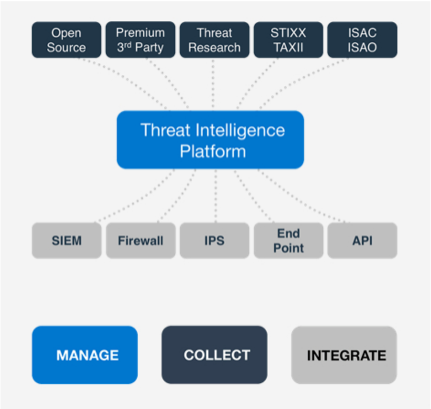
# Threat Intelligence Platforms

This lesson is going to cover what Threat Intelligence Platforms (TIPs) are, why they're used, and provide some examples of TIPs that are used in industry including; MISP, ThreatConnect, ThreatQ, Lookingglass, Intsights, Anomali. We will also talk about how threat feeds can be aggregated into Threat Intelligence Platforms, allowing organizations to create threat intelligence repositories, full of malicious indicators, and indicators of compromise.

## WHAT ARE TIPS?

Threat Intelligence Platforms can be deployed as Software-as-a-Service or an on-premises solution to effectively manage a large volume of cyber threat intelligence, such as; actors, campaigns, signatures, bulletins, and Tools, Techniques, and Procedures (TTPs). TIPs are designed to provide the following functionality for security teams:

1. Aggregation and normalization of intelligence collected from multiple sources.
2. Integrate with existing security controls such as firewalls and intrusion prevention systems.
3. Analysis and sharing of threat intelligence.



*Source: Anomali*

The above diagram from Anomali clearly shows how TIPs work to collect intelligence, and distribute it to security tools, such as firewalls, intrusion prevention systems, and endpoint protection controls.

## WHY USE A TIP?

Simply put, a Threat Intelligence Platform allows an organization to store everything related to threat intelligence in one single location. Whether it's technical indicators of compromise or high-level awareness reports, TIPs provide a solid foundation for any cyber threat intelligence function. Anomali have defined three main groups that will benefit from the implementation of a TIP:

### Security Operations Center (SOC) Teams

- These teams are focused on operational day to day tasks and responding to threats as they occur. A TIP provides automation for routine activities such as integrations, enrichment, and scoring.

### Threat Intelligence Teams

- These teams look to make predictions based on associations and contextual information between actors, campaigns, etc. A TIP provides them with a "library" of information that simplifies and streamlines this process.

### Management and Executive Teams

- A TIP provides management with a single platform through which to view reports at both technical and high levels. This enables them to effectively share and analyze data as incidents occur.

## DATA AGGREGATION

A Threat Intelligence Platform automatically collects and reconciles data from various sources and formats. Ingesting information from a variety of sources is a critical component to a strong security infrastructure. Supported sources and formats include:

**Sources:**

- Open source
- 3rd party paid
- Government
- Trusted Sharing Communities (ISACs)
- Internal

**Formats:**

- STIX/TAXII
- JSON and XML
- Email
- .csv, .txt, PDF, Word document

## TIP PRODUCTS

There are numerous Threat Intelligence Platform products in the industry. Let's briefly take a look at some of them and their features.

## Malware Information Sharing Platform (MISP)

**Website:** https://www.misp-project.org/

MISP is an open-source, community-ran project, developed and maintained by an awesome group of volunteers. MISP is used by over 6000 organizations around the world, and has been designed to be as simple as possible, making it accessible and usable. MISP offers an absolute ton of features providing extended functionality for multiple use-cases, including the ability to easily share intelligence with fellow humans, and even automated defenses.

## ThreatConnect

**Website:** https://threatconnect.com/solution/threat-intelligence-platform/

ThreatConnect have produced their own Threat Intelligence Platform that can completely automate the intelligence collection process, regardless of the source format. Whether it's an email, RSS feed, or blog, ThreatConnect can ingest it and store the intelligence within the TIP. ThreatConnect also provides automation in the form of runbooks, allowing human analysts to determine what actions should be taken under specific circumstances.

## Anomali

**Website:** https://www.anomali.com/

The TIP produced and maintained by Anomali is utilized by many different Information Sharing and Analysis Centers including the Financial Services Information Sharing and Analysis Center (FS-ISAC). Anomali offers the ability for an organization to quickly and easily create their own ISAC, allowing other organizations to partner together and share intelligence together. The website also offers an "app store" where organizations can purchase integrations and threat feeds to boost the capabilities or the TIP and other security controls utilized by the organization.

## ThreatQ

**Website:** https://www.threatq.com/threat-intelligence-platform/

The ThreatQ platform is based on a threat-centric approach to security operations, allowing security teams to "prioritize based on threat and risk, collaborate across teams, automate actions and workflows and integrate point products into a single security infrastructure". ThreatQ also states that it can do more than a typical TIP, and can assist with security practices such as Vulnerability Management, Spear Phishing, Incident Response, and Threat Hunting.

In the next lesson, we're going to cover the open-source TIP, Malware Information Sharing Platform in more detail, and show you how to setup your own local instance of MISP! We have decided to use this TIP for demonstration and exercise purposes as it is relatively simple to setup, and is open-source, meaning that it is accessible for all of our BTL1 students. Having the practical ability to setup a TIP will really set you apart from other threat intelligence analysts, whether you're already in the security industry, or trying to land your first role.

‹ Previous Topic     Mark Complete ✓     Next Topic ›
Back to Lesson