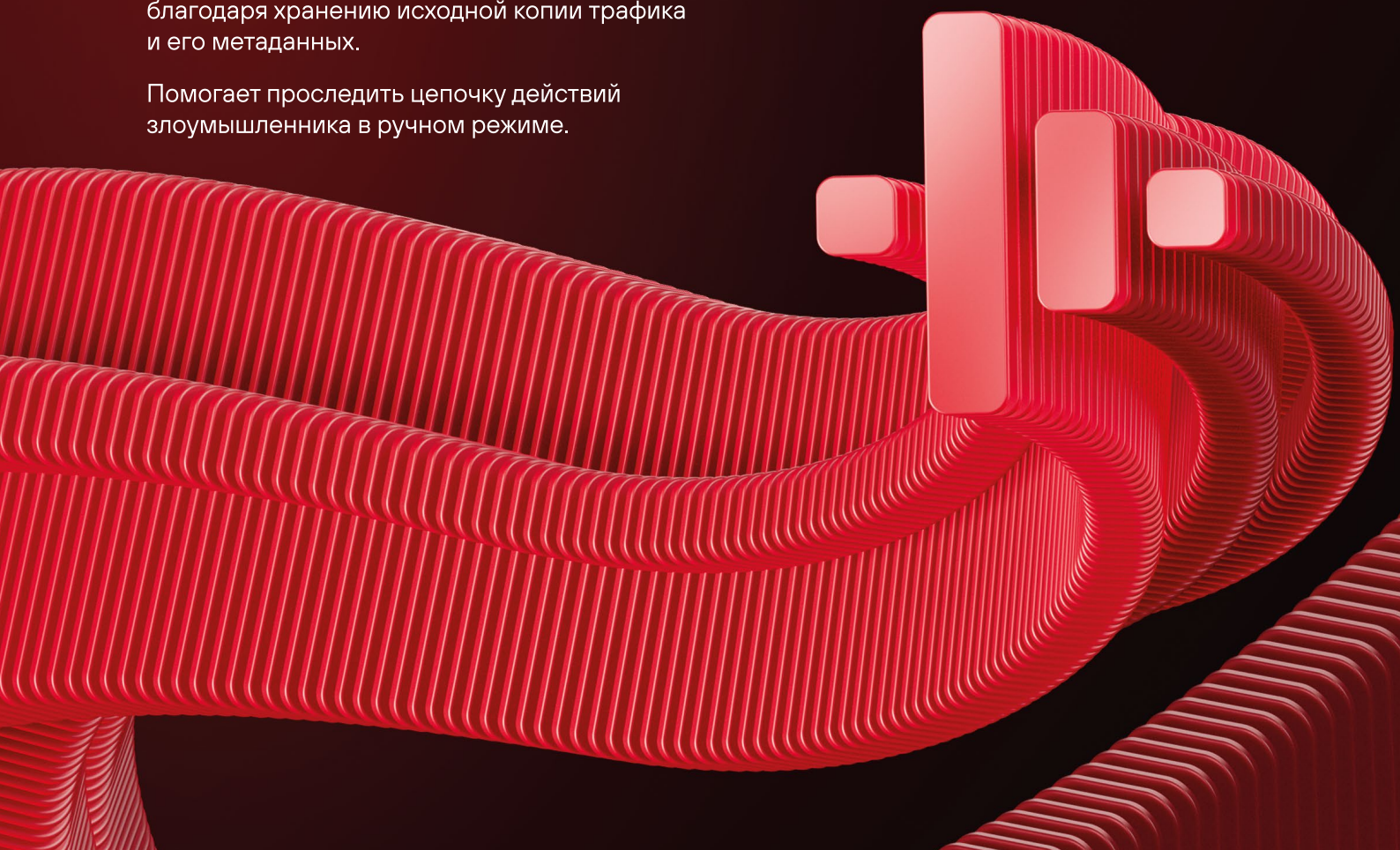
positive technologies

2 шага для работы с PT NAD

PT NAD - система поведенческого анализа трафика для выявления сложных атак внутри сети:

Позволяет проверять ложные срабатывания правил благодаря хранению исходной копии трафика и его метаданных.

Помогает проследить цепочку действий злоумышленника в ручном режиме.



positive technologies

Что делать, если

В интерфейсе слишком много алертов и непонятно, с чего начать.

Непонятно, происходит ли инцидент прямо сейчас.

Неочевидно, какие алерты являются реальными атаками.

Неясно, какие алерты смотреть в первую очередь.

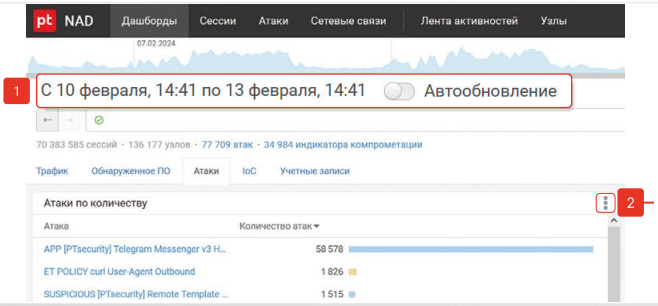
Шаг 1 Скачиваем все алерты

1

Выбираем временной интервал

(чем больше интервал, тем больше видно алертов, но важно не перегружать PT NAD).

Оптимально — три дня.



Скачать в формате JSON

Скачать в формате CSV

2

Скачиваем CSV-файл

Дашборды → Виджет «Атаки по количеству» → ⋮ → «Скачать в формате CSV».

CSV-файл содержит колонки: msg, pr, count.

Алерты имеют три приоритета: красный (1), желтый (2) и серый (3).

Префиксы помогают распределить правила по категориям.

	A	B	C
1	msg	pr	count(*)
2	APP [PTsecurity] Telegram Messenger v3 HTTP	[[3,58611]]	58611
3	ET POLICY curl User-Agent Outbound	[[2,1827]]	1827
4	SUSPICIOUS [PTsecurity] Remote Template Retrieving Doc with VBA Project	[[3,1515]]	1515
5	REMOTE [PTsecurity] RMS	[[1,1381]]	1381
6	APP [PTsecurity] Viber Connection	[[3,1313]]	1313
7	ET EXPLOIT Hikvision IP Camera RCE Attempt (CVE-2021-36260)	[[2,1216]]	1216
8	ET SCAN Sipvicious Scan	[[2,1200]]	1200
9	ET SCAN Sipvicious User-Agent Detected (friendly-scanner)	[[2,1200]]	1200
10	APP [PTsecurity] Possible MTproto Telegram	[[3,838]]	838
11	ATTACK AD [PTsecurity] Access to Account Management ADWS via net-tcp	[[2,702]]	702
12	ATTACK [PTsecurity] Possible SMTP Bruteforce	[[2,684]]	684
13	ET POLICY Powershell Command With NonInteractive Argument Over SMB - Likely Lateral Movement	[[1,675]]	675
14	ATTACK AD [PTsecurity] KRB enumeration by username list 60 in a 2 minute	[[2,639]]	639
15	ET INFO External IP Lookup Service in DNS Query (ip-info .ff .avast .com)	[[3,567]]	567
16	SCAN [PTsecurity] zgrab Banner Grabber User-Agent Detected	[[2,494]]	494
17	SUSPICIOUS [PTsecurity] HTTP POST to jpg	[[3,447]]	447

Приоритеты

?

Что означают префиксы

TOOLS

— активность хакерских инструментов и фреймворков для постэксплуатации зараженных систем.

SHELL

— активность реверс- и веб-шеллов, иногда фреймворков для постэксплуатации зараженных систем.

ATTACK, ATTACK AD

— эксплуатация уязвимостей, проведение атак на периметре и в Active Directory.

MALWARE, REMOTE, STEALER, RANSOMWARE

— активность ВПО.

Примеры префиксов в ptrules

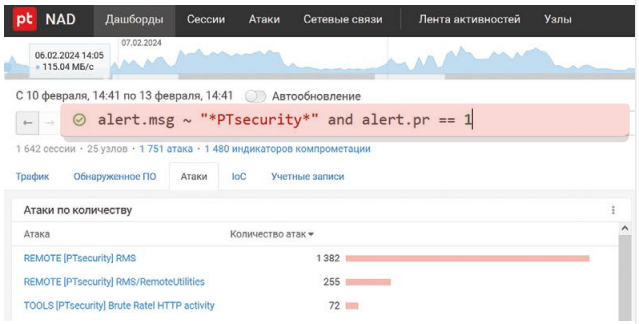
ATTACK [PTsecurity] Anonymous SMB connect to IPC share
MINER [PTsecurity] CoinMiner
TOOLS [PTsecurity] CobaltStrike SSH default banner
[ANOMALY] [PTsecurity] Unseen before ldap search query
LOGIN [PTsecurity] Joomla Login Successful
SINKHOLE [PTsecurity] snkz HTTP cookie set
TOOLS [PTsecurity] Ligolo TLS tunnel
POLICY [PTsecurity] SMB NTLM auth request to external net
DNS CANARY [PTsecurity] DNS Canary oastify.com resolution
SHELL [PTsecurity] Meterpreter TCP session opened
ATTACK AD [PTsecurity] NetSess enumeration user hosts
ADWARE [PTsecurity] DealPly
SENSITIVE [PTsecurity] Potentially APP_SECRET leaked
REMOTE [PTsecurity] RMS

positive technologies

Шаг 2 Разбираемся с алертами

1

- Фильтруем правила с первым приоритетом из нашего набора:
  `alert.msg ~ "*PTsecurity*" and alert.pr == 1`
- Это самые важные алерты, проверяем их в первую очередь. Обычно их не более 10 уникальных.
- Эти алерты срабатывают на присутствие злоумышленников в сети либо на активность ВПО.
- С ними можно разобраться всего за пару часов.
- Проверили эти алерты — все остальные проверяем без спешки.

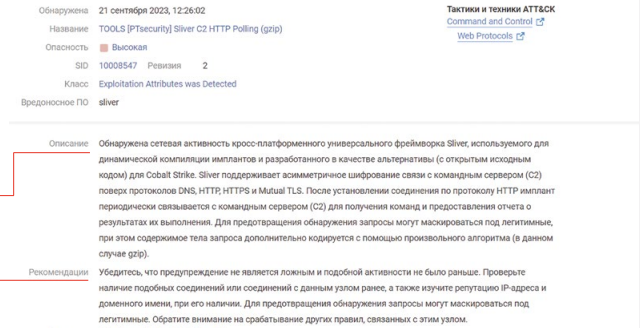


Уникальные описания и рекомендации

к алертам помогут оперативно проверить срабатывания и отреагировать на них:

Описание помогает определить, на какую активность сработало правило и чем она грозит.

Рекомендация содержит перечень шагов для проверки срабатывания.

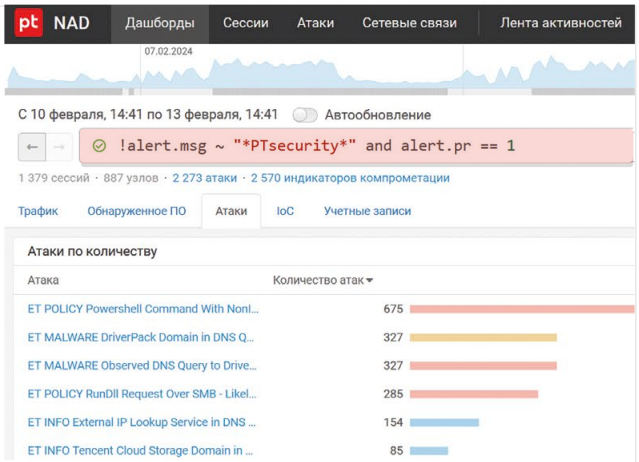


2

- Фильтруем правила с первым приоритетом из сторонних наборов:
  `!alert.msg ~ "*PTsecurity*" and alert.pr == 1`
- Описаний и рекомендаций для этих правил нет.
- Проверка ложных срабатываний может выполняться так же, как и проверка правил из нашего набора

! Если в вашей сети произошел инцидент, вы точно обнаружите его с помощью наших правил.

Важно понимать, что могут быть срабатывания без инцидентов (на легитимную активность).

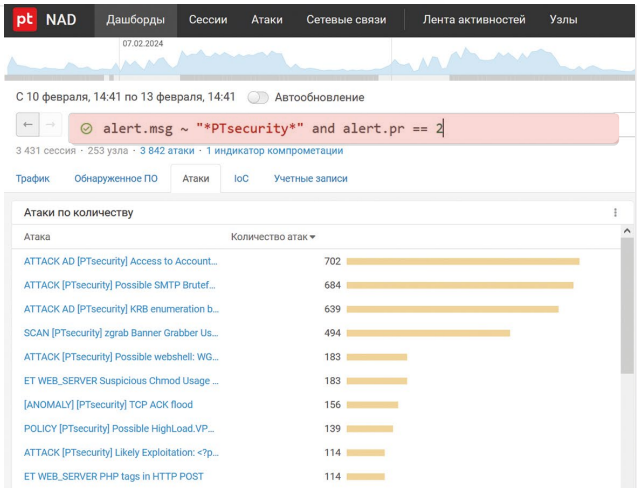


3

Фильтруем любые правила второго приоритета:
`alert.pr == 2`

В список могут попадать срабатывания на эксплуатацию уязвимостей на периметре или на активность внутри домена Active Directory. Их сложно однозначно отнести к вредоносным, но тоже важно проверять.

! Если правила срабатывают на легитимную активность в вашей сети (например, на TeamViewer, активность скриптов, сбор информации средствами защиты) — добавляйте их в исключения, чтобы в будущем снизить число таких алертов.



Итак, вы обработали срабатывания критически важных правил. Кроме красных и желтых существуют еще серые алерты. Они срабатывают на незначительные события, например на активность рекламного ПО (adware) или обращения к легитимным сервисам разных категорий, но могут помочь при расследовании инцидентов.

Репутационные списки

Кроме того, аналитику стоит проверять срабатывания репутационных списков и ленты активностей.

Принцип работы с лентой активностей тот же:

приоритеты обозначены цветами

в каждой карточке есть описания.

Обработать репутационные списки можно по алгоритму:

1. В первую очередь проверяем срабатывания ручных репутационных списков на домены.

Фильтр: `rpt.cat ~ "ESC-manual-*-dns"`

2. Во вторую — срабатывания ручных репутационных списков на IP-адреса.

Фильтр: `rpt.cat ~ "ESC-manual-*-ip"`

3. В третью — все остальное.

Важно

IP-адреса устаревают быстрее доменов, поэтому приоритет у репутационных списков DNS выше.

Средства защиты, например Check Point, могут во время работы резолвить вредоносные домены DNS. Обычно это выглядит как срабатывание множества разных репутационных списков с одного адреса. Проверяйте также сессии TCP/UDP на вредоносные индикаторы.

Злоумышленники могут сканировать интернет с вредоносных адресов. Эта активность генерирует множество неопасных срабатываний репутационных списков на входящие соединения.

Если индикатор сработал на большую DNS-сессию и вы не можете найти, на какой именно запрос он сработал, — перенесите эту сессию в хранилище, и она распадется на множество небольших сессий.

Репутационные списки по числу срабатываний

Посмотреть вебинар «Выявление сетевых атак с помощью PT NAD. Быстрый старт»

Телеграм канал по продукту PT NAD