

Updated on September 11, 2026

Sign Up

TryHackMe SEC1 Certification Training

3 days (21 hours)

Overview

The TryHackMe SEC1 Certification Training prepares you for the official Cyber Security 101 (SEC1) certification, a practical validation of cybersecurity fundamentals. You'll learn to analyze, investigate, and secure simulated environments through hands-on labs based on real-world scenarios.

This course allows you to methodically prepare for the Cyber Security 101 (SEC1) exam, which is designed to assess practical skills rather than simply testing knowledge recall. You will cover the fundamentals of systems, networks, offensive security, and defensive security.

You will learn to use the command line in Linux and Windows, interpret network traffic, identify web vulnerabilities, and understand the mechanisms for protecting identities, passwords, and workstations.

The preparation also covers log analysis, SOC monitoring principles, incident response, an introduction to malware analysis, and essential diagnostic tools. Each concept is applied in progressive scenarios that closely mimic the certification format.

Upon completion of the training, you will be able to approach the practical exam with a clear methodology, solve technical tasks in a controlled environment, and demonstrate the fundamental skills validated by the Cyber Security 101 (SEC1) certification.

Like all our training courses, this one will introduce you to **the latest stable version** of the technology and its new features.

Objectives

- Understand the scope and process of the Cyber Security 101 (SEC1) certification
- Use essential commands in Linux and Windows
- Analyze key network protocols, packets, and security logs
- Identify web vulnerabilities and apply a structured testing approach
- Perform the fundamental steps of incident investigation, detection, and response
- Prepare to solve practical scenarios in the TryHackMe environment

Target Audience

- Junior Cybersecurity Analyst
- Junior SOC Analyst
- Junior system administrator
- IT Support Technician
- Cybersecurity Student

Prerequisites

- Basic knowledge of workstations and operating systems
- Basic understanding of TCP/IP networks and IP addressing
- Familiarity with web browsing and file management
- Basic familiarity with the Linux or Windows command line

Technical Prerequisites

- Computer running Windows 10 or later, macOS, or a recent Linux distribution
- Up-to-date Google Chrome or Mozilla Firefox browser
- Stable internet connection allowing access to online labs without any security filters blocking access
- Active TryHackMe personal account
- Monitor with a minimum resolution of 1366 x 768; 8 GB of RAM recommended

TryHackMe SEC1 Training Curriculum

[Day 1 - Morning]

Understanding the Certification and Cybersecurity Fundamentals

- Introduction to the Cyber Security 101 (SEC1) certification, its entry-level status, and the skills it assesses
- Overview of the hands-on format: scenarios, technical tasks, related questions, and managing the exam window
- Overview of roles, Red Team and Blue Team roles, and investigation workflows
- Review of operating systems, files, processes, users, and permissions

- Getting started with the TryHackMe lab environment and the methodology for solving a task
- Hands-on workshop: exploring a guided lab, identifying system components, and gathering initial useful information

[Day 1 – Afternoon]

Systems, command line, and access management

- Linux Fundamentals: Directory structure, navigation, file search, and permissions
- Windows Fundamentals: Accounts, Services, File System, and Common Commands
- Progressive use of shells, redirection, and query commands
- Understanding users, groups, privileges, and authentication mechanisms
- Best practices for collecting technical evidence and formulating an accurate response during an examination
- Hands-on workshop: conducting a guided investigation on Linux and Windows to retrieve information, accounts, and access rights

[Day 2 - Morning]

Networks and Traffic Analysis

- Review of TCP/IP concepts, addressing, ports, services, and network traffic
- Reading common protocols: DNS, HTTP, HTTPS, SSH, and SMB
- Network security principles: segmentation, filtering, encryption, and secure protocols
- Introduction to packet capture and analysis using Wireshark and tcpdump
- Exploring service discovery with Nmap in a controlled environment
- Hands-on workshop: Analyzing a network capture, identifying exposed services, and detecting abnormal traffic

[Day 2 - Afternoon]

Cryptography, Passwords, and Web Security

- Understanding the roles of encryption, hashing, keys, and certificates
- Distinguishing between authentication, authorization, session management, and credential protection
- Identify dictionary and brute-force attacks, as well as appropriate protective measures
- Learn how a web application works: requests, responses, parameters, cookies, and forms
- Identify fundamental web vulnerabilities and adopt a responsible testing approach with Burp Suite
- Hands-on workshop: observe web requests, identify a simple vulnerability, and propose a corrective measure

[Day 3 - Morning]

Offensive Security and Defensive Investigation

- Understanding the phases of an offensive approach: reconnaissance, enumeration, exploitation, and post-exploitation
- Discover the fundamental tools for enumeration, content search, and remote access in a controlled lab
- Introduction to the principles of vulnerability exploitation and the ethical and legal limitations of testing
- Fundamentals of defense: logs, alerts, indicators of compromise, and SOC monitoring
- Initial triage steps: qualifying an event, collecting evidence, and prioritizing an investigation
- Hands-on workshop: conducting a detection scenario, correlating logs, and producing an initial incident assessment

[Day 3 - Afternoon]

Targeted review and certification simulation

- Review of key areas: systems, networks, web security, offensive tools, and defensive operations
- Introduction to malware analysis: types of threats, observable behaviors, and precautions for handling
- Use of technical data: logs, files, hashes, URLs, and indicators of compromise
- Method for resolving a scenario: read the context, test, verify, document, and respond
- Strategy for preparing for the Cyber Security 101 (SEC1) exam: organization, time management, and reviewing answers
- Hands-on Workshop: Conduct a certification simulation combining system, network, web analysis, and defensive investigation

Target Audience

This training is intended for both individuals and companies—large or small—that wish to train their teams in new, advanced IT technologies or to acquire specific professional knowledge or modern methods.

Pre-training Assessment

The pre-training assessment complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency in various types of technologies, as well as their expectations and personal goals for the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could pose challenges for monitoring and ensuring the smooth running of the training session.

Teaching Methods

Hands-On Training: 60% Practical, 40% Theoretical. Training materials distributed in

digital format to all participants.

Organization

The course alternates between theoretical input from the instructor—supported by examples and reflection sessions—and group work.

Assessment

At the end of the session, a multiple-choice quiz is administered to verify that participants have successfully acquired the skills.

Certification

A certificate will be issued to each trainee who has completed the entire training program.