Общество с ограниченной ответственностью

«Софт Плюс»

КРАТКОЕ ОПИСАНИЕ СИСТЕМЫ

Программы для ЭВМ

Платформа управления пентестами

и организации команд

Листов 11

2025

Содержание

1. Введение

1.1 Общие сведения и область применения

Платформа предназначена для работы квалифицированных специалистов по ИБ, оптимизирующий внутренние процессы, упрощающий внутри-командную и кросс-командную коммуникацию без потери контекста. А также аналитическая платформа, упрощающая работу как с результатами автоматизированных средств, так и с ручным анализом. На пересечении массивов данных из различных источников, за счет накопления и обогащения информацией о одних и тех же объектах, но в различном контексте появляется возможность эффективного выявления как типовых, так и ранее неизвестных дефектов ИБ (уязвимостей).

Результаты работы в рамках Платформы в свою очередь уже могут быть экспортированы как в виде аналитических отчетов, так и сконвертированы в задачи в системах отслеживания задач (СОЗО).

1.2 Термины, сокращения и определения

Термин (сокращение)	**Определение**
ПО	Программное обеспечение
ПЭВМ	Программа для ЭВМ
Платформа	ПЭВМ “Система управления безопасной разработкой”
СОЗО	Система Отслеживания Задач и Ошибок

2 Назначение и условия применения

2.1 Предмет автоматизации

ПЭВМ Платформа управления пентестами и организации команд предоставляет возможность автоматизации следующих задач:

- Решение задач, связанных с анализом защищенности сопряжено с обработкой большого объема разнородных данных, поступающих из различных источников таких как:
    - сетевые сканеры

        - сканеры уязвимостей
        - сканеры веб-приложений
        - инструменты ручного анализа
        - узкоспециализированные инструменты
        - сторонние провайдеры информации о дефектах ИБ
        - разнородные базы данных и базы знаний
- Консолидация и нормализация поступающих массивов специализированной информации в едином информационном пространстве и возможность совместной работы с ними в контексте объекта исследования (инфраструктуры, приложения, итп).
- Генерация аналитических отчетов с применением шаблонизации
- Организация методического подхода к решению задач за счет применения чеклистов

2.2 Перечень функций реализуемых Платформой

2.2.1 Функции компонента “Управление проектами” модуля Hive

В рамках данного компонента пользователи могут:

- создавать иерархию групп проектов;
- создавать проекты в различных группах и переносить их между проектами;
- назначать сотрудников на проект;
- следить за ходом тестирования и готовностью задач;
- мониторить действия команды и составлять отчеты на всех этапах тестирования.

Так же данный компонент даёт возможность создания и управления шаблонами проектов.

2.2.2 Функции компонента “Проект” модуля Hive

Проект—это основное хранилище данных в процессе работы команды тестирования.

Во время тестирования и анализа целевых систем весь объем данных будет попадать сюда. Пользователи могут добавлять результаты тестирования как вручную, так и экспортировать их напрямую из таких инструментов как *Nmap*, *Masscan*, *Nessus*, *Metasploit*, *Cobalt Strike*, и прочих приложений. Вся команда, участвующая в проекте, будет видеть обновления данных проекта.

В рамках проекта пользователи работают с таким данными о целевой системе, как:

- ip адреса;
- имена хостов;
- порты;
- сервисы.

В рамках работы над проектом пользователи могут пользоваться такими функциями:

- На вкладке **Приложения** пользователи могут хранить информацию из различных приложений.
- С помощью **чек-листов** пользователи могут планировать и оценить объем работ, а также проверить, все ли тесты выполнены в срок. Менеджеры и рядовые аудиторы могут использовать чек-листы в качестве базы данных, добавляя в них описания, файлы, и уязвимости. Так же чеклисты могут синхронизироваться с модулем Apiary на котором заказчик может контролировать процесс проведения пентеста.
- **Уязвимости** — это проблемы в безопасности, которые были обнаружены в целевых системах во время тестирования на проникновение и зарегистрированы аудиторами на Платформе в модуле Hive. Уязвимости могут иметь несколько статусов для подтверждения или опровержения их наличия. Могут быть синхронизированы с проектом в модуле Apiary для своевременного реагирования заказчика пентеста.
- **Схема уязвимости** - позволяет гибко настраивать список полей, которые пользователь хочет видеть в уязвимостях. Одна схема может использоваться в нескольких проектах.
- На вкладке **Credentials** пользователи могут хранить учетные данные (логины и пароли) полученные ими из различных сервисов или систем.
- На страницах **Wiki** пользователи могут собирать и классифицировать знания по проекту или группе проектов, уязвимостям и чек-листам, а также хранить все загруженные файлы.

По завершению тестирования или, в его процессе, команда может передать все собранные данные конечным клиентам в удобном формате, а также общаться с клиентами непосредственно в проекте посредством интеграции с модулем Apiary.

2.2.3 Функции компонента “Генератор отчётов” модуля Hive

Для формирования отчёта об уязвимостях и чеклистах в человеко-читаемом виде модуль Hive предоставляет возможность генерировать отчёт в формате DOCX по пользовательскому шаблону.

Функции данного компонента:

- загрузка собственного шаблона отчёта;
- отладка шаблона;
- выбор уязвимостей для включения в отчёт;
- генерация отчёта.

2.2.4 Функции компонента “Информационная панель” в модуле Hive

Данного компонент позволяет:

- просматривать уязвимости из всех проектов;
- просматривать статистику действий пентестеров по неделям, месяцам и так далее.

2.2.5 Функции компонента “Интеграция” модулей Hive и Apiary

Части данного компонента присутствуют в каждом из модулей Hive и Apiary. При этом в модуле Apiary реализована основная логика данного компонента, а в модуле Hive только необходимая для работы данной интеграции. Интеграция проектов и систем построена на базе RabbitMQ, который может быть развёрнут вместе с модулем Apiary или предоставлен заказчиком. Важной особенностью данного компонента является то, что модули не обязательно должны быть онлайн всё время - данные могут быть синхронизированы постфактум.

Данный компонент обеспечивает:

- создание соединений, которое включает создание очередей в RabbitMQ и их настройку;
- соединение проектов для передачи данных между ними;
- регулярную проверку статуса соединения;
- обмен данными в реальном времени и отложенный.

2.2.6 Функции компонента “Управление проектами” в модуле Apiary

Компонент “Управление проектами” позволяет:

- создавать проекты в модуле Apiary;
- создавать и модифицировать иерархическую систему групп проектов;
- назначать пользователям различные роли на группы и проекты.

2.2.7 Функции компонента “Информационная панель” в модуле Apiary

Компонент “Информационная панель” позволяет:

- просматривать агрегированную информацию об известных уязвимостях во всех проектах в виде информационных карточек;
- создавать собственные информационные карточки;
- настраивать отображение информационных карточек.

2.2.8 Функции компонента “Проект” в модуле Apiary

Компонент “Проект” позволяет:

- просматривать агрегированную информацию об известных уязвимостях в рамках данного проекта в виде информационной панели с информационными карточками;
- создавать собственные информационные карточки;
- настраивать отображение информационных карточек;
- управлять уязвимостями, полученными из модуля Hive;
- наблюдать за ходом выполнения проекта через изменения статуса чеклистов;
- назначать роли пользователям проекта;
- автоматически изменять статус уязвимости в модуле Hive путём изменения статуса в Apiary;
- создавать задачи во внешней СОЗО по имеющимся уязвимостям.

2.2.9 Функции компонента “Интеграция с СОЗО” в модуле Apiary

Одна из важных функций модуля Apiary: интеграция с внешними СОЗО. На текущий момент реализована поддержка одной такой системы только системы: Jira.

Функции данного компонента включают:

- отправка уязвимостей в виде задач во внешнюю СОЗО;
- отправка комментариев к уязвимости во внешнюю СОЗО;
- настройка сопоставления статуса задач во внешней СОЗО со статусом внутри модуля Apiary;
- отслеживание статуса задачи во внешней СОЗО и автоматической смены статуса уязвимости в модуле Apiary;
- синхронизация комментариев к уязвимости из внешней СОЗО.

2.2.10 Функции компонента “SMTP уведомления” в модуле Apiary

Пользователь может настроить получение уведомлений по SMTP из модуля Apiary.

Функции модуля включают:

- настройки интеграции уведомлений по SMTP;
- настройки шаблона писем-уведомлений;
- гибкую настройку типа уведомлений, которые хочет получать пользователь.

2.2.11 Функции компонента “Генератор отчётов” в модуле Apiary

Для формирования отчёта об уязвимостях в человеко-читаемом виде модуля Apiary предоставляет возможность генерировать отчёт в формате DOCX по пользовательскому шаблону.

Функции данного компонента:

- загрузка собственного шаблона отчёта;
- отладка шаблона;
- выбор уязвимостей для включения в отчёт;
- генерация отчёта.

3 Описание Платформы

3.1 Структура Платформы

Платформа состоит из двух модулей:

- модуль Hive: рабочее пространство пентест-команд.
- модуль Apiary: витрину предоставления результатов. Опциональный модуль.

3.2 Варианты поставки Платформы заказчику

Платформа предполагает развёртывание в инфрастуктуре заказчика при помощи дистрибутивного пакета, представляющего собой самораспаковывающийся архив с инсталлятором;

При инсталляции на одной машине при помощи дистрибутивного пакета так же есть два варианта инсталляции:

- установка с доступом в интернет;
- установка без доступом в интернет.

4 Внедрение и обслуживание системы

4.1 Внедрение системы

Внедрение Платформы осуществляется при поддержке службы технической поддержки по запросу пользователя.

4.2 Обслуживание системы

Техническая поддержка пользователей Платформы по вопросам установки, переустановки, администрирования и эксплуатации осуществляется посредством электронной почты.

В рамках технической поддержки программного обеспечения предоставляются следующие услуги:

- Помощь в установке программного обеспечения.
- Помощь в настройке и администрировании.
- Помощь в установке обновлений программного обеспечения.
- Устранение неисправностей, выявленных в ходе эксплуатации.
- Помощь в поиске и устранении проблем в случае некорректной установки обновления Системы.
- Пояснение функционала модулей Системы и помощь в эксплуатации.
- Предоставление актуальной документации по установке, настройке и работе Системы.
- Общие консультации по выбору серверного программного обеспечения для обеспечения более высокой производительности работы Системы.

Неисправности, обнаруженные в процессе эксплуатации Системы, могут быть устранены следующими методами:

- Работа специалиста службы технической поддержки по запросу пользователя.
- Техническая поддержка Системы осуществляется в соответствии с действующими правилами компании и выполняется специалистами ООО «Софт Плюс».

4.3 Требования к программному и аппаратному обеспечению

В варианте по умолчанию, каждый из модулей Hive и Apiary устанавливается на отдельную машину. Для того что бы выполнить такую инсталляцию требуется:

- подготовить физическую или виртуальную машину, удовлетворяющую минимальным системным требованиям;
- установить на неё одну из поддерживаемых ОС;
- установить на неё требуемое ПО.

Минимальные системные требования модуля Hive:

- RAM: 4GB
- CPU: 2 core
- Скорость диска: 50 IOps
- Место на диске: 40GB

Минимальные системные требования модуля Apiary:

- RAM: 4GB
- CPU: 2 core
- Скорость диска: 50 Iops
- Место на диске: 40GB

Платформа поддерживает установку на следующие операционные системы:

- CentOS 8
- RHEL 8
- RedOS 7.3
- Ubuntu 20.04
- Ubuntu 22.04
- Ubuntu 24.04
- Debian 11
- Debian 12
- Astra Linux Орёл 1.7
- другие ОС, совместимые с указанными выше.

Требования с стороннему программному обеспечению:

- docker engine (https://docs.docker.com/engine/install/)
- docker compose plugin (https://docs.docker.com/compose/install/linux/).

4.4 Требования к каналам связи

Для стабильной работы ПЭВМ «Платформа управления пентестами и организации команд» требуется стабильное сетевое соединение со скоростью от 100 Мбит\с от машин, на которых развёрнуты модули Hive и Apiary Платформы до

серверов СУБД PostgreSQL и Redis, а также RabbitMQ в случае, если их предоставляет заказчик.

Для стабильного доступа к пользовательскому интерфейсу Платформы требуется стабильное сетевое соединение со скоростью от 10 Мбит\с от машины пользователя до машин с развёрнутыми модулями Hive и Apiary Платформы.