Программное обеспечение для электронно-вычислительных машин «Платформа управления внешними угрозами SENTRA»

Описание функциональных характеристик

Листов 8

г. Москва, 2025 г.

СОДЕРЖАНИЕ

ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ, СОКРАЩЕНИЯ 3
1. Введение 4
2. Функциональные характеристики Системы 5
3. Выполнение Системы 8

ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ, СОКРАЩЕНИЯ

Термин	Определение
Актив	IP-адрес или домен
АРМ	Автоматизированное рабочее место
ПО	Программное обеспечение
ЭВМ	Электронно-вычислительная машина
ASN	Номер автономной системы (Autonomous System Number)
CIDR	Бесклассовая междоменная маршрутизация (Classless Inter-Domain Routing)

1. Введение

Настоящий документ содержит описание функциональных характеристик платформы управления внешними угрозами SENTRA (далее - Система). Система предназначена для отслеживания внешних угроз в реальном времени.

Исключительные права на Систему принадлежат Обществу с ограниченной ответственностью «ЗАЩИЩЕННЫЕ СИСТЕМЫ» на основании договоров отчуждения.

Система введена в эксплуатацию, поименована как программа для ЭВМ Платформа управления внешними угрозами SENTRA и поставлена на бухгалтерский учет согласно Акту о приеме объекта нематериальных активов №1 от 13.03.2025 г, Приказу о вводе в эксплуатацию нематериальных активов № 1 от 13.03.2025 г., Карточки учета НМА №00-000001 от 13.03.2025 г.

1.1.Краткое описание возможностей

Основными возможностями Системы являются:

- автоматизированный поиск корпоративных ресурсов, доступных из сети Интернет;
- регулярное обогащение списка ресурсов;
- регулярный мониторинг портов сервисов;
- выявление уязвимостей систем, сервисов и веб-приложений;
- классификацию уязвимостей по уровню критичности;
- автоматизированный подбор паролей для ssh, ftp, telnet, mssql, postgresql, imap, pop3, smtp, snmp, mysql, vmauthd, vnc, mongodb, asterisk, oracle, xmpp, rdp;
- подбор доменных учетных данных;
- анализ настроек доступа к файлам и папкам веб-серверов с целью предотвращения утечек конфиденциальных данных;
- управление и контроль процесса устранения уязвимостей при экспертной поддержке специалистов ООО «ЗАЩИЩЕННЫЕ СИСТЕМЫ».

1.2.Уровень подготовки пользователя

Все пользователи Системы должны иметь навыки работы с браузерами. Наличие профильного образования или сертификата о переподготовке позволит быстрее погрузиться в существующие процессы управления уязвимостями и оценки цифровых угроз.

Для получения доступа к ресурсам Системы пользователю необходимо использовать автоматизированное рабочее место (АРМ) в виде электронного вычислительного устройства, имеющего доступ в сеть Интернет, с установленным на него браузером.

2. Функциональные характеристики Системы

Система содержит следующие вкладки интерфейса:

- Главная;
- Активы;
- Уязвимости;
- Сканирования;
- Сотрудники;
- Уведомления;
- Документы.

2.1. Функциональные характеристики вкладки «Главная»

Вкладка «Главная» представляет собой графическую панель (дашборд), на которой пользователь может просмотреть аналитику внешних угроз, отображенную на виджетах. Виджет – небольшое вспомогательное приложение, которое позволяет получать быструю информацию или выполнять какие-либо действия без необходимости переходить на другие страницы.

Функциональными возможностями вкладки являются:

- просмотр виджетов.

2.2. Функциональные характеристики вкладки «Активы»

Вкладка «Активы» состоит из трех дочерних разделов:

- IP-Адреса;
- Домены;
- Добавить активы.

Раздел «IP-Адреса» предназначен для просмотра списка IP-адресов, добавленных в Систему.

Раздел «IP-Адреса» предоставляет пользователю следующие функциональные возможности:

- просмотр списка IP-адресов;
- поиск, фильтрация и сортировка IP-адресов;
- создание и настройка наборов фильтров;
- выбор типа просмотра списка IP-адресов (в виде таблицы или карточек);
- изменение статуса IP-адресов;
- добавление новых IP-адресов;
- конфигурация таблицы с IP-адресами для скачивания;
- скачивание таблицы с IP-адресами в формате Excel-файла;
- согласование и отклонение добавленных IP-адресов;
- просмотр карточек добавленных IP-адресов или доменов (далее – активов).

Раздел «Домены» предназначен для просмотра списка доменов, добавленных в Систему.

Раздел «Домены» предоставляет пользователю следующие функциональные возможности:

- просмотр списка доменов;
- поиск, фильтрация и сортировка доменов;
- создание и настройка наборов фильтров;
- выбор типа просмотра списка доменов (в виде таблицы или карточек);
- изменение статуса домена;
- добавление новых доменов;
- конфигурация таблицы с доменами для скачивания;
- скачивание таблицы с доменами в формате Excel-файла;

- согласование и отклонение добавленных доменов;
- просмотр карточек активов.

Раздел «Добавить активы» предназначен для добавления в Систему новых активов

Раздел «Добавить активы» предоставляет пользователю следующие функциональные возможности:

- добавление активов, представленных в виде IP-адреса, домена, CIDR и/или ASN.

2.3. Функциональные характеристики вкладки «Уязвимости»

Вкладка «Уязвимости» предназначена для управления жизненным циклом уязвимостей. На вкладке представлена таблица с описанием уязвимостей.

Вкладка «Уязвимости» предоставляет пользователю следующие функциональные возможности:

- просмотр списка уязвимостей на каждой стадии жизненного цикла;
- изменение статуса уязвимостей;
- поиск, фильтрация и сортировка уязвимостей;
- создание и настройка наборов фильтров;
- просмотр карточек уязвимостей с возможностью оставить комментарий к карточке и приложить файл к комментарию;
- добавление уязвимости.

2.4. Функциональные характеристики вкладки «Сканирования»

Вкладка «Сканирования» предназначена для просмотра информации о сканированиях. На вкладке представлена таблица с описанием сканирований.

Вкладка «Сканирования» предоставляет пользователю следующие функциональные возможности:

- просмотр списка сканирований с описанием;
- поиск, фильтрация и сортировка сканирований;
- создание и настройка наборов фильтров.

2.5. Функциональные характеристики вкладки «Сотрудники»

Вкладка «Сотрудники» предназначена для просмотра информации о сотрудниках организации. На вкладке представлена таблица со списком сотрудников.

Вкладка «Сотрудники» предоставляет пользователю следующие функциональные возможности:

- просмотр списка сотрудников с описанием;
- поиск, фильтрация и сортировка сотрудников;
- создание и настройка наборов фильтров;
- добавление сотрудника;
- просмотр карточек сотрудников;
- сброс пароля сотрудника;
- приостановка доступа сотрудника к Системе.

2.6. Функциональные характеристики вкладки «Уведомления»

Вкладка «Уведомления» предназначена для просмотра списка уведомлений о событиях в Системе.

Вкладка «Уведомления» предоставляет пользователю следующие функциональные возможности:

- просмотр списка системных уведомлений;
- поиск, фильтрация и сортировка уведомлений;

- создание и настройка наборов фильтров;
- изменение статуса уведомлений;
- просмотр описание уведомления;
- настройка уведомлений.

2.7. Функциональные характеристики вкладки «Документы»

Вкладка «Документы» предназначена для просмотра списка документов организации.

Вкладка «Документы» предоставляет пользователю следующие функциональные возможности:

- просмотр документации.

2.8. Прочие функциональные характеристики Системы

Прочими функциональными характеристиками Системы являются:

- просмотр карточки текущего пользователя;
- редактирование информации о текущем пользователе;
- изменение пароля;
- просмотр списка организаций и добавление новых организаций;
- настройка расписаний сканирований.

3. Выполнение Системы

3.1 Загрузка и запуск Системы

Для получения доступа к Системе профиль пользователя веб-приложением должен быть добавлен в Систему администратором после заключения договора. Запуск Системы происходит при открытии ссылки https://easm-dev.pt.singleton-security.ru/ в веб-браузере.

3.2 Выполнение Системы

Вся функциональность Системы доступна конечному пользователю через веб-браузер и выполняется при нажатии на гиперссылки. Система доступна только при наличии подключения к сети Интернет.

3.3 Завершение работы Системы

В Системе не предусмотрена возможность завершения работы. Пользовательский сеанс считается завершенным в тот момент, когда конечный пользователь производит деавторизацию в Системе или закрывает все браузеры (окна браузеров), которые относятся к Системе.