MaxPatrol VM версия 2.0

Обзор новых возможностей

Дата редакции документа: 02.10.2023

Содержание

1. Новые возможности

В этом разделе перечислены новые возможности MaxPatrol VM и дано их краткое описание.

1.1. Стартовый дашборд

Для контроля несоответствий активов стандартам в MaxPatrol HCC реализован стандартный дашборд **Соответствие стандартам**. С его помощью вы можете отслеживать активы, у которых не указана значимость или неактуальны данные сканирования; контролировать применение стандартов, добавленных в систему; выявлять несоответствия активов стандартам и устранять их.

1.2. Статусы несоответствий активов стандартам

Для управления несоответствиями активов стандартам недостаточно только отслеживать информацию о наличии активов с несоответствиями. В MaxPatrol HCC появилась возможность присваивать несоответствиям статусы, чтобы планировать и контролировать их устранение.

Кроме того, вы можете фильтровать данные об активах и настраивать их представление с помощью запросов на языке PDQL, используя псевдонимы для статусов несоответствий.

1.3. Автоматизация устранения несоответствий активов стандартам

При большом количестве активов процесс регулярного устранения несоответствий стандартам может занимать значительное время и требует совместной работы специалистов по ИБ и системных администраторов.

Теперь в MaxPatrol HCC доступен механизм для автоматизации регулярного устранения несоответствий стандартам — политики для статусов несоответствий. С помощью политик можно автоматически изменять статусы несоответствий, определять даты и способ их устранения, а также откладывать обработку несоответствий на определенный срок.

1.4. Доставка трендовых уязвимостей за 12 часов

Создание эксплойта для трендовой уязвимости может занимать у злоумышленника около 24 часов. Наличие в инфраструктуре компании трендовой уязвимости, для которой уже создан эксплойт, — это крайне опасно. Поэтому важно определять трендовые уязвимости в максимально короткий срок.

Теперь информация о трендовых уязвимостях с рекомендациями по их устранению будет попадать к пользователям в течение 12 часов с момента появления уязвимостей. Это стало возможным благодаря изменению модели хранения и обновления экспертных данных.

Инструкции по настройке обновления экспертных данных приведены в Руководстве по внедрению.

1.5. Аудит активов с Microsoft Windows

Теперь MaxPatrol VM может проводить аудит активов с Microsoft Windows в случаях, когда MP 10 Collector установлен на Linux.

1.6. Оценка уровня опасности уязвимостей по методике ФСТЭК

Для эффективного управления уязвимостями важно правильно расставить приоритеты по их устранению. Существует множество способов определения уровня опасности уязвимостей, один из которых описан в документе ФСТЭК России «Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств».

Эксперты Positive Technologies расширили возможности языка PDQL и сформировали PDQL-запрос, который поможет пользователям рассчитать уровень опасности уязвимостей в соответствии с методикой ФСТЭК России.

1.7. Множественный выбор коллекторов

Начиная с версии 2.0 при создании или редактировании задачи вы можете выбрать несколько коллекторов, которые будут выполнять сбор данных (в том числе коллекторы, относящиеся к разным конвейерам). Подзадачи будут распределяться между выбранными коллекторами.

1.8. Стандартные запросы для контроля конфигурации активов

Эксперты Positive Technologies выделили ряд типичных задач, связанных с применением стандартов на активах и контролем за устранением выявленных несоответствий, и сформировали PDQL-запросы, которые могут помочь пользователям в решении этих задач. Новые запросы можно найти на странице **Активы** в панели **Запросы** в папке **Стандартные**.

1.9. Добавление меток для требований

Стандарты в MaxPatrol HCC содержат множество требований, число которых со временем будет только увеличиваться.

Теперь вы можете добавлять для требований ключевые слова (метки) для их быстрого поиска, идентификации или категоризации.

Кроме того, вы можете фильтровать данные об активах и настраивать их представление с помощью запросов на языке PDQL, используя псевдонимы для меток.

2. Технические особенности

Информация, представленная в этом разделе, поможет избежать возможных ошибок при обновлении и последующей работе с продуктом.

Обновление экспертных данных

Начиная с версии 2.0 мы переходим на новую модель хранения и обновления экспертных данных. Обновление экспертных данных в MaxPatrol VM будет осуществляться с помощью сервиса Package Management, который входит в состав компонента PT MC. Сервис получает пакеты обновлений с сервера Positive Technologies и устанавливает их в продукты с соответствующими лицензиями. Для перехода к новой модели хранения и обновления экспертных данных необходимо:

— При наличии прямого подключения MaxPatrol VM к интернету — выбрать `Online` в качестве значения параметра ExpertDataUpdateMethod, указать в качестве значения параметра PackagesSourceUri роли Management and Configuration адрес глобального сервера обновлений `https://update.ptsecurity.com/packman/v1/`, а в качестве значения параметра PackagesSourceCredentialToken — токен для аутентификации, полученный с лицензией или дистрибутивом в файле `instance-access-token.key`.

— При отсутствии прямого подключения MaxPatrol VM к интернету — установить локальный сервер обновлений и настроить параметры ExpertDataUpdateMethod, PackagesSourceUri и PackagesSourceCredentialToken в соответствии с инструкциями в разделе «Настройка обновления экспертных данных» в Руководстве по внедрению.

  Внимание! Описанные выше действия обязательны для прохождения процесса миграции на новую модель хранения экспертных данных и получения обновлений с сервера Positive Technologies.

Процесс миграции на новую модель хранения экспертных данных является обязательным, запускается после обновления MaxPatrol VM и может занимать до полутора часов. Во время миграции на главной странице в виджетах на дашбордах не отображается информация об уязвимостях, а также недоступны следующие страницы MaxPatrol VM **Активы**, **Стандарты**, **Система** → **Политики**, **Система** → **Управление системой** → **База уязвимостей** и **Система** → **Управление системой** → **Обработка активов**.

Замена термина

Начиная с версии 2.0 вместо слова «агент» мы будем использовать слово «коллектор». Новое название более точно отражает задачи компонента; работа самого компонента при этом не меняется.

Существует ряд особенностей версии 2.0:

— Версия 2.0 поддерживает обновление с версии 1.5.

— Версия 2.0 поддерживает интеграцию с PT NAD версии 11.0, 10.3, 10.2, 10.1.

— Прежде чем приступать к обновлению MaxPatrol VM, рекомендуется остановить все задачи на сбор данных, а также убедиться, что на период обновления не запланирован запуск задач по расписанию. Это позволит избежать накопления очередей во время обновления, а также ошибок при выполнении задач после обновления.

— Если MP 10 Collector установлен на Linux, MaxPatrol VM не сможет проводить аудит активов с Microsoft Windows по протоколу SMBv1.

— Теперь для развития продукта, повышения качества экспертизы и решения других задач в MaxPatrol VM выполняется сбор телеметрических данных о производительности микросервисов MP 10 Core и действиях пользователя.

3. Улучшения

В этом разделе описаны улучшения MaxPatrol VM новой версии.

Поиск групп активов

В MaxPatrol VM может быть создано большое количество групп активов с множеством уровней вложенности. Добавлена возможность поиска групп активов по названию.

Описание задачи

При создании новой или изменении уже существующей задачи теперь можно добавить информацию о задаче по ссылке **Добавить описание**. Это позволит дополнительно описать контекст задачи и поможет ее идентифицировать. Информация отображается в карточке при выборе задачи в списке и при просмотре истории запусков задачи. Поиск и фильтрация по этой информации не выполняются.

Расширение настроек расписания

Теперь вы можете настраивать расписание выполнения задач сбора и создания отчетов дополнительно в следующих форматах: однократно, ежедневно, еженедельно, ежемесячно и в виде строки crontab.

positive
technologies

Positive Technologies — лидер рынка результативной кибербезопасности. Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Наши технологии используют более 3300 организаций по всему миру, в том числе 80% компаний из рейтинга «Эксперт-400». Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI), у нее более 170 тысяч акционеров.