Проактивная защита внешнего периметра: подходы и актуальные решения

```
→ ~ $ whoami
Брагин Максим

R&D Lead Singleton Security
Penetration testing
Bug Bounty
```

@esetal

Проблемы

- **~100%** компаний имеют уязвимости уровня **Высокий** на своем внешнем периметре

Проблемы

- **~100%** компаний имеют уязвимости уровня **Высокий** на своем внешнем периметре
- **~80%** цифровых активов изменяются в течение года

Проблемы

- **~100%** компаний имеют уязвимости уровня **Высокий** на своем внешнем периметре
- **~80%** цифровых активов изменяются в течение года
- в среднем компании не знают о **~30%** имеющихся у них цифровых активов

Проблемы

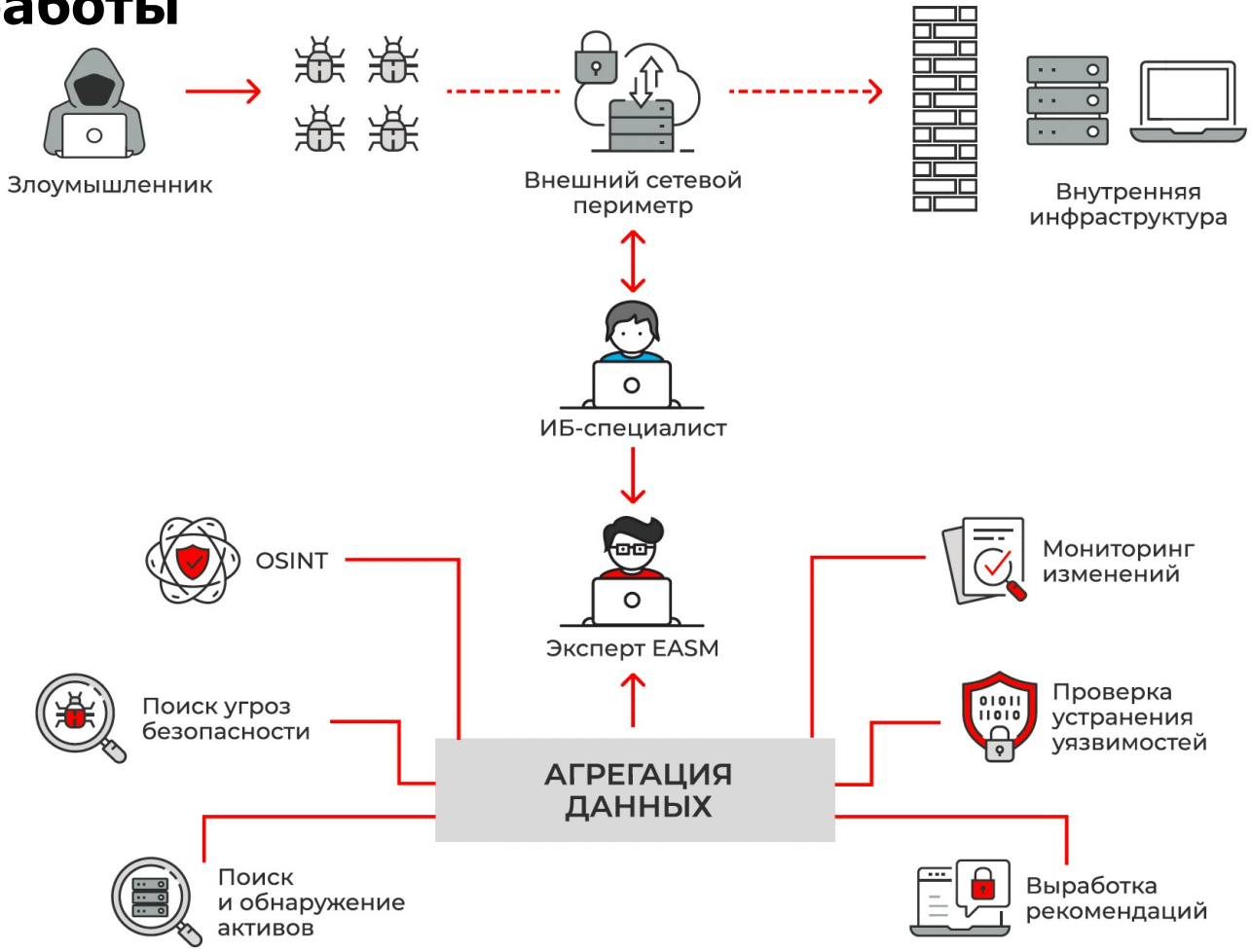
- **~100%** компаний имеют уязвимости уровня **Высокий** на своем внешнем периметре
- **~80%** цифровых активов изменяются в течение года
- в среднем компании не знают о **~30%** имеющихся у них цифровых активов
- **5.5** месяцев — среднее время жизни уязвимости на внешнем периметре

Проблемы

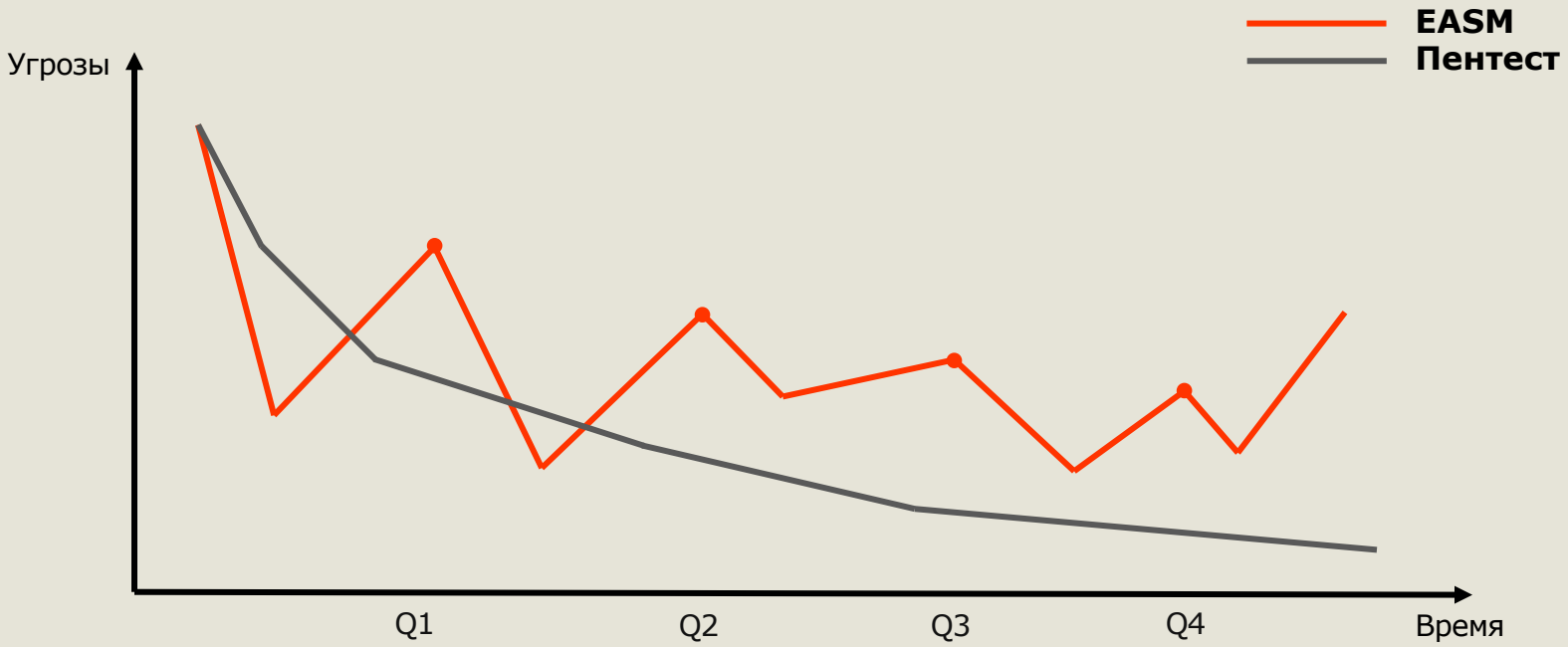
- **~100%** компаний имеют уязвимости уровня **Высокий** на своем внешнем периметре
- **~80%** цифровых активов изменяются в течение года
- в среднем компании не знают о **~30%** имеющихся у них цифровых активов
- **5.5** месяцев — среднее время жизни уязвимости на внешнем периметре
- менее **50%** зафиксированных уязвимостей устраняются быстрее, чем за 3 месяца

EASM
External attack surface management

Схема работы



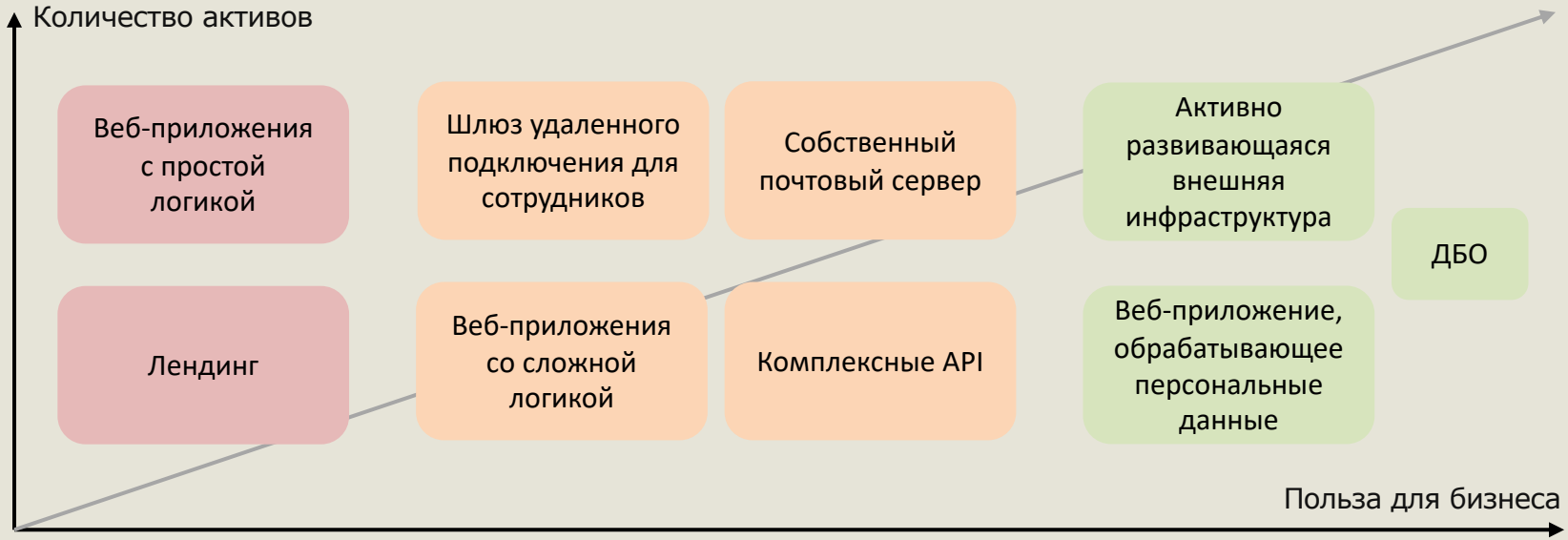
EASM или Pentest?



EASM и CPT (Continuous Penetration Testing): в чем разница?

Актуальность для бизнеса

Уровень помощи платформы для компании растет вместе с объемами её инфраструктуры - активами, доступными из сети Интернет



Больше активов - больше пользы от использования платформы

Ключевые особенности Singleton EASM

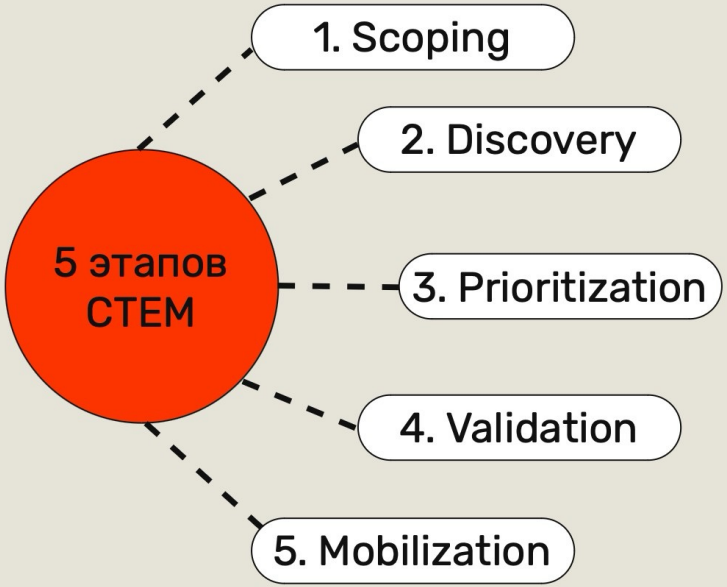
01 Максимизация количества обнаруженных уязвимостей за счет применения собственных инструментов

02 Использование многолетней богатой экспертизы команды анализа защищенности

03 Экспертное сопровождение, выработка наиболее релевантных рекомендаций по устранению каждой уязвимости

04 Приоритизация наиболее критичных активов и уязвимостей, которые с наибольшей вероятностью будут использованы против организации.

CTEM (Continuous Threat Exposure Management) – комплексный подход к обеспечению безопасности



Приходите к нам

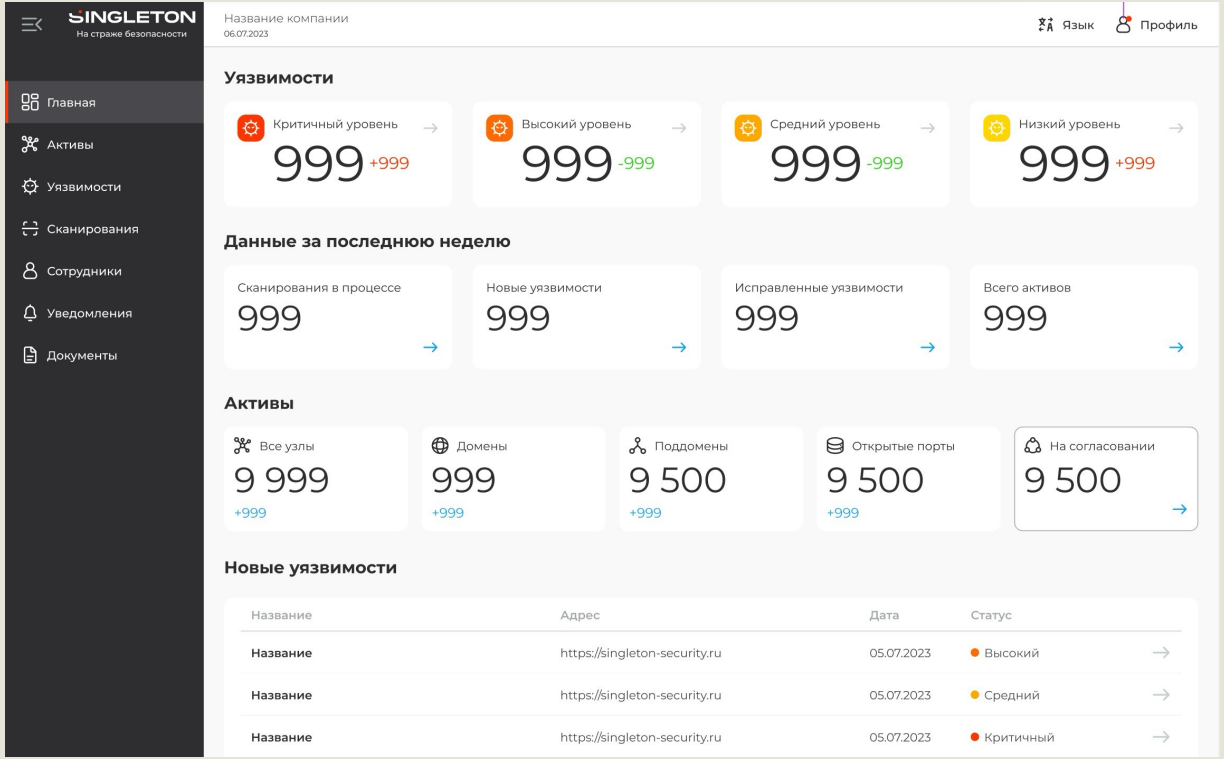
01 Мы будем следить за вашими активами в Интернете

02 Будем непрерывно искать уязвимости в вашей инфраструктуре

03 Научим вас превентивно защищаться от атак

Book a Demo

Свяжитесь с нами



@POSTNIKOVAVA

или заполните форму


SINGLETON
SECURITY