

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

☐ Section Introduction, Report Writing☐ Email Header, Artifacts, and Body Content☐ Analysis Process, Tools, and Results☐ Defensive Measures Taken☐ Artifact Sanitization☐ Activity) Report Writing Exercise☐ Activity Cont.) Report Writing Exercise Answers☒ Activity) End of Section Review, Report Writing☐ 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 1 Quiz

☐ TI5) Strategic Threat Intelligence

5 Topics 1 Quiz

☐ TI6) Malware and Global Campaigns

6 Topics 1 Quiz

**DIGITAL FORENSICS DOMAIN**

# Activity) End of Section Review, Report Writing

Blue Team Level 1 Certification (Standard) &gt; PA7) Report Writing &gt; Activity) End of Section Review, Report Writi...

## Phishing Analysis END OF SECTION REVIEW



Congratulations on completing this section of the Phishing Analysis domain! This knowledge review is designed to test what you have learned regarding writing investigation reports for phishing attacks and campaigns. 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 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

Which report section is often the longest, and contains the most detail?

- ☐ Email Artifacts & Description
- ☐ Users Affected & Actions Taken to Notify
- ☐ Artifact Analysis, Tools, and Process
- ☐ Defensive Measures Taken

**Check**

Privacy &amp; Cookies Policy

