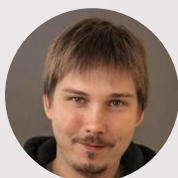




MaxPatrol SIEM

Обзор новых возможностей



Станислав Черкасов
Менеджер по продвижению продуктов



Антон Исаев
Старший специалист отдела систем мониторинга безопасности

A large, stylized 3D number '6.1' rendered in a metallic, reflective silver color. The number is set against a background of a 3D grid of light gray cubes. A small red square is positioned between the '6' and the '1'.

План вебинара

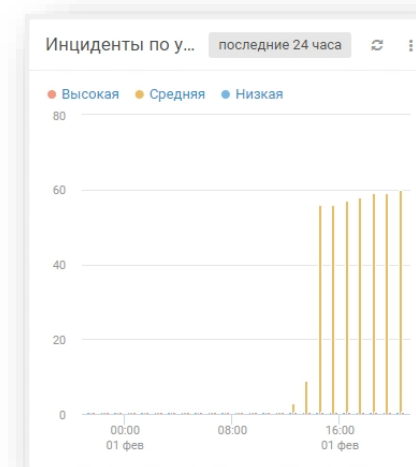
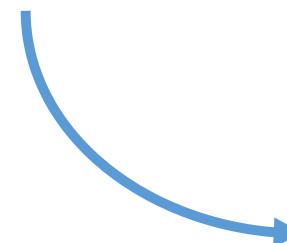
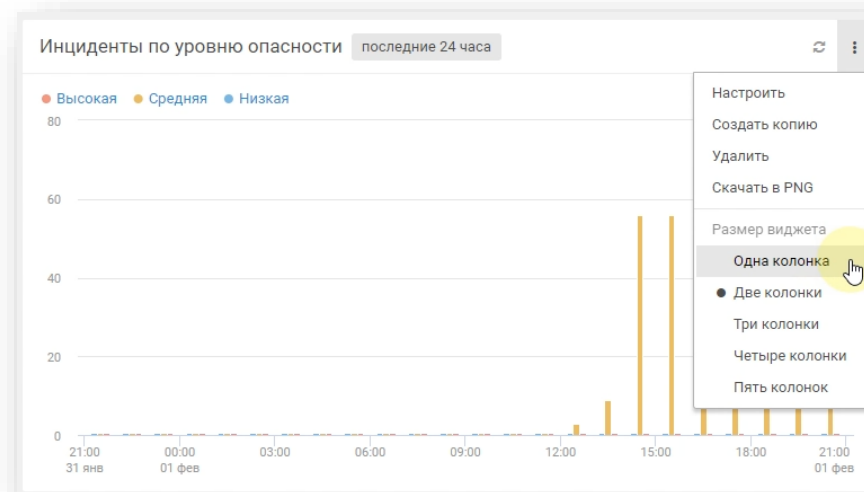
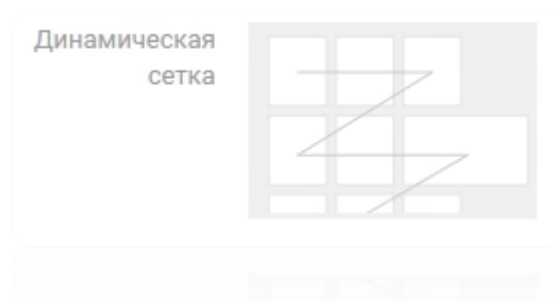
- Новое в дашбордах и активах
- Интеграция IAM с Microsoft Active Directory
- Конструктор профиля для сбора данных
- Мониторинг работы правил корреляции
- Импорт данных в ПТ КБ
- С чем попрощаемся в 6.1
- Приятные мелочи

Новое в дашбордах



Динамическая сетка виджетов:

Размещайте любое количество нужных виджетов и настраивайте размер для каждого

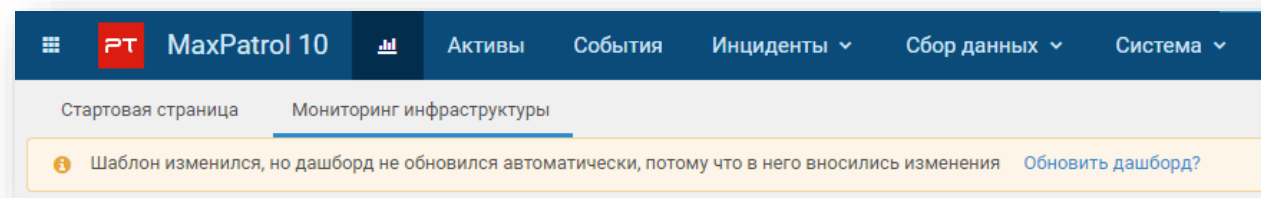
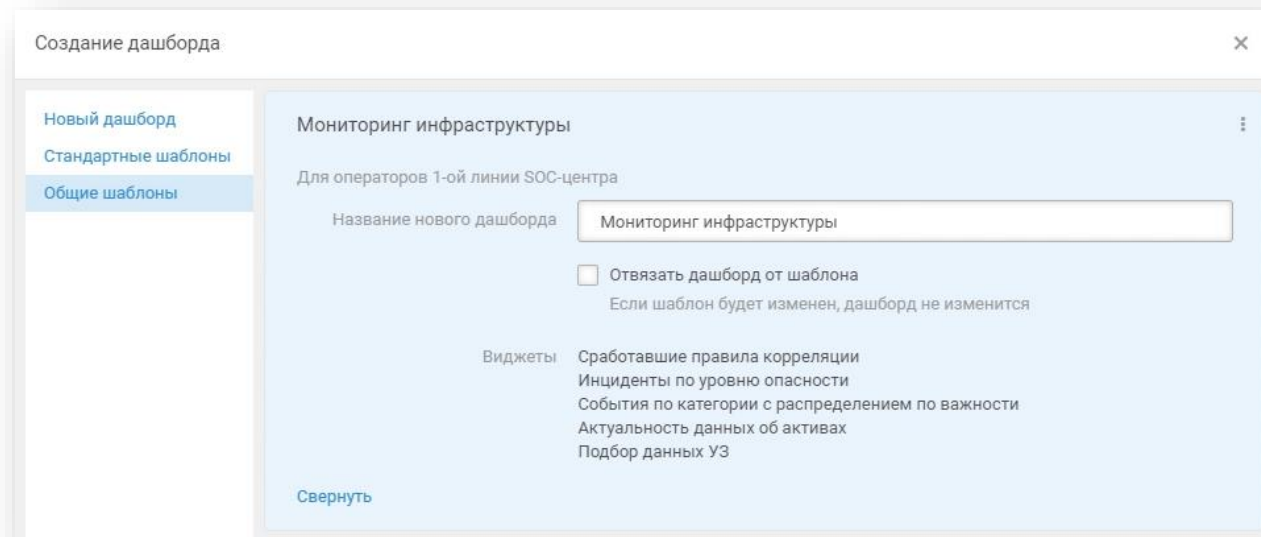
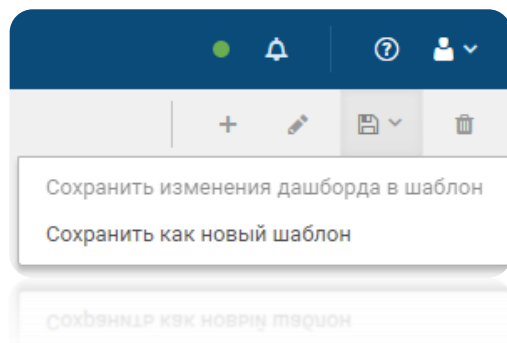


Новое в дашбордах

Дашборды как шаблоны:

Сохраняйте дашборды как шаблоны, которые станут доступны для других пользователей.

При создании дашборда у вас будет выбор между новым, предустановленными системными или общими шаблонами дашбордов.

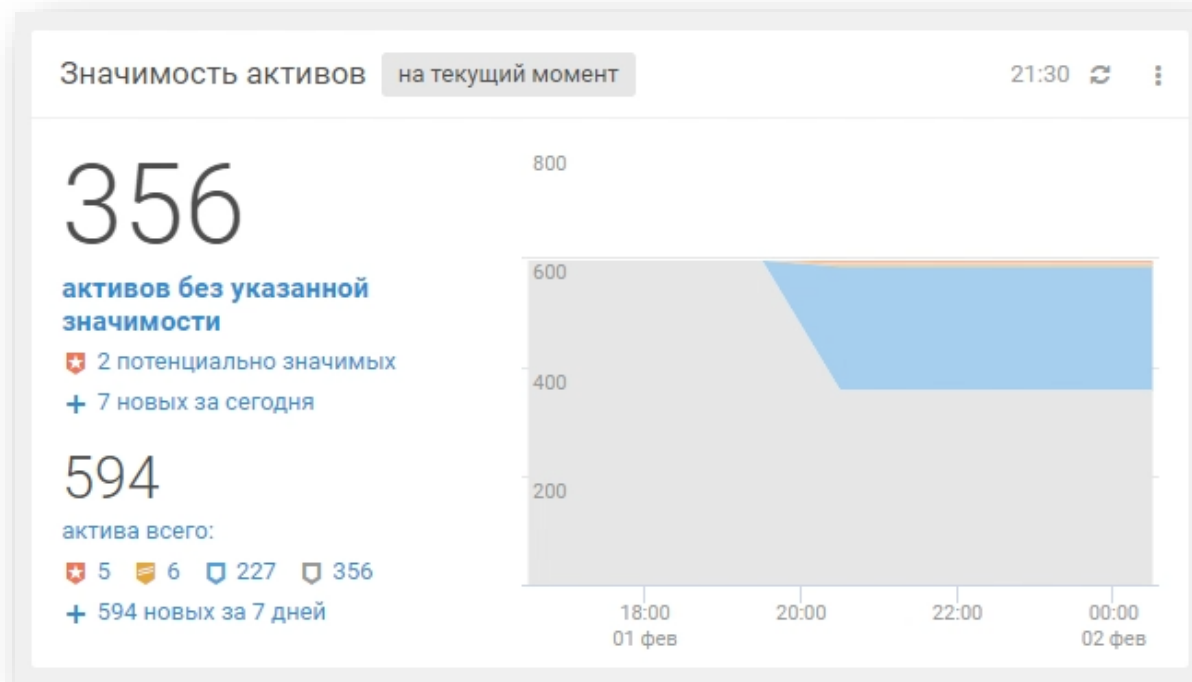


Новые дашборды

«Значимость активов»

Отслеживание новых активов в инфраструктуре, с которыми вы ещё не успели поработать:

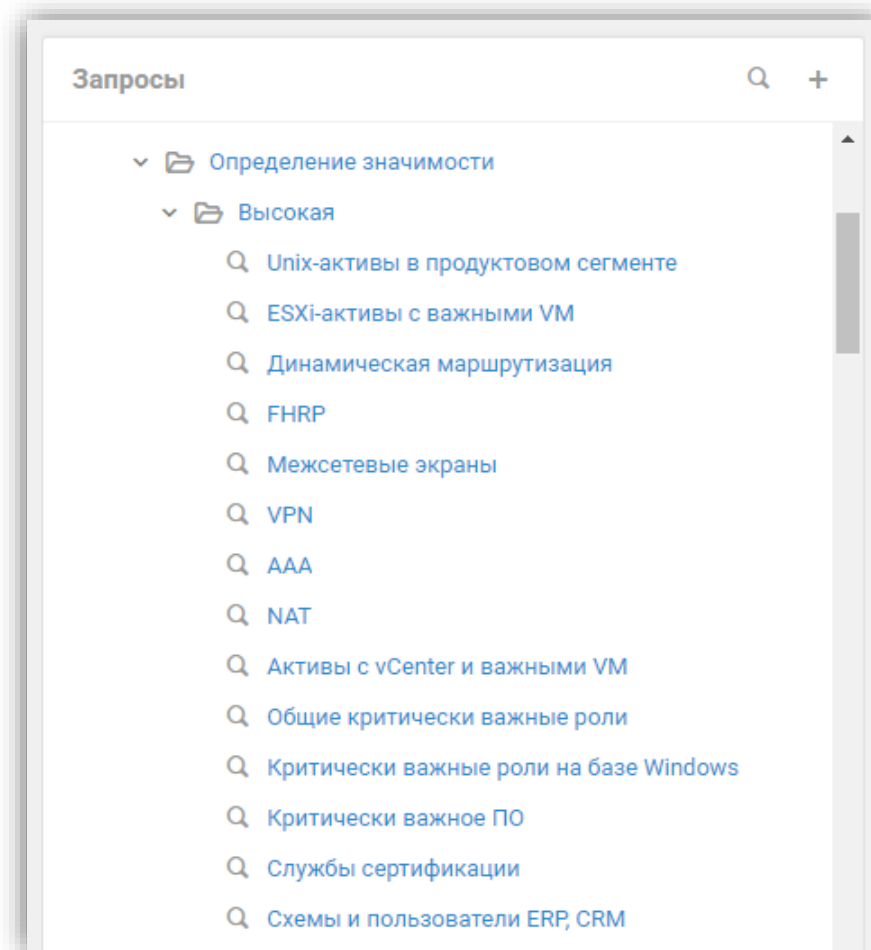
- не задан соответствующий уровень значимости
- потенциально значимые активы, которые вы, скорее всего, могли пропустить
- текущая сводка по всем активам организации + по заданным уровням значимости
- динамика назначения значимости активам вашей инфраструктуры



«Значимость» — какая?

Предустановленные PDQL-запросы:

Эксперты Positive Technologies подготовили предустановленные PDQL-запросы, которые помогут задать соответствующий уровень значимости активам вашей организации.



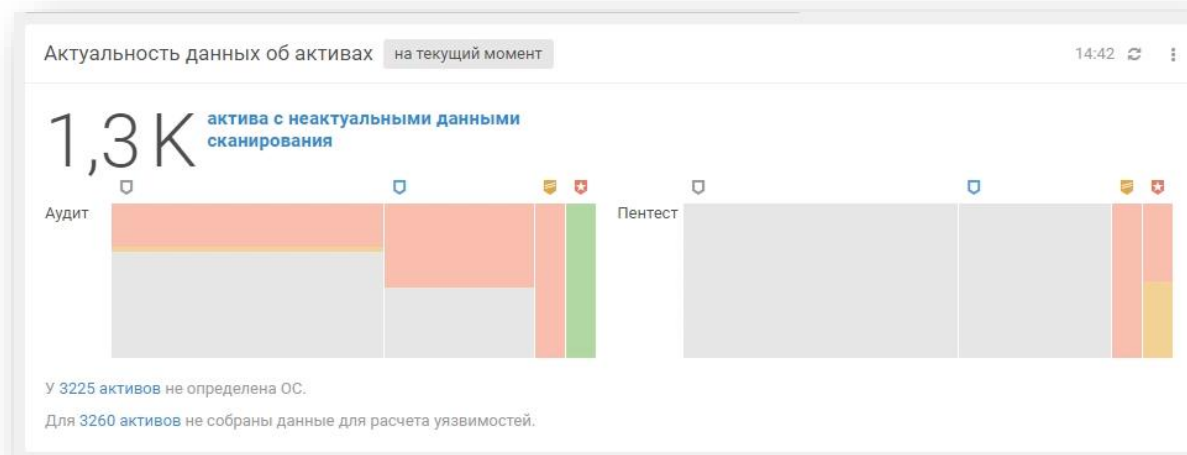
<https://youtu.be/Z0Uv5yKxFDM>

Новые дашборды

«Актуальность данных об активах»

Отслеживание регулярного сканирования активов в инфраструктуре для:

- Создания точечных правил корреляции, направленных на конкретные активы
- Формирования отчётов по нелегитимному ПО/некорректным конфигурациям ИТ-систем в инфраструктуре
- Помощи в расследовании инцидентов



VideoLAN	VLC Media Player	19
Microsoft	Microsoft Hyper-V	16
TeamViewer Gmbh	TeamViewer	15
Adobe Systems	Adobe Flash Player	14
OpenVPN	OpenVPN	14
Media Player Classic	Media Player Classic	13

Управление устареванием данных



В карточках активов

Настройка временных интервалов
актуальности данных сканирования
Audit / Pentest

Статусы актуальности данных

Вы можете настроить время, в течение которого данные об активе будут считаться актуальными, — отдельно для каждого режима сканирования.

Аудит	Данные актуальны 7 дней Данные устареют через 12 дней Установлены вручную Сбросить
Пентест	Не задано Настроить вручную

Механизм «Политик»

Регулярное автоматическое
назначение сроков актуальности
данных сканирования

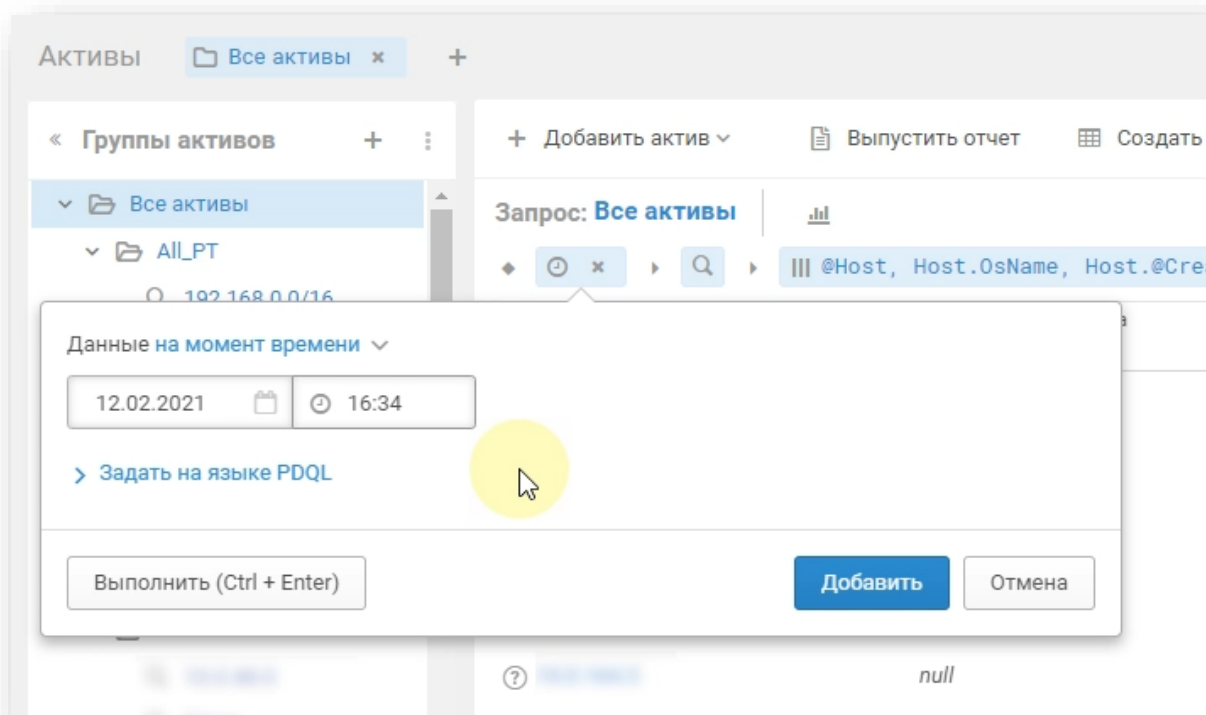
Политика для сроков актуальности данных (аудит)

Порядок	Состояние	Название
⋮ 1	🔵	Сроки актуальности активов высокой значимости для метода Audit
⋮ 2	🔵	Сроки актуальности активов средней значимости для метода Audit

Оператор «Время»

Ретроспектива по активам

Анализ состояния IT-инфраструктуры и оценка изменения показателей защищенности активов с течением времени



Оператор «Время»

Пример №1:

Контроль процесса перехода хостов
вашей организации с устаревших
операционных систем на новые

Запрос: **Все активы ***

1 мес, 1 нед, now()

@Host, Host.OsName as OS, Host.@Time

OS in ['windows 7', 'windows 10']

Host.@Time, OS, COUNT(*)

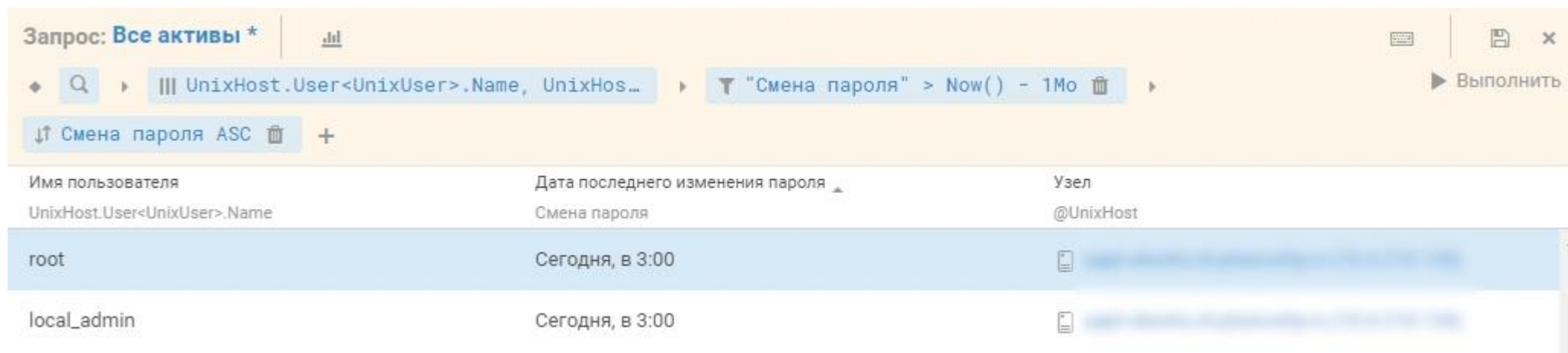
OS ASC

Дата и время для расчета... Host.@Time	Операционная си... OS	COU...	Узел @Host	Операционная система OS
02 февраля, 16:43	Windows 10	76		Windows 10
09 февраля, 16:43	Windows 10	87		Windows 10
Сегодня, в 16:43	Windows 10	87		Windows 10
02 февраля, 16:43	Windows 7	3		Windows 10
09 февраля, 16:43	Windows 7	28		Windows 10
Сегодня, в 16:43	Windows 7	28		Windows 10

Оператор «Время»

Пример №2:

Поиск учетных записей Unix-хостов, у которых менялся пароль за последний месяц



Запрос: Все активы *

UnixHost.User<UnixUser>.Name, UnixHos... "Смена пароля" > Now() - 1Mo

Выполнить

Смена пароля ASC

Имя пользователя	Дата последнего изменения пароля	Узел
UnixHost.User<UnixUser>.Name	Смена пароля	@UnixHost
root	Сегодня, в 3:00	
local_admin	Сегодня, в 3:00	

Массовые операции по активам

Ускорение работы с активами

Выбирайте сразу несколько активов для:

- Редактирования их паспортов
- Назначения уровня значимости
- Создания задач сбора данных
- Расчёта достижимости
- И т.д...



Выбраны 5 активов

- ✎ Редактировать ▾
 - 📁 Расположение в группах
 - 🛡️ Назначение значимости
 - 🗑️ Удалить
-
- ↔️ Сравнить конфигурации
 - 🔍 Найти ▾
 - 📡 Создать задачу по сбору данных
 - 🔄 Расчет достижимости ▾
 - ✖️ Сбросить выделение

Управление пользователями из Active Directory



Сопоставление ролей и групп в системе

Интеграция с Active Directory позволит вам задать соответствия групп пользователей с их ролями в SIEM, чтобы централизованно управлять пользователями и их правами в системе

Соответствие ролей и групп

Укажите соответствие ролей в приложениях и групп Active Directory. Роли пользователей обновляются при каждой синхронизации.

[Обновить список групп](#)

Роли в приложениях	Группы Active Directory
Knowledge Base	
Администратор	<input type="text"/>
Role KB R1	<input type="text"/>
Management and Configuration	
Администратор	<input type="text"/>
Role MC R1	<input type="text"/>
Пользователь	<input type="text"/>
MaxPatrol 10	
Администратор	<input type="text"/>
Оператор	<input type="text"/>

Обновленный конструктор профиля для сбора данных

PT

Больше никакого «JSON»!

Настраивайте задачи сбора через новый
удобный конструктор профилей

Новый профиль

Название: Fast PenTest

Описание:

Создать на основе: Fast PenTest

Базовый профиль: Fast PenTest

Модуль: pentest

Параметры профиля Импорт Экспорт

Общие параметры сканирования

Сканирование портов

Сканирование UDP-служб

Поиск уязвимостей

Подбор учетных данных

- IBM DB2
- Microsoft SQL Server
- Oracle Database
- Oracle Database, подбор SID
- Oracle MySQL
- SAP Sybase ASE
- SAP через DIAG
- SAP через RFC
- Symantec pcAnywhere
- Virtual Network Computing
- VMware vSphere
- Windows через Microsoft SQL Server

Общие параметры сканирования

Метод сканирования портов

SYN-пакеты Подключение

Искать сетевые принтеры

Мониторинг работы правил корреляций

Отображение цепочек событий

Следите за корректностью самописных правил корреляций через новый механизм отслеживания цепочек событий в каждом правиле

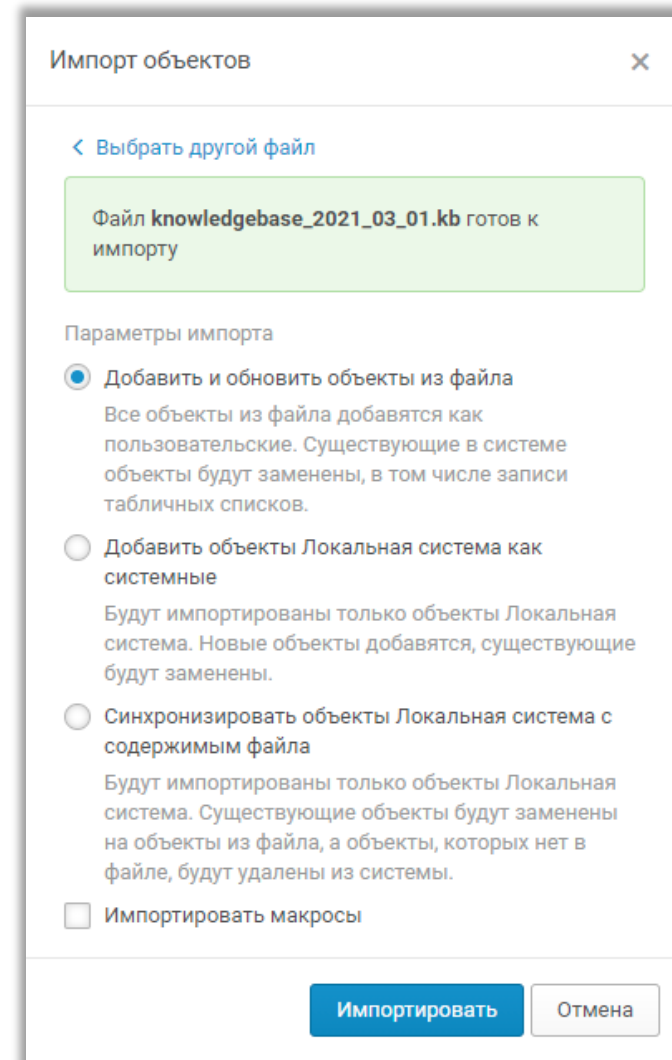
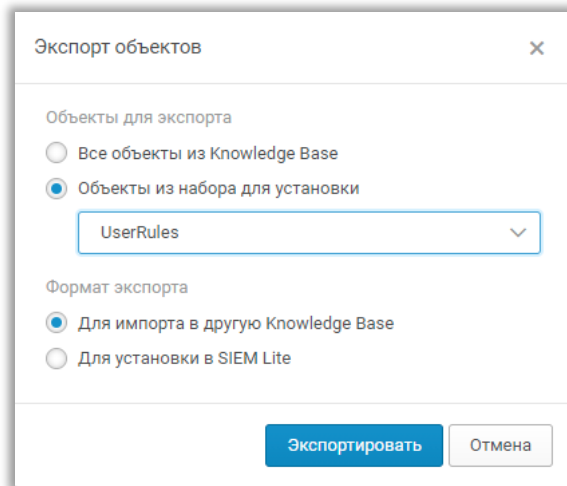
Список правил корреляции							🔍	🗒
Статус	Идентификатор	Название	Категория	Тип	Срабатываний за сут...	Цепочки	Событий в цепочках	⚙
🔴	PT-CR-403	Sliver_Shell_Subrule_1	//	🛡	0	3 485	0	
🔴	PT-CR-307	Detect_Possible_Credential_Dump_via_Local_Memory_Acce	Attack / Credential Access / Credential Dumping	🛡	0	2 440	145 144	
🔴	PT-CR-305	Detect_Possible_Credential_Dump_via_Local_Memory_Acce	Attack / Credential Access / Credential Dumping	🛡	0	2 438	0	
🔴	PT-CR-309	Detect_Possible_Credential_Dump_via_Local_Memory_Acce	Attack / Credential Access / Credential Dumping	🛡	0	1 924	45 756	
🔴	PT-CR-286	Detect_bind_shell	Attack / Persistence / Bind-shell	🛡	0	1 628	183	
🔴	PT-CR-296	Detect_run_reverse_shell_by_something	Attack / Command And Control / Reverse-shell	🛡	4	301	430	
🔴	PT-CR-294	Detect_run_bash_for_reverse_shell	Attack / Command And Control / Reverse-shell	🛡	0	166	2 304	

Импорт данных в ПТ КБ

РТ

Распространение контента в РТКВ

Переносите ваш контент из одной инсталляции в другую через новый механизм экспорта/импорта объектов в РТКВ



Что пропало в 6.1?

Прекращение поддержки:

- Endpoint Monitor
 - Выдаём рекомендации по настройке Sysmon для расширенного аудита Windows
- Шаблоны мониторинга для Zabbix
 - Замена мониторинга производительности через Grafana + Telegraf
- Работа с уязвимостями в SIEM
 - Выпуск полноценного продукта MaxPatrol VM по управлению уязвимостями в вашей организации

*Internet Explorer уходит тоже



«Мелочь, а приятно...»

Технические улучшения:

- Версия PostgreSQL обновлена до 12.5
- Версия Elasticsearch обновлена до 7.9
- Улучшения в работе установщика системы
- Поддержка Debian версий 9.11 — 9.13 и 10.x
- Поддержка развертывания в виртуальной среде
- Оптимизация обмена данными между компонентами
- Оптимизация алгоритма распределения подзадач по агентам

Что дальше

PT

Задать вопрос:

t.me/MPSIEMChat

Обновить версию:

support.ptsecurity.com

Пройти обучение:

edu@ptsecurity.com

ПИЛОТ:

ptsecurity.com/ru-ru/products/mpsiem/#free-demo

