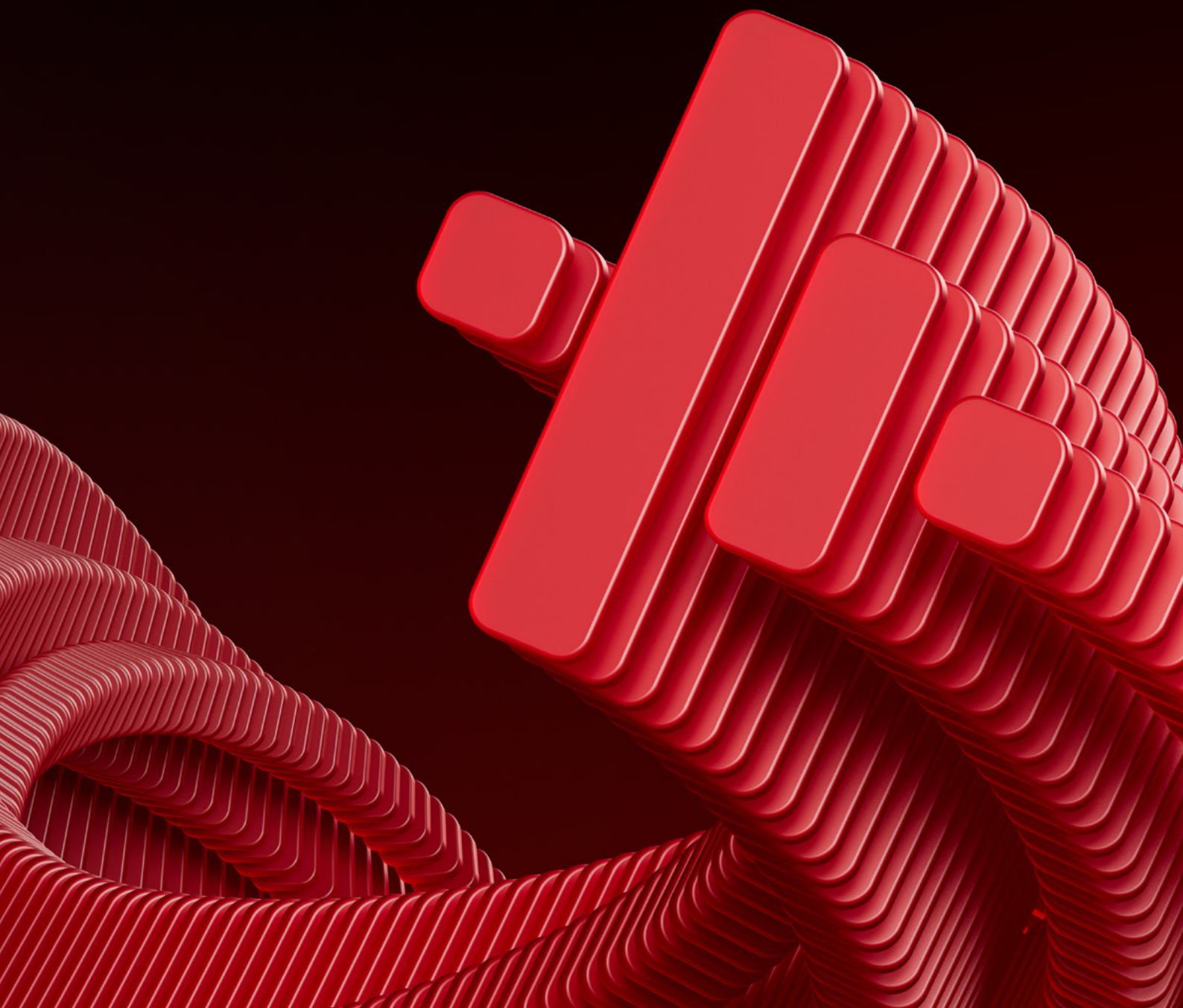


ПРАВИЛА ДЛЯ АКТИВНОСТЕЙ В РТ NAD

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 отдельными 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 <code>src.groups == «USERS» && dst.groups == «SERVERS» && ssh</code>.
Результат	Оператору будут приходить мгновенные оповещения о любых нелегитимных попытках соединения между заданными сегментами.

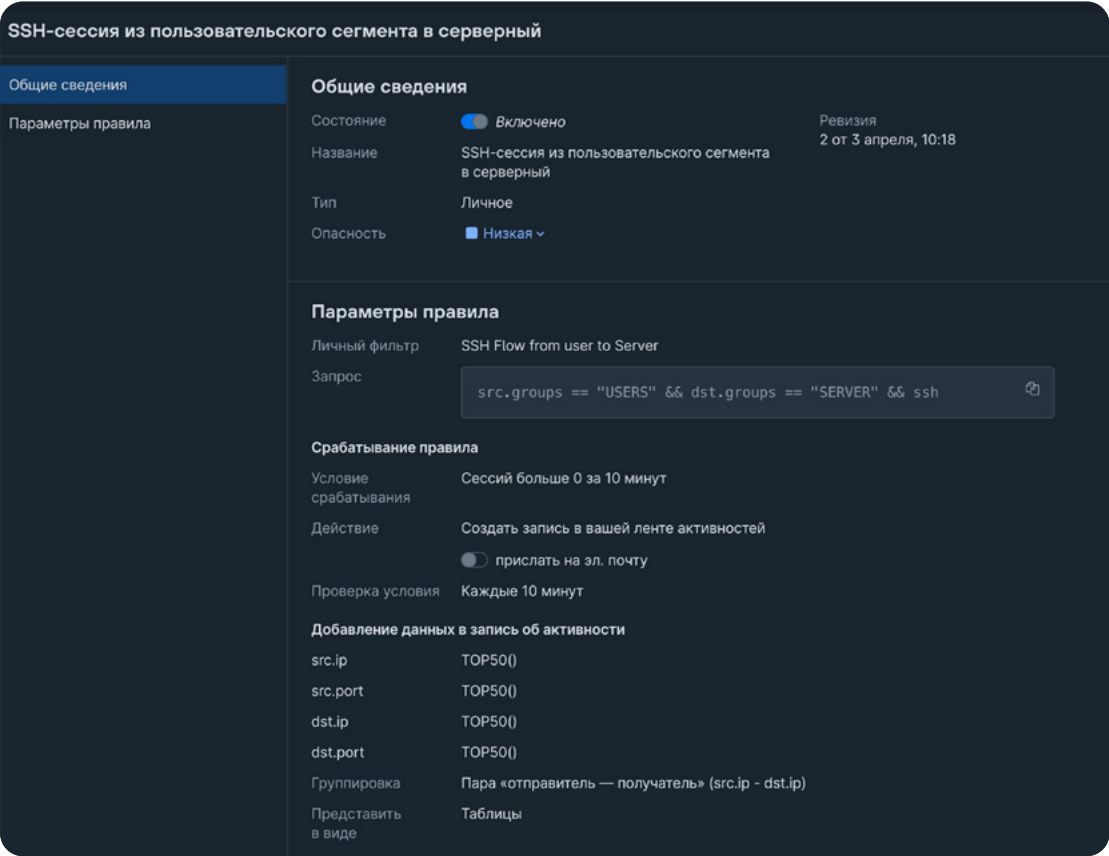


Рисунок 1. Пример правила для активностей, детектирующего нелегитимный информационный поток

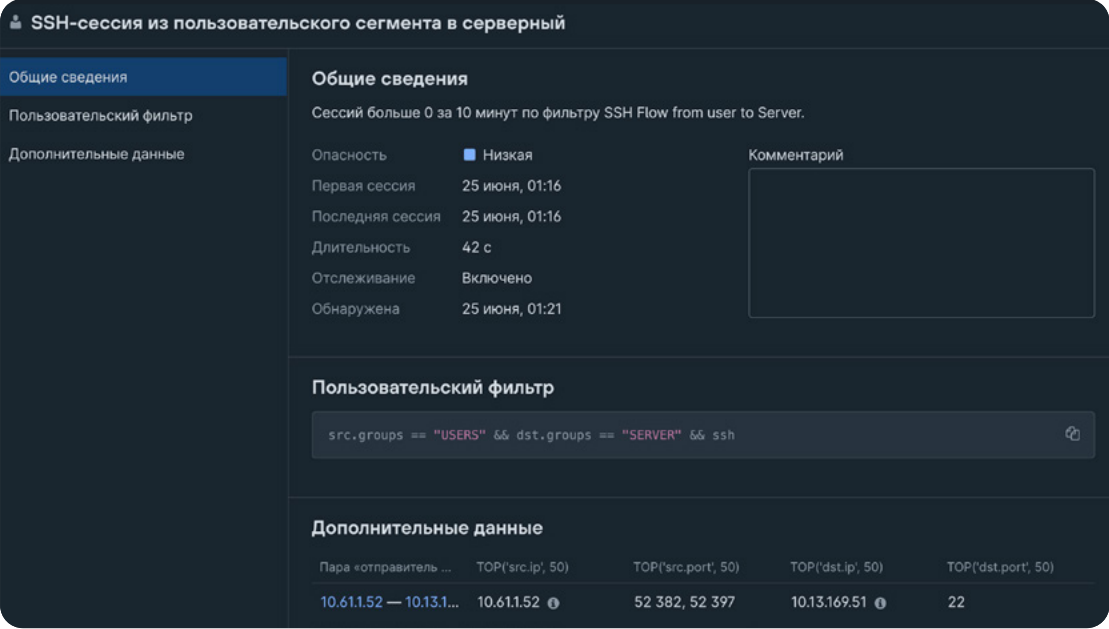


Рисунок 2. Карточка в ленте активностей, содержащая информацию о детектировании нелегитимного информационного потока

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.

Параметры правила

Личный фильтр

Sandbox malware file

Запрос

rpt.verdict && !rpt.type == "dga"

Срабатывание правила

Условие срабатывания

Сессий больше 0 за 10 минут

Действие

Создать запись в вашей ленте активностей

прислать на эл. почту

Проверка условия

Каждые 10 минут

Добавление данных в запись об активности

src.ip

TOP1()

dst.ip

TOP1()

app_proto

TOP1()

files.filename

TOP10() — Имя файла

rpt.verdict

TOP10() — Вердикт Sandbox

files.md5

TOP10() — md5

Представить в виде

Таблицы

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

Общие сведения

Сессий больше 0 за 10 минут по фильтру Sandbox malware file.

Опасность

Высокая

Первая сессия

20 июня, 14:05

Последняя сессия

2 июля, 16:05

Длительность

12 д 2 ч 1 с

Отслеживание

Включено

Обнаружена

20 июня, 14:13

Данные дополнены

2 июля, 16:13

Комментарий

Пользовательский фильтр

rpt.verdict && !rpt.type == "dga"

Дополнительные данные

TOP('src.ip')

10.125.124.26 ⓘ

TOP('dst.ip')

10.158.3.2 ⓘ

TOP('app_proto')

http

Имя файла

(upx-ssf.exe)

Вердикт Sandbox

trojan_proxy

md5

2e40b75c20b...

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

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 заполните 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.

Общие сведения

Состояние

Включено

Название

Обнаружен IOC из репутационного списка "Indicator"

Тип

Личное

Опасность

Высокая

Ревизия

1 от 20 декабря 2024, 11:28

Параметры правила

Личный фильтр

Репутационный список "Indicator"

Запрос

rpt.cat == "Indicator"

Срабатывание правила

Условие срабатывания

Сессий больше 0 за 10 минут

Действие

Создать запись в вашей ленте активностей

прислать на эл. почту

Проверка условия

Каждые 10 минут

Добавление данных в запись об активности

src.ip

TOP10()

src.port

TOP10()

dst.ip

TOP10()

dst.port

TOP10()

app_proto

TOP10()

credentials.login

TOP10()

app_service

TOP10()

Группировка

Пара «отправитель — получатель» (src.ip - dst.ip)

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

Общие сведения

Сессий больше 0 за 10 минут по фильтру Репутационный список "Indicator".

Опасность

Высокая

Первая сессия

29 апреля, 12:30

Последняя сессия

17 июня, 01:56

Длительность

48 д 13 ч 26 мин 30 с

Отслеживание

Включено

Обнаружена

29 апреля, 12:55

Данные дополнены

17 июня, 01:58

Комментарий

Пользовательский фильтр

rpt.cat == "Indicator"

Дополнительные данные

Пара «отпр...

192.168.64...

TOP(src.ip, ...

192.168.64...

TOP(src.por...

51 736

TOP(dst.ip, ...

52.111.243...

TOP(dst.por...

443

TOP(app_pr...

tls

TOP(creden...

—

TOP(app_s...

Office365

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

МОНИТОРИНГ ПОСТУПЛЕНИЯ ТРАФИКА В РТ NAD

Проблема	Сбой подачи трафика (со SPAN, TAP, агента) в РТ 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»).

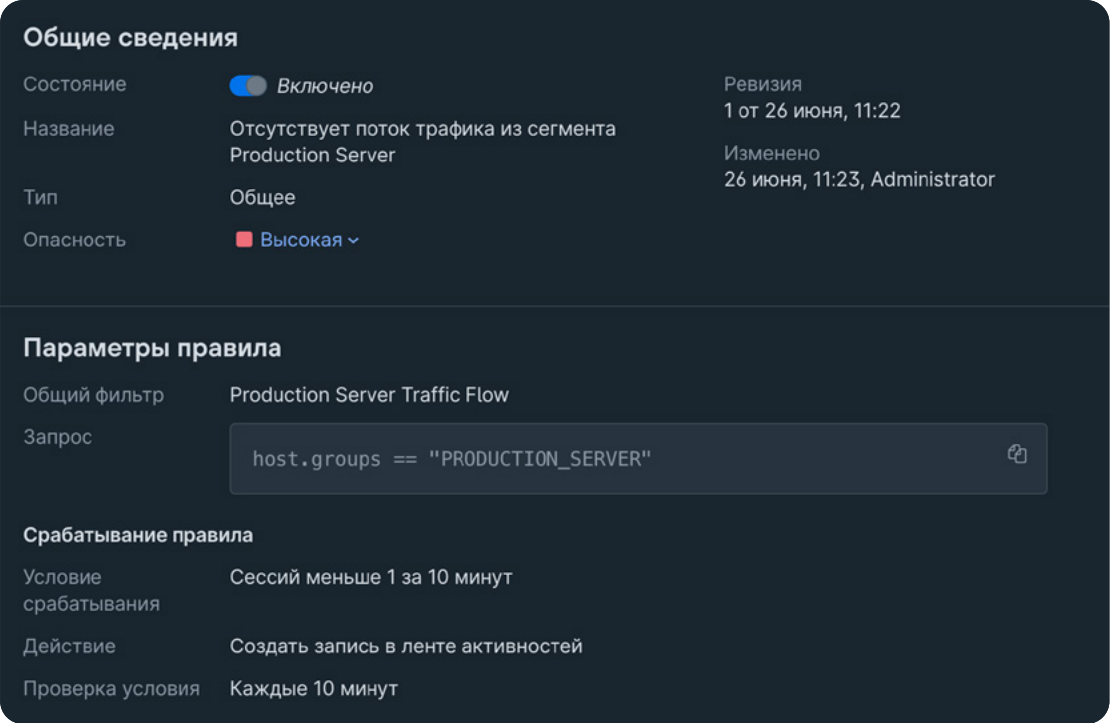


Рисунок 7. Пример правила для активностей, предназначенного для отслеживания поступления трафика

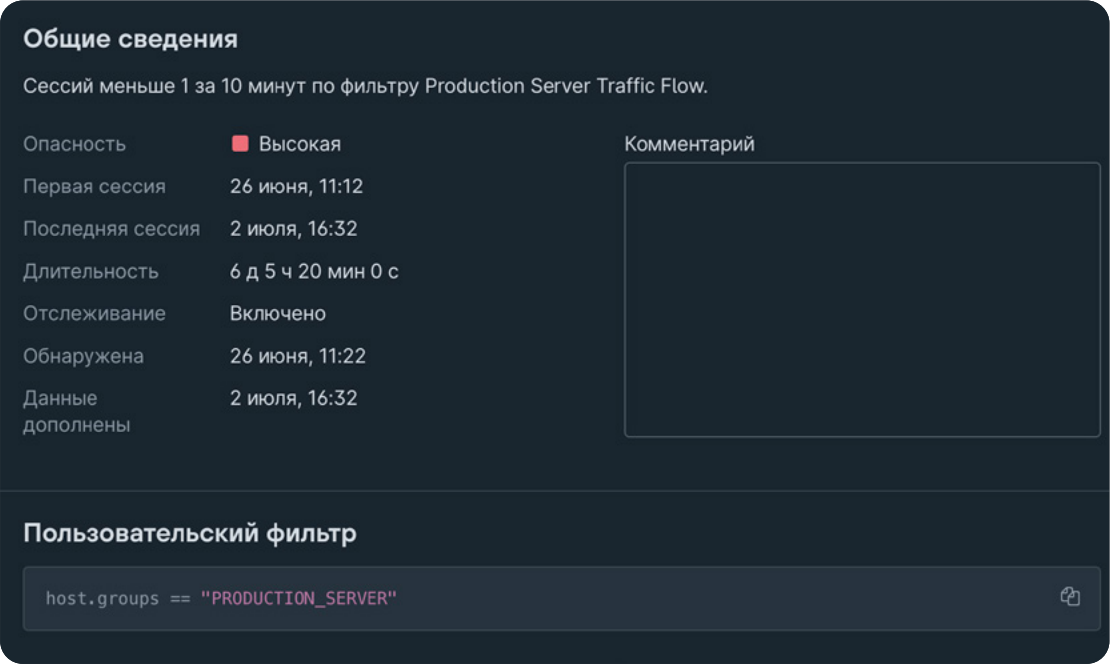


Рисунок 8. Карточка в ленте активностей с информацией об отсутствии трафика

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

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.

Общие сведения

Состояние

Включено

Название

Доступ подрядчика в неразрешенный сегмент сети

Тип

Общее

Опасность

Высокая

Ревизия

1 от 27 июня, 12:20

Создано

27 июня, 12:20, Administrator

Параметры правила

Общий фильтр

Integrator Danger Traffic Flow

Запрос

src.groups == "INTEGRATOR_SUBNET" && dst.groups != "SERVICE_SUBNET"

Срабатывание правила

Условие срабатывания

Сессий больше 1 за 10 минут

Действие

Создать запись в ленте активностей

Проверка условия

Каждые 10 минут

Добавление данных в запись об активности

src.ip

TOP10()

app_proto

TOP1()

dst.ip

TOP1()

credentials.login

TOP1()

Представить в виде

Таблицы

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

Общие сведения

Сессий больше 1 за 10 минут по фильтру Integrator Danger Traffic Flow.

Опасность

Высокая

Первая сессия

27 июня, 13:03

Последняя сессия

2 июля, 16:05

Длительность

5 д 3 ч 2 мин 25 с

Отслеживание

Включено

Обнаружена

27 июня, 13:10

Данные дополнены

2 июля, 16:10

Комментарий

Пользовательский фильтр

src.groups == "INTEGRATOR_SUBNET" && dst.groups != "SERVICE_SUBNET"

Дополнительные данные

TOP('src.ip', 10)

10.125.124.26 ⓘ

TOP('app_proto')

smb

TOP('dst.ip')

10.125.120.3 ⓘ

TOP('credentials.login')

PLAT\dalfereva_admin

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