Blue Team Level 1 Certification (Standard) ‹

● 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

○ DF1) Introduction to Digital Forensics

● 5 Topics

○ DF2) Forensics Fundamentals

● 10 Topics | 5 Quizzes

○ DF3) Digital Evidence Collection

● 8 Topics | 1 Quiz

○ DF4) Windows Investigations

● 3 Topics | 3 Quizzes

○ DF5) Linux Investigations

● 4 Topics | 2 Quizzes

○ DF6) Volatility

● 3 Topics | 1 Quiz

○ DF7) Autopsy

● 4 Topics | 1 Quiz

SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN

○ SI1) Introduction to SIEM

● 7 Topics | 1 Quiz

Activity) Report Writing Exercise

Blue Team Level 1 Certification (Standard) > PA7) Report Writing > Activity) Report Writing Exe... IN PROGRESS

This activity is designed to test and improve your ability to write phishing reports which are a crucial part of phishing analysis when working for organizations. A good report is the difference between a good security analyst and a great security analyst. You need to be able to clearly and concisely get across information from the observed attack, how you analyzed the email and artifacts, and the actions you have taken or want to take in order to protect the organization.

CHALLENGE BRIEF

A fellow security analyst began investigating a phishing email but has had to stop and join an incident response team with a potential system compromise, so they have passed over their rough notes to you. Whilst the investigating analyst had almost completed their assessment, they didn't have time to write up their report and select appropriate defensive measures. Using the analyst's notes you need to take over their investigation and write a full report detailing the actions that they took in a neat and presentable format, and suggest defensive measures that would best protect the company. **The initial analyst has mentioned that you should just keep the case for yourself, and talk as if you have completed the actions instead of referring to him throughout the report.** Below you can download the analyst's rough notes. Use the skills you've learned throughout this section of the course to write a report. We have included a basic report template to help you format your report.

Download Analyst's Notes & Report Template

Your report should include the following sections:

1. Email description and a list of email, web, and file artifacts.
2. Analysis of artifacts.
3. Suggested defensive measures.

Due to the volume of BTL1 students, we are currently unable to provide hand-marked results for this activity. In the next lesson, we have written our own report based on the below challenge brief so that you can compare it with the report you have produced. While it would be possible to skip this activity, **we strongly suggest** you take it seriously, as this will help you a lot during phishing analysis tasks within the BTL1 practical exam and secure you points so you can become certified.

‹ Previous Topic

Mark Complete ✓

Next Topic ›

Back to Lesson