# OffSec SEC-100 CyberCore - Security Essentials Eğitimi

Süre: **5 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

SEC-100 Security Essentials provides a comprehensive foundation in cybersecurity for learners at the beginning of their careers. Covering a breadth of essential topics across governance and risk frameworks, offensive, defensive, and secure-by-design disciplines. The course also integrates general technical competencies, including scripting, networking, and cloud fundamentals. With a focus on practical application, participants will engage in hands-on labs, building core skills.

Learners who successfully complete the course and pass the proctored, hands-on OSCC SEC-100 exam will earn the OffSec CyberCore Certified certification, validating their readiness to enter the cybersecurity field.

## Prerequisites

There are no formal prerequisites.

Recommended:

- Basic computer literacy and familiarity with operating systems
- Willingness to learn and engage with hands-on technical content

Please note – learners are required to read the document in your MyQA portal after your course booking is confirmed. This document will advise learners to use a suitable personal computer, as corporate or organisation-managed laptops frequently restrict VPN connections, external lab access, and practical hacking activities, even when access is provided remotely by QA.

If learners must use a corporate laptop, they should ask their IT department to approve and test all required access before the course starts, or arrange an alternative computer without any restrictions.

### Target audience

This course is ideal for:

- Career starters and recent graduates seeking entry into cybersecurity
- IT professionals looking to transition into security-focused roles
- Service Desk and Helpdesk teams responsible for triaging security incidents
- Organisations aiming to upskill staff in foundational cybersecurity disciplines

# OffSec SEC-100 CyberCore - Security Essentials Eğitimi

Süre: **5 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

## Neler Öğreneceksiniz

By the end of this course, learners will be able to:

- Identify offensive and defensive techniques used in modern cyber operations
- Apply basic scripting in Python and PowerShell to security tasks
- Configure and manage secure systems across Windows, Linux, and cloud environments
- Recognise and respond to common security incidents and threats
- Demonstrate secure-by-design principles in software and system architecture
- Understanding the anatomy of cybersecurity and the CIA Triad, a foundational model that defines core security objectives
- Integrating industry-recognised frameworks like NIST and ISO 27001 to implement effective security practices
- Address the risks and vulnerabilities associated with cloud computing
- Examine AI's influence, both as a threat and as a tool to enhance offensive and defensive capabilities
- Exploring what a Penetration Test (Pentest) is, how they are performed, and what their objectives are