

Blue Team Level 1 Certification  
(Standard)

## Introduction to BTL1

✓ Welcome to Blue Team Level 1

● 4 Topics

✓ Lab and Forum Access

## SECURITY FUNDAMENTALS DOMAIN

✓ Introduction to Security Fundamentals

● 1 Topic

✓ Soft Skills

● 7 Topics

✓ Security Controls

● 5 Topics 1 Quiz

✓ Networking 101

● 6 Topics 1 Quiz

✓ Management Principles

● 4 Topics 1 Quiz

## PHISHING ANALYSIS DOMAIN

✓ PA1) Introduction to Emails and Phishing

● 7 Topics 1 Quiz

✓ PA2) Types of Phishing Emails

● 10 Topics 2 Quizzes

✓ PA3) Tactics and Techniques Used

● 12 Topics 2 Quizzes

✓ PA4) Investigating a Phishing Email

● 8 Topics 2 Quizzes

✓ PA5) Analysing URLs, Attachments, and Artifacts

● 8 Topics 1 Quiz

○ PA6) Taking Defensive Actions

● 12 Topics 1 Quiz

○ PA7) Report Writing

● 7 Topics 1 Quiz

○ PA8) Phishing Response Challenge

● 3 Topics 1 Quiz

## THREAT INTELLIGENCE DOMAIN

○ TI1) Introduction to Threat Intelligence

● 7 Topics

○ TI2) Threat Actors &amp; APTs

● 6 Topics 2 Quizzes

○ TI3) Operational Threat Intelligence

● 7 Topics 1 Quiz

○ **TI4) Tactical Threat Intelligence**

● 7 Topics 1 Quiz

○ Section Introduction, Tactical Intelligence

○ Threat Exposure Checks Explained

○ Watchlists/IOC Monitoring

○ Public Exposure Checks Explained

○ **Threat Intelligence Platforms**

○ Malware Information Sharing Platform (MISP)

○ Activity) Deploying MISP

□ Activity) End of Section Review, Tactical Intelligence

# Threat Intelligence Platforms

Blue Team Level 1 Certification (Standard) &gt; TI4) Tactical Threat Intelligence &gt; Threat Intelligen...

IN PROGRESS



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, Intsigths, 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:

<input type="radio"/> TI5) Strategic Threat Intelligence
● 5 Topics 1 Quiz
<input type="radio"/> TI6) Malware and Global Campaigns
● 6 Topics 1 Quiz
<b>DIGITAL FORENSICS DOMAIN</b>
<input type="radio"/> DF1) Introduction to Digital Forensics
● 5 Topics
<input type="radio"/> DF2) Forensics Fundamentals
● 10 Topics 5 Quizzes
<input type="radio"/> DF3) Digital Evidence Collection
● 8 Topics 1 Quiz
<input type="radio"/> DF4) Windows Investigations
● 3 Topics 3 Quizzes
<input type="radio"/> DF5) Linux Investigations
● 4 Topics 2 Quizzes
<input type="radio"/> DF6) Volatility
● 3 Topics 1 Quiz
<input type="radio"/> DF7) Autopsy
● 4 Topics 1 Quiz
<b>SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN</b>
<input type="radio"/> SI1) Introduction to SIEM
● 7 Topics 1 Quiz
<input type="radio"/> SI2) Logging
● 6 Topics 2 Quizzes
<input type="radio"/> SI3) Aggregation
● 2 Topics 1 Quiz
<input type="radio"/> SI4) Correlation
● 6 Topics 1 Quiz
<input type="radio"/> SI5) Using Splunk
● 5 Topics 2 Quizzes
<b>INCIDENT RESPONSE DOMAIN</b>
<input type="radio"/> IR1) Introduction to Incident Response
● 8 Topics 1 Quiz
<input type="radio"/> IR2) Preparation Phase
● 10 Topics 2 Quizzes
<input type="radio"/> IR3) Detection and Analysis Phase
● 7 Topics 4 Quizzes
<input type="radio"/> IR4) Containment, Eradication, and Recovery Phase
● 5 Topics 1 Quiz
<input type="radio"/> IR5) Lessons Learned and Reporting
● 7 Topics
<input type="radio"/> IR6) MITRE ATT&CK
● 13 Topics 2 Quizzes
<b>BTL1 EXAM</b>
<input type="radio"/> Exam Preparation
<input type="radio"/> Using RDP and SSH
<input type="radio"/> How to Start Your Exam

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

## 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 of 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 ✓](#)[Back to Lesson](#)[Next Topic >](#)[Privacy & Cookies Policy](#)