Cybersecurity for IT Professionals {Fundamentals Course}

To be good in cyber security, one MUST have a solid grasp of the fundamentals. The '**Cybersecurity for IT Professionals'** course is about building those fundamentals and creating that foundation.

The course validates a practitioner's knowledge of security's foundation, computer functions and networking, introductory level cryptography, and cybersecurity technologies. Those completing this course will be able to demonstrate key concepts of information security including: understanding the threats and risks to information and information resources, identifying best practices that can be used to protect them, and learning to diversify our protection strategy.

Dates: TBA

Delivery Mode: Virtual Class/Physical Class

Who should attend?

DB Administrators, System Administrators, Network Administrators, SOC Analysts, IT Managers, IT Auditors

1. People who are new to information security and in need of an introduction to the fundamentals of security
2. Those who feel bombarded with complex technical security terms they don't understand but want to understand
3. Professionals who need to be conversant in security concepts, principles, and terms, but who don't need too much detail
4. Those who have decided to make a career change to take advantage of the job opportunities in information security and need formal training/certification
5. IT Managers looking for a better understanding on profiling cyberattack vectors targeting their organizations

Topics

1. Cybersecurity career roadmap
1. Building an IT security skills matrix
2. The mindset of an attacker
3. Cybersecurity terminology
4. Basics of computer networks
5. The cyberattack kill chain
6. Understanding common web and mobile application attack vectors
7. Understanding common network and infrastructure attack vectors
8. Policies, procedures and compliance
9. Secure network design; design for defense in depth
10. Secure systems/networks architecture
11. Monitoring, detection and logging
12. Building defensible applications
13. Understanding Cyber Measurements and Metrics

You Will Be Able To:

1. Communicate with confidence regarding information security topics, terms, and concepts
2. Understand and apply the Principles of Least Privilege
3. Understand and apply the Confidentiality, Integrity, and Availability (CIA) for prioritization of critical security resources
4. Build better passwords that are more secure while also being easier to remember and type
5. Grasp basic cryptographic principles, processes, procedures, and applications
6. Understand how a computer works
7. Understand computer network basics
8. Have a fundamental grasp of any number of technical acronyms: TCP/IP, IP, TCP, UDP, MAC, ARP, NAT, ICMP, and DNS, and the list goes on.
9. Utilize built-in Windows tools to see your network settings
10. Recognize and be able to discuss various security technologies, including anti-malware, firewalls, intrusion detection systems, sniffers, ethical hacking, active defense, and threat hunting.
11. Understand wireless technologies including WiFi, Bluetooth, mobile phones and the Internet of Things (IoT)
12. Explain a variety of frequent attacks such as social engineering, drive-by downloads, watering hole attacks, lateral movement, and other attacks
13. Understand different types of malware
14. Understand browser security and the privacy issues associated with web browsing
15. Explain system hardening
16. Discuss system patching
17. Understand virtual machines and cloud computing

Laptop Requirements

Important! Bring your own system configured according to these instructions!

A properly configured system is required to fully participate in this course. If you do not carefully read and follow these instructions, you will likely leave the class unsatisfied because you will not be able to participate in hands-on exercises that are essential to this course. Therefore, we strongly urge you to arrive with a system meeting all the requirements specified for the course.

This course includes both lecture and hands-on labs. There are specific computer configuration requirements to perform hands-on labs.

- A laptop running any version of Microsoft Windows or a Mac.
- We do not recommend attempting to perform the labs with a tablet such as an iPad or Android. A Surface tablet can perform the labs, but smaller screens are problematic.
- A Web Browser. We strongly recommend the Google Chrome browser, but Internet Explorer, Firefox, Opera, Safari, or any other modern browser works.
- Have the ability to connect to a wireless (WiFi) network.

Prerequisite - This course assumes only the most basic knowledge of computers and makes no assumptions regarding prior security knowledge.