

CYBER SECURITY

SKILLS | ELEVEZ
FOR HIRE | VOS COMPÉTENCES
Atlantique

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.

Week 3 -

Assignment 1 will be shared via Slack.

Week 3 - Python 3 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.

CYBER SECURITY

SKILLS | ELEVEZ
FOR HIRE | VOS COMPÉTENCES
Atlantique

Week 5 - 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 6 - 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 7 - 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 8 - 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.

CYBER SECURITY

SKILLS | ELEVEZ
FOR HIRE | VOS COMPÉTENCES
Atlantique

Week 9 - Network Activity and Packet Analysis with Python

You'll learn about several concepts that enable a network security engineer/consultant to design and deploy solutions that aid in their day-to-day activities and help expand on their potential abilities. First, you'll learn how Scapy's packet engine is designed and implemented to perform actions on individual packets. Next, you'll learn how to use Scapy to sniff network traffic, monitor for brute force attacks and perform port scanning and traceroute functions. Finally, you'll learn how to perform connection hijacking and perform traffic replay. When you're finished with this course, you'll have the skills and knowledge required to utilize Python and Scapy for some of the most common network security tasks that can then be used to extend your security toolkit.

Week 10 - 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 11 -

Assignment 2 will be shared via Slack.

Week 12 - Security Principles for CCSM

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.

CYBER SECURITY

SKILLS | ELEVEZ
FOR HIRE | VOS COMPÉTENCES
Atlantique

Week 13 -Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts for CCSM

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 14 - 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.

Week 15 -Network Security for CCSM

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 16 -

Assignment 3 will be shared via Slack.

Week 17 - Fundamental Cloud Concepts

Will explain one of the four major areas that are covered by the AWS Certified Cloud Practitioner Exam. First, you will review the concept of cloud computing and the value it provides to organizations. Next, you will learn the organization of AWS global infrastructure. Next, you will discover the economics of cloud computing. Finally, you will review the tools and services that AWS provides to support the infrastructure running on their platform. When you are finished with this course, you will have a clear understanding of the cloud and the fundamentals needed for a portion of the AWS Certified Cloud Practitioner exam. In this course you'll learn the different forms of cloud computing, how they can help you, and what makes them so powerful. You'll see numerous hands-on demos of cloud computing solutions including infrastructure as a service and software as a service solution. Finally, you'll learn how to secure your cloud and protect your data in the cloud. When you're done with this course, you'll have the skills and knowledge that you need to understand and use cloud computing.

CYBER SECURITY

SKILLS | ELEVEZ
FOR HIRE | VOS COMPÉTENCES
Atlantique

Week 19 -

In this course, we will through the services from AWS that you will need to know before you take the AWS Certified Cloud Practitioner Exam. First, you will review the ways you interact with AWS services. Next, you will explore the major categories including computing, networking and content delivery, file storage, databases, app integration, and management and governance. Finally, you will discover an approach to preparing for the certification exam. When you are finished with this course, you will have a clear understanding of these core services whether you want to take the AWS Certified Cloud Practitioner exam or just have a better understanding of the services that AWS provides.

Week 20 -

In this course, you will learn foundational knowledge of both security on AWS as well as how to architect solutions on the platform. This information is valuable for anyone using AWS, but it is essential for preparing to take the AWS Certified Cloud Practitioner Exam. First, you will review three core concepts that affect how you use the platform: the AWS Well-Architected Framework, the shared responsibility model, and the acceptable use policy. Then, you will learn security and user management on AWS. Next, you will discover key architectural concepts around fault tolerance, high availability, and disaster recovery. Finally, you will explore concepts around scalable and secure applications on Amazon EC2. When you are finished with this course, you will have a clear understanding of the concepts needed for a portion of the AWS Certified Cloud Practitioner exam as well as the knowledge needed to begin implementing applications in the cloud.