

Blue Team Level 1 Certification
(Standard)

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

Section Introduction, Actors

Common Threat Agents

Motivations

Actor Naming Conventions

What are APTs?

Tools, Techniques, Procedures

Activity) Threat Actor Research

Activity) End of Section Review, Actors

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

Activity) Threat Actor Research

Blue Team Level 1 Certification (Standard) > TI2) Threat Actors & APTs > Activity) Threat Actor Research



In this activity you will be using free intelligence sources to collect information on an advanced persistent threat (APT). This exercise is designed to develop your ability to complete research tasks and increase your understanding of APT groups and how they operate, by investigating associated tactics, techniques and procedures (TTPs) and motives behind their cyber operations.

CHALLENGE SCENARIO

You have joined a financial institution in Eastern Europe as a Junior Threat Intelligence Analyst, and to test your knowledge of APTs and your ability to manage research projects, you have been assigned to collect information on the threat group "APT41," which are known to target organizations operating in this industry. Below are two important resources, but you should still look to find additional sources of your own:

- MITRE Groups Page
- FireEye Report on APT41

Don't forget to check multiple sources to ensure that you're submitting the right answer!

CHALLENGE SUBMISSION

[1/10] What other name is APT41 known as, that features an animal?

Check

Privacy & Cookies Policy

