Threat Intelligence Feeds

Описание продукта

© Positive Technologies, 2025.

Настоящий документ является собственностью Positive Technologies и защищен законодательством Российской Федерации и международными соглашениями об авторских правах и интеллектуальной собственности.

Копирование документа либо его фрагментов в любой форме, распространение, в том числе в переводе, а также их передача третьим лицам возможны только с письменного разрешения Positive Technologies.

Документ может быть изменен без предварительного уведомления.

Товарные знаки, использованные в тексте, приведены исключительно в информационных целях, исключительные права на них принадлежат соответствующим правообладателям.

Дата редакции документа: 05.08.2025

Содержание

1. Общие сведения **4**

2. Особенности и преимущества **5**

3. Доступный перечень фидов **6**

4. Перечень атрибутов объектов **9**

4.1. Итоговые вердикты по индикаторам 9

4.2. Роль сетевого индикатора в инфраструктуре злоумышленника 10

4.3. Перечень атрибутов индикаторов компрометации 10

4.3.1. File 11

4.3.2. IPaddress, Domain, URL 12

1. Общие сведения

PT Threat Intelligence Feeds (PT Feeds) позволяет командам SOC быть в курсе актуальных угроз ИБ. Продукт содержит широкий спектр индикаторов компрометации, включая:

— домены,

— IP-адреса,

— ссылки,

— хеш-суммы файлов.

Экспертизу PT Feeds формируют специалисты отдела Threat Intelligence департамента PT ESC, используя данные киберразведки, материалы расследований инцидентов, обработанную информацию из открытых источников, а также обезличенные данные телеметрии продуктов Positive Technologies.

2. Особенности и преимущества

Защита от реальных угроз

Данные из сотен источников информации об угрозах позволяет противодействовать всем современным угрозам ИБ.

Репутация и оценка потенциального ущерба

Для каждого индикатора рассчитываются показатели «Репутация» и «Потенциальный ущерб». Это помогает приоритизировать угрозы, оценить возможный ущерб от их реализации и сфокусироваться на предотвращении самых опасных из них.

Ускорение реагирования на инциденты ИБ

Наличие контекстных данных позволяет быстро и точно выстроить процесс по сдерживанию угроз ИБ.

Широкий спектр применения

Разнообразие фидов позволяет использовать их для любых целей: от защиты от актуальных угроз до применения политик безопасности в вашей организации.

Интеграция с продуктами разных вендоров

PT Feeds поддерживает разные форматы и широкий перечень средств защиты информации, который постоянно дополняется.

3. Доступный перечень фидов

В таблице ниже представлен доступный заказчикам перечень потоков данных с индикаторами. Перечень приведен для демонстрации возможных срезов данных репутационного сервиса Positive Technologies. По запросу заказчика могут быть сформированы индивидуальные потоки данных.

Таблица 1. Доступный перечень фидов

№	Наименование коллекции и состав	Описание	Назначение
Коллекции опасных индикаторов			
1	**current-act** domains, URLs, IPs, hashes	Вредоносные индикаторы, активные за последнюю неделю	1. **IDS**, **NTA**, **NGFW** — для детектирования наиболее актуальных индикаторов на периметре сетевой инфраструктуры компании. 2. **SIEM** — для приоритизации срабатываний (чем актуальнее индикатор, тем выше вероятность, что он «живой», и тем более высокий приоритет инцидента). 3. **IRP**, **SOAR** — для обогащения контекста в карточке инцидента. 4. **EDR** —для приоритетного сканирования системы и удаления вредоносных образцов
2	**recent-act** domains, URLs, IPs, hashes	Вредоносные индикаторы, активные за последний месяц	
3	**retro** domains, URLs, IPs, hashes	Вредоносные индикаторы, активные за последний год	Фид предназначен для реализации сценариев threat hunting. Фид может быть использован в различных СЗИ, а также других инфраструктурных сервисах для поиска событий с представленными в фиде индикаторами. Например, фид retrospective IPs может быть использован для поиска событий в NetFlow и журналах FW или NGFW, фид retrospective domains — в NTA и журналах DNS,

№	Наименование коллекции и состав	Описание	Назначение
			а фид retrospective hashes — для анализа почтовых вложений в SEG-решениях, а также для сканирования конечных узлов с помощью EDR
Коллекции категорирующих индикаторов			
4	**tor** IPs	IP-адреса, размеченные как TOR Node	1. **NGFW** — для применения политики безопасности на межсетевом экране, в зависимости от которой взаимодействие с определенными типами сетевых ресурсов может быть разрешено, заблокировано или обнаружено в СЗИ. 2. **IRP**, **SOAR** — для категоризации индикаторов, обнаруженных в процессе реагирования на инцидент или его расследования. Категоризация может служить как для приоритизации инцидента, так и для ускорения его обработки (не потребуется тратить время на уточнение информации об индикаторе)
5	**dyndns** domains	Домены, относящиеся к инфраструктуре DynDNS	
6	**cloud** IPs, IP ranges	IP-адреса, относящиеся к облачной инфраструктуре	
7	**vpn** IPs, IP ranges	IP-адреса, относящиеся к VPN	
8	**cdn** domains, IPs, IP ranges	Вредоносные домены и IP-адреса, относящиеся к CDN-инфраструктуре	
9	**torrent-trackers** domains, IPs, URLs	Вредоносные домены, URL и IP-адреса, относящиеся к торрент-трекерам	
10	**proxy** domains, IPs, URLs	Вредоносные домены, URL и IP-адреса, относящиеся к инфраструктуре Proxy	
11	**scanner** IPs	Перечень IP-адресов, относящихся к сервисам, которые собирают информацию об открытых сетевых ресурсах	
12	**service** domains, IPs, URLs	Домены, URL и IP-адреса, относящиеся к различным сервисам	

№	Наименование коллекции и состав	Описание	Назначение
13	**cryptomining** domains, URLs, IPs	Вредоносные сетевые индикаторы, связанные с криптомайнингом	
14	**fincert** domains, URLs, IPs, hashes	Вредоносные индикаторы, передаваемые по линии «ФинЦЕРТ»	Обнаружение угроз на базе индикаторов, поставляемых из «ФинЦЕРТ». Актуально для любых детектирующих классов СЗИ
Коллекции белых индикаторов			
15	**whitelist** domains, URLs, IPs, hashes	Белый список индикаторов	Фид предназначен для формирования белых списков индикаторов для уменьшения количества ложноположительных срабатываний. Актуально для любых детектирующих классов СЗИ. **IRP**, **SOAR** — фид может использоваться для категоризации индикаторов, обнаруженных в процессе реагирования на инцидент или его расследования. Категоризация может служить как для приоритизации инцидента, так и для ускорения его расследования (не потребуется тратить время на уточнение информации об индикаторе)

4. Перечень атрибутов объектов

Ниже представлены атрибуты объектов, которые могут быть описаны в коллекции. Список не является исчерпывающим и может корректироваться в зависимости от схемы, согласно которой формируется коллекция.

Общий список атрибутов индикаторов:

- Репутация индикатора на момент выгрузки.
- Итоговый вердикт по индикатору.
- Флаг, указывающий на связь индикатора с деятельностью APT-группировок.
- Временные метки.
- Принадлежность или связь:
  - с другими индикаторами,
  - с классом вредоносного ПО,
  - с семейством вредоносного ПО,
  - с группировками APT, киберпреступностью.
- Потенциальный ущерб — опасность угрозы, связанной с индикатором, для инфраструктуры организации.
- Роли узла в сети.

Детальные описания атрибутов каждой сущности приведены ниже.

В этом разделе

Итоговые вердикты по индикаторам (см. раздел 4.1)

Роль сетевого индикатора в инфраструктуре злоумышленника (см. раздел 4.2)

Перечень атрибутов индикаторов компрометации (см. раздел 4.3)

4.1. Итоговые вердикты по индикаторам

Класс `Verdict` — это перечисление, объекты которого принимают следующие значения:

- `Suspicious` — подозрительный индикатор, который нельзя явно отнести к `Clean` или `Malicious`;
- `Malicious` — вредоносный индикатор;
- `Whitelisted` — индикатор, признанный безопасным на основе белых списков;
- `TorrentTracker` — индикатор, связанный с инфраструктурой торрент-трекеров;
- `Scanner` — индикатор, связанный с активностью сканеров сетевых ресурсов;

- `Cloud` — индикатор, относящийся к облачной инфраструктуре крупных компаний;
- `Stun` — индикатор, относящийся к STUN-серверам;
- `TorNode` — индикатор, относящийся к узлам Tor;
- `CDN` — индикатор, относящийся к инфраструктуре CDN;
- `VPNGate` — индикатор, относящийся к инфраструктуре VPN;
- `Service` — индикатор, относящийся к различным сервисам (например, ПО для удаленного доступа);
- `Proxy` — индикатор, относящийся к прокси-инфраструктуре;
- `DynDNS` — индикатор, относящийся к DynDNS-доменам;
- `Cryptomining` — индикатор, относящийся к ресурсам, связанным с криптомайнингом.

4.2. Роль сетевого индикатора в инфраструктуре злоумышленника

Класс `Role` — это перечисление, объекты которого принимают следующие значения:

- `unknown` — роль узла не определена;
- `CnC` — управляющий сервер злоумышленников;
- `Phishing` — сетевой узел, связанный с фишингом;
- `Download` — сетевой узел, связанный с загрузкой вредоносного ПО;
- `Upload` — сетевой узел, связанный с эксфильтрацией данных;
- `Exploiter` — сетевой узел, связанный с эксплуатацией уязвимостей.

4.3. Перечень атрибутов индикаторов компрометации

Ниже представлено описание имеющихся атрибутов для различных типов индикаторов компрометации.

В этом разделе

File (см. раздел 4.3.1)

IPaddress, Domain, URL (см. раздел 4.3.2)

4.3.1. File

Таблица 2. File

Атрибут	Тип (формат)	Описание
`normalized_score`	Integer	Репутация объекта на момент выгрузки. От 0 до 100, где 100 — вредоносный, 0 — безопасный
`verdict`	String	Результат проверки. Возможные значения: `Suspicious`, `Clean`, `Malicious`, `Whitelisted`, `TorrentTracker`, `DynDNS`, `Cloud`, `TorNode`, `CDN`, `VPNGate`, `proxy`, `Crytomining`, `Service`
`timestamps`	Object	Временные метки
`timestamps → first_seen`	String (date-time)	Дата и время первого наблюдения объекта
`timestamps → last_seen`	String (date-time)	Дата и время последнего наблюдения объекта
`malware_class`	Array of strings	Классы вредоносного ПО, с которым связан объект
`malware_family`	Array of strings	Семейства вредоносного ПО, с которым связан объект
`malware_group`	Array of strings	Объект используется злоумышленниками
`severity`	String	Потенциальный ущерб — возможное негативное влияние объекта на инфраструктуру организации. Возможные значения: — High — большой; — Medium — средний; — Low — малый; — None — неизвестен
`is_apt`	Boolean	Объект связан с активностью APT-группировок

Атрибут	Тип (формат)	Описание
relations	Array of objects	Информация о связях объекта с другими объектами
relations → target_type	String	Объект — цель связи. Возможные значения: IP, DOMAIN, FILE, URL, IP_RANGE
relations → type	String	Тип связи. Возможные значения: none, DroppedFile, IPResolved, CalledIP, CalledDomain, CalledURL, DownloadedFile, Subdomain, IPRange, URLParentDomain, URLParentIP, URLResolved, PTRResolve, SPFDomain
relations → key	String	Ключевой атрибут объекта — цели связи
relations → direction	String	Направление связи. Возможные значения: NONE, SOURCE, RECEIVER
tags	Array of strings	Метки

4.3.2. IPaddress, Domain, URL

Таблица 3. IPaddress, Domain, URL

Атрибут	Тип (формат)	Описание
normalized_score	Integer	Репутация объекта на момент выгрузки. От 0 до 100, где 100 — вредоносный, 0 — безопасный
verdict	String	Результат проверки. Возможные значения: Suspicious, Clean, Malicious, Whitelisted, TorrentTracker, DynDNS, Cloud, TorNode, CDN, VPNGate, proxy, Crytomining, Service
timestamps	Object	Временные метки

Атрибут	Тип (формат)	Описание
`timestamps → first_seen`	String (date-time)	Дата и время первого наблюдения объекта
`timestamps → last_seen`	String (date-time)	Дата и время последнего наблюдения объекта
`malware_class`	Array of strings	Классы вредоносного ПО, с которыми связан объект
`malware_family`	Array of strings	Семейства вредоносного ПО, с которыми связан объект
`malware_group`	Array of strings	Файл используется злоумышленниками
`severity`	String	Потенциальный ущерб — возможное негативное влияние объекта на инфраструктуру организации. Возможные значения: — High — большой; — Medium — средний; — Low — малый; — None — неизвестен
`role`	Array of strings	Вредоносные роли узла в сети. Возможные значения атрибута: `Unknown, CnC, Phishing, Download, Upload, Ex-ploiter`
`is_apt`	Boolean	Объект связан с активностью APT-группировок
`relations`	Array of objects	Информация о связях объекта с другими объектами
`relations → target_type`	String	Объект — цель связи. Возможные значения: `IP, DOMAIN, FILE, URL, IP_RANGE`
`relations → type`	String	Результат проверки. Возможные значения: `Suspicious, Clean, Malicious, Whitelisted, TorrentTracker, DynDNS,`

Атрибут	Тип (формат)	Описание
		`Cloud, TorNode, CDN, VPNGate, proxy, Crytomining, Service`
`relations → key`	String	Ключевой атрибут объекта — цели связи
`relations → direction`	String	Направление связи. Возможные значения: `NONE, SOURCE, RECEIVER`
`av_verdicts`	Array of strings	Результат проверки файла средствами антивирусной защиты
`tags`	Array of strings	Метки

positive technologies

Positive Technologies — один из лидеров в области результативной кибербезопасности. Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI). Количество акционеров превышает 220 тысяч.