ГАРДА

Гарда Монитор

Руководство администратора

garda.ai

2024

Тип документа:	Руководство администратора
Дата выпуска:	24.06.2024
Статус документа:	Released
Версия:	4.0

Содержание

1 Введение

1.1 Аннотация

Данный документ представляет собой Руководство администратора программного комплекса "Гарда Монитор" (далее – ПК "Гарда Монитор", Программный Комплекс, Комплекс).

1.2 Аудитория

Документ предназначен для администраторов программного комплекса "Гарда Монитор". Материал, изложенный в документе, предполагает у читателя наличие знаний сетевых технологий.

1.3 Использование имен, номеров телефонов, сетевых адресов

Приведенные в настоящем документе сведения о юридических и физических лицах, включая любые их данные, являются вымышленными, а IP-адреса и номера телефонов не соответствуют их действительным владельцам. Любые совпадения случайны.

1.4 О компании

Гарда Технологии (входит в группу компаний Гарда) – разработчик семейства продуктов в области защиты данных и сетевой безопасности. Решения Гарда защищают данные крупнейших государственных организаций и корпораций, защищают 50% всего российского интернета от DDoS-атак, обеспечивают защиту цифровых сервисов и мероприятий федерального масштаба. Продуктовый портфель холдинга построен на основе технологий собственной разработки, которые не требуют сторонних лицензий, включены в Единый реестр российского ПО и сертифицированы ФСТЭК.

1.5 Техническая поддержка

По всем вопросам, связанным с работой продукта, обращайтесь в Службу технической поддержки компании "Гарда Технологии":

- Тел. +7 (831) 422-12-20 (с 9-00 до 18-00 по Московскому времени).
- Email: gm.support@gardatech.ru.

2 Обзор

2.1 Назначение Комплекса

ПК «Гарда Монитор» – это комплекс, предназначенный для аудита сетевых соединений на транспортном и прикладном уровнях. Программный комплекс анализирует соединения с помощью:

- Глубокого разбора сетевых пакетов (DPI – Deep Packet Inspection).
- Сигнатурного анализа (IDS – Intrusion Detection System).
- Поведенческой аналитики (EBA – Entity Behavior Analytics).
- Индикаторов компрометации (IoC – Indicator of Compromise).
- Журнала авторизаций (Мониторинг авторизаций пользователей в домене).

Результаты аудита сохраняются в виде объектов, доступных для последующего просмотра и анализа. В случае если сетевое соединение удовлетворяет заданным параметрам (Политикам информационной безопасности), Комплекс автоматически информирует об этом службу безопасности. Комплекс обеспечивает длительное хранение собранных данных для ретроспективного анализа.

Решение предназначено для использования службами информационной безопасности предприятий.

2.2 Структура Комплекса и принцип работы

ПК «Гарда Монитор» состоит из следующих функциональных подсистем:

- подсистема съема трафика. Обеспечивает сбор зеркалированной копии трафика по технологии SPAN (ERSPAN/GRE) с анализом содержимого сетевых пакетов и применением сигнатурного анализа, прием статистики по протоколам NetFlow/sFlow и преобразование имени хоста в ip-адрес с помощью DNS-сервера;
- подсистема интеграции с журналом событий контроллера домена. Обеспечивает получение информации о событиях авторизации пользователей на рабочих станциях;
- подсистема анализа и хранения. Выполняет обогащение и сохранение данных, полученных от подсистемы съема трафика. Реализует функцию обнаружения новых устройств и сервисов, и выявления отклонений в профилях поведения наблюдаемых устройств;

- подсистема управления. Обеспечивает предоставление единого интерфейса, выполняет агрегацию пользовательских запросов, а также отвечает за автоматическое обновление баз данных сигнатур, индикаторов компрометации и прочей справочной информации.

Весь объем перехватываемых событий помещается в подсистему анализа и хранения, откуда пользователь в любое время может извлекать необходимые объекты с помощью фильтрации по заданным параметрам.

2.3 Задачи администрирования Комплекса

В обязанности администратора ПК "Гарда Монитор" входит:

- Подготовка сети предприятия к установке Комплекса.
- Пост-инсталляционные настройки Комплекса.
- Изменение настроек Комплекса.
- Диагностика состояния Комплекса и исправление проблем.

3 Подготовка к установке Комплекса

3.1 Подготовка сети предприятия к установке Комплекса

Подготовка сети предприятия к установке ПК "Гарда Монитор" заключается в следующем:

1. Подготовка точки съема трафика.
2. Выбор способа подачи трафика.
3. Подготовка необходимых настроек на контроллере домена для персонификации трафика (в случае необходимости).
4. Подготовка сервера для установки Комплекса.
5. Подготовка необходимых данных для интеграции Комплекса.

3.2 Подготовка сервера для установки системы

Необходимо подготовить сервер для установки ПК "Гарда Монитор".

ПК «Гарда Монитор» устанавливается на серверные аппаратные платформы с характеристиками не ниже:

- Количество процессоров – от 2x Intel Xeon Silver;
- Количество ядер – от 16;
- Объем оперативной памяти – от 32 ГБ;
- Логическая емкость дискового пространства – от 10 ТБ;
- Сетевые интерфейсы – от 2x*1Гб.

Более точно выбор аппаратных характеристик сервера для функционирования Изделия осуществляется на основании требований по скорости обработки трафика.

Возможна установка ПК "Гарда Монитор" в виртуальной среде. Требования к ресурсам платформы виртуализации аналогичные. При внедрении на платформе виртуализации необходимо обеспечить наличие выделенных физических Ethernet-портов для приема трафика.

3.3 Подготовка необходимых данных для интеграции Комплекса

Перед установкой Комплекса следует выполнить следующие действия:

1. Подготовить сетевые настройки для ПК "Гарда Монитор" (IP-адрес, шлюз, адрес DNS-сервера).
2. При необходимости персонификации трафика выполнить настройки контроллера домена. Для получения инструкций обратитесь в Службу технической поддержки.
    2.1. Необходимо подготовить список адресов контроллеров доменов, прокси-серверов, точек доступа wi-fi, терминальных серверов. Для корректной персонификации трафика адреса данных сервисов добавляются в исключения персонификации.
3. Открыть необходимые порты для корректной работы комплекса.

4 Запуск Комплекса

После успешной установки Комплекса для доступа к веб-интерфейсу выполните следующее:

1. Откройте рекомендуемый веб-браузер Google Chrome.
2. В адресной строке веб-браузера введите http://IP-address, где IP-address – это IP-адрес сервера "Гарда Монитор".
3. В открывшемся окне укажите имя пользователя и пароль в соответствующих полях.
   Имя пользователя и пароль для входа в Комплекс необходимо запросить в службе технической поддержки.

> ***Примечание:*** *После первого входа в Комплекс рекомендуется сразу же сменить пароль предустановленного пользователя* ***Администратор комплекса*** *(логин* ***admin****).*

4. Нажмите кнопку **Войти**.

На экране появится главная страница веб-интерфейса ПК "Гарда Монитор".