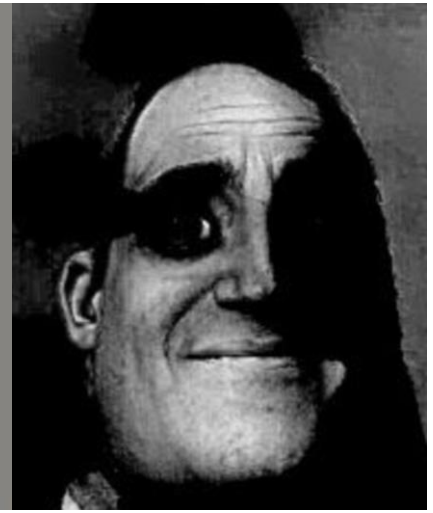
- Переход с open source библиотек на суверенный репозиторий библиотек
- Покрытие юнит-тестами всей поверхности атаки
- Покрытие фаззинг-тестами всей поверхности атаки
- Автоматизация сборки контейнеров и запрет на их формирование при непрохождении Quality Gates
- Ведение реестра уязвимостей
- Анализ всех исходных кодов на наличие секретов
- Pentest и Bug Bounty
- Сертификация процесса безопасной разработки

ПИСЬМО СЧАСТЬЯ ИЗ ФСТЭК РФ

Изготовители, осуществляющие сертифицированное производство средств защиты информации (при наличии сертификата соответствия с действующим сроком) или сертификацию серийного производства средств защиты информации, должны до 1 января 2025 г. представить в ФСТЭК России в электронном виде перечни заимствованных программных компонентов с открытым исходным кодом по каждому сертифицированному средству защиты информации, оформленные в соответствии с приложениями к порядку, прилагаемому к настоящему письму, для получения плана поддержки безопасности заимствованных компонентов сертифицированного средства защиты.

Получил письмо

Получил письмо из ФСТЭК



ПОЧЕМУ ВАЖНОСТЬ DEVSECOPS РАСТЁТ

Заказчики начали требовать от вендоров сертификаты ФСТЭК не только на продукты, но и на процесс безопасной разработки

ФСТЭК РФ ужесточает требования к заимствуемым компонентам и повышает контроль за ними

С 2025 года самостоятельно вносить изменения в сертифицированные продукты смогут только вендоры, у которых сертифицирован процесс безопасной разработки

Сертифицировать продукт или процесс безопасной разработки без реальной работы – невозможно

Количество угроз и уязвимостей только растёт

Это сложно, долго и дорого – нужно начинать уже сейчас

SecretTechnologies

Леонид Варламов

заместитель генерального директора
Сикрет Технолоджис

info@secretgroup.ru
+7(495)109-29-50