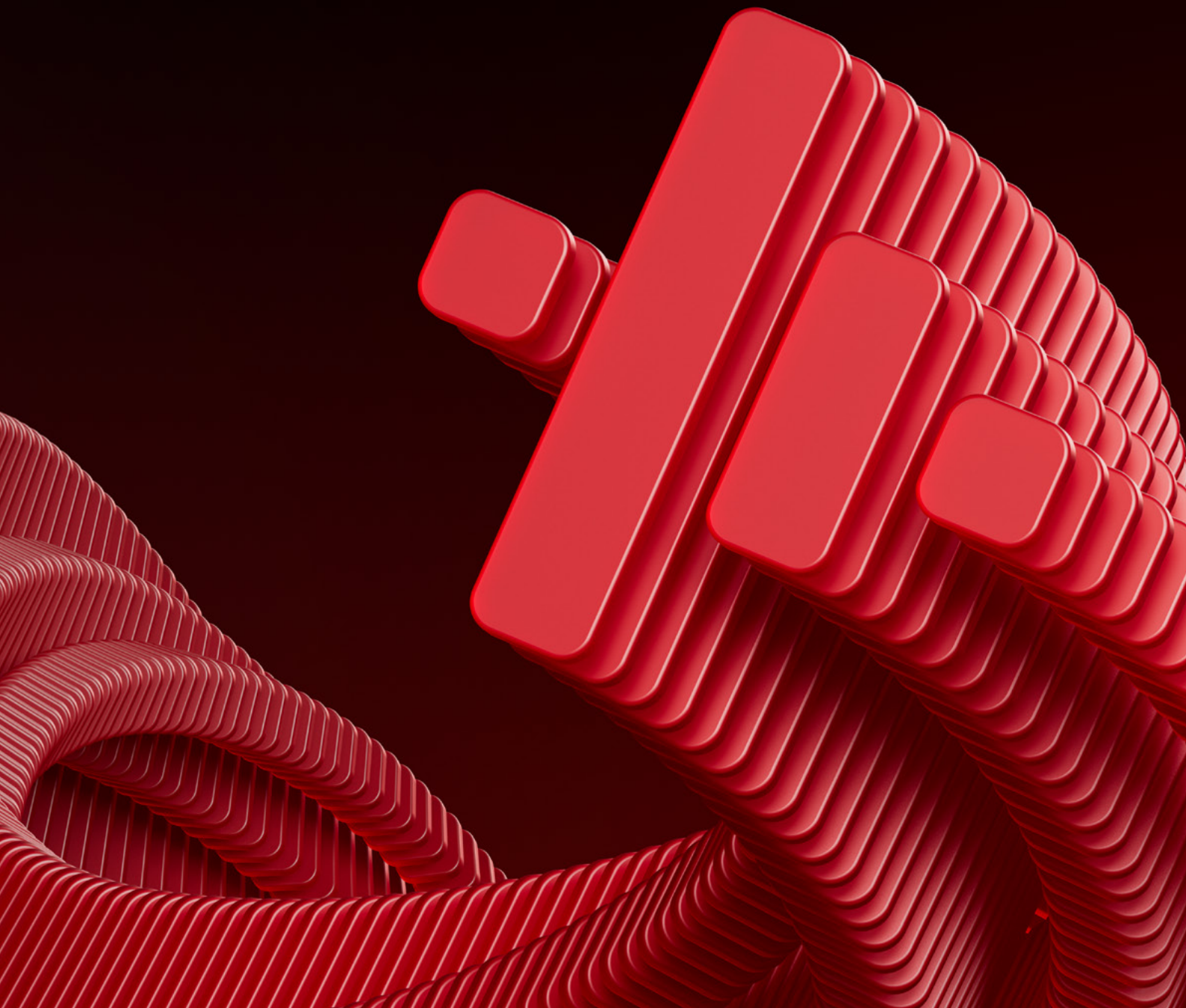
positive technologies

ПРАВИЛА ДЛЯ АКТИВНОСТЕЙ В PT NAD

Практические сценарии для операторов



Правила для активностей — механизм поиска индикаторов атаки (IoA) и подозрительных событий в сетевом трафике на основе индексированных PT NAD метаданных.

1. Благодаря идентификации нелегитимных информационных потоков возможно митигировать уязвимость до ее обнаружения злоумышленником.

2. Принцип работы: пользователь задает фильтр, используя атрибуты трафика (например, IP-адреса, порты, протоколы, значения заголовков, в том числе прикладных протоколов, группы узлов, сервисы, данные PT Sandbox, репутационные списки). При совпадении данных из трафика с фильтром в ленте активностей создается событие.

3. Результат — автоматическое создание карточек в ленте активностей для оперативного оповещения оператора и расследования.

4. Гибкость: используйте встроенные правила или создавайте собственные под специфические задачи ИБ.

ПРАКТИЧЕСКИЕ СЦЕНАРИИ (USE CASES)

Конкретные задачи, решаемые правилами для активностей в PT NAD

Сценарий 1

ПОИСК НЕЛЕГИТИМНЫХ ИНФОРМАЦИОННЫХ ПОТОКОВ МЕЖДУ СЕГМЕНТАМИ СЕТИ (нарушение политик доступа)

Проблема

Необходимо контролировать соблюдение политик сегментации (например, доступ к ДМЗ только по HTTPS/443), а также отслеживать ошибки при настройке временного доступа.

В компаниях часто используется логическая сегментация сети с раздельными политиками доступа. Важно проверять, что запрещенные информационные потоки отсутствуют. Например, доступ к сегменту ДМЗ может быть разрешен только через порт 443, но ошибки при выдаче прав доступа, особенно временных, могут привести к уязвимостям. Правила для активностей помогают выявлять нелегитимные сетевые потоки и предотвращать угрозы.

Решение

1. Создайте группы узлов: определите IP-адрес сети для сегментов (например, USERS, SERVERS, DMZ) в настройках групп узлов.
2. Настройте правило: используйте фильтр, например **src.groups == «USERS» && dst.groups == «SERVERS» && ssh.**

Результат

Оператору будут приходить мгновенные оповещения о любых нелегитимных попытках соединения между заданными сегментами.

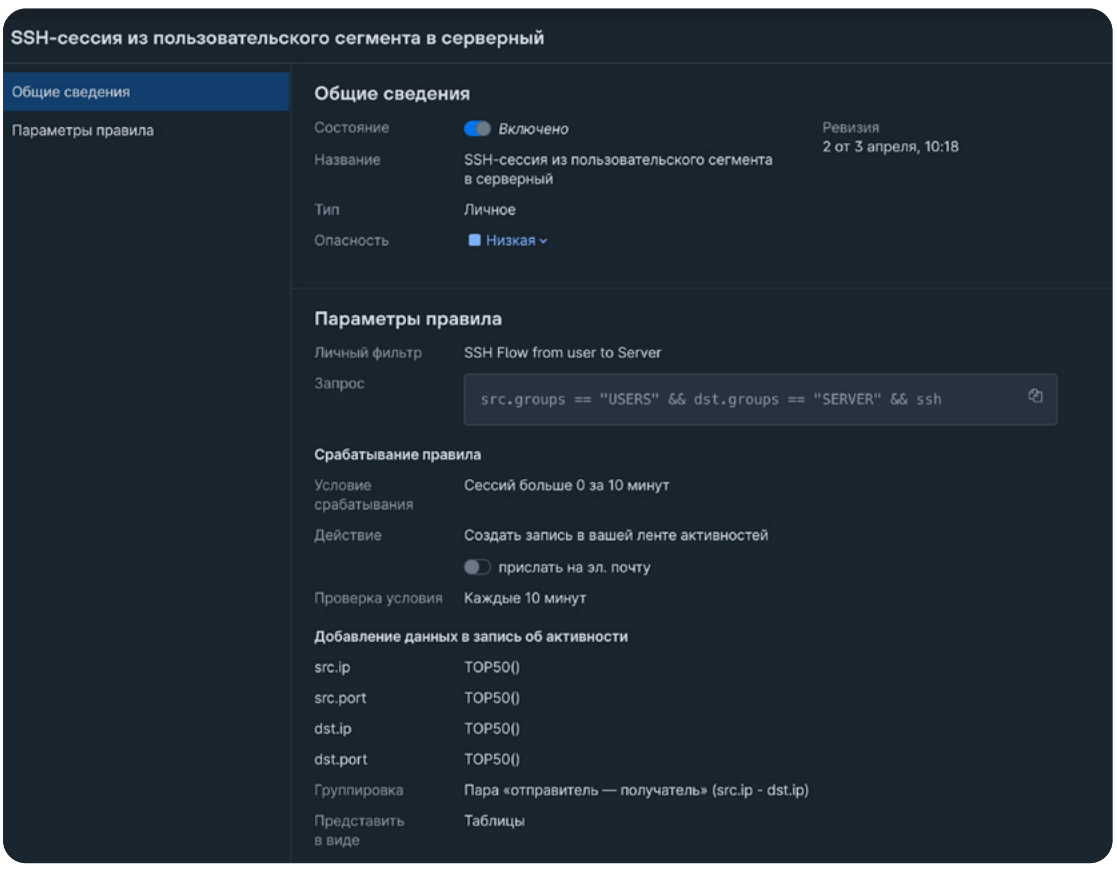


Рисунок 1. Пример правила для активностей, детектирующего нелегитимный информационный поток

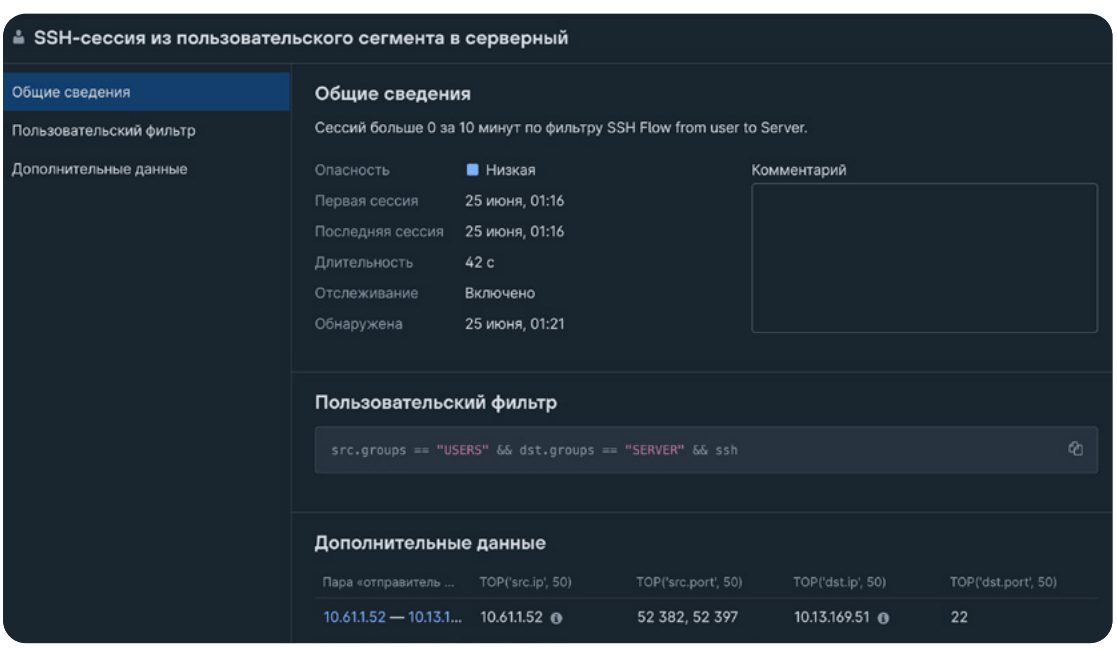


Рисунок 2. Карточка в ленте активностей, содержащая информацию о детектировании нелегитимного информационного потока

Сценарий 2

МОНИТОРИНГ ПОЛОЖИТЕЛЬНЫХ ВЕРДИКТОВ PT SANDBOX

Проблема

Необходимо быстро реагировать на файлы, признанные вредоносными песочницей PT Sandbox.

Решение

1. Изучите атрибуты отчетов PT Sandbox: **rpt.verdict** (наличие вердикта), **rpt.type** (тип угрозы).
2. Настройте правило: используйте фильтр, например **rpt.verdict && rpt.type != “dga”** (события с положительным вердиктом PT Sandbox, где тип угрозы не dga).

Результат

В ленте активностей появятся события, в которых указан вердикт песочницы (Malicious, Suspicious). Детальная информация о файле и отчете из PT Sandbox будет доступна в карточке события.

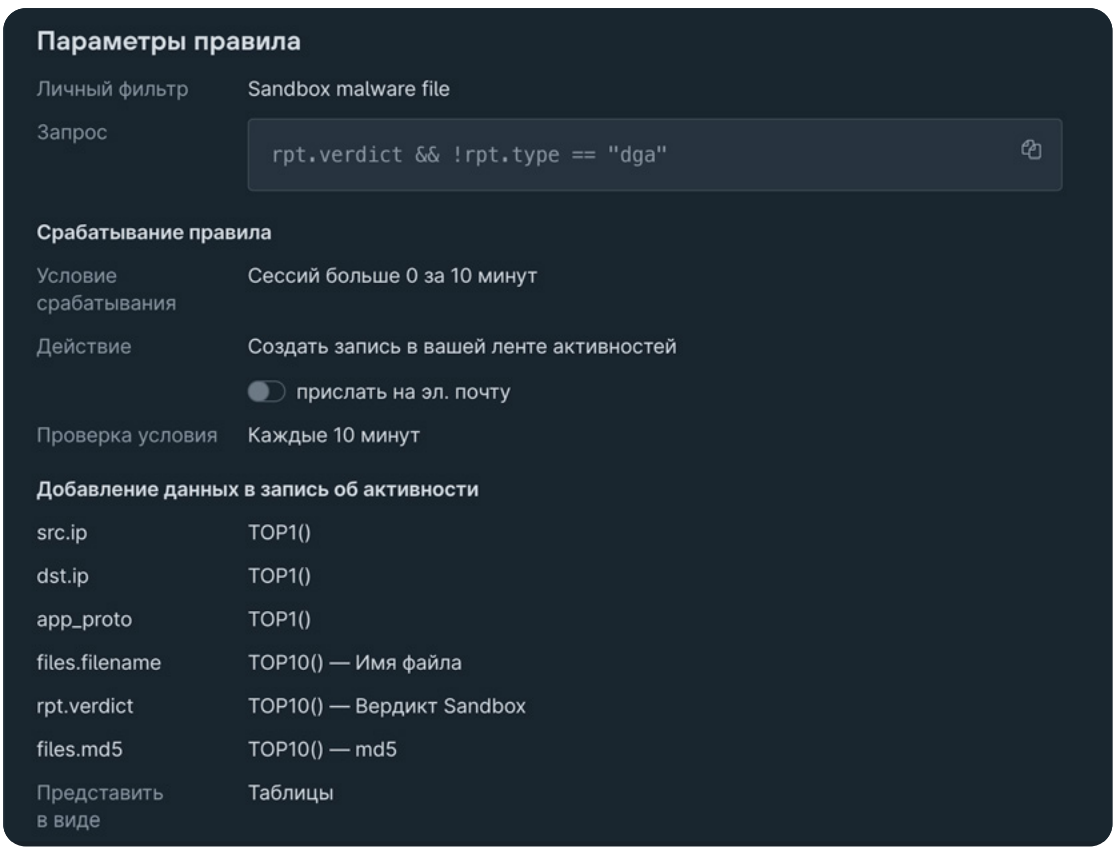


Рисунок 3. Пример правила для активностей, предназначенного для получения подробной информации о сессии, в которой передавался вредоносный файл

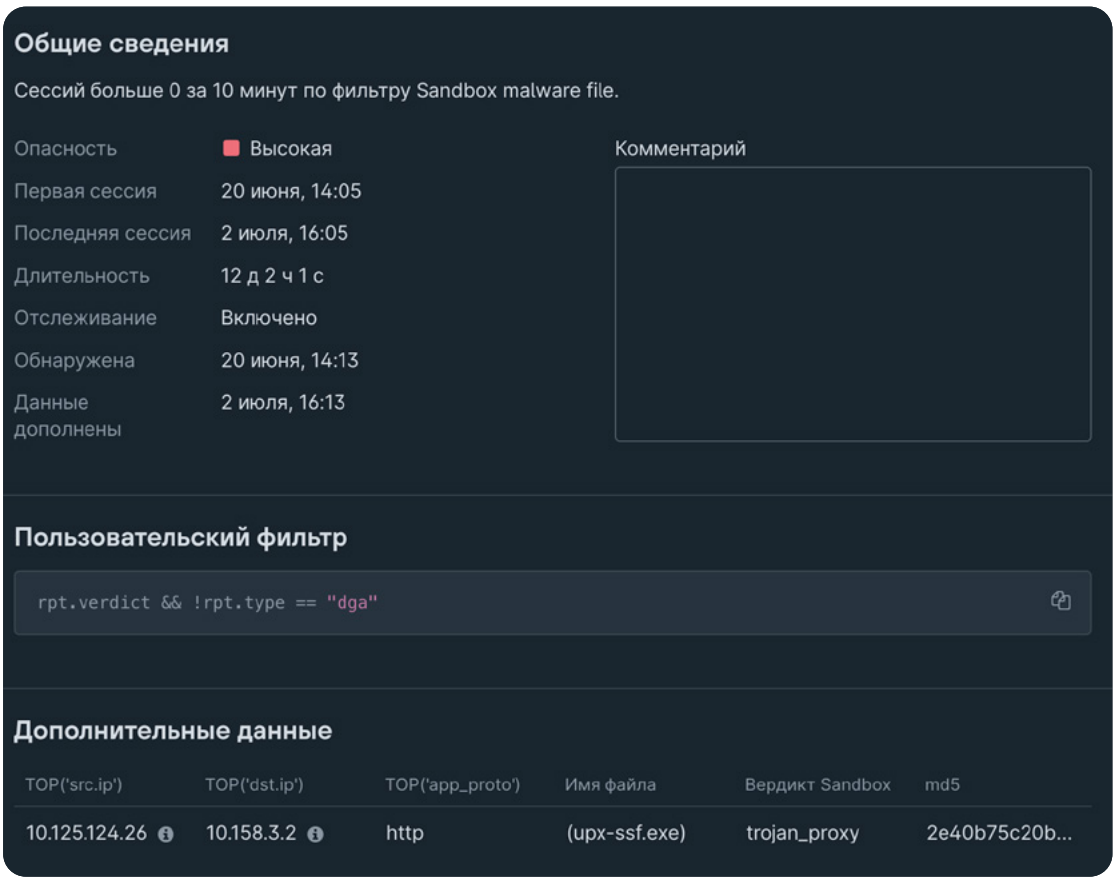


Рисунок 4. Карточка в ленте активностей с подробной информацией о сессии, содержащей вредоносный файл

Сценарий 3

ОТОБРАЖЕНИЕ СРАБАТЫВАНИЯ ПРАВИЛА НА КОНКРЕТНЫЙ РЕПУТАЦИОННЫЙ СПИСОК

Проблема

Критически важно мгновенно узнавать о появлении в трафике индикаторов (IP-адресов, доменов, URL) из ваших собственных черных списков.

Решение

1. Создайте и наполните репутационный список.
2. Настройте правило: фильтр по категории списка — **rpt.cat == «Имя репутационного списка».**

Результат

События в ленте активностей будут появляться при каждом совпадении данных из трафика с индикатором из вашего списка.

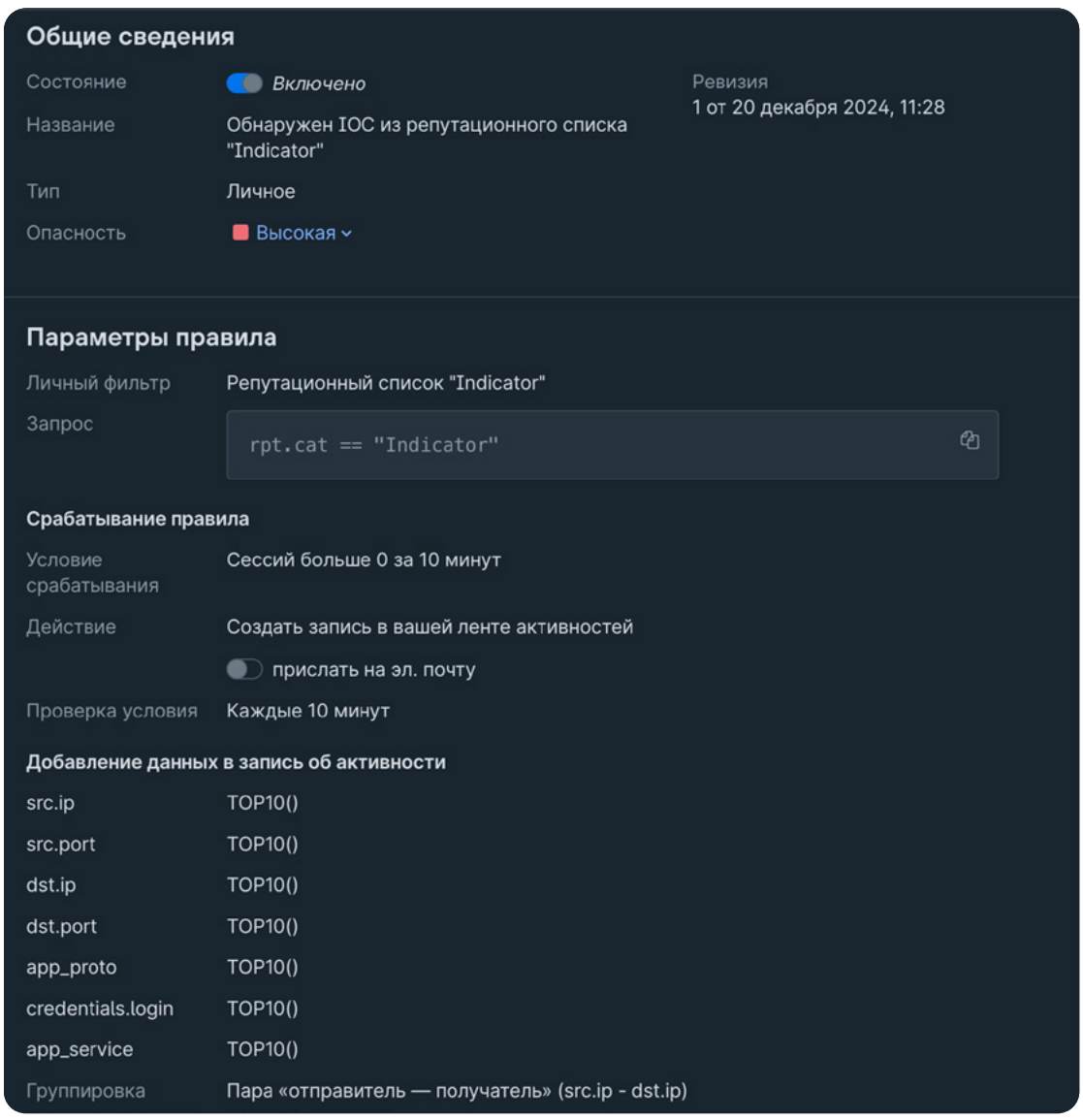


Рисунок 5. Пример правила для активностей, предназначенного для отображения подробной информации о зафиксированных индикаторах компрометации

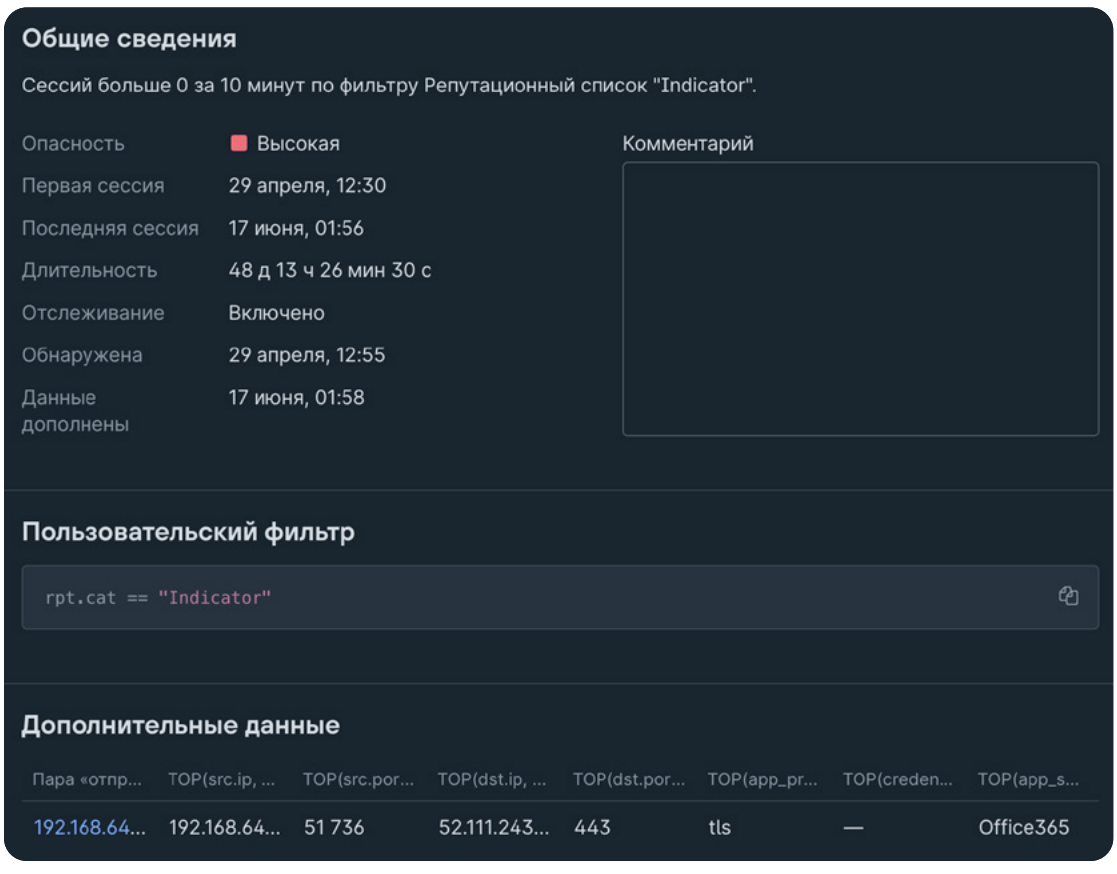


Рисунок 6. Карточка в ленте активностей, содержащая подробную информацию о зафиксированных индикаторах компрометации

Сценарий 4

МОНИТОРИНГ ПОСТУПЛЕНИЯ ТРАФИКА В PT NAD

Проблема

Сбой подачи трафика (со SPAN, TAP, агента) в PT NAD — это слепота системы. Нужен оперативный контроль.

Решение

1. Определите источники трафика.
2. Создайте группу узлов (например, **PRODUCTION_SERVERS**) и включите в нее IP-адреса ключевых серверов.
3. Настройте правило: укажите общий фильтр, условие срабатывания, периодичность проверки, важность и действие (например, «Создать карточку в ленте активностей»).

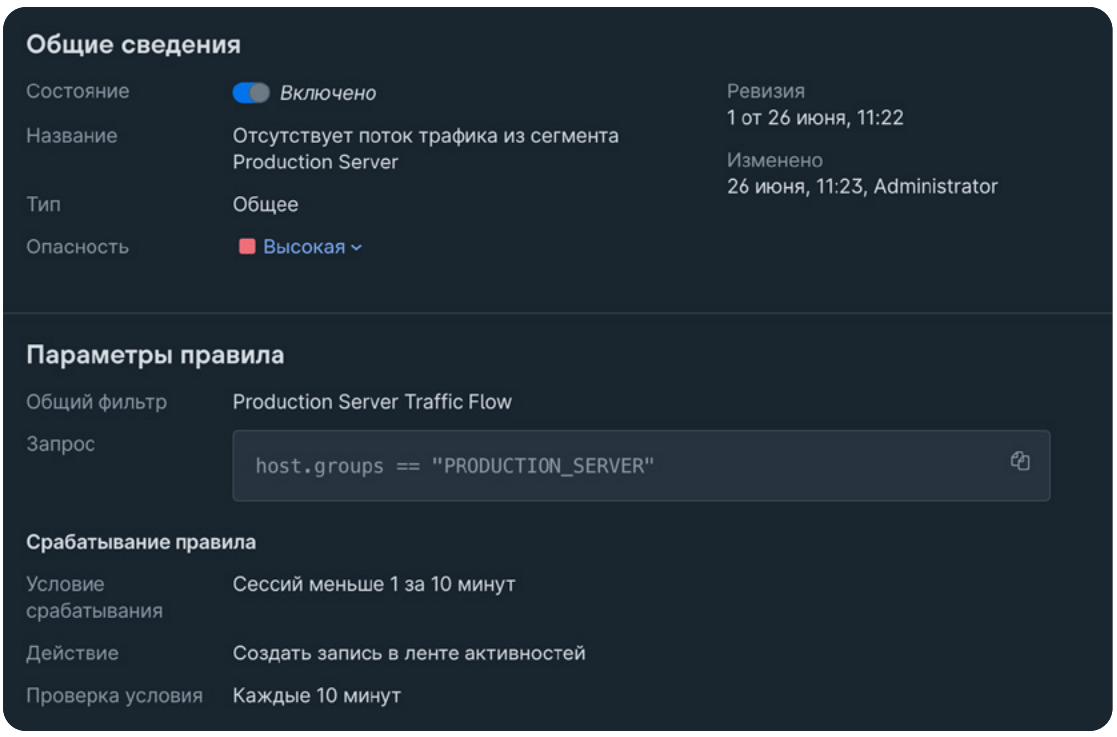


Рисунок 7. Пример правила для активностей, предназначенного для отслеживания поступления трафика

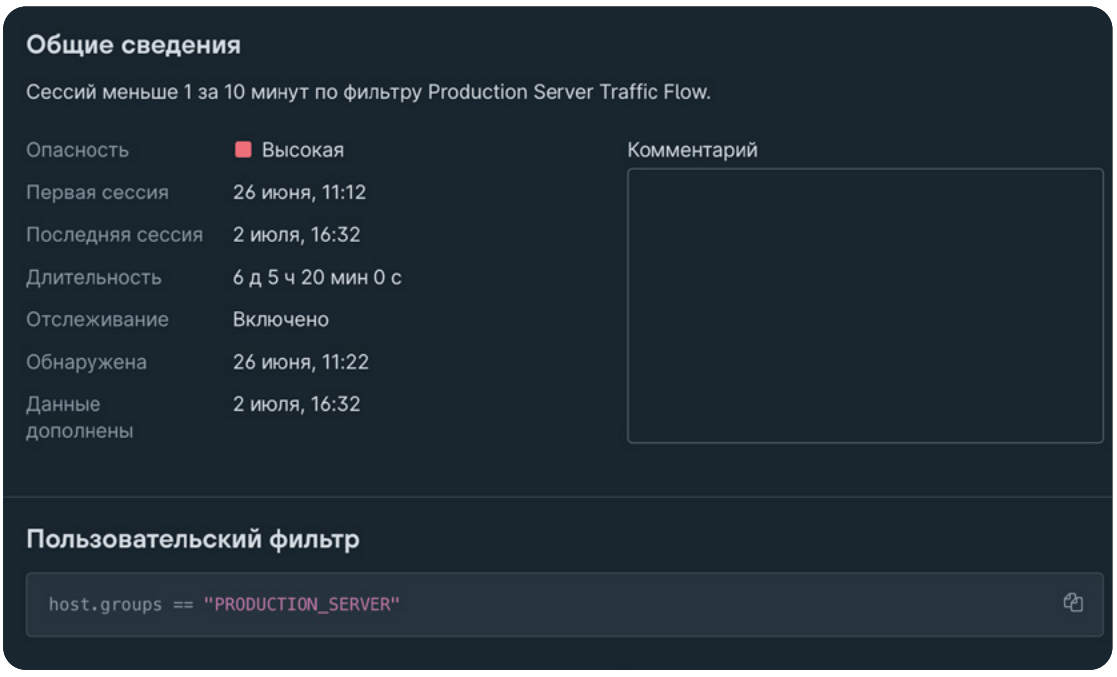


Рисунок 8. Карточка в ленте активностей с информацией об отсутствии трафика

Результат

Оперативные оповещения о резком падении или отсутствии трафика, позволяющие быстро выявить и устранить проблему сбора данных.

Сценарий 5

КОНТРОЛЬ СЕТЕВОЙ АКТИВНОСТИ ПОДРЯДЧИКОВ

Проблема

Необходимо отслеживать и ограничивать сетевую активность внешних подрядчиков в соответствии с политиками.

Решение

1. Создайте группы узлов.
2. Настройте правило с параметрами.

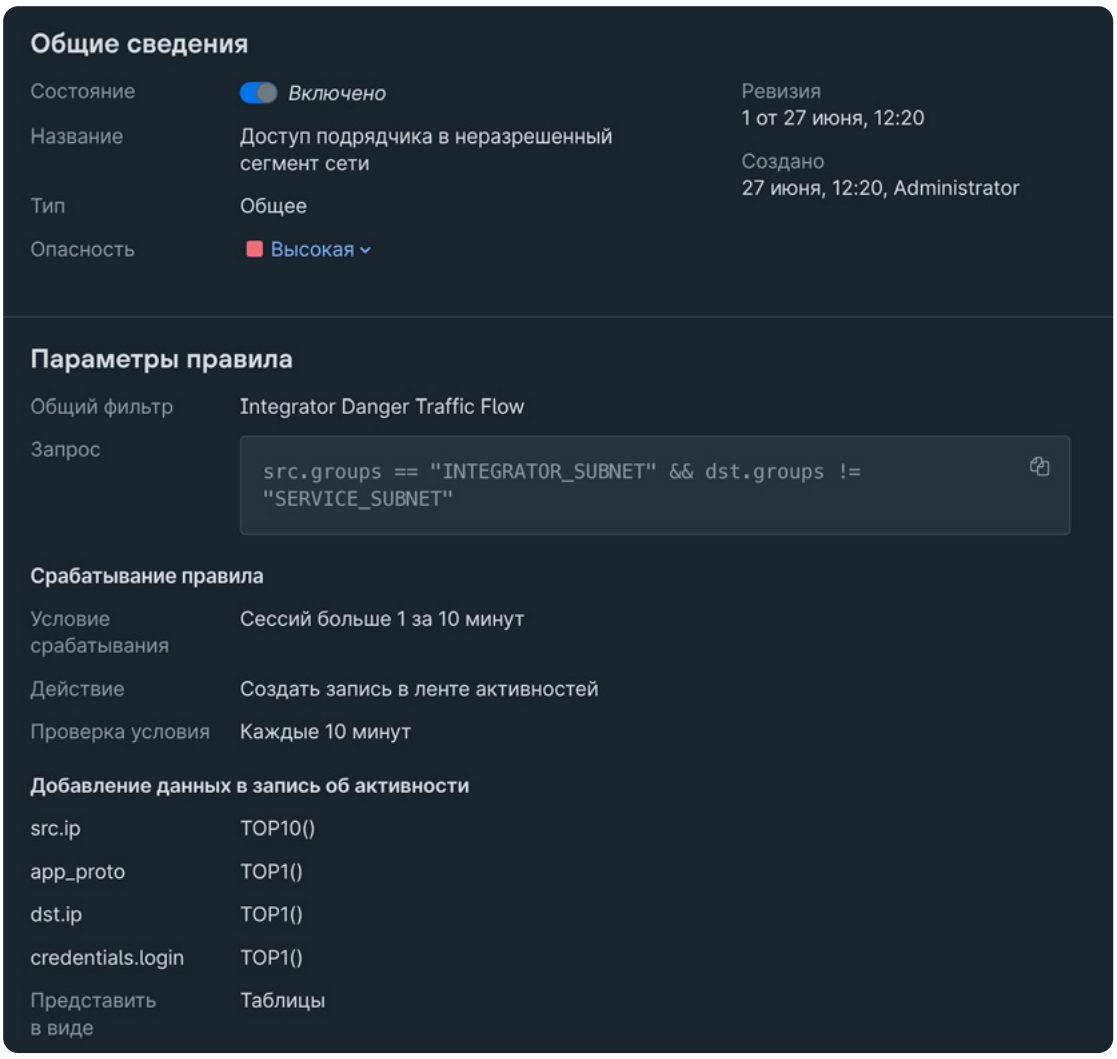


Рисунок 9. Пример правила для активностей, детектирующего доступ подрядчика к запрещенному для него сегменту сети

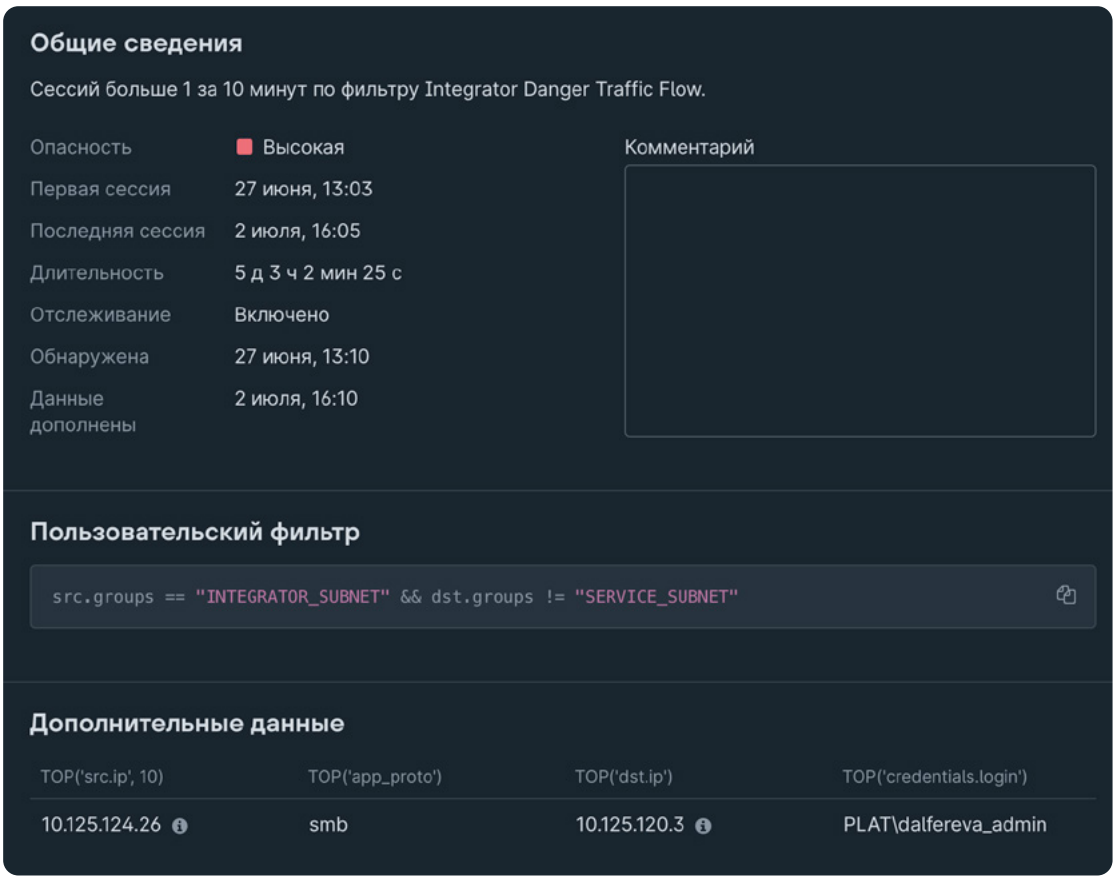


Рисунок 10. Карточка в ленте активностей, содержащая подробную информацию о нелегитимных сетевых потоках подрядчика

Результат

Прозрачность и контроль действий подрядчиков в вашей сети, быстрое выявление нарушений политик.

НЕ ОГРАНИЧИВАЙТЕСЬ ВСТРОЕННЫМИ ПРАВИЛАМИ!
СОЗДАВАЙТЕ СВОИ ПОД КОНКРЕТНЫЕ ЗАДАЧИ SOC И ОСОБЕННОСТИ ИНФРАСТРУКТУРЫ.

Телеграм-канал
о PT NAD

Узнать больше
о PT NAD