



Проактивная защита внешнего периметра: подходы и актуальные решения



```
→ ~ $ whoami  
Брагин Максим  
  
R&D Lead Singleton Security  
Penetration testing  
Bug Bounty
```

h   @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

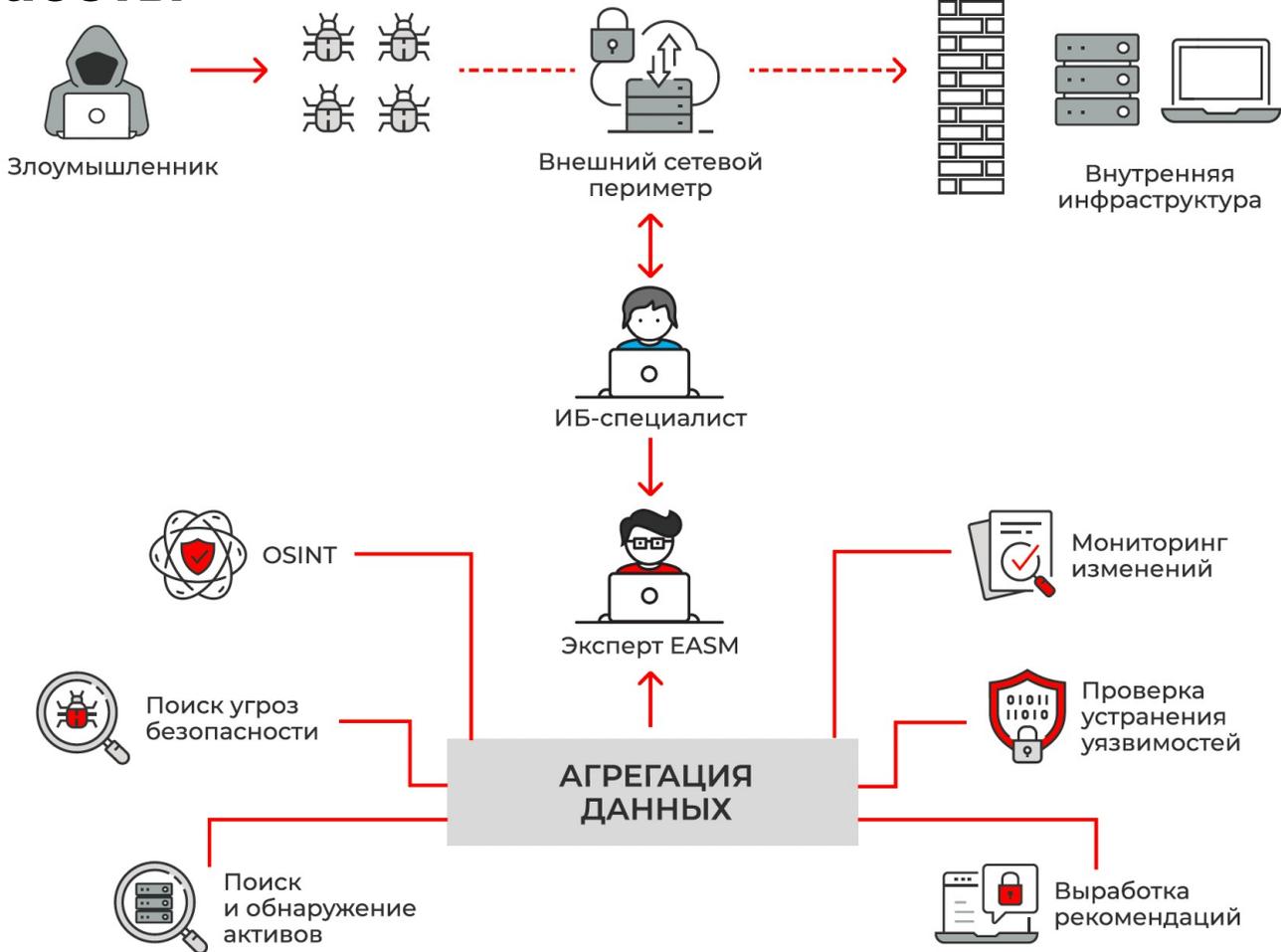
- **~100%** компаний имеют уязвимости уровня **Высокий** на своем внешнем периметре
- **~80%** цифровых активов изменяются в течение года
- в среднем компании не знают о **~30%** имеющихся у них цифровых активов
- **5.5** месяцев — среднее время жизни уязвимости на внешнем периметре
- менее **50%** зафиксированных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



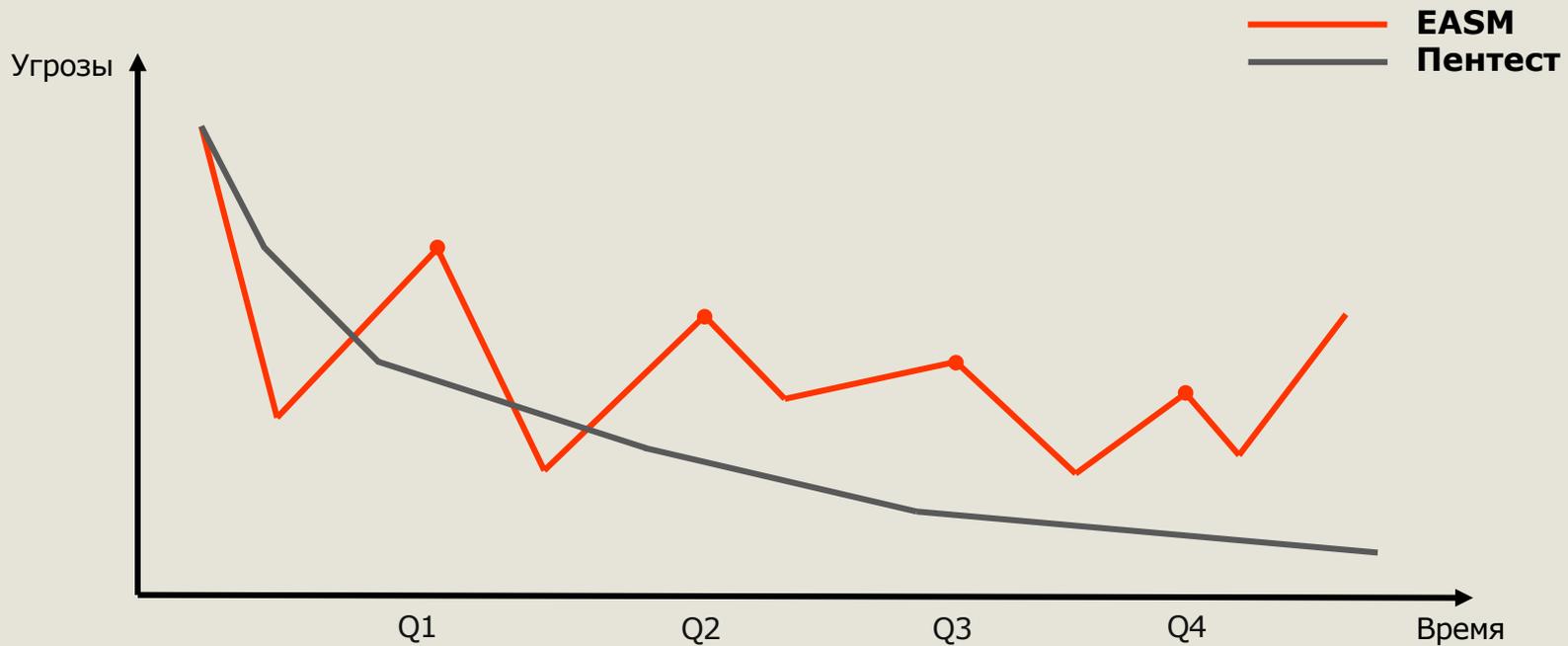
EASM

External attack surface management

Схема работы



EASM или Pentest?



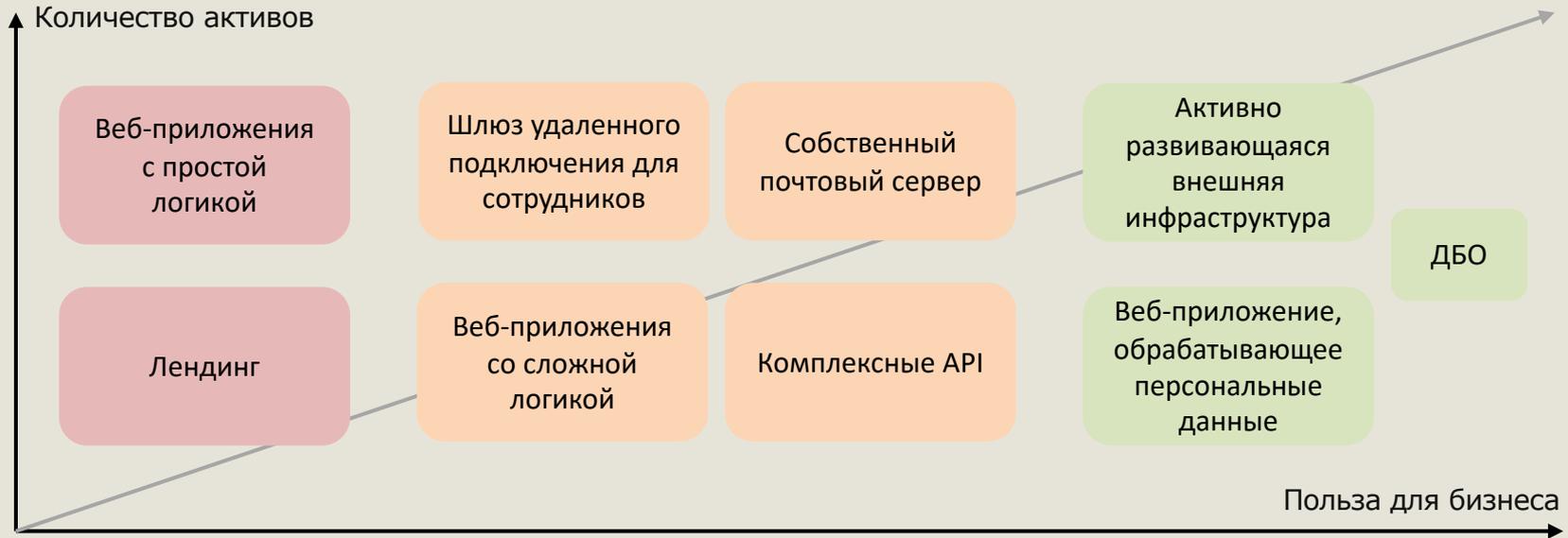
EASM и CPT (Continuous Penetration Testing): в чем разница?



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

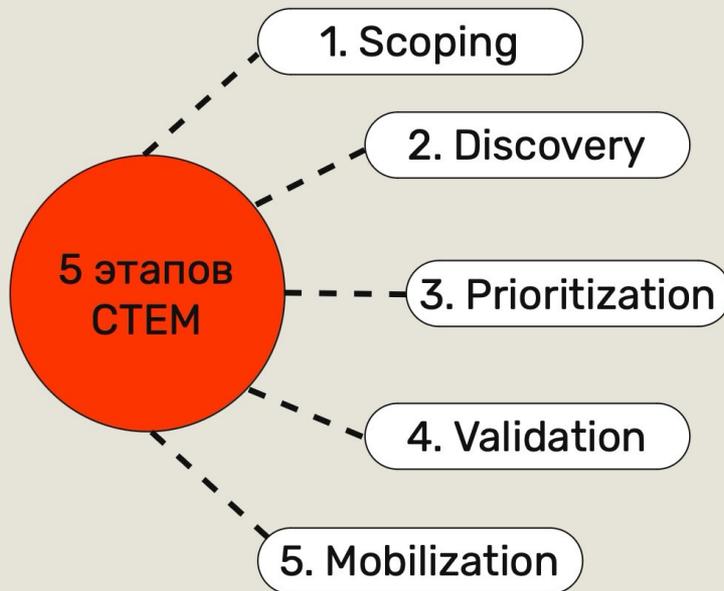
03

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.

STEM (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

SINGLETON
На страже безопасности

Название компании
06.07.2023

Язык Профиль

Уязвимости

Критичный уровень → 999 +999	Высокий уровень → 999 -999	Средний уровень → 999 -999	Низкий уровень → 999 +999
---------------------------------	-------------------------------	-------------------------------	------------------------------

Данные за последнюю неделю

Сканирования в процессе 999 →	Новые уязвимости 999 →	Исправленные уязвимости 999 →	Всего активов 999 →
----------------------------------	---------------------------	----------------------------------	------------------------

Активы

Все узлы 9 999 +999	Домены 999 +999	Поддомены 9 500 +999	Открытые порты 9 500 +999	На согласовании 9 500 →
---------------------------	-----------------------	----------------------------	---------------------------------	----------------------------

Новые уязвимости

Название	Адрес	Дата	Статус
Название	https://singleton-security.ru	05.07.2023	Высокий →
Название	https://singleton-security.ru	05.07.2023	Средний →
Название	https://singleton-security.ru	05.07.2023	Критичный →



или заполните форму



SINGLETON
SECURITY