Securaa TIP Administration Guide

Contact Information
support@securaa.io

668/A,9th Cross, 1st Stage Vijay Eswari, Vijaya Nagar, Mysore KA 570017 IN

Last Revised: 25 January 2025

Table Of Contents

Securaa TIP Platform Overview

Securaa TIP provides in-depth security analysis at the fingertips of your users. It offers a completely automated cyber threat intelligence service that includes data collecting, processing, threat analysis, and enrichment, as well as threat information dissemination and mitigation actions. It delivers identified threats to stakeholders in an easy-to-triage format, employing a visual network graph view that anybody can use to categorize threats by risk factor and activate actions to minimize risks.

The main features of Securaa TIP are

- 130+ open-source feeds.
- Deduplication.
- Normalization and Geolocation enrichment for addresses.
- Confidence at the source level.
- Set Interval for data retrieval from open-source feeds.
- Set Indicator Expiry by source.
- Option to add Investigation links for Indicator type.
- Export and Import of Indicators.
- Association of Indicators with Malware - Auto and Manual.
- Set Indicator Tags, TLP, Comments, MITRE Tactics, and Techniques, etc.
- Stix Visualization of Indicator.

Installation Process

Prerequisites for Deployment

Securaa TIP needs the following for a successful deployment

- Connectivity to Securaa Servers to download the latest software versions and docker images and connectivity to open-source feed URLs to get the latest feeds (URLs mentioned in network requirements).
- Port 7000 should be open in the TIP machine to establish connectivity with SOAR.
- Administrative privileges on the operations system platform.
- SSH Connectivity tools like Putty to connect with Securaa TIP machine.
- Browser software like Chrome to access the Securaa web interface.

Operating system requirements

Securaa TIP can be deployed on the following operating systems and must meet the minimum hardware requirements.

Operating System	**Supported Version**
RHEL	9.x, 8.x
Rocky Linux	8.x
Alma Linux	8.x
Centos	9.x

Hardware Requirements

MSSP POC (Proof of concept)

COMPONENT	**Specification**
CPU	4 CPU
Memory	16 GB RAM

Storage	300 GB SSD [~ 20 Million Records]

MSSP (PRODUCTION)

COMPONENT	**Specification**
CPU	8 CPU
Memory	32 GB RAM
Storage	500 GB SSD [~ 30 Million Records]

Note : More storage needs to be added if records exceed 30 million.

Network Connectivity Requirements

The following URLs need to be whitelisted before installation. Securaa downloads the latest software version, docker images, and other dependencies from these URLs:

- https://s3.us-east-2.amazonaws.com/
- https://665853670667.dkr.ecr.us-east-2.amazonaws.com/
- https://release.securaa.io:9002
- https://repo.securaa.io/

Open-source feed URLs to be whitelisted in the firewall:

- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/7777%20Botnet%20IPs.txt
- https://raw.githubusercontent.com/halilozturkci/APT10-Threat-Analysis-Report-from-ADEO/refs/heads/master/Indicators%20of%20Compromise-FileNames.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Ares%20RAT%20C2%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/AsyncRAT%20IPs.txt
- https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/Sample%20Data/Feeds/Log4j_IOC_List.csv
- https://faf.bambenekconsulting.com/feeds/dga-feed-high.gz

- https://faf.bambenekconsulting.com/feeds/maldomainml/malware-master.txt
- https://faf.bambenekconsulting.com/feeds/maldomainml/phishing-master.txt
- https://www.binarydefense.com/banlist.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/BitRAT%20IPs.txt
- https://www.blocklist.de/downloads/export-ips_ssh.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Browser%20Exploitation%20Framework%20(BeEF)%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Brute%20Ratel%20C4%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/BurpSuite%20IPs.txt
- https://raw.githubusercontent.com/halilozturkci/APT10-Threat-Analysis-Report-from-ADEO/refs/heads/master/Indicators%20of%20Compromise-C2Address.txt
- https://hole.cert.pl/domains/domains.txt
- https://cinsscore.com/list/ci-badguys.txt
- https://www.cisa.gov/sites/default/files/publications/AA19-024A_IOCs.csv
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Caldera%20C2%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Cobalt%20Strike%20C2%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Collector%20Stealer%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Covenant%20C2%20IPs.txt
- https://raw.githubusercontent.com/mitchellkrogza/Phishing.Database/refs/heads/master/phishing-domains-ACTIVE.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/DarkComet%20Trojan%20IPs.txt
- https://dataplane.org/proto41.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/DcRAT%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Deimos%20C2%20IPs.txt
- https://www.dshield.org/ipsascii.html
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Patriot%20Stealer%20IPs.txt

- https://cdn.ellio.tech/community-feed
- https://raw.githubusercontent.com/austinheap/sophos-xg-block-lists/refs/heads/master/dan-pollock-someonewhocares-org.txt
- https://raw.githubusercontent.com/ktsaou/blocklist-ipsets/master/firehol_level1.netset
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Gh0st%20RAT%20Trojan%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/GoPhish%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Gozi%20Trojan%20IPs.txt
- https://content.govdelivery.com/attachments/USDHSCIKR/2020/03/23/file_attachments/1408126/ACSC%20Advisory%20-%202020-005%20-%20Indicators%20of%20Compromise%20-%20COVID-19%20malicious%20activity.csv
- https://blocklist.greensnow.co/greensnow.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Hachcat%20IPs.txt
- https://raw.githubusercontent.com/mitchellkrogza/The-Big-List-of-Hacked-Malware-Web-Sites/refs/heads/master/.dev-tools/_strip_domains/domains.tmp
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Hak5%20Cloud%20C2%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Havoc%20C2%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Hookbot%20IPs.txt
- https://raw.githubusercontent.com/stamparm/ipsum/master/levels/1.txt
- https://raw.githubusercontent.com/stamparm/ipsum/master/levels/2.txt
- https://raw.githubusercontent.com/stamparm/ipsum/master/levels/3.txt
- https://raw.githubusercontent.com/stamparm/ipsum/master/levels/4.txt
- https://raw.githubusercontent.com/stamparm/ipsum/master/levels/5.txt
- https://raw.githubusercontent.com/stamparm/ipsum/master/levels/6.txt
- https://raw.githubusercontent.com/stamparm/ipsum/master/levels/7.txt
- https://raw.githubusercontent.com/stamparm/ipsum/master/levels/8.txt
- https://raw.githubusercontent.com/ktsaou/blocklist-ipsets/master/firehol_level1.netset
- https://lolbas-project.github.io/api/lolbas.csv
- https://raw.githubusercontent.com/halilozturkci/APT10-Threat-Analysis-Report-f

rom-ADEO/refs/heads/master/Indicators%20of%20Compromise-MD5Hashes.txt
- https://malsilo.gitlab.io/feeds/dumps/url_list.txt
- https://malshare.com/daily/malshare.current.all.txt
- https://bazaar.abuse.ch/export/txt/md5/recent/
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Metasploit%20Framework%20C2%20IPs.txt
- https://mirai.security.gives/data/ip_list.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/MobSF%20IPs.txt
- http://multiproxy.org/txt_anon/proxy.txt
- https://myip.ms/files/blacklist/general/latest_blacklist.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Mythic%20C2%20IPs.txt
- https://www.ncsc.gov.uk/static-assets/documents/malware-analysis-reports/cold-steel/NCSC-MAR-Cold-Steel-indicators.csv
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/NanoCore%20RAT%20Trojan%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/NetBus%20Trojan%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/NimPlant%20C2%20IPs.txt
- https://gitlab.com/quidsup/notrack-blocklists/-/raw/master/notrack-malware.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Orcus%20RAT%20Trojan%20IPs.txt
- https://raw.githubusercontent.com/romainmarcoux/malicious-ip/refs/heads/main/sources/projecthoneypot.org-aa.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Oyster%20C2%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/PANDA%20C2%20IPs.txt
- https://raw.githubusercontent.com/pan-unit42/iocs/master/diamondfox/diamondfox_panels.txt
- https://raw.githubusercontent.com/austinheap/sophos-xg-block-lists/refs/heads/master/adaway.txt
- https://raw.githubusercontent.com/ph00lt0/blocklist/refs/heads/master/domains.txt
- https://raw.githubusercontent.com/austinheap/sophos-xg-block-lists/refs/heads

/master/kadhosts.txt

- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Poseidon%20C2%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Posh%20C2%20IPs.txt
- https://raw.githubusercontent.com/stamparm/ipsum/master/ipsum.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Pupy%20RAT%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Quasar%20RAT%20IPs.txt
- https://api.recordedfuture.com/v2/ip/risklist?format=csv%2Fsplunk
- https://api.recordedfuture.com/v2/domain/risklist?format=csv%2Fsplunk
- https://api.recordedfuture.com/v2/hash/risklist?format=csv%2Fsplunk
- https://api.recordedfuture.com/v2/url/risklist?format=csv%2Fsplunk
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/RedGuard%20C2%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Remcos%20Pro%20RAT%20Trojan%20IPs.txt
- https://rules.emergingthreats.net/fwrules/emerging-Block-IPs.txt
- https://isc.sans.edu/api/threatlist
- https://raw.githubusercontent.com/halilozturkci/APT10-Threat-Analysis-Report-from-ADEO/refs/heads/master/Indicators%20of%20Compromise-SHA1Hashes.txt
- https://socprime.com/wp-content/uploads/WannaCry_IOCs_public-sources-and-VT.csv
- https://raw.githubusercontent.com/austinheap/sophos-xg-block-lists/refs/heads/master/easyprivacy.txt
- https://raw.githubusercontent.com/austinheap/sophos-xg-block-lists/refs/heads/master/nocoin.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/ShadowPad%20IPs.txt
- https://raw.githubusercontent.com/brakmic/Sinkholes/master/Sinkholes_List.csv
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Sliver%20C2%20IPs.txt
- https://www.spamhaus.org/drop/drop.txt
- https://www.spamhaus.org/drop/edrop.txt
- https://www.spamhaus.org/drop/dropv6.txt

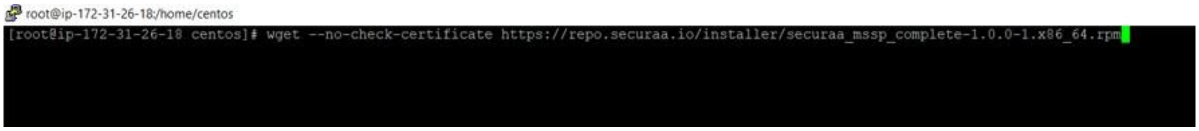
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/SpiceRAT%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/SpyAgent%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Supershell%20C2%20IPs.txt
- https://www.blocklist.de/downloads/export-ips_all.txt
- https://raw.githubusercontent.com/botherder/targetedthreats/master/targetedthreats.csv
- https://threatview.io/Downloads/IP-High-Confidence-Feed.txt
- https://www.dan.me.uk/torlist/
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/UnamWebPanel%20IPs.txt
- https://urlabuse.com/public/data/malware_url.txt
- https://urlabuse.com/public/data/phishing_url.txt
- https://dataplane.org/vncrfb.txt
- http://vxvault.net/URL_List.php
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/VenomRAT%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Villain%20C2%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Viper%20C2%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/Vshell%20C2%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/XMRig%20Monero%20Cryptominer%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/XtremeRAT%20Trojan%20IPs.txt
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/ZeroAccess%20Trojan%20IPs.txt
- https://zerodot1.deteque.com/main/ipfeeds/mining/ZeroDot1sMinerIPsLATESTv6.txt
- https://feodotracker.abuse.ch/downloads/ipblocklist_recommended.json
- https://sslbl.abuse.ch/blacklist/sslipblacklist.csv
- https://urlhaus.abuse.ch/downloads/csv_online/
- https://otx.alienvault.com/api/v1/pulses/subscribed?limit=50

- https://lists.blocklist.de/lists/apache.txt
- https://lists.blocklist.de/lists/bots.txt
- https://lists.blocklist.de/lists/bruteforcelogin.txt
- https://lists.blocklist.de/lists/ftp.txt
- https://lists.blocklist.de/lists/imap.txt
- https://lists.blocklist.de/lists/mail.txt
- https://lists.blocklist.de/lists/sip.txt
- https://lists.blocklist.de/lists/ssh.txt
- https://lists.blocklist.de/lists/strongips.txt
- https://www.team-cymru.org/Services/Bogons/fullbogons-ipv4.txt
- https://www.team-cymru.org/Services/Bogons/fullbogons-ipv6.txt
- http://danger.rulez.sk/projects/bruteforceblocker/blist.php
- http://rules.emergingthreats.net/blockrules/compromised-ips.txt
- https://v.firebog.net/hosts/Prigent-Malware.txt
- https://3.12.164.173/events/restSearch
- https://raw.githubusercontent.com/montysecurity/C2-Tracker/refs/heads/main/data/njRAT%20Trojan%20IPs.txt
- https://openphish.com/feed.txt
- https://osint.digitalside.it/Threat-Intel/lists/latesturls.txt
- https://osint.digitalside.it/Threat-Intel/lists/latestips.txt
- https://osint.digitalside.it/Threat-Intel/lists/latestdomains.txt
- https://phishing.army/download/phishing_army_blocklist_extended.txt
- https://home.nuug.no/~peter/pop3gropers.txt
- https://sblam.com/blacklist.txt
- https://secneurx.app/API/v1/getfeeds
- http://tracker.viriback.com/dump.php
- https://raw.githubusercontent.com/romainmarcoux/malicious-ip/refs/heads/main/sources/akamai.com-aa.txt
- https://raw.githubusercontent.com/romainmarcoux/malicious-ip/refs/heads/main/sources/sekio-aa.txt
- https://raw.githubusercontent.com/romainmarcoux/malicious-ip/refs/heads/main/sources/sekio-aa.txt
- https://raw.githubusercontent.com/mitchellkrogza/phishing/refs/heads/main/IP-addr.in-addr.arpa
- https://raw.githubusercontent.com/tsirolnik/spam-domains-list/master/spamdomains.txt

Securaa TIP Installation

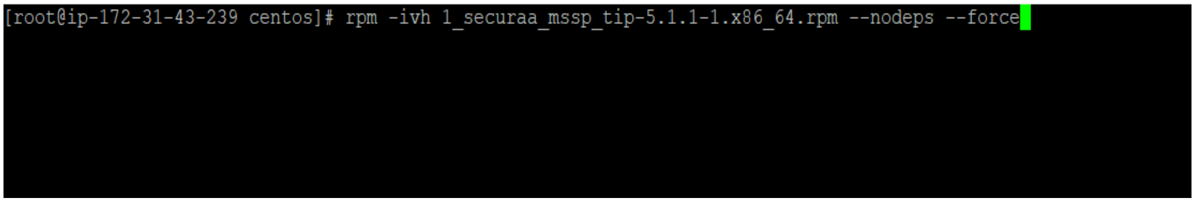
Below steps can be used to set up Securaa TIP on a single virtual machine:

1. Take server SSH access and download the installer with the help of a URL shared by the securaa team.



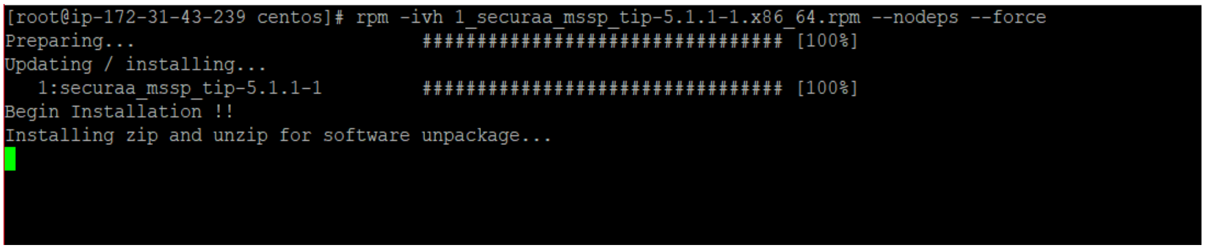
```
[root@ip-172-31-26-18 centos]# wget --no-check-certificate https://repo.securaa.io/installer/securaa_mssp_complete-1.0.0-1.x86_64.rpm
```

2. Below mentioned command can be used to run the RPM for the TIP installation. Refer snap for more details.
   COMMAND : rpm –ivh RPM_NAME –nodeps –force



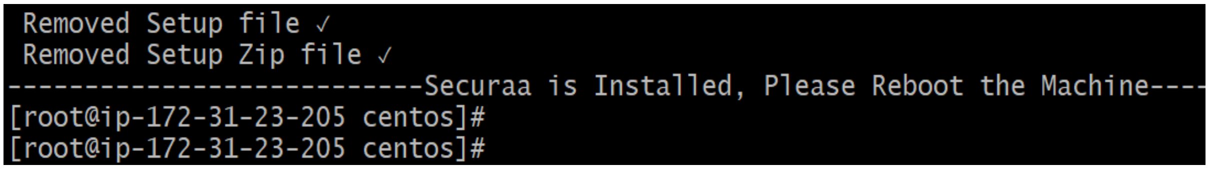
```
[root@ip-172-31-43-239 centos]# rpm -ivh 1_securaa_mssp_tip-5.1.1-1.x86_64.rpm --nodeps --force
```

3. The installation will start.



```
[root@ip-172-31-43-239 centos]# rpm -ivh 1_securaa_mssp_tip-5.1.1-1.x86_64.rpm --nodeps --force
Preparing...                          ################################# [100%]
Updating / installing...
   1:securaa_mssp_tip-5.1.1-1         ################################# [100%]
Begin Installation !!
Installing zip and unzip for software unpackage...
```

4. After installation, Reboot the server.

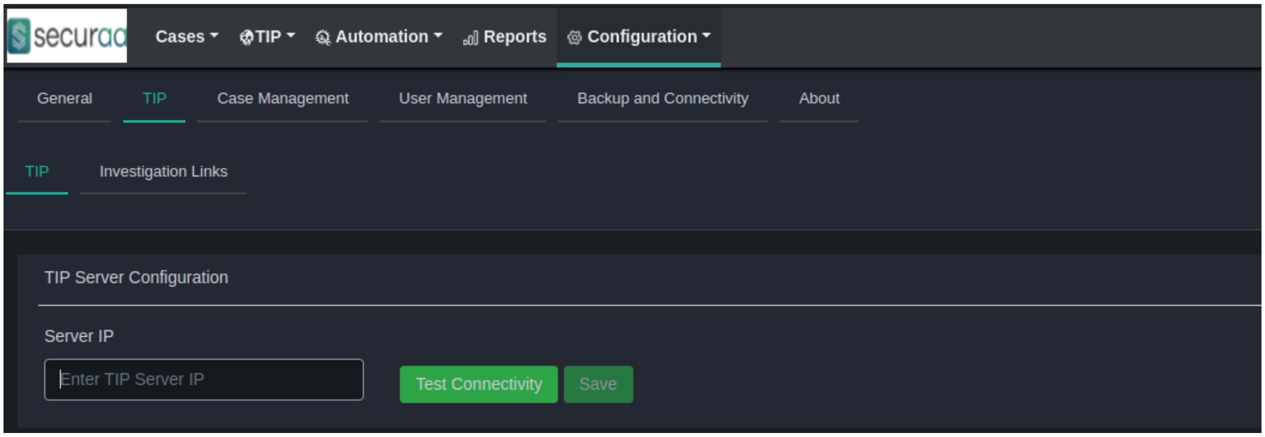


```
 Removed Setup file ✓
 Removed Setup Zip file ✓
---------------------------Securaa is Installed, Please Reboot the Machine----
[root@ip-172-31-23-205 centos]#
[root@ip-172-31-23-205 centos]#
```

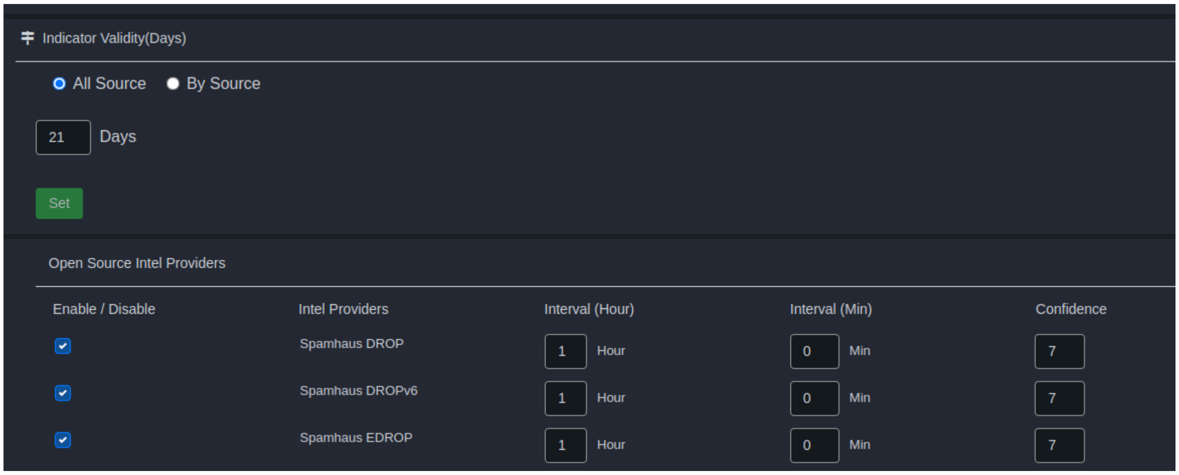
Post Installation Configuration

NOTE: Please configure the following settings before you start using TIP from securaa soar portal.

1. Login to Securaa Portal.
2. Connect Securaa SOAR platform to TIP machine by providing TIP server private IP address in Configuration → Platform → TIP → TIP → TIP Server Configuration.



3. Do a Test connectivity after entering the IP address and click on save once connectivity is successful.
4. On successful connectivity, the User will be able to configure the following:-
   - Enable or DIsable an open-source feed.
   - Interval to fetch the feeds from different sources.
   - Alter confidence for each source.
   - Set Indicator validity for each source.



Indicator Validity(Days)

● All Source ○ By Source

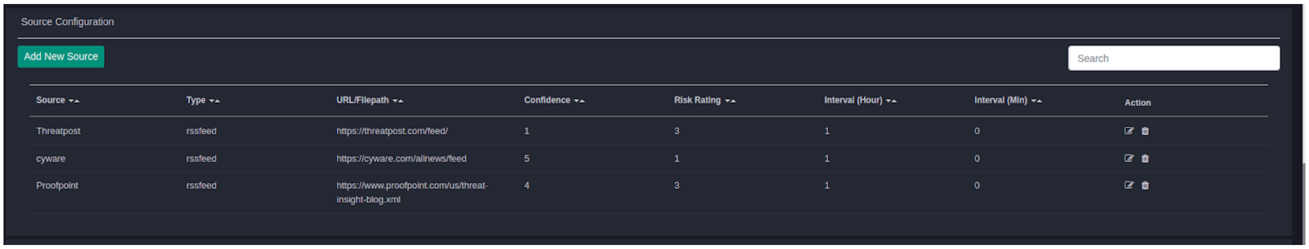
21 Days

Set

Open Source Intel Providers

Enable / Disable	Intel Providers	Interval (Hour)	Interval (Min)	Confidence
☑	Spamhaus DROP	1 Hour	0 Min	7
☑	Spamhaus DROPv6	1 Hour	0 Min	7
☑	Spamhaus EDROP	1 Hour	0 Min	7

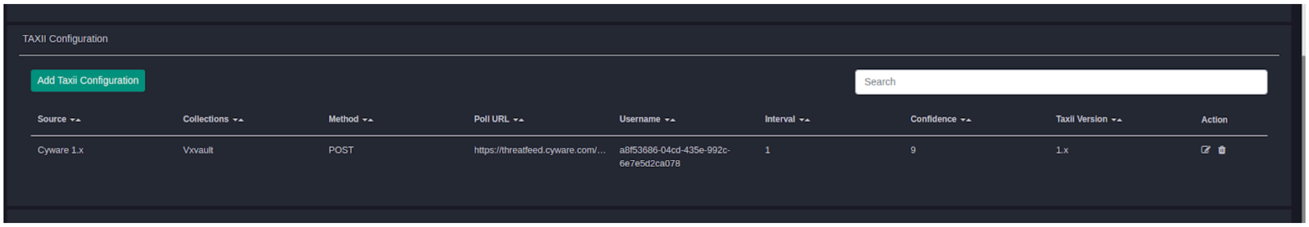
- Users can also configure a data source by specifying the file path, URL, or RSS feed. This configuration allows the system to fetch data from the selected sources accordingly.



Source Configuration

Source	Type	URL/Filepath	Confidence	Risk Rating	Interval (Hour)	Interval (Min)	Action
Threatpost	rssfeed	https://threatpost.com/feed/	1	3	1	0	
cyware	rssfeed	https://cyware.com/allnews/feed	5	1	1	0	
Proofpoint	rssfeed	https://www.proofpoint.com/us/threat-insight-blog.xml	4	3	1	0	

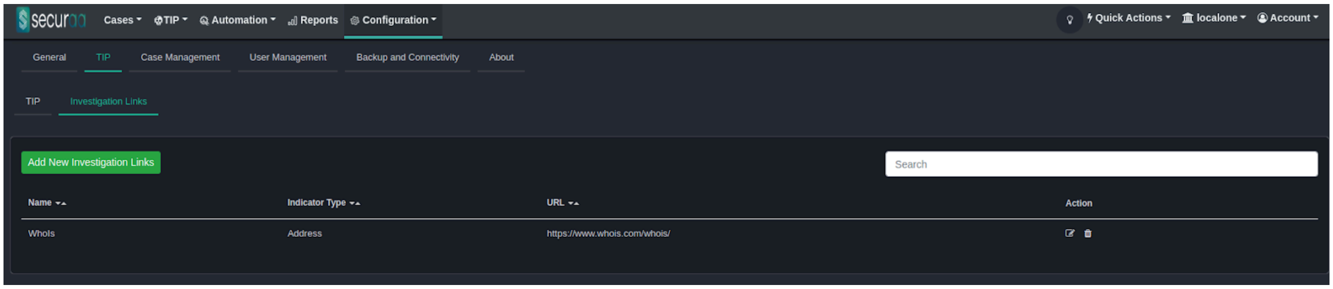
- Analysts can add a TAXII configuration to fetch indicators based on various parameters such as Source, Collections, User Name, Password, Poll URL, and TAXII Version, etc.



TAXII Configuration

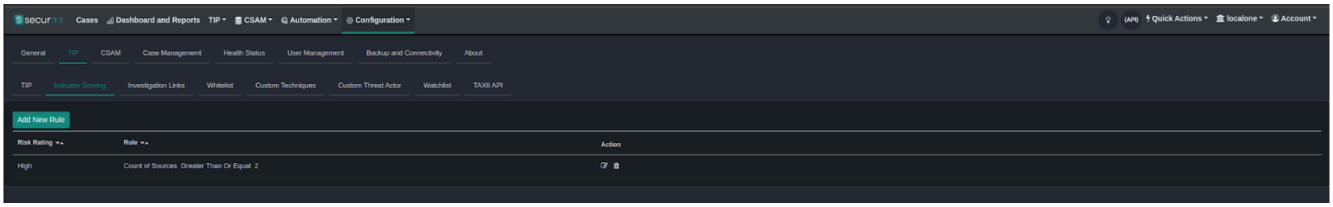
Source	Collections	Method	Poll URL	Username	Interval	Confidence	Taxii Version	Action
Cyware 1.x	Vxvault	POST	https://threatfeed.cyware.com/…	a8f53686-04cd-435e-992c-6e7e5d2ca078	1	9	1.x	

5. Analysts can also add Investigation links for each indicator type which helps them analyze specific indicators.



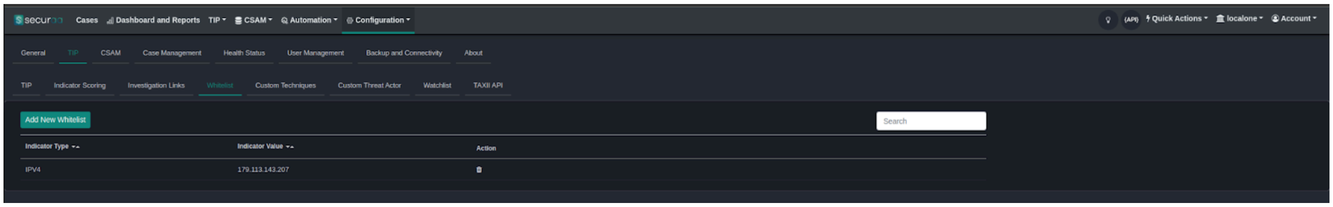
Name	Indicator Type	URL	Action
WhoIs	Address	https://www.whois.com/whois/	

6. Most open-source providers do not offer ratings for indicators. Therefore, analysts can create scoring rules for indicators based on predefined parameters. These ratings are specific to each tenant.



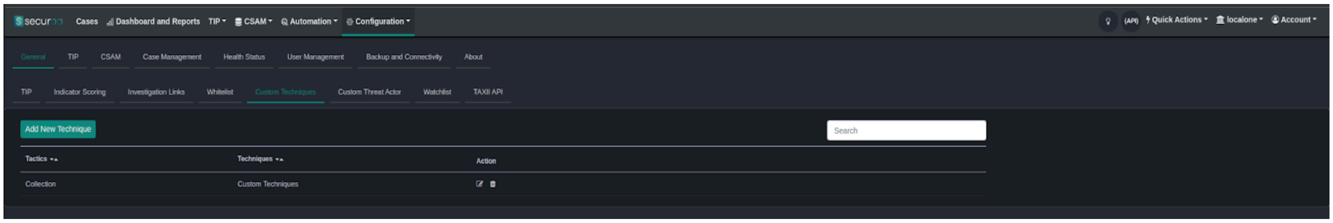
Risk Rating	Rule	Action
High	Count of Sources Greater Than Or Equal 2	

7. When an analyst adds an indicator to the whitelist, the indicator's risk rating should be displayed as "whitelisted." This status should be monitored to ensure it remains secure and does not pose any risk.



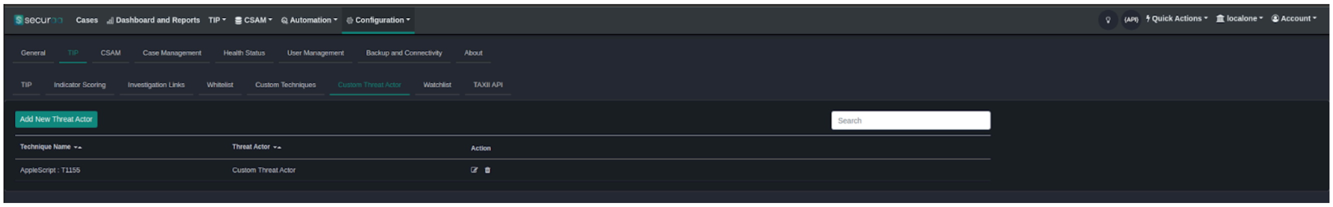
Indicator Type	Indicator Value	Action
IPV4	179.113.143.207	

8. Analysts can also add custom techniques to the MITRE ATT&CK framework to address specific threats or attack methods unique to their environment. These custom techniques allow organizations to tailor the framework to their specific needs, enhancing their ability to detect, respond to, and mitigate threats that may not be covered by standard techniques.



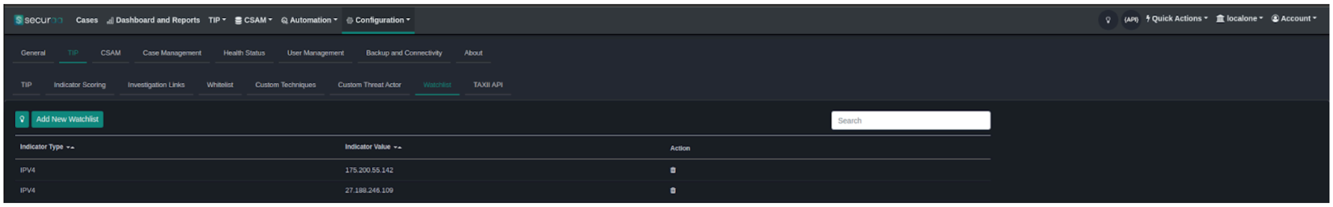
Tactics	Techniques	Action
Collection	Custom Techniques	

9. Analysts can also add custom Threat actors, which encompass individuals, groups, or organizations engaged in malicious activities aimed at compromising or harming a target.



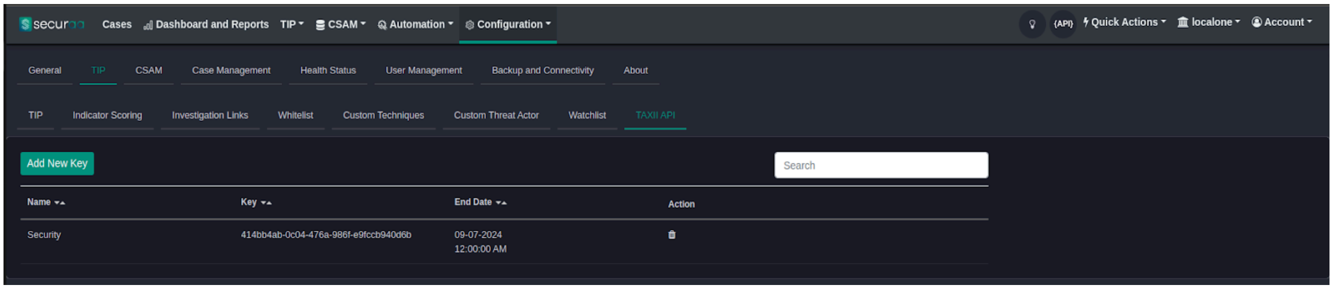
Technique Name	Threat Actor	Action
AppleScript : T1155	Custom Threat Actor	

10. Analysts can add a watchlist indicator to monitor if the same indicator appears in an alert or case. When detected, an email can be sent to the configured email ID with the specified subject.



Indicator Type	Indicator Value	Action
IPV4	175.200.55.142	🗑
IPV4	27.188.246.109	🗑

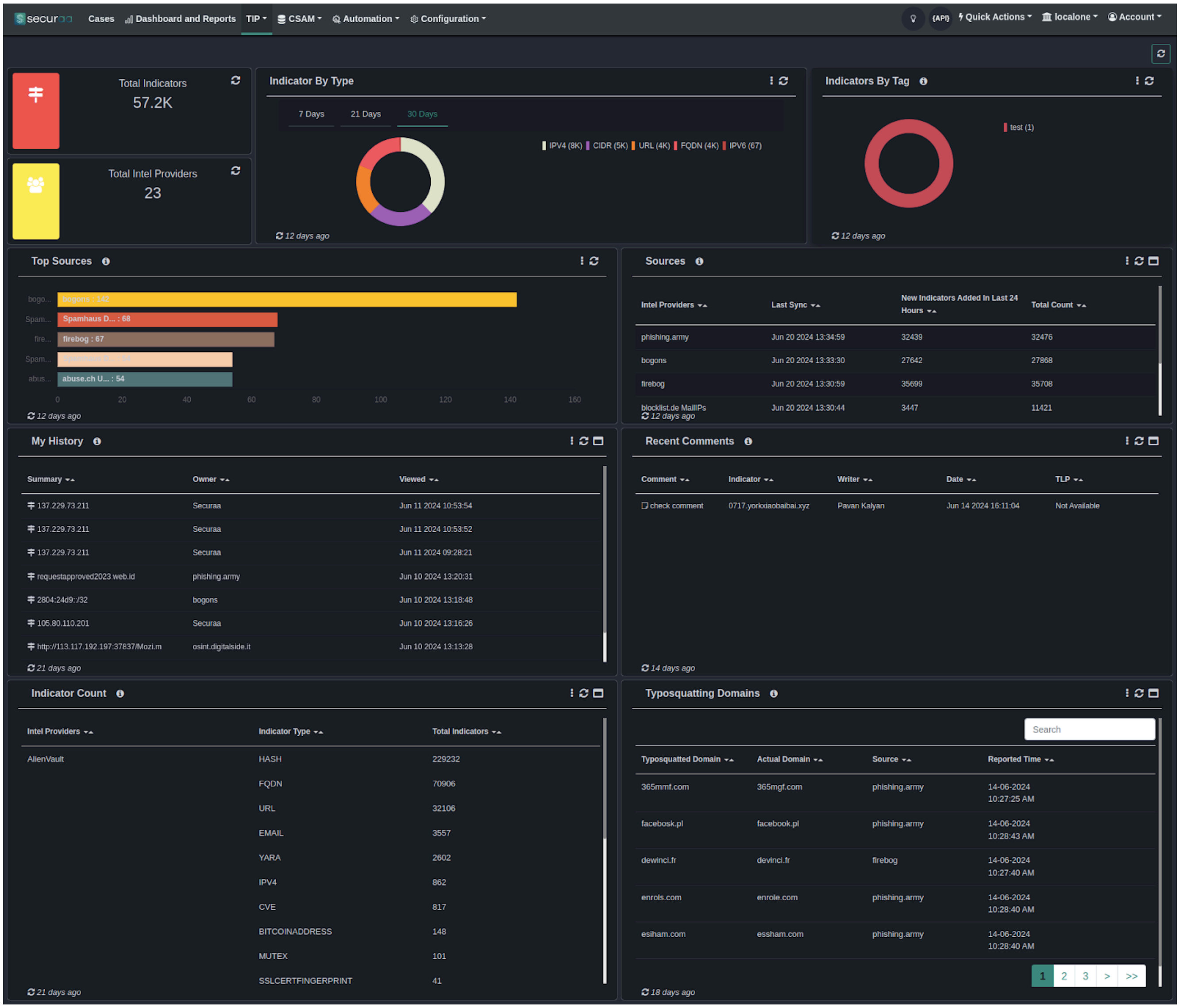
11. Analysts can share threat intelligence data by adding API keys to the TAXII API to authenticate and secure the exchange of cyber threat information, ensuring only authorized systems and users can access and share sensitive data.



Name	Key	End Date	Action
Security	414bb4ab-0c04-476a-986f-e9fccb940d6b	09-07-2024 12:00:00 AM	🗑

TIP Dashboard

The TIP dashboard contains widgets such as Indicator by Type, Total Indicators, Top Sources, Indicator By Type, etc. TIP is integrated with Securaa as a threat intelligence tool that will help manage and analyze if there are any threats to the system or networks and will display all the information as a graphical representation within the widgets. The SOC Analyst can easily access/view the information by clicking the widgets.



Sources

Intel Providers	Last Sync	New Indicators Added In Last 24 Hours	Total Count
phishing.army	Jun 20 2024 13:34:59	32439	32476
bogons	Jun 20 2024 13:33:30	27642	27868
firebog	Jun 20 2024 13:30:59	35699	35708
blocklist.de MailIPs	Jun 20 2024 13:30:44	3447	11421

12 days ago

My History

Summary	Owner	Viewed
137.229.73.211	Securaa	Jun 11 2024 10:53:54
137.229.73.211	Securaa	Jun 11 2024 10:53:52
137.229.73.211	Securaa	Jun 11 2024 09:28:21
requestapproved2023.web.id	phishing.army	Jun 10 2024 13:20:31
2804:24d9::/32	bogons	Jun 10 2024 13:18:48
105.80.110.201	Securaa	Jun 10 2024 13:16:26
http://113.117.192.197:37837/Mozi.m	osint.digitalside.it	Jun 10 2024 13:13:28

21 days ago

Recent Comments

Comment	Indicator	Writer	Date	TLP
check comment	0717.yorkxiaobaibai.xyz	Pavan Kalyan	Jun 14 2024 16:11:04	Not Available

14 days ago

Indicator Count

Intel Providers	Indicator Type	Total Indicators
AlienVault	HASH	229232
	FQDN	70906
	URL	32106
	EMAIL	3557
	YARA	2602
	IPV4	862
	CVE	817
	BITCOINADDRESS	148
	MUTEX	101
	SSLCERTFINGERPRINT	41

21 days ago

Typosquatting Domains

Search

Typosquatted Domain	Actual Domain	Source	Reported Time
365mmf.com	365mgf.com	phishing.army	14-06-2024 10:27:25 AM
facebosk.pl	facebook.pl	phishing.army	14-06-2024 10:28:43 AM
dewinci.fr	devinci.fr	firebog	14-06-2024 10:27:40 AM
enrols.com	enrole.com	phishing.army	14-06-2024 10:28:40 AM
esiham.com	essham.com	phishing.army	14-06-2024 10:28:40 AM

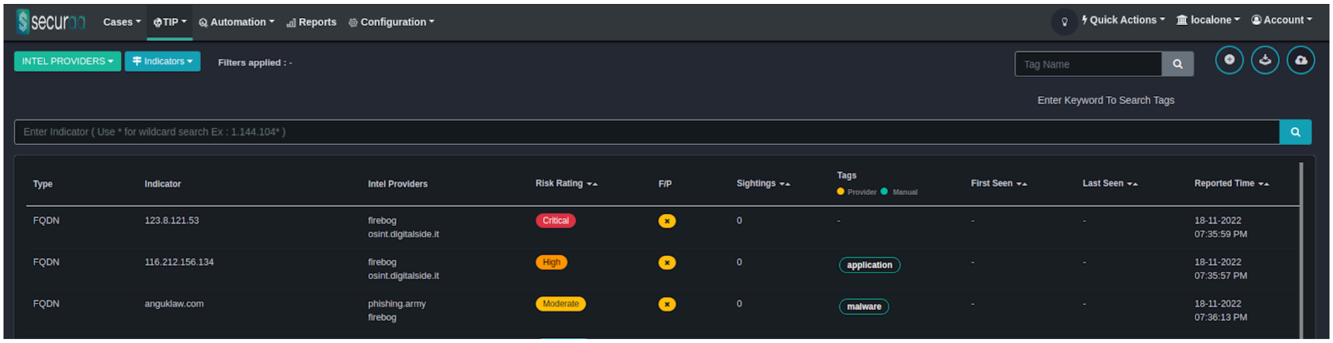
18 days ago

Indicator

Indicator Browser

Analysts can click on the Total Indicators Widget in the dashboard or can navigate from the TIP menu to go to the Indicator browser screen. The indicator browser screen displays a list of all indicators available in the TIP platform. Users will have the option to filter indicators based on Intel Provider, Indicator Type, Tags, etc. Also, users can search for specific indicators in the search bar Or can use wildcard queries to find patterns in an indicator.

E.g.: 120.* will list down all indicators which start from ‘120.’



Filters applied : -

Tag Name

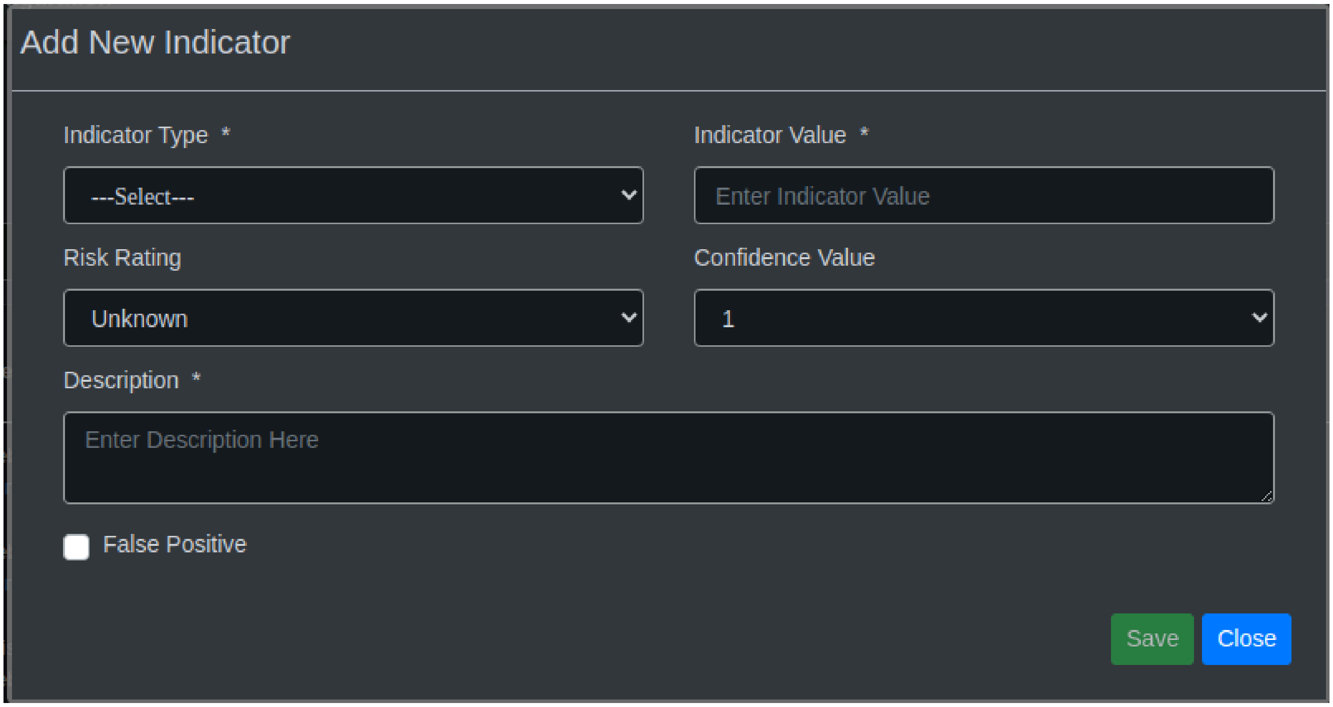
Enter Keyword To Search Tags

Enter Indicator (Use * for wildcard search Ex : 1.144.104*)

Type	Indicator	Intel Providers	Risk Rating	F/P	Sightings	Tags ● Provider ● Manual	First Seen	Last Seen	Reported Time
FQDN	123.8.121.53	firebog osint.digitalside.it	Critical	×	0	-	-	-	18-11-2022 07:35:59 PM
FQDN	116.212.156.134	firebog osint.digitalside.it	High	×	0	application	-	-	18-11-2022 07:35:57 PM
FQDN	anguklaw.com	phishing.army firebog	Moderate	×	0	malware	-	-	18-11-2022 07:36:13 PM

Add Indicator

Analysts can also add new Indicators manually by clicking on ⊕ the icon at the top right corner of the indicator browser screen. The details needed to add a new Indicator manually are as shown in the screenshot below.



Add New Indicator

Indicator Type *
---Select---

Indicator Value *
Enter Indicator Value

Risk Rating
Unknown

Confidence Value
1

Description *
Enter Description Here

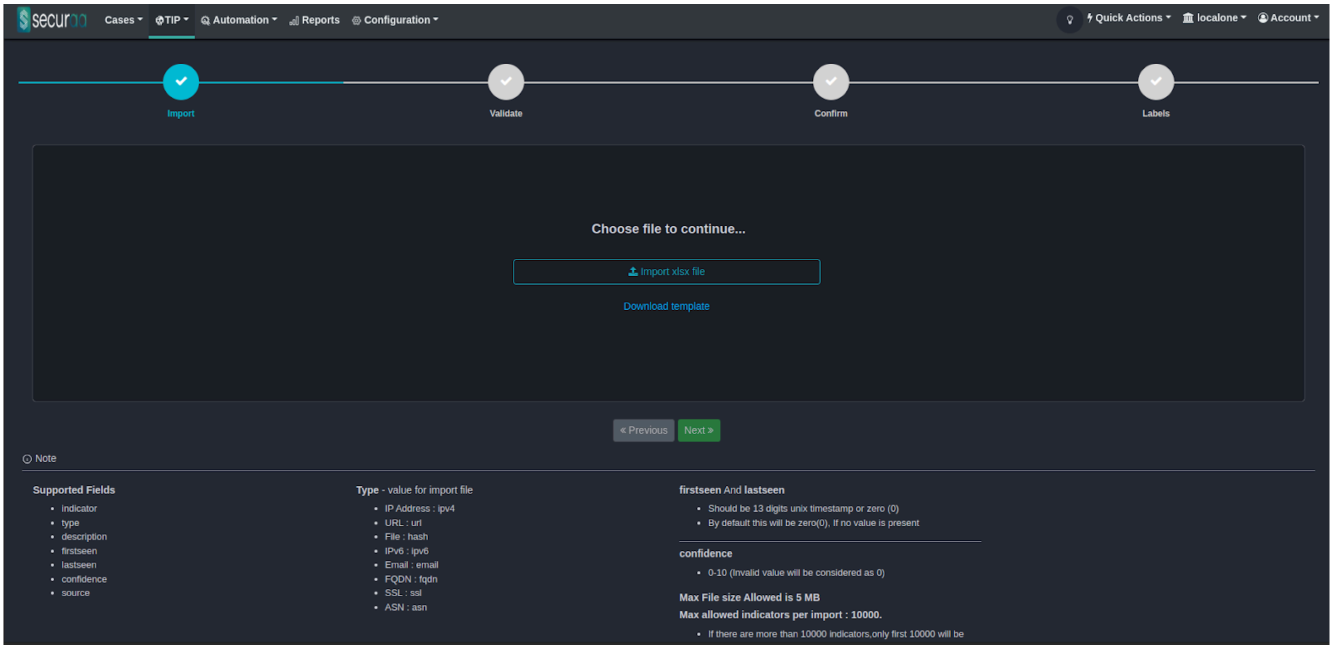
□ False Positive

Export Indicators

Analysts can download all the indicator data available in the TIP in .CSV format by clicking on the ⤓ icon at the top right corner of the indicator browser screen.

Import Indicators

Analysts can import indicators to Securaa TIP by clicking on the icon at the top right corner of the indicator browser screen.



Choose file to continue...

Note

Supported Fields

- indicator
- type
- description
- firstseen
- lastseen
- confidence
- source

Type - value for import file

- IP Address : ipv4
- URL : url
- File : hash
- IPv6 : ipv6
- Email : email
- FQDN : fqdn
- SSL : ssl
- ASN : asn

firstseen And **lastseen**

- Should be 13 digits unix timestamp or zero (0)
- By default this will be zero(0), If no value is present

confidence

- 0-10 (Invalid value will be considered as 0)

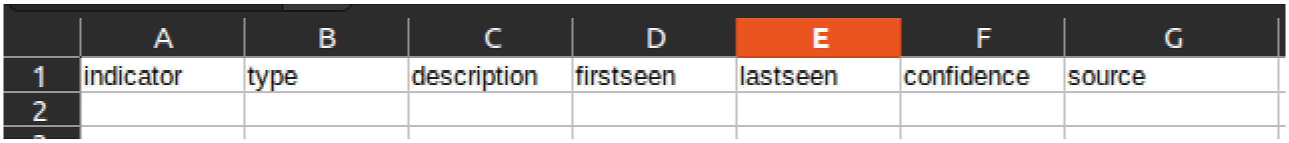
Max File size Allowed is 5 MB

Max allowed indicators per import : 10000.

- If there are more than 10000 indicators,only first 10000 will be

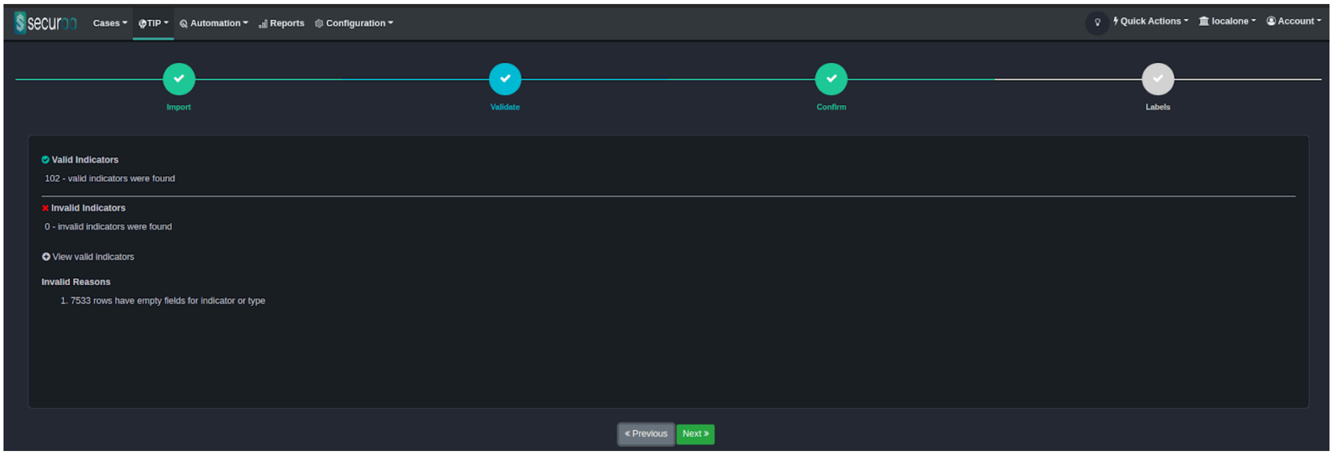
The steps to Import are as follows

1. Download template.
2. Fill all the indicator data in CSV file in the format shown in the below snapshot



	A	B	C	D	E	F	G
1	indicator	type	description	firstseen	lastseen	confidence	source
2							

3. Upload the CSV containing indicator data.
4. verify indicator details and confirm indicators that are being uploaded.



Valid Indicators

102 - valid indicators were found

Invalid Indicators

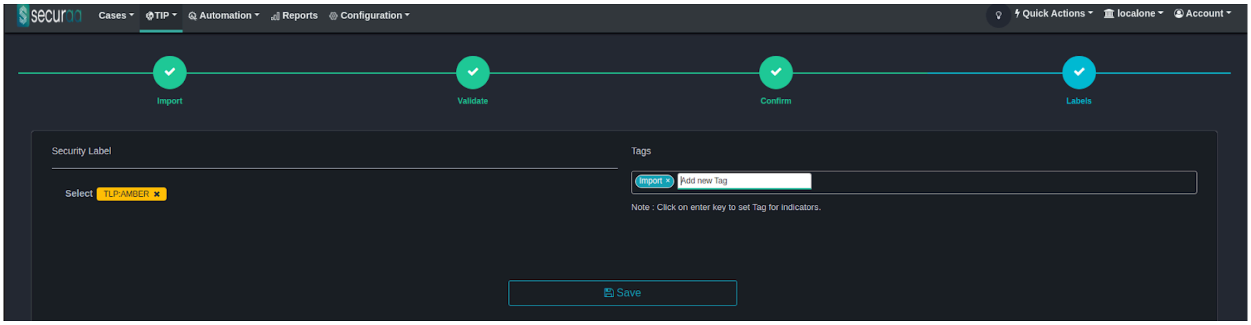
0 - invalid indicators were found

View valid indicators

Invalid Reasons

1. 7533 rows have empty fields for indicator or type

5. Set TLP and tags for Indicators being imported and click on Save.



Security Label

Select TLP:AMBER

Tags

Import

Add new Tag

Note : Click on enter key to set Tag for indicators.

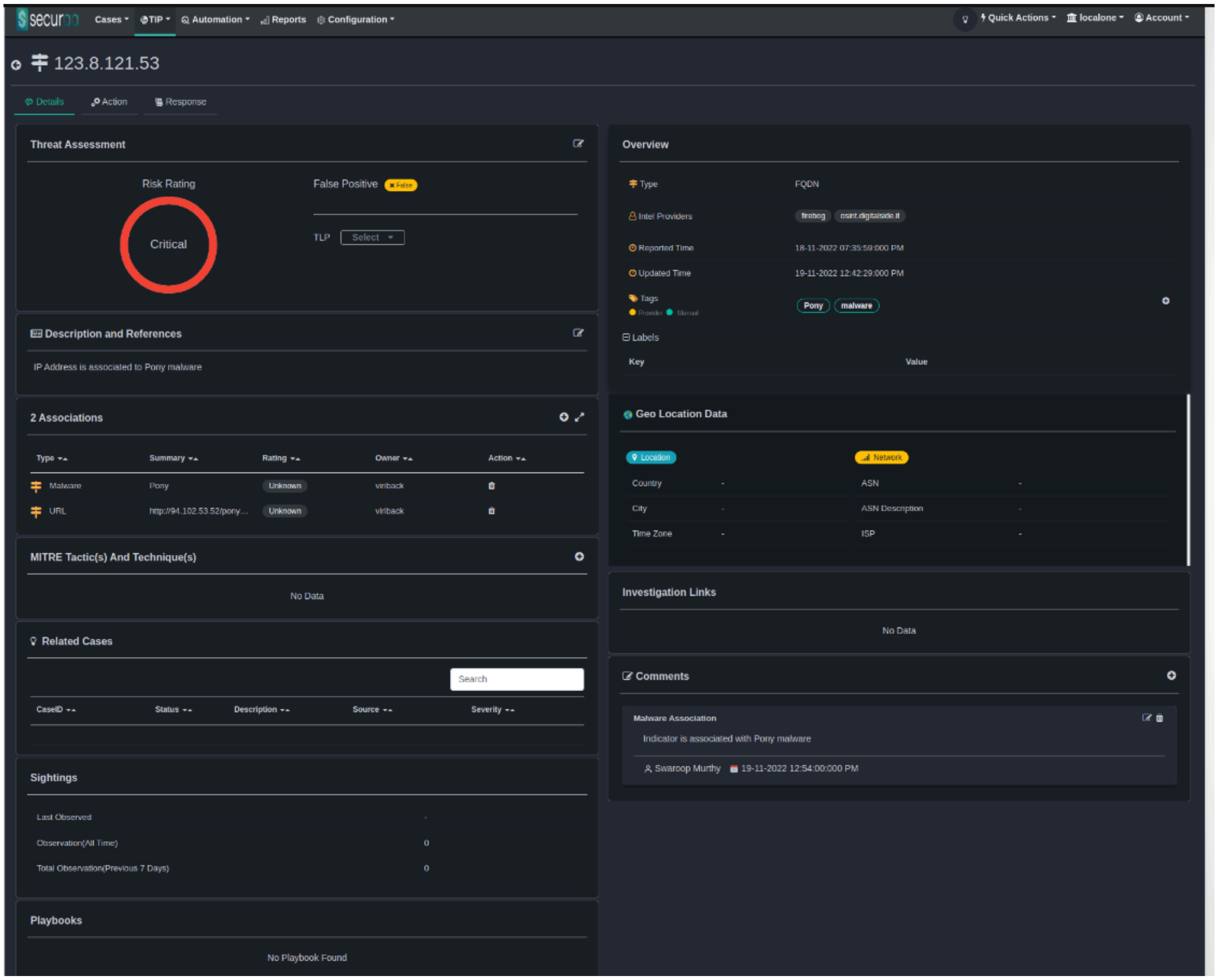
Indicator Overview

Users can drill down by clicking on any indicator in the browser screen to learn about details like the Source of the Indicator, when was the indicator first seen, last seen, The time it was imported to the Securaa TIP platform, risk rating, tags, comments, location information, etc.

Analysts can perform the following operations on the indicator overview screen

- Update Indicator Risk rating
- Set the Indicator as False Positive.
- Set TLP for indicator.
- Set Indicator reference and description.
- Set Mitre Technique and Tactics
- View Location Information
- Set Tags and Comments for Indicator.
- View / Export Stix representation of indicator.

- View Incidents/ Cases related to the Indicator.
- Click on Investigation Links to get more information.



123.8.121.53

Threat Assessment

Risk Rating: Critical

False Positive: False

TLP: Select

Description and References

IP Address is associated to Pony malware

2 Associations

Type	Summary	Rating	Owner	Action
Malware	Pony	Unknown	viriback	
URL	http://94.102.53.52/pony...	Unknown	viriback	

MITRE Tactic(s) And Technique(s)

No Data

Related Cases

Search

CaseID	Status	Description	Source	Severity

Sightings

Last Observed	-
Observation(All Time)	0
Total Observation(Previous 7 Days)	0

Playbooks

No Playbook Found

Overview

Type	FQDN
Intel Providers	firebog osint.digitalside.it
Reported Time	18-11-2022 07:35:59:000 PM
Updated Time	19-11-2022 12:42:29:000 PM
Tags ● Provider ● Manual	Pony malware

Labels

Key	Value

Geo Location Data

Location		Network	
Country	-	ASN	-
City	-	ASN Description	-
Time Zone	-	ISP	-

Investigation Links

No Data

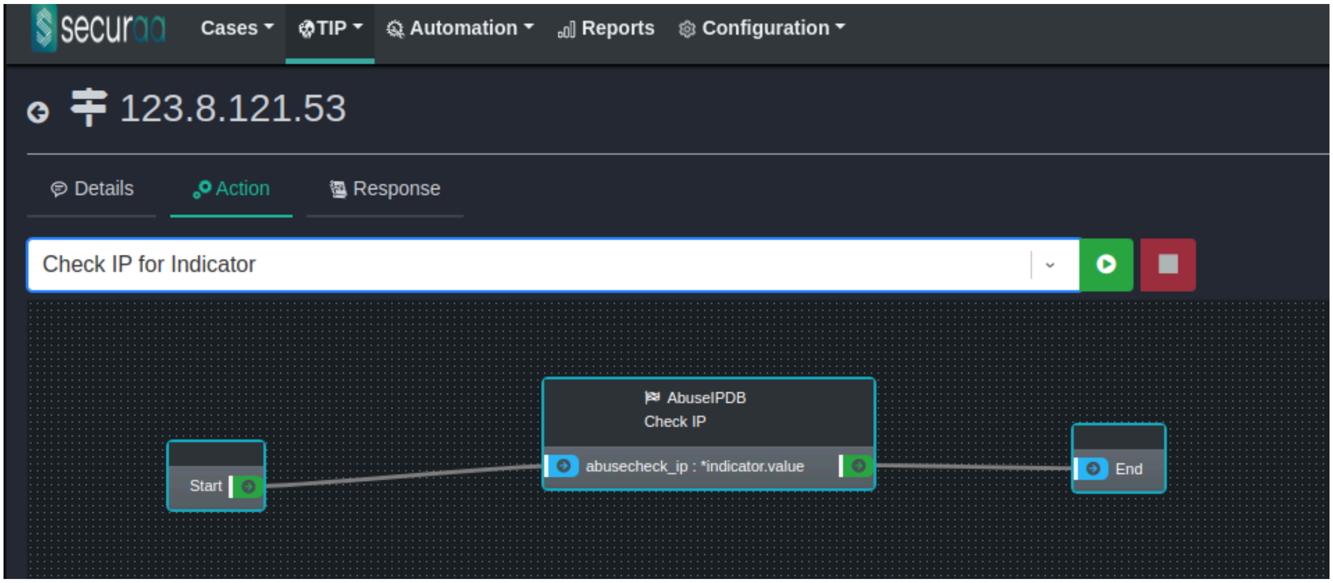
Comments

Malware Association

Indicator is associated with Pony malware

Swaroop Murthy 19-11-2022 12:54:00:000 PM

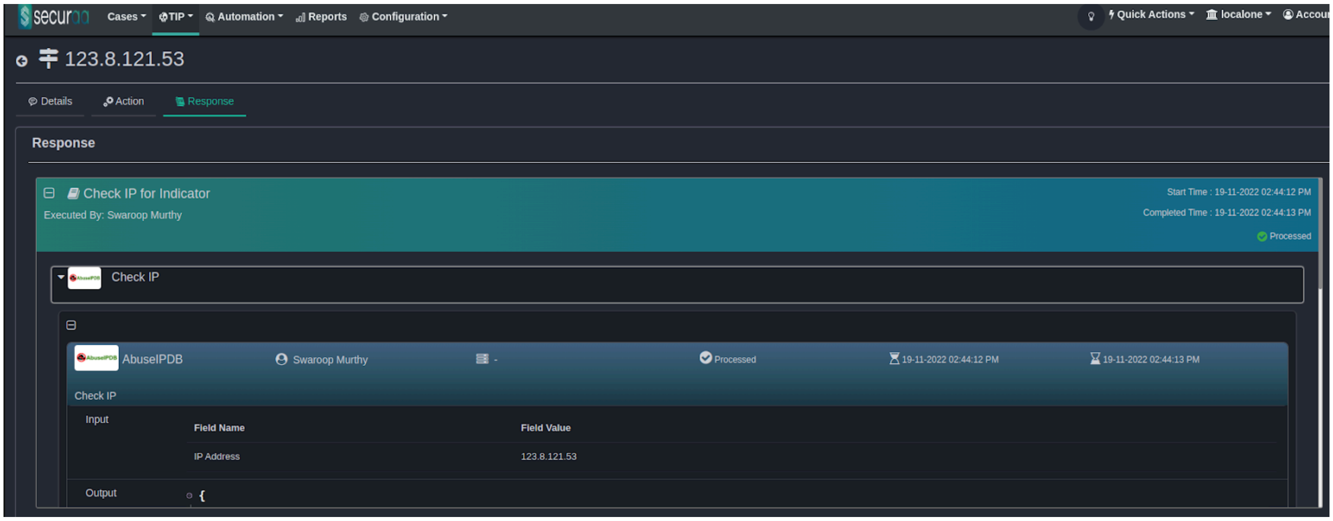
Analysts can click on the Action Tab to execute the playbook for the indicator and see the output in the response tab.



123.8.121.53

Check IP for Indicator

AbuseIPDB
Check IP
abusecheck_ip : *indicator.value



123.8.121.53

Response

Check IP for Indicator
Executed By: Swaroop Murthy
Start Time : 19-11-2022 02:44:12 PM
Completed Time : 19-11-2022 02:44:13 PM
Processed

Check IP

AbuseIPDB | Swaroop Murthy | - | Processed | 19-11-2022 02:44:12 PM | 19-11-2022 02:44:13 PM

Check IP

Input

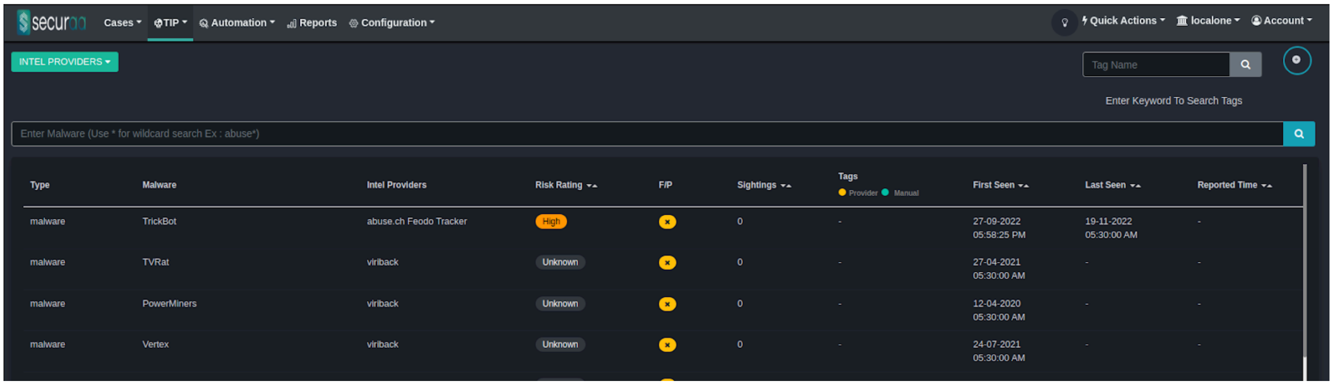
Field Name	Field Value
IP Address	123.8.121.53

Output {

Malware

Malware Browser

Analysts can view lists of malwares by navigating from the TIP menu. I.e., TIP-> Objects->Malware to go to the malware browser screen. The malware browser screen displays a list of all malwares available in the TIP platform. Analysts will have the option to filter malwares based on Intel Provider and can search for specific malware in the search bar and also filter by tags.



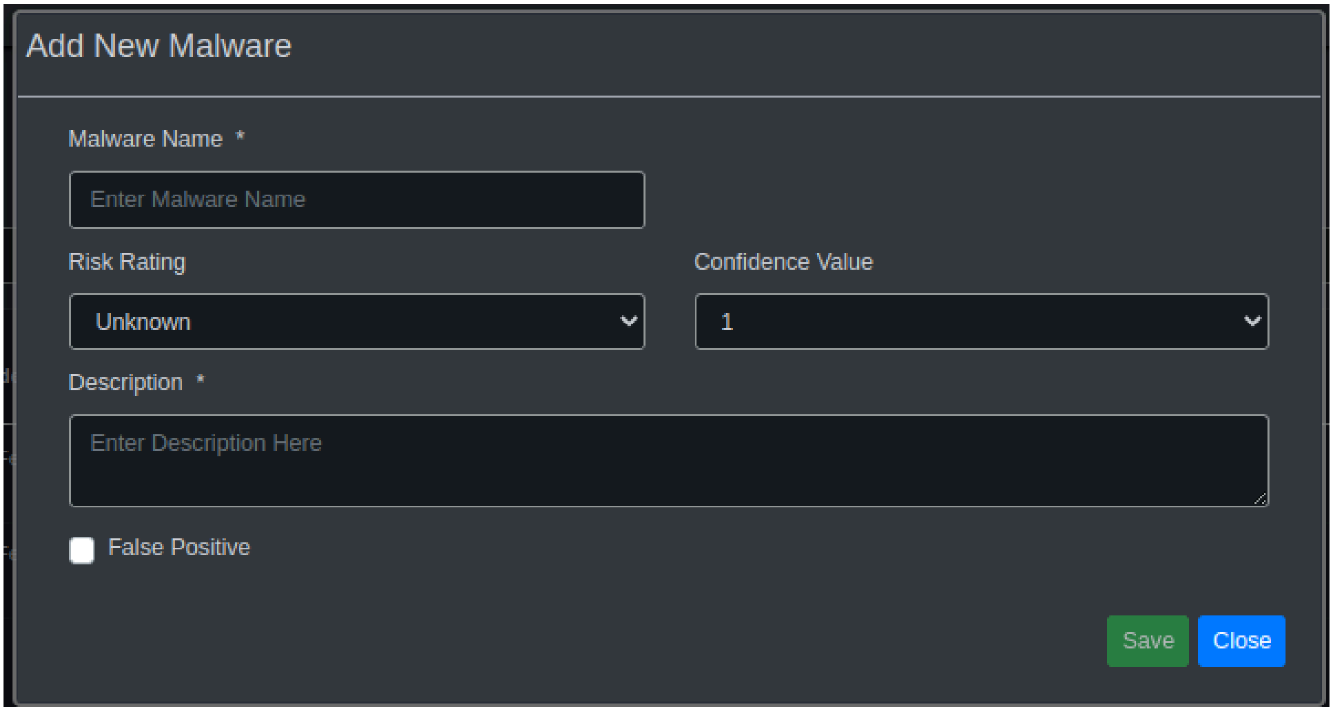
Enter Keyword To Search Tags

Enter Malware (Use * for wildcard search Ex : abuse*)

Type	Malware	Intel Providers	Risk Rating	F/P	Sightings	Tags ● Provider ● Manual	First Seen	Last Seen	Reported Time
malware	TrickBot	abuse.ch Feodo Tracker	High	×	0	-	27-09-2022 05:58:25 PM	19-11-2022 05:30:00 AM	-
malware	TVRat	viriback	Unknown	×	0	-	27-04-2021 05:30:00 AM	-	-
malware	PowerMiners	viriback	Unknown	×	0	-	12-04-2020 05:30:00 AM	-	-
malware	Vertex	viriback	Unknown	×	0	-	24-07-2021 05:30:00 AM	-	-

Add Malware

Analysts can also add new malwares manually by clicking on icon at top right corner of malware browser screen. The details needed to add a new malware manually is as shown in the screenshot below.



Add New Malware

Malware Name *

Enter Malware Name

Risk Rating: Unknown

Confidence Value: 1

Description *

Enter Description Here

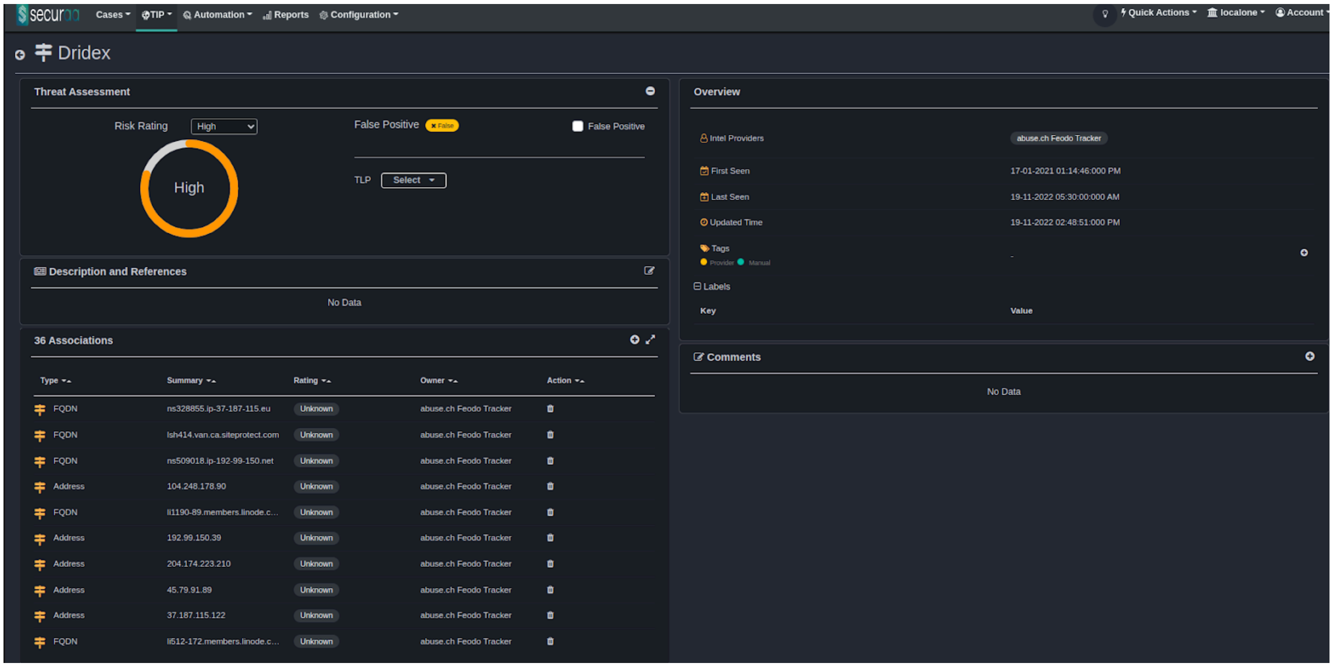
□ False Positive

Malware Overview

Analysts can drill down by clicking on any malware in the browser screen to know about details like Source of malware, when was the malware first seen, last seen, The time it was imported to securaa TIP platform, risk rating, tags, comments etc.

Analysts can perform following operations on the malware overview screen

- Update malware Risk rating
- Set malware as False Positive.
- Set TLP for malware.
- Set malware reference and description.
- Set Mitre Technique and Tactics
- Set Tags and Comments for malware.
- View / Export Stix representation of malware and associations.
- Associate Other Indicators/ Malware/ Campaign.



Dridex

Threat Assessment

Risk Rating: High

False Positive: ✕ False

☐ False Positive

TLP: Select

Description and References

No Data

36 Associations

Type	Summary	Rating	Owner	Action
FQDN	ns328855.ip-37-187-115.eu	Unknown	abuse.ch Feodo Tracker	🗑
FQDN	lsh414.van.ca.siteprotect.com	Unknown	abuse.ch Feodo Tracker	🗑
FQDN	ns509018.ip-192-99-150.net	Unknown	abuse.ch Feodo Tracker	🗑
Address	104.248.178.90	Unknown	abuse.ch Feodo Tracker	🗑
FQDN	li1190-89.members.linode.c…	Unknown	abuse.ch Feodo Tracker	🗑
Address	192.99.150.39	Unknown	abuse.ch Feodo Tracker	🗑
Address	204.174.223.210	Unknown	abuse.ch Feodo Tracker	🗑
Address	45.79.91.89	Unknown	abuse.ch Feodo Tracker	🗑
Address	37.187.115.122	Unknown	abuse.ch Feodo Tracker	🗑
FQDN	li512-172.members.linode.c…	Unknown	abuse.ch Feodo Tracker	🗑

Overview

Intel Providers	abuse.ch Feodo Tracker
First Seen	17-01-2021 01:14:46:000 PM
Last Seen	19-11-2022 05:30:00:000 AM
Updated Time	19-11-2022 02:48:51:000 PM
Tags ● Provider ● Manual	-

Labels

Key	Value

Comments

No Data

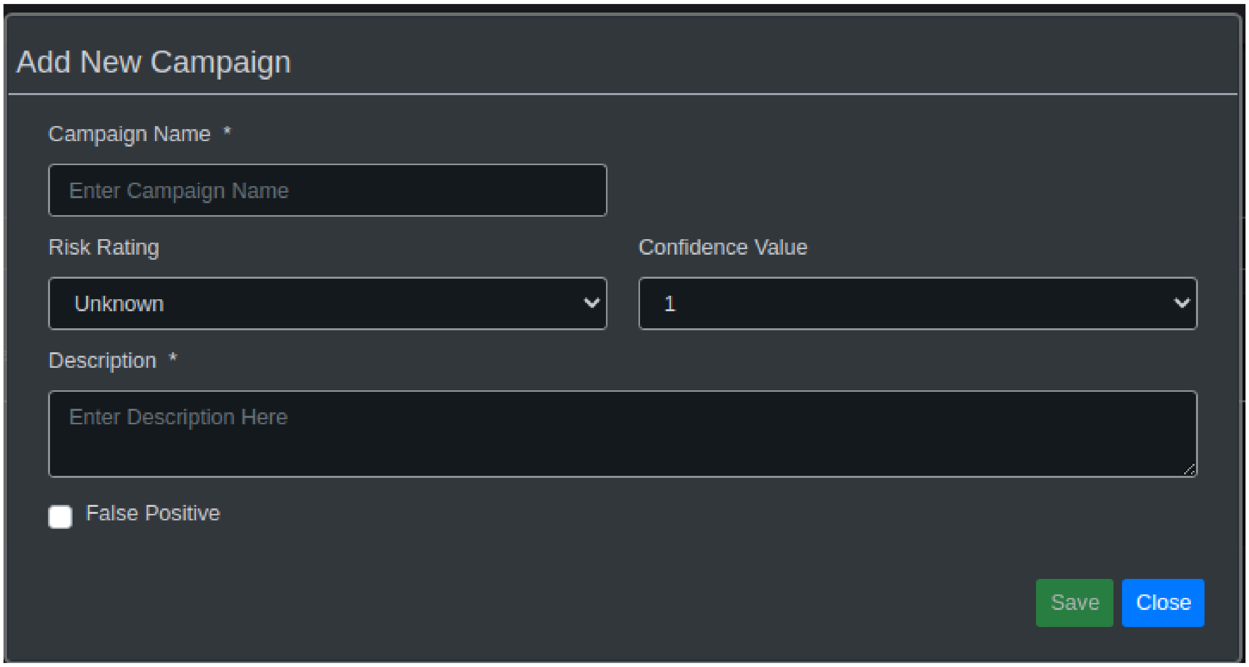
Campaign

Campaign Browser

Analysts can view lists of campaigns by navigating from the TIP menu. I.e., TIP-> Objects->Campaign to go to the campaign browser screen. The campaign browser screen displays a list of all campaigns available in the TIP platform. Analysts will have the option to filter campaigns based on Intel Provider and can search for specific campaigns in the search bar and also filter by tags.

Add Campaign

Analysts can also add new campaigns manually by clicking on icon at top right corner of campaign browser screen. The details needed to add a new campaign manually is as shown in the screenshot below.



Add New Campaign

Campaign Name *

Enter Campaign Name

Risk Rating: Unknown

Confidence Value: 1

Description *

Enter Description Here

□ False Positive

Campaign Overview

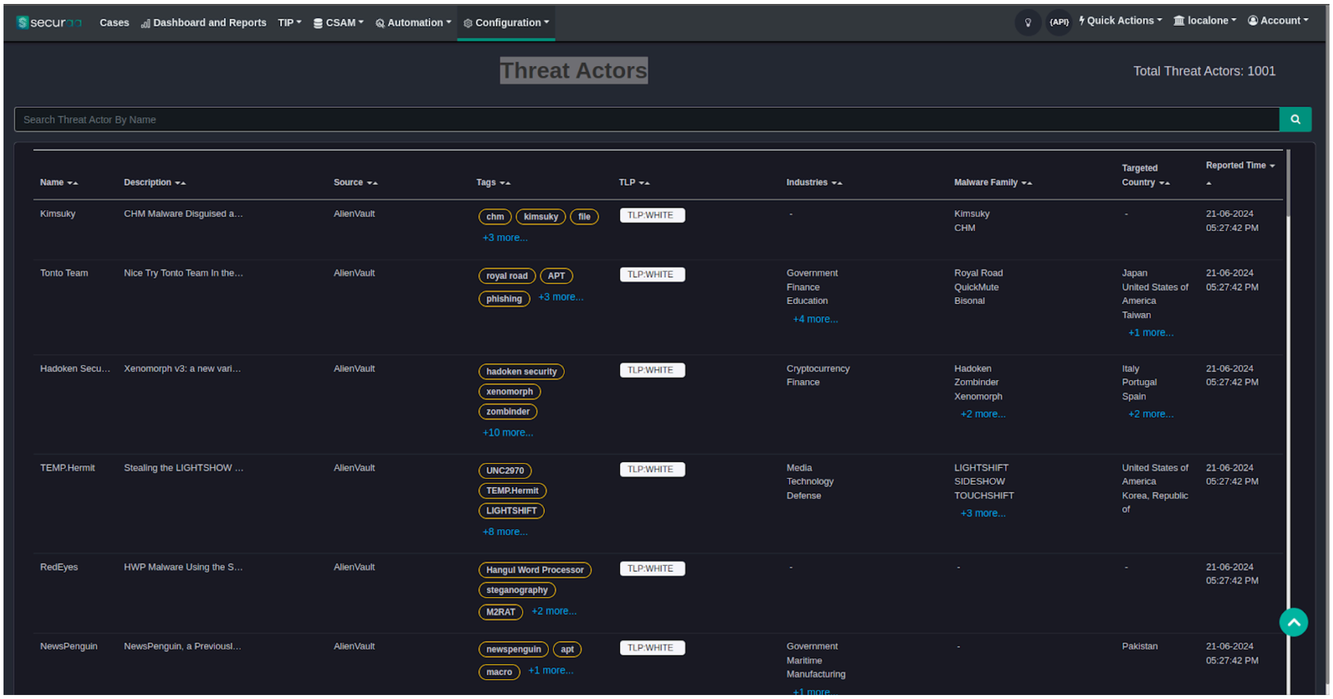
Analysts can drill down by clicking on any campaign in the browser screen to know about details like Source of campaign, when was the campaign first seen, last seen, The time it was imported to securaa TIP platform, risk rating, tags, comments etc.

Analysts can perform following operations on the campaign overview screen

- Update campaign Risk rating
- Set campaign as False Positive.
- Set TLP for campaign.
- Set campaign reference and description.
- Set Mitre Technique and Tactics
- Set Tags and Comments for the campaign.
- View / Export Stix representation of campaign and associations.
- Associate Other Indicators/ Malware/ Campaign.

Threat Actors

Threat actors are individuals, groups, or organizations that engage in malicious activities with the intent to compromise, damage, or disrupt their targets. They vary in their motivations, which can include financial gain, political objectives, ideological beliefs, or personal grievances. Understanding threat actors is crucial for developing effective cybersecurity defenses and response strategies.



Threat Actors

Total Threat Actors: 1001

Name	Description	Source	Tags	TLP	Industries	Malware Family	Targeted Country	Reported Time
Kimsuky	CHM Malware Disguised a…	AlienVault	chm kimsuky file +3 more...	TLP:WHITE	-	Kimsuky CHM	-	21-06-2024 05:27:42 PM
Tonto Team	Nice Try Tonto Team In the…	AlienVault	royal road APT phishing +3 more...	TLP:WHITE	Government Finance Education +4 more...	Royal Road QuickMute Bisonal	Japan United States of America Taiwan +1 more...	21-06-2024 05:27:42 PM
Hadoken Secu…	Xenomorph v3: a new vari…	AlienVault	hadoken security xenomorph zombinder +10 more...	TLP:WHITE	Cryptocurrency Finance	Hadoken Zombinder Xenomorph +2 more...	Italy Portugal Spain +2 more...	21-06-2024 05:27:42 PM
TEMP.Hermit	Stealing the LIGHTSHOW …	AlienVault	UNC2970 TEMP.Hermit LIGHTSHIFT +8 more...	TLP:WHITE	Media Technology Defense	LIGHTSHIFT SIDESHOW TOUCHSHIFT +3 more...	United States of America Korea, Republic of	21-06-2024 05:27:42 PM
RedEyes	HWP Malware Using the S…	AlienVault	Hangul Word Processor steganography M2RAT +2 more...	TLP:WHITE	-	-	-	21-06-2024 05:27:42 PM
NewsPenguin	NewsPenguin, a Previousl…	AlienVault	newspenguin apt macro +1 more...	TLP:WHITE	Government Maritime Manufacturing +1 more...	-	Pakistan	21-06-2024 05:27:42 PM

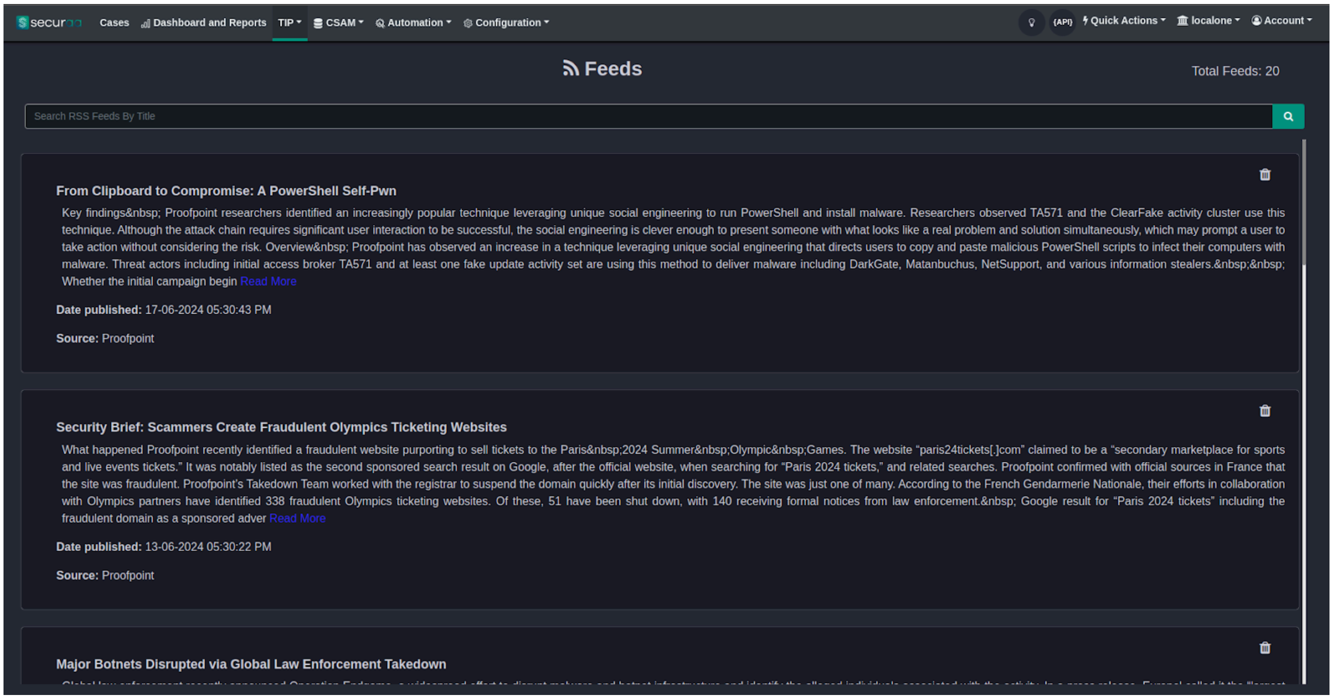
Feeds

In cybersecurity, feeds refer to streams of data that provide continuous, real-time updates on potential threats, vulnerabilities, and other relevant security information. These feeds help organizations stay informed about the latest security risks and take proactive measures to protect their systems. Common types of cybersecurity feeds include:

1. **Threat Intelligence Feeds**: Provide information on emerging threats, including indicators of compromise (IOCs), attack patterns, and threat actor activities.

2. **Vulnerability Feeds**: Offer updates on newly discovered vulnerabilities in software, hardware, and systems, often including patches and mitigation strategies.
3. **Malware Feeds**: Supply data on new malware variants, including their signatures, behaviors, and detection methods.
4. **Reputation Feeds**: Track the reputation of IP addresses, domains, and URLs, identifying those associated with malicious activity.
5. **Phishing Feeds**: Report on new phishing campaigns, tactics, and targets, helping organizations identify and block phishing attempts.

By integrating these feeds into their security systems, organizations can enhance their ability to detect and respond to threats promptly.



From Clipboard to Compromise: A PowerShell Self-Pwn

Key findings Proofpoint researchers identified an increasingly popular technique leveraging unique social engineering to run PowerShell and install malware. Researchers observed TA571 and the ClearFake activity cluster use this technique. Although the attack chain requires significant user interaction to be successful, the social engineering is clever enough to present someone with what looks like a real problem and solution simultaneously, which may prompt a user to take action without considering the risk. Overview Proofpoint has observed an increase in a technique leveraging unique social engineering that directs users to copy and paste malicious PowerShell scripts to infect their computers with malware. Threat actors including initial access broker TA571 and at least one fake update activity set are using this method to deliver malware including DarkGate, Matanbuchus, NetSupport, and various information stealers.   Whether the initial campaign begin Read More

Date published: 17-06-2024 05:30:43 PM

Source: Proofpoint

Security Brief: Scammers Create Fraudulent Olympics Ticketing Websites

What happened Proofpoint recently identified a fraudulent website purporting to sell tickets to the Paris 2024 Summer Olympic Games. The website "paris24tickets[.]com" claimed to be a "secondary marketplace for sports and live events tickets." It was notably listed as the second sponsored search result on Google, after the official website, when searching for "Paris 2024 tickets," and related searches. Proofpoint confirmed with official sources in France that the site was fraudulent. Proofpoint's Takedown Team worked with the registrar to suspend the domain quickly after its initial discovery. The site was just one of many. According to the French Gendarmerie Nationale, their efforts in collaboration with Olympics partners have identified 338 fraudulent Olympics ticketing websites. Of these, 51 have been shut down, with 140 receiving formal notices from law enforcement. Google result for "Paris 2024 tickets" including the fraudulent domain as a sponsored adver Read More

Date published: 13-06-2024 05:30:22 PM

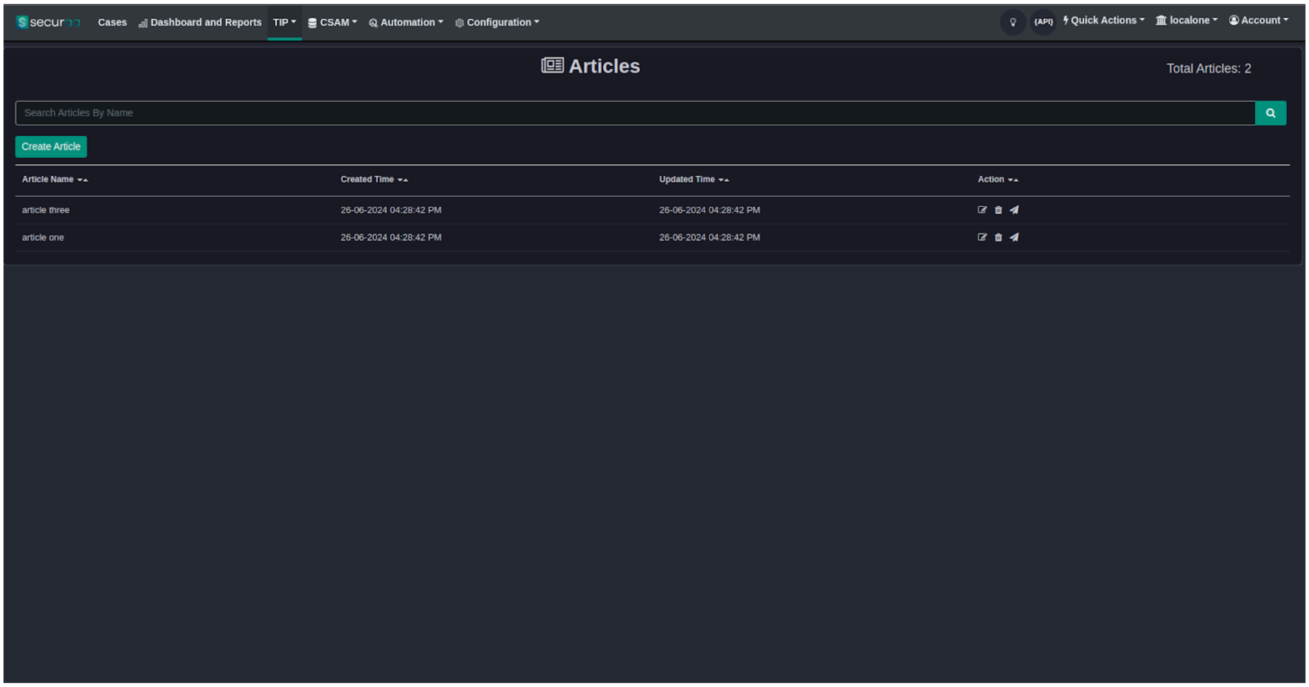
Source: Proofpoint

Major Botnets Disrupted via Global Law Enforcement Takedown

Global law enforcement recently announced Operation Endgame, a widespread effort to disrupt malware and botnet infrastructure and identify the alleged individuals associated with the activity. In a press release, Europol called it the "largest

Articles

Analysts can create their articles to document and share detailed information about various cybersecurity topics, such as indicators of compromise (IOCs), malware, and campaigns. These articles can serve as valuable resources for both internal teams and the wider cybersecurity community



Articles

Total Articles: 2

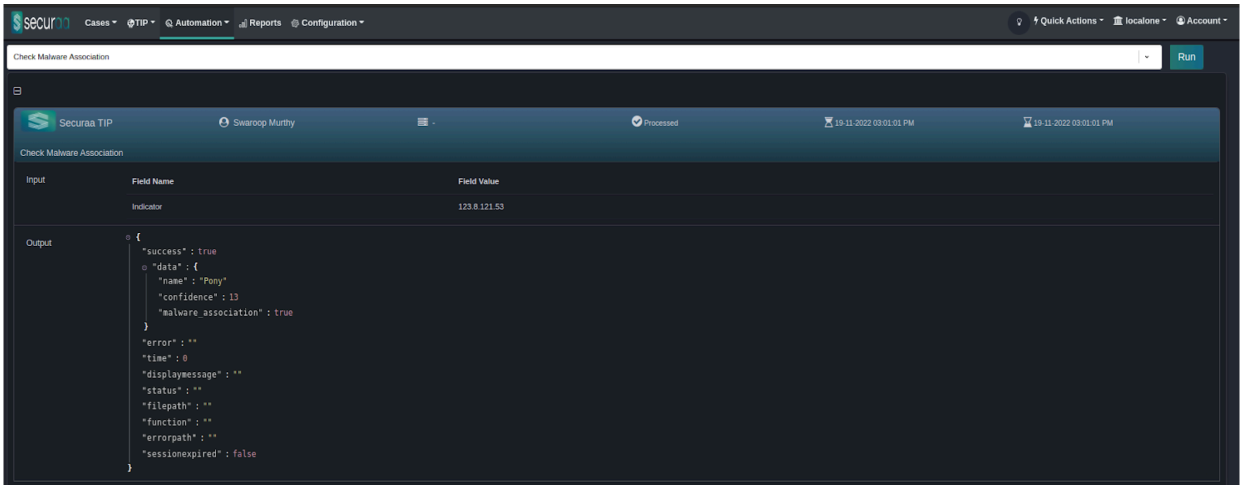
Article Name	Created Time	Updated Time	Action
article three	26-06-2024 04:28:42 PM	26-06-2024 04:28:42 PM	
article one	26-06-2024 04:28:42 PM	26-06-2024 04:28:42 PM	

TIP Automation Tasks

Securaa TIP supports many automated tasks. Below are the details of few tasks

1. **Task to verify malware association of an Indicator**.

This helps in enriching firewall rules to block indicators if they are associated with malware.



Check Malware Association

Securaa TIP — Swaroop Murthy — - — Processed — 19-11-2022 03:01:01 PM — 19-11-2022 03:01:01 PM

Check Malware Association

Input

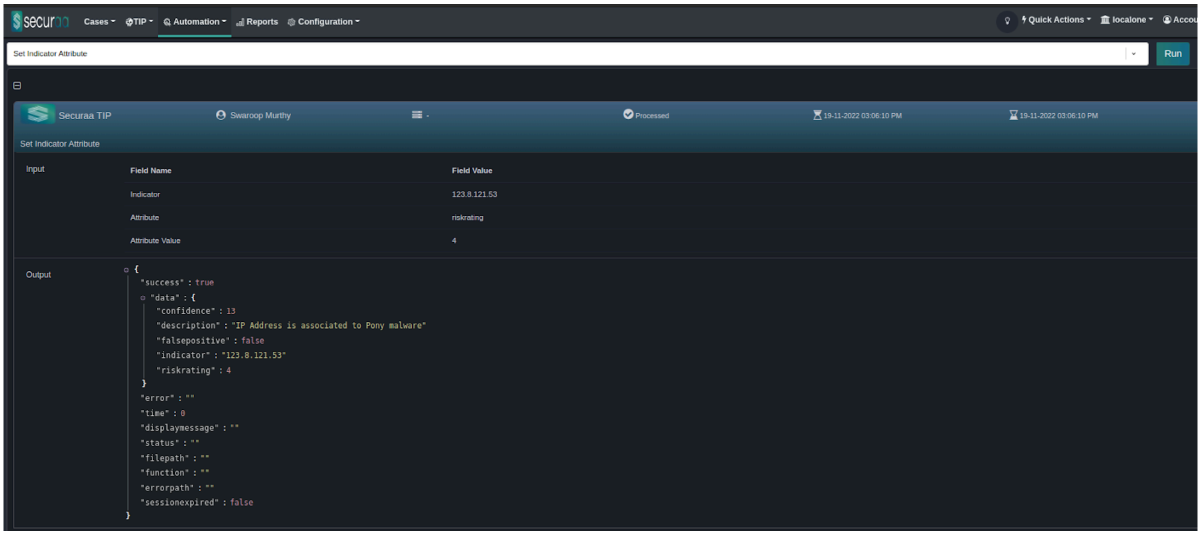
Field Name	Field Value
Indicator	123.8.121.53

Output

```
{
  "success" : true
  "data" : {
    "name" : "Pony"
    "confidence" : 13
    "malware_association" : true
  }
  "error" : ""
  "time" : 0
  "displaymessage" : ""
  "status" : ""
  "filepath" : ""
  "function" : ""
  "errorpath" : ""
  "sessionexpired" : false
}
```

2. **Task to set Indicator Attributes**.

This task helps to enrich the TIP database by setting risk rating, description, and confidence and also to set indicators as false positives.



Set Indicator Attribute

Securaa TIP | Swaroop Murthy | - | Processed | 19-11-2022 03:06:10 PM | 19-11-2022 03:06:10 PM

Set Indicator Attribute

Input

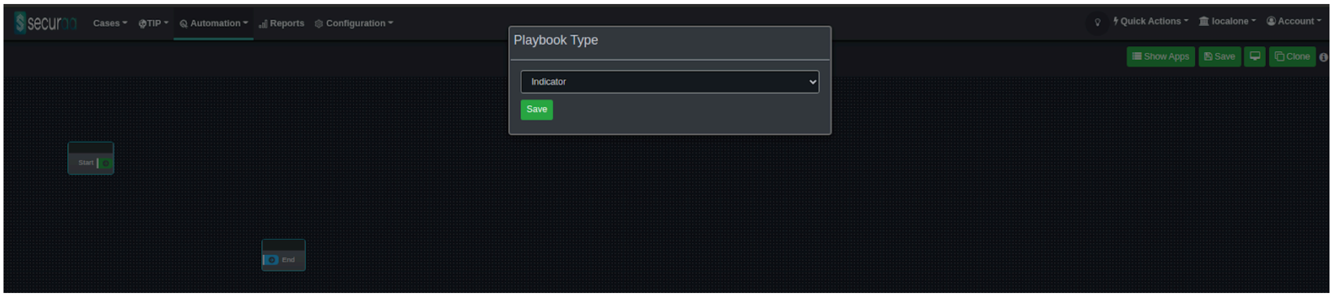
Field Name	Field Value
Indicator	123.8.121.53
Attribute	riskrating
Attribute Value	4

Output

```
{
  "success" : true
  "data" : {
    "confidence" : 13
    "description" : "IP Address is associated to Pony malware"
    "falsepositive" : false
    "indicator" : "123.8.121.53"
    "riskrating" : 4
  }
  "error" : ""
  "time" : 0
  "displaymessage" : ""
  "status" : ""
  "filepath" : ""
  "function" : ""
  "errorpath" : ""
  "sessionexpired" : false
}
```

Playbook Support for Indicators

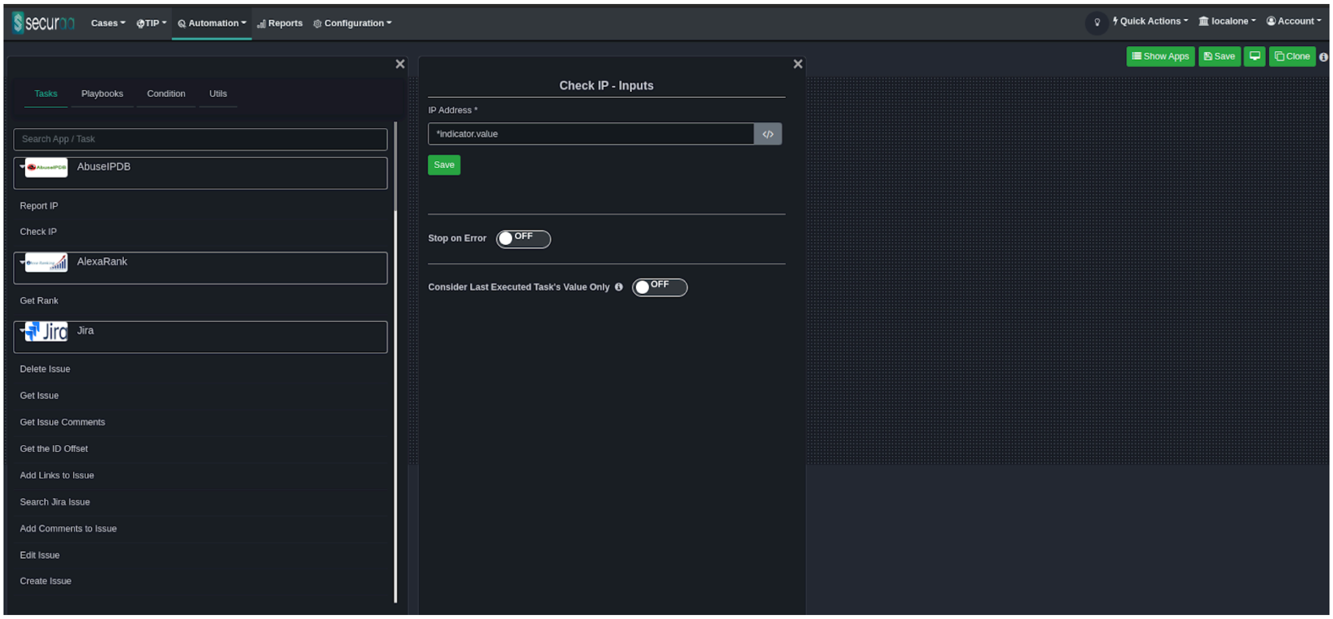
Securaa provides support to execute playbooks not only for cases but also for Indicators. While creating a playbook we can select the playbook type as Indicator as shown below screenshot.



Playbook Type

Indicator

Also you need to select input as *indicator.value to execute playbook for any indicator as shown below.



Check IP - Inputs

IP Address *: *indicator.value

Stop on Error: OFF

Consider Last Executed Task's Value Only: OFF

API Support.

Securaa TIP provides support to import indicators from other third party tools through API. Users can add a new Indicator to securaa using the below API.

URL : https://<tip_server_host>:7000/addlocalindicator/
Method : POST
Sample Request Body :

```
{
  "indicator": "8.8.8.8",
  "indicator_type": "ipv4",
  "description" : "Indicator description",
  "tenantcode": "tenantcode"
}
```