Quick Heal

Security Simplified

Threat Intelligence Feeds

Strengthening your Cybersecurity

with QUICK HEAL Technologies Ltd.

Authors
Vijay Shankar Yadav | Ganesh Lakariya

Quick Heal
Security Simplified

Table Of Contents

Quick Heal
Security Simplified

Abstract

Threat Intelligence is evidence-based information about cyber-attacks that cyber security experts organize and analyze to improve cyber security. The public needs to know the threats, how they operate, and how their organizations can protect themselves from attacks. However, many businesses are unsure how to handle these cyber-attacks or cyber threats.

For many organizations, the term "threat intelligence" is still new. While many organizations have become more risk-conscious in recent years, threat intelligence has evolved as a term for a decade. What is threat intelligence? How does it prevent data breaches? This research paper covers the answers to these and some other questions about threat intelligence, explaining why it is essential for today's organizations. Also, Threat Intel is a critical resource that can help companies identify how threats impact their business.

Quick Heal's threat intelligence helps answer most of the above questions with the help of simple but powerful intelligence built around the data from millions of endpoints. Quick heal has ~8 million active user base as of 2022, enabling our users to take preventive steps from cyberattacks.

Introduction

Cyber-criminals have created numerous ways to deliver malware and execute attacks through internet. Threat intelligence is the practice of acquiring, gathering, analyzing, and sharing information to manage the cyber security risks. It is one of the best ways to keep an individual or organization safe.

How do you find and interpret threat intelligence data? Read on to understand the essential characteristics of threat intelligence and find out how businesses can use it to gain an advantage over cyber-criminals.

Threat intelligence is a vital component for modern businesses that helps organizations to keep their cyber security in check and understand their vulnerabilities to identify potential threats.

Now, Quick Heal is evolving as a Threat intelligence provider and trying to secure its customers in every possible aspect. Read more to understand the working principle of our Threat Intelligence.

What is
Cyber Threat Intelligence?

Cyber security is one of the hottest topics in the public and private sectors. However, cyber-attacks are becoming more frequent, complex, and sophisticated, and our government and organizations are trying to catch up to these threats via readily- available solutions. The solution emerges as the knowledge of Threat Intelligence, which is evidence-based information about cyber-attacks.

Threat intelligence data is collected, processed, and analyzed to understand what motivates an aggressor's target choice, the level of surveillance done for each target, the type of attack behavior being utilized by the aggressor, and more. This data can then be used to develop policies, countermeasures, and procedures to defend against cyber-attacks. Without threat intelligence, it is impossible to differentiate between real threats and false positives. Our research will look at how to collect, process, and analyze the different data points that define threat intelligence lifecycle.

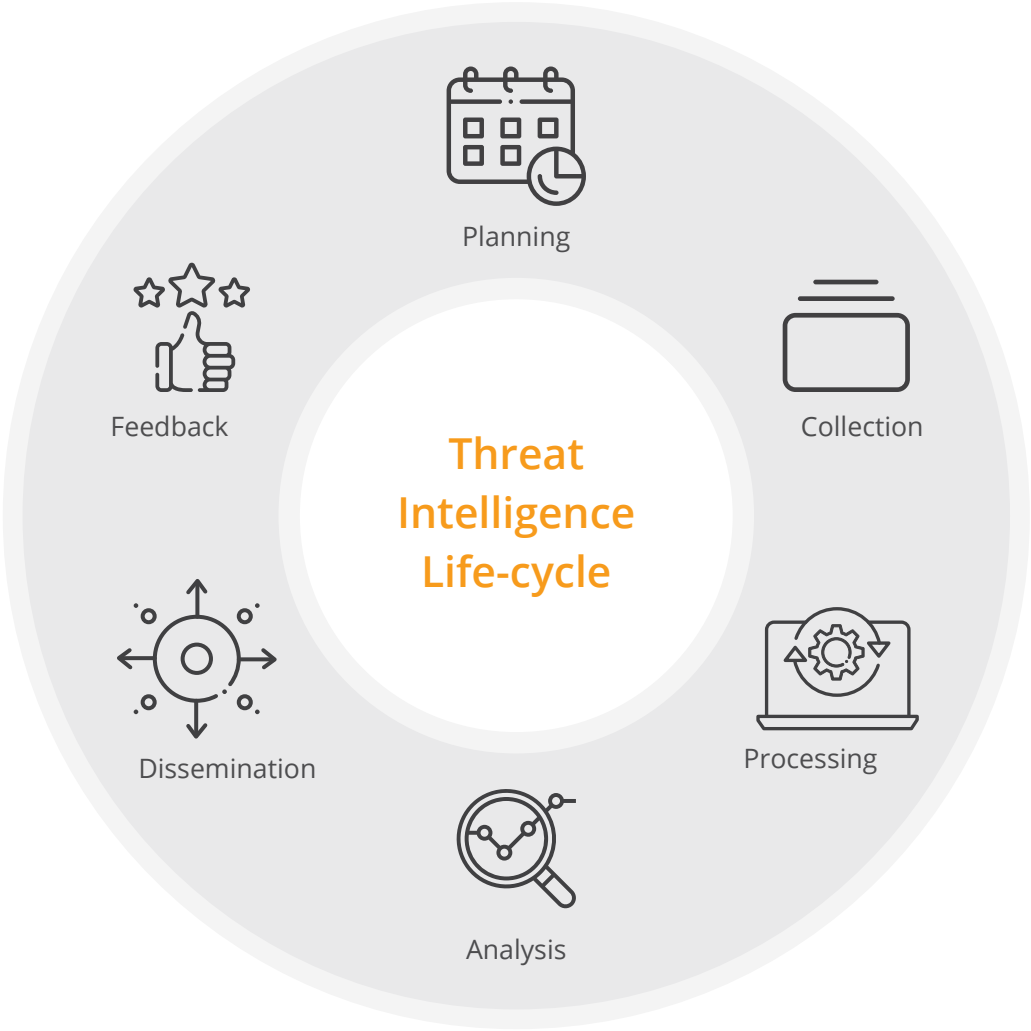


IMAGE 1.0 [Cyber Threat Intelligence Life-cycle]

What is **STIX?**

Structured Threat Information Expression (STIX) is a standardized language and serialization format specific to cyber threats that can be used to exchange intelligence regarding threats as they happen. One of how it's being used involves collecting data related to threats and sending it to those who can help prevent them from making their way onto your systems.

It uses a custom schema to convey data about cybersecurity threats in a way that humans and security technologies can easily understand. STIX is designed for use by organizations, governments, and nonprofit institutions working together on cyber threat information sharing efforts worldwide.

Using STIX makes it a lot easier to share CTI. And why? Because it can be visualized and quickly turned into JSON, making it easy to read by machines and humans. STIX enables you to portray information in a way that is transparent and easy to read and makes the content much more effective. Using STIX visualizes any evidence of cyber-attacks, and using JSON makes it quickly accessible or government agencies.

STIX Structure

- **Architecture**

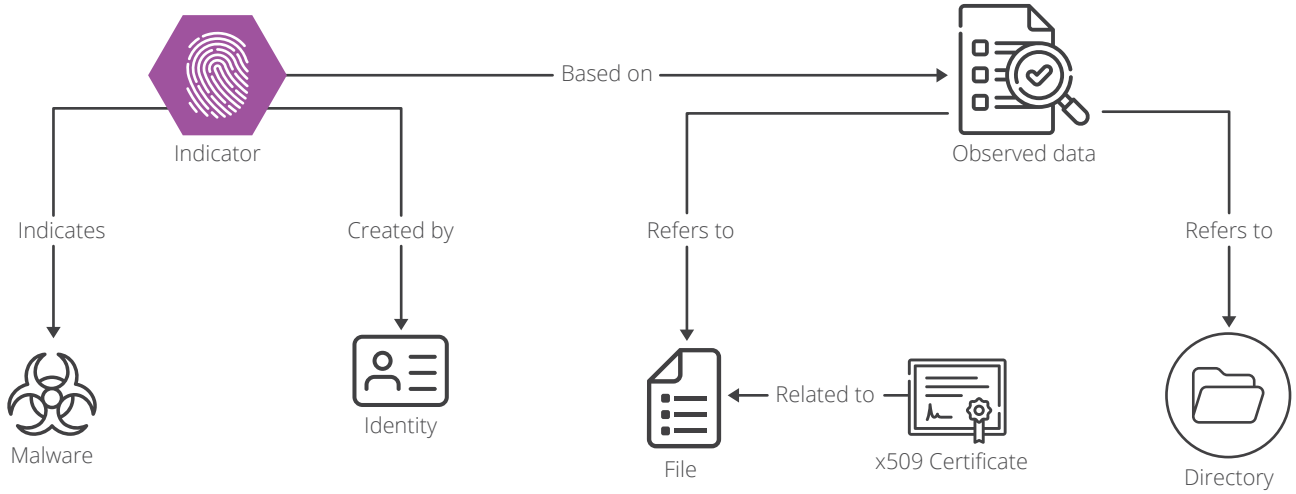


IMAGE 2.0 [STIX Architecture]

- **STIX Domain Objects (SDOs)**

Name	Description
Attack Pattern	Attack Patterns are essential for describing tactics, techniques, and procedures adversaries use to compromise targets.
Campaign	A grouping of malicious activities or attacks that occur over a period of time against a specific set of targets.
Course of Action	A suggestion is made to a consumer on the actions they can take in response to intelligence.
Grouping	Unlike a STIX Bundle, it implicitly communicates that the referenced STIX Objects have a shared context.
Identity	Actual individuals, systems, groups, or organizations. Ex-Quick Heal Technologies.
Indicator	Holds a pattern that can be used to identify suspicious/malicious cyber activity.
Infrastructure	Exemplifies a type of TTP and depicts any systems, software services, hardware, or any associated physical or virtual resources intended to support some purpose.
Intrusion Set	A grouped set of adversarial behaviors and resources with common properties.
Location	Contains geographic properties.
Malware	A type of Tactics, Techniques, and Procedures that show malicious information.
Malware Analysis	A malware instance is composed of metadata and results from a static or dynamic analysis.
Note	Provides additional data that supplies further context or contains information that supports the original STIX Objects and Approved Narrative Content.

Name	Description
Observed Data	Conveys specific information about cyber entities in a standardized format using the STIX Cyber-observable Objects (SCOs).
Opinion	Confirmation of whether or not the information in a STIX Object that was prepared by another entity is correct.
Report	Collection of Relevant information related to threat intelligence focuses on one or more objects like Threat actors, malware, and more.
Threat Actor	Intended Malicious activity performed by actual individuals, groups, or organization.
Tool	Cyber-attacks performed by a threat actor with the help of egitimate tools/software
Vulnerability	An attacker can use a software malfunction to gain access to your system or network.

Table 1.0 [STIX Objects (SDOs)]

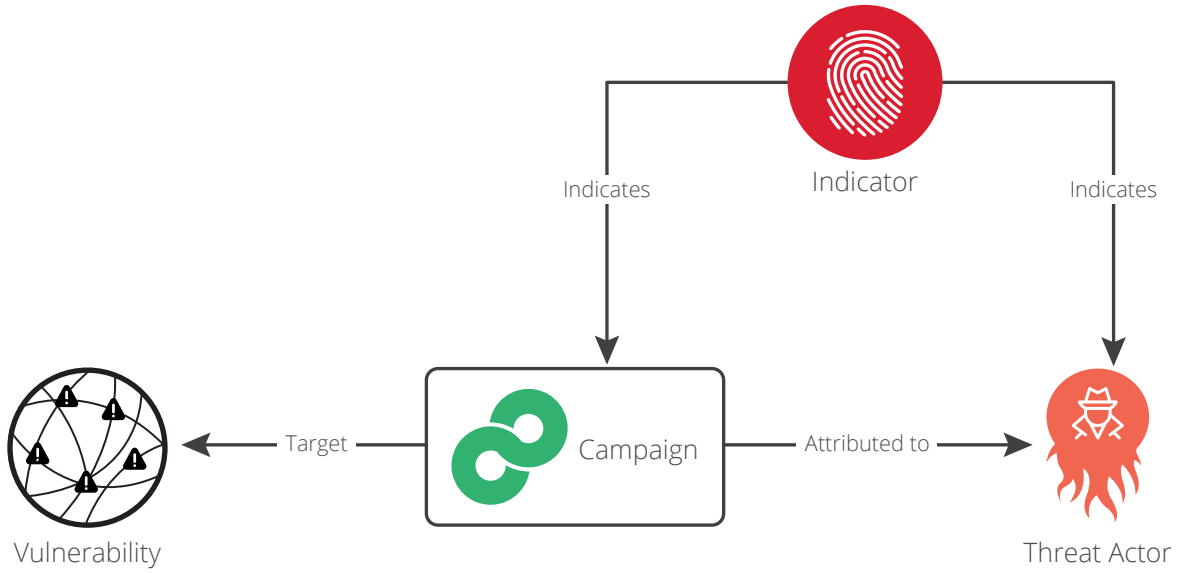

```
{
    "type": "indicator",
    "spec_version": "2.1",
    "id": "indicator--7dd48191-567a-40e5-abb5-1c0b05ea1210",
    "created_by_ref": "identity--bb34042b-f6ab-4d32-81ef-35d936a8c224",
    "created": "2022-04-08T08:46:02.59751Z",
    "modified": "2022-04-08T08:46:02.59751Z",
    "name": "Trojan.Agent",
    "description": "This file hash indicates malware of a Trojan",
    "indicator_types": [
        "Trojan"
    ],
    "pattern": "[file:hashes.'MD5' = '8F8550B49F1A7BE810D25E2E79D727F6']",
    "pattern_type": "stix",
    "pattern_version": "2.1",
    "valid_from": "2022-04-08T08:46:02.59751Z"
},
```


EXAMPLE 1.0 [Indicator JSON Schema]

- **STIX Relationship Objects (SROs)**

Name	Description
Relationship	Used to describe the relationship between two SDOs or SCOs and how they are connected.
Sighting	Affirmative indication of something (malware, indicator, threat actor, etc.) seen in cyber threat intelligence (CTI).

Table 2.0 [Relationship Object (SROs)]



EXAMPLE 2.0 [Relationship Example (SROs)]

STIX
Implementation (Feed Process)

Threat Intel services aggregate raw data from various sources to create actionable information focusing on how threats are identified, discovered, and counteracted by specifically tailored algorithms. The most obvious function of threat intel is to separate the false leads that slow enterprise security teams down daily. They organize the information in such a way that it gives us, their clients, a heads up of what we can expect as well as what security measures need to be taken for that risk in question.

Data

Data refers to information that comes in large amounts. In the world of cyber security, IP addresses, URLs, malware signatures, Hashes, or logs are typical examples. Data by itself is not very useful in most cases and needs to be analyzed properly before it can be used.

Information

Information is made from data that has been put together using a particular procedure. Take, for instance, an aggregated collection of logs relating to suspicious activity that may have occurred across a network.

Intelligence

Intelligence comes from looking at all the information that was gathered. This can be used to inform decision-making. For example, when a new incident report is received, it's collated with prior ones and compared to other incidents that may have had similar activity to alert users if a new attack trend appears.

- **Collection**

  The collection involves bringing together facts and information which support a particular concept or idea. This is typically accomplished by accessing multiple sources within a specific field. As with any collection process, it's essential to identify which sources are likely to produce the desired insights, be reliable, and possibly those that can provide access to the data you seek in a reasonable time frame.

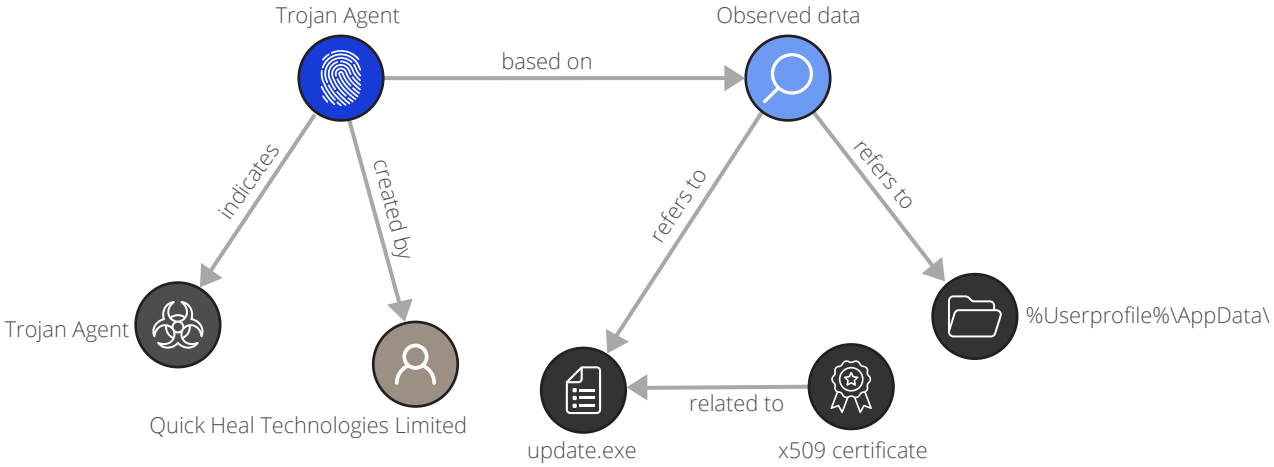
- **Prossessing**

  Analysts use many different techniques to decide what information is most helpful for describing events. Qualitative techniques focus on exploring and understanding the meaning behind certain events or situations, whereas quantitative techniques focus on counting things and taking a more reified stance. Analysts often use various techniques to ensure accurate and unbiased evaluations of which their forecasts and findings are predictive, actionable, and cost-effective. Before intelligence can be extracted from the raw data and used for analysis, researchers must check for the author's credibility and material.

- **Creation**

  Anyone can create the industry standard Threat Intel feeds with the help of processed data and using the STIX standard object. The preferred data used in making the threat feeds are Hash, malware name, malware category, IP address, URLs, Filesize, Directory, Email address, registry information, OS execution information, and many more using different STIX objects.

  Threat Intel feeds are dynamic regarding their Feed Size or contained information also, Threat Intel feeds can be stored in different formats like JSON, XML, etc.



EXAMPLE 3.0 [CTI Graph]

- **Sharing (TAXII)**

  TAXII (Trusted Automated eXchange of Indicator Information) is the primary mode of transport for Cyber threat information, and STIX is the main inform strap-on. TAXII services are automated when individuals want to share cyber threat data securely.

  An organization can also share these Threat Intel feeds by using their own secure platform/product so that consumers can directly use those feeds without any issue.

Quick Heal
Security Simplified

Difference between
Threat Feeds and Threat Intel Feeds

Comprehensive threat feeds are a valuable source of information regarding your adversaries and their capabilities. They are constantly evolving and changing, but they can also be unreliable.

Threat intelligence feeds focus on specific areas of interest for cyber threat response, thus providing actionable threat data related to indicators and artifacts collected from third-party vendors. One example or area of interest could be ordered to find and track botnet activity based on a malicious command and control server's hostname.

Then there are free feeds. These data lists typically come from open sources and can add to the burden of a SOC rather than help reduce it. Often these free threat feeds contain non-prioritized data with no context included, so they're not always the most helpful way to get information.

Free feeds are not always worth your time. They can cost you important resources, fail to provide helpful information to empower you against cyber threats, and lack context that could make a difference within your organization. Despite these shortcomings, free feeds can play a role in threat intelligence, providing raw data and potential leads that might need more research or attention to be meaningful.

Deriving Use Cases from
Threat Information

1. Threat Analysis

As threat intelligence is contextual, it can assist the organization in better defining their risk models and understanding the assumptions, variables, and outcomes. Ensuring that threat actors are identified at the outset and along with their frequency of attacks and exploitable vulnerabilities can help them to assess a better idea of the kind of risks to focus on when it comes to assessing potential threats.

2. Security Operations and Triage

Due to large volume alerts, manually triaging them can be extremely taxing and it is important to detect early threats. With threat intelligence, you can make threat management more efficient than ever by enabling security teams to prioritize or filter out alarms, triage alerts and analyze incidents.

3. Vulnerability Assessment

By taking advantage of threat intelligence tools, security teams can identify vulnerabilities that pose the biggest risks to an organization. They can determine the bigger threats before they steal their customers' valuable information and affect the bottom line. The use of threat intelligence is crucial to ensure the safety and success of companies that can't afford to be put behind in this global competition due to cyber-security issues.

4. Fraud Prevention

It helps prevent data breaches. It also prevents any unauthorized login attempts on your website or mobile app. It also ensures that cybercriminals can’t quickly and illegally impersonate your brand online to defraud your customers. It raises alerts on phishing and typo-squatting domains that cybercriminals often use to run phishing scams, etc.

5. Long term security practice

Threat Intel is more than simply warning of or information about possible impending threats. Threat Intel also consists of longer-term assessments that enable organizations to understand their current and future security landscapes better, assess risk factors, develop mitigation strategies and make investment decisions to strengthen their cybersecurity.

Business Benefits

Quick Heal Threat Intel Feeds can enhance your security shelf:

- Quick Heal's comprehensive Threat Intelligence Feeds protects your infrastructure from malware, phishing attacks and unsafe URLs.
- Malware has been on the rise in recent years, and it continues to get more elaborated, complicated and pervasive; Quick Heal Security Labs detect millions of unique malware samples daily.
- Anti-malware software, IDS/IPS, and ARW are commonly used security measures deployed to protect an organization's endpoints from threats.
- Quick Heal Security Labs, using Threat Intel Feeds from Quick Heal Security Labs, is a solution for governments, telecommunication providers, and other large organizations to block malware at the infrastructure level.

Unique offerings by

Quick Heal TI Feeds

Multi-support feeds/Types of Feeds

1. Malware hash feeds: The distribution of malicious objects can be blocked by recognizing their digital fingerprints based on MD5
2. Malicious and phishing URL feeds Web-based defenses and protection. If a potential malicious URL is seen in traffic, then network-level gateways or firewalls should already have it included in their blacklists
3. IP reputation feeds: To proactively and intelligently assign IP-based policy at the gateway level

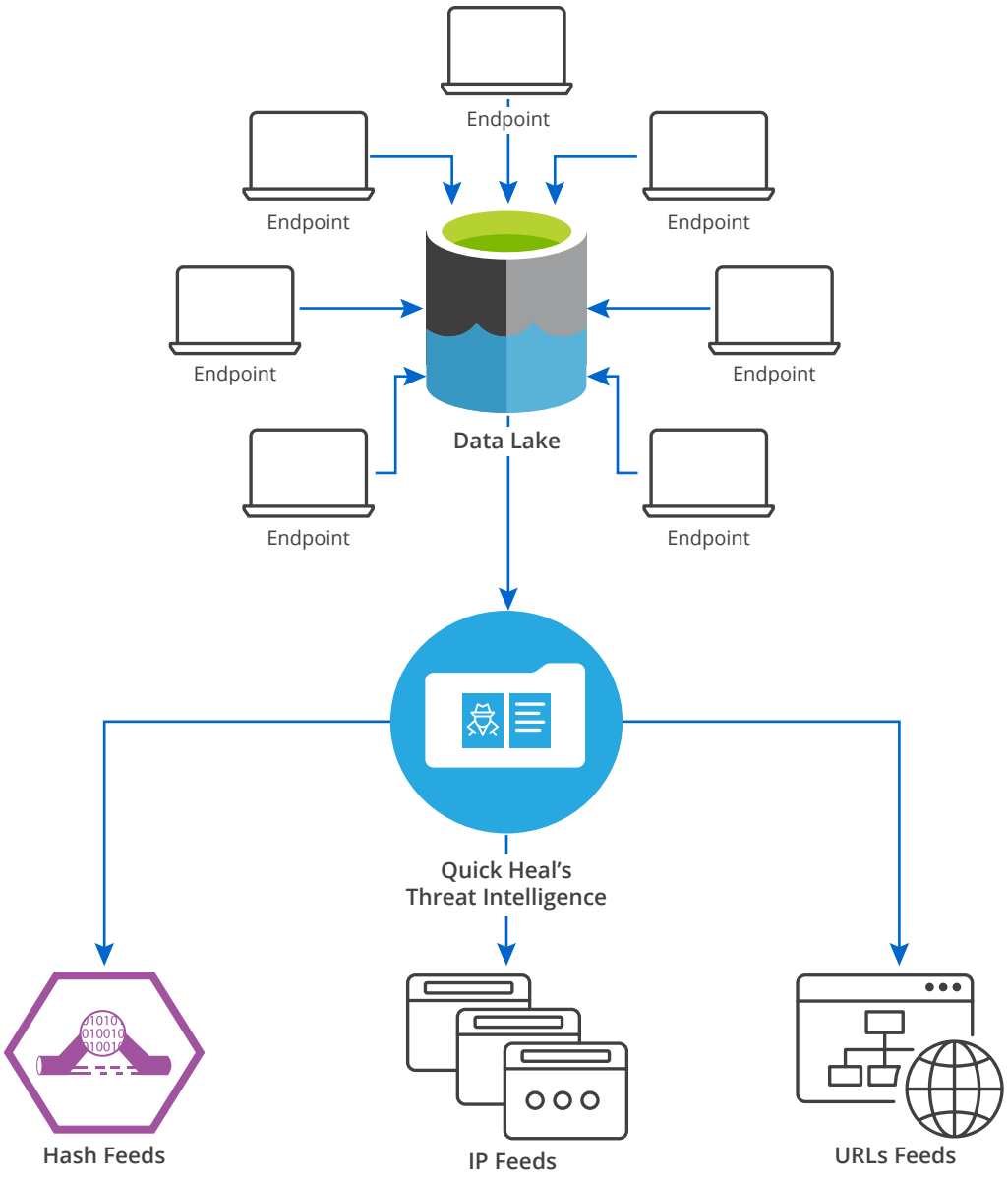


IMAGE 3.0 [QH Threat Intelligence]

Parameter	Description
Data Source	Data gets collected from millions of endpoints
Volume of feeds	Daily, some millions of feeds get added to the database
Update	Feed databases are updated regularly with the latest findings correlated from the sources
File-format	JSON, CSV
Feeds types	It can be a single feed for a single hash OR single feeds for multiple hashes that target specific campaign
Feed Sharing	Supports the TAXII platform, which is one of the reliable and approved channels to share feeds or to share on the user location as needed
Flexibility	Intelligence Feed databases can be integrated into third party cyber-threat intelligence solutions

TABLE 3.0 [Properties of CTI feeds]

Enrichment of
Quick Heal's TI Feeds

Quick Heal's threat intelligence feeds are more enriched than its competitors and provide intelligence feeds from authentic and unique data sources.

- Data sources are from ~8million active endpoints around the globe
- The number of malicious activities is increasing day by day
- Feeds are being created with STIX industry standard
- The size of a single feed is around 6KB and stored in a STIX supported JSON format
- Quick Heal also provides an archive for all the feeds which have been created for the particular day
- Active monitoring of malicious activity is done at our security lab
- Data is processed on a daily basis; at the end of the day, our threat intelligence can create a huge number of intelligence feeds that contain-

Types of feeds	Number of feeds/daily
Hash feeds	~6 Lakh
URL feeds	~2.5 Lakh
IP feeds	~6 Lakh

Conclusion

Threat intelligence feeds are a specific application of technology that can provide you with access to real-time information about threats, vulnerabilities, and exploits. Threat intelligence feeds can be tech-driven or updated manually. Reviewing threat intelligence feeds can be done in person or by implementing automated software systems to help you review it on an ongoing basis as new content is released.

There are many kinds of threat intelligence feeds. Each has a different purpose and covers information, data about existing potential risks or threats. Threat intelligence feeds typically provide context about the risk so that others can act on it appropriately.

Analysts can have so many different sources of information about the same subject that is easy for them to get overwhelmed. Sometimes all these threats and attack reports can blend and make it challenging to identify which ones are relevant and new. Having too much information to manage is almost as bad as having too little. Unless there is a way to filter out some of the unnecessary scenarios, your organization is not able to protect itself as it should do against cyber threats.

Quick heal has initiated and is continuously working toward Threat Intelligence to ensure their each user and partner are secured in every possible way.

References

https://oasis-open.github.io/cti-documentation/

https://oasis-open.github.io/cti-documentation/stix/intro

https://oasis-open.github.io/cti-documentation/taxii/intro.html

https://en.wikipedia.org/wiki/Threat_intelligence

Cyber Observable eXpression (CybOX). URL https://cybox.mitre.org

https://ieeexplore.ieee.org/abstract/document/7568916

Quick Heal

Security Simplified

Quick Heal Technologies Ltd.
Marvel Edge, Office No. 7010 C & D, 7th Floor, Viman Nagar, Pune,
Maharashtra, India - 411014.
Phone: 1800 212 7377 | info@quickheal.co.in | www.quickheal.com