Threat Intelligence Feeds

Datasheet

Last edited: 8/12/2025

Contents

1. Overview

PT Threat Intelligence Feeds (PT Feeds) keeps SOC teams up to date on current cybersecurity threats. The product contains a wide range of indicators of compromise (IoCs) that include the following:

- Domains
- IP addresses
- Links
- File hashes

Expertise for PT Feeds comes from the Threat Intelligence team at the PT ESC department, who draw on cyberintelligence, incident investigations, data from public sources, and anonymized telemetry data from Positive Technologies products.

2. Features and benefits

Protection against real threats

Hundreds of sources with threat information help counteract all modern cybersecurity threats.

Reputation and potential damage assessment

For each indicator of compromise, reputation and potential damage are estimated. This helps prioritize threats, estimate possible damage from attacks, and focus on preventing the most dangerous ones.

Accelerated response to security incidents

Contextual data helps quickly and accurately build a cyberthreat prevention process.

Wide range of application

Feeds of various kinds can be used for any purpose, ranging from protection against current threats to security policy enforcement in organizations.

Integration with products by a variety of vendors

PT Feeds supports various formats and a wide range of cybersecurity products that keeps expanding.

3. List of available feeds

The table below presents a list of IoC data feeds available to customers. The purpose of the list is to demonstrate possible data dimensions provided by the Positive Technologies reputation service. Custom data feeds are available on request.

Table 1. List of available feeds

No.	Collection name and included indicators	Description	Purpose
Collections of malicious indicators			
1	**current-act** domains, URLs, IPs, hashes	Malicious indicators active in the last week	1. **IDS**, **NTA**, **NGFW**: detection of the most relevant indicators on a company's network perimeter. 2. **SIEM**: prioritization of threats (the more relevant an indicator, the higher the probability that it is active and the higher the priority of the incident). 3. **IRP**, **SOAR**: enrichment of context for the incident card. 4. **EDR**: priority scanning of the system and deletion of malicious samples
2	**recent-act** domains, URLs, IPs, hashes	Malicious indicators active in the last month	
3	**retro** domains, URLs, IPs, hashes	Malicious indicators active in the last year	The feed is designed to implement threat hunting scenarios. The feed can be used by various information security tools and other infrastructure services to search for events with the indicators specified in the feed. For example, the retrospective IPs feed can be used to search for events in NetFlow and FW or NGFW logs, retrospective domains can be used to search for events in NTA and DNS logs, and retrospective hashes can be used to analyze email attachments in SEG solutions and scan endpoints using EDR

No.	Collection name and included indicators	Description	Purpose
Collections of categorizing indicators			
4	**tor** IPs	IP addresses labeled as TOR Node	1. **NGFW**: configuring a security policy on the firewall that allows information security tools to enable, block, or detect interactions with certain network resources. 2. **IRP**, **SOAR**: categorization of indicators detected during response to or investigation of incidents. Categorization can help both prioritize incidents and accelerate processing, because it saves time that would otherwise be spent on clarification of indicator details
5	**dyndns** domains	Domains that belong to Dyn-DNS infrastructure	
6	**cloud** IPs, IP ranges	IP addresses that belong to cloud infrastructure	
7	**vpn** IPs, IP ranges	IP addresses that belong to VPNs	
8	**cdn** domains, IPs, IP ranges	Malicious domains and IP addresses that belong to CDN infrastructure	
9	**torrent-trackers** domains, IPs, URLs	Malicious domains, URLs, and IP addresses that belong to torrent trackers	
10	**proxy** domains, IPs, URLs	Malicious domains, URLs, and IP addresses that belong to proxy infrastructure	
11	**scanner** IPs	A list of IP addresses that belong to services that collect information about public network resources	
12	**service** domains, IPs, URLs	Domains, URLs, and IP addresses that belong to various services	
13	**cryptomining** domains, URLs, IPs	Malicious network indicators associated with cryptomining	
14	**fincert**	Malicious indicators received from FinCERT	Detection of threats based on indicators provided by FinCERT.

No.	Collection name and included indicators	Description	Purpose
	domains, URLs, IPs, hashes		Relevant for any information security tools that perform detection
Collections of whitelist indicators			
15	**whitelist** domains, URLs, IPs, hashes	Indicator whitelist	The feed is designed to generate whitelists of indicators to help reduce the number of false positives. It is relevant for any information security tools that perform detection. **IRP**, **SOAR**: the feed can be used to categorize indicators detected during response or investigation of incidents. Categorization can help both prioritize incidents and accelerate investigation, because it saves time that would otherwise be spent on clarification of indicator details

4. List of object attributes

The list below presents the attributes of objects that can be described as part of a collection. This is not an exhaustive list, and it may be adjusted according to the pattern used to build the collection.

General list of IoC attributes:

- Indicator reputation at extraction time
- Final verdicts on the IoC
- Flag that associates the indicator with APT groups
- Timestamps
- Attribution to or relationship with:
  - Other IoCs
  - Malware category
  - Malware family
  - APT group/cybercrime
- Potential damage: severity of the threat associated with the indicator in terms of impact on corporate infrastructure
- Node roles in the network

The detailed descriptions of each entity's attributes are given below.

In this section

4.1. Final verdicts on IoCs

The `Verdict` attribute can take the following values:

- `Suspicious`: suspicious indicator that cannot be unequivocally categorized as `Clean` or `Malicious`
- `Malicious`: malicious indicator
- `Whitelisted`: indicator declared safe according to whitelists
- `TorrentTracker`: indicator associated with a torrent tracker network
- `Scanner`: indicator associated with network scanner activity
- `Cloud`: indicator that belongs to enterprise clouds

- `Stun`: indicator that belongs to STUN servers
- `TorNode`: indicator that belongs to Tor nodes
- `CDN`: indicator that belongs to CDN infrastructure
- `VPNGate`: indicator that belongs to VPN infrastructure
- `Service`: indicator that belongs to various services (for example, of remote access tools)
- `Proxy`: indicator that belongs to proxy server infrastructure
- `DynDNS`: indicator that belongs to DynDNS domains
- `Cryptomining`: indicator that belongs to resources associates with cryptomining

4.2. Network indicator role in a malicious actor's infrastructure

The `Role` attribute can take the following values:

- `unknown`: node role undefined
- `CnC`: command-and-control server
- `Phishing`: network node associated with phishing
- `Download`: network node associated with malware downloads
- `Upload`: network node associated with data exfiltration
- `Exploiter`: network node associated with vulnerability exploitation

4.3. List of IoC attributes

A description of available attributes for various IoCs is given below.

In this section

4.3.1. File

Table 2. File

Attribute	Type (format)	Description
`normalized_score`	Integer	Object reputation at extraction time. 0 to 100, where 100 stands for malicious and 0 stands for safe
`verdict`	String	Check results. Possible values: `Suspicious`, `Clean`, `Malicious`, `Whitelisted`, `TorrentTracker`, `DynDNS`, `Cloud`, `TorNode`, `CDN`, `VPNGate`, `proxy`, `Cryptomining`, `Service`
`timestamps`	Object	Timestamps
`timestamps → first_seen`	String (date-time)	Date and time when the object was first detected
`timestamps → last_seen`	String (date-time)	Date and time when the object was last detected
`malware_class`	Array of strings	Malware categories related to the object
`malware_family`	Array of strings	Malware families related to the object
`malware_group`	Array of strings	Malicious actors using the object
`severity`	String	Potential damage: possible adverse impact on the corporate infrastructure. Possible values: • High • Medium • Low • None: unknown
`is_apt`	Boolean	Object is associated with APT group activity
`relations`	Array of objects	Information about relationships with other objects

Attribute	Type (format)	Description
relations → target_type	String	Related object. Possible values: IP, DOMAIN, FILE, URL, IP_RANGE
relations → type	String	Relationship type. Possible values: none, DroppedFile, IPResolved, CalledIP, CalledDomain, CalledURL, DownloadedFile, Subdomain, IPRange, URL-ParentDomain, URL-ParentIP, URLResolved, PTRResolve, SPFDomain
relations → key	String	Key attribute of the related object
relations → direction	String	Relationship direction. Possible values: NONE, SOURCE, RECEIVER
tags	Array of strings	Labels

4.3.2. IPaddress, Domain, URL

Table 3. IPaddress, Domain, URL

Attribute	Type (format)	Description
normalized_score	Integer	Object reputation at extraction time. 0 to 100, where 100 stands for malicious and 0 stands for safe
verdict	String	Check results. Possible values: Suspicious, Clean, Malicious, Whitelisted, TorrentTracker, DynDNS, Cloud, TorNode, CDN, VPNGate, proxy, Cryptomining, Service
timestamps	Object	Timestamps
timestamps → first_seen	String (date-time)	Date and time when the object was first detected
timestamps → last_seen	String (date-time)	Date and time when the object was last detected

Attribute	Type (format)	Description
malware_class	Array of strings	Malware categories related to the object
malware_family	Array of strings	Malware families related to the object
malware_group	Array of strings	Malicious actors using the file
severity	String	Potential damage: possible adverse impact on the corporate infrastructure. Possible values: • High • Medium • Low • None: unknown
role	Array of strings	Malicious roles of the network node Possible attribute values: Unknown, CnC, Phishing, Download, Upload, Exploiter
is_apt	Boolean	Object is associated with APT group activity
relations	Array of objects	Information about relationships with other objects
relations → target_type	String	Related object. Possible values: IP, DOMAIN, FILE, URL, IP_RANGE
relations → type	String	Check results. Possible values: Suspicious, Clean, Malicious, Whitelisted, TorrentTracker, DynDNS, Cloud, TorNode, CDN, VPNGate, proxy, Cryptomining, Service
relations → key	String	Key attribute of the related object
relations → direction	String	Relationship direction. Possible values: NONE, SOURCE, RECEIVER

Attribute	Type (format)	Description
av_verdicts	Array of strings	Object scan result provided by an antivirus
tags	Array of strings	Labels

positive technologies

Positive Technologies is an industry leader in result-driven cybersecurity and a major global provider of information security solutions. Our mission is to safeguard businesses and entire industries against cyberattacks and non-tolerable damage. Positive Technologies is the first and only cybersecurity company in Russia on the Moscow Exchange (MOEX: POSI), with 220,000 shareholders and counting.