Blue Team Level 1 Certification (Standard)

Introduction to BTL1

- Welcome to Blue Team Level 1!
  - 4 Topics
  - Boring Legal Stuff
  - Course Overview
  - Navigating the Course
  - Credits & Special Mentions
- Lab and Forum Access

SECURITY FUNDAMENTALS DOMAIN

- Introduction to Security Fundamentals
  - 1 Topic
- Soft Skills
  - 7 Topics
- Security Controls
  - 5 Topics | 1 Quiz
- 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

Course Overview

Welcome to the BTL1 training course, it's great to have you here! You've just begun your journey to become Blue Team Level 1 (BTL1) certified, an achievement that showcases your practical ability to defend networks from cyber threats. The next few lessons will introduce you to our learning environment, as well as BTL1's content and exam to get you ready to begin training.

Our course covers 5 technical domains, which are as follows:

PHISHING ANALYSIS

You will learn about different phishing and related social engineering attacks, how to identify phishing emails, collecting artefacts and indicators of compromise via both manual and automated methods, determine the risk of attachments and hyperlinks, suggest appropriate defensive measures (both preventative and reactive), and write consistently clear and useful reports regarding the observed attack.

THREAT INTELLIGENCE

In this domain you will learn about intelligence, the different types, and the benefits that threat intelligence has in the fight against cybercrime. Actionable intelligence can help security professionals to implement stronger defences, and understand the threat actors that may target different organisations. We will cover indicators of compromise (IOCs), tools, techniques and procedures (TTPs), and precursors, all of which give information throughout the entire attack lifecycle.

DIGITAL FORENSICS

In this highly technical domain, you will be taught how to conduct forensic investigations by collecting artefacts from Windows and Linux-based operating systems, as well as browser forensics. The techniques taught will reflect real-world practices and covers how to ensure evidence is maintained with strict integrity so it can be submitted as evidence in court as part of legal proceedings.

SIEM INFRASTRUCTURE & ANALYSIS

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
SI2) Logging
6 Topics | 2 Quizzes
SI3) Aggregation
2 Topics | 1 Quiz
SI4) Correlation
6 Topics | 1 Quiz
SI5) Using Splunk
5 Topics | 2 Quizzes
INCIDENT RESPONSE DOMAIN
IR1) Introduction to Incident Response
8 Topics | 1 Quiz
IR2) Preparation Phase
10 Topics | 3 Quizzes
IR3) Detection and Analysis Phase
7 Topics | 5 Quizzes
IR4) Containment, Eradication, and Recovery

This domain covers what security information and event management is, how logging, aggregation and correlation works, and provides hands-on activities where you'll use SIEM for analysis in order to respond to a range of common cyber attacks that defenders deal with on a daily basis. You will become familiar with different log types, how to setup logging, the architecture of SIEM platforms, performing searches within a SIEM platform, and reporting on observed activity from a range of sources.

INCIDENT RESPONSE

You will learn all the stages of incident response under the NIST SP 800 61r2 framework:

- **Preparation** – Implementing network defences, policies, procedures, and the need for an incident response team with sufficient resources.
- **Detection & Analysis** – How to distinguish malicious activity from normal activity, and confirm the existence of a security incident so that appropriate individuals can begin to monitor and analyse the situation.
- **Containment, Eradication, Recovery** – Learning how to stop an incident from spreading, removing any malicious artefacts so that an attacker can no longer gain access to compromised systems, and working to fix any security flaws that were exploited or discovered as a result of the breach.
- **Post-Incident Activity** – Reflecting on the incident and learning from any strengths and weaknesses that were presented, so that a similar event doesn't occur in the future, or the team is better equipped and trained to respond.

ADDITIONAL INFORMATION

We also have a domain that covers security basics, called 'Security Fundamentals'. If you already have some experience in cybersecurity, then you'll fly through this section. If you're completely new, then this domain will give you a foundation for the rest of the training, and covers areas such as security systems, management principles, soft skills, and more.

Once you have completed the training course and feel confident, you are able to start your online exam and attempt to become BTL1 certified! ***Please note: You do not need 100% course completion to start the exam, this is just to help you keep track of what material you have covered.***

Previous Topic
Back to Lesson
Next Topic

Privacy & Cookies Policy
Privacy - Terms