МКБ

Мы — клиентский банк

Есть ли SEC между DEV и OPS

Александр Васин

Начальник управления
комплексной защиты информации

О себе

Васин Александр Сергеевич

Начальник управления Комплексной защиты информации

Карьерный путь

Более 14 лет в ИБ — прошел путь от технического специалиста до руководителя управления в системно значимых банках России. Управлял командами 30+ специалистов:

- Райффайзенбанк: с 2005 года 14 лет системного администрирования и ИБ
- ПАО «СИБУР Холдинг»: построение и развитие DevSecOps-практик
- ООО «Платежи и переводы»: построение ИБ с нуля
- ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК»: развитие процессов ИБ, в том числе процессов безопасной разработки.

Чем могу поделиться с аудиторией АБИСС

- практическими кейсами построения процессов ИБ
- решениями сложных управленческих задач
- опытом достижения компромисса между безопасностью и бизнес-задачами

Цели и задачи SEC в DevOps …

Основные цели SEC-компонента

- Автоматизированная проверка и обеспечение защиты артефактов (кода, контейнерных образов) приложений на всех этапах сборки и публикации приложений
- Обнаружение уязвимостей в артефактах на максимально возможно ранних стадиях разработки и развертывания
- Обеспечение прослеживаемости результатов проверок приложения от разработки до публикации на продуктовом контуре
- Обеспечение наблюдаемости и измеримости результатов проверок
- Защита при эксплуатации приложений – runtime security (как в legacy, так и в контейнеризированных средах для микросервисов)
- Мониторинг состояния защищенности процессов разработки, своевременное обнаружение уязвимостей, патчинг
- Построение процесса управления уязвимостями для разработки и её окружения – обнаружение, анализ, триаж, исправление, тестирование, публикация, проверка

… в стране розовых пони …

Делай SAST, Делай DAST

- Мы купим SAST!
- Мы купим DAST!
- Мы купим SCA!
- Заставим ИТ все это настроить!
- PROFIT! ….?

… и в суровой реальности

Рифы и подводные камни

- Огромное количество False Positive невозможно разобрать к релизу
- DAST templates некому разрабатывать
- Проверки образов в SCA занимает несколько часов, а их очень много
- Container Runtime Security съел 100% ресурса worker-node

Импортозамещение CS в реальности

Вендоры отечественных решений еще не проработали все жизненные кейсы, поэтому в нечастых типовых ситуациях поведение продукта сильно отличается от ожиданий заказчика… часто в худшую сторону.

Кейс	Ожидание	Реальность
Поиск паттернов по regex при анализе кода в SAST	SAST поддерживает поиск по пользовательским фильтрам	Поддержки пользовательских фильтров нет
Проверка больших образов в CS	CS оценит образ. При возможности проверит, при невозможности – выдаст детальную информацию и остановит публикацию	CS «подавится» таким образом, job проверки аварийно завершится без какой-либо информации
Выявлен инцидент компрометации внешнего репозитория	Вендор оперативно обновит репутационные базы и SCA заблокирует только скомпрометированные библиотеки	SCA заблокировал все версии одноименных библиотек

В командах разработки...

Недостаточные Skills в части безопасной разработки. Как следствие:

- Разработчик: «Я не знаю, какие версии библиотек используются на frontend, они берутся из транзитивных зависимостей, а мы используем Webkit, в котором таких много»
- DevOps: «Мне нужно запускать контейнеры с privileged:true, так как сборка продуктовых образов осуществляется на изолированной виртуальной машине с Docker, а в Kubernetes executor мы пока не умеем»
- Team Lead: «При планировании ресурсов бэклога на ближайшие десять лет мы не планировали ресурсы на задачи безопасной разработки»

… и в команде ИБ

Аналитик ИБ: Что вы, черт возьми, такое несёте ?

О Security Champions

Security Champion

- Член команды разработки
- Отвечает за запуск и сопровождение практик защищенной разработки внутри своей команды
- Лидирует анализ защищенности ПО
- Сопровождает процесс исправления найденных уязвимостей (дефектов)
- Дает рекомендации по исправлению уязвимостей коллегам
- Проверяет код и документацию на предмет следования практикам безопасной разработки
- Взаимодействует с департаментом информационной безопасности по всем другим вопросам, связанным с процессом безопасной разработки

… не взлетело

Конфликт интересов

- Security Champion хочет больше заниматься вопросами безопасности
- Добавление проверок, санитайзеров, поиск безопасных методов и функций приводит к значительному увеличению времени на разработку
- DevOps’ы не готовы к дополнительным задачам (изменение базовых образов, использование Vault и т.д.)
- Team Lead не готов выделять ограниченный ресурс команды на практики DevSecOps.

Результат:

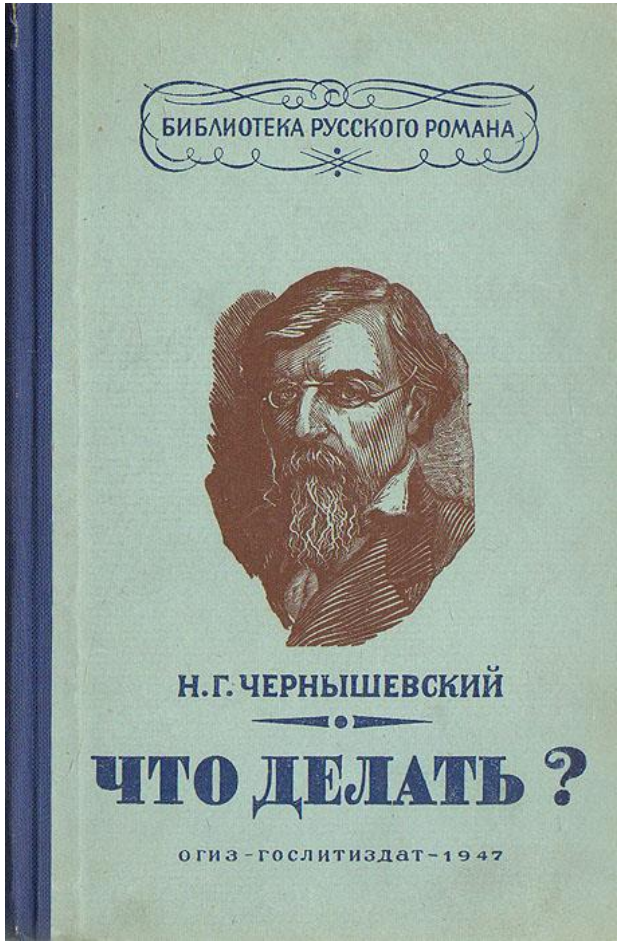
- Команды разработки, DevOps и тестирования получили дополнительные (ранее не запланированные) задачи
- Team Lead (полностью или частично) потеряли часть ресурса команды разработки и DevOps, потраченные на активность Security Champion
- Security Champions получили рюкзаки с корпоративной символикой и обструкцию от коллег по командам
- Департамент ИБ не получил ничего …

Что делать?

Что нужно для Sec между Dev и Ops

- Собрать команду со скиллами Dev, Sec и Ops
- Спроектировать в первом приближении процессы безопасной разработки
- Выбрать и развернуть нужный софт (SAST, DAST, SCA, container runtime security)
- Провести инвентаризацию всех сущностей процесса разработки
- Договориться с ИТ о внедрении механизмов проверок ИБ в процессы разработки, а главное - выделении со стороны ИТ ресурсов на эти работы

И тогда вы окажетесь в самом начале пути …



Про деньги

Внедрение Sec

- Стоит очень дорого
- Сложность при внедрении и эксплуатации
- Сопротивление всех новым процессам
- Отрицательные экономический эффект в моменте, т.к. увеличивает текущие затраты на ИТ и ИБ, а не снижает их

Работающий DevSecOps

- Существенно расширяет покрытие проверок / наблюдаемость процессов разработки метриками ИБ
- После внедрения позволяет обеспечивать техническую защиты большего количество сущностей меньшим количеством сотрудников
- Эффективно митигирует новые типы современных атак
- Развивает компетенции, которые могут быть использованы в соседних областях (например, для AISecOps и MLSecOps)
- Повышает качество разработки и безопасность итогового продукта
- Снижает риски ИБ для всей компании
- И в итоге приводит к снижению расходов

МКБ

Спасибо за внимание

2025