Infltip

THREAT INTELLIGENCE PLATFORM

Threat intelligence Platform Featureset

Modules of Threat Intelligence	■ Threat Data Feeds(IP, Domains, URLs, File Hash & CVE) ■ Threat Dashbaord/News ■ IOC/IOA Enrichment with Real Time Risk Score & Evidence
Platform type	■ Software
Hosting Enviroment/ Deployment Option	■ VM or Bare metal
Downloadable Threat intelligence feeds in form of	■ JSON, CSV, XML, STIX, STIX2, TAXII
Type of Threat Data Feeds Records	■ IP reputation ■ Malicious URLs ■ Phishing URLs feed ■ Botnet C&C URLs feed ■ Ransomware URLs feed ■ Malicious Hashes feed ■ Malicious Domains Feeds ■ Vulnerability ■ Open Proxies ■ Active C&C ■ DDOS ■ Fast Flux ■ Honey Pot ■ Positive Malware Verdicts ■ TOR Entry/Exit Nodes ■ Verified/Unverified Proof of Concept ■ Vulnerbility feeds for Exploits in the wild ■ Pre-NVD Vulnerability Feed
Threat Feeds Data related to URL Feeds	■ Malicious URLs ■ Phishing URLs ■ Botnet C&C URLs ■ Ransomware URLs ■ Recent Ransomware Distribution URL ■ URL on Weaponized Domain ■ URLs Reported by DHS AIS ■ Fraudulent Content URLs ■ Cryptocurrency Mining Techniques URLs ■ Spam or Unwanted Content URL ■ Defanged URL ■ Risk Score for respective URL

Threat Feeds Data related to IP Feeds	Active C&C IPs Botnet Traffic IP DDOS involved IP Phishing related IP 5. OEM Research Reported IP Nameserver for C&C Bad SSL Associated IP DNs Abuse IP Honeypot Related IP Brute Force Login related IP Spam Source IP linked to APT 12. IP related to Cyber Attack TOR Node IP Threat Actor Infrastucture IP
Threat Feeds Data related to Hash Feeds	Hasesh with Positive Malware Verdict Recently Active Feeds Targeting Vulnerabilities in the Wild Observed in Underground Virus Testing Sites Malware SSL Certificate Fingerprint Linked to Malware, Attack Vector, Vulneraility or Cyber attack
Threat Feeds Data related to Domain Feeds	C&C DNS Name Malware Related Phishing Related Fraudulant Content Domains Weaponized Domains COVID-19 related domain lure Cryptocurrency Mining related Doamin Typosquat domains Newly Registered Certificate With Potential for Domain Abuse - DNS Sandwich Typo or Homograph Domains Domains resolving to Malicious IP
Threat Feeds Data related to Vulnerability Feeds	Exploited in the Wild by Recently Active Malware Vendor Severity : Critical, High, Medium NIST Severity : Critical, High, Medium Exploited in the Wild by Malware Recent Verified Proof of Concept Available Using Remote Execution Linked to Penetration Testing Tools Linked to Remote Acces Trojan, Malware, Ransomware Web Reporting Prior to NVD Disclosure

InfiTip features

- Infitip provides a GUI where multiple teams can collaborate in real-time and role-based access can be provided for restricted or entire access.

- It provides a single platform for threat data aggregation/consumption from multiple vendors and different data sources like 3rd party blogs, articles and feeds. Moreover, it also allows to publish data to such kind of sources.

- The 3rd party data can be plotted on a timeline and data enrichment can be done. It also allows to enrich data using various 3rd party options like MISP, Maxmind etc.

- It can work on VMs or as a standalone system. It can also work in an AIR gap system.
  User can create custom dashboards.

- It allows the user to set various indicators and custom tagging for the attributes. The scoring of indicators is also possible.

- It allows to setup custom playbooks that run through native integration with leading industry SOAR platforms.
- It provides ability to integrate with various data sources like SIEM, SOAR, TIP and ticketing systems.
- It supports various data models and standards by allowing the user to define and make use of taxonomies.
- Data from standard formats like TAXII, STIX1.x and STIX2.x can be imported and exported.
- It allows to do basic search based on keywords, filters as well as advanced search using operators like arithmetic and boolean. In addition, you can save the searches too.
- It provides detailed analysis and reports of the data collected using various sources. Moreover, the timestamps are set for every piece of data which facilitates historical analysis and reporting including duration based searches.
- The entire data management like import, export, search is possible using the APIs and SDKs. Thus, seamless integration is possible.
- All the additional attributes and contexts provided by the threat intel sources can be parsed and stored. Search and filtering is possible for these additional attributes and contexts.
- It supports manual upload of TTP and IOC and can extract and categorize indicators from such uploaded data.

Infinity labs

Registered Office :
Teerth-Technospace, C-609,
Bangalore-Mumbai Highway, Baner,Pune, IN – 411045
Website : www.infinitylabs.inEmail: sales@infinitylabs.in

• Founded in 2014, Infinity Labs is one of the fastest growing Technology Consulting & Software Solutions.
• Serving customers across the Globe (India, US, UK & Middle East)
• Solutions customised for Telecom, Banking, Media, Retail, Education & Government verticals

All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Infinity Labs assumes no responsibility for any inaccuracies in this document. Infinity Labs reserves the right to change, modify, transfer or otherwise revise this publication without notice.