WILDBERRIES

Безопасновизация

Алексей Федулаев
DevSecOps Team Lead

$whoami

- **Алексей Федулаев**
- В ИБ с 2011 года
- DevSecOps Team Lead в Wildberries
- Специалист по безопасности контейнерных перевозок
- Спикер крупнейших российских конференций, состою в программном комитете DevOops Conf и SafeCode Conf, автор канала @ever_secure

С чем же я к вам пришел?

- С болью безопасника
- С историей от отрицания до принятия

И вот моя история

…disclaimer

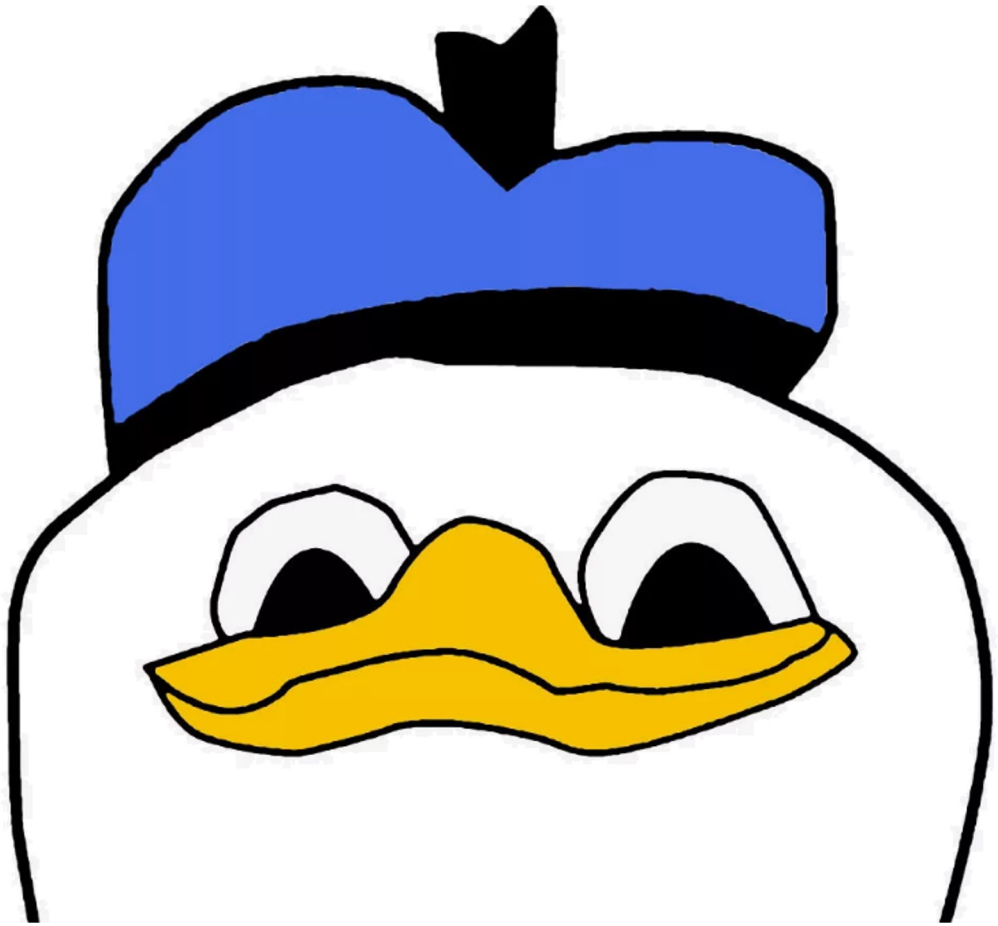
- Все персонажи в ней конечно же вымышленные

…disclaimer

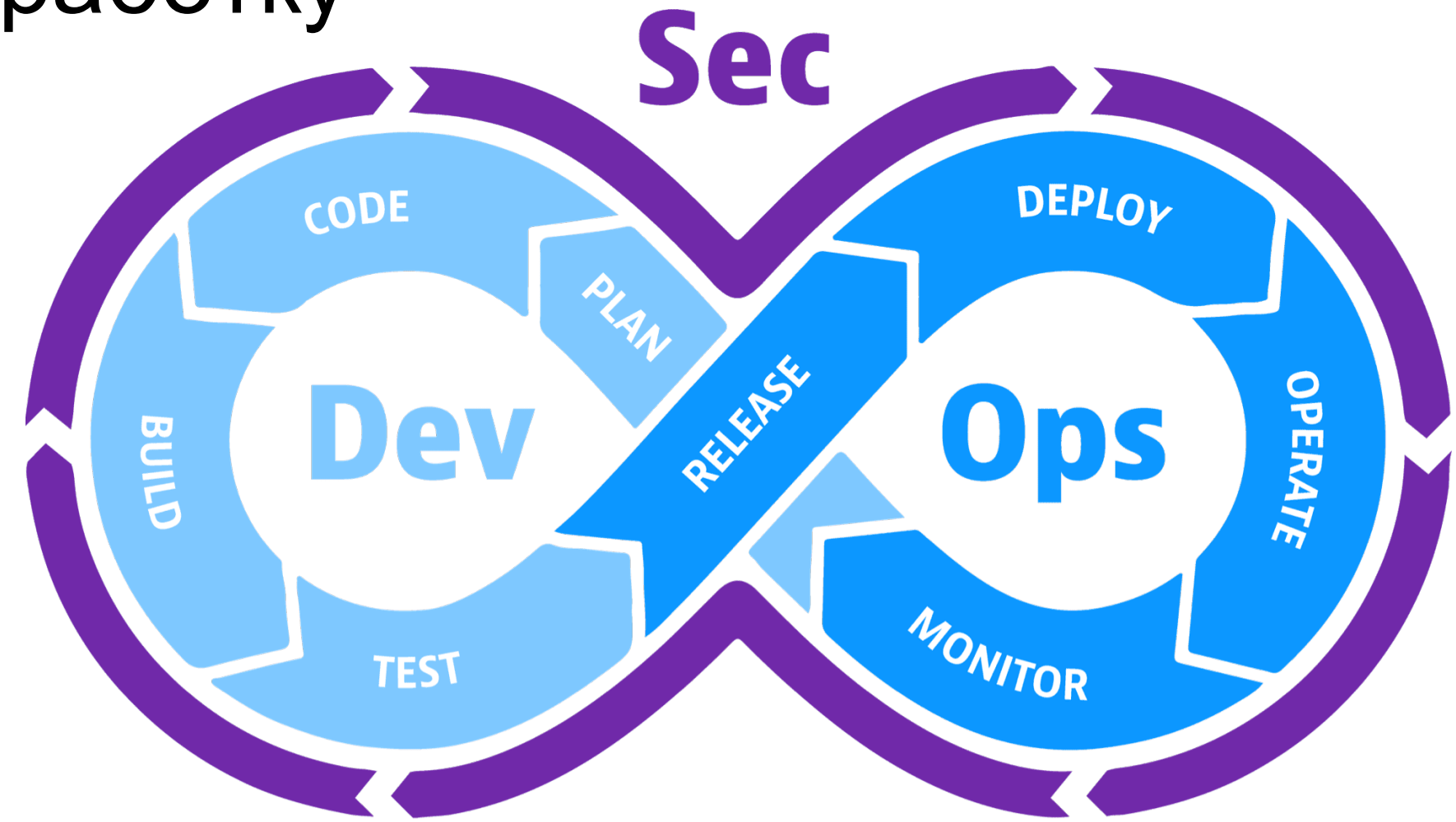
- Все персонажи в ней конечно же вымышленные
- И произошла она не со мной (мне друг рассказывал)

Пришел как-то Алексей в компанию X

Пришел как-то Алексей в компанию X



Пришел строить безопасную разработку



Но сначала -

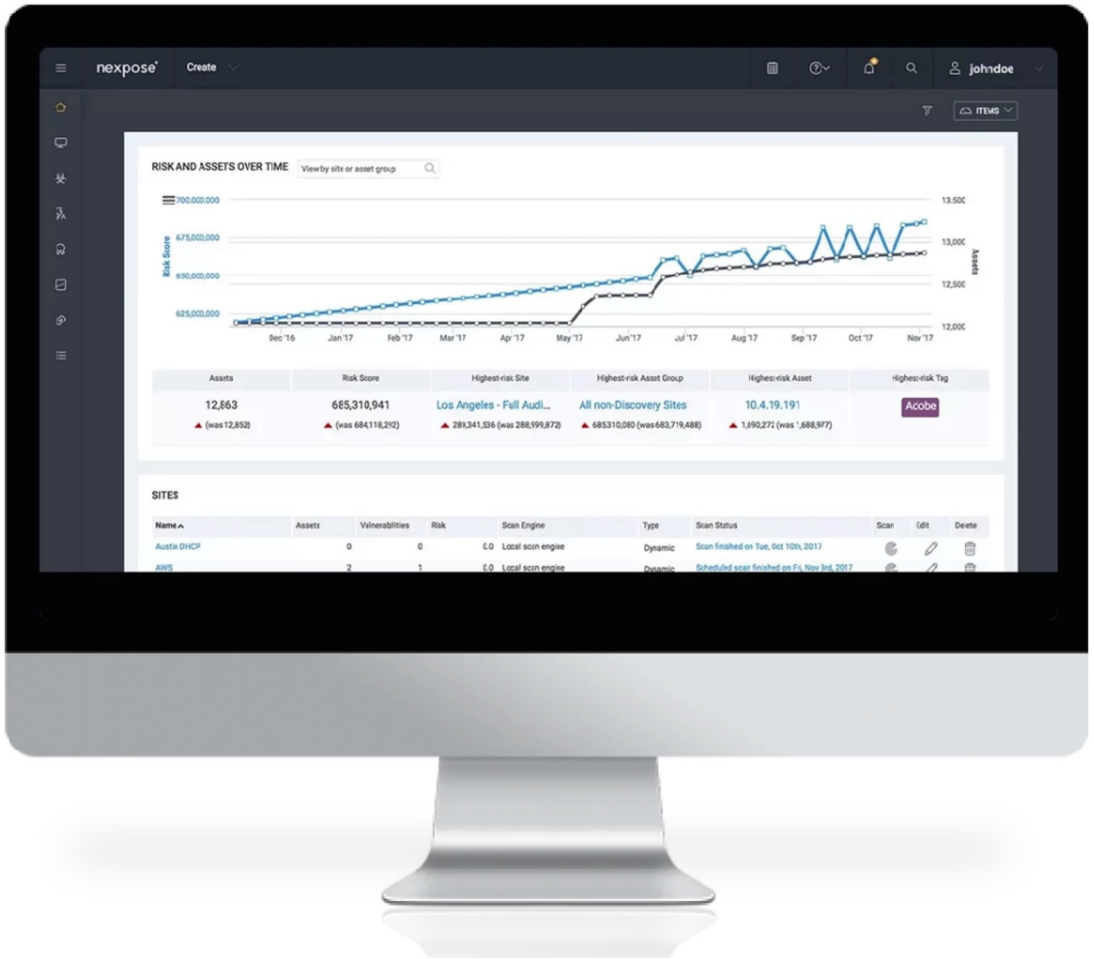
- Надо поднять необходимые инструменты безопасности
- Получить Вмки у администраторов

Получил VM с дефолтными кредами

И тогда подумал

Seems like Дыра в безопасности

Развернул триал любимого сканера

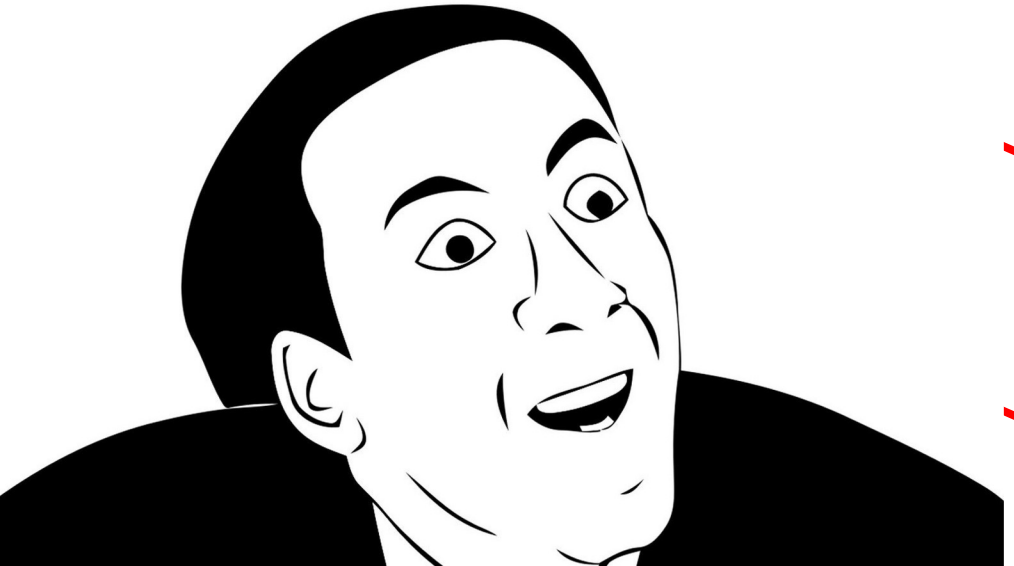


Nexpose Vulnerability Scanner

Your on-prem vulnerability scanner

GET STARTED

Искал медь, а нашел золото



Operating System	Vulnerabilities	Scan Duration
Ubuntu Linux 14.04	470	5 minutes
Ubuntu Linux 14.04	370	5 minutes
CentOS Linux	270	15 minutes
Debian Linux 7.0	201	7 minutes
Microsoft Windows Server 2008 Standard Edition SP2	98	19 minutes
Ubuntu Linux 16.04	77	5 minutes
Ubuntu Linux 12.04	67	10 minutes
Microsoft Windows	42	9 minutes
Microsoft Windows Server 2016 Standard Edition	36	8 minutes
Microsoft Windows Server 2012 R2 Standard Edition	34	9 minutes

С этим надо что-то делать

Пошел к директору

Ожидание

Реальность

Более того

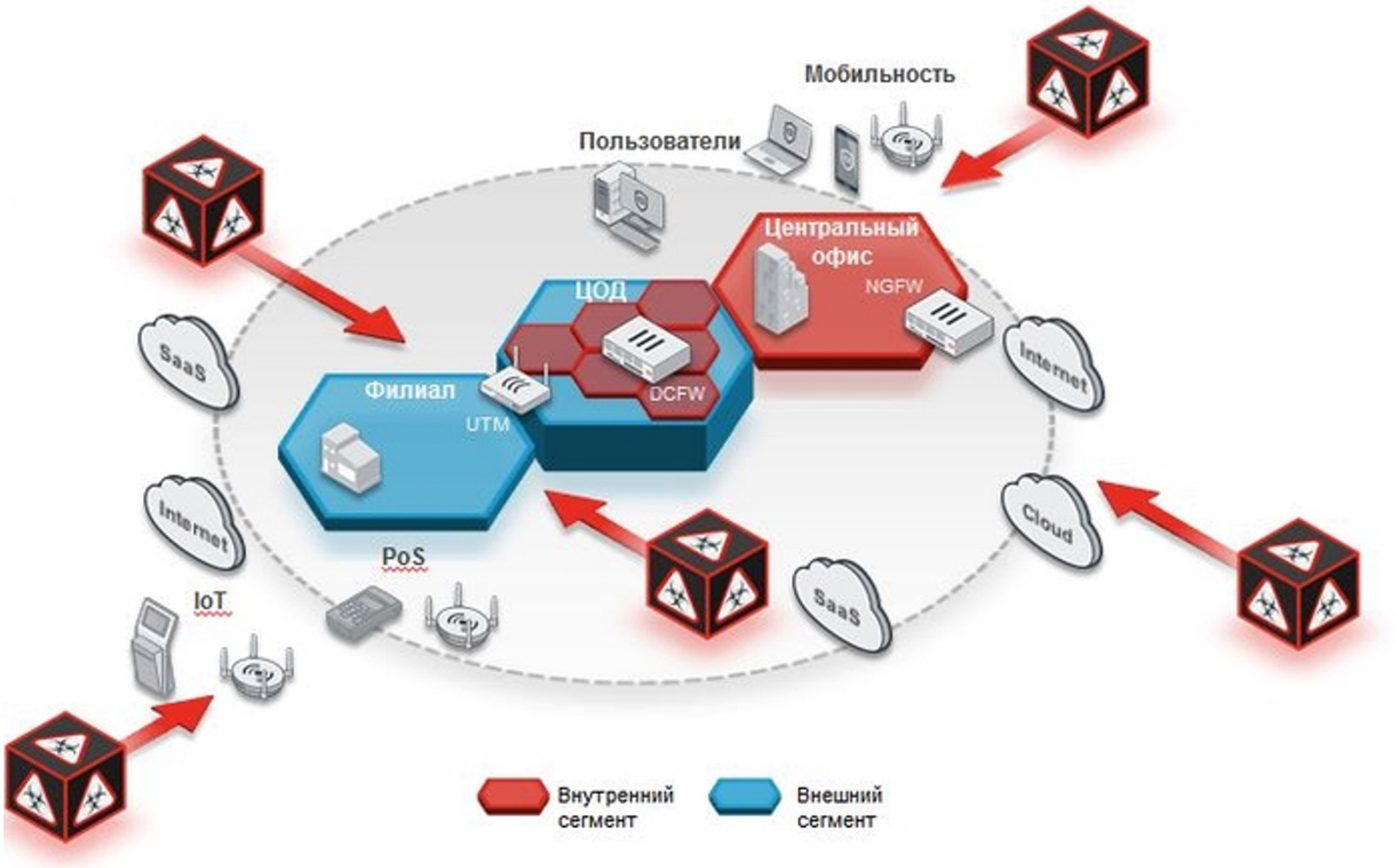
- Мы хотим безопасную разработку
- А ты говоришь про Infrasec, а зачем он нам?
- У компании нет как такового продакшена, терпимо и так

Потом их пошифровали

Уже потом наняли еще безопасников

Какая мораль?

Нельзя сделать безопасно какую-то часть



Безопасность должна быть комплексной

то есть

- по аналогии с цифровизацией)

то есть

- по аналогии с цифровизацией)
- нам нужно начать трансформироваться в безопасность

то есть

- по аналогии с цифровизацией)
- нам нужно начать трансформироваться в безопасность
  шуточно я назвал ее безопасновизацией

Если мы не хотим такое

Если мы не хотим такое

- нам нужно быть готовыми к сегодняшним вызовам

Если мы не хотим такое

- нам нужно быть готовыми к сегодняшним вызовам
- мы должны уже сегодня начать трансформироваться в безопасность

И не превращаться из супергероя в

- 0 сотрудников в ИБ
- 0 бюджета на инструменты
- 7 инцидентов в неделю

Опыт других, всегда поучителен!

Надеюсь и моя история сдвинет вашу безопасность с мертвой точки

Спасибо за внимание!

Алексей Федулаев

tg: @int0x80h