Dr.WEB

Dr.Web FixIt!: новое слово в расследовании инцидентов информационной безопасности

Обнаружит следы проникновения в ИТ-инфраструктуру, выявит текущие и уже произошедшие атаки и устранит их последствия.

Сервис Dr.Web FixIt!

Dr.Web FixIt! — инструмент для детального анализа безопасности компьютеров и серверов под управлением Windows и устранения как выявленных заражений, так и потенциальных угроз. Он не требует установки и не вступает в конфликт с антивирусами.

Три фазы работы **Dr.Web FixIt!**:

1. Аудит системы: сбор данных на компьютере пользователя.

2. Анализ собранных данных и выработка механизмов для устранения последствий инцидента.

3. Лечение системы: устранение выявленных зараженных объектов, нарушений правил ИБ и возможных целевых атак в системе пользователя.

Dr.WEB

1. Аудит системы

Сервис генерирует диагностическую утилиту **FixIt!**, которая собирает данные, исследуя:

- установленные программы и обновления,
- запущенные и запускаемые процессы,
- подозрительные записи в реестре и их связи с другими объектами,
- установленные драйверы и расширения браузеров,
- модули, загруженные в процессы,
- системные журналы (они содержат информацию, что происходило на компьютере, а в ряде случаев — и о том, как на этот компьютер проник злоумышленник),
- сектора диска, в том числе скрытые буткитами (для этого используется уникальный модуль, позволяющий обходить все известные буткиты и считывать настоящие сектора диска).

Затем утилита формирует отчет, в котором объединяет все собранные данные для дальнейшего анализа.

2. Анализ собранных данных

Отчет, сформированный диагностической утилитой, загружается в веб-сервис **Dr.Web FixIt!**, и оператор проводит анализ собранных данных. Для этого в **Dr.Web FixIt!** используются фильтры и сравнение с предыдущими отчетами о состоянии системы, если диагностическая утилита уже запускалась ранее. В результате выявляются следы вредоносной активности, и оператор выбирает действия, которые необходимо применить к вредоносным объектам.

> Благодаря разработанным специалистами «Доктор Веб» фильтрам **Dr.Web FixIt!** можно сравнить с работой целой команды ИТ-специалистов, которые шаг за шагом собирают данные и анализируют вектор заражения, чтобы разработать механизмы лечения.

3. Лечение

На основе выбранных оператором действий, которые необходимо применить к вредоносным объектам, создается и запускается лечащая утилита **FixIt!** После завершения ее работы система исследуется снова — и если устранены не все последствия инцидента, то формируется и запускается новая лечащая утилита. Этот процесс повторяется столько раз, сколько нужно для полного устранения всех последствий инцидента.

> Каждая лечащая утилита **FixIt!** — это уникальная сборка под конкретную ситуацию. Она выполняет набор инструкций, подготовленный на основе отчета диагностической утилиты.

Нашей идеей было сделать сервис, в котором мы бы объединили все свои знания о заражениях ОС и алгоритмов их детектирования и лечения. **Dr.Web FixIt!** собирает огромное количество данных о системе пользователя — и в зависимости от задач оператор анализирует нужный ему срез данных. Благодаря этому есть возможность оперативно все вылечить в системе.

Главная ценность **Dr.Web FixIt!** — это уникальные фильтры, которые из тонны данных выявляют нужные срезы, заражения, проблемы и аномалии.

Константин Юдин
Руководитель проектов «Доктор Веб»

Dr.WEB

Лицензирование Dr.Web FixIt!

- Сервис лицензируется по числу задач.

> Задача — это выполнение трех фаз работы **Dr.Web FixIt!**: сбор данных, их анализ и дальнейшее лечение ОС на одном компьютере или сервере.

- Приобрести **Dr.Web FixIt!** можно пакетами по 1, 10, 20, 50 или 100 задач. Срок лицензии **Dr.Web FixIt!** — 1 год.
- Работа с задачами осуществляется через личный кабинет пользователя **Dr.Web FixIt!**, доступ к которому предоставляется после активации лицензии.
- Задача активна в течение 10 календарных дней с момента первого запуска, после чего автоматически закрывается без права повторного открытия.

Экспертное сопровождение

Специалисты компании «Доктор Веб» могут:

Проанализировать данные, полученные с помощью Dr.Web FixIt!.

Помочь устранить последствия заражения.

Определить потенциальные масштабы ущерба.

Предложить меры по минимизации потерь и предотвращению повторения атак.

Чтобы воспользоваться этой услугой, нужно приобрести сертификат на экспертное сопровождение задачи. Каждый сертификат дает право на получение экспертного сопровождения одной задачи. При этом срок действия сертификата не ограничен.

Кому, когда и чем поможет Dr.Web FixIt!?
Конкретные ситуации и пути их решения

Ситуация ?

Рабочая станция заражена вредоносным ПО.

Необходимо оперативно вылечить зараженную систему.

Решение ✓

Dr.Web FixIt! быстро и точно выявит следы вредоносного ПО с помощью диагностической утилиты, а затем лечащая утилита нейтрализует заражения и потенциальные угрозы.

Ситуация ?

Есть подозрение, что в корпоративной сети присутствует вредоносное ПО.

Нужен быстрый аудит безопасности сети.

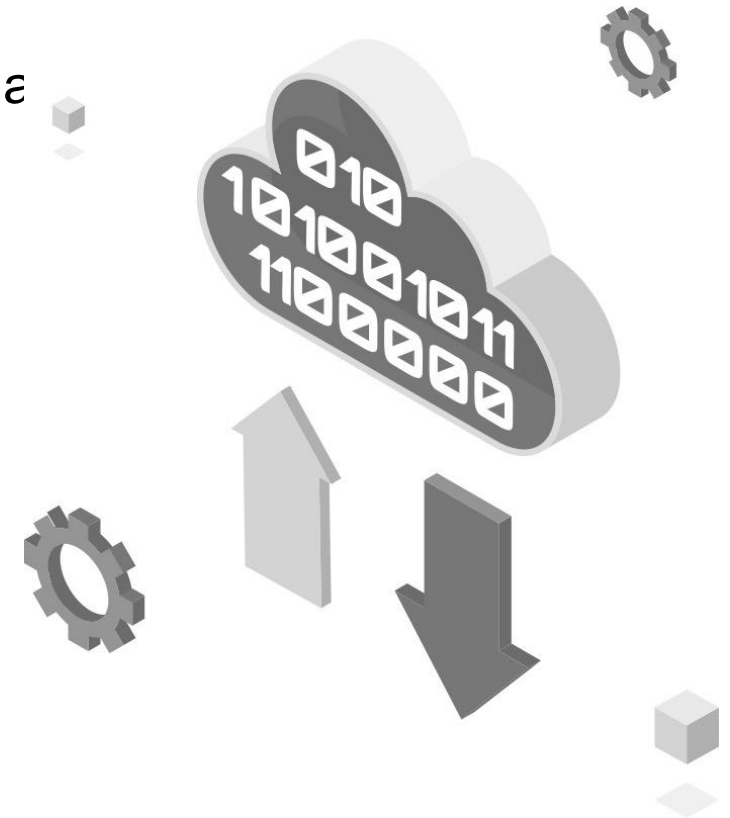
Решение ✓

Dr.Web FixIt! быстро проведет анализ системы на наличие следов скрытого проникновения, соберет данные с серверов и рабочих станций, покажет, на что необходимо обратить внимание в первую очередь, и поможет создать утилиту для устранения заражений и возможных угроз.

Ситуация ?

Служба информационной безопасности компании выявила ИБ-инцидент и устранила последствия, но его причина неясна

Необходимо провести глубокий анализ произошедшего, собрать историю и выявить причины инцидента.



Решение ✓

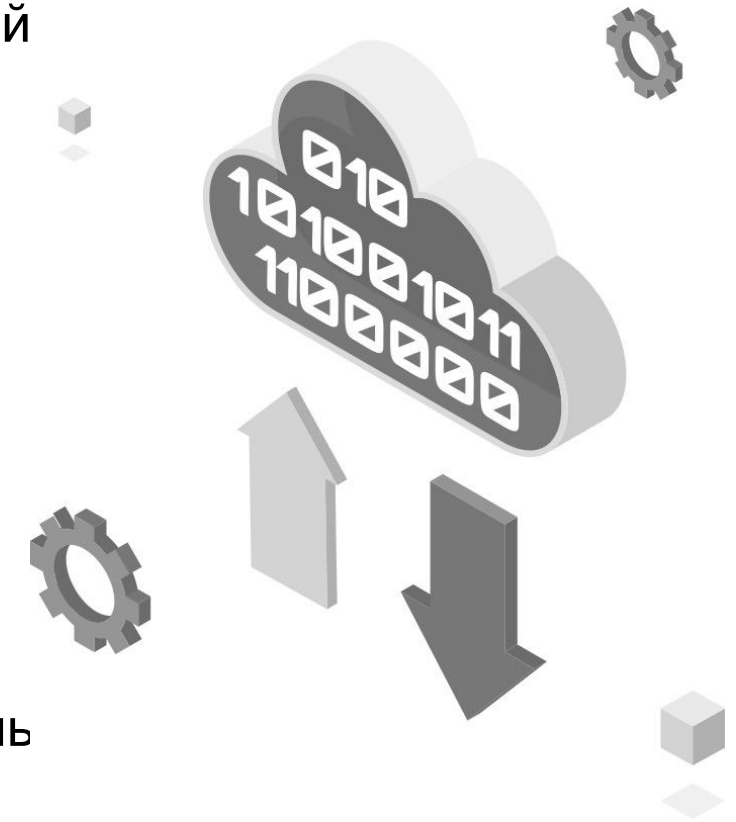
Dr.Web FixIt! поможет разобраться в логах, собрать данные о причинах произошедшего и провести ретроспективный анализ состояния защиты системы, проследить во времени ситуацию и поведение критических сервисов и программ. А также позволит сделать выгрузку подозрительных файлов для их последующего анализа в лаборатории или изучения с помощью **Dr.Web vxCube**.

Dr.WEB

Ситуация ?

Сотрудник компании жалуется на «странную» работу рабочей станции, но служба технической поддержки не может установить причины аномалии. Штатные средства диагностики и установленный антивирус не помогают.

Необходимо определить причины аномалии.



Решение ✓

Dr.Web FixIt! поможет проанализировать компьютер пользователя, найти конкретные нарушения в работе системы и устранить их. Даже если стоит другой антивирус.

Ситуация ?

В компании есть рабочие станции, безопасность которых критична для компании.

Необходима регулярная проверка определенных компьютеров корпоративной сети.

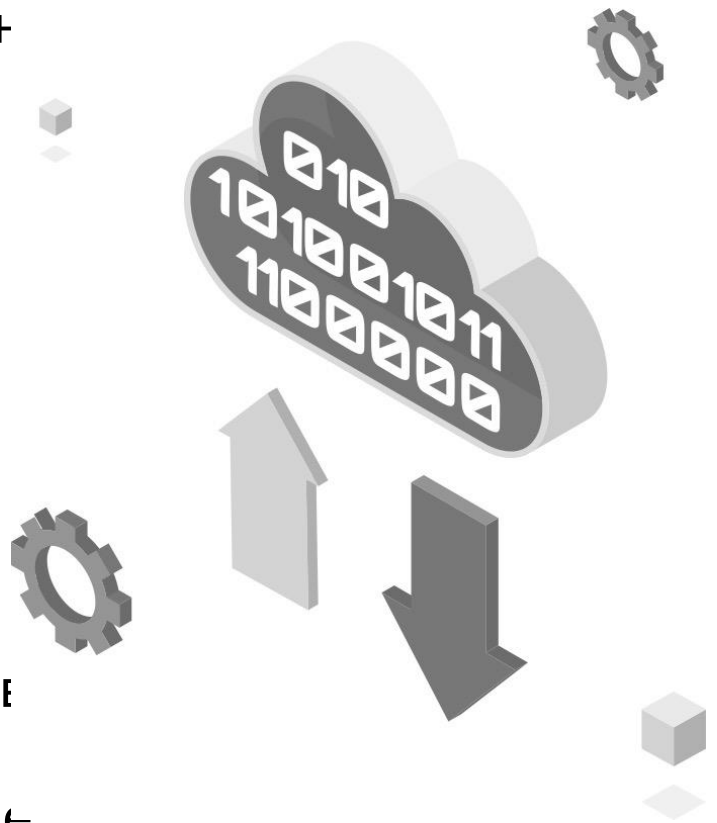
Решение ✓

Dr.Web FixIt! проверяет состояния выбранных рабочих станций в динамике и помогает выявлять скрытые APT-атаки (целевые продолжительные атаки повышенной сложности) на них, в том числе на регулярной основе.

Ситуация

Возможностей службы информационной безопасности компан
не хватает для полноценного расследования ИБ-инцидентов.

Нужно найти единый инструмент, быстрый и доступный, для полноценного лечения зараженных систем, предотвращения потенциальных угроз и установления причин произошедших инцидентов.



Решение

Dr.Web FixIt! проводит исследование любого инцидента ИБ, помогает установить его причины и нейтрализовать последст
не требуя для этого диагностики всей корпоративной сети, больших ресурсов и отдельного штата персонала — в отличие от дорогих и ресурсозатратных EDR-решений.

Ситуация ?

Сотрудники, работающие удаленно, используют свои компьютеры для рабочих целей.

Требуется проверить их ПК и убедиться, что они защищены от угроз заражения.

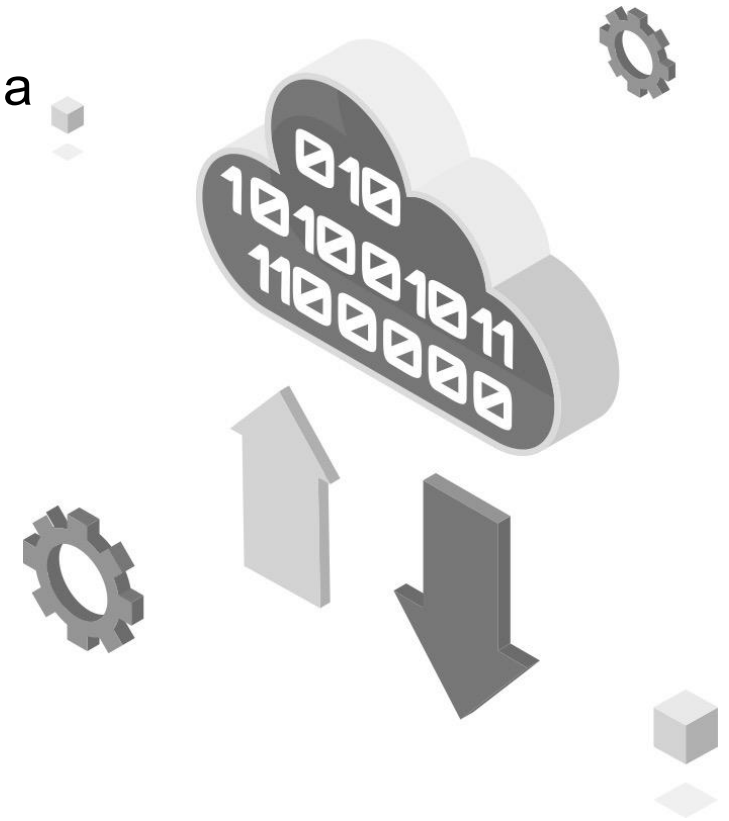
Решение ✓

С помощью **Dr.Web FixIt!** сотрудник может запустить на своем ПК удаленно сгенерированную диагностическую утилиту, отчет которой позволит понять, есть ли проблемы в защите системы, и удалить следы заражений, если такие есть. Проверку можно проводить на регулярной основе.

Ситуация

Компания использует аутсорсинг. Есть подозрение, что на компьютерах внештатных работников нарушаются правила и политики ИБ.

Необходимо найти нарушения информационной безопасности — например, отдельные настройки операционной системы и нерегламентированное ПО.



Решение

Dr.Web FixIt! поможет быстро выявить нарушения ИБ-политики компании и ликвидировать их последствия.

С помощью **Dr.Web FixIt!** были выявлены целевые атаки на различные государственные учреждения нескольких стран.

Выявляйте скрытые угрозы до того, как они нанесли вам ущерб!

fixit.drweb.com/login

Центральный офис

125124, Россия, Москва,
3-я улица Ямского поля, д. 2, к.12А

+7 (495) 789-45-87
(по будням с 9:30 до 18:00)

+7 (495) 789-45-97 (факс)

Телеграм: @DrWeb_Office
(только для звонков)

Техническая поддержка и поддержка продаж

Бесплатно по России:

8-800-333-7932

Бесплатно по Москве:

+7 (495) 789-45-86

Через Телеграм: @DrWeb_Call_Center
(только для звонков)

Ваш лучший партнер «Доктор Веб»

© ООО «Доктор Веб»
2023