IBM Skills Academy

Cybersecurity Practitioners Course

Build expertise in developing security systems that understand, reason and learn; proactively reacting to cyber threats.

Organizations across all industries are faced with unmanageable levels of cyber threats brought on by a changing threat landscape.

The optimum strategy to respond to these threats is to make security an integral part of culture and overall structure—to help organizations better prepare for digital transformation in the age of the fourth industrial revolution.

About this course

This course comprises a unique mix of cybersecurity technical and real-world industry skills, designed to provide awareness on the impact of cybersecurity threats in key industries across geographies.

Cybersecurity Practitioners can elevate organizations’ overall security posture, by adopting practices, methods and tools that increase enterprise cyber resilience. Practitioners provide awareness on the latest cyber threats and can help set the foundation for implementing an incident response team and a security operations center.

Audience

Individuals with an active interest in applying for entry level jobs to work in cybersecurity related fields

Prerequisite skills for this course:

- Basic IT literacy skills

Journey: 75 hours

25% Lecture

Expanding knowledge and understanding of the topic through lectures, examples, videos and quizzes.

35% Hands-on Lab

Implement concepts learnt with hands-on lab activities, games and simulations.

40% Group Work Activities

Explore industry case studies to understand the real-world impact of the topics covered.
Objectives

This course covers the following objectives:

- Analyze top targeted industries and trends
- Explore how cyber criminals are using operating system tools to get control
- Uncover why cyber criminals are changing their techniques
- Determine what steps you can take to protect your organization against these threats
- Understand the tools used by penetration testers and ethical hackers (network CLI tools, Telnet, SSH, Nmap, Wireshark, and many others)
- Leverage high-end security enterprise solutions in high demand such as: IBM QRadar SIEM, Vulnerability Manager, UBA, IBM QRadar Advisor with Watson, I2 Analyst Notebook and IBM Cloud X-Force Exchange
- Gain real-world practice on critical threat modeling methodologies and frameworks such as MITRE, Diamond, IBM IRIS, and IBM Threat Hunting
- Participate in Security Operation Center (SOC) role-playing scenarios: experiencing research insights through design thinking practices
- Experience the basis for SOC—enacting the roles of triage analysts, incident response analysts, and threat intelligence analysts

Analyze tens of millions of spam and phishing attacks daily, and billions of web pages and images to detect fraudulent activity and brand abuse.