

Blue Team Level 1 Certification
(Standard)

7 Topics

Security Controls

5 Topics | 1 Quiz

Section Introduction, Security Controls

Physical Security

Network Security

Endpoint Security

Email Security

Activity: End-of-Section Review, Security Controls

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

TI4) Tactical Threat Intelligence

7 Topics | 2 Quizzes

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

Section Introduction, Security Controls

Blue Team Level 1 Certification (Standard) > Security Controls > Section Introduction, Security Co...

COMPLETE

Security Fundamentals SECTION INTRODUCTION



This section of the Security Fundamentals domain will briefly cover security controls, as they will be covered in greater detail throughout the course. We will take a look at the following:

- **Physical Security Controls** (Deterrents, access controls, monitoring controls)
- **Network Security Controls** (Firewalls, NIPS, NIDS, SIEM, NAC)
- **Endpoint Security Controls** (HIPS, HIDS, EDR, Anti-Virus, SIEM)
- **Email Security Controls** (Spam filters, DLP, email scanning)

Although this lesson is looking at security controls grouped by where they are deployed (such as endpoints vs email systems), security controls are actually categorized into the below three groups. We have included a few examples in each.



TECHNICAL CONTROLS

- Firewalls
- Intrusion Prevention Systems
- Anti-Virus
- Endpoint Detection and Response



ADMINISTRATIVE CONTROLS

- Security Awareness Training
- Organisational Policies
- Disciplinary Programs



PHYSICAL CONTROLS

- Security Guards
- Perimeter Fencing
- Security Checkpoints
- CCTV and Lighting

LEARNING OBJECTIVES

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

- Understand the basics of physical, network, host, and email security technologies.
- Explain what the different security controls do to reduce risk and protect the organization.
- Build a foundation of security controls that will be developed throughout the course.

5 Topics

DF2) Forensics Fundamentals

10 Topics 5 Quizzes

Previous Lesson

Next Lesson

Next topic

Privacy & Cookies Policy

