F6

Attack Surface Management

White Paper

Сканирование методами атакующих: возможности ASM TRY

Оглавление

Введение

По данным **F6 доминирующими векторами атак в 2026 году** станут эксплуатация уязвимостей и атаки через цепочки поставок. Одновременно сокращается время между публикацией **PoC (Proof of Concept — готового сценария эксплуатации)** и попытками атак на системы, для которых еще не были установлены обновления (патчи) безопасности. После появления готового сценария атаки злоумышленникам больше не требуется самостоятельно разрабатывать инструменты эксплуатации, вследствие чего поиск уязвимых сервисов и попытки компрометации начинаются практически сразу.

По данным Центра кибербезопасности F6

Использование уязвимостей на публично доступных активах стало одним из основных способов компрометации организаций и составляет **19%** от общего числа инцидентов. При этом **32%** критических атак относятся к человекоуправляемым сценариям, способным обходить штатные средства защиты.

Итог

В результате модель работы с внешним периметром меняется. Помимо поиска и фиксации активов компаниям необходимо понимать, какие из них могут быть использованы в реальной атаке.

Почему рынку потребовалось активное сканирование

ASM помогает перевести состояние внешнего периметра в понятные метрики, тогда как ASM TRY проверяет, какие из выявленных рисков действительно могут быть использованы.

Бизнес инвестирует в информационную безопасность, однако топ-менеджменту зачастую сложно оценить реальный эффект этих вложений. F6 ASM помогает перевести состояние внешнего цифрового периметра (всех цифровых ресурсов компании, доступных из интернета) в измеримые данные, показывая, какие активы находятся под контролем, где формируются риски и как меняется общий уровень защищенности.

Аудит внешней поверхности атаки производится по восьми категориям киберустойчивости:

- **Уязвимости:** CVE, открытые логин-формы, ошибки конфигурации.
- **Сетевая безопасность:** открытые порты, публичные базы данных, небезопасные сетевые заголовки.
- **Почтовая безопасность:** настройки DMARC, DKIM и SPF. DNS и домены: DNSSEC, DNS SOA и корректность доменных записей.
- **Упоминания в дарквебе:** обсуждения доменов и активов компании на теневых площадках.
- **Утечки данных:** корпоративные учетные данные сотрудников, попавшие в открытый доступ или сторонние сервисы.
- **Вредоносное ПО:** признаки вредоносной активности, связанной с активами компании.
- **SSL/TLS-сертификаты:** просроченные, самоподписанные или истекающие сертификаты.

Однако по мере развития угроз и усложнения внешних инфраструктур рынок сформировал новый запрос. **Компаниям стало важно не только видеть поверхность атаки, но и понимать, насколько она действительно устойчива к действиям злоумышленников.**

Такой запрос также связан с появлением множества систем, которые генерируют большое количество алертов, но не всегда помогают оценить их реальную критичность. **В результате нагрузка на SOC и ИБ-команды растет, время уходит на разбор уведомлений, а важные уязвимости пропускаются.**

ASM формирует оценку защищенности внешнего периметра по шкале от 0 до 10 баллов, где:

8 – 10 баллов

Зеленая зона, существенные риски не выявлены;

5 – 7,9 баллов

Средний уровень риска, присутствуют проблемы, требующие контроля и устранения;

0 – 4,9 баллов

Высокий уровень риска, внешний периметр содержит критичные проблемы и потенциальные точки входа для атаки.

Как работает ASM TRY

Активное сканирование отвечает на запросы рынка, помогая перейти от предположений к проверенным фактам. Решение позволяет понять, может ли уязвимость быть использована в реальной атаке, имитируя поведение атакующих в контролируемом режиме.

ASM TRY включает четыре ключевых типа проверок:

Брутфорс

Фаззинг

Сканирование портов

Эксплойт-тестирование

Ниже рассмотрим, какие задачи решает каждый из них и в каких ситуациях помогает выявлять реальные риски.

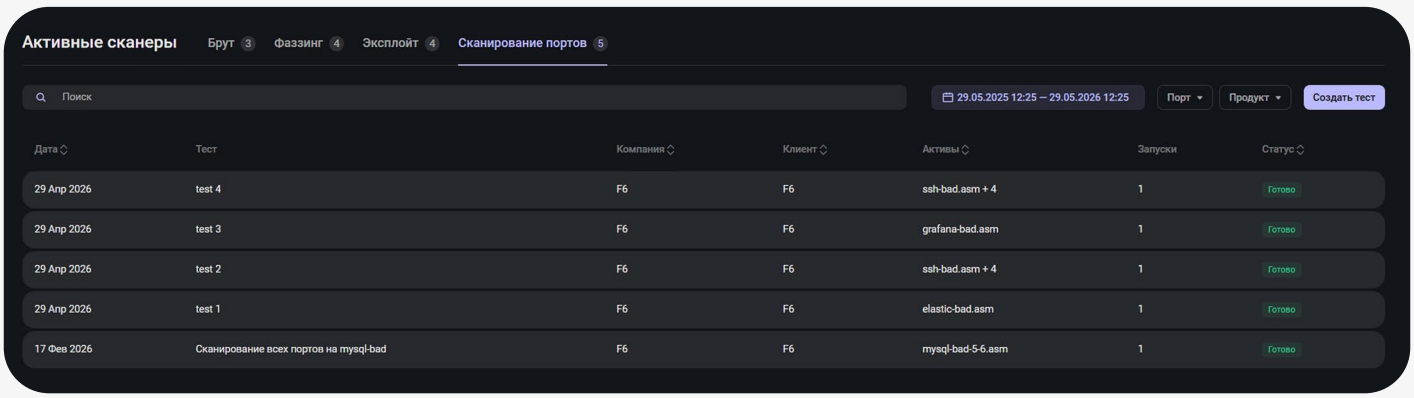


Рис.1 Скриншот интерфейса ASM TRY, возможности решения - 4 этапа проверки

Фаззинг

Фаззинг позволяет выявлять скрытые директории, нестандартные пути, ошибки обработки запросов и потенциально уязвимые элементы веб-приложений и API.

Во время проверки ASM TRY автоматически перебирает большое количество путей и вариантов запросов, анализируя ответы сервисов. **Система способна проверить до 1,2 млн путей за 15–50 минут, в зависимости от параметров проверки и особенностей инфраструктуры.** Это помогает быстро выявлять скрытые сервисы, забытые интерфейсы и неучтенные элементы внешнего контура.

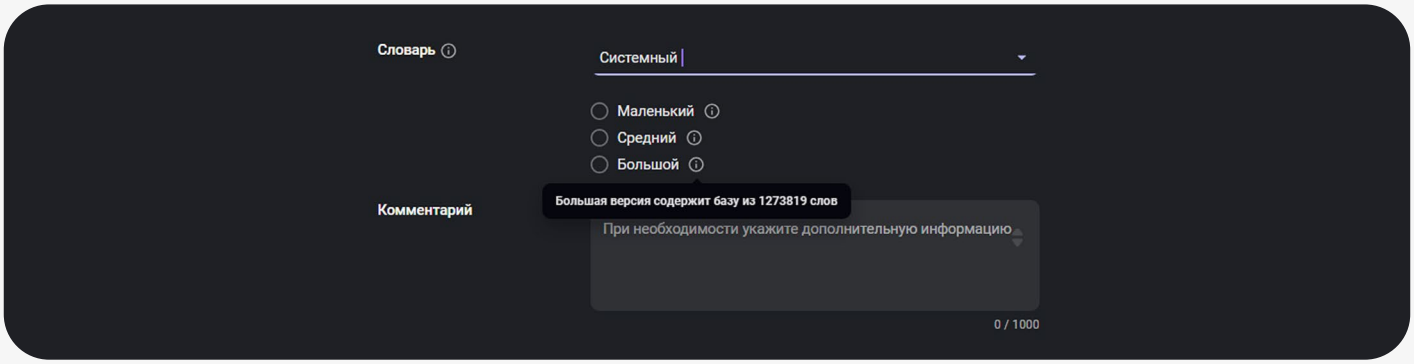


Рис.2 Скриншот интерфейса ASM TRY, возможность выбора словаря в фаззинге

Фаззинг помогает:

Выявлять скрытые директории и эндпоинты

Находить забытые веб-интерфейсы

Выявлять потенциальные точки компрометации

В решении поддерживается проверка неограниченного количества доменов и IP-адресов, а также возможность добавления собственных путей и сценариев проверки.

При этом проверки выполняются в контролируемом режиме и гибко настраиваются под инфраструктуру компании.

Брутфорс-проверки

Брутфорс-проверки позволяют оценить устойчивость внешних сервисов к подбору учетных данных и другим атакам на механизмы аутентификации.

Злоумышленники часто начинают атаку именно с попыток подключения к публичным сервисам через:

- **VPN;**
- **RDP;**
- **SSH;**
- **почтовые сервисы;**
- **административные протоколы.**

ASM TRY поддерживает проверку более 20 протоколов и позволяет использовать системные либо собственные словари логинов и паролей, адаптированные под специфику компании или отрасли. Самый большой системный словарь содержит 15 тыс логинов и паролей, из которых складывается 225 млн комбинаций.

Для снижения нагрузки на инфраструктуру и во избежание пересечения проверок с активностью клиентов в данной категории также предусмотрена гибкая настройка скорости, потоков и расписания проверок.

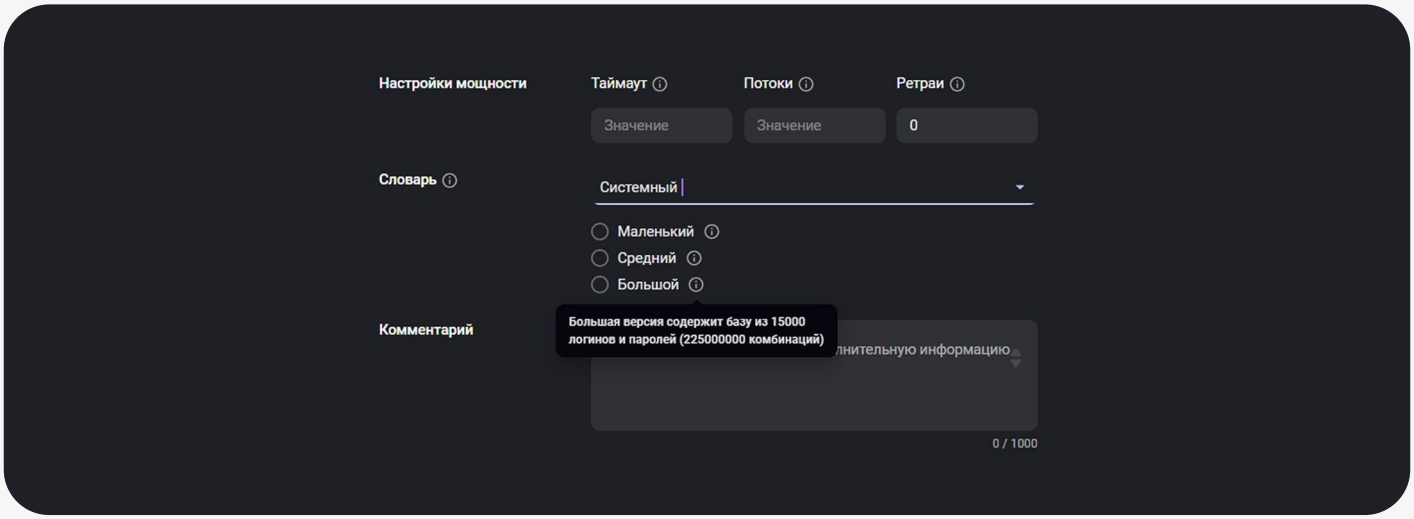


Рис 3. Скриншот интерфейса ASM TRY,возможность выбора словаря логинов и паролей в бруте

Сканирование портов

Сканирование портов позволяет определить, какие сетевые сервисы доступны из интернета и могут использоваться как потенциальные точки входа. **В среднем у системы уходит около 3–15 минут на полное сканирование одного IP-адреса и около одного-двух часов на проверку внешнего периметра всей организации, в зависимости от масштаба инфраструктуры и параметров проверки.**

Особенности данной проверки:

1. точечное и полное сканирование;
2. проверка отдельных IP-адресов и диапазонов;
3. автоматический контроль появления новых сервисов;
4. регулярный мониторинг изменений внешнего контура.

Высокая скорость сканирования позволяет оперативно анализировать крупные инфраструктуры и выявлять:

- открытые порты;
- забытые сервисы;
- временные подключения;
- изменения конфигурации внешнего периметра.

Это особенно важно для динамически изменяющихся инфраструктур, где новые точки входа могут появляться ежедневно.

Эксплойт-тестирование

Одной из ключевых особенностей решения стал первый евразийский патент на безопасную загрузку и запуск пользовательских эксплойтов.

Это позволяет компаниям проверять свои гипотезы и атаковать инфраструктуру собственным кодом в контролируемом режиме, адаптируя тестирование под реальные особенности внешнего периметра. В данной категории также доступна гибкая настройка графика проверок.

Такой подход особенно важен для крупных организаций с собственными командами, которым требуется самостоятельно проверять реальные сценарии атак.

Все вышеперечисленные категории являются настраиваемыми, постоянно обновляющимися, в результате чего сотруднику ИБ остается только проверить есть ли сработка для дальнейшего реагирования.

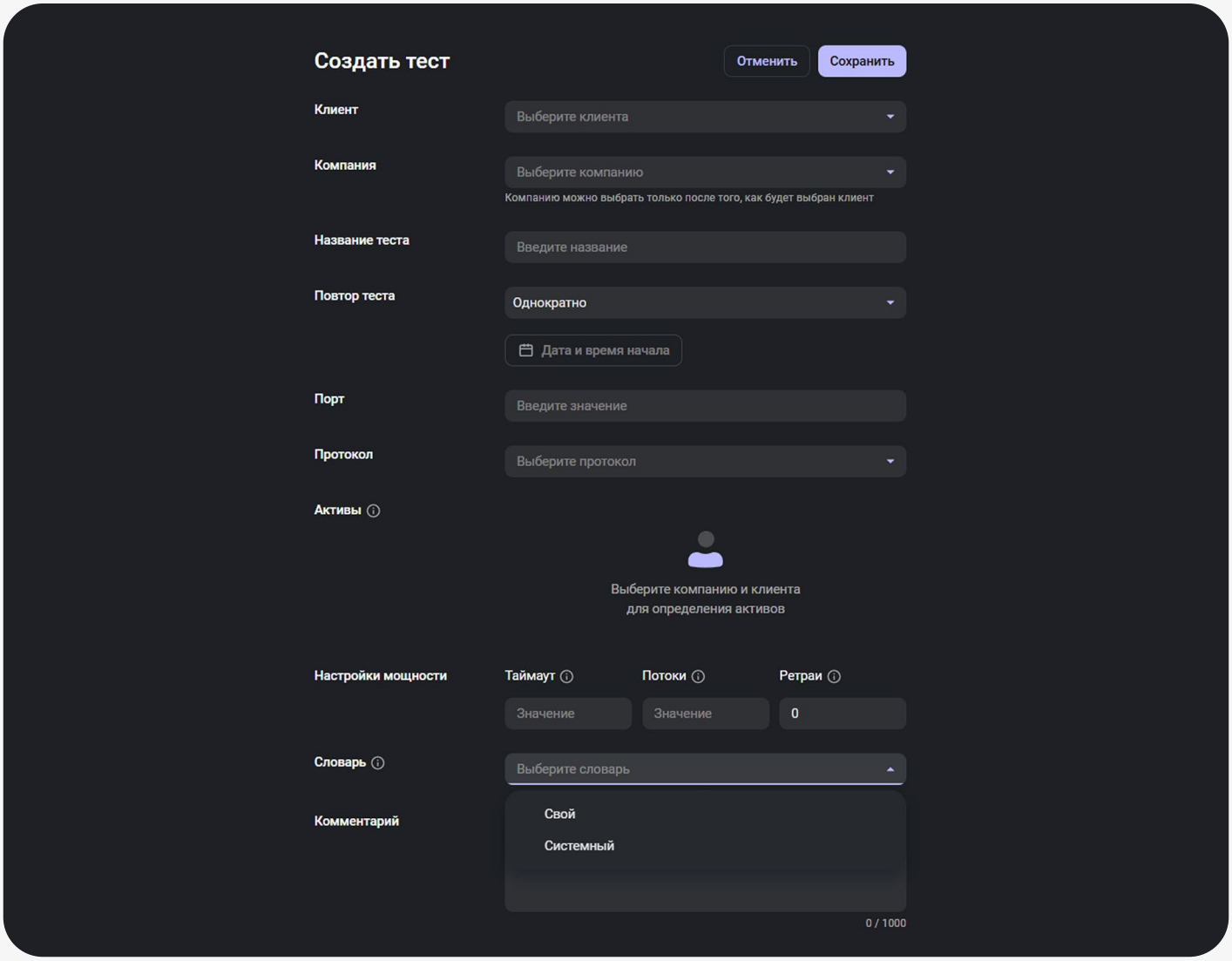


Рис 4. Скриншот интерфейса ASM TRY, возможность кастомизации настроек

Сценарии использования активного сканирования

Ниже рассмотрим реальные примеры проблем, обнаруженных в ходе проверок ASM TRY.

Кейс 1. Эскалация атаки через один внешний актив

В ходе мониторинга был обнаружен корпоративный ресурс, доступный из внешнего контура. После этого к активу были применены инструменты активного сканирования, включая фаззинг и проверку доступных путей.

В результате удалось выявить:

1. внутреннюю документацию компании;
2. открытую логин-форму корпоративного сервиса;
3. сведения об используемом ПО;
4. список внутренних пользователей и сотрудников.

Вывод. Этот сценарий показывает, как один внешне доступный ресурс может стать отправной точкой для дальнейшего раскрытия внутренней инфраструктуры компании и расширять возможности для развития атаки.

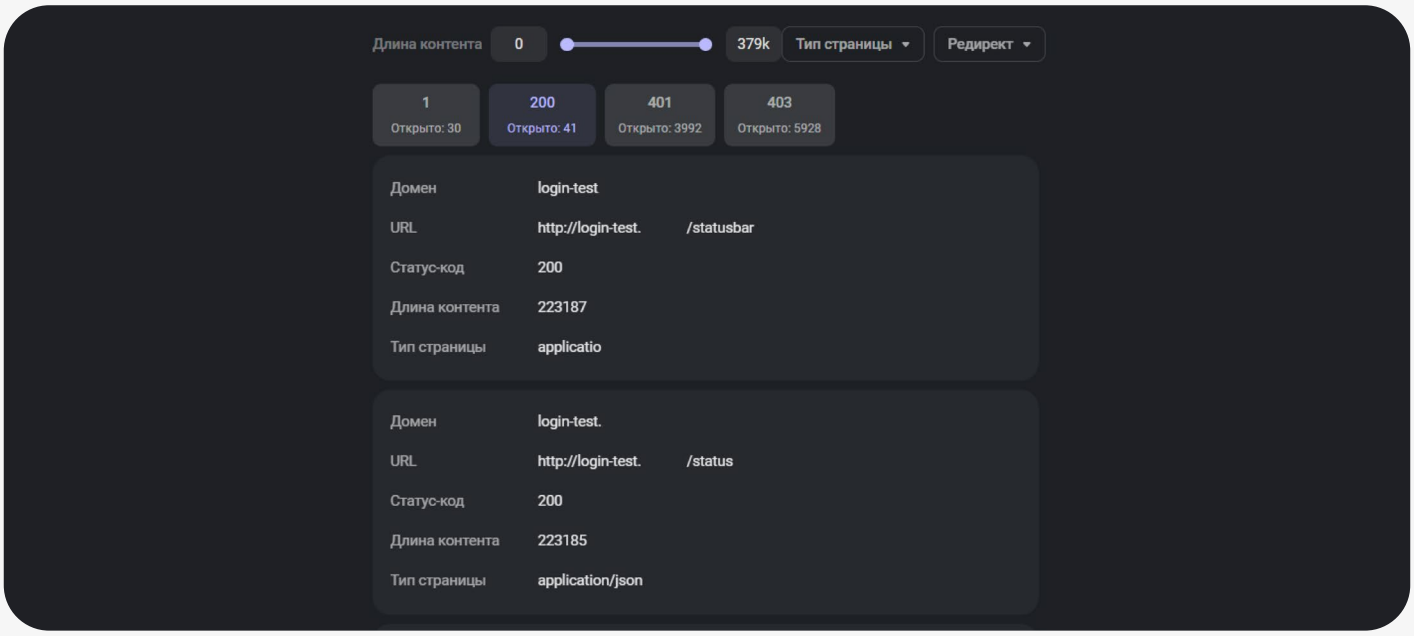


Рис. 5 Скриншот интерфейса ASM TRY, отображение найденных ошибок и детальная информация по ним

Кейс 2. Скрытый сервис доступнее, чем кажется

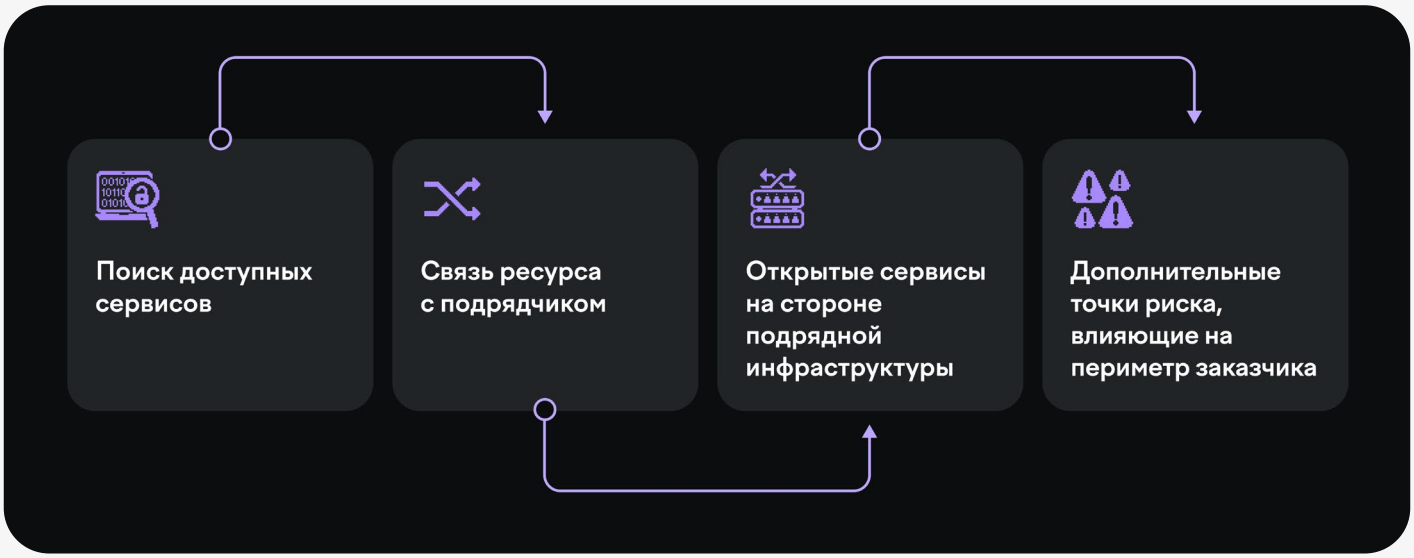
В рамках проверки ASM TRY были запущены несколько инструментов одновременно. За счет высокой производительности и тонкой настройки мощности сканирования удалось выявить открытые порты и сервисы, которые заказчик считал недоступными извне.

Проверка строилась по следующей цепочке: один инструмент находил доступные сервисы, другой уточнял их назначение, третий помогал проверить потенциальные уязвимости. Такой подход позволил последовательно раскрыть реальную картину доступности ресурса.

В результате были обнаружены:

1. связь ресурса с подрядчиком;
2. открытые сервисы на стороне подрядной инфраструктуры;
3. уязвимости в сервисах подрядчика;
4. дополнительные точки риска, влияющие на внешний периметр заказчика.

Вывод: даже если сервис считается скрытым или не связанным напрямую с компанией, активная проверка может показать обратное. Один внешний ресурс способен раскрыть зависимость от подрядчика, уязвимости на его стороне и риски, которые уже влияют на безопасность заказчика.



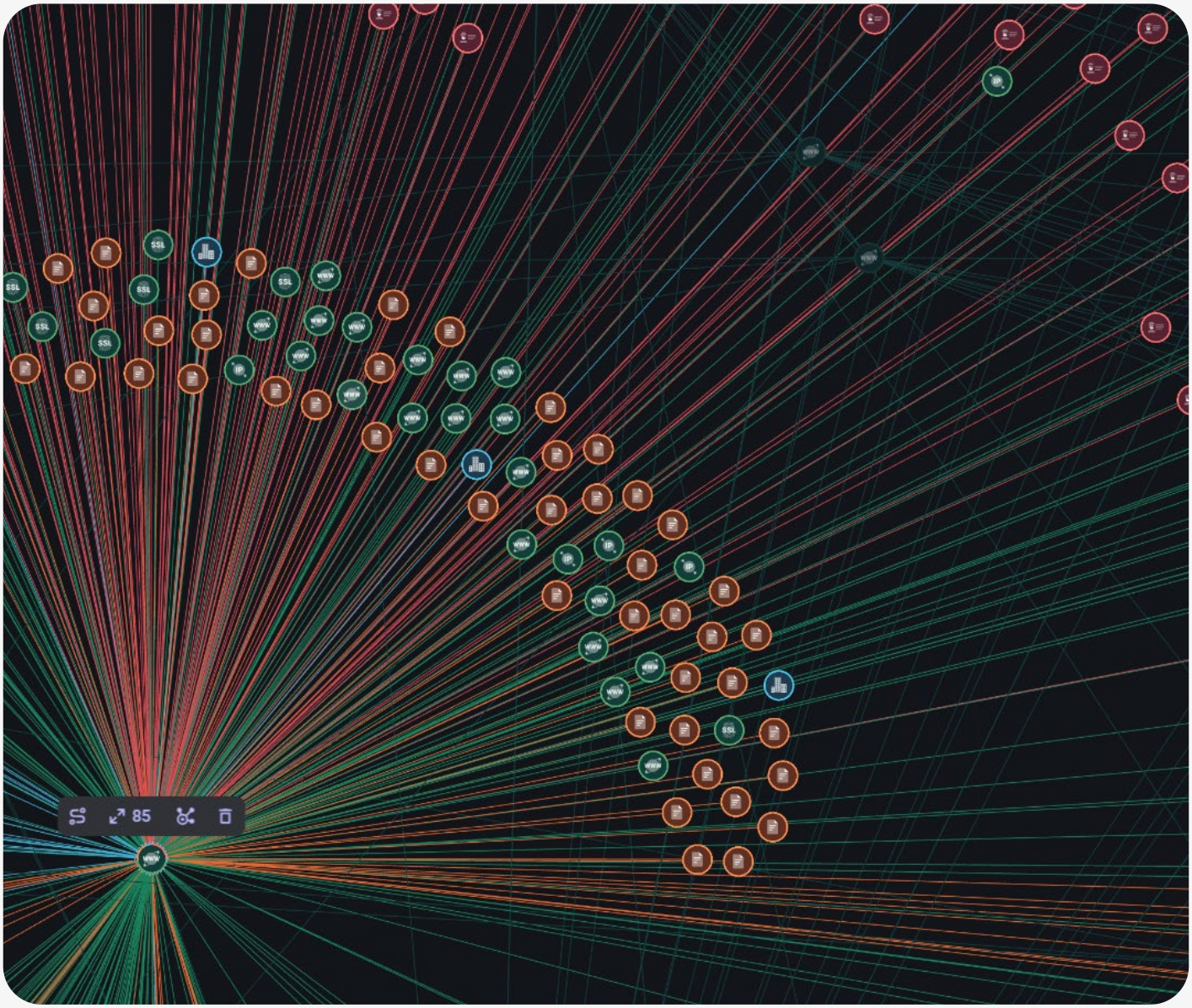


Рис.6 Скриншот интерфейса ASM TRY,отображение связей ресурса с другими активами

Кейс 3. Работа над ошибками

Выявленная ранее уязвимость передана на устранение провайдеру или внутренней команде. После завершения работ команда сообщает, что проблема закрыта, но клиенту важно убедиться в этом самостоятельно.

Вывод: ASM TRY позволяет быстро подтвердить, что уязвимость действительно исправлена и больше не может быть использована как точка входа.

ASM TRY позволяет проверить устранение ошибки в любое время по заранее настроенному расписанию или вручную. В ручном режиме повторная проверка может быть выполнена в течение 15 минут.

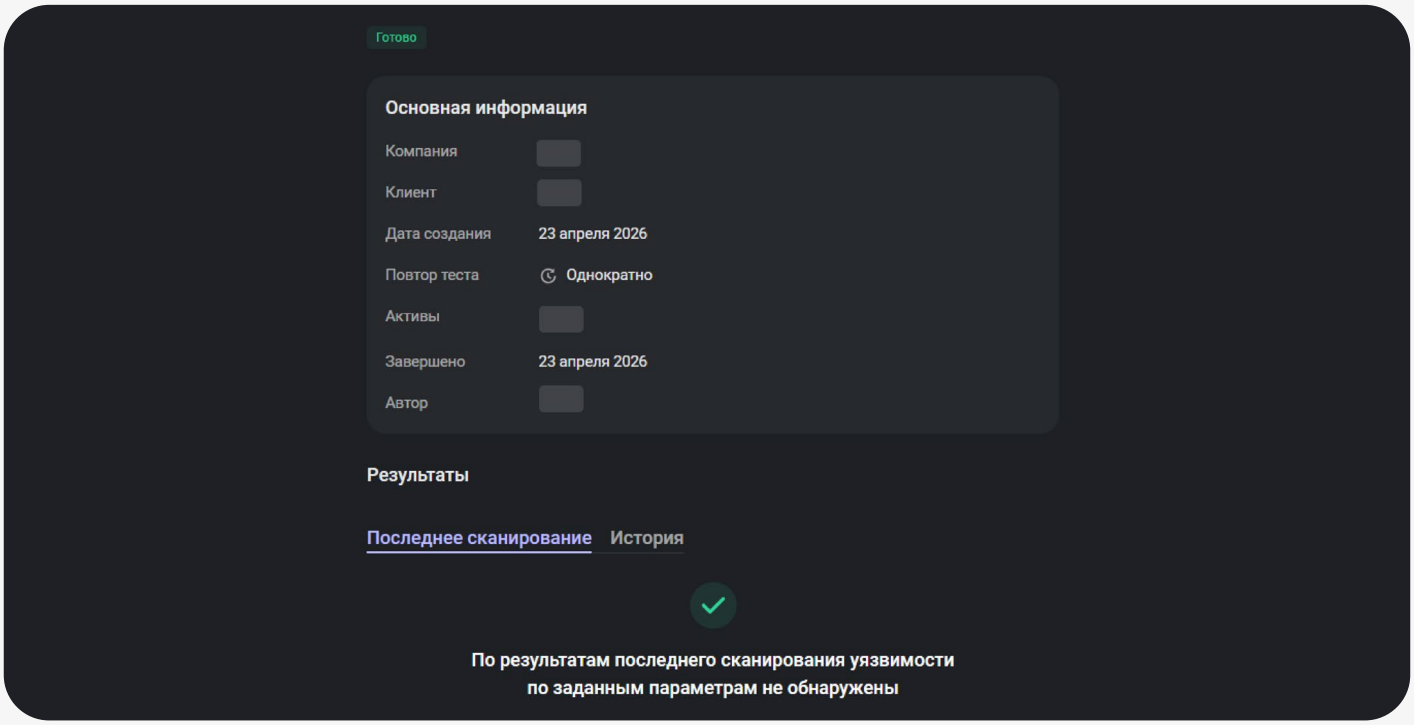


Рис. 7 Скриншот интерфейса ASM TRY, результаты проведенной проверки

Кейс 4. СЗИ в условиях реальной нагрузки

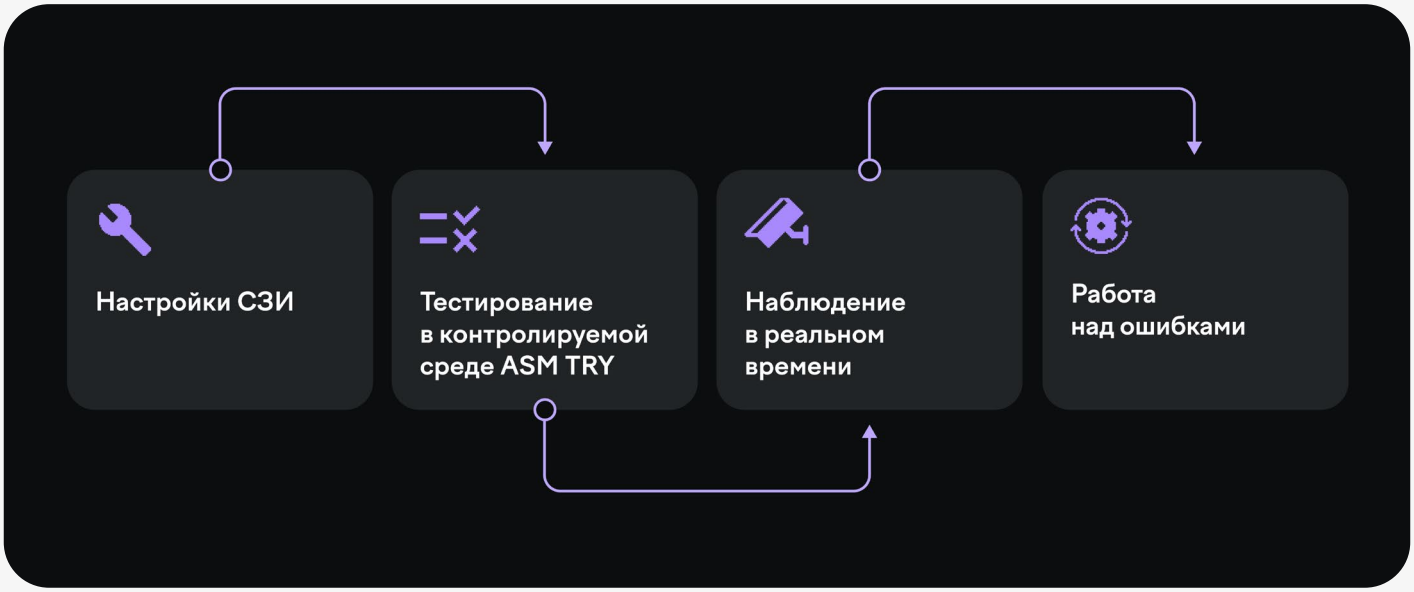
С помощью ASM TRY крупная государственная организация смогла проверить работу настроенных средств защиты информации в реальном времени и в управляемом режиме. Проверка была направлена на оценку текущих защитных решений, которые реагируют на активность, похожую на действия злоумышленника.

В рамках сценария проверялись:

- чувствительность СЗИ к DDoS-нагрузке;
- реакция IPS/IDS на попытки подключения;
- поведение NTA при сканировании и аномальной сетевой активности;
- корректность срабатываний при разных уровнях критичности событий.

В результате были выявлены критические недочеты в настройке СЗИ. Часть защитных механизмов реагировала чрезмерно жестко и отключала сервисы даже при срабатываниях с низкой критичностью.

Далее рассмотрим типовые сценарии и потенциальные риски, которые также могут быть выявлены с помощью ASM TRY.



Кейс 5. Забытый сервис удаленного доступа

После завершения проекта подрядчик оставил открытый RDP-сервис во внешнем контуре компании. Формально ресурс больше не использовался, поэтому не попадал в регулярный контроль ИБ-команды.

Во время сканирования ASM TRY:

1. обнаружил открытый порт;
2. определил доступный сервис;
3. провел брутфорс-проверку с использованием типовых корпоративных словарей.

Результат: система подтвердила возможность подбора стандартного пароля к используемому протоколу.

Такой сценарий показывает, как один забытый сервис может стать полноценной точкой входа для атаки.

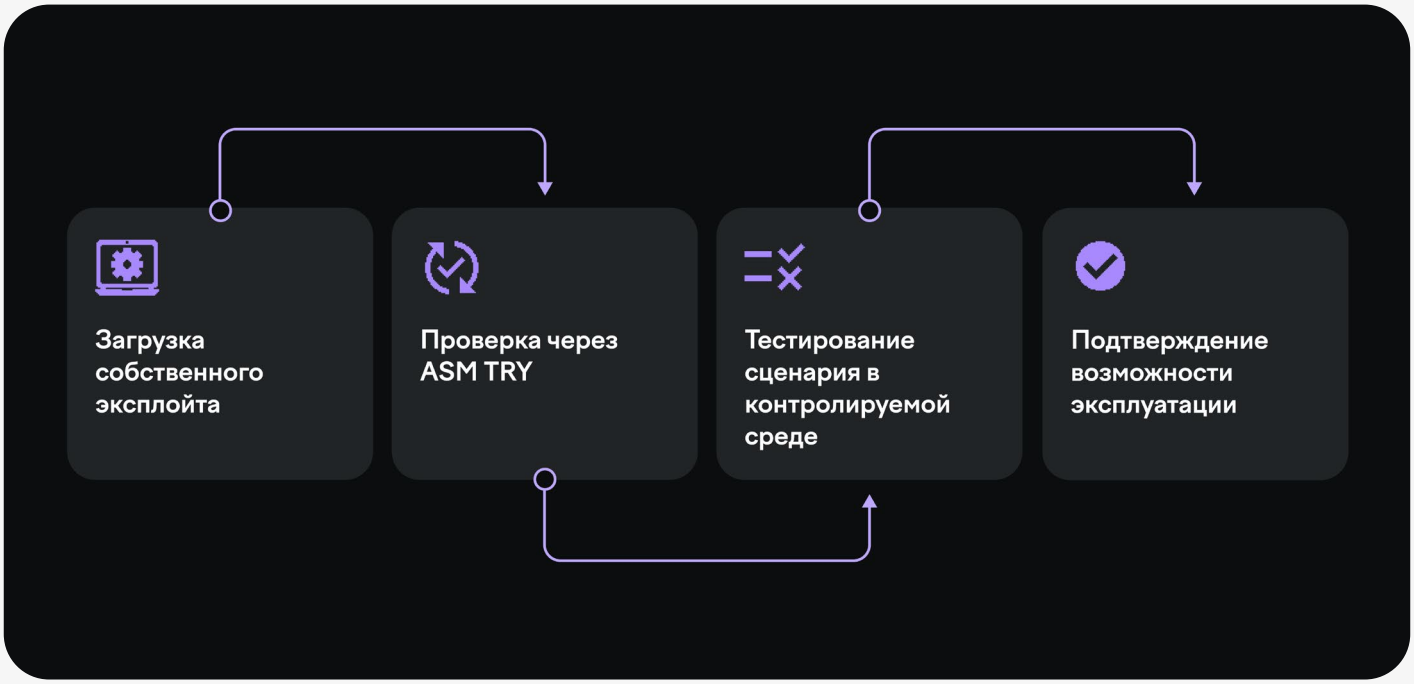
Кейс 6. Проверка собственной гипотезы атаки

У внутренней команды возникла гипотеза о возможности эксплуатации нестандартного сценария атаки на один из внешних сервисов компании.

Вместо обращения к внешним подрядчикам специалисты:

1. загрузили собственный эксплойт;
2. выполнили проверку через ASM TRY;
3. протестировали сценарий в контролируемой среде;
4. подтвердили возможность эксплуатации без риска для инфраструктуры.

Такой подход позволяет крупным организациям самостоятельно проверять собственные гипотезы и адаптировать сценарии тестирования под особенности инфраструктуры.



Отличие ASM TRY от VM, пентеста и BAS

Активное сканирование часто сравнивают со сканерами уязвимостей, пентестами или BAS-платформами. Однако ASM TRY занимает отдельную нишу между этими классами решений.

Отличие от VM (Vulnerability Management)

Системы Vulnerability Management ориентированы прежде всего на поиск известных уязвимостей **во внутренней инфраструктуре компании.** Как правило, они работают с заранее известными активами и помогают управлять процессом устранения проблем. Однако инфраструктура современной организации постоянно меняется: появляются новые сервисы, временные подключения, тестовые среды, дополнительные точки доступа и внешние ресурсы. VM-системы не всегда способны оперативно учитывать такие изменения, особенно если активы появляются вне централизованного процесса учета.

Кроме того, **ASM TRY позволяет подтверждать риск** не только по признакам наличия уязвимой версии ПО, но и через активную проверку и PoC.

ASM TRY фокусируется на внешнем периметре и проверяет:

Какие сервисы доступны из интернета

Какие точки входа реально видит атакующий

Можно ли использовать проблему на практике

Отличие от пентеста

Пентест представляет собой глубокое ручное исследование инфраструктуры, которое проводится **ограниченное количество раз.** Фактически ASM TRY закрывает задачу постоянной active validation между полноценными пентестами.

ASM TRY не заменяет пентест, а дополняет его:

Позволяет непрерывно контролировать внешний периметр

Автоматически отслеживает изменения инфраструктуры

Помогает регулярно проверять новые точки входа

Дает возможность быстро тестировать отдельные гипотезы и сценарии атак

Отличие от BAS

BAS-платформы (Breach & Attack Simulation) обычно используются для проверки эффективности внутренних средств защиты и сценариев реагирования внутри инфраструктуры.

ASM TRY работает с внешней поверхностью атаки и моделирует действия злоумышленника именно со стороны интернета:

При этом **ASM TRY не требует установки агентов для проведения базовых проверок** и позволяет быстро запускать тестирование внешнего контура.

Сканирование сервисов

Проверку аутентификации

Поиск скрытых ресурсов

Тестирование внешних точек входа

Эксплуатацию уязвимостей

Возможность	VM	Пентест	BAS	ASM TRY
Адаптация под динамические изменения внешней инфраструктуры	Нет	Нет	Нет	Да
Проверка возможности эксплуатации уязвимости	Нет	Да	Нет	Да
Запуск PoC-проверок	Нет	Да	Нет	Да
Регулярные автоматизированные проверки	Да	Нет	Да	Да
Проверка открытых портов и новых точек входа	Да	Да	Нет	Да
Проверка устойчивости логин-форм и внешней аутентификации	Нет	Да	Нет	Да
Фаззинг внешних сервисов и API	Нет	Да	Нет	Да
Собственные сценарии проверок	Нет	Да	Да	Да
Базовая проверка внешнего контура без установки агентов	Нет	Да	Нет	Да

Таким образом, ASM TRY занимает отдельную нишу между VM, пентестом и BAS.

VM-системы в первую очередь помогают управлять известными уязвимостями внутри инфраструктуры. Пентесты позволяют глубоко исследовать отдельные системы вручную. BAS-платформы проверяют эффективность внутренних средств защиты и сценариев реагирования.

ASM TRY использует реальные техники атакующих.

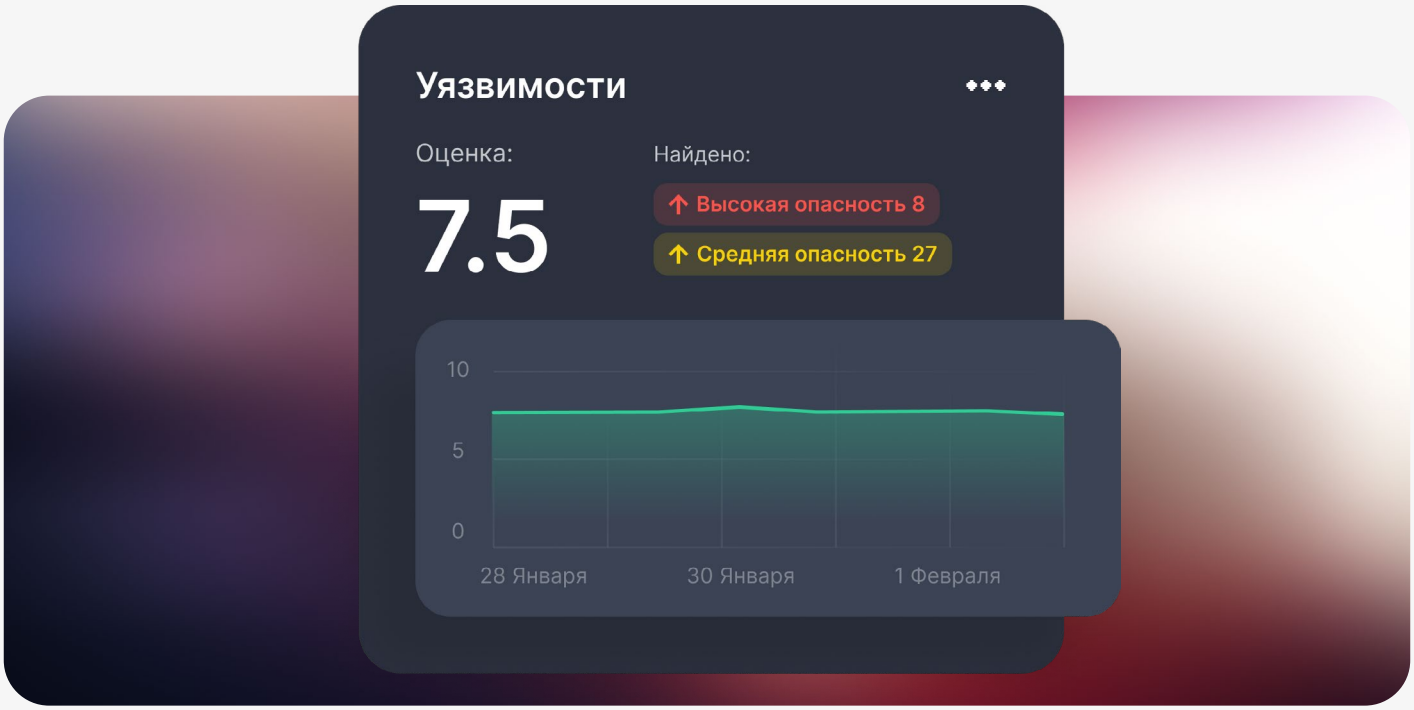
Регулярно проверяет внешний периметр с позиции злоумышленника, используя сценарии и техники, которые применяются в атаках.

Бизнес-эффект активного сканирования

Практическая ценность ASM TRY лучше всего раскрывается через простую логику: если у бизнеса есть внешний сервис, значит, его нужно проверять так, как это сделал бы атакующий:

- **У компании есть публичные формы входа, VPN, почтовые шлюзы или административные панели** → брутфорс-проверки помогут оценить устойчивость к подбору учетных данных.
- **Во внешнем контуре работают веб-приложения, API, тестовые среды или часто обновляемые сервисы** → фаззинг позволяет находить скрытые директории, нестандартные пути и ошибки обработки запросов.
- **Инфраструктура постоянно меняется** → сканирование портов помогает отслеживать новые сервисы, забытые точки доступа и изменения внешнего периметра.
- **Уязвимость уже обнаружена** → эксплойт-тестирование позволяет проверить, может ли она быть использована на практике.
- **У компании есть собственные гипотезы и экспертиза** → безопасный запуск пользовательских эксплойтов дает возможность проверить их собственным кодом в контролируемом режиме.

Именно так ASM TRY переводит работу с внешним периметром от предположений к проверенным фактам.



Заключение

Активное сканирование внешнего периметра — это новый, углубленный уровень контроля над поверхностью атаки. ASM помогает увидеть внешние активы и потенциальные точки входа, ASM TRY позволяет проверить, какие из них действительно могут быть использованы злоумышленниками на практике.

Проблемы, которые выявляет ASM TRY, не уникальны. Они повторяются в разных организациях и отраслях: слабая аутентификация, открытые порты, скрытые директории, устаревшие сервисы, неустраненные уязвимости и забытые внешние ресурсы. Разница только в том, насколько быстро компания успевает их обнаружить и проверить.

ASM TRY помогает:

1. подтверждать реальную эксплуатируемость уязвимостей;
2. проводить брутфорс-проверки внешних сервисов;
3. выполнять фаззинг веб-приложений и API;
4. контролировать открытые порты и новые точки входа;
5. запускать PoC-проверки и пользовательские эксплойты;
6. настраивать сценарии проверок под инфраструктуру компании;
7. снижать нагрузку на SOC за счет приоритизации реальных рисков.

Активное сканирование помогает отделить потенциальные риски от проблем, которые действительно могут привести к компрометации.

В результате компания получает подтвержденные, регулярно обновляемые результаты проверок, которые адаптируются под особенности бизнеса и показывают, какие проблемы действительно могут стать точкой входа для атаки с позиции злоумышленника.

F6

Технологии для борьбы с киберугрозами

info@f6.ru +7 495 984-33-64 f6.ru