

**Blue Team Level 1 Certification
(Standard)**

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

9 Topics 1 Quiz

THREAT INTELLIGENCE DOMAIN☐ TI1) Introduction to Threat Intelligence

7 Topics

☐ TI2) Threat Actors & 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☐ TI5) Strategic Threat Intelligence

5 Topics 1 Quiz

☐ TI6) Malware and Global Campaigns

6 Topics 1 Quiz

DIGITAL FORENSICS DOMAIN☐ DF1) Introduction to Digital Forensics

5 Topics

☐ DF2) Forensics Fundamentals

Section Introduction, Tactical Intelligence

Blue Team Level 1 Certification (Standard) > TI4) Tactical Threat Intelligence > Section Introd...

IN PROGRESS

Threat Intelligence SECTION INTRODUCTION



This section of the Threat Intelligence domain will focus on tactical intelligence roles and responsibilities. A typical day in the life as a Cyber Threat Intelligence Analyst focusing on tactical intelligence typically involves performing threat exposure checks to see if malicious indicators have been identified within the environment, conducting public exposure assessments to see how what information about the company and it's employees is freely available online, and if that could be exploited in any way, and collecting and using actionable intelligence to improve defenses by implementing threat feeds to power automated defenses and provide context to security investigations.

LEARNING OBJECTIVES

By the end of this section you will have achieved the following objectives:

- Understand how threat exposure checks are conducted to identify the presence of indicators of compromise.
- Understand how organizations can monitor for IOCs using SIEM, EDR, and IDS systems to alert for positive matches.
- Understand what public exposure assessments are and why they can be valuable to defenders and attackers.
- Understand how information can be collected from open and dark-web sources and the legal constraints of this activity.
- Understand what MISP is, why it's used, and how to deploy it.

[< Previous Lesson](#)[Mark Complete ✓](#)[Back to Lesson](#)[Next Topic >](#)