



POSITIVE  
TECHNOLOGIES

Наполняем продукт вашими желаниями:  
**обзор MaxPatrol SIEM 5.1**

**Станислав Черкасов**  
Эксперт отдела мониторинга событий ИБ

[ptsecurity.com](https://ptsecurity.com)

# Новое в MaxPatrol SIEM 5.1



- Сырые события в интерфейсе
- Ретроспективные корреляции
- Агрегация инцидентов
- Визуализация контента в РТКВ
- Алиасы столбцов
- Гибкая ролевая модель v. 1.0
- Сбор информации из Active Directory

# Новое в MaxPatrol SIEM 5.1



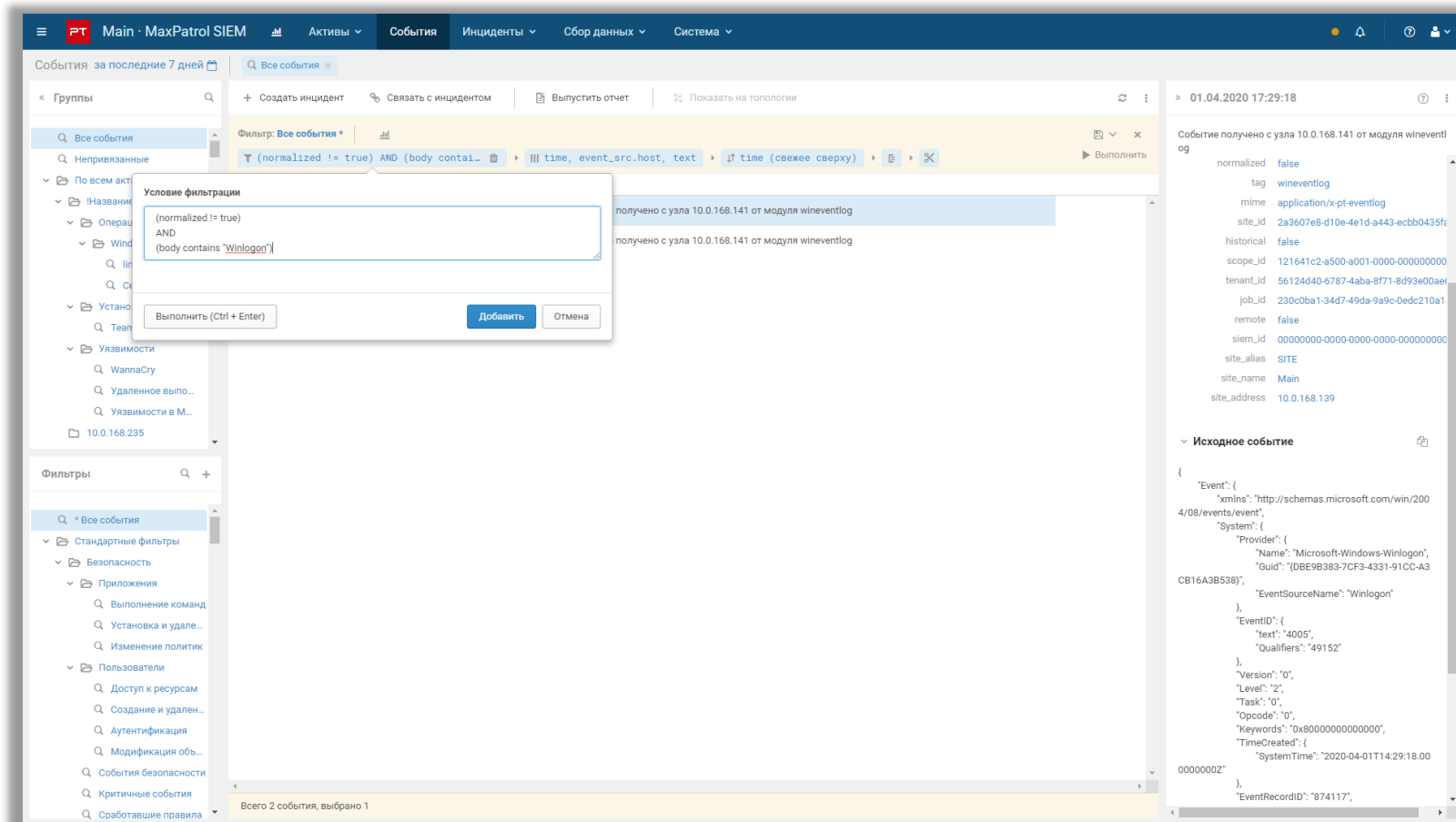
- **Сырые события в интерфейсе**
- Ретроспективные корреляции
- Агрегация инцидентов
- Визуализация контента в РТКВ
- Алиасы столбцов
- Гибкая ролевая модель v. 1.0
- Сбор информации из Active Directory

# Ненормализованные события в интерфейсе



Работайте с ненормализованными событиями прямо в интерфейсе:

1. Просматривайте содержимое события.
2. Применяйте фильтры в сырых событиях.
3. Ищите по содержимому события.
4. Разработка нормализации никогда еще не была такой легкой.



# **Демо работы с ненормализованными событиями**





POSITIVE  
TECHNOLOGIES

# MaxPatrol SIEM 5.1

Работа с сырыми событиями  
в интерфейсе

[ptsecurity.com](http://ptsecurity.com)

# Новое в MaxPatrol SIEM 5.1



- Сырые события в интерфейсе
- **Ретроспективные корреляции**
- Агрегация инцидентов
- Визуализация контента в РТКВ
- Алиасы столбцов
- Гибкая ролевая модель v. 1.0
- Сбор информации из Active Directory


# Коррелируем прошлое

РТ

## Ретроспективный анализ с помощью правил корреляции

Теперь вы можете проверить уже прошедшие события на предмет совпадений по любым правилам корреляции

*Включая новые правила  
из пакетов экспертизы!*



### Чтобы заработало:

1. Обновите версию продукта.
2. Установите ретроспективный коррелятор.
3. Создайте задачу на проверку событий ИБ.
4. Выберите условия создания инцидентов/событий.



# Демо ретроспективных корреляций



POSITIVE  
TECHNOLOGIES

# MaxPatrol SIEM 5.1

Ретроспективный анализ

[ptsecurity.com](http://ptsecurity.com)

# Новое в MaxPatrol SIEM 5.1



- Сырые события в интерфейсе
- Ретроспективные корреляции
- **Агрегация инцидентов**
- Визуализация контента в РТКВ
- Алиасы столбцов
- Гибкая ролевая модель v. 1.0
- Сбор информации из Active Directory

# Агрегация инцидентов в MaxPatrol SIEM

- Работает в режиме реального времени
- Позволяет настроить подклейку инцидентов по массе параметров
- Помогает упорядочить работу с инцидентами
- Представляет более структурированную картину инцидентов

# Демо агрегации инцидентов





POSITIVE  
TECHNOLOGIES

# MaxPatrol SIEM 5.1

Агрегация инцидентов

[ptsecurity.com](http://ptsecurity.com)

# Новое в MaxPatrol SIEM 5.1



- Сырые события в интерфейсе
- Ретроспективные корреляции
- Агрегация инцидентов
- **Визуализация контента в РТКВ**
- Алиасы столбцов
- Гибкая ролевая модель v. 1.0
- Сбор информации из Active Directory

# Удобство работы с базой знаний

PT

Теперь элементы базы знаний собраны по логическим группам, в которые входят:

- Правила корреляции
- Правила обогащения
- Формулы нормализации
- Табличные списки

## Возможности:

1. Работа непосредственно с пакетом данных.
2. Выбор установки пакетов, релевантных для вашей инфраструктуры.
3. Описание и руководства по работе с пакетами прямо в интерфейсе.

The screenshot displays the PT MaxPatrol SIEM Knowledge Base interface. The left sidebar shows a tree structure of knowledge packages, with 'ATT&CK: «Разведка»' selected. The main content area shows the configuration for this package, including its version (1.0), parameters (System XML, 4.6 KB), and description (PDF, 437.3 KB). The 'О пакете экспертизы' (About the expert package) section explains that the package includes correlation rules for detecting attacks on Windows systems using the 'Discovery' tactic. It also provides instructions on how to enable event registration in the SIEM server and how to use the 'Incidents\_muting' rule to filter out false positives. A table at the bottom lists the events registered for the 'Discovery' tactic, showing the technique 'Account Discovery' and the event 'Computer\_object\_ldap\_request'.

Техника	Событие ИБ
Account Discovery	Computer_object_ldap_request — обнаружена выгрузка списка компьютеров домена с контроллера домена (с использованием

# Демо визуализации контента РТКВ





POSITIVE  
TECHNOLOGIES

# MaxPatrol SIEM 5.1

Пакеты экспертизы

[ptsecurity.com](http://ptsecurity.com)



# Новое в MaxPatrol SIEM 5.1

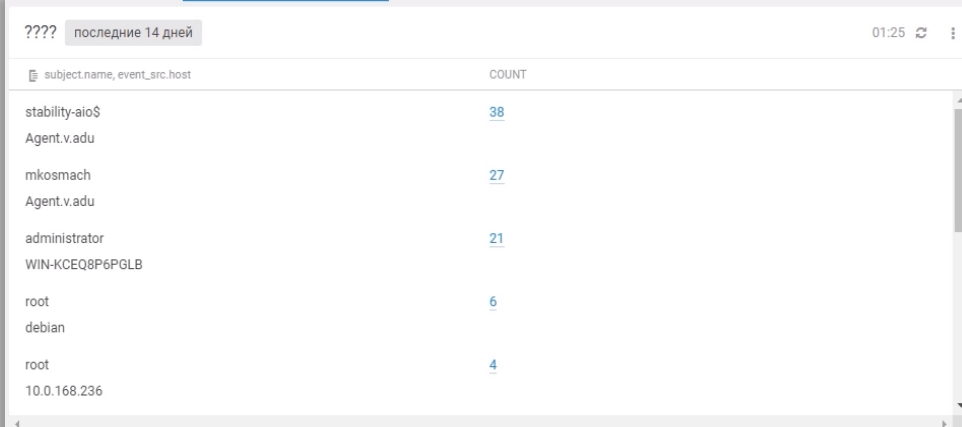


- Сырые события в интерфейсе
- Ретроспективные корреляции
- Агрегация инцидентов
- Визуализация контента в РТКВ
- **Алиасы столбцов**
- Гибкая ролевая модель v. 1.0
- Сбор информации из Active Directory

# Собственные названия полей в виджетах


## Создание более информативных виджетов и таблиц для дашбордов:

1. Вы можете именовать поля в выборках по собственному желанию.
2. Позволяет создавать более информативные графики.
3. Позволяет создавать красивые логичные отчеты.



Скриншот виджета с таблицей. В заголовке таблицы указаны поля: subject.name, event\_src.host и COUNT. Данные представлены в виде списка строк с именами пользователей и их количеством.

subject.name, event_src.host	COUNT
stability-aio\$	38
Agent.v.adu	
mkosmach	27
Agent.v.adu	
administrator	21
WIN-KCEQ8P6PGLB	
root	6
debian	
root	4
10.0.168.236	



Скриншот виджета с таблицей. В заголовке таблицы указаны поля: Пользователь, Источник события и Количество неудачных попыток входа. Данные представлены в виде списка строк с именами пользователей и их количеством неудачных попыток входа.

Пользователь, Источник события	Количество неудачных попыток входа
stability-aio\$	38
Agent.v.adu	
mkosmach	27
Agent.v.adu	
administrator	15
WIN-KCEQ8P6PGLB	
administrator	2
Agent.v.adu	
guest	2
Agent.v.adu	

Всего 8 строк, выбрано 0 строк

# Демо алиасы столбцов



POSITIVE  
TECHNOLOGIES

# MaxPatrol SIEM 5.1

Кастомизации в названии полей  
событий и активов

[ptsecurity.com](https://ptsecurity.com)

# Новое в MaxPatrol SIEM 5.1



- Сырые события в интерфейсе
- Ретроспективные корреляции
- Агрегация инцидентов
- Визуализация контента в РТКВ
- Алиасы столбцов
- **Гибкая ролевая модель v. 1.0**
- Сбор информации из Active Directory



# Отключение определенных разделов интерфейса

В комплекте с уже существующими возможностями фильтрации, например:

1. Доступ только к определенным событиям и никуда более.
2. Доступ только к инцидентам определенной группы активов.
3. Возможность дать доступ службе IT управлять задачами и профилями сбора.

The screenshot displays the configuration interface for a role in the MaxPatrol SIEM system. At the top, the 'Приложение' (Application) is set to 'MaxPatrol SIEM'. Below it, the 'Название роли' (Role name) is 'просмотр событий' (View events). A link 'Добавить описание' (Add description) is visible. The main section is titled 'Права доступа' (Access rights) and contains a table of permissions.

Права доступа	
Привилегия	
Общее	<input type="checkbox"/>
Доступ с административными полном...	<input type="checkbox"/>
Активы	<input checked="" type="checkbox"/>
Активы	<input checked="" type="checkbox"/>
События	<input checked="" type="checkbox"/>
События	<input checked="" type="checkbox"/>
Инциденты	<input type="checkbox"/>
Инциденты	<input type="checkbox"/>
Сбор данных	<input type="checkbox"/>
Профили	<input type="checkbox"/>
Мониторинг источников	<input type="checkbox"/>
Учетные записи	<input type="checkbox"/>
Задачи	<input type="checkbox"/>
Транспорты	<input type="checkbox"/>
Инфраструктура	<input type="checkbox"/>
Справочники	<input type="checkbox"/>
Правила и табличные списки	<input type="checkbox"/>

# Демо ролевой модели v. 1.0.



POSITIVE  
TECHNOLOGIES

# MaxPatrol SIEM 5.1

Гибкая ролевая модель

[ptsecurity.com](http://ptsecurity.com)

# Новое в MaxPatrol SIEM 5.1

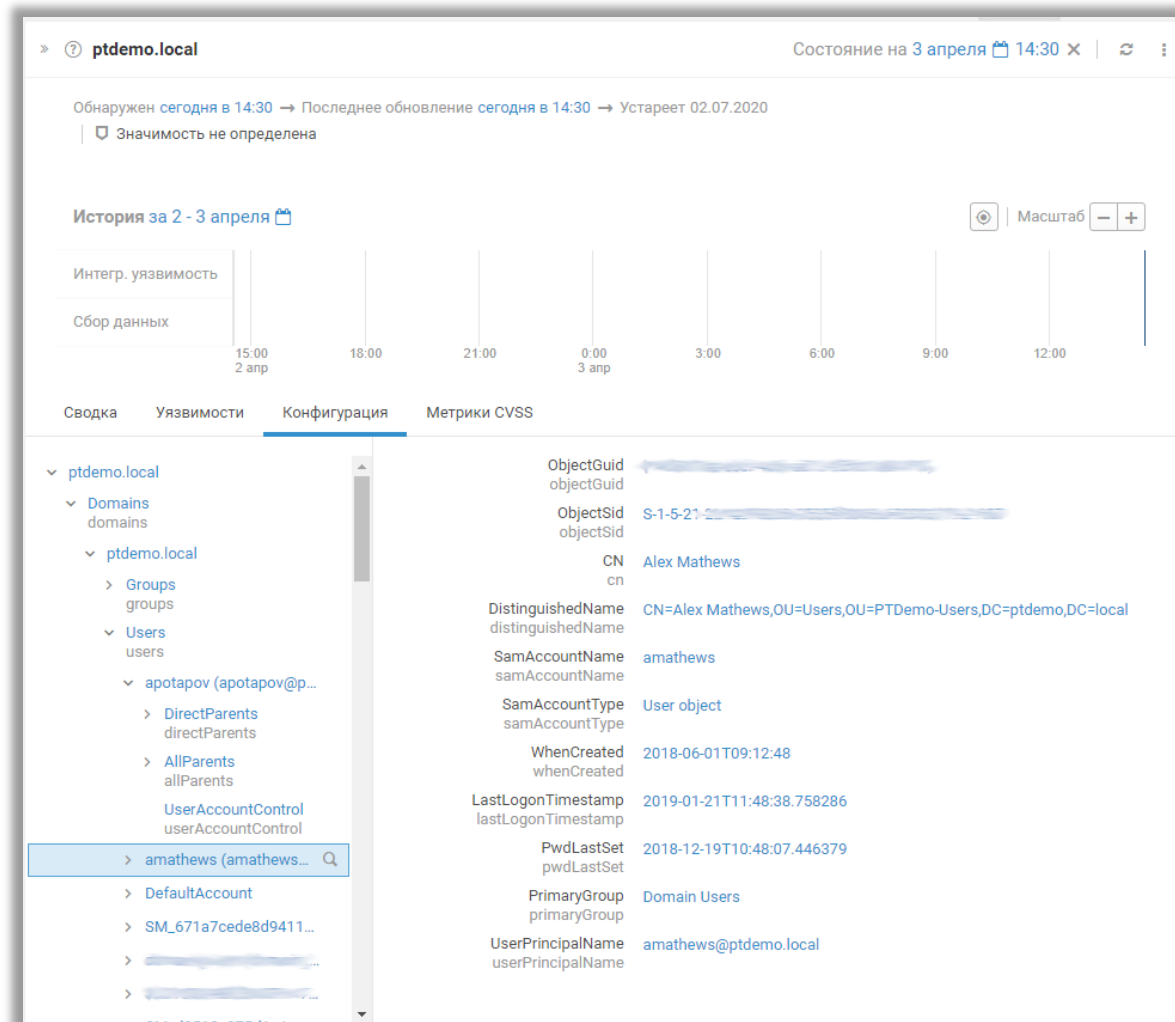


- Сырые события в интерфейсе
- Ретроспективные корреляции
- Агрегация инцидентов
- Визуализация контента в РТКВ
- Алиасы столбцов
- Гибкая ролевая модель v. 1.0
- **Сбор информации из Active Directory**

# Извлечение информации из Active Directory

## Сбор информации путём сканирования содержимого Active Directory:

1. Собирает содержимое групп пользователей, самих пользователей, и компьютеров.
2. Компьютеры из AD автоматически сливаются с активами (если таковые уже есть).
3. Никаких особых настроек не требует.





# Что дальше:



Обновить версию:  
[support.ptsecurity.com](https://support.ptsecurity.com)

Заказать пилот:  
[ptsecurity.com/ru-ru/products/mpsiem/](https://ptsecurity.com/ru-ru/products/mpsiem/)

Пройти обучение:  
[edu@ptsecurity.com](mailto:edu@ptsecurity.com)

Купить:  
[sales@ptsecurity.com](mailto:sales@ptsecurity.com)

Чат в Telegram:  
[t.me/MPSIEMChat](https://t.me/MPSIEMChat)



**Станислав Черкасов**  
Эксперт отдела мониторинга  
событий ИБ  
[scherkasov@ptsecurity.com](mailto:scherkasov@ptsecurity.com)

# КАК ОРГАНИЗОВАНА УДАЛЕНКА В ВАШЕЙ КОМПАНИИ?

Пройти опрос

[bit.ly/homeofficesurvey](https://bit.ly/homeofficesurvey)

