КОД ИБ

ИТОГИ

# АРХИТЕКТУРА НА ЭТАПЕ ПРОДУКТОВОГО ПЛАНИРОВАНИЯ

МОНА АРХИПОВА
Независимый эксперт

КОД ИБ

ИТОГИ

# SHIFT-LEFT ALL*

QA
2001 (!!!)

SEC

DevSecOps

КОД ИБ

ИТОГИ

# «ОБЩИЕ» ПРАКТИКИ

- Отказоустойчивость/масштабирование
- Перетряхиваем API
- Все существенное – только server-side
- Требования Compliance

КОД ИБ

ИТОГИ

# ЧАСТНЫЕ ПРАКТИКИ

- Аварийные ручки (ограничения регистраций, логинов, лимиты на транзакции и т.д.)
- Таймауты с учетом бизнесовых вводных
- Моделирование угроз – через примеры и здравый смысл

КОД ИБ

ИТОГИ

# SEC+SA

- UML-схемы
- Общие требования (управление сессиями, логи и т.п.)
- Требования к data-at-rest

КОД ИБ

ИТОГИ

# SEC+QA

- Проверка валидаций
- Проверка AAA
- Проверка сообщений об ошибках

КОД ИБ

ИТОГИ

# SEC+DEV

- Встраивание во внутренние правила и практики
- Согласованные затраты по времени
- Чем ИБ может быть полезно?

КОД ИБ

ИТОГИ

# ВСЁ ЛИ СДВИГАТЬ?

- Фокус на логику
- Обучение системных аналитиков
- Часть передать на QA (на любой этап до деплоя)
- Малая автоматизация

КОД ИБ

ИТОГИ

# СПАСИБО ЗА ВНИМАНИЕ!

Мона Архипова
Mona.arkhipova@gmail.com
https://t.me/Mona_Sax