

Blue Team Level 1 Certification  
(Standard)

4 Topics

☒ Lab and Forum Access

## SECURITY FUNDAMENTALS DOMAIN

☒ Introduction to Security Fundamentals

1 Topic

☒ Blue Team Roles☒ 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 & APTs

6 Topics | 2 Quizzes

☐ TI3) Operational Threat Intelligence

7 Topics | 1 Quiz

# Introduction to Security Fundamentals

Blue Team Level 1 Certification (Standard) &gt; Introduction to Security Fundamentals

COMPLETE



Welcome to the first domain in the Blue Team Level 1 (BTL1) training course! This section is designed for individuals that have little experience or knowledge in cybersecurity, and will provide a foundational understanding so that the rest of the course can build upon it. If you already work in the industry, you will get through this section really quickly, but we still highly recommend reading all of the material and attempting the activities.

The Security Fundamentals domain covers the following:

- **Soft Skills** – Soft skills are extremely important to make you more employable and ensure you can effectively work in a team, communicate with stakeholders, and enjoy your time working in this field.
- **Networking 101** – Having knowledge of how systems communicate and IT infrastructure is important for most cybersecurity roles, especially technical positions such as a SOC analyst or incident responder. This section is designed to give a brief introduction into networking, with further reading material for students that want to learn more.
- **Security Controls** – This part of the domain will cover technical, administrative and physical security defences, from firewalls to security guards, learn how organisations defend themselves from cyber threats and physical intruders!
- **Management Principles** – Learn about important management topics of cybersecurity, covering risk, policies and procedures, and compliance. While these topics may seem dry, they are really important when working with information security management systems.

## Lesson Content

100% Complete | 1/1 Steps

☒ Blue Team Roles[< Previous Lesson](#)[Back to Course](#)[Next Lesson >](#)