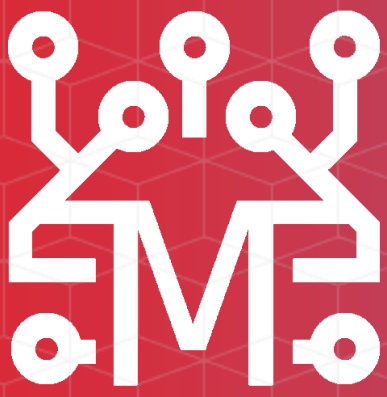


# METASCAN

**Простое управление безопасностью**

# Оглавление



По данным Фонда развития интернет-инициатив (ФРИИ), Microsoft и Group-IB в 2016 году 95% компаний столкнулись с внешними киберугрозами.
50% из них потеряли деньги в результате атак.

В наше время, любой сайт в интернете находится под угрозой взлома. С тех пор, как появились первые киберпреступники, прогресс шагнул далеко вперед. В наши дни, большинство взломов совершаются автоматически. Вредоносные программы используют известные уязвимости и ошибки в конфигурации для получения доступа к серверам.

---

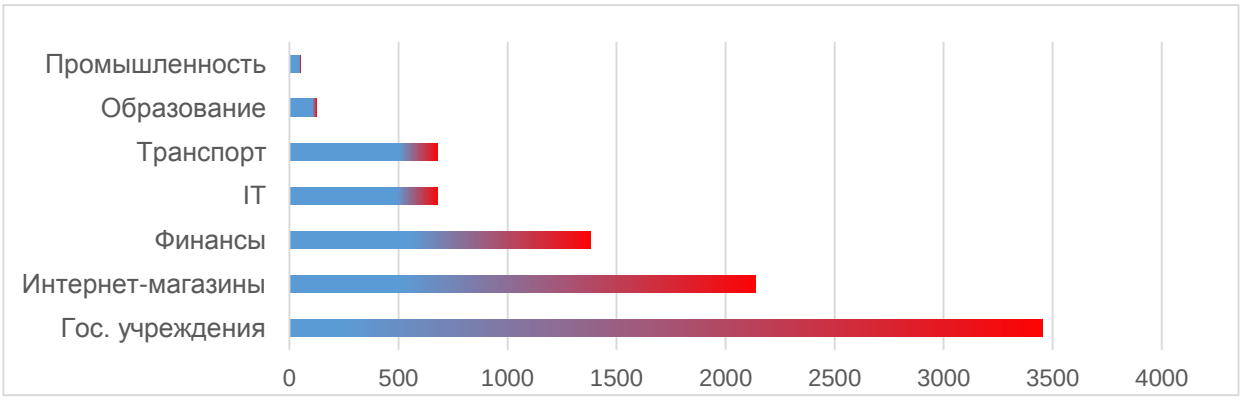
*Потери от одной успешной атаки, в среднем:*
*11 миллионов рублей для крупной компании*
*1.6 миллиона рублей для малого и среднего бизнеса*

---

Зараженные сайты используются для проведения DDoS атак, рассылки спама и с целью получения выкупа у владельцев. Если ваш сайт использует злоумышленник, то поисковые системы исключат его из выдачи, перестанут показывать на нем рекламу. Если ваш сайт помогает вам продавать, то его простой напрямую отнимает деньги у вашего бизнеса.

Чтобы защитить бизнес, нужно понимать, как злоумышленник может проникнуть в вашу систему.
Мы сделали METASCAN – сервис который проверяет можно ли взломать ваш сайт и сообщает об этом.

Среднее количество атак в день в зависимости от типа компании.



# Как работает METASCAN

METASCAN решает комплекс задач по обеспечению веб-безопасности для больших и маленьких инфраструктур.

## Обнаружение

- Внешняя инвентаризация (portcontrol).
  Администраторы часто забывают или неправильно конфигурируют межсетевые экраны. Из-за этого порты приложений, предназначенных для внутреннего пользования, становятся общедоступны. METASCAN постоянно отслеживает состояние портов защищаемой системы и уведомляет в случае добавления новых\исчезновения старых сетевых портов.

- Обнаружение уязвимостей в прикладном ПО.
  Одной из главных причин взломов является устаревшее ПО или неустановленные патчи. METASCAN определяет используемые приложения и платформы и использует 8 различных баз уязвимостей, чтобы сопоставить возможные атаки и приложения. В результате, вы всегда будете уведомлены, если какая-то из компонент вашей системы станет уязвимой для взлома.

- Обнаружение уязвимостей в веб-приложениях.
  METASCAN обнаруживает уязвимости типа SQL-Injection, XSS, CSRF, Sensitive Data Exposure и другие **OWASP top 10** ошибки совершаемые разработчиками веб-приложений. Для каждой найденной проблемы, мы даем инструкцию по устранению.

- Обнаружение слабых и стандартных паролей.
  Большинство современных ботнетов, например, Mirai, построены на основе устройств взломанных перебором паролей. Такие заражения трудно отследить, так как злоумышленник действует от имени легитимного пользователя. В METASCAN мы используем парольные базы, генерируемые специально для ваших сервисов.

- Обнаружение уязвимостей в сетевом оборудовании.
  Находим уязвимости в Cisco, Juniper, Check Point, Arbor, Huawei, Nortel, Alcatel, беспроводных VOIP-устройствах и телекоммуникационном оборудовании.

## Уведомление

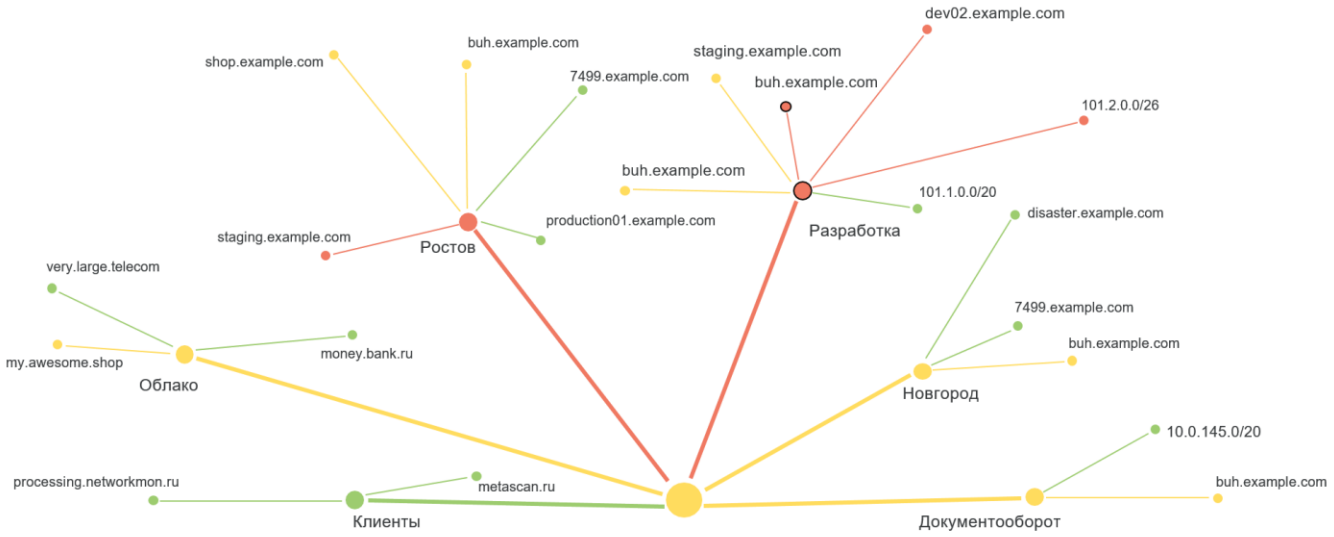
METASCAN умеет уведомлять вас с помощью:

- Почты
- CMC
- Telegram
- Syslog

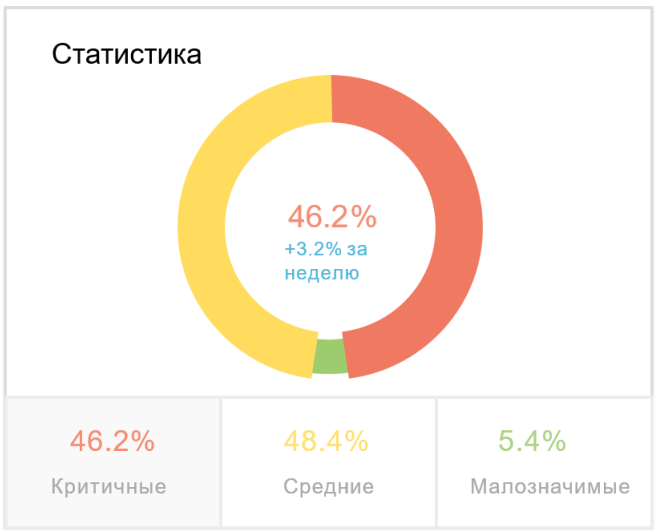
Вы всегда будете в курсе изменений в вашей системе!

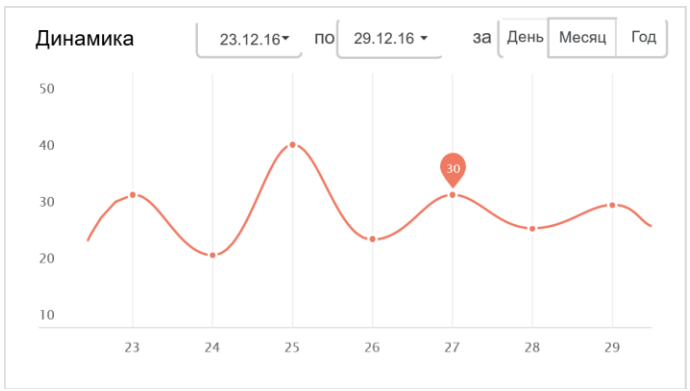
# Для руководителей

METASCAN сделан для того, чтобы дать вам глобальное видение веб-безопасности компании.
С помощью веб-интерфейса вы увидите уязвимые места инфраструктуры без необходимости вникать в проблемы каждого хоста




METASCAN позволяет вам разделить инфраструктуру вашей компании на группы, для каждой из которых можно установить уровень критичности и назначить ответственного. В зависимости от важности этой группы для бизнеса и уровня критичности уязвимостей мы автоматически сгенерируем план устранения уязвимостей. План ориентирован на максимально эффективное снижение рисков от внешних кибер-угроз.




В интерфейсе отображается эффективность процесса управления уязвимостями для каждой из групп. Зная сколько уязвимостей, когда и кем было устранено, вы сможете оценить работу отдела ИБ и разработчиков. А генерируемая отчетность позволит вам красиво донести суть работы отдела ИБ до руководства.

Мы того, чтобы вам было удобно пользоваться METASCAN мы предоставляем:

- Уведомления по телефону 24/7.
- Техническую поддержка на русском и английском языках.
- Инструкции по исправлению проблем.
- Адекватную стоимость сервиса.
- Автоматическое построение карты угроз для организации.
- Возможность увидеть ваш сайт и компанию так, как видят их злоумышленники и хакеры.

По вопросам  связанным с проведением пилотных проектов и тестированием пишите на **support@metascan.ru**

В документе используются данные из следующих отчётов:
https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Web-Applications-Attacks-rus.pdf,
https://info.whitehatsec.com/rs/675-YBI-674/images/WH-2016-Stats-Report-FINAL.pdf
https://www.imperva.com/docs/HII_Web_Application_Attack_Report_Ed6.pdf
https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q3-2016-state-of-the-internet-security-report.pdf