ГАРДА

Гарда Монитор

Руководство пользователя

garda.ai

2024

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

Содержание

1 Введение 4
1.1 Аннотация 4
1.2 Аудитория 4
1.3 Использование имен, номеров телефонов, сетевых адресов 4
1.4 О компании 4
1.5 Техническая поддержка 4
2 Обзор 5
2.1 Назначение Комплекса 5
2.2 Структура Комплекса и принцип работы 5
2.3 Функциональные возможности 6
2.4 Возможности интерфейса пользователя 7
2.5 Масштабируемость Комплекса 8
2.6 Надежность Комплекса 8
3 Работа с Комплексом 9
3.1 ПО для работы пользователя 9
3.2 Вход в Комплекс 9
3.3 Общий вид интерфейса Комплекса 10

1 Введение

1.1 Аннотация

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

1.2 Аудитория

Документ предназначен для пользователей 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

Программный комплекс «Гарда Монитор» предназначен для мониторинга IP-трафика локальной сети, анализа содержимого сетевых соединений, ведения архива объектов и событий информационного обмена с возможностью ретроспективного анализа.

Основные задачи, решаемые Комплексом:

- долгосрочное хранение копии сетевого трафика, с возможностью выгрузки интересующих сессий в формате PCAP;
- обнаружение сетевых атак;
- обнаружение обращений к вредоносным ресурсам;
- мониторинг появления и исчезновения новых устройств и служб в заданном сегменте сети;
- построение профилей поведения устройств. Выявление отклонений в поведении устройства от его профиля.

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;
- 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.

Комплекс поддерживает различные варианты компоновки:

- совмещенная компоновка: все подсистемы установлены на одной серверной аппаратной платформе или платформе виртуализации;
- разнесенная компоновка: подсистемы разнесены на разные серверные аппаратные платформы или платформы виртуализации, связанные между собой информационной вычислительной сетью.

ПК «Гарда Монитор» определяет события безопасности, относящиеся к следующим типам:

- Разведка (Reconnaissance);
- Подготовка ресурсов (Resource Development);
- Первоначальный доступ (Initial Access);
- Выполнение (Execution);
- Закрепление (Persistence);
- Повышение привилегий (Privilege Escalation);
- Предотвращение обнаружения (Defense Evasion);
- Получение учетных данных (Credential Access);
- Изучение (Discovery);
- Перемещение внутри периметра (Lateral Movement);
- Сбор данных (Collection);
- Организация управления (Command and Control);
- Эксфильтрация данных (Exfiltration);
- Деструктивное воздействие (Impact).

Данные типы соответствуют тактикам матрицы MITRE ATT&CK, которая описывает тактики и техники, которыми злоумышленники пользуются в своих атаках на корпоративную инфраструктуру.

2.3 Функциональные возможности

ПК «Гарда Монитор» выполняет следующие функциональные возможности:

- запись, категоризация и хранение IP-трафика;
- многокритериальный поиск по сохраненным данным с возможностью получения копии записанного трафика в формате PCAP;
- анализ содержимого сетевых пакетов;
- обнаружение событий информационной безопасности на основе сигнатурного анализа и модели машинного обучения;

- обнаружение фактов сканирования сети предприятия и нелегитимной сетевой активности, а также признаков вредоносного программного обеспечения;
- анализ трафика на наличие индикаторов компрометации;
- обнаружение фактов обращения к скомпрометированным ресурсам на основе принадлежности к репутационным спискам IP-адресов, доменных имен и URL-адресов;
- выявление аномальной сетевой активности устройств;
- информирование о появление новых устройств, сервисов и портов получателей в заданном сегменте сети;
- отображение данных об авторизациях сотрудников на компьютерах предприятия;
- построение карты сети в виде графического представления взаимодействия сетевых устройств;
- интеграция с внешними системами;
- запись в журналы действий пользователей и системных сообщений о работе компонентов ОО;
- автоматическое обновление баз данных сигнатур ОО.

2.4 Возможности интерфейса пользователя

Интерфейс пользователя обеспечивает:

- Поиск по свойствам, извлеченным из сетевых потоков с возможностью получения исходного сетевого потока в формате PCAP.
- Построение графиков и диаграмм по интересующим срезам информации.
- Отображение информации и событий Информационной безопасности.
- Быстрая навигация от информации о событии к содержащему его потоку.
- Отображение профилей поведения устройств.
- Отображение информации о появлении/исчезновении устройств и сервисов в заданных сегментах сети.
- Отображение сетевых взаимодействий на карте сети.
- Одновременный поиск во всех хранилищах данных.

2.5 Масштабируемость Комплекса

Масштабирование Комплекса подразумевает возможность использования нескольких анализаторов, расположенных в разных сегментах сети и передающих данные на подсистему управления.

2.6 Надежность Комплекса

- Круглосуточная работа 24/7 в необслуживаемом режиме.
- Коэффициент готовности Комплекса – 99,0%.

3 Работа с Комплексом

3.1 ПО для работы пользователя

Доступ к графическому веб-интерфейсу осуществляется с использованием одного из следующих браузеров:

- Google Chrome версии 120.0.6099.130 и выше;
- Яндекс Браузер версии 23.11.1.731 и выше;
- Mozilla Firefox 121.0 и выше;
- Opera 106.0.4998.16 и выше.

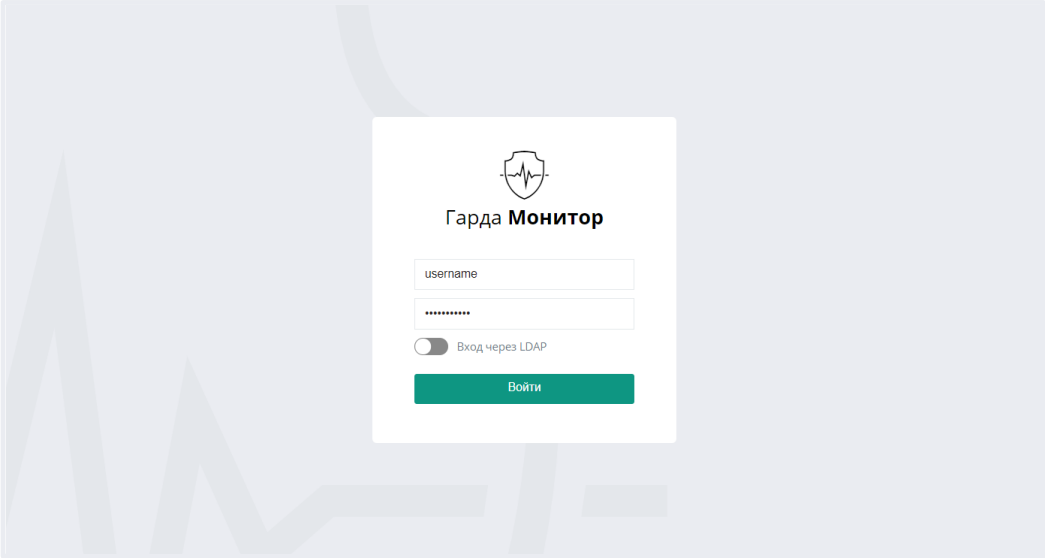
3.2 Вход в Комплекс

Для доступа к веб-интерфейсу Комплекса выполните следующие действия:

1. Откройте рабочий веб-браузер.
2. В адресной строке веб-браузера введите http://IP-address, где IP-address – это IP-адрес, указанный администратором.
3. В открывшемся окне укажите имя пользователя и пароль.
   - Для входа в Комплекс при помощи доменной учетной записи активируйте переключатель **Вход через LDAP** и укажите имя пользователя и пароль доменной учетной записи.
4. Нажмите кнопку **Войти**.

Примечание: *Функция доменной авторизации доступна только при настроенной синхронизации с сервером службы каталогов. Настройка синхронизации с сервером службы каталогов описана в документе Руководство администратора раздел Аутентификация через LDAP.*

Примечание: *После 10 неуспешных попыток входа в Комплекс доступ к форме для входа блокируется на 10 минут.*



На экране появится раздел веб-интерфейса **Главная**.

3.3 Общий вид интерфейса Комплекса

Веб-интерфейс Комплекса содержит следующие основные области:

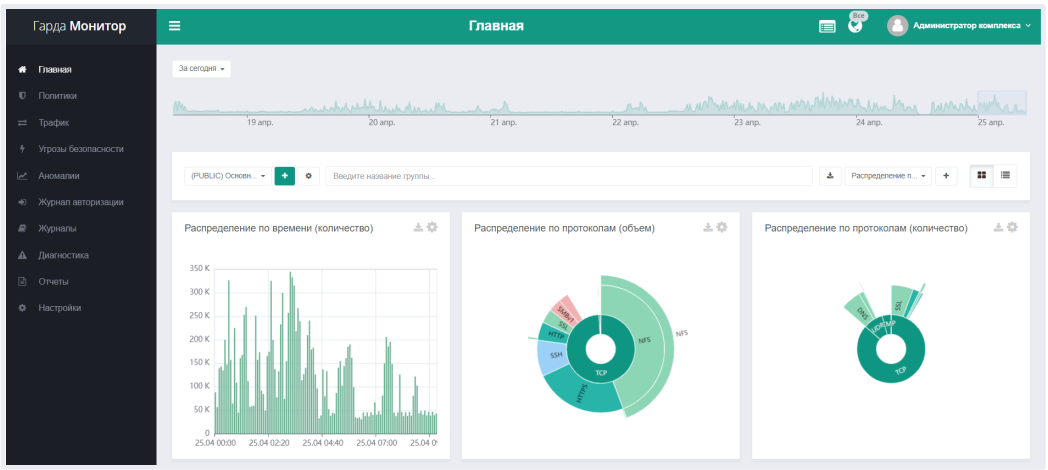
1. В левой части веб-интерфейса расположена панель меню, которая содержит список разделов, доступных пользователю Комплекса:
   - **Главная** - отображает статистическую информацию о работе Комплекса.
   - **Политики** - содержит политики информационной безопасности и отображает события, обнаруженные в рамках данных политик.
   - **Трафик** - содержит инструменты для поиска и просмотра информации о сетевых событиях.
   - **Угрозы безопасности** - содержит инструменты для поиска и просмотра информации о фактах сетевой разведки и угрозах безопасности.
   - **Аномалии** - содержит инструменты для поиска и просмотра информации об аномальных сетевых событиях, а также информацию о появлении новых устройств и сервисов.
   - **Журнал авторизации** - содержит инструменты для поиска и просмотра информации об авторизациях сотрудников на компьютерах предприятия.
   - **Журнал** - содержит журнал действий пользователей.
   - **Диагностика** - содержит инструменты для диагностики комплекса.
   - **Отчеты** - содержит список отчётов, которые создаются по заданному пользователем расписанию.

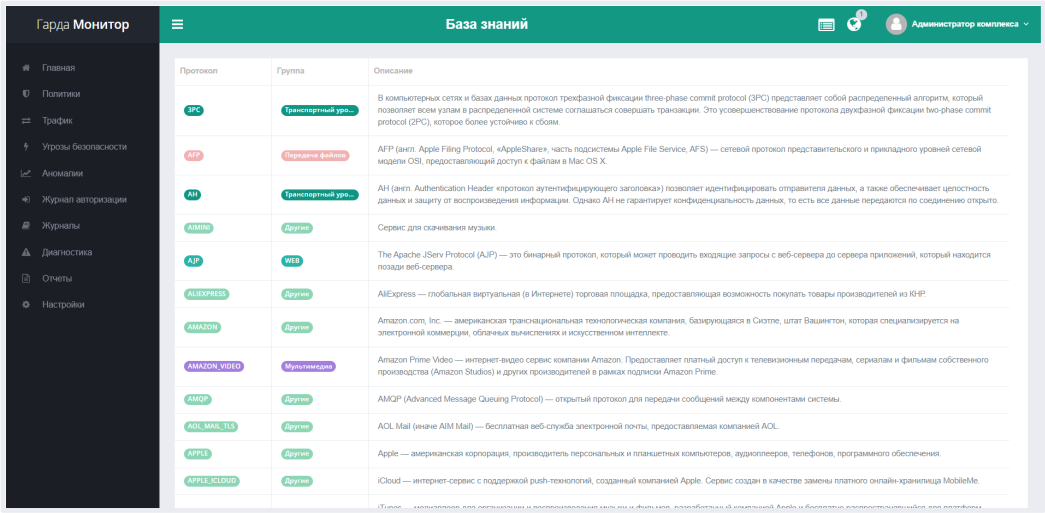
- **Настройки** - содержит настройки учетных записей пользователей Комплекса, настройки списков хостов, IP-адресов, Email-адресов и URL-адресов, логические группы, протоколы, настройки экспорта данных в SIEM-систему, решающие правила, профили мониторинга и прочие настройки.

2. В правой части веб-интерфейса расположена область отображения данных в соответствии с выбранным в меню разделом.

В правом верхнем углу находятся следующие элементы:

-  - загрузка файлов PCAP. Данная кнопка отображается в веб-интерфейсе при наличии соответствующих настроек. Подробнее см. *Руководство администратора* раздел *Загрузка файлов PCAP*.
-  - выбор филиалов, данные по которым будут отображаться в веб-интерфейсе. Подробнее см. *Руководство администратора* раздел *Филиалы*. При выборе тех или иных филиалов данные в веб-интерфейсе сразу же обновляются.
-  - имя пользователя, по нажатию на которое раскрывается список со следующими пунктами:
  - **Справка** - вызывает Руководство пользователя, Руководство администратора и **Базу знаний** - таблицу с описанием протоколов.
  - **О программе** - содержит информацию о версии, лицензии лицензии и целостности Комплекса.
  - **Изменить пароль** - открывает окно изменения пароля.
  - **Выход** - кнопка выхода из Комплекса.
- запросы других пользователей Комплекса.




Гарда Монитор
Главная
Политики
Трафик
Угрозы безопасности
Аномалии
Журнал авторизации
Журналы
Диагностика
Отчеты
Настройки
База знаний
Администратор комплекса
Протокол
Группа
Описание
3PC
Транспортный уро...
В компьютерных сетях и базах данных протокол трехфазной фиксации three-phase commit protocol (3PC) представляет собой распределенный алгоритм, который позволяет всем узлам в распределенной системе соглашаться совершать транзакции. Это усовершенствование протокола двухфазной фиксации two-phase commit protocol (2PC), которое более устойчиво к сбоям.
AFP
Передача файлов
AFP (англ. Apple Filing Protocol, «AppleShare», часть подсистемы Apple File Service, AFS) — сетевой протокол представительского и прикладного уровней сетевой модели OSI, предоставляющий доступ к файлам в Mac OS X.
AH
Транспортный уро...
AH (англ. Authentication Header «протокол аутентифицирующего заголовка») позволяет идентифицировать отправителя данных, а также обеспечивает целостность данных и защиту от воспроизведения информации. Однако AH не гарантирует конфиденциальность данных, то есть все данные передаются по соединению открыто.
AIMINI
Другие
Сервис для скачивания музыки.
AJP
WEB
The Apache JServ Protocol (AJP) — это бинарный протокол, который может проводить входящие запросы с веб-сервера до сервера приложений, который находится позади веб-сервера.
ALIEXPRESS
Другие
AliExpress — глобальная виртуальная (в Интернете) торговая площадка, предоставляющая возможность покупать товары производителей из КНР.
AMAZON
Другие
Amazon.com, Inc. — американская транснациональная технологическая компания, базирующаяся в Сиэтле, штат Вашингтон, которая специализируется на электронной коммерции, облачных вычислениях и искусственном интеллекте.
AMAZON_VIDEO
Мультимедиа
Amazon Prime Video — интернет-видео сервис компании Amazon. Предоставляет платный доступ к телевизионным передачам, сериалам и фильмам собственного производства (Amazon Studios) и других производителей в рамках подписки Amazon Prime.
AMQP
Другие
AMQP (Advanced Message Queuing Protocol) — открытый протокол для передачи сообщений между компонентами системы.
AOL_MAIL_TLS
Другие
AOL Mail (иначе AIM Mail) — бесплатная веб-служба электронной почты, предоставляемая компанией AOL.
APPLE
Другие
Apple — американская корпорация, производитель персональных и планшетных компьютеров, аудиоплееров, телефонов, программного обеспечения.
APPLE_ICLOUD
Другие
iCloud — интернет-сервис с поддержкой push-технологий, созданный компанией Apple. Сервис создан в качестве замены платного онлайн-хранилища MobileMe.