IBM **Skills Academy**

Cybersecurity

PRACTITIONERS COURSE

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

Today many organizations across all industries are faced with unmanageable levels of cyber threats brought on by the changing threat landscape, the risk of exposure, and an ever-growing attack surface.

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

IBM **Global University Programs**

CYBERSECURITY

Practitioner

About this course

This course comprises a unique mix of cybersecurity technical and real-world industry skills, brought to provide awareness on the impact of cybersecurity threats in key industries and 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 foundations for the implementation of 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*
- *Fundamentals of Internet networking, such as IP addresses, ports, routing browsers, servers, HTTP, web sites, encryption*

Journey

75 hours

- **25% Concepts**
  Expanding the knowledge and understanding of the topic through lecture training, examples, videos and quizzes.
- **35% Technologies**
  Actual implementation of the concepts learned through simulations, hands-on labs and games.
- **40% Industry Use Cases**
  Realization of the real-world impact of the topics covered through the exposure to industry case studies.

Objectives

- Analyze top targeted industries and annual trends.
- Explore how cyber criminals are using operating system tools to get control.
- Uncover why cyber criminals are changing their techniques to gain illegal profits.
- Determine what steps you can take to protect your organization against these threats.
- Understand the tools used by penetration testers and ethical hackers such as: network CLI tools, Telnet, SSH, Nmap, Wireshark, and many others
- Leveraging 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.
- Gaining real-world practice on critical threat modeling methodologies and frameworks such as MITRE, Diamond, IBM IRIS, IBM Threat Hunting, and security intelligence approaches to threat management.
- 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.

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

ibm.com/security

IBM