Алексей Гришин
Руководитель программы BugBounty

mail.ru group

# Опыт применения программы Bug Bounty для управления уязвимостями

DevSecOps #3

23.09.2021


# Что такое Bug Bounty?

Пишите свои варианты ответа в чат конференции

# Bug Bounty программа

Программа, предлагаемая компанией, с помощью которой независимые исследователи информационной безопасности могут получить **признание** и **вознаграждение** за нахождение ошибок, которые касаются уязвимостей в продуктах или утечек данных компании. Программа позволяет обнаружить и **устранить ошибки в программном обеспечении и процессах компании**, прежде чем широкая общественность узнает о них.

# Программа Bug Bounty Mail.Ru Group

about 1 day
Average time to first response

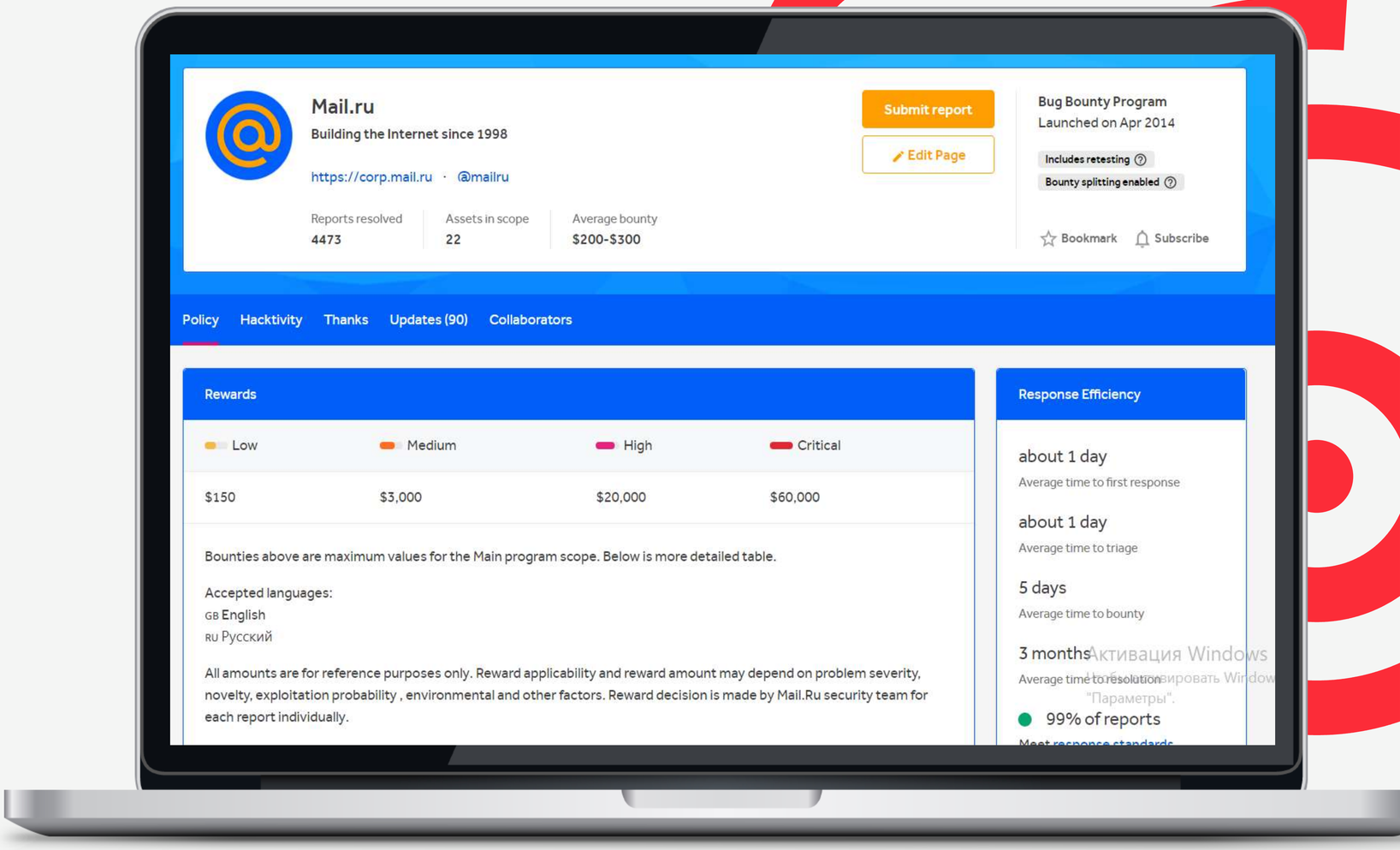
about 1 day
Average time to triage

5 days
Average time to bounty

3 months
Average time to resolution

99% of reports
Meet response standards

Данные: https://hackerone.com/mailru, 2021



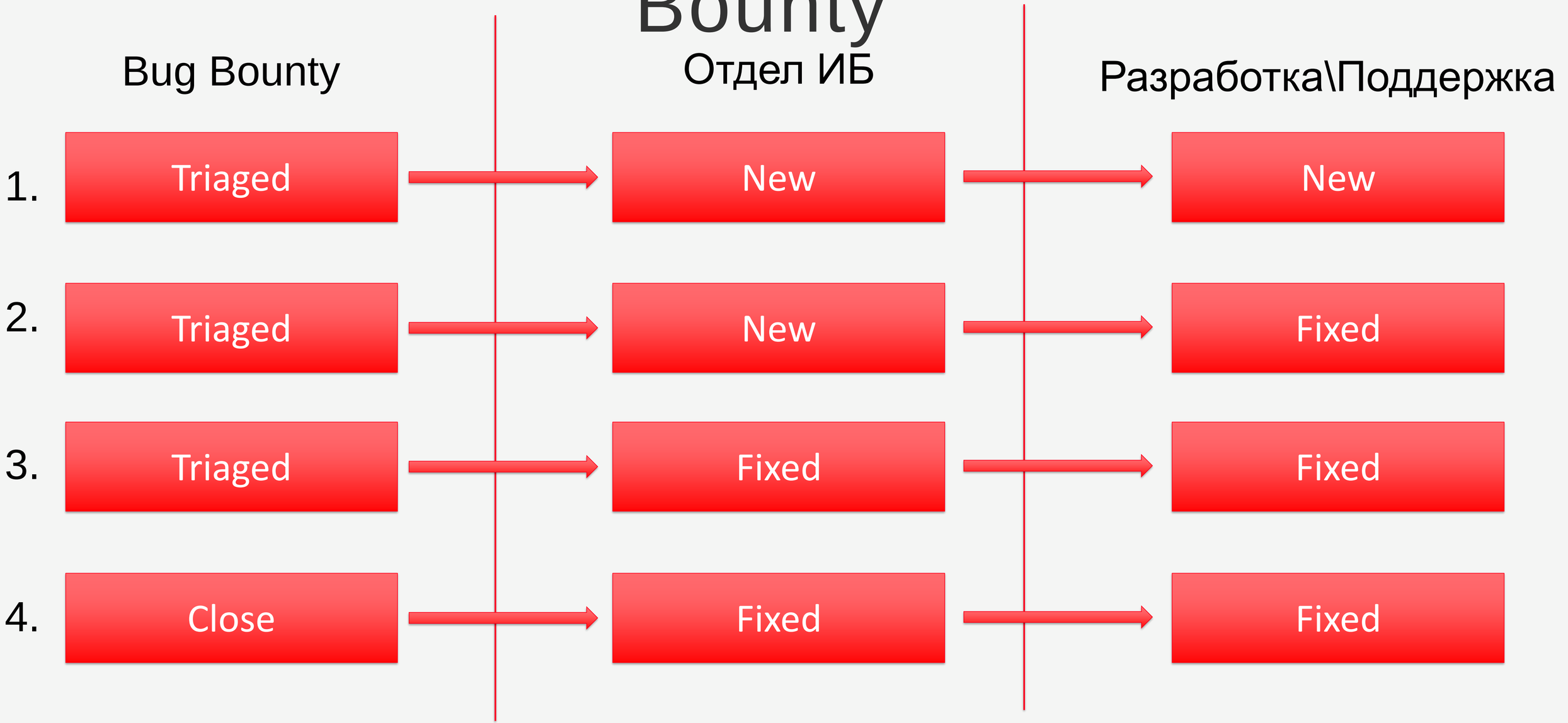
# Мифы о Bug Bounty

| Распространенное мнение | Реальность |
| --- | --- |
| С помощью Bug Bounty выкупаем баги с «черного» рынка | • Уязвимости в Bug Bounty сильно отличаются от тех, что продаются на «черном» рынке |
| Взятка исследователю, защищающая от репутационных рисков и шантажа | • Нет никаких гарантий. Не все исследователи этичны |
| Альтернатива аудитам и процессам тестирования | • Сложности отпугивают исследователей, остается много белых пятен |
| Самодостаточный процесс информационной безопасности | • Работает только в связке с другими процессами ИБ |
| Можно быть уверенным в высоком уровне защищенности, если у тебя высокие выплаты вознаграждений | • Размер выплат напрямую не влияет на уровень защищенности |
| Позволяет снижать затраты на ИБ | • Требует больших финансовых вложений и высокого уровня ИБ специалистов |

# Что такое Bug Bounty на самом деле…

- Bug Bounty это обратная связь от сообществ исследователей информационной безопасности со всего мира для процессов ИБ существующих в компании.
- Повышение практических навыков системных администраторов, сетевых инженеров, разработчиков и сотрудников службы информационной безопасности.
- Получение сведений о некоторых векторах атаки на организацию, не выявляемых другими способами или инструментами (яркий пример – 0day).
- Возможное повышение уровня безопасности через увеличение стоимости уязвимости и снижение репутационных рисков.

# Процесс обработки отчета Bug Bounty



# Готовность к Bug Bounty

## Технологическая готовность:

- Есть платформа приема уязвимостей;
- Продукт удовлетворяет базовым требованиям и рекомендациям ИБ;
- Есть процессы работы с уязвимостей или готовы их строить;
- Есть понимание области и цели исследования.

## Готовность команды:

- Есть компетентные сотрудники, готовые вести процесс (аутсорсинг);
- Сотрудники умеют честно признавать промахи и не оперативные действия;
- Есть бюджет на Bug Bounty.


Данные: https://otvet.mail.ru/question/180357348, 2016 год


# Что будет после запуска программы Bug Bounty?

Пишите свои варианты ответа в чат конференции

# Вместо итогов:

## Ожидание

Станем более защищенными

Закроем важные уязвимости

Расширим компетенции в ИБ

Оптимизируем затраты на пентесты и сканы

## Реальность

Увидите белые пятна в ИБ

Закроем 10 мелких уязвимостей и большую, если повезет

Все так!

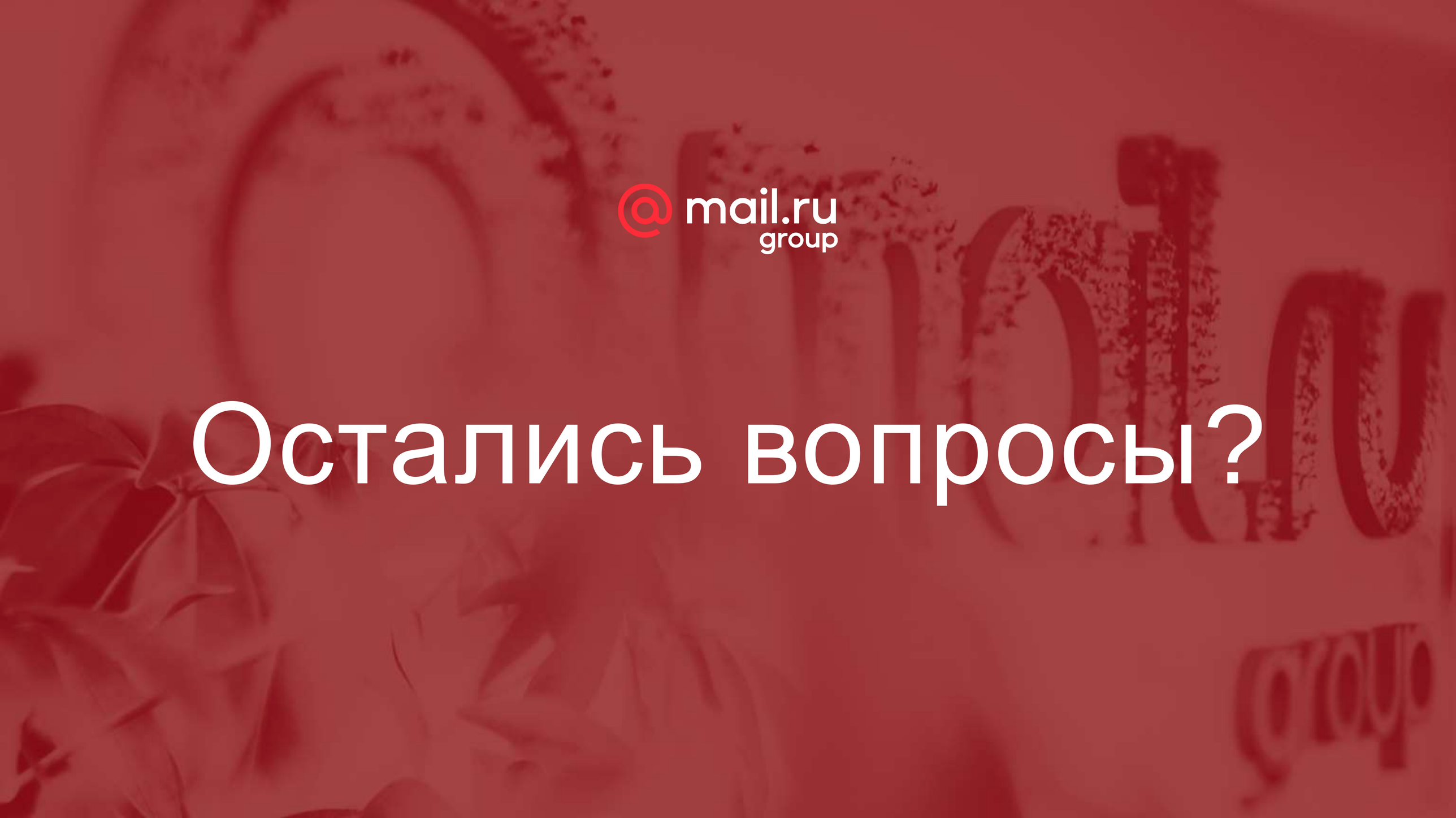
Пентесты и сканы все еще нужны

# Гришин Алексей

Руководитель программы Bug Bounty Mail.Ru Group

+7 999 835 12 20
Aleks.grishin@corp.mail.ru


mail.ru
group




# Остались вопросы?