Blue Team Level 1 Certification (Standard)

~~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
~~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

Activity) End of Section Review, Security Controls

Congratulations on completing this section of the Security Fundamentals domain! This knowledge review is designed to test what you have learned about common security controls that are deployed on-premises, on systems, and inside the private network to mitigate cyber risk. You will be able to re-take the quiz as many times as you like but will need a score of 70% or above to pass. It is important that you feel confident in answering these questions to ensure that you can complete tasks within the BTL1 exam and pass to become certified. If you get stuck, use the **Hint** feature!

Good luck!

KNOWLEDGE REVIEW

[1/6] Match the security controls with the appropriate descriptions.

Sort elements

- Uses blacklists and reputation checks to stop unwanted emails being delivered to employee mailboxes.
- A technical control that can restrict the traffic coming in and going out of it and generate logs about network activity.
- Reacts to unusual or malicious system activity and generates alerts.
- Takes automated actions to react to unusual or malicious network activity.
- Can use infrared to detect the presence of a human passing in front of a sensor.

Firewall	
Spam Filter	
NIPS	
HIDS	
Motion Detector	

Check