CYBER SECURITY

I. Networking & Cyber Security Fundamentals

Week 1 - Network Concepts & Protocols

In this course, you will learn how the most important protocols on the Internet, like IP, TCP, and HTTP work together to deliver a web page from a server on the Internet to your desktop's web browser. First, you will explore using the OSI model to organize protocols to better understand how they interact. Next, you will learn the secrets of the IP address. Finally, you will discover the most important rules to help you understand whether two devices can communicate. By the end of this course, you will be able to quickly examine network configuration on your workstation and clearly understand the different components.

Week 2 – Network Security Basics

You will get a very basic introduction to IT attacks as well as how to detect and prevent them. First, we will describe basic security concepts, explaining threats, vulnerabilities, and exploits. Next, we will compare common attacks and then discuss some mitigation techniques. Then we will discuss the security implications of remote access into corporate networks and wrap up the course by discussing the physical security needs of an organization. When you're finished with this course, you'll have the knowledge and skills of network monitoring and documentation to understand how enterprise IT maintains IT infrastructure for optimum performance.

II. Python

Week 3 - Python Fundamentals

In this course, you'll learn the fundamentals of Python while building practical Python programs. First, you'll explore data types, conditionals, and loops. Next, you'll discover Python libraries, functions, and classes. Finally, you'll learn how to manipulate files and do web requests. When you're finished with this course, you'll have the skills and knowledge of Python needed to create complex Python applications to solve a variety of problems.

digital
nova scotia

CYBER SECURITY

Week 4 - Python Functions & Libraries

In this course, you'll learn the core set of libraries and functions that will allow you to automate and customize tools to meet the need of your business. First, you'll explore third-party packages developed to solve specific needs important to the information security industry. Next, you'll discover functions provided by those libraries that allow you to speed up the development process and turn around tools to serve the need of your business to better secure your infrastructure. When you're finished with this course, you'll have the skills and knowledge needed to extend your Python coding skills into the information security space.

Week 5 - Cryptography: The Big Picture

You'll learn how cryptography fits into an overall security strategy for any business or government entity. First, you'll dive into learning about the history of cryptography. Next, you'll explore all the different types of cryptographic algorithms. Finally, you'll discover how to start using cryptography to protect your information - today. By the end of this course, you'll know how encryption plays a vital role in the security strategy of any business.

Week 6 - Practical Encryption and Cryptography Using Python

You will learn the practical aspect of cryptography using the amazing programming language Python, and you will gain the confidence to master the skill of crypto by using real-life examples. First, you will learn about hashing algorithms. Next, you will discover Symmetric Encryption using Python. Finally, you will explore the multiple angles of Asymmetric Encryption using public and private keys. When you're finished with this course, you will have the necessary skills and knowledge about cryptography to use in your career.

Week 7 - Log file analysis with Python

You'll learn how to automate the analysis of log files using Python. First, you'll explore how to parse log files. Next, you'll discover log data analysis. Finally, you'll learn how to integrate with other solutions to submit enriched data. When you're finished with this course, you'll have the skills and knowledge of Log file analysis needed to automate log analysis.

digital
nova scotia

Week 8 – Malware Detection and Analysis with Python

You'll learn to automate malware triage, detection, and analysis. First, you'll explore some of the core packages such as yara-python that facilitate triage and classification. Next, you'll discover how to interact with 3rd-party services to establish the file disposition/reputation. Finally, you'll learn how to extract artifacts and indicators from files to enable more in- depth analysis. When you're finished with this course, you'll have the skills and knowledge of python scripting and automation needed to uplift malware detection and analysis workflows and capabilities.

Week 9 – Assignment on Cybersecurity Fundamentals and Python

Assignment 2 will be shared on the Learning Management System.

III. Cyber Security Fundamentals – ISC2 Certified in Cybersecurity

Week 10 – Security Principles for CC℠

You'll learn essential security concepts. First, you'll explore Information assurance and governance. Next, you'll discover Risk Management. When you're finished with this course, you'll have the skills and knowledge of Information protection and assurance.

Week 11 –Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts for CC℠

You'll learn to prepare for and mitigate incidents that could affect business operations. First, you'll explore incident response. Next, you'll discover business continuity. Finally, you'll learn how to recover from a disaster.

Week 12 – Access Controls Concepts for CC®

You'll learn to appreciate the importance of access controls in relation to protecting the assets and data of the organization. First, you'll explore access control concepts and terminology. Next, you'll discover physical access controls. Finally, you'll learn how information systems are secured using logical access controls.

CYBER SECURITY

Week 13 –Network Security for CC℠

You'll learn about securing computer networks. First, you'll explore network concepts, protocols, and terminology. Next, you'll discover Network threats and attacks. Finally, you'll learn how tools are used to secure the network.

Week 14 - Security operations for CC℠

In this course, Security Operations for CC℠, you'll learn to protect the information assets of the organization through good security practices. First, you'll explore data protection and cryptography. Next, you'll discover Security principles and administration. Finally, you'll learn the value of security awareness training and monitoring.

Week 15 - Assignment on Cyber Security Fundamentals - ISC2 Certified in Cybersecurity

 Assignment 3 will be shared on the Learning Management System.

IV. Generative AI for Security

Week 16 - Generative AI and Cybersecurity

In this path, you will discover the data and privacy concerns of using Generative AI. What attacks can happen? How do I keep my data secure? Learn how to reduce security risks and utilize Generative AI to the best of its ability. Next, lean into Generative AI integrating into security operations to improve your organization's security maturity. We'll discuss how to leverage AI's abilities to increase and expand your offensive and defense security operation's capabilities.

digital
nova scotia