SWORDFISH
SECURITY

Безопасная разработка. Cloud Native подхо

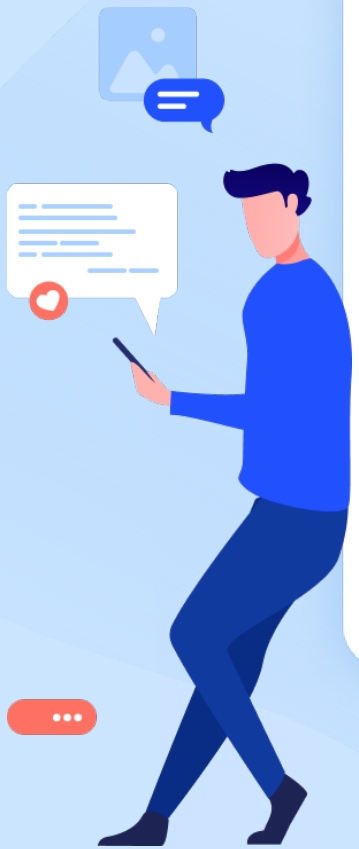
Юрий Шабалин
Ведущий архитектор ИБ

swordfishsecurity.ru

Who Am I

Юрий Шабалин

- Ведущий архитектор ИБ в Swordfish Security
- Эксперт по анализу защищенности мобильных приложений
- Security Researcher
- Евангелист DevSecOps



Базовые практики DevSecOps

Базовые практики DevSecOps

SAST (Статический анализ кода)

- Работа с исходным кодом
- Интеграция с CI

DAST (Динамический анализ)

- Взаимодействие с реально работающим приложением
- Интеграция с CD

SWORDFISH SECURITY

Базовые практики DevSecOps

OSA / SCA (Безопасность компонент с открытым исходным кодом)

- Работа с исходным кодом, собранным дистрибутивом и артефакторием
- Интеграция в CI/CD

Container Security (Безопасность контейнеров)

- Работа с собранными образами и развернутыми приложениями
- Интеграция в CI и Operation

SWORDFISH SECURITY

Базовые практики DevSecOps

ASOC (Оркестрация и корреляция)

- Связь инструментов ИБ и разработки
- Сбор метрик и мониторинг процесса
- Интеграция со всеми стадиями разработки

SWORDFISH SECURITY

Основные советы при построении любого процесса

- Самое главное не инструменты, а продуманный процесс
- Безопасность должна быть вместе с разработкой, внедрением и сопровождением
- Инструменты должны выбираться исходя из особенностей процесса
- Необходимо контролировать процесс безопасной разработки (метрики)

SWORDFISH SECURITY

Что такое Cloud Native подход

SWORDFISH SECURITY

- Принцип частного облака, у каждой компании свой экземпляр ПО
- Инструменты предоставляются как сервис
- Вся работа по поддержанию их в рабочем и актуальном состоянии на стороне поставщика
- Работа с самим инструментом и анализ результатов проводятся самостоятельно

Плюсы подхода

SWORDFISH SECURITY

- Нет необходимости в долгой и мучительной установке и обновлении продуктов, все разворачивается по клику
- Динамическое масштабирование ресурсов под трудоемкие задачи
- Готовая «палитра» инструментов
- Возможность быстро опробовать решение
- Удобный процесс оплаты инструментов

Минусы подхода

SWORDFISH SECURITY

- Безопасность самих сервисов, оперирующих чувствительными данными
- Проблемы с интеграцией различных практик, если не вся разработка ведется в облаке
- Возможно долгое решение проблем, связанных с «неидельностью» инструментов
- Готовность самих вендоров к подобным решениям

Что в итоге?

SWORDFISH SECURITY

- На данный момент нет готового предложения, покрывающего все базовые практики
- Подобное решение может стать крайне удобным и полезным для всех участников процесса
- Нет готовности перейти «в облака»
- Нет документальной базы для подобных сервисов (?)

SWORDFISH
SECURITY

Q&A

Юрий Шабалин

Ведущий архитектор ИБ

yshabalin@swordfishsecurity.ru

https://t.me/Mr_R1p

swordfishsecurity.ru