ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
«F.A.C.C.T. Attack Surface Management»

Руководство по установке и эксплуатации ПО

Содержание

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Введение

Настоящий документ содержит руководство по установке и эксплуатации программного обеспечения «F.A.C.C.T. Attack Surface Management» (далее — ПО, Система).

2 НАЧАЛО РАБОТЫ

F.A.C.C.T. Attack Surface Management не требует установки на устройстве Пользователя.

ПО поставляется Заказчику как услуга (SaaS) – в виде облачного интернет-сервиса. Доступ к системе предоставляется через веб-интерфейс.

2.1 Программно-аппаратные среды функционирования ПО

ПО функционирует в следующих программно-аппаратных средах:

- Windows Internet Explorer версии 11.0 и выше
- Google Chrome версии 8.6.395 и выше
- Mozilla Firefox версии 82.0.1 и выше
- Apple Safari версии 14.0 и выше
- Opera версии 10.5 и выше
- iOS Safari версии 14.0 и выше
- Opera Mobile версии 10.0 и выше
- Google Chrome for Android версии 11.0 и выше
- Mozilla Firefox for Android версии 82.0 и выше
- Windows Internet Explorer Mobile версии 10.0 и выше.

Также для доступа к ПО требуется стабильное интернет-соединение (не менее 30 Мбит/с).

2.2 Настройки доступа и учетных записей

Доступ к Веб-интерфейсу доступен авторизованным клиентам системы. Перед началом работы с ПО обратитесь к сотрудникам Разработчика и предоставьте следующие данные:

- ФИО сотрудника;
- Адрес электронной почты сотрудника.

Разработчик предоставит в электронном письме на указанную почту учетные данные, необходимые для входа в Систему.

2.3 Вход в учетную запись

1. Перейдите на сайт Системы по адресу https://asm.facct.ru/.
2. Введите логин и пароль, полученные от Разработчика, в соответствующие поля.
3. Нажмите кнопку «Войти». После успешной авторизации отобразится главная страница F.A.C.C.T. Attack Surface Management.

Внимание! При возникновении проблем со входом в Систему обратитесь в службу Технической поддержки Разработчика по электронной почте asm@facct.ru.

3 ОБНАРУЖЕНИЕ АКТИВОВ

Для обнаружения активов и обеспечения работы ПО выполняются следующие действия:

1. При входе в систему пользователь автоматически переходит на вкладку **Компании** главного меню. Для добавления компании необходимо нажать кнопку «Добавить компанию» 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 «Добавить». На экране появится индикатор выполнения, содержащий информацию о проверках.
2. Разработчик собирает данные обо всех известных зарегистрированных доменах и поддоменах, выданных и созданных сертификатах, 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 **Компании**. Раздел **Компании** содержит виджеты компаний с активными подписками, к которым предоставлен доступ. На виджете отображена следующая информация:
    a. название компании;
    b. доменное имя;
    c. категория, к которой относится компания;
    d. текущая оценка защищенности компании;
    e. цифровой след — количество обнаруженных доменных имен и IP-адресов, связанных с данной компанией;
    f. график, отображающий динамику оценки защищенности компании в указанный промежуток времени.

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

4 УПРАВЛЕНИЕ АКТИВАМИ

По умолчанию, система определяет активы компании автоматически. Но для улучшения результатов могут быть выполнены дополнительные действия, например загрузка списка известных доменов и IP-адресов на страницу настроек компании. Эти активы будут просканированы и отображены на графе. Для этого необходимо:

1. Перейти в меню **Компании**, выбрать компанию, которую необходимо отредактировать, и внести изменения с помощью кнопки **Редактировать** 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 **Игнорировать**.

5 ОБНАРУЖЕНИЕ ПРОБЛЕМ

ПО 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	На основе результатов регулярного сканирования ПО 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. • 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	ПО сканирует сеть 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.

Защита от вредоносного ПО	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 ПО попадают следующие данные F.A.C.C.T. Threat Intelligence: • 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	ПО получает данные, собираемые ежедневно F.A.C.C.T. Threat 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. ПО предоставляет доступ к информации с закрытых форумов для детальной оценки угроз.
Безопасность SSL/TLS	ПО 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	Для защиты от спама, фишинговых атак и атак, использующих бренд и домены компании используются DNSSEC, SPF и DMARC. ПО 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	ПО проверяет настройки DNS инфраструктуры компании, чтобы выявить потенциальные слабые места и проверить, соответствуют ли настройки лучшим практикам. Кроме того, ПО 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:

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

7 УПРАВЛЕНИЕ ПРОБЛЕМАМИ

Обнаруженные проблемы обрабатываются в следующем порядке:

1. **Обнаруженные** — проблемы, которые были обнаружены, но еще не были приняты в работу.

2. **В работе** — проблемы, которые проходят проверку аналитиком (в случаях, если это не ложное срабатывание).
3. Проблеме присвоен один из следующих статусов:
    a. **Решено** — проблемы, которым аналитиком вручную или системой в автоматическом режиме присвоен статус «Решено».
    b. **Игнорируемые** — проблемы, которым аналитиком вручную присвоен статус «Игнорировать». В случае присвоения проблеме данного статуса последующие проверки актива будут отменены;
    c. **Ложно-позитивные** — 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 **Панель управления** 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 и Ошибка), и по причине или активу.

После выбора необходимых параметров в раскрывающихся списках необходимо ввести ключевые слова, по которым будет осуществлена фильтрация обнаруженных проблем.

8 ГРАФ

Раздел **Граф** 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 «Граф» 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 «Файлы» также отсутствует).
- Карточки активов — список активов, относящихся к выбранной категории и представленных в виде карточки. Карточка содержит краткую информацию об активе, непосредственно с которым работает аналитик при взаимодействии с графом.
- Детальная информация — при нажатии на карточку актива на экране появляется детальная информация о данном активе.

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

Цвет	Значение	Описание
Синий	Социальные сети	Ресурсы социальных сетей и мессенджеров
Зеленый	Сеть	Сущности, связанные с сетью Интернет
Красный	Вредоносная активность	Все сущности, связанные с вредоносным ПО
Оранжевый	Хакерская активность	Профили на специализированных форумах
Желтый	Контактная информация	Перечисление контактных данных