ИНТЕЛЛЕКТУАЛЬНАЯ ПЛАТФОРМА ПО УПРАВЛЕНИЮ УЯЗВИМОСТЯМИ SOLIDLAB

Руководство по эксплуатации

Листов 16

2024 г.

АННОТАЦИЯ

Настоящий документ является руководством по эксплуатации компонентов интеллектуальной платформы по управлению уязвимостями SolidLab (далее по тексту — SolidLab VMS, продукт).

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ

1.1 Область применения

Область применения SolidLab VMS – анализ защищённости приложений и управление выявленными уязвимостями.

1.2 Краткое описание возможностей

Платформа по управлению уязвимостями SolidLab предназначена для поиска и анализа недостатков и уязвимостей в ИТ-инфраструктуре с целью повышения уровня защищенности обслуживаемого сегмента. Компоненты, входящие в состав сервиса, осуществляют сканирование объектов ИТ-инфраструктуры по заданным алгоритмам, а найденные недостатки передаются в единый интерфейс для автоматического и ручного анализа. Defect Tracker – инструмент, входящий в состав SolidLab VMS, позволяет ознакомиться с информацией о выявленных проблемах в инфраструктуре, управлять постановкой задач по устранению выявленных проблем, в том числе приоритизировать данные задачи.

Сервис размещается на стороне Исполнителя и является комплексом технических и программных средств на базе распределённой сети центров обработки данных, предназначенный для оказания услуг по модели облачных вычислений.

Сценарии использования:

– Автоматизация инвентаризации ИТ-инфраструктуры, веб-приложений и используемого программного обеспечения;

– Автоматизация сканирования на уязвимости найденных активов;

– Получение информации об отсутствующих обновлениях безопасности (со списком CVE, устраняемых данным обновлением);

– Выявление уязвимостей, определение уровня критичности и реализация процесса устранения уязвимостей;

– Автоматизация мониторинга производимых изменений в ИТ-инфраструктуре, веб-приложениях и используемом программном обеспечении;

– Фильтрация и валидация результатов работ по поиску уязвимостей.

2 ОБЩИЕ СВЕДЕНИЯ

Продукт выполняет функции активного сканирования на известные уязвимости в объектах внешней инфраструктуры Заказчика.

Активное сканирование включает в себя:

- сканирование открытых портов и определение сервисов (например, 22 TCP SSH);
- поиск неправильных конфигураций приложений (например, некорректная конфигурация grafana или zabbix);
- брутфорс в приложениях на стандартные комбинации логина и пароля (например, admin admin);
- проведение проверок таких как SSL и TLS, Buffer overflow, Denial of Service, проблемы с SMTP и других известных уязвимостей;
- отправка сформированных запросов к уязвимым приложениям для имитации атак на узел (например, уязвимости, классифицированные как CVE).

3 ТРЕБОВАНИЯ К АППАРАТНОМУ И ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ

3.1 Требования к обеспечению рабочего места пользователя

Продукт предоставляется как сервис, который развёрнут в выделенном облаке исполнителя. Платформа по управлению уязвимостями SolidLab является программным обеспечением типа «Программное обеспечение как услуга» и не требует установки на рабочие станции пользователей. Для работы с продуктом требуется только браузер и подключение к сети Интернет.

В случае если на рабочей станции пользователя нет доступа к сети Интернет или в операционной системе не установлен браузер, то необходимо обратиться в отдел технической поддержки пользователей компании с запросом на предоставление доступа к сети Интернет и/или установку одного из веб-браузеров.

Рекомендуемые браузеры:

- Google Chrome версии 100 и выше;
- Firefox Browser версии 100 и выше;
- Яндекс.Браузер версии 21 и выше;
- Safari версии 14 и выше.

3.2 Требования к инфраструктуре

Для обеспечения непрерывности сканирования, необходимо открыть доступ к информационным системам для IP-адреса сканера на СЗИ (на решениях Anti-DDoS, IDS/IPS, WAF, сетевых маршрутизаторах, балансировщиках нагрузки и т.д.) и подтвердить круглосуточную возможность работы сканеров по обследуемым объектам.

Влияние работы платформы на сканируемые системы будет средним и не должно снижать работоспособность обслуживаемых систем. В ходе сканирования возможно незначительное увеличение нагрузки на интернет-сервисы, подлежащие сканированию, и обнаружение системами мониторинга некоторого количества запросов от IP-адреса сканера.

4 ДОСТУП К ПЛАТФОРМЕ

Настройку платформы осуществляет инженер исполнителя на этапе развёртывания SolidLab VMS. В рамках данных работ определяются:

– Компоненты платформы, которые будут задействованы в системе управления уязвимостями;

– Границы анализируемой области (ИТ-инфраструктуры/веб-приложения/сайта/ и др.), а также разделение анализируемой области по продуктам;

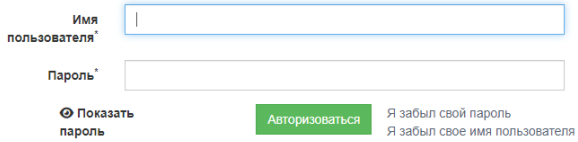
– Частота сканирований и подготовки отчётности.

Настройку сканирований осуществляет инженер исполнителя при развёртывании платформы для нужд заказчика.

Сотрудники заказчика отслеживают результаты работы компонентов платформы через единое окно мониторинга Defect Tracker (DT) и на их основании принимают решения об изменениях в продукте, обслуживаемом платформой.

Для доступа к единому окну управления платформой пользователя, эксплуатирующего систему, необходимо в адресной строке браузера ввести путь, который имеет вид «https://<secret>.vms.solidlab.ru», где «<secret>» - уникальный идентификатор юридического лица заказчика. «Secret» выдаётся уполномоченным лицам заказчика совместно с учётными данными для входа.

В открывшемся окне появятся поля для ввода учётных данных. Для первой авторизации необходимо ввести выданные исполнителем по договору учётные данные, и сменить пароль после успешной авторизации.



Снимок экрана 1. Авторизация на платформе

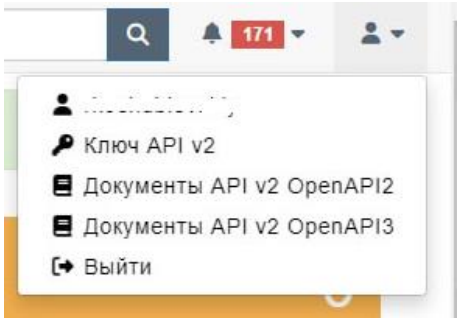
5 РАБОТА С DEFECT TRACKER

После успешной авторизации откроется окно с общей информацией о недостатках.

Слева располагается меню, которое можно свернуть, нажав «Свернуть меню», в нижней части меню. Меню содержит ссылки на инструменты :

- Дашборд – содержит общую информацию о выявленных недостатках;
- Продукты – содержит полную информацию об обслуживаемых платформой продуктах, связанных с данным «secret»;
- Проверки – содержит полную информацию о настроенных проверках;
- Недостатки – содержит полную информацию о выявленных недостатках;
- Компоненты – содержит полную информацию о компонентах продуктов, в которых выявлены недостатки;
- Конечные точки – содержит полную информацию о выявленных конечных точках продуктов;
- Отчёты – позволяет генерировать отчёты по работе платформы;
- Метрики – содержит широкий спектр диаграмм с результирующей информацией о состоянии продуктов;
- Пользователи – позволяет создавать новых пользователей и просматривать информацию о текущих пользователях платформы в рамках своего сегмента;
- Календарь - отображается календарь проверок;
- Конфигурация – позволяет произвести некоторые настройки платформы в рамках своего сегмента;
- Свернуть меню.

Для завершения работы с платформой необходимо завершить сессию, нажав на пиктограмму с изображением человека в правом верхнем меню, в появившемся меню нажать «Выйти» (см. снимок экрана 2).



Снимок экрана 2. Завершение работы

5.1 Автоматизация инвентаризации ИТ-инфраструктуры, веб-приложений и используемого программного обеспечения

На этапе подписания договора на оказание услуг определяются границы и объёмы оказания услуг.

На основании переданных данных инженеры исполнителя настраивают объем и частоту проведения сканирования компонентом автоматизированного пассивного и активного сбора данных об ИТ-инфраструктуре компании из открытых источников (OSINT). Все проверки, выполняемые OSINT, появляются в DT в инструменте «Проверки» со статусом «Running», что говорит о том, что сканирование запущено.

Для того, чтобы просмотреть информацию о проверке необходимо:

1. Выбрать инструмент «Проверки» в левом меню DT.
2. Затем выбрать из выпадающего списка необходимое представление:

- Активные проверки;
- Все проверки;
- Проверки по продукту;
- Типы тестов;
- Окружение.

3. В открывшемся окне найти нужную проверку. Каждая строка списка проверок содержит название компонента, который осуществляет проверку, сроки проведения проверки, название и тип продукта, который был подвергнут проверке, и иную информацию о проверках. Для удобства поиска нужной проверки рекомендуется воспользоваться фильтрами.
4. Для открытия карточки проверки необходимо нажать на соответствующую строку проверки.
5. В карточке проверки представлены следующие данные:

5.1. Описание проверки;

5.2. Проведенные тесты;

5.3. Принятые риски;

5.4. Дополнительную информацию в составе:

- Чеклист;
- Анкеты;
- Заметки с журналом заметок;
- Прикреплённые файлы.

5.5. Мета информация.

Результатом выполнения OSINT может быть:

1. Добавление в DT конечных точек в указанный при запуске продукт – данная информация отображается в инструменте «Конечные точки».
2. Создание в тесте файла с картой конечных точек – файл хранится в карточке теста (п. 5.2).
3. Создание в тесте файлов со снимками экрана и дополнительной информацией в описании – файл хранится в карточке теста (п. 5.2).

По завершению выполнения теста статус теста сменится на «Done».

5.2 Автоматизация сканирования на уязвимости найденных активов

На этапе подписания договора на оказание услуг определяются границы и объёмы оказания услуг.

На основании переданных данных инженеры исполнителя настраивают объем и частоту проведения сканирования на уязвимости в компоненте поиска известных уязвимостей внешнего периметра (EVM). Все проверки, выполняемые EVM, появляются в DT в карточке «Проверки» со статусом «Running», что говорит о том, что сканирование запущено.

Каждому запущенному сканированию присваивается SCAN ID, который отображается в карточке теста.

Завершённое сканирование имеет статус «Done», полученный результат загружается в указанную Проверку в DT.

Для того, чтобы просмотреть информацию о проверке необходимо:

1. Выбрать инструмент «Проверки» в левом меню DT.
2. Затем выбрать из выпадающего списка необходимое представление:

- Активные проверки;
- Все проверки;
- Проверки по продукту;
- Типы тестов;
- Окружение.

3. В открывшемся окне найти нужную проверку. Каждая строка списка проверок содержит название компонента, который осуществляет проверку, сроки проведения проверки, название и тип продукта, который был подвергнут проверке, и иную информацию о проверках. Для удобства поиска нужной проверки рекомендуется воспользоваться фильтрами или использовать известный SCAN ID.
4. Для открытия карточки проверки необходимо нажать на соответствующую строку проверки.
5. В карточке проверки представлены следующие данные:

- Описание проверки;
- Проведенные тесты;
- Принятые риски;

- Дополнительную информацию в составе:
  - Чеклист;
  - Анкеты;
  - Заметки с журналом заметок;
  - Прикреплённые файлы.
- Мета информация.

Список недостатков выявленных активов отражается в инструменте «Недостатки».

5.3 Получение информации об отсутствующих обновлениях безопасности (со списком CVE, устраняемых данным обновлением)

Все проверки, выполняемые EVM, появляются в DT в карточке «Проверки» со статусом «Running», что говорит о том, что сканирование запущено.

Завершённое сканирование имеет статус «Done», полученный результат загружается в указанную Проверку в DT.

Для того, чтобы просмотреть информацию о проверке необходимо:

1. Выбрать инструмент «Проверки» в левом меню DT.
2. Затем выбрать из выпадающего списка необходимое представление:

- Активные проверки;
- Все проверки;
- Проверки по продукту;
- Типы тестов;
- Окружение.

3. В открывшемся окне найти нужную проверку. Каждая строка списка проверок содержит название компонента, который осуществляет проверку, сроки проведения проверки, название и тип продукта, который был подвергнут проверке, и иную информацию о проверках. Для удобства поиска нужной проверки рекомендуется воспользоваться фильтрами.
4. Для открытия карточки проверки необходимо нажать на соответствующую строку проверки.
5. В карточке проверки представлены следующие данные:

- Описание проверки;
- Проведенные тесты;
- Принятые риски;
- Дополнительную информацию в составе:
  - Чеклист;
  - Анкеты;

- Заметки с журналом заметок;
- Прикреплённые файлы.

– Мета информация;
– Учетные данные.

После проведения сканирования на уязвимости EVM в инструменте «Недостатки» появится список выявленных фактов отсутствия обновлений информация об отсутствующих обновлениях безопасности.

5.4 Выявление уязвимостей, определение уровня критичности и реализация процесса устранения уязвимостей

Все выявленные уязвимости доступны к ознакомлению через инструмент «Недостатки». При наведении мышки на соответствующую строку откроется контекстное меню, позволяющее:

– Открыть активные недостатки;
– Открыть активные подтверждённые недостатки;
– Открыть критические недостатки;
– Открыть недостатки за последнюю неделю;
– Открыть недостатки с принятым риском;
– Открыть все недостатки;
– Открыть закрытые недостатки;
– Добавить новую уязвимость;
– Импортировать результаты сканирования.

Каждому недостатку присваивается уровень критичности, который может быть скорректирован пользователем системы или инженером исполнителя.

5.5 Автоматизация мониторинга производимых изменений в ИТ-инфраструктуре, веб-приложениях и используемом программном обеспечении

На этапе подписания договора на оказание услуг определяются границы и объёмы оказания услуг.

На основании переданных данных инженеры исполнителя настраивают объем и частоту проведения контроля изменений в ИТ-инфраструктуре, веб-приложениях и используемом программном обеспечении в компоненте поиска известных уязвимостей внешнего периметра (EVM). Все проверки, выполняемые EVM, появляются в DT в инструменте «Проверки» со статусом «Running», что говорит о том, что сканирование запущено.

Каждому запущенному сканированию присваивается SCAN ID, который отображается в карточке теста.

Для того, чтобы просмотреть информацию о проверке необходимо:

1. Выбрать инструмент «Проверки» в левом меню DT.
2. Затем выбрать из выпадающего списка необходимое представление:

- Активные проверки;
- Все проверки;
- Проверки по продукту;
- Типы тестов;
- Окружение.

3. В открывшемся окне найти нужную проверку. Каждая строка списка проверок содержит название компонента, который осуществляет проверку, сроки проведения проверки, название и тип продукта, который был подвергнут проверке, и иную информацию о проверках. Для удобства поиска нужной проверки рекомендуется воспользоваться фильтрами или использовать известный SCAN ID.

4. Для открытия карточки проверки необходимо нажать на соответствующую строку проверки.
5. В карточке проверки представлены следующие данные:

- Описание проверки;
- Проведенные тесты;
- Принятые риски;
- Дополнительную информацию в составе:
    - Чеклист;
    - Анкеты;
    - Заметки с журналом заметок;
    - Прикреплённые файлы.
- Мета информация.

Завершённое сканирование имеет статус «Done», полученный результат загружается в указанную Проверку в DT.

Все обнаруженные изменения будут отражены в карточке теста соответствующей проверки.

5.6 Фильтрация и валидация результатов работ по поиску уязвимостей

В инструменте «Недостатки» доступны представления:

- Открытые недостатков;
- Все недостатки;
- Закрытые недостатки;
- Недостатки с принятым риском;

– Шаблоны недостатков.

В каждом из представлений доступна фильтрация недостатков по широкому списку параметров, например:

– Название компонента;
– Версия компонента;
– Дата;
– CWE;
– Критичность;
– Последняя проверка;
– Последнее обновление статуса;
– Дата исправления недостатка;
– Сообщил;
– Проверка;
– Тест;
– Тип теста;
– Версия проверки;
– Версия теста;
– Статус;
– Активно;
– Подтверждён;
– Устраняется;
– Выходит за рамки;
– Ложноположительный результат;
– Риск принят;
– Имеет компонент;
– Имеет заметки;
– И др.

Всем выявленным недостаткам присваивается уровень критичности в зависимости от влияния на продукт заказчика:

– Critical – недостаток оказывает серьёзное негативное влияние на продукт, которое может привести к полному или частичному выходу из строя обслуживаемого продукта, или к серьёзным последствиям для пользователей или компании.

– High - недостаток оказывает высокое негативное влияние на продукт, которое может привести к сбоям в работе обслуживаемого продукта, или к серьёзным последствиям для пользователей или компании.

– Medium - недостаток оказывает значительное негативное влияние на продукт, которое может привести к некоторым ограничениям в работе обслуживаемого продукта.

– Low - недостаток оказывает низкое негативное влияние на продукт.

– Info – недостаток не оказывает влияние на работу продукта, но в последствии может стать причиной появления более значительных недостатков.

Решение о присвоении уровня критичности принимается сканером на основании CVSS. Аналитики исполнителя отслеживают недостатки и в карточке недостатка вносят коррективы и рекомендации по устранению недостатка.

6 КОНТАКТЫ

Для получения детализированного руководства DT VMS необходимо направить обращение на электронный адрес info@solidlab.ru.

Детализированное описание функциональных характеристик программного обеспечения содержится в документе «Интеллектуальная платформа по управлению уязвимостями SolidLab. Описание функциональных характеристик», которое может быть предоставлено по запросу на электронный адрес info@solidlab.ru.