ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ «Group-IB AssetZero»

Версия 1.0

РУКОВОДСТВО АДМИНИСТРАТОРА

СОДЕРЖАНИЕ

1. Аннотация 3
2. Настройки доступа и учетных записей 3
3. Обнаружение активов (Asset detection) 3
4. Управление активами (Asset Management) 4
5. Обнаружение проблем 5
6. Классификация проблем 7
7. Управление проблемами 7
8. Граф (Graph) 8

1. Аннотация

Настоящий документ содержит руководство пользователя по использованию программного обеспечения «Group-IB AssetZero» версии 1.0 (далее – ПО).

2. Настройки доступа и учетных записей

Доступ к системе предоставляется через веб-интерфейс. Доступ к веб-интерфейсу доступен авторизованным клиентам системы.

Для получения экземпляра ПО необходимо перейти по ссылке на сайт https://assetzero.group-ib.ru/. На сайте присутствует форма для ввода логина и пароля, которые находятся в файле AZ.txt. После ввода логина и пароля ПО становится доступным для использования. Порядок получения экземпляра ПО также указан в отдельном файле «Порядок получения экземпляра ПО».

Внимание! На любом этапе установки вы можете обратиться за консультацией в службу Технической поддержки, где наши специалисты помогут на всех этапах получения доступа и настройки ПО.

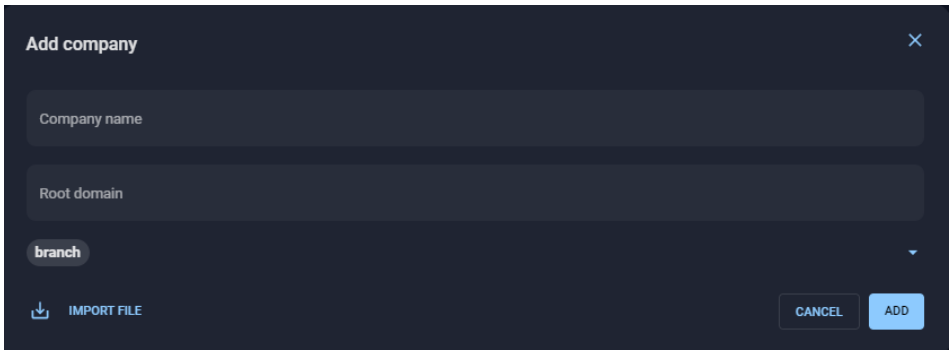
Разграничение прав доступа

Количество пользователей в системе не ограничивается и определяется политикой компании. Пользователи обладают одинаковыми правами.

3. Обнаружение активов (Asset detection)

Для обнаружения активов и обеспечения работы AssetZero выполняются следующие действия:

1. При входе в систему пользователь автоматически переходит на вкладку **Companies** главного меню. Для добавления компании необходимо нажать кнопку **Add company** в правом верхнем углу экрана. При нажатии данной кнопки на экране появится окно добавления компании.



   В появившемся окне необходимо указать название компании и основное доменное имя, которое будет использоваться для поиска активов компании, затем нажать кнопку **Add**. На экране появится индикатор выполнения, содержащий информацию о проверках.

2. Group-IB собирает данные обо всех известных зарегистрированных доменах и поддоменах, выданных и созданных сертификаты и объединяет их с результатами интернет- и веб-сканирования, обнаружения вредоносных программ и др. Затем строится граф всего интернета, который накладывается на активы компании. Для этого используются исторические данные WHOIS и DNS, а также данные сервисов, которые позволяют получить непрерывную картину интернета на ежедневной основе. Следовательно, для обнаружения активов компании необходимо указать только доменное имя основного веб-сайта данной

компании. Использование графа позволяет обнаружить все текущие и исторические активы компании, связанные с основным доменом. Для отображения максимально релевантных результатов осуществляется автоматическая чистка графа от лишних элементов, которые не принадлежат компании, но используют одну и ту же инфраструктуру Интернета, например, общие DNS или почтовые службы. В результате проведения данной процедуры определяются активы компании: IP-адреса, доменные имена, сертификаты SSL/TLS, bucket-хранилища и список публично доступного программного обеспечения.

3. Для пополнения данных, полученных в результате предыдущей процедуры, Система повторно использует выявленные активы и сопоставляет диапазоны IP-адресов, зарегистрированных на компанию или ее дочерние предприятия. В результате этого шага определяются: IP-диапазоны, SSL/TLS-сертификаты и публичное программное обеспечение только в указанных диапазонах.

4. После завершения анализа карточка отобразится в меню **Companies**. Раздел **Companies** содержит виджеты компаний с активными подписками, к которым предоставлен доступ. На виджете отображена следующая информация:

   - название компании;
   - доменное имя;
   - категория, к которой относится компания;
   - текущая оценка защищенности компании;
   - цифровой след — количество обнаруженных доменных имен и IP-адресов, связанных с данной компанией;
   - график, отображающий динамику оценки защищенности компании в указанный промежуток времени.

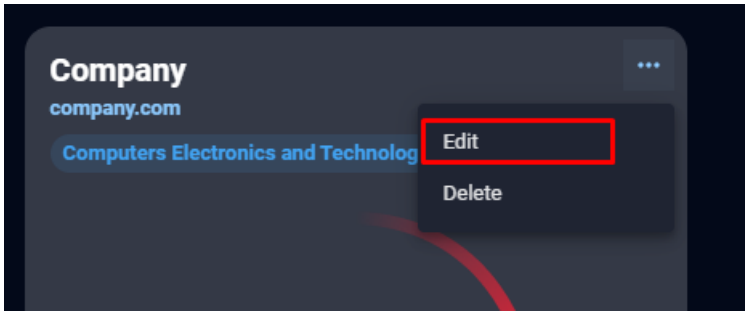
   При нажатии на карточку компании произойдет переход в меню **Dashboard**. В меню **Dashboard** отобразятся виджеты с результатами проверок по различным категориям.

4. Управление активами (Asset Management)

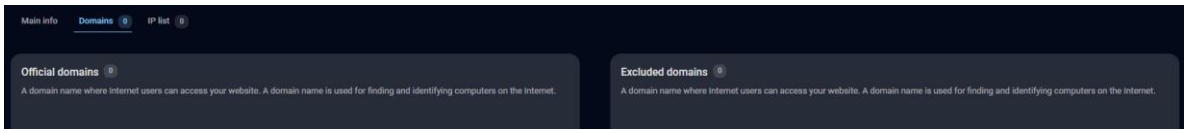
По умолчанию, система определяет активы компании автоматически. Но для улучшения результатов могут быть выполнены два дополнительных действия:

Загрузка списка известных доменов и IP-адресов на страницу настроек компании — все они будут просканированы и отображены на графе. Для этого необходимо:

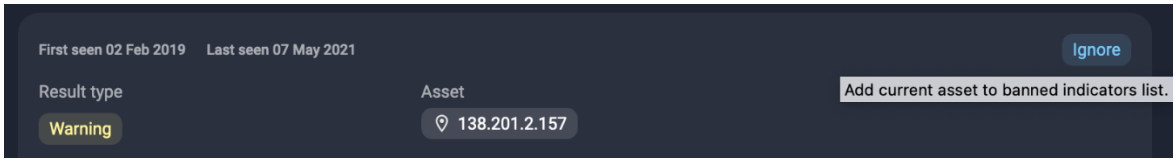
1. Перейти в меню **Companies**, выбрать компанию, которую необходимо отредактировать, и внести изменения с помощью кнопки **Edit** в правой части карточки компании.



2. Добавить доменное имя или IP-адрес в список официальных активов или создать список активов для исключения из анализа.



3. Исключить неактуальные активы из списка обнаруженных с помощью кнопки **Ignore**.



5. Обнаружение проблем

AssetZero оценивает уровень безопасности компании по восьми категориям. Каждой категории присваивается индивидуальный показатель, среднее значение которого составляет оценку безопасности для данной компании.

Категория проблемы	**Описание**
Уязвимости (Vulnerabilities)	На основе результатов регулярного сканирования AssetZero проверяет, подвержены ли активы компании риску уязвимостей или неправильных конфигураций операционных систем, сервисов, приложений, программного и аппаратного обеспечения. Подходы для обнаружения уязвимостей: • Во время интернет-сканирования обнаруживаются службы, запущенные на серверах, эта информация сопоставляется с известными уязвимостями. В случае совпадения проверяется уровень критичности уязвимости, и присваивается статус **Error** или **Warning**. • Для обнаружения веб-уязвимостей проверяется каждый IP-адрес, домен и страницы веб-сайта с целью обнаружения фреймворков. Эта информацию также сопоставляется с известными уязвимостями. • В рамках обнаружения уязвимостей проверяется наличие на серверах открытых баз данных, файловых хранилищ, открытых списков каталогов и других потенциально «неправильных» конфигураций.
Безопасность сети (Network security)	AssetZero сканирует Интернет и подсети клиентов для выявления открытых портов, сервисов (включая их ранние версии) и используемых веб-приложений. Сканирование не подразумевает использование уязвимостей или загрузку какого-либо содержимого — оно не влияет на работающие сервисы. В эту категорию входят открытые порты служб удаленного администрирования (RDP, SSH, VPN и т.д.), порты баз данных, ненадежные заголовки служб, открытые прокси или работающие узлы Tor, а также результаты проверки, был ли хост целью DDoS-атаки.

Утечки баз данных (Leaked credentials)	В эту категорию попадают результаты проверок на наличие утечек баз данных, связанных с отслеживаемыми активами. Проверяются утечки следующих категорий: • Целенаправленные атаки — утечка конфиденциальных данных происходит в результате действий злоумышленника, осуществляющего атаку с помощью вредоносного ПО или фишинга. Похищенные данные используются для проведения еще более сложных атак или перепродаются в даркнет. Group-IB Threat Intelligence & Attribution (система киберразведки) обнаруживает такие утечки и уведомляет клиентов в режиме реального времени через AssetZero. • Публикации в различных источниках — команда аналитиков Group-IB также занимается сбором информации о публикации баз данных в открытых источниках или утечках баз в даркнет. Эти массивные наборы логинов и паролей от сторонних утечек могут затрагивать пользователей связанных организаций. Соответственно, оповещения об этих инцидентах поступают в систему мониторинга AssetZero.
Защита от вредоносного ПО (Malware security)	Злоумышленники используют уязвимости сети для размещения фишингового контента, распространения ВПО и внедрения вредоносного кода в приложения и веб-сайты компании (например, вредоносные программы типа JS-sniffers используются для сбора конфиденциальных данных клиентов). В эту категорию AssetZero попадают следующие данные Group-IB Threat Intelligence & Attribution: • результат работы внутренних и внешних «песочниц», необходимых для взаимодействия между вредоносными программами и активами компании; • веб-контент для фишинговых или мошеннических сайтов, автоматически создаваемых мошенниками на легитимных и пользующихся высоким доверием ресурсах; • технологии графа и системы поиска внешних угроз для обнаружения командных серверов контроля и управления вредоносным ПО или схем атак, связанных с активами компании; • веб-контент на страницах сайтов, который помогает обнаружить внедренный вредоносный код и веб-шелл.
Публикации в даркнет (DarkWeb mentions)	AssetZero получает данные, собираемые ежедневно Group-IB Intelligence. Эти данные автоматически сопоставляются с уведомлениями для обнаружения того, упомянуты ли активы компании в даркнет. Чем чаще упоминаются активы компании, тем выше вероятность того, что против нее будут совершены или уже совершены атаки. AssetZero предоставляет доступ к информации с закрытых форумов для детальной оценки угроз.
Безопасность SSL/TLS (SSL/TLS security)	AssetZero проверяет наличие самоподписанных сертификатов, актуальных версий SSL/TLS и факт использования надежных алгоритмов шифрования. Отсутствие надлежащих конфигураций может привести как к использованию уязвимостей, так и к нарушению нормативных

	требований и отзыву лицензий. Поэтому они включены в метрики и оповещения. Другие ситуационные риски также включаются в анализ чтобы обеспечить их своевременное устранение (например, истечение срока действия сертификатов).
Защита почты (Email security)	Для защиты от спама, фишинговых атак и атак, использующих бренд и домены компании используются DNSSEC, SPF и DMARC. AssetZero проверяет, развернуты ли рекомендуемые конфигурации, чтобы сделать такие атаки менее вероятными. Зачастую компании включают эти параметры безопасности только для основных доменов и оставляют потенциальные риски, пренебрегая полным соответствием всем технологическим требованиям.
DNS & Домены (DNS & Domains)	AssetZero проверяет настройки DNS инфраструктуры компании, чтобы выявить потенциальные слабые места и проверить, соответствуют ли настройки лучшим практикам. Кроме того, AssetZero проводит проверку, чтобы определить, есть ли домены или связанные с ними активы, срок действия которых может скоро истечь.

6. Классификация проблем

Система тестирует каждый актив, связанный с компанией. Тесты могут иметь один из трех результатов:

- **Error** — возникла критическая проблема и могут потребоваться срочные действия;
- **Warning**— является потенциальной проблемой, но не критической, и требует анализа, чтобы определить, является ли это приемлемым статусом для данного актива;
- **Passed** — означает, что проблем не обнаружено и предупреждение не создано.

7. Управление проблемами

Обнаруженные проблемы обрабатываются в следующем порядке:

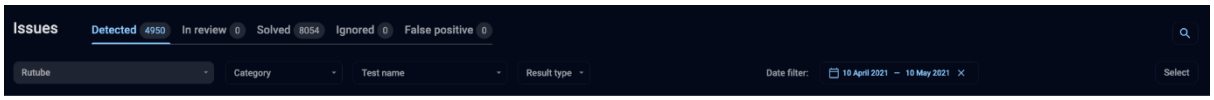
1. **Detected** — проблемы, которые были обнаружены, но еще не были приняты в работу.
2. **Under review** — проблемы, которые проходят проверку аналитиком (в случаях, если это не ложное срабатывание).
3. Проблеме присвоен один из следующих статусов:
    - **Solved** — проблемы, которым аналитиком вручную или системой в автоматическом режиме присвоен статус «Решено».
    - **Ignored** — проблемы, которым аналитиком вручную присвоен статус «Игнорировать». В случае присвоения проблеме данного статуса последующие проверки актива будут отменены;
    - **False positive** — проблемы, которые не были приняты в работу по решению клиента. Статус «Ложное срабатывание» устанавливается аналитиком вручную.

Поиск и фильтрация

Для осуществления быстрого поиска в меню **Dashboard** присутствует возможность фильтрации проблем по выбранной категории. Для фильтрации необходимо выбрать категорию, нажав на её карточку. При нажатии на карточку справа появится боковая панель со строкой поиска, расположенной сверху. Слева от строки поиска расположены раскрывающиеся списки, с помощью которых можно настроить поиск по статусам, присвоенным по результатам анализа

(Предупреждение — **Warning** и Ошибка — **Error**), и по причине — **Reason** или активу — **Asset**. После выбора необходимых параметров в раскрывающихся списках, необходимо ввести ключевые слова, по которым будет осуществлена фильтрация обнаруженных проблем.

В меню **Issues** для поиска необходимо нажать на иконку лупы в правом верхнем углу.



При необходимости выполнить более сложный поиск, присутствует возможность экспортировать наборы данных для дальнейшего анализа или запроса.

8. Граф (Graph)

Раздел **Graph** предназначен для визуализации инфраструктуры компании извне (в сети Интернет) для выявления имеющихся или вероятных угроз. У пользователя существует возможность ввести один из параметров (IP-адрес, домен, SSL и SSH-сертификат, Email-адрес, номер телефона, имя пользователя, хэш) интересующего его объекта и получить по нему дополнительный контекст в виде графа с узлами связи.

Инструментарий раздела позволяет автоматически производить построение графа связности исследуемого ресурса или узла с другими типами объектов:

- **Домены** — узлы графа, связанные с доменным именем ресурса;
- **IP-адреса** — узлы графа, отражающие внешние IP-адреса, к которым привязаны домены;
- **SSL-сертификаты** — связанные с исследуемыми HTTPS-доменами сертификаты;
- **SSH-ключи**, связанные с исследуемым хостом;
- **Файлы**, связанные с IP-адресами и доменными именами;
- **Email-адреса**, используемые при регистрации доменов;
- **Телефонные номера**, используемые при регистрации доменов.

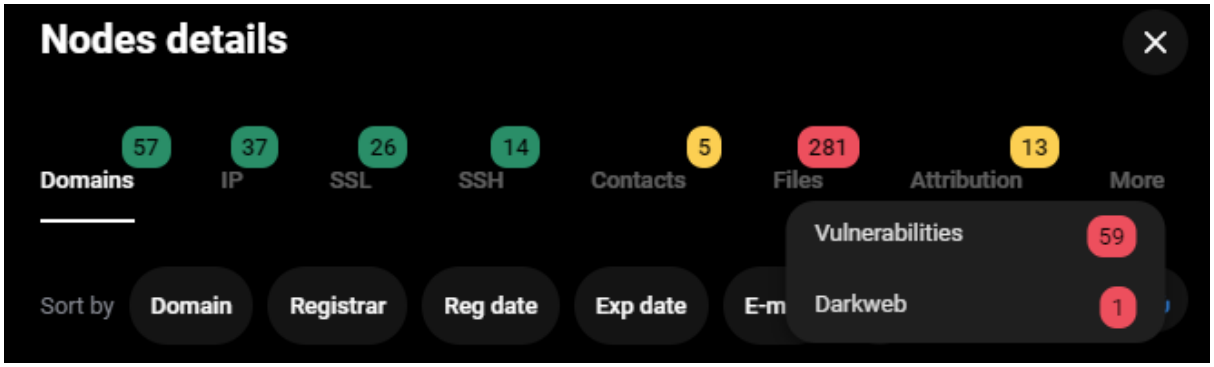
При переходе в меню «Graph» сам граф отображается слева. Справа находится панель с данными по каждому элементу графа и включает в себя следующую информацию:

- Категории — адаптивные вкладки, отображающиеся только тогда, когда на графе присутствуют активы, входящие в ту или иную категорию (например, если на графе отсутствуют вредоносные файлы, то вкладка «Files» также отсутствует).
- Карточки активов — список активов, относящихся к выбранной категории и представленных в виде карточки, которая содержит краткую информацию об активе, с которой непосредственно работает аналитик при взаимодействии с графом.
- Детальная информация — при нажатии на карточку актива на экране появляется детальная информация о данном архиве.

Поскольку граф объединяет в себе данные о сетевой инфраструктуре, контактной информации с хакерских форумов, а также вредоносной активности, узлы графа обозначены разными цветами:

Значение	Цвет	Описание	Примеры
Социальные сети		Ресурсы социальных сетей и мессенджеров	Skype, Telegram, VK и др.
Сеть		Сущности, связанные с сетью Интернет	Доменные имена, IP адреса, SSL и SSH ключи
Вредоносная активность		Все сущности, связанные с вредоносным ПО	Файлы, группировки, сигнатуры, теги, панели управления ВПО
Хакерская активность		Профили злоумышленников на специализированных форумах	*форум_ИмяПрофиля*, например: xss.is_difor. Известные хэши паролей на форуме
Контактная информация		Перечисление контактных данных	Телефоны, email-адреса, известные никнеймы

Описание боковой панели графа (sidebar):



На рисунке выше перечислены все доступные вкладки (по умолчанию отображаются только те, по которым есть данные), в каждой вкладке есть набор карточек. Карточки могут быть отсортированы по преднастроенным «быстрым» фильтрам. Также, присутствует возможность поиска с использованием поисковой строки и экспорта всех активов в формате CSV с помощью кнопки загрузки в правом верхнем углу боковой панели.

При раскрытии карточки открывается второй уровень данных, также содержащий в себе вкладки с более подробной информацией, относящейся к выбранной вкладке актива. Например, карточка актива из категории «Files» содержит следующие вкладки:

- **File details** — общие сведения о файле;
- **DNS** — запросы к службе доменных имен, которые были обнаружены в результате анализа файла в платформе детонации ВПО;
- **HTTP** — запросы по протоколу HTTP, которые были обнаружены в результате анализа файла в платформе детонации ВПО;
- **TCP** — TCP-соединения, которые были обнаружены в результате анализа файла в платформе детонации ВПО.