Blue Team Level 1 Certification (Standard)
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 & APTs
6 Topics | 2 Quizzes
Section Introduction, Actors
Common Threat Agents
Motivations
Actor Naming Conventions
What are APTs?
Tools, Techniques, Procedures
Activity) Threat Actor Research
Activity) End of Section Review, Actors
TI3) Operational Threat Intelligence
7 Topics | 1 Quiz
TI4) Tactical Threat Intelligence

Section Introduction, Actors

This section of the Threat Intelligence domain will introduce you to malicious actors, what they are, how they operate, and why they conduct cyberattacks. We will cover aspects such as naming conventions, motivations, and common targets for different groups.

LEARNING OBJECTIVES

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

- Understand different malicious actors and the categories they are typically placed into.
- Understand the different naming conventions used, and why they're used.
- Understand the common motivations for cyberattacks and operations.
- Understand the common targets for different malicious actor categories, and how these align with their motivations.