



Пользовательские правила профилирования в РТ NAD

(они же ППП)

ML-алгоритм для поиска аномальных всплесков трафика:

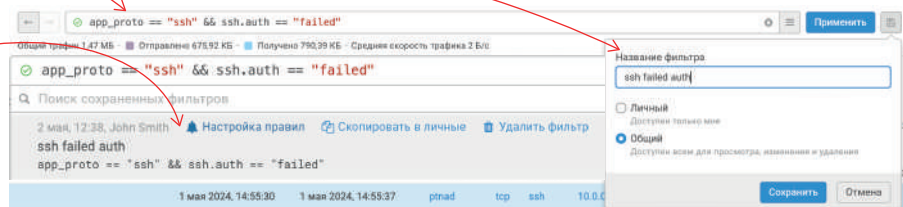
- Определяет аномалии, которые не выявить иначе (например, непредсказуемые активности).
- Обучается, учитывая средние значения и ежедневные отклонения.
- Распределяет слишком различающиеся узлы в разные кластеры.

Принцип работы ППП

- Автоматически распределяет найденные узлы в кластеры в зависимости от уровня их активности.
- Значения средней активности каждого кластера используются для расчета индивидуального порога срабатывания.
- Порог срабатывания ППП на аномальный всплеск зависит от степени чувствительности механизма: низкий (в 100 раз выше референсного значения), средний (в 10 раз выше) или высокий (в 2 раза выше).
- Объектами мониторинга могут быть узлы, клиенты, серверы, пары «клиент — сервер» или весь трафик.
- Параметром для отслеживания может быть, например, объем входящего трафика или количество сетевых сессий.

Как использовать?

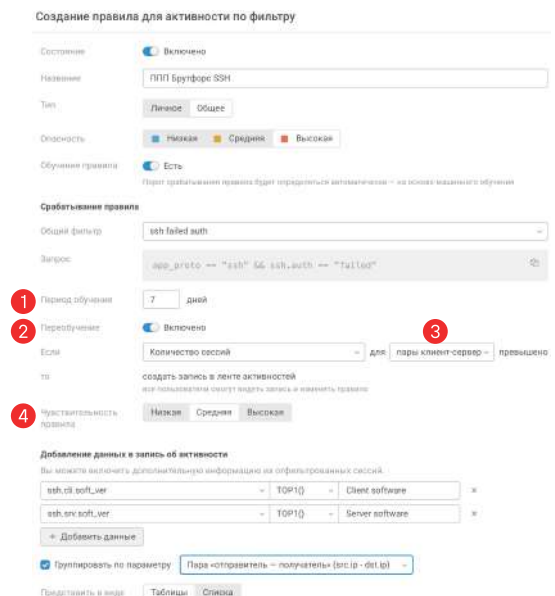
- Подготовьте и сохраните пользовательский фильтр.
- Нажмите кнопку «Настройка правил» в сохраненном фильтре.
- В открывшемся окне включите обучение (Обучение правил ☒ Есть) после чего появится блок параметров ППП.



Настройка ППП

- 1 Период обучения.**
Если исторические данные есть в Elasticsearch, ППП обучится на них — это займет несколько минут. Если данных нет, придется их собрать — потребуется минимум 7 дней.
- 2 Переобучение правила.**
По умолчанию переобучение включено, что позволяет PT NAD каждый день дообучаться на актуальных данных. При возникновении аномалий ППП будет срабатывать на них только один день.
- 3 Объект мониторинга и параметр.**
PT NAD будет уведомлять о превышении порогового значения параметра.
- 4 Чувствительность правила.**
Ее можно изменить в будущем: увеличить, если требуется уведомлять даже о незначительных аномалиях, или уменьшить, если правило генерирует излишние срабатывания.

 Оператор может дополнительно указать, какими данными сессии необходимо обогатить карточку срабатывания ППП в ленте активностей, а также добавить собственное описание.



 После создания ППП обучение запустится автоматически. Вам останется дожидаться всплывающего сообщения «Обучение завершено» в разделе с правилами.

 Обучение завершено
Период обучения — с 25 апреля, 12:41 по 2 мая, 12:41  Перезапустить

Обнаружение брутфорса SSH

С помощью этого правила PT NAD обнаруживает попытки подбора учетных данных. Для его создания используйте фильтр:

```
app_proto == "ssh" && ssh.auth == "failed"
```

Пример: объект мониторинга — пара «клиент — сервер», параметр для отслеживания — количество сессий между ними. Аномальный рост числа таких сессий может указывать на попытку брутфорса.

Создание этого правила активности было рассмотрено выше. Для проверки мы эмулировали атаку с подбором учетных данных SSH, которую и обнаружил ППП. В карточке срабатывания ППП в ленте активностей находится информация о пользовательском фильтре, клиенте, сервере, логарифмический график с аномальным всплеском и секция с дополнительными данными, которые указал оператор.

На графике видно, что порогом срабатывания стало значение 10 сессий в час, а во время подбора пароля мы сгенерировали 160 сессий.

Общие сведения

Обнаружено превышение количества сессий с клиентом 10.0.0.10 и сервером

Опасность: ■ Высокая
Первая сессия: 2 мая, 12:55
Последняя сессия: 2 мая, 13:27
Длительность: 31 мин 59 с
Обнаружена: 2 мая, 13:41
Чувствительность правила: Средняя

Пользовательский фильтр

```
app_proto == "ssh" && ssh.auth == "failed"
```

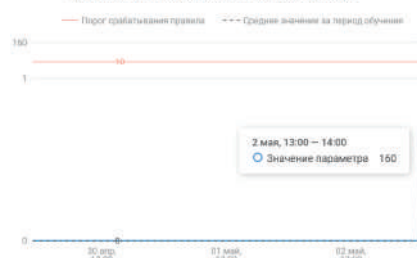
Информация о клиенте

Узел: H1337
IP-адрес: 10.0.0.10
Группы: HOME_NET, VPN

Информация о сервере

Узел: H96333
IP-адрес: 10.1.0.100
Группы: SERVERS, HOME_NET

Превышение порога срабатывания правила



Обнаружение эксфильтрации данных на облачные сервисы

С помощью этого правила можно вовремя обнаружить эксфильтрацию данных.

Возьмем для примера облачные сервисы, которые PT NAD определяет автоматически на основании полей протоколов:

```
app_service in ["Yandex.disk", "DropBox", "GoogleDrive", "MS_OneDrive"]
```



Полный список приложений, которые обнаруживает PT NAD, можно найти в онлайн-документе

Для проверки ППП мы также сгенерировали аномальный всплеск активности. На графике в карточке активности видно, что после обучения порогом для срабатывания стало значение в 134 МБ данных, отправленных на облачные сервисы, а размер аномальной активности составил более 2 ГБ исходящего трафика.

Создание правила для активности по фильтру

Состояние: ☒ Включено

Название: ППП Автоматическая выгрузка данных на облачные сервисы

Тип: ☒ Базовое ☐ Общее

Опасность: ☒ Низкая ☐ Средняя ☐ Высокая

Обучение правилу: ☒ Есть

Порог срабатывания правила будет определяться автоматически на основе начального обучения

Срабатывание правила

Общий фильтр: Cloud Storage Services

Запрос: app_service in ["Yandex.disk", "DropBox", "GoogleDrive", "MS_OneDrive"]

Период обучения: 14 дней

Параметры обучения: ☒ Включено

Единица: Объем исходящего трафика для клиента - превышение

Число: создать запись в ленте активностей

Чувствительность правила: ☒ Низкая ☐ Средняя ☐ Высокая

Общие сведения

Обнаружено превышение объема исходящего

Опасность: ■ Средняя
Первая сессия: 2 мая, 18:55
Последняя сессия: 2 мая, 19:00
Длительность: 12 ч 57 мин 4 с
Обнаружена: 2 мая, 18:55
Чувствительность правила: Средняя

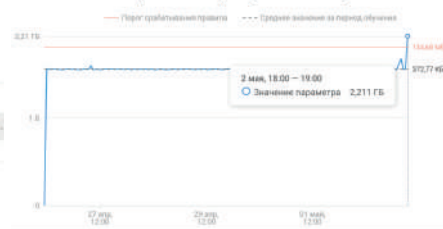
Пользовательский фильтр

```
app_service in ["Yandex.disk", "DropBox"]
```

Информация о клиенте

Узел: H96333
IP-адрес: 10.1.0.100
Группы: SERVERS, HOME_NET

Превышение порога срабатывания правила



Чтобы получить более детальную информацию, оставьте заявку



Подписывайтесь на телеграм-канал PT NAD — получайте ответы на вопросы и самые свежие новости о продукте