Positive Technologies Anti-APT

Версия 1.0

Руководство по установке

POSITIVE TECHNOLOGIES

Дата редакции документа: 26.07.2019

Содержание

1. Об этом документе

Руководство по установке содержит информацию, касающуюся установки PT Anti-APT, и не содержит инструкций по настройке, администрированию и использованию основных функций продукта.

Руководство адресовано специалистам, выполняющим установку PT Anti-APT.

Комплект документации PT Anti-APT включает в себя следующие документы:

- Этот документ.
- Руководство администратора PT MS — содержит справочную информацию и инструкции по установке, настройке и администрированию PT MS.
- Руководство администратора PT NAD — содержит справочную информацию и инструкции по установке, настройке и администрированию PT NAD.
- Руководство оператора безопасности — содержит информацию об использовании PT Anti-APT для управления событиями информационными безопасности.
- Руководство оператора безопасности PT MS — содержит сценарии использования PT MS для управления событиями информационной безопасности.
- Руководство оператора безопасности PT NAD — содержит сценарии использования PT NAD для управления информационными активами организации и событиями информационной безопасности.

2. О PT Anti-APT

Positive Technologies Anti-APT (далее также — комплекс, PT Anti-APT) — программный комплекс, предназначенный для раннего выявления сложных угроз и сокращения присутствия злоумышленника в инфраструктуре. Комплекс позволяет максимально быстро обнаружить присутствие злоумышленника в сети и воссоздать полную картину атаки для детального расследования. Цели применения комплекса:

- предотвратить проникновение в инфраструктуру через основные векторы атак;
- максимально быстро выявлять присутствие злоумышленника в сети;
- повысить эффективность расследований благодаря возможности детально восстановить путь перемещения злоумышленника в сети;
- выявлять слабые места защиты и получать экспертные рекомендации для повышения уровня защищенности.

3. Архитектура PT Anti-APT

PT Anti-APT — это комплекс, объединяющий два компонента:

- Система обнаружения и предотвращения вторжений «Positive Technologies Network Attack Discovery» (далее также — PT NAD) для анализа трафика и выявления атак на периметре и внутри инфраструктуры;
- Система многопоточной проверки файловых ресурсов Positive Technologies MultiScanner (далее также — PT MS) для комплексного анализа файлов, передаваемых в почтовом, сетевом и веб-трафике.

В рамках анализа сетевого трафика комплекс выполняет следующие задачи:

- глубоко разбирает протоколы до уровня приложений;
- реконструирует сетевые сессии вне зависимости от наличия или отсутствия атаки;
- извлекает параметры сессии — IP-адреса и значения полей протоколов, репутацию передаваемых объектов, задействованные порты, приложения и другое;
- обнаруживает атаки и признаки компрометации с использованием различных технологий выявления;
- извлекает файлы, передаваемых в сетевом трафике;
- позволяет при необходимости хранить сырой трафик всей сессии, вне зависимости от наличия или отсутствия атаки;
- позволяет проводить ретроспективный анализ трафика на наличие атак в прошлом.

В рамках анализа передаваемых файлов комплекс выполняет следующие задачи:

- выявляет и блокирует вредоносное содержимое;
- осуществляет проверку на наличие вредоносного ПО с использованием баз знаний антивирусных вендоров;
- проверяет файлы с использованием репутационных списков;
- проводит динамический анализ в песочнице;
- формирует граф поведения анализируемых объектов;
- сохраняет все события, сгенерированные в ходе динамического анализа;
- проводит ретроспективный анализ для выявления вредоносного ПО в прошлом.

Алгоритм работы PT Anti-APT:

1. Комплекс анализирует зеркалируемый сетевой трафик и файлы на наличие признаков атак и вредоносного ПО. Комплекс анализирует файлы в следующих каналах:
    - пользовательском,
    - веб-канале;

- почтовом;
- каналах передачи файлов на хранилища.

2. По результатам анализа данные о выявленных атаках и образцах вредоносного ПО передаются команде ИБ организации. Информация может передаваться следующими способами:
    - уведомление на почту,
    - уведомление в веб-интерфейсе,
    - зафиксированное событие информационной безопасности, передаваемое в SIEM-систему для дальнейшей корреляции.
3. На основе переданных данных команда ИБ организации проводит дальнейшей анализ, чтобы определить ложное срабатывание или подтвердить и расследовать инцидент.
4. Команда PT Expert Security Center дополняет команду ИБ или полностью берет на себя задачи по мониторингу сетевого трафика и объектов и расследованию атак. Эксперты раз в две недели подключаются к комплексу:
    - для восстановления хронологии атаки,
    - оценки нанесенного ущерба,
    - выявления уязвимых мест в инфраструктуре,
    - формирования компенсирующих мер для предотвращения аналогичных атак,
    - сбора доказательной базы.

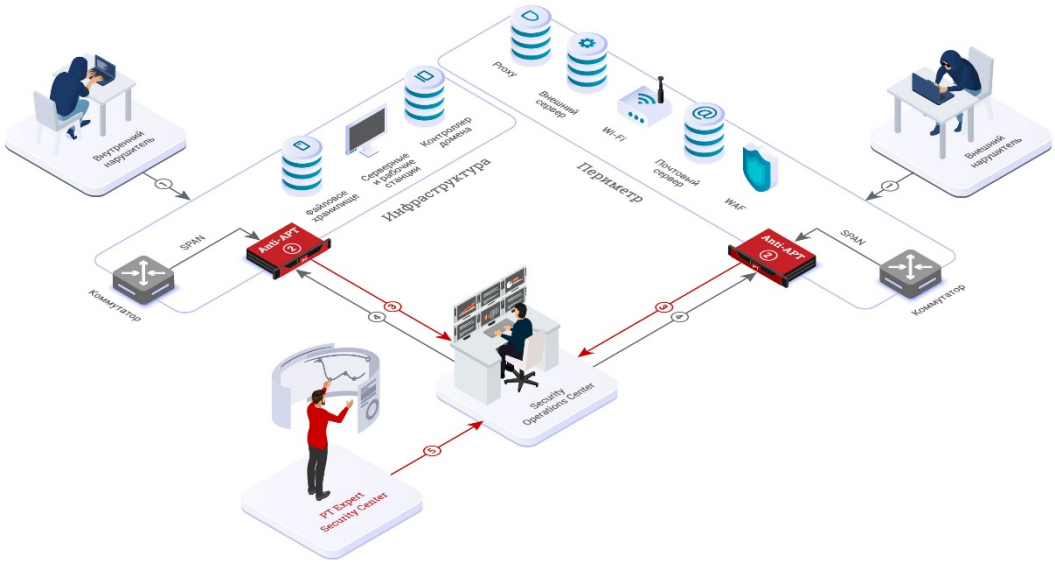

Рисунок 1. Алгоритм работы PT Anti-APT

4. Аппаратные и программные требования

Компоненты PT Anti-APT можно использовать как на физическом сервере, так и в виртуальной инфраструктуре.

Таблица 1. Аппаратные и программные требования

Компоненты комплекса	Компоненты сервера, программные компоненты	Минимальные требования	Рекомендуемые требования
PT NAD, установленный в виртуальной инфраструктуре[1]	Процессор	16 ядер	18 ядер
	ОЗУ	32 ГБ	48 ГБ
	Жесткий диск (SSD/SATA)	400 ГБ	350 ГБ/4096 ГБ
	Сетевая карта	2×Intel i350	2×Intel i350
	ОС	Ubuntu Server 16.04 x64;	Ubuntu Server 16.04 x64;
PT MS, установленный в виртуальной инфраструктуре	Процессор	4 ядра	16 ядер
	ОЗУ	13 ГБ	32 ГБ
	Жесткий диск (SSD/SATA)	200 ГБ	150 ГБ/2048 ГБ
	ОС	Ubuntu Server 18.04.1 x64	Ubuntu Server 18.04.1 x64
PT MS с модулем динамического анализа, установленный на физическом сервере (установка в виртуальной инфраструктуре невозможна)	Процессор	8 ядер	2×Intel Xeon Gold 5120 2.2GHz 14C/28T
	ОЗУ	16 ГБ	256 ГБ
	Жесткий диск (SSD/SATA)	300 ГБ	4×0.96TB (RAID 5)/4×4TB 7.2K RPM
	Сетевая карта	2×Intel i350	2×Intel i350
	ОС	Ubuntu Server 18.04.1 x64	Ubuntu Server 18.04.1 x64
PT MS, установленный на физическом сервере	Процессор	8 ядер	2×Intel Xeon Silver 4108 1.8GHz 8C/16T
	ОЗУ	16 ГБ	32 ГБ
	Жесткий диск (SSD/SATA)	300 ГБ	960 ГБ/4096 ГБ

[1] Использование PT NAD в виртуальной инфраструктуре возможно только при обработке трафика до 100 Мбит/с.

Компоненты комплекса	Компоненты сервера, программные компоненты	Минимальные требования	Рекомендуемые требования
	Сетевая карта	2×Intel i350	2×Intel i350
	ОС	Ubuntu Server 18.04.1 x64	Ubuntu Server 18.04.1 x64
PT NAD, установленный на физическом сервере	Процессор	2× Intel Xeon Silver 4108 1.8GHz 8C/16T	2×Intel Xeon Silver 4108 1.8GHz 8C/16T
	ОЗУ	128 ГБ	128 ГБ
	Жесткий диск (SSD/SATA)	960 ГБ/4096 ГБ	960 ГБ/4096 ГБ
	Сетевая карта	2×Intel i350	2×Intel i350
	ОС	Ubuntu Server 16.04 x64;	Ubuntu Server 16.04 x64;
PT NAD и PT MS, установленные на физическом сервере и в виртуальной инфраструктуре	Веб-браузер	– Google Chrome версии 49 и выше; – Mozilla Firefox версии 45 и выше	– Google Chrome версии 49 и выше; – Mozilla Firefox версии 45 и выше

5. Установка PT Anti-APT

PT Anti-APT поставляется в виде ISO-файла для установки на сервер или виртуальную машину без установленной операционной системы. Для установки PT Anti-APT требуется на разных серверах отдельно установить его компоненты.

Установка компонентов PT Anti-APT выполняется аналогично установке любой операционной системы — путем создания установочного носителя из ISO-файла или с помощью монтирования этого файла при настройке виртуальной машины. При запуске установки автоматически устанавливается и настраивается 64-разрядная версия Ubuntu Server, после чего устанавливаются PT MS или PT NAD, входящие в состав PT Anti-APT.

Перед установкой вам нужно убедиться, что физический сервер или виртуальная машина, на которую вы планируете устанавливать компонент PT Anti-APT, соответствуют аппаратным требованиям (см. раздел 4).

- Чтобы установить ОС и компонент PT Anti-APT:

  1. Запустите виртуальную машину со смонтированным установочным ISO-файлом PT Anti-APT или сервер с установочным носителем, собранным из этого ISO-файла.

     Откроется главное меню установщика PT Anti-APT.

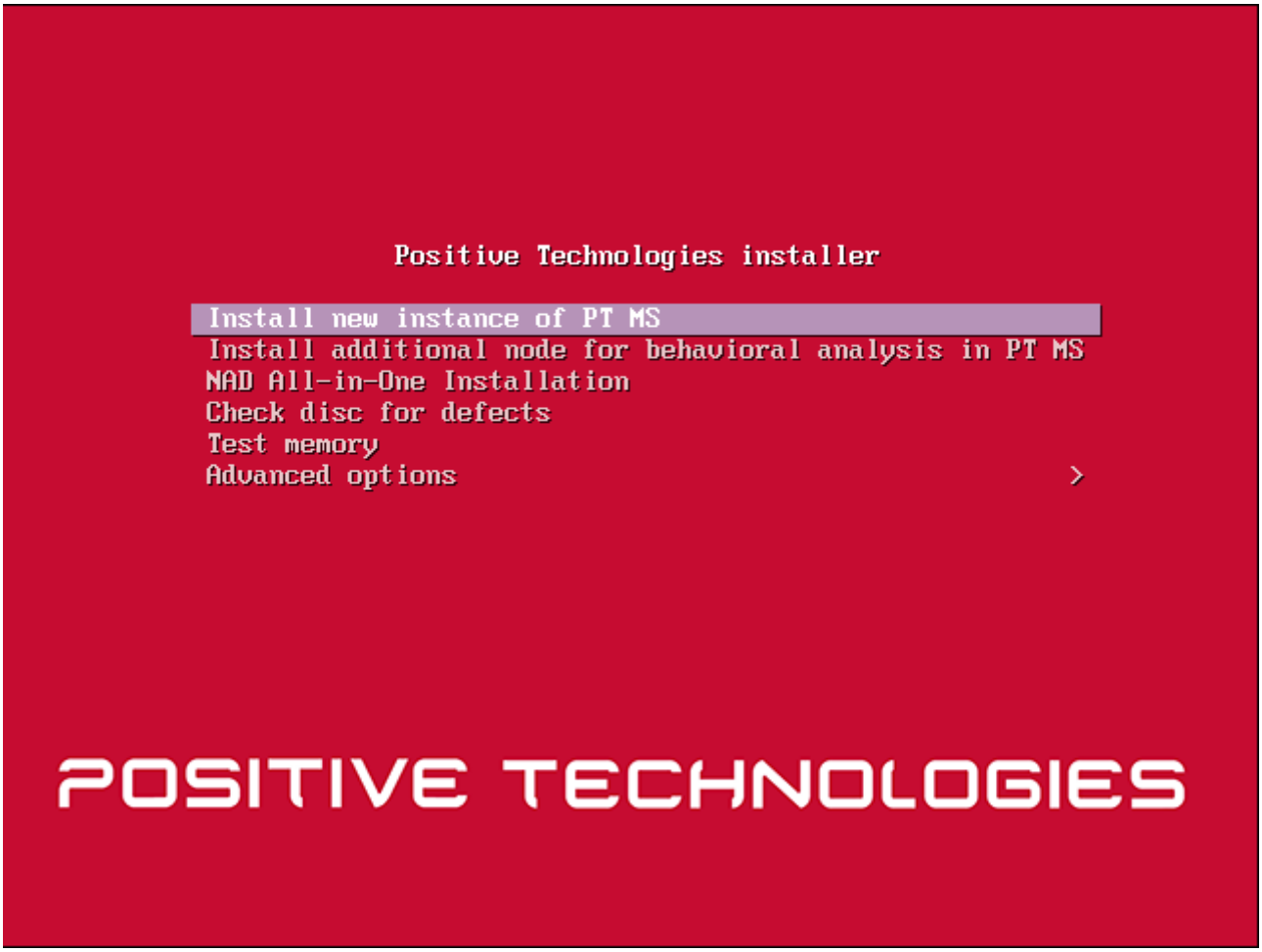

Рисунок 2. Окно установщика

2. Выберите нужный компонент и нажмите клавишу Enter.

   Начнется установка 64-разрядной версии Ubuntu Server. По окончании установки появится приветственное сообщение ОС.

   Установка PT MS или PT NAD, входящих в состав PT Anti-APT, запустится в фоновом режиме и продлится несколько минут.

Компонент PT Anti-APT установлен.

Теперь вы можете перейти к первоначальной настройке PT MS и PT NAD (см. одноименные разделы в Руководстве администратора PT MS и Руководстве администратора PT NAD).

См. также

Архитектура PT Anti-APT (см. раздел 3)

6. Активация лицензии

Для работы PT MS и PT NAD, входящих в комплекс PT Anti-APT, вам нужно активировать лицензии на их использование. Подробнее об этом см. в разделах об активации лицензии в Руководстве администратора PT MS и Руководстве администратора PT NAD.

7. Вход в PT Anti-APT

Вход во все продукты, входящие в состав PT Anti-APT осуществляется с помощью сервиса управления пользователями и доступом Positive Technologies Identity and Access Management (PT IAM).

Сервис управления пользователями и доступом Positive Technologies Identity and Access Management (PT IAM) обеспечивает механизм единого входа (технология single sign-on) в приложения "Позитив Текнолоджиз".

Перед выполнением инструкции вам нужно убедиться, что в браузере разрешены всплывающие окна.

- Чтобы войти в PT IAM:

  1. В адресной строке браузера введите ссылку для входа в PT IAM в формате `https://<IP-адрес хоста с установленным PT Anti-APT>` или `https://<имя хоста с установленным PT Anti-APT>`.

     Откроется страница входа в сервис PT IAM.
  2. В поле **Логин** введите `Administrator`.
  3. В поле **Пароль** введите `P@ssw0rd`.
  4. Нажмите кнопку **Войти**.

  Система проверит введенные вами учетные данные. Если вы указали верные данные, откроется стартовая страница PT IAM. Если вы указали неверные данные, отобразится сообщение об ошибке.

- Чтобы перейти в интерфейс нужного продукта:

  1. Нажмите кнопку  главного меню PT IAM.

     Откроется главное меню PT IAM.
  2. Выберите пункт с названием продукта.

  Переход в интерфейс продукта выполнен.

8. Настройка и администрирование

Информацию о настройке и администрировании PT MS и PT NAD, входящих в комплекс PT Anti-APT, см. в Руководстве администратора PT MS и Руководстве администратора PT NAD.

О компании

"Позитив Текнолоджиз" — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения "Позитив Текнолоджиз" для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты "Позитив Текнолоджиз" заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов. Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.

POSITIVE TECHNOLOGIES

pt@ptsecurity.com ptsecurity.com