Positive Technologies Industrial Security Incident Manager

Руководство по установке

POSITIVE TECHNOLOGIES

Содержание

1. Об этом документе

Руководство по установке содержит инструкции и справочную информацию об установке, первоначальной настройке, обновлении и удалении Positive Technologies Industrial Security Incident Manager (далее также — PT ISIM). Руководство не содержит инструкций по использованию основных функций продукта.

Руководство адресовано специалистам, выполняющим установку и администрирование PT ISIM в организации.

Комплект документации PT ISIM включает в себя следующие документы:

- Этот документ.
- Руководство оператора безопасности — содержит сценарии использования продукта для управления информационными активами организации и событиями информационной безопасности.

В этом разделе

1.1. Условные обозначения

В этом документе могут встречаться условные обозначения (см. таблицу 1).

Таблица 1. Условные обозначения

Пример текста с условным обозначением	Описание
Внимание! При выключении модуля снижается уровень защищенности сети...	Предупреждения. Содержат информацию о действиях или событиях, которые могут иметь нежелательные последствия
Примечание. Вы можете создать дополнительные отчеты...	Примечания. Содержат советы, описания важных частных случаев, дополнительную или справочную информацию, которая может быть полезна при работе с продуктом
Нажмите кнопку **OK**.	Названия элементов интерфейса (например, кнопок, полей, пунктов меню) выделены полужирным шрифтом
Выполните команду `Stop-Service`	Текст командной строки, примеры кода, прочие данные, которые нужно ввести с клавиатуры, выделены специальным шрифтом
Ctrl+Alt+Delete	Комбинация клавиш. Чтобы использовать комбинацию, клавиши нужно нажимать одновременно

Пример текста с условным обозначением	Описание
<Название программы>	Переменные заключены в угловые скобки

1.2. Другие источники информации о продукте

Вы можете найти дополнительную информацию о "Позитив Текнолоджиз" на www.ptsecurity.com и на портале технической поддержки support.ptsecurity.com.

Портал support.ptsecurity.com содержит статьи базы знаний, новости обновлений продуктов ЗАО "Позитив Текнолоджиз", ответы на часто задаваемые вопросы пользователей. Для доступа к базе знаний и всем новостям нужно создать учетную запись на портале.

Если вы не нашли нужную информацию или решение проблемы самостоятельно, обратитесь в службу технической поддержки (см. раздел 5.).

2. О PT ISIM

Positive Technologies Industrial Security Incident Manager (PT ISIM) — это программно- аппаратный комплекс для обеспечения кибербезопасности автоматизированных систем управления технологическим процессом (АСУ ТП).

Основные функции PT ISIM:

- анализ трафика с целью обнаружения атак на промышленную сеть;
- снижение рисков возникновения таких угроз информационной безопасности, как несанкционированное подключение, атаки методом перебора пароля, неправомерные управляющие команды и подмена прошивки промышленного оборудования;
- расследование инцидентов, включая ретроспективный анализ на основе сохраненной копии трафика.

3. Принцип работы PT ISIM

Ниже приводится основная информация о принципе работы PT ISIM.

В этом разделе

3.1. Алгоритм обработки трафика

PT ISIM анализирует сетевой трафик и выявляет инциденты на основе правил корреляции и моделирования.

Обработка трафика в PT ISIM происходит в несколько этапов:

1. Сбор — захват трафика по протоколам FTP, HTTP, Telnet, ARP, MMS, МЭК 104, DIGSI, GOOSE, NTP, SNTP, а также по протоколам Bombardier (COS и FEU) с целью извлечения информации о каждом событии. Собранная информация передается на нормализацию, а исходная копия трафика сохраняется на жестком диске сервера в формате Pcap.
2. Нормализация — извлечение данных из атрибутов записей, которые могут иметь разный формат, и приведение их к единому формату нормализованных сообщений. Нормализованное сообщение имеет заданный набор полей, каждое из которых имеет определенные допустимые значения. Такой формат сообщения позволяет однозначно определить основные параметры события, отнести его к определенному узлу и устройству, а также провести дальнейший анализ события на основе значений отдельных полей.
3. Фильтрация — удаление сообщений, не представляющих интереса с точки зрения информационной безопасности.
4. Агрегация — группировка повторяющихся сообщений об однотипных событиях в единое сообщение согласно правилам агрегации. Правила агрегации определяют набор полей, совпадение по которым приводит к группировке нескольких сообщений в одно, а также период, на который распространяется агрегация.
5. Корреляция — проверка потока событий на соответствие определенному правилу. Результатом сработавшего правила корреляции является скоррелированное сообщение.
6. Моделирование — составление актуальной карты вычислительной сети, отражающей ее реальный состав и взаимодействие между узлами. На основе правил, учитывающих текущие данные модели, PT ISIM принимает решение о том, является ли событие или скоррелированное сообщение инцидентом.

Итогом обработки трафика является заведение записей о событиях и инцидентах в PT ISIM.

3.2. Безопасность хранения и передачи данных

Безопасность хранения и передачи данных при работе с PT ISIM имеет два аспекта:

- Исключается любое воздействие PT ISIM на технологические процессы предприятия, поскольку для сбора трафика PT ISIM подключается к SPAN-портам коммутаторов через диод данных. Подобное решение делает невозможным передачу данных от PT ISIM в сеть АСУ ТП как при нормальной работе продукта, так и в случае непредвиденного изменения настроек коммутатора или PT ISIM.
- Используются следующие инструменты обеспечения собственной безопасности PT ISIM:
  - Сценарий secure.sh. Его запуск реализует настраивает межсетевой экран таким образом, что запрещаются любые соединения с внешней сетью, кроме входящих TCP-соединений на порты 22, 80, 443 и входящих IMCP-соединений (эхо-запросов), а также ограничивает доступ к компонентам Redis и RabbitMQ, устанавливая пароли и разрешая соединения только в пределах сервера.
  - Защищенное соединение с веб-интерфейсом пользователя по HTTPS, а также перенаправление запросов, адресованных порту 80 (HTTP), на порт 443 (HTTPS).
  - Компонент Firewall, который предотвращает изменение настроек межсетевого экрана или его отключение.
  - Мониторинг состояния сетевого подключения PT ISIM к коммутаторам, с которых собирается трафик. Отсутствие подключения рассматривается как инцидент.
  - Мониторинг состояния компонентов Redis и RabbitMQ. Служба Watchdog периодически отправляет им запросы и принудительно перезапускает их, если они не отвечают на запросы в течение заданного времени или отвечают сообщением с ошибкой.

4. Установка PT ISIM

В этом разделе содержатся инструкции, необходимые для установки PT ISIM.

В этом разделе

4.1. Подготовка к установке

Чтобы подготовить сервер к установке PT ISIM:

1. Установите операционную систему Debian версий 8.2—8.5 AMD64. Подробнее об установке ОС Debian см. Сетевая установка с минимальным компакт-диском.

   Во время установки ОС Debian:

   - Выберите UTC в качестве часового пояса.
   - На этапе выбора и установки программного обеспечения выберите для установки стандартные системные утилиты (Standard system utilities) и SSH-сервер; исключите из устанавливаемых пакетов среду рабочего стола (desktop), веб-сервер (web-server) и сервер печати (print-server).
2. Убедитесь, что выполняются следующие условия:
   - наличие прав пользователя root в ОС Debian;
   - наличие соединения с интернетом.

4.2. Процедура установки

Чтобы установить PT ISIM, выполните следующие шаги:

1. Распакуйте архив, содержащий deb-пакет PT ISIM и вспомогательные сценарии.

   ```
   tar -xvf isim.<номер_версии_PT_ISIM>.tar.gz
   ```
2. Запустите сценарий prepare.sh.

   Данный сценарий выполняет предварительную настройку сервера и устанавливает следующие сторонние компоненты:

   - Redis — СУБД, необходимая для хранения активных списков;
   - RabbitMQ — компонент, реализующий функцию шины передачи данных;
   - nginx — веб-сервер, принимающий и обрабатывающий HTTPS-запросы от клиентского ПО (браузера пользователя).
3. Убедитесь, что запущены сервисы rabbitmq-server, redis-server, nginx, выполнив для каждого из них следующую команду:

   ```
   systemctl status -l <имя_сервиса>.service
   ```

   Пример:

   ```
   systemctl status -l nginx.service
   ```

Статус сервиса в ответном сообщении должен быть `Active: active (running)`. Если статус сервиса отличается (например, имеет вид `Active: failed`), обратитесь в техническую поддержку "Позитив Текнолоджиз".

4. Установите deb-пакет с PT ISIM, выполнив следующую команду:

   ```
   dpkg -i ptisim_<номер_версии_PT_ISIM>/ptisim_<номер_версии_PT_ISIM>.deb
   ```

5. Для разрешения зависимостей выполните следующую команду:

   ```
   apt-get install -f
   ```

6. Настройте сетевой интерфейс для сбора трафика:
   - Откройте конфигурационный файл ptdpi:

     ```
     nano /opt/ptdpi/ptdpi.config
     ```

   - В параметре PTDPI_CAPTURE_IF смените значение eth0 на имя сетевого интерфейса, с которого необходимо собирать трафик.
7. Настройте утилиту мониторинга ARP-трафика Arpwatch:
   - Откройте файл с настройками Arpwatch:

     ```
     nano /etc/default/arpwatch
     ```

   - В секции ARGS добавьте `-i ethN`

   где `ethN` — имя сетевого интерфейса, добавленного на шаге 6.
8. Настройте компонент Goosewatch, отвечающий за разбор сообщений протокола GOOSE:
   - Откройте файл с настройками Goosewatch:

     ```
     nano /opt/ptisim/etc/goosewatch.conf
     ```

   - В параметре `iface` замените значение по умолчанию (lo) на имя сетевого интерфейса, с которого необходимо собирать трафик.
9. Запустите сценарий secure.sh.

   Данный сценарий выполняет настройку безопасности сервера (межсетевого экрана, доступа к компонентам Redis и RabbitMQ).

4.3. Проверка работы PT ISIM

Для проверки корректности установки PT ISIM выполните вход в веб-интерфейс продукта (см. раздел 6). На главной странице должен отображаться обрабатываемый трафик в виде списка событий (см. рисунок 2).

Если события не отображаются, выполните следующие действия:

1. Установите утилиту анализа сетевого трафика tcpdump:

   ```
   apt-get install tcpdump
   ```

2. Выполните команду:

   ```
   tcpdump -nli ethN
   ```

   где `ethN` — имя сетевого интерфейса, с которого необходимо собирать трафик.

Если на указанном сетевом интерфейсе действительно проходит трафик, в результате выполнения данной команды будут отображаться сведения о перехватываемых сетевых пакетах.

Обнаружение трафика утилитой tcpdump и его отсутствие в интерфейсе пользователя PT ISIM свидетельствует о некорректной установке или настройке продукта. В таком случае обратитесь в техническую поддержку "Позитив Текнолоджиз".

Если утилита tcpdump также не обнаружила трафик, проверьте корректность подключения к коммутатору, трафик с которого необходимо собирать, исправность и подключенность Ethernet-кабеля, а также убедитесь в том, что узлы сети обмениваются данными.

5. Обращение в службу технической поддержки

Техническая поддержка продукта включает в себя следующие услуги:

- решение вопросов эксплуатации продукта, помощь в использовании его функциональных возможностей;
- диагностику сбоев продукта, включая поиск причины сбоя и информирование клиента о найденных проблемах;
- разрешение проблем с продуктом, предоставление решений или возможностей обойти проблему с сохранением всей необходимой производительности;
- устранение ошибок в продукте (в рамках выпуска обновлений к продукту).

Вы можете получать техническую поддержку на портале support.ptsecurity.com или по телефону. Заявки на портале являются основным каналом обработки обращений за технической поддержкой.

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

В этом разделе

5.1. Техническая поддержка на портале

Портал support.ptsecurity.com предоставляет вам возможность создавать заявки на техническую поддержку.

Вы можете создать учетную запись на портале, используя адреса электронной почты, расположенные на официальном домене вашей организации. Вы также можете указывать другие адреса электронной почты для учетной записи в качестве дополнительных. Для оперативной связи укажите в профиле учетной записи название вашей организации и контактный телефон.

Портал support.ptsecurity.com содержит статьи базы знаний, новости обновлений продуктов ЗАО "Позитив Текнолоджиз", ответы на часто задаваемые вопросы пользователей. Для доступа к базе знаний и всем новостям нужно создать учетную запись на портале.

Портал технической поддержки доступен на русском, английском, немецком и итальянском языках.

5.2. Техническая поддержка по телефону

Вы можете связаться со службой технической поддержки по следующим телефонам:

- Великобритания +44 203 769 3606.
- США +1 857 208 7273.

- Италия +39 0 697631532.
- Швеция +46 8 121 111 86
- Южная Корея +82 264 108 582.
- Россия +7 495 744 01 44.

Техническая поддержка по телефону предоставляется на русском и английском языке.

Сотрудники технической поддержки по телефону могут выполнить оперативную диагностику, ответить на простые вопросы или уточнить текущий статус работ по ранее созданной заявке.

Если решить вопрос по телефону в разумное время (15—20 минут) невозможно, создайте заявку на портале support.ptsecurity.com. Заявка на портале, созданная и обновляемая по рекомендациям специалиста технической поддержки, гарантирует дальнейшие работы по вашему обращению.

5.3. Время работы технической поддержки

На портале технической поддержки вы можете круглосуточно создавать и обновлять заявки, читать новости продуктов и пользоваться базой знаний. Сотрудники технической поддержки работают по имеющимся заявкам и принимают обращения по телефону с понедельника по пятницу с 9:00 до 19:00 UTC+3.

5.4. Как служба технической поддержки работает с заявками

При получении вашей заявки специалист службы технической поддержки классифицирует инцидент, указанный в заявке (присваивает инциденту тип и уровень значимости) и выполняет дальнейшие шаги по разрешению инцидента.

В этом разделе

- Предоставление информации для технической поддержки (см. раздел 5.4.1.)
- Типы инцидентов (см. раздел 5.4.2.)
- Время реакции на обращение и приоритизация инцидентов (см. раздел 5.4.3.)
- Выполнение работ по заявке (см. раздел 5.4.4.)

5.4.1. Предоставление информации для технической поддержки

При обращении за технической поддержкой по первому требованию специалиста ЗАО "Позитив Текнолоджиз" нужно предоставить:

- номер лицензии на использование продукта;
- файлы журналов и другие наборы диагностических данных, хранящихся в продукте;
- снимки экрана;
- результаты выполнения рекомендаций специалиста технической поддержки;

- каналы для удаленного доступа к продукту (по взаимному согласованию оптимального канала диагностики).

ЗАО "Позитив Текнолоджиз" не несет обязательств по оказанию технической поддержки в случае отказа предоставить указанную выше информацию.

Если информация по обращению не предоставлена в течение значительного времени (от двух недель с момента последней активности), специалист технической поддержки имеет право считать ваше обращение неактуальным и, уведомив вас, закрыть заявку.

5.4.2. Типы инцидентов

Специалист технической поддержки относит инцидент в вашей заявке к одному из следующих типов.

Вопросы по установке, повторной установке и предстартовой настройке продукта

Подразумевается помощь в подготовке продукта к работе, ответы на вопросы на данном этапе эксплуатации продукта. Техническая поддержка по этим вопросам доступна в течение 30 дней с момента активации продукта.

Вопросы по администрированию и настройке продукта

Включают в себя вопросы, возникающие в процессе эксплуатации продукта, рекомендации по оптимизации и настройке параметров продукта.

Восстановление работоспособности продукта

В случае критического сбоя и потери доступа к основной функциональности продукта специалист ЗАО "Позитив Текнолоджиз" оказывает помощь в восстановлении работоспособности продукта. Восстановление заключается либо в помощи по установке продукта заново с потенциальной потерей накопленных до сбоя данных, либо в откате продукта на доступную резервную копию (резервное копирование должно быть настроено заблаговременно). ЗАО "Позитив Текнолоджиз" не несет ответственность за потерю данных в случае неверно настроенного резервного копирования.

Обновление продукта

ЗАО "Позитив Текнолоджиз" поставляет пакеты обновления продукта в течение срока действия лицензии на продукт. ЗАО "Позитив Текнолоджиз" не несет ответственности за инциденты, возникшие при нарушении регламентированного процесса обновления.

Устранение дефектов продукта

Если по результатам диагностики обнаружен дефект продукта, ЗАО "Позитив Текнолоджиз" обязуется предпринять разумные усилия по предоставлению обходного решения (если возможно), а также включить исправление дефекта в ближайшие возможные обновления продукта.

5.4.3. Время реакции на обращение и приоритизация инцидентов

Время реакции на ваше обращение рассчитывается как время с момента получения от вас информации по обращению до ответа специалиста технической поддержки с описанием дальнейших шагов по разрешению инцидента. Время реакции зависит от указанного вами уровня значимости инцидента (см. таблицу ниже). Специалист технической поддержки может переопределять уровень значимости инцидента по приведенным ниже критериям. Значения сроков являются целевыми и подразумевают стремление и разумные усилия специалистов ЗАО "Позитив Текнолоджиз" для их соблюдения, но возможны отклонения от данных сроков по объективным причинам.

Таблица 2. Время реакции технической поддержки на обращение

Уровень значимости инцидента	Критерии значимости инцидента	Время реакции на обращение по инциденту
Критический	Аварийные сбои, полностью препятствующие штатной работе продукта (исключая первоначальную установку) либо оказывающие критическое влияние на бизнес	До 2 часов
Высокий	Сбои, затрагивающие часть функциональности продукта и проявляющиеся в любых условиях эксплуатации либо оказывающие значительное влияние на бизнес	До 4 часов
Обычный	Сбои, проявляющиеся в специфических условиях эксплуатации продукта либо не оказывающие значительное влияние на бизнес	До 8 часов
Низкий	Вопросы информационного характера либо сбои, не влияющие на эксплуатацию продукта	До 16 часов

Указанные часы относятся только к рабочему времени специалистов технической поддержки (времени обработки обращений).

5.4.4. Выполнение работ по заявке

По мере выполнения работ по вашей заявке специалист технической поддержки сообщает вам:

- о диагностике инцидента и ее результатах,
- поиске решения или возможности обойти причины возникновения инцидента,
- планировании и выпуске обновления продукта (если требуется для разрешения инцидента).

Если по итогам решения инцидента необходимо внести изменения в продукт, ЗАО "Позитив Текнолоджиз" включает работы по исправлению в ближайшее возможное плановое обновление продукта (в зависимости от сложности изменений).

Работы по заявке считаются выполненными, если:

- предоставлено решение или возможность обойти проблему, не влияющая на производительность и критически важную функцию продукта;
- инцидент диагностирован как дефект продукта, собрана техническая информация о дефекте и условиях его воспроизведения; исправление дефекта запланировано к выходу в рамках планового обновления продукта;
- инцидент идентифицирован как вызванный программными продуктами или оборудованием сторонних производителей и не подпадающий под гарантийные обязательства по продукту;
- инцидент классифицирован как неподдерживаемый.