SWORDFISH
SECURITY

Мифические Security Champion’ы или как не сойти с ума в мире безопасной разработки

Газизова Светлана
Swordfish Security

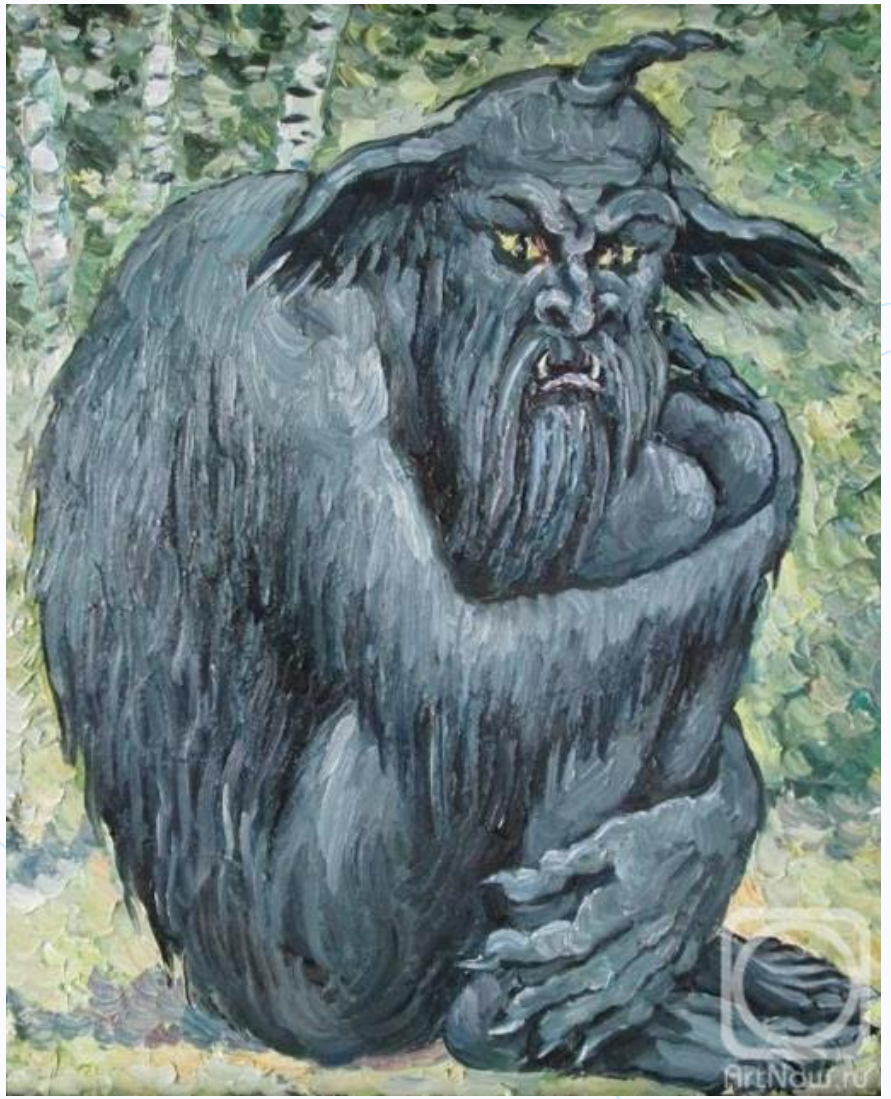
Шурале

Шурале обитает преимущественно в лесу - в одном лесу могут обитать сразу несколько особей.

Занимается тем, что сбивает одиноко идущих по лесу людей с пути, заманивает в глухие чащи; способен защекотать до смерти своими длинными пальцами.

Шурале боится воды, что можно использовать как один из способов спастись от него — перепрыгнуть ручей. Также боится огня. Шурале можно поймать в ловушку, например, уговорив его засунуть палец в расщеплённое дерево, после чего вышибить клин.

(с) Википедия



Картина Ягужинской Анны
artnow.ru

Security Champion

...

SWORDFISH
SECURITY

Сирена

Дед Мороз

Русалка

Единорог

Валькирия

Вампир

Феникс

Зубная фея

Шурале

Security Champion

Йети

Оборотень

Дракон

SWORDFISH SECURITY

DISCLAIMER

Все совпадения с реальностью являются чистейшей случайностью!

SWORDFISH SECURITY

Почему есть смысл меня слушать?

#ктоя

руководитель направления аудита безопасной разработки: выстраиваю процессы, занимаюсь стратегией AppSec и всея, что около☺
автор и тренер курсов DevSecOps

#ктомы

архитекторы, консультанты, инженеры процессов безопасной разработки
внедряли DevSecOps/Appsec в финтех, банки, ИТ-компании, здравоохранение, гос.сектор

SWORDFISH SECURITY

Агенда

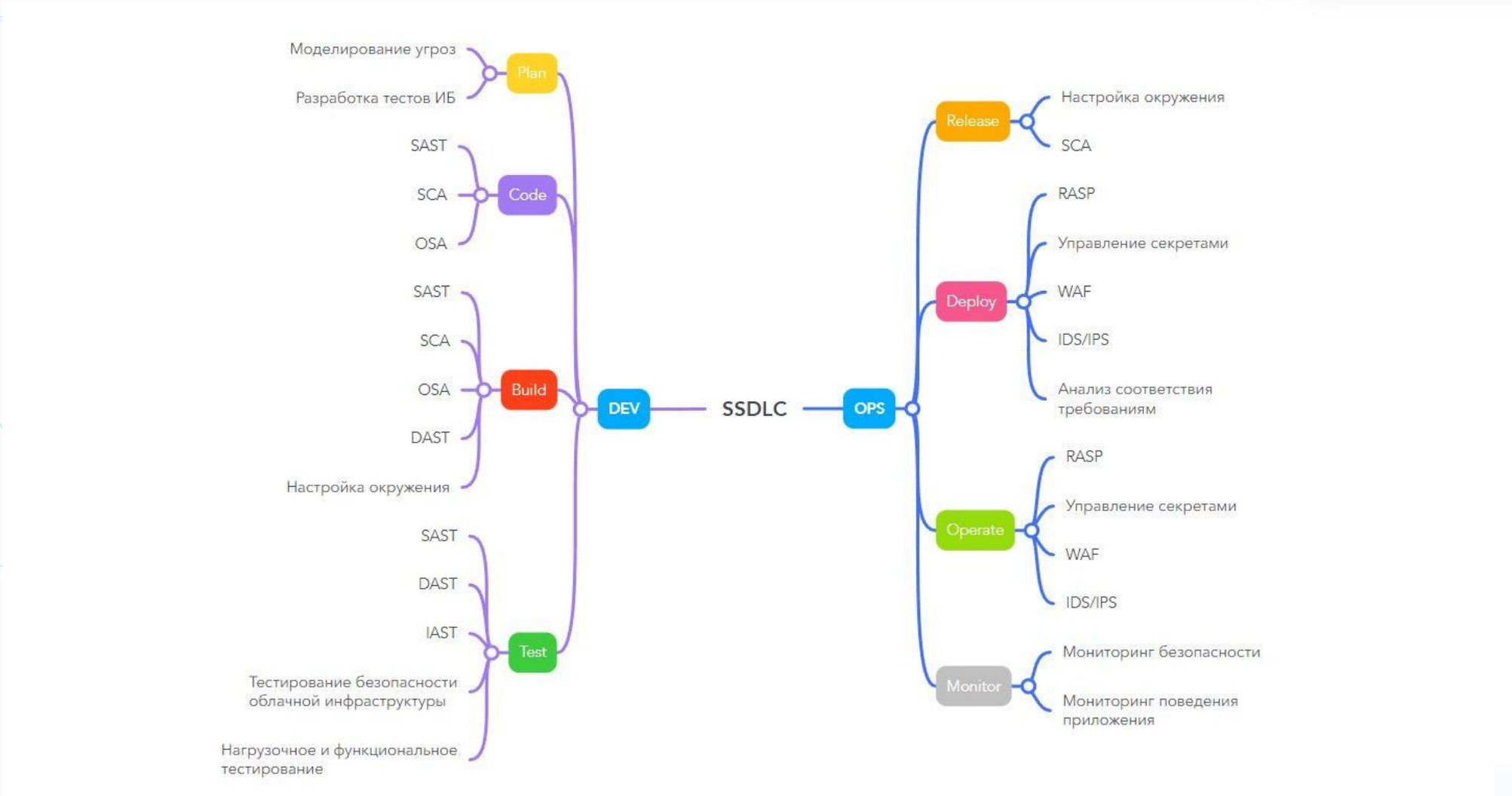
1. Кто такие Security Champion’ы?

2. Почему они нужны и почему их нет?

3. Как сделать сказку явью?

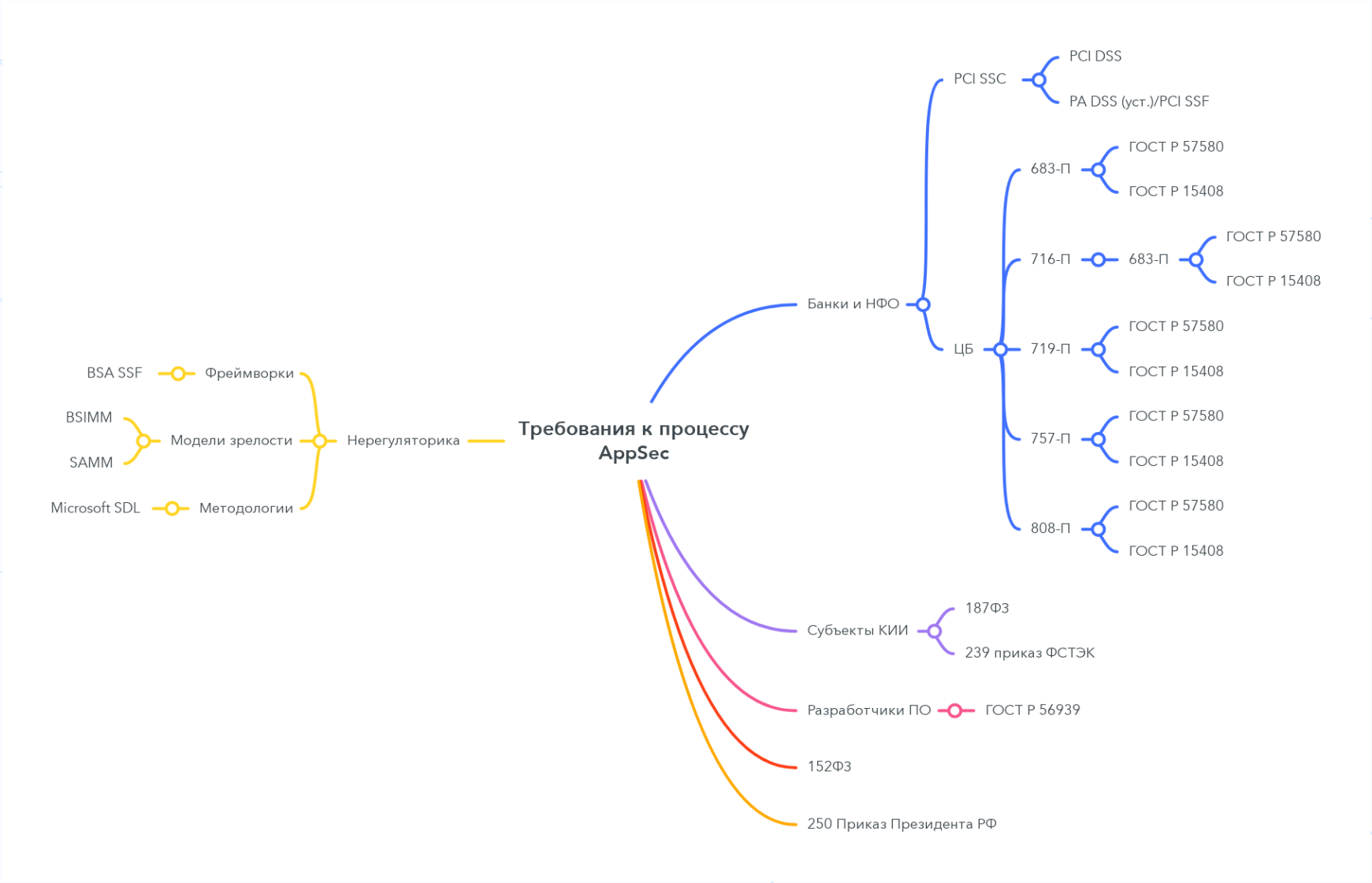
SWORDFISH SECURITY

Лирическое отступление



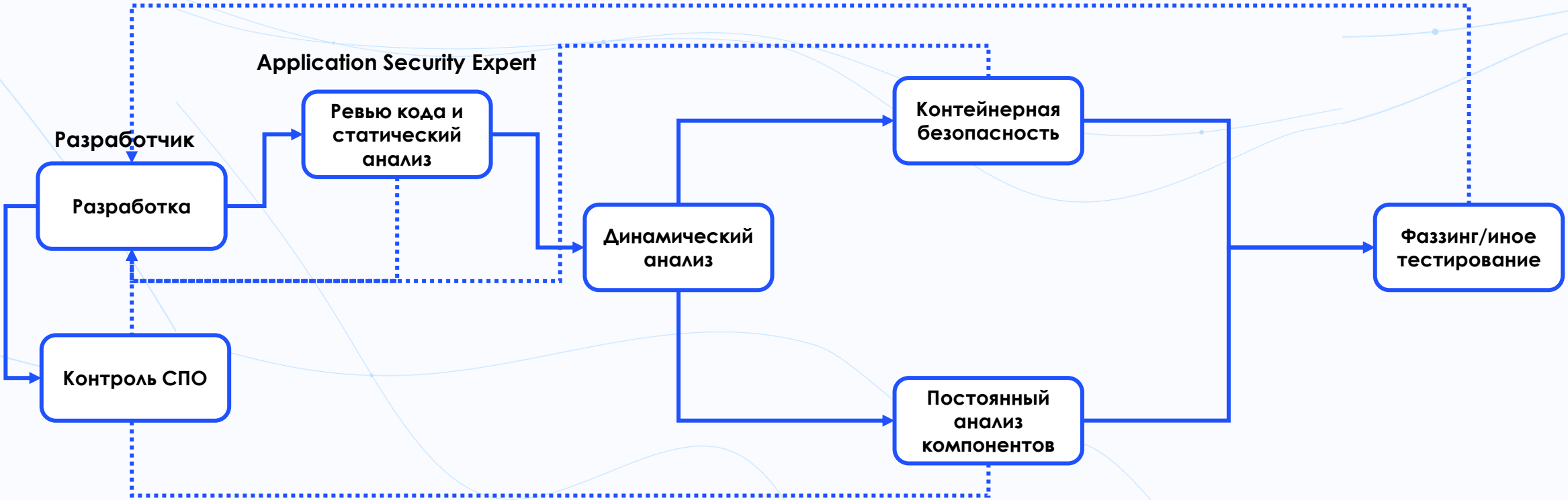
SWORDFISH SECURITY

Лирическое отступление



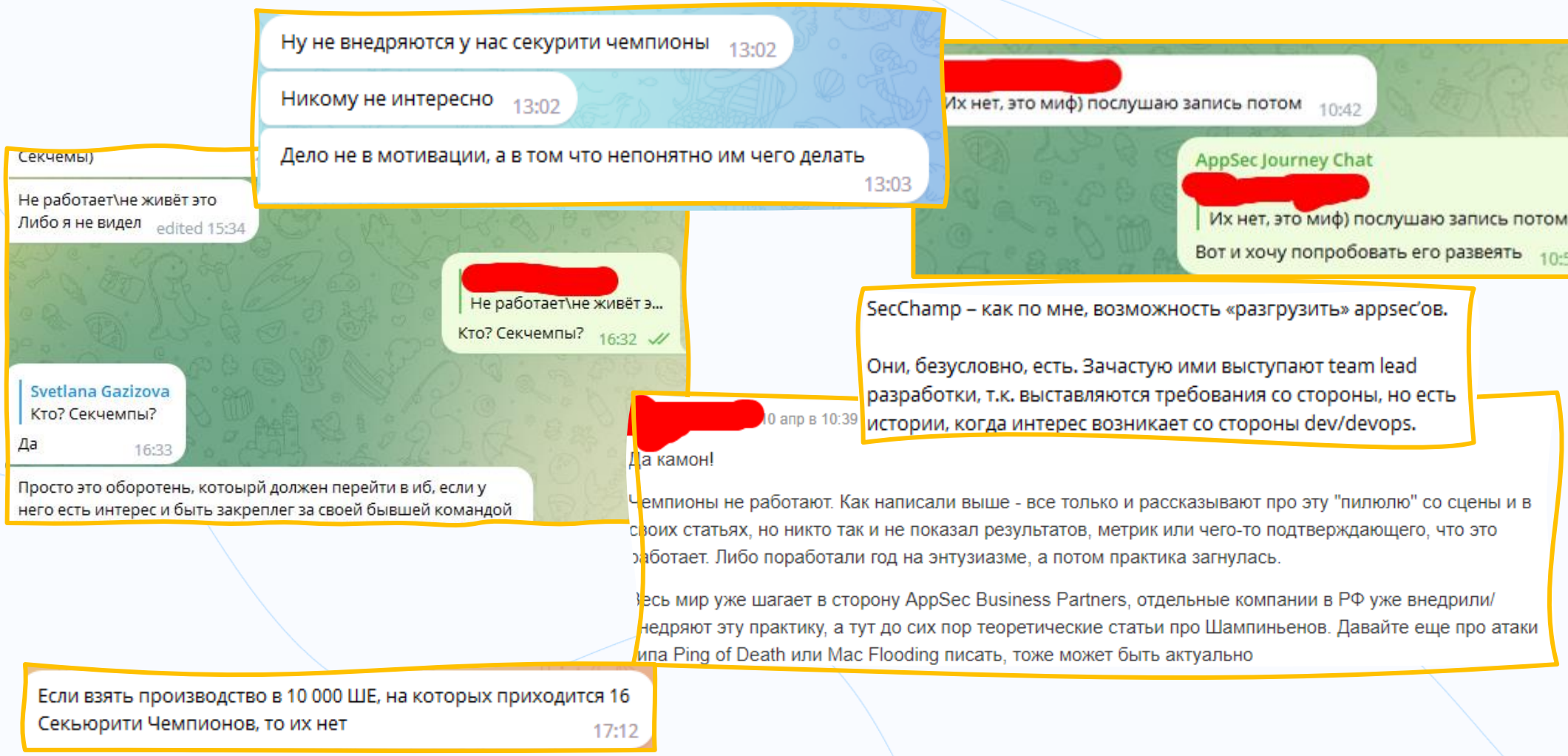
SWORDFISH SECURITY

Хороший DevSecOps



SWORDFISH SECURITY

Security Champion. Понять



SWORDFISH SECURITY

Security Champion. Что говорит интернет?

Обычно так называют сотрудников команды разработки, выступающих в интересах группы ИБ. Они участвуют в повседневной разработке, понимают цели, процессы и особенности команды. Чемпионами могут быть QA, проект-менеджеры, разработчики — кто угодно, лишь бы сотрудник «радел» за безопасность. Чемпионы выступают в качестве «точки входа», «мостика» к безопасности приложений для своей команды.

(c) статья на Хабр
https://habr.com/ru/companies/vk/articles/725088/

Security Champion. Что говорит регулятор?

Security Champion – активный член команды, как правило, не являющийся сотрудником подразделения информационной безопасности, который вводит и поддерживает в рамках командных практик лучшие практики по обеспечению информационной безопасности, идентификации рисков ИБ и т.д. Такой член команды может сочетать роль Security Champion с ролью разработчика, тестировщика и др.

(c) Профиль Защиты
https://www.cbr.ru/content/document/file/132666/inf_note_feb_0422.pdf

Security Champion. Что думаю я?

Security Champion – *(не)вымышленный персонаж*, который находится в ИТ-команде и помогает Application Security подразделению в разборе дефектов и адаптации практик ИБ внутри своей команды.

Вопросы, которые может решать SC:
- исправление уязвимостей
- принятие риска
- security awareness/продвижение культуры
- доработка правил на инструменте
....
и много-много чего еще!

SWORDFISH SECURITY

Почему они вообще появились?

Мы не вывозим!

SWORDFISH SECURITY

Автономия команд

Учитывая нехватку ИБ-кадров, нужно иметь своих «агентов» внутри команд разработки.
Помимо очевидной пользы, это позволит не контролировать работу инструментов и технический долг в каждой отдельно взятой команде разработки. Цель сделать команды разработчиков более самодостаточными и автономными может быть достигнута только при наличии знаний и понимания.

Автономия команд

SWORDFISH
SECURITY

Нелинейное развитие ИБ

Важно, чтобы безопасные методы разработки были признаны и поняты всеми командами разработчиков. Если инженеры обучают инженеров, это гораздо более успешный подход к развитию этих знаний и образования. Единственный способ масштабировать безопасную разработку — через инженерную организацию, предоставив команде безопасности полномочия и поддержку разработчиков.

Нелинейное развитие ИБ

Нам нужны союзники

Почему их нет?

SWORDFISH
SECURITY

(Не)очевидные причины

Свой среди чужих и чужой среди своих

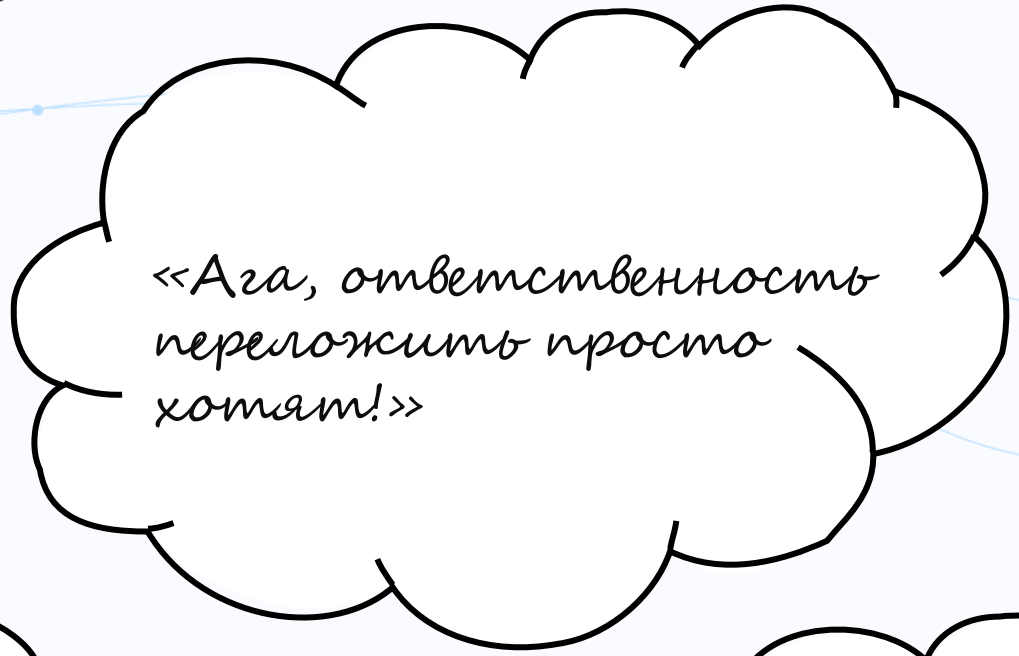
Задачи, вроде бы, как у разработчика.
KPI, вроде бы, как у разработчика.

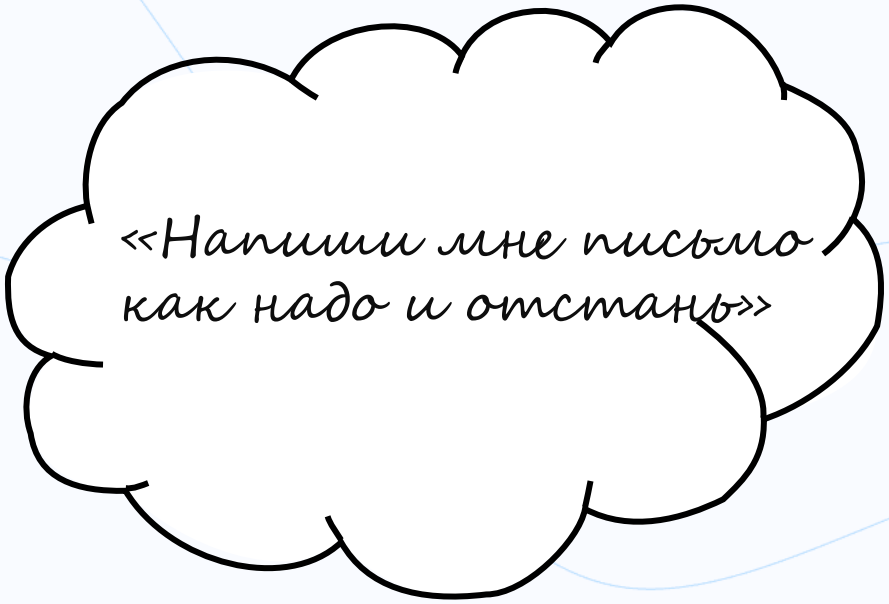
Свой среди чужих и чужой среди своих

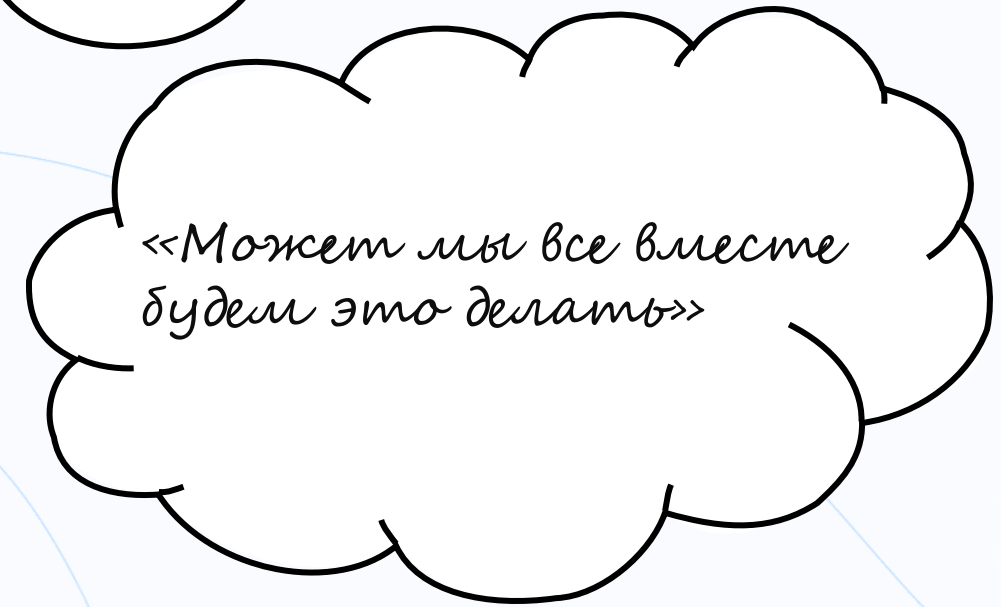
Задачи, вроде бы, как у разработчика.
KPI, вроде бы, как у разработчика.

ВРОДЕ БЫ?!

А мне это зачем?!

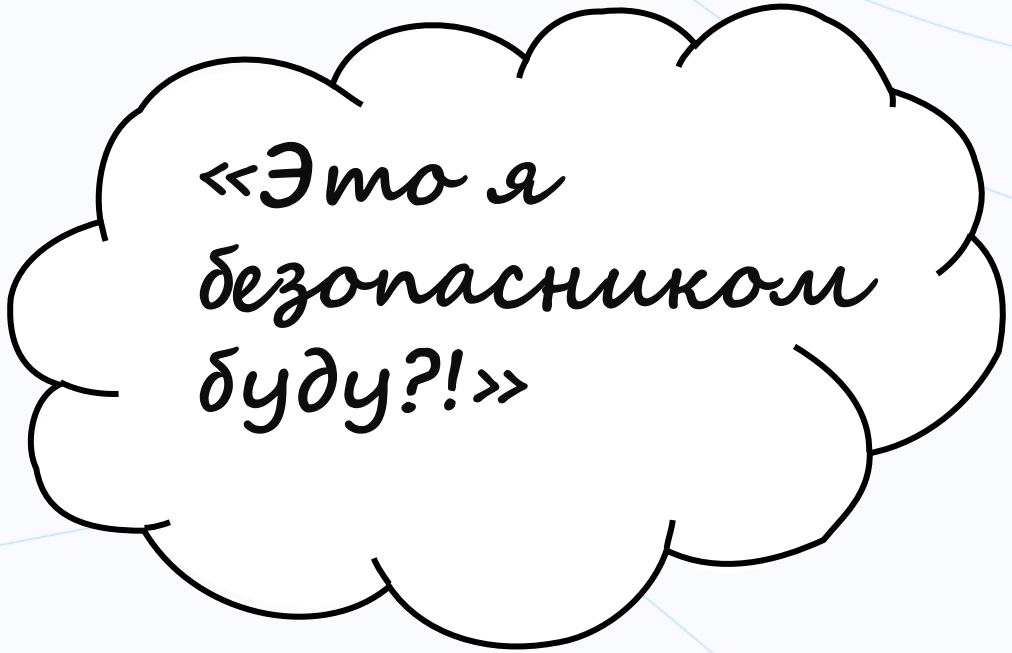






SWORDFISH SECURITY

А мне это зачем?!



Где взять Security Champion’ов?

SWORDFISH
SECURITY

Категорическое «нет»

Нанять с рынка!

SWORDFISH
SECURITY

Категорическое «нет»

~~Нанять с рынка!~~

SWORDFISH SECURITY

Категорическое «нет»

Перевести кого-то из ИБ!

SWORDFISH SECURITY

Категорическое «нет»

~~Перевести кого-то из ИБ!~~

SWORDFISH SECURITY

Категорическое «нет»

Прописать в должностной инструкции!

SWORDFISH SECURITY

Категорическое «нет»

~~Прописать в должностной инструкции!~~

SWORDFISH SECURITY

Категорическое «да»

Привлечь HR!

SWORDFISH SECURITY

Привлечь HR!

Любые около-кадровые перестройки должны быть под надзором тех, кто понимает немного психологии сотрудников.

Если человек будет демотивирован, выполняя второстепенную для него работу – в чем смысл?

SWORDFISH SECURITY

Категорическое «да»

Поговорить с командой!

SWORDFISH SECURITY

Поговорить с командой!

Все программы по обучению специалистов, создаются, как правило с привлечением экспертов отрасли, ресурсов извне и авторским надзором.

А учиться-то не им... **Поговорите с командой, что они хотят?**

SWORDFISH SECURITY

Категорическое «да»

Выделить бонусов!

SWORDFISH SECURITY

Выделить бонусов!

«За деньги да»

Пожалуйста, прекратите предлагать хвалить специалистов, дарить нам кружки, футболки, ручки и внутри говорить: «А вот Вася после работы еще два часа триажит!»

ДАЙТЕ ВАСЕ ДЕНЕГ И СВОБОДУ ДЕЙСТВИЙ!

Что можно сделать конкретно мне?

SWORDFISH
SECURITY

SWORDFISH SECURITY

Спасибо, что вы здесь!

Визитка

Кое-что невошедшее

@APPSECJOURNEY

За шаблоны для мемов спасибо: https://www.meme-arsenal.com