Security Training & Awareness

Клочкова Елена

ТИНЬКОФФ

Как было в компании 2 года назад

01 Много проектов

Как было в компании 2 года назад

01 Много проектов

02 Много команд

Как было в компании 2 года назад

01 Много проектов

02 Много команд

03 Много денег

Как было в компании 2 года назад

01 Много проектов

02 Много команд

03 Много денег

04 Много критичной информации

Как было в компании 2 года назад

01 Много проектов

02 Много команд

03 Много денег

04 Много критичной информации

05 Нет процессов безопасности

Как было в компании 2 года назад

01 Много проектов

02 Много команд

03 Много денег

04 Много критичной информации

05 Нет процессов безопасности

06 AppSec только появился

Что уже было в AppSec

- План по внедрению secure SDLC
- Тимлиды про нас знали
- Правила запуска/изменения продукта по secure SDLC
- Процесс Security Patch Development & Deploy Workflow
- SAST
- DAST
- 4 ручных аудита
- Bug-bounty

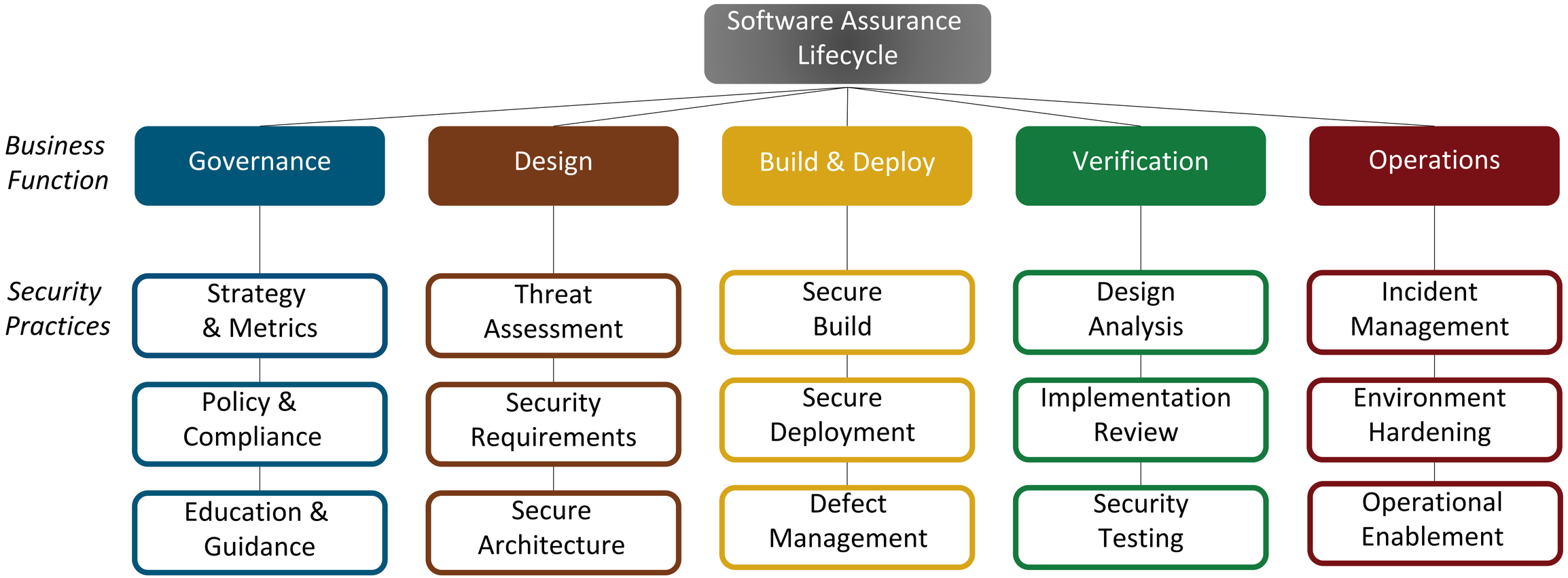
Какие проблемы

- Мало кто знает про AppSec
- Безопасность отстает от высокого темпа развития продуктов

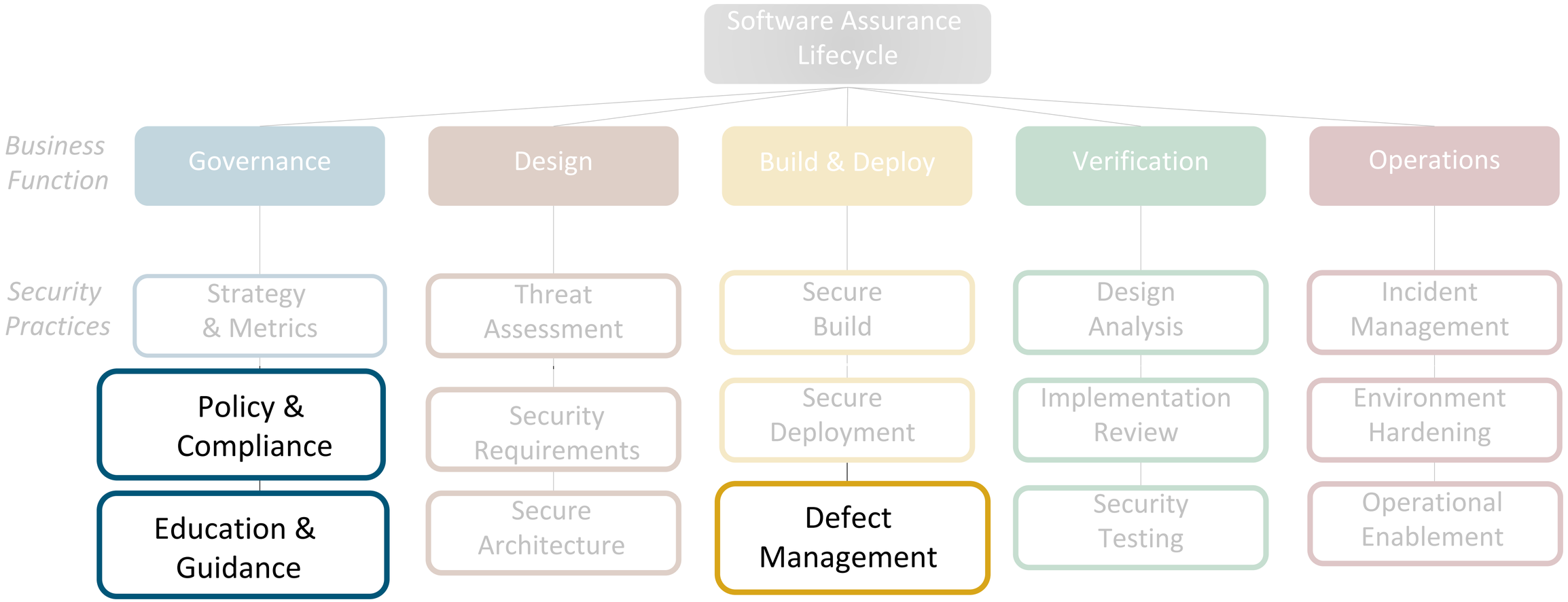
Что необходимо было сделать?

- Поднять узнаваемость AppSec
- Подогреть интерес к безопасности
- Повысить осведомленность в области безопасности
- Развивать secure SDLC

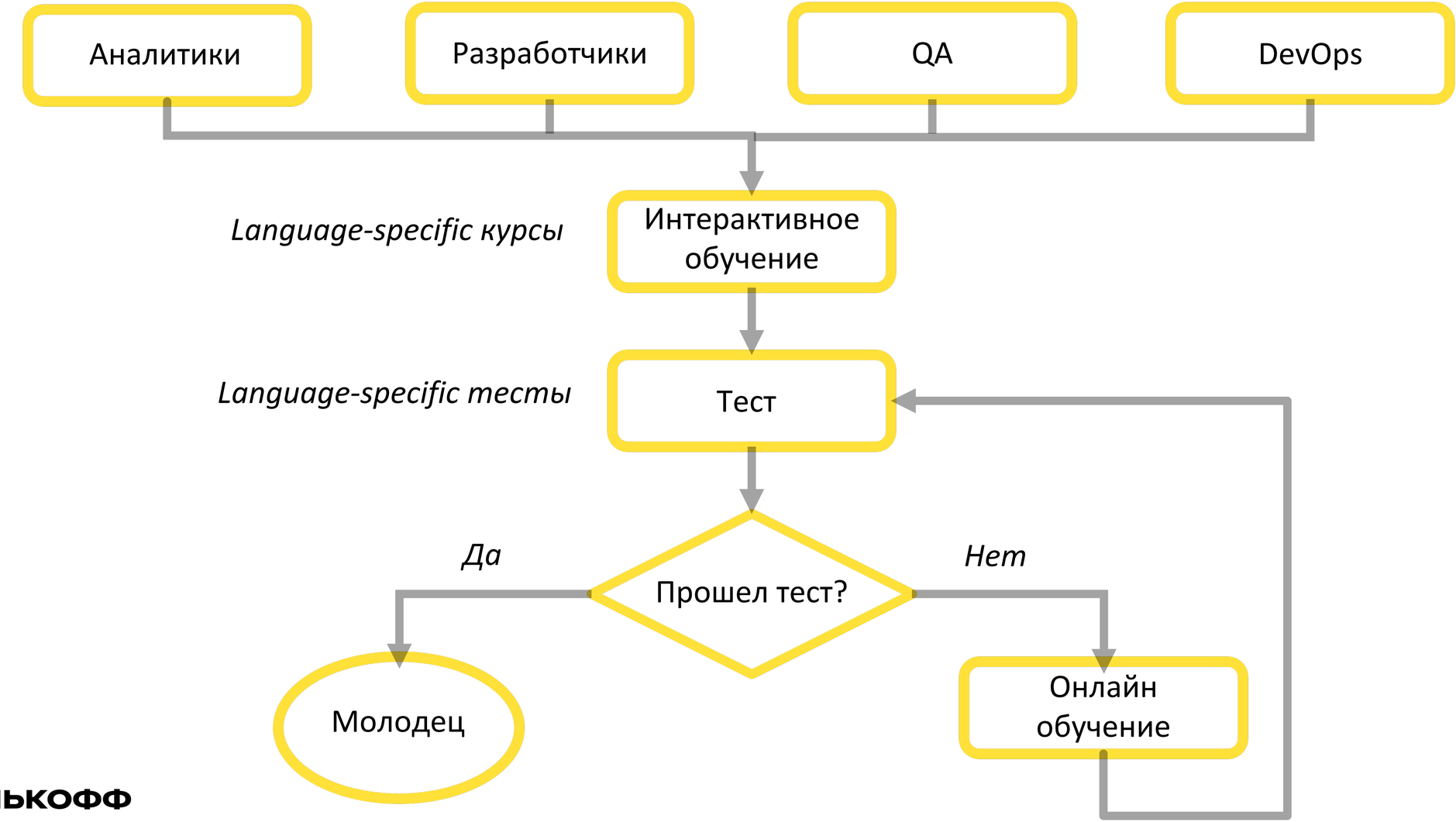
The Software Assurance Lifecycle



The Software Assurance Lifecycle



Онбординг новых сотрудников



Security Development Training

- Знакомство с основными классами уязвимостей из категорий OWASP Top 10
- Понимание причин возникновения и способах предотвращения уязвимостей
- Демонстрация уязвимостей на реальных приложениях

Гайды

- Knowledge Base
- Security Requirements
- Implementation Review Guide (ASVS/MASVS)

Security Champions

Что это?

Security Champions.
Профиты для участников

01 Обучение у лучших экспертов

Security Champions.
Профиты для участников

01 Обучение у лучших экспертов

02 Опыт в развитии безопасной архитектуры

Security Champions.
Профиты для участников

01 Обучение у лучших экспертов

02 Опыт в развитии безопасной архитектуры

03 Внедрение Secure Software Development Lifecycle

Security Champions.
Профиты для участников

01 Обучение у лучших экспертов

02 Опыт в развитии безопасной архитектуры

03 Внедрение Secure Software Development Lifecycle

04 Самостоятельная разработка best practice

Security Champions.
Профиты для участников

01 Обучение у лучших экспертов

02 Опыт в развитии безопасной архитектуры

03 Внедрение Secure Software Development Lifecycle

04 Самостоятельная разработка best practice

05 Расширение кругозора, опыт организации процесса

Security Champions.
Профиты для участников

01 Обучение у лучших экспертов

02 Опыт в развитии безопасной архитектуры

03 Внедрение Secure Software Development Lifecycle

04 Самостоятельная разработка best practice

05 Расширение кругозора, опыт организации процесса

06 Повышение собственной ценности и стоимости на рынке

Security Champions.
Что мы получили?

- Повышение узнаваемости AppSec
- Определение точек входа для безопасности в командах
- Развитие сильного комьюнити внутри компании

Internal Bug-Bounty

Программа поиска сотрудниками уязвимостей в сервисах Тинькофф

Сыщик

репорт Low уязвимости в продуктах банка.

Исследователь

репорт High уязвимости в продуктах банка.

Хакер

репорт Medium уязвимости в продуктах банка.

Month of Bugs

Внутренний конкурс на поиск уязвимостей в сервисах Тинькофф

- Ограниченный по времени (всего 1 месяц)
- Дополнительно освещается и анонсируется
- Призы победителям

Internal Bug-Bounty & Month of Bugs

По программе BB найдено:

~ 15 % от всех уязвимостей

за 1,5 года

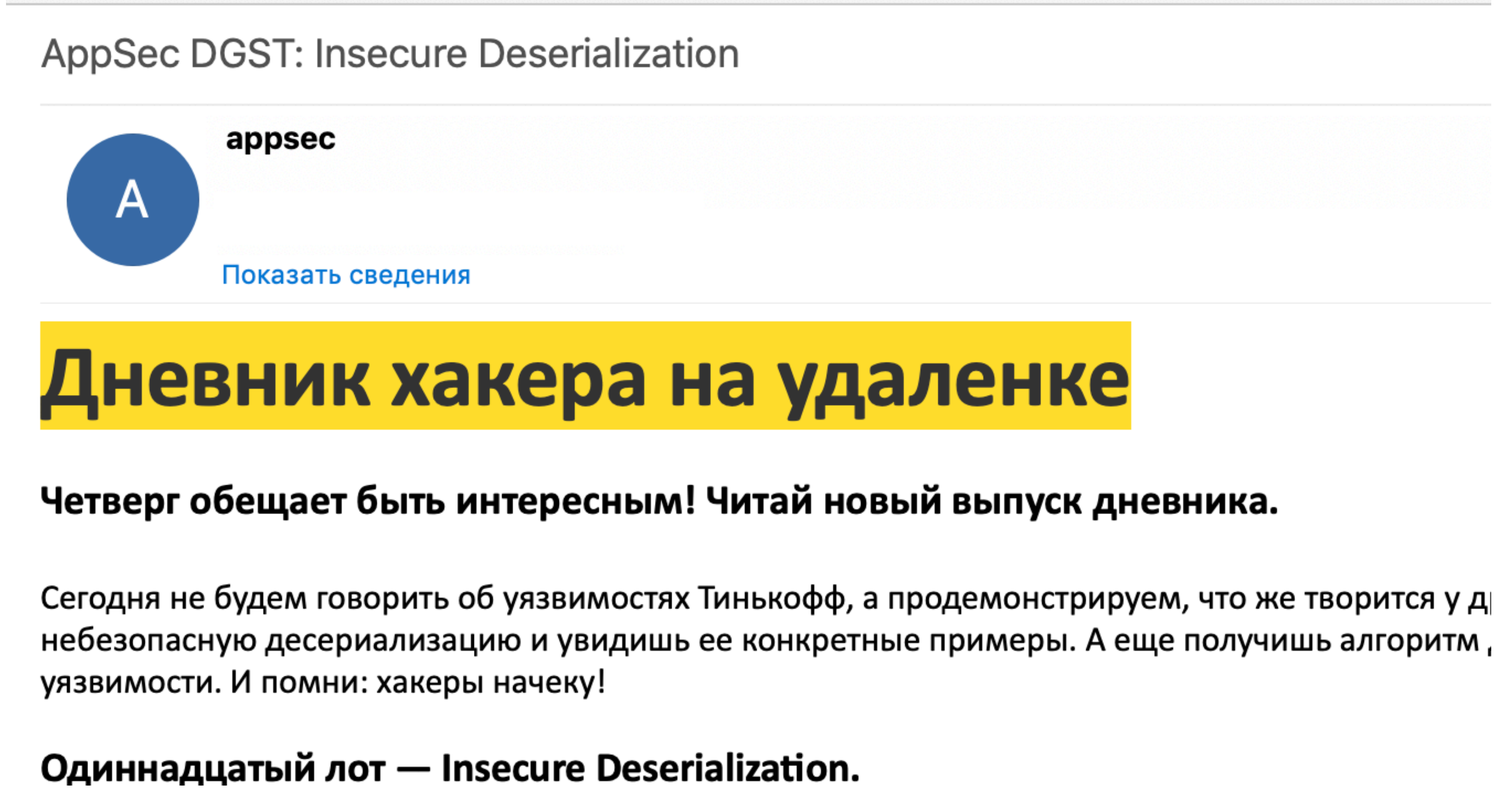
По программе Month of Bugs найдено:

~ 5 % от всех уязвимостей

за 1 месяц

AppSec Digest

Обзор типовых уязвимостей на широкую внутреннюю аудиторию с примерами и рекомендациями по устранению

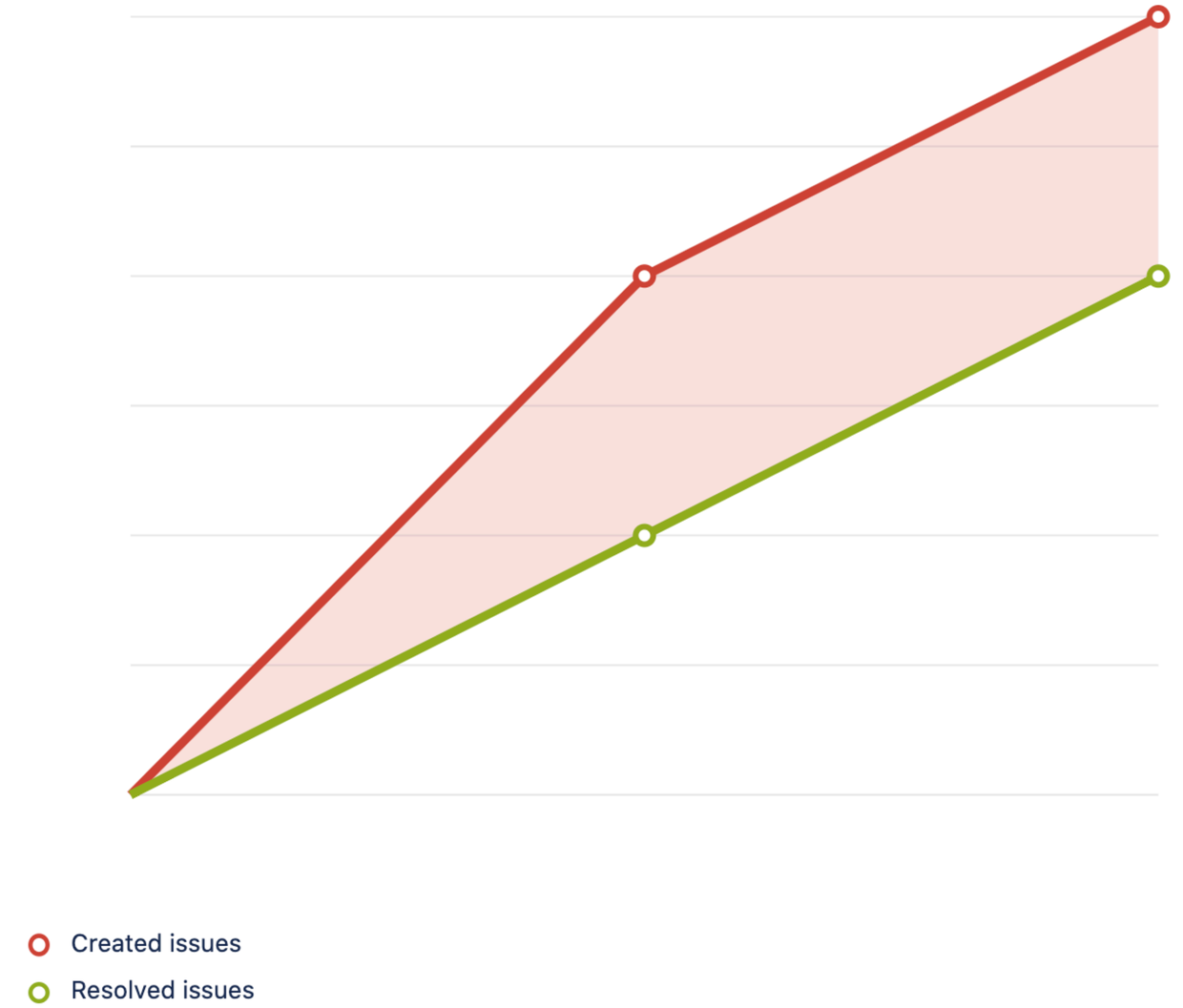


Итоги

- Повысили узнаваемость AppSec внутри компании
- Увеличили приток новых уязвимостей внутренними силами
- Минимизировали появление типовых уязвимостей
- Повысили заинтересованность к поиску уязвимостей
- Повысили интерес к обучению и внутренним гайдам

Новая проблема

Кол-во найденных уязвимостей растет быстрее чем кол-во фиксов



Vulnerability Management – зачем?

- Не выстроенные приоритеты для фиксов
- Отсутствие понимания со стороны разработки «насколько реальна уязвимость»

Vulnerability Management – первая попытка выстроить процесс

Цель - сконцентрироваться на критичных уязвимостях

Подход - индивидуальный по каждой уязвимости к каждому ответственному

Результат – неэффективный процесс

Vulnerability Management & Application Vulnerability Treatment Policy

Цель – сделать процесс прозрачным и сконцентрироваться на критичных уязвимостях

Подход – использовать общую политику исправления уязвимостей, которая включает в себя систему расчета рисков

Vulnerability Assessment. Модель оценки риска

Threat agent factors

Motive
Opportunity
Size

Vulnerability factors

Ease of discovery
Ease of exploit
User interaction

Technical Impact

Loss of confidentiality
Loss of integrity
Loss of availability

Business Impact

Financial damage
Reputation damage
Affected users

Vulnerability Assessment. Как подобрать?

01 Экспертная оценка

02 DREAD

03 CVSS

04 OWASP Risk Rating Calculator

Vulnerability Assessment. Как подобрать?

Модифицируем под себя

04

OWASP Risk Rating Calculator

Vulnerability Assessment. Модель оценки риска

Likelihood Factors

Threat agent factors

Motive
Opportunity
Size

Vulnerability Assessment. Модель оценки риска

Likelihood Factors

Threat agent factors

Motive
Opportunity
Size

Vulnerability factors

Ease of discovery
Ease of exploit
User interaction

Vulnerability Assessment. Модель оценки риска

Impact Factors

Technical Impact

Loss of confidentiality
Loss of integrity
Loss of availability

Vulnerability Assessment. Модель оценки риска

Impact Factors

Technical Impact

Loss of confidentiality
Loss of integrity
Loss of availability

Business Impact

Financial damage
Reputation damage
Affected users

Vulnerability Assessment. Модель оценки риска

Threat agent factors

Motive
Opportunity
Size

Vulnerability factors

Ease of discovery
Ease of exploit
User interaction

Technical Impact

Loss of confidentiality
Loss of integrity
Loss of availability

Business Impact

Financial damage
Reputation damage
Affected users

Application Vulnerability Treatment Policy

Blocker: 10, 9	Фикс - 3 дня
Critical: 8, 7	Фикс – 7 дней
Major: 6, 5	Фикс – 30 дней
Normal: 4, 3	Фикс – 90 дней
Minor: 2, 1	Фикс – 180 дней
Trivial: 0	Фикс по усмотрению владельца

Vulnerability Management & Application Vulnerability Treatment Policy

- Экономит время и избавляет от споров о приоритетах
- Помогает гарантировать, что бизнес не будет отвлечен незначительными рисками, игнорируя при этом более серьезные риски.

Вопросы?

тинькофф