



Проактивная защита внешнего периметра: подходы и актуальные решения



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

h   @esetal



Singleton Security – это **провайдер решений** в сфере кибербезопасности. Оказываем услуги **по оценке защищенности компаний**

Что мы предлагаем?

Услуги по анализу и оценке защищенности компаний, тесты на проникновение, внедрение процессов безопасной разработки.

Решение Singleton EASM - **External attack surface management**- Непрерывный мониторинг уязвимостей и угроз ИТ-инфраструктуры

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

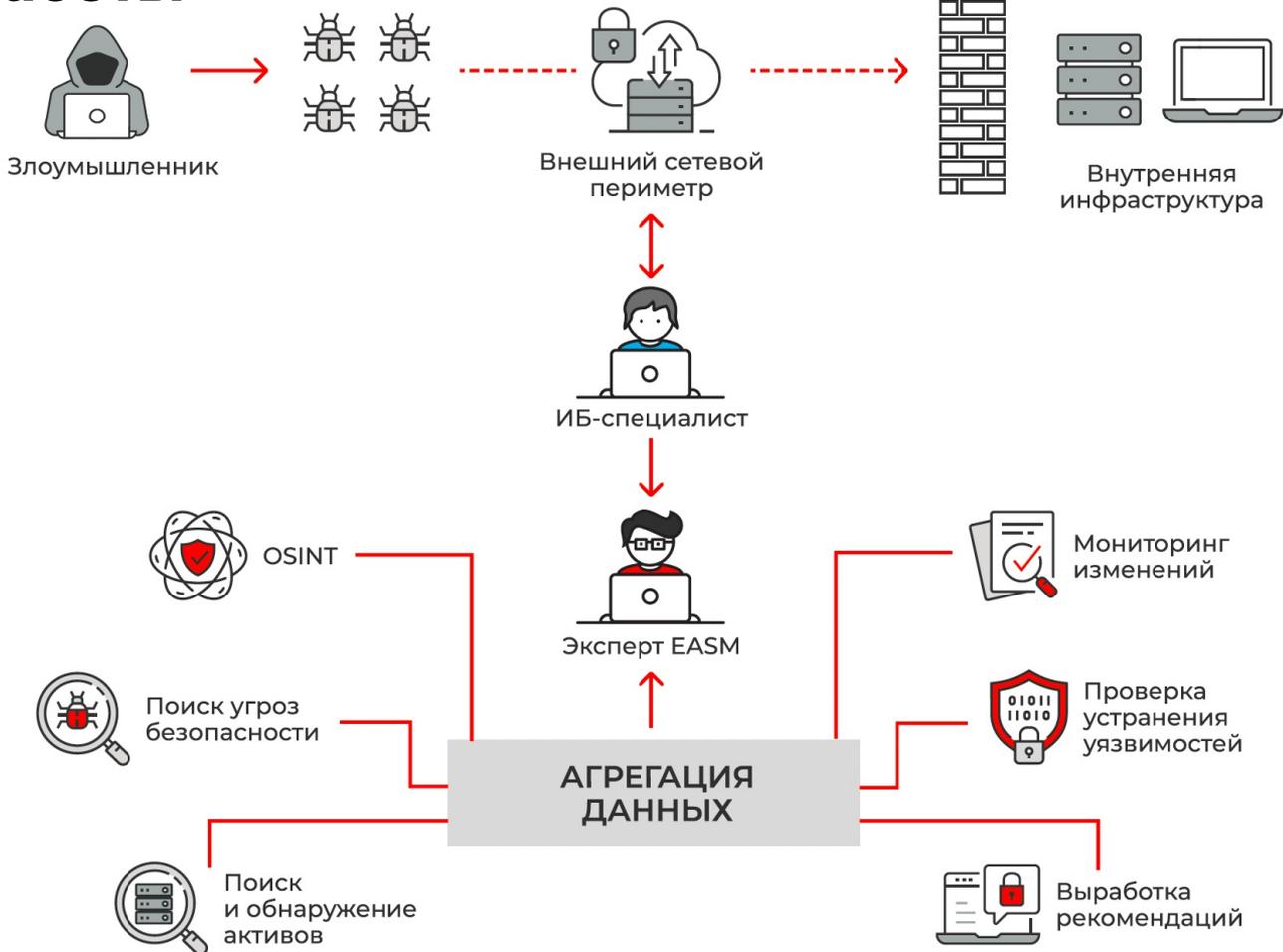
- **~100%** компаний имеют уязвимости уровня **Высокий** на своем внешнем периметре
- **~80%** цифровых активов изменяются в течение года
- в среднем компании не знают о **~30%** имеющихся у них цифровых активов
- **5.5** месяцев — среднее время жизни уязвимости на внешнем периметре
- менее **50%** зафиксированных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



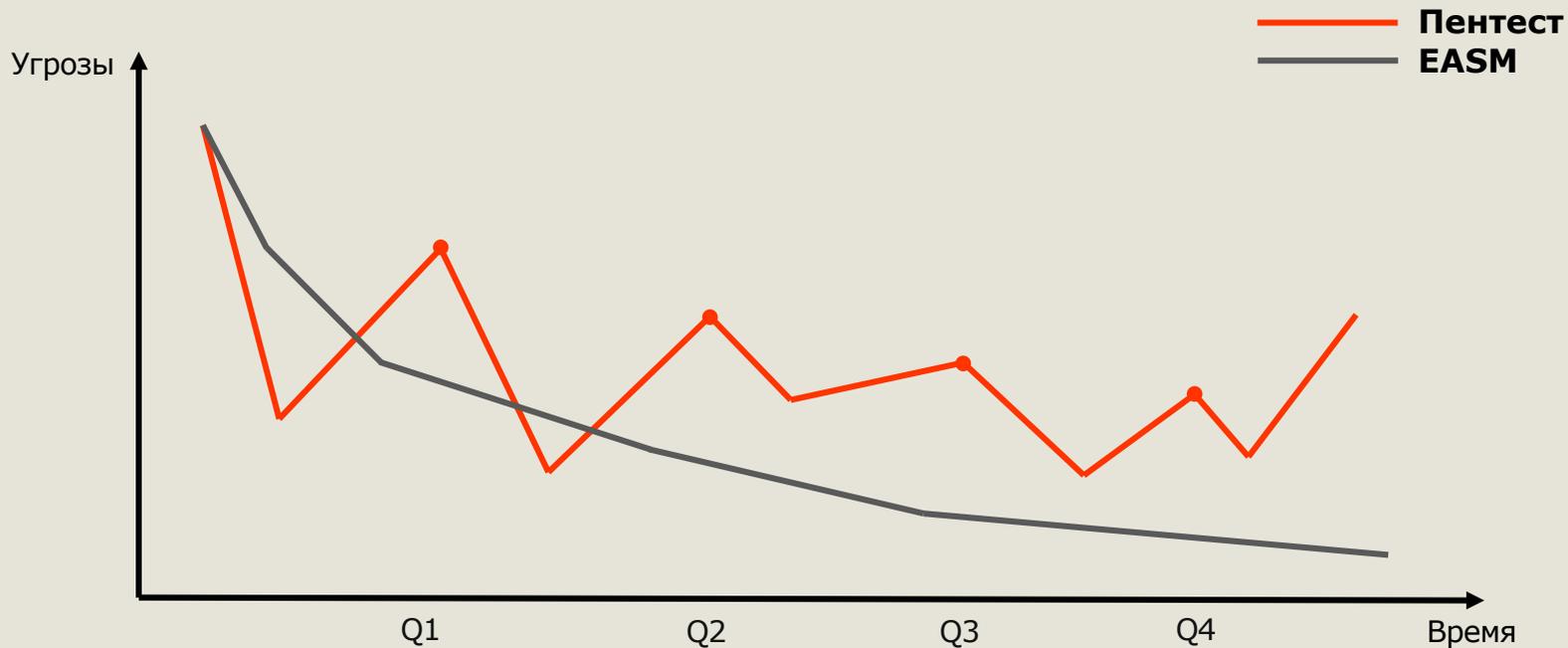
EASM

External attack surface management

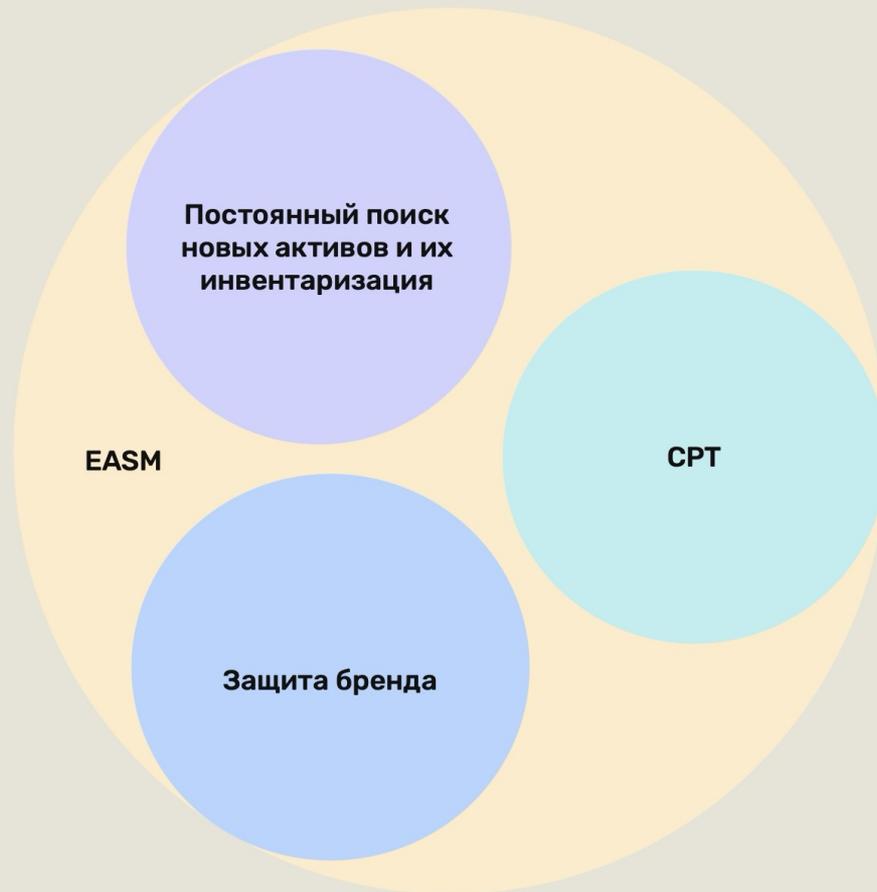
Схема работы



EASM или Pentest?



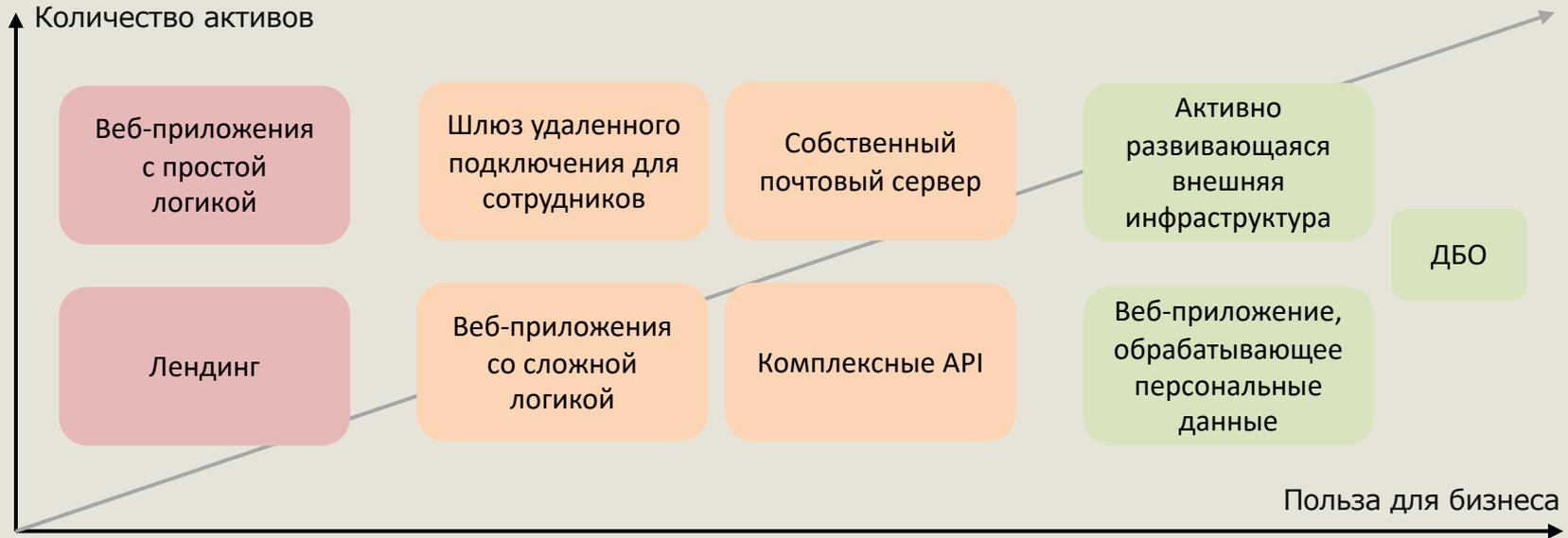
EASM и CPT (Continuous Penetration Testing): в чем разница?



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

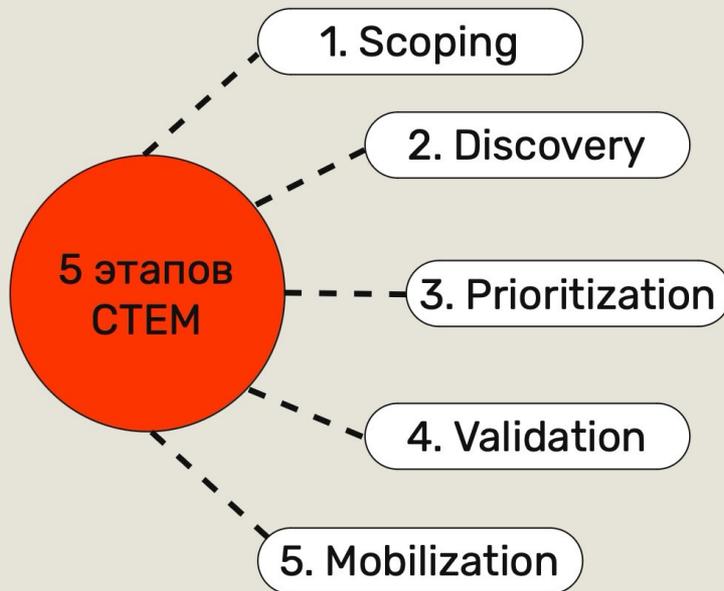
03

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

04

Поможем построить процессы ИБ

Book a Demo



Свяжитесь с нами

The screenshot shows the Singleton security dashboard. At the top, it displays the company name and date. The main section is titled 'Уязвимости' (Vulnerabilities) and shows four cards representing different severity levels: Critical (999 +999), High (999 -999), Medium (999 -999), and Low (999 +999). Below this is a section for 'Данные за последнюю неделю' (Data for the last week) with four cards: Scanning in progress (999), New vulnerabilities (999), Fixed vulnerabilities (999), and Total assets (999). The 'Активы' (Assets) section shows five cards: All nodes (9 999 +999), Domains (999 +999), Subdomains (9 500 +999), Open ports (9 500 +999), and On agreement (9 500). The 'Новые уязвимости' (New vulnerabilities) section contains a table with columns for Name, Address, Date, and Status.

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