ГАРДА СТАЛКЕР

ФУНКЦИОНАЛЬНАЯ СПЕЦИФИКАЦИЯ

Дата выпуска:	24.03.2023
Статус документа:	Released
Версия ПО:	1.0.0

Содержание

1. ИНФОРМАЦИЯ О ДОКУМЕНТЕ

1.1. Аннотация

Документ содержит информацию о возможностях ПО «Гарда Сталкер», а также требования к обеспечению его ресурсами.

1.2. Область применения

Документ предназначен для ПО «Гарда Сталкер» версии 1.0.0.

1.3. Целевая аудитория

Документ предназначен для сотрудников, осуществляющих закупки и юридическое сопровождение таких сделок, для сотрудников отдела информационных технологий и службы информационной безопасности организации.

1.4. Термины, определения и сокращения

Термин	Значение
ПО «Гарда Сталкер»	Далее Система. Программное обеспечение «Гарда Сталкер» получения списков индикаторов компрометации.
Фид	Форматированный список индикаторов компрометации.
Индикатор компрометации	Это активность и/или вредоносный объект, обнаруженный в сети или на конечной точке.
Пользователь Системы	Сотрудник, использующий в своей работе Систему
Администратор Системы	Сотрудник, производящий установку, настройку и обслуживание Системы
ОС	Операционная система
Браузер	Программное средство навигации и просмотра ресурсов сети интернет
ИТ / IT	Информационные технологии
ИБ	Информационная безопасность
Стороннее ПО	Программное обеспечение разработанное независимыми разработчиками и не по заказу ООО «Гарда Технологии»; к нему относится

Термин	Значение
	операционные системы, различные прикладные приложения и т.д.

2. ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

2.1. Назначение Системы

«Гарда Сталкер» – это ПО предназначенное для предоставления данных об индикаторах компрометации, собранных как из открытых, так и из собственных источников компании, обогащенных, проанализированных и ранжированных.

2.2. Структура Системы

«Гарда Сталкер» состоит из следующих функциональных частей:

- Модуль сбора данных.
  Модуль собирает данные из различных источников, как доступных в сети интернет, так и собственных источников компании.
- Модуль хранения и обработки данных.
  Модуль хранит данные индикаторов компрометации, обогащает их дополнительной информацией от разных источников, маркирует и фильтрует данные.
- Модуль формирования фидов (списков индикаторов компрометации).
  Модуль формирует фиды в виде форматированных списков, в машиночитаемом и человекочитаемом виде.
- Модуль предоставления данных пользователю (веб-интерфейс).
  Модуль предоставляет интерфейс пользователя, для получения фидов, как с использованием веб-браузера, так и утилит командной строки.

2.3. Принцип работы

Данные полученные от источников загружаются в Систему. На этапе загрузки данные обогащается информацией о географической принадлежности, принадлежности к организации, принадлежности к доверенным сервисам, фильтруются. В Системе конкретные индикаторы компрометации связываются между собой и ранее полученными данными по характерным признакам и обогащаются дополнительным контекстом. С определенной периодичностью, из полученных данных формируются форматированные списки (фиды), которые предоставляются пользователю, через веб-интерфейс личного кабинета.

2.4. Функциональные возможности комплекса

2.4.1. Основные функции

К основным функциям Системы относится:

- Сбор данных.
- Обогащение данных.
- Фильтрация данных.
- Формирование форматированных списков (фидов), на основании собранных данных.

2.4.2. Функциональные возможности компонентов Системы

2.4.2.1. Веб-интерфейс

Аутентификация Пользователей Системы

Аутентификация пользователя в Системе осуществляется с помощью веб-браузера и пары логин/пароль, или с использованием инструментов командной строки типа curl/wget и уникального ключа доступа. Аутентификационные данные индивидуальны для каждого пользователя.

Получение фидов

Пользователь может получать фиды используя веб-интерфейс Системы, как с помощью веб-браузера, так и с использованием инструментов командной строки типа curl/wget.

Изменение учетных данных

При доступе к веб-интерфейсу Системы с помощью веб-браузера пользователь может самостоятельно изменить свои учетные данные:

- Пароль
- Уникальный ключ доступа

Информация о лицензии

При доступе к веб-интерфейсу Системы с помощью веб-браузера пользователь может ознакомиться с информацией о лицензии:

- Номер лицензии
- Срок действия лицензии
- Доступные категории индикаторов компрометации

2.4.2.2. Сборка данных

Компонент сборки данных позволяет собирать данные от различных источников и преобразовывать их в форматированные списки, доступные для загрузки в Систему.

2.4.2.3. Обработка данных

Компонент позволяет проанализировать загружаемые в Систему данные, установить связи между индикаторами компрометации, добавить индикатору маркировку и дополнительный контекст.

2.4.3. Категории индикаторов компрометации

Система предоставляет данные об индикаторах следующих категорий:

- C&C Botnet – индикаторы управляющих центров ботнет-сетей;
- Botnet – индикаторы узлов ботнет;
- DDoS – индикаторы узлов DDoS;
- Phishing – индикаторы фишинг-узлов;
- Spam – индикаторы спам-узлов;
- VPN – индикаторы vpn-узлов;
- Proxy – индикаторы proxy-узлов;
- Tor – индикаторы tor-узлов;
- Suspicious – индикаторы узлов, проявивших «подозрительную» активность;

2.4.4. Формат фидов

- json – текстовый формат обмена данными, основанный на JavaScript. Легко читается человеком и машиной;
- csv – текстовый формат, предназначенный для представления табличных данных;
- txt – текст без форматирования;
- sig – собственный формат. Представляет собой txt обогащенный дополнительной информацией о портах и протоколах.

3. ТРЕБОВАНИЯ К ОБЕСПЕЧЕНИЮ

3.1. РМ Пользователя Системы

Графический интерфейс Пользователя Системы выполнен в виде веб-приложения. Доступ к интерфейсу осуществляется с использованием одного из следующих веб-браузеров:

- Google Chrome версии 42.0.2311.90 и выше;
- Яндекс Браузер версии 18.9.1 и выше;
- Mozilla Firefox версии 41.0.1 и выше;
- Opera версии 29.0.1795.60 и выше;

Так же возможен доступ с использование инструментов командной строки:

- Curl версии 7.61.1 и выше;
- Wget версии 1.19.5 и выше.

Операционная система, на которой запускается веб-браузер, может быть любой из поддерживаемых конкретной версией браузера.

3.2. Сервер Системы

3.2.1. Программное обеспечение

Для штатного функционирования Системы необходимо следующе ПО:

- ОС «Ubuntu 20.04»
- Контейнизатор приложений Docker версии 20.10.2 или более ранней

3.2.2. Аппаратное обеспечение

ПО «Гарда Сталкер» использует все доступные ресурсы аппаратного обеспечения для оптимальной скорости обезличивания и копирования данных.

Скорость копирования данных напрямую зависит от состава аппаратного обеспечения целевых серверов.

Минимальные требования к аппаратной части Системы не предъявляются.

3.3. Необходимые навыки пользователей

3.3.1. Пользователь Системы

Для эффективного использования функционала, Пользователь Системы должен обладать:

- Пониманием политики информационной безопасности предприятия
- Навыками работы с ПК

3.3.2. Администратор Системы

Для установки, настройки и обслуживания Системы сотруднику необходим опыт администрирования ОС «Ubuntu Linux».