IBM **Security**

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.

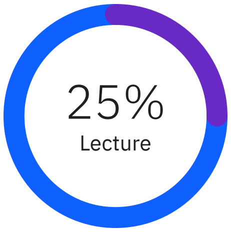
Audience

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

Prerequisite skills for thiscourse:

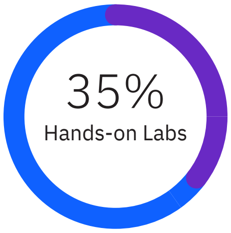
– Basic IT literacy skills

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

40% Group Work Activities

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

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

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

Badge

Student Badge

IBM Cybersecurity Practitioner Course

https://ibm.biz/Bdq7P4

IBM Corporation
New Orchard Road
Armonk, NY 10504
Produced in the United States of America,
December 2020

IBM, the IBM logo, ibm.com and Watson are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at ibm.com/legal/copytrade.shtml.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

This report is intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. IBM shall not be responsible for any loss whatsoever sustained by any organization or person who relies on this publication.

The data used in this report may be derived from third-party sources and IBM does not independently verify, validate or audit such data. The results from the use of such data are provided on an “as is” basis and IBM makes no representations or warranties, express or implied.