

Роли и кадровое обеспечение процессов DevSecOps

14 июля 2021



01



Про процесс
Dev_Sec_Ops



Внедрение практик DevOps

- Практики DevOps помогают организациям получать ряд дополнительных преимуществ, таких как повышенная гибкость, скорость и снижение затрат в разработке.



Снижение time to market

- DevOps позволил разрабатывать бизнес-приложения в гораздо более короткие сроки.
- Автоматизация процессов разработки, тестирования и развертывания.



Повышение гибкости в разработке

- Согласование процессов разработки и поставки ПО с эксплуатацией.
- Непрерывное тестирование качества приложений.
- Гибкий процесс управления изменениями.



Снижение затрат (бессерверные вычисления)

- Использование бессерверных вычислений
- Распил монолита на микросервисы и использование микросерверной инфраструктуры



Динамическое выделение ИТ-ресурсов

- Управление инфраструктурой как кодом.
- Непрерывный мониторинг производительности приложений и состояния инфраструктуры.



Увеличение количества уязвимостей

- В большинстве случаев Security не уделяется внимания при реализации практик DevOps, и часто воспринимается как препятствие на пути к быстрому развитию как следствие увеличение количества угроз и уязвимостей в продукте.



Разница между DevOps и DevSecOps

- В то время как DevOps базируется на принципе взаимодействия между группами разработки, тестирования и эксплуатации для непрерывной доставки, продукта потребителю.
- DevSecOps включает интеграцию компонента безопасности в процесс DevOps.
- DevSecOps фокусируется на решении проблем безопасности, таких как создание безопасной архитектуры приложения, анализ кода и зависимостей, управление конфигурацией.



Что такое DevSecOps?

- DevSecOps принцип управления безопасностью в процессе разработки приложения.
- Принципы безопасности вводятся на ранних этапах процесса разработки и реализуются на протяжении всего жизненного цикла разработки.
- DevSecOps не только предоставляет командам DevOps знания и практики в области безопасности, но и объединяет знания и процессы разработки приложений в группы безопасности для эффективного взаимодействия между командами.



Основные компоненты DevSecOps

- Анализ кода
- Управление изменениями
- Мониторинг соответствия
- Исследование угроз
- Оценка уязвимости
- Обучение

Принятие стратегии DevSecOps

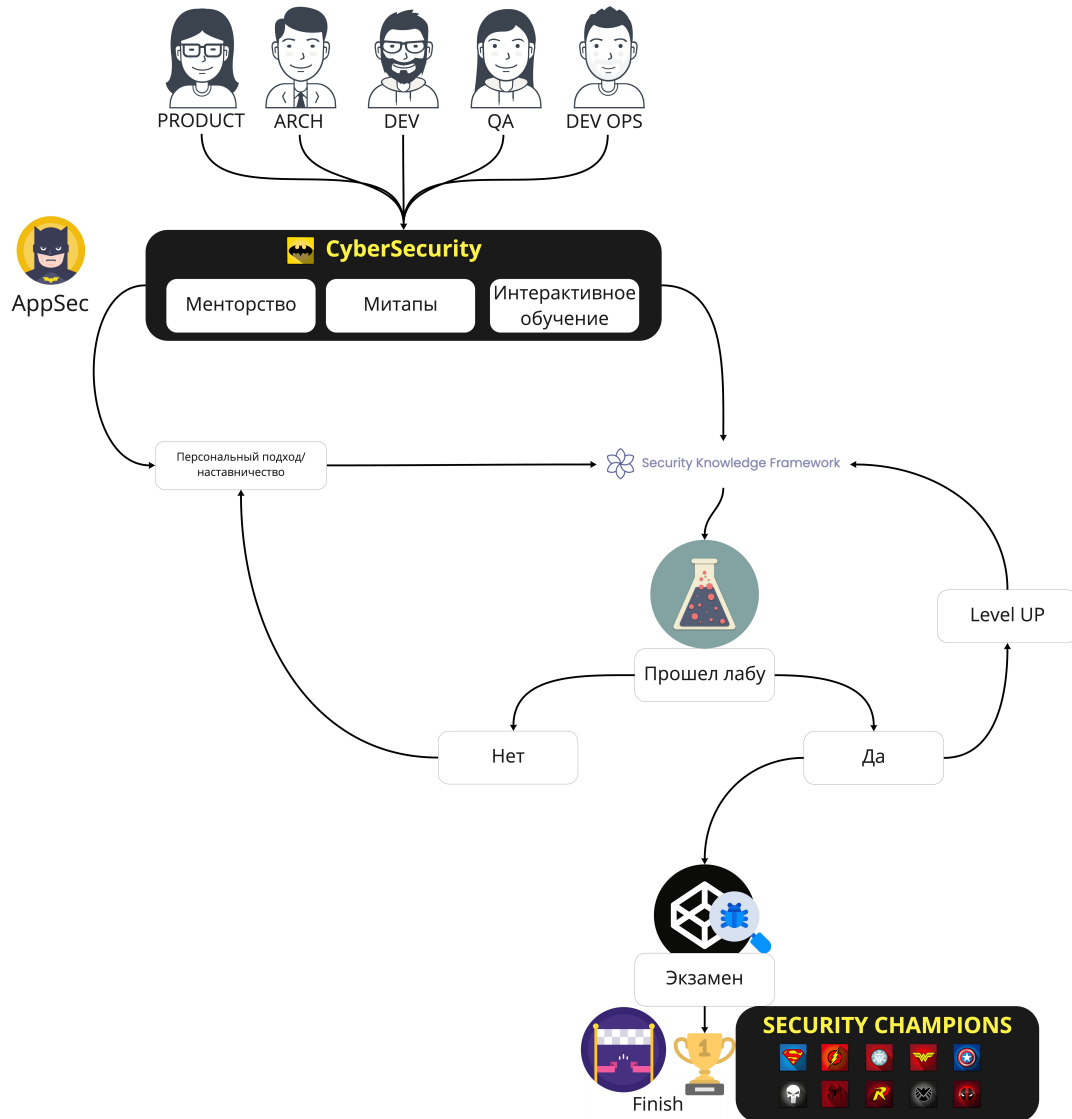


02



Роли в процессе
Dev_Sec_Ops





Основные компоненты DevSecOps

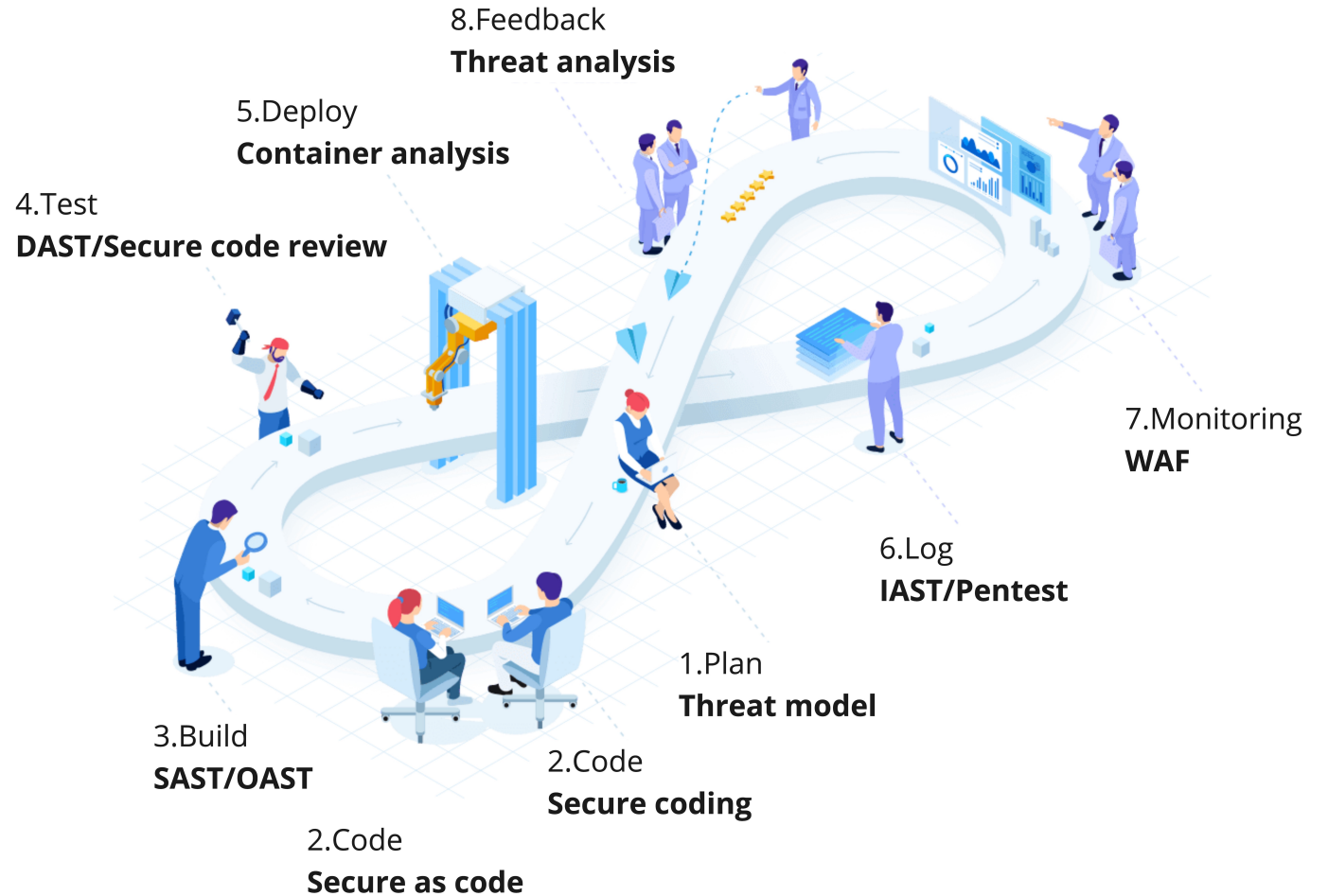
- Разрабатываем стандарты, гайды, чек-листы по безопасной разработке
- Рассказываем о существующих угрозах
- Знакомим с OWASP TOP 10
- Рассказываем про типовые уязвимости.
- Каждое занятие 7-15 минут
- 1 занятие = 1 уязвимость/кроме SQL
- Даем домашку в виде лабы
- Разбираем домашку
- Экзамен - разворачиваем juice shop для того чтобы пошатать.
- Вход комьюнити, отличительная история мерчи
- Участие в киберполигонах/соревнованиях
- Проводим предпроектную подготовку
- Обсуждаем тест кейсы на тестирование бизнес-логики
- Оцениваем риски

Какие преимущества Security Champions приносят компании?



Основные преимущества SecChamp

- Масштабирование безопасности с помощью нескольких команд
- Привлечение людей, не связанных с безопасностью, но связанных с DevOps
- Создание культуры безопасности



Спасибо за внимание!

Кирилл Ильин

CISO - руководитель отдела кибербезопасности

SberAuto

📞 +7 (916) 655-14-57

✉ k.ilin@sberauto.com

