EVIARE

CYBERSECURITY EXPERT

EVIARE

TABLE OF CONTENTS

PROGRAMME OVERVIEW

WHO IS THIS PROGRAMME FOR?

KEY FEATURES OF THE PROGRAMME

PROGRAMME OUTCOMES

LEARNING PATH

COURSES

- INTRODUCTION TO CYBERSECURITY
- COMPTIA NETWORK+
- COMPTIA SECURITY+
- CISSP

DELIVERY METHOD & CERTIFICATE

PROGRAMME HIGHLIGHTS

EVIARE

Programme Overview

The Cyber Security Master's Program will equip you with the full range of skills needed to become an expert in this rapidly growing domain. You will learn comprehensive approaches to protecting your infrastructure, including securing data and information, running risk analysis and mitigation, architecting cloud-based security, achieving compliance and much more with this best-in-class program.

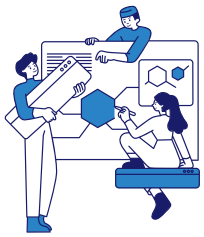
Who Is This Program For?

This program caters to a wide audience, from those who are hoping to enter the industry to those who have already gained some experience and are aspiring to become full stack developers.

KEY PROGRAMME FEATURES

Comprehensive Applied Learning program

96+ hours of instructor-led online classes



64+ hours of e-learning

Master's Certificate upon course completion

EVIARE

PROGRAMME OUTCOMES

- Install, configure and deploy public key infrastructure and network components while assessing and troubleshooting issues to support organizational security
- Master advanced hacking concepts to manage information security efficiently
- Build a working industry application from scratch
- Master advanced hacking concepts to manage information security efficiently
- Master advanced hacking concepts to manage information security efficiently
- Focus on IT compliance and the integrity of enterprise systems to establish a more secure enterprise IT framework

EVIARE

Learning Path

1. Introduction to Cyber Security
2. CompTIA Network+
3. CompTIA Security+
4. CISSP® Training

EVIARE

Course 1

Introduction to Cyber Security

Introduction to Cyber Security course for beginners is designed to give you a foundational look at today's cybersecurity landscape and provide you with the tools to evaluate and manage security protocols in information processing systems.

Key Learning Objectives

- Gain a comprehensive overview of cyber security principles and concepts
- Learn the challenges of designing a security program
- Develop and manage an information security program, perform business impact analysis, and carry out disaster recovery testing

EVIARE

Course 2

CompTIA Network+

The CompTIA Network+ course is designed to provide students with the knowledge and skills to configure, manage, and troubleshoot networked systems. It also provides an understanding of network security and the fundamentals of virtualization and cloud computing.

The Network+ certification is an industry-standard certification that is highly respected and sought after by employers. It is also a prerequisite for many higher-level certifications such as the CCNA and MCSE.

Key Learning Objectives

- Configure, manage, and troubleshoot network devices such as routers, switches, and wireless access points.
- Understand the fundamentals of networking protocols such as TCP/IP, OSI model, and Ethernet.
- Implement virtual private networks (VPNs) and security protocols.
- Understand the basics of designing and deploying a network.
- Understand network topologies and technologies such as cloud, virtualization, and wireless.
- Utilize tools and techniques to troubleshoot network issues.
- Understand network performance optimization, monitoring, and management.
- Understand the implications of network architecture and design on performance and security.
- Implement best practices in the installation, configuration, and maintenance of networked systems.

EVIARE

Course 3

CompTIA Security+

CompTIA Security+ is an industry-leading certification for IT professionals looking to develop their cybersecurity skills. It is designed to provide a foundation of security knowledge, which can be applied to a wide range of environments and technologies.

The CompTIA Security+ course covers a wide range of topics, including network security, security protocols, application security, encryption, access control, identity management, and firewalls. It also covers operational security, such as risk assessment, incident response, and compliance. The course also covers topics such as cybercrime, ethical hacking, and digital forensics.

Key Learning Objectives

- Understand the core concepts of cybersecurity and risk management, such as identifying threats and vulnerabilities, developing mitigation strategies, and implementing security protocols.
- Demonstrate an understanding of encryption, authentication, access control, and network security.
- Develop an understanding of network security tools and techniques, such as firewalls, intrusion detection systems, and antivirus programs.
- Understand identity and access management systems and technologies, such as biometrics, single sign-on, and two-factor authentication.
- Develop an understanding of the principles of system and application security, such as patch management, secure coding practices, and vulnerability management.
- Develop an understanding of the principles of physical security and disaster recovery.
- Demonstrate an understanding of compliance regulations, standards, and best practices.

EVIARE

Course 4

CISSP

The Certified Information Systems Security Professional (CISSP) course is a comprehensive certification program that provides IT professionals with the knowledge and skills needed to design, implement, and manage secure information systems. The CISSP course covers a wide range of topics, including cryptography, access control, network security, risk management, and security architecture.

The CISSP course consists of eight domains, each of which is designed to provide an in-depth understanding of a specific security topic. The eight domains are: Security and Risk Management, Asset Security, Security Engineering, Communications and Network Security, Identity and Access Management, Security Assessment and Testing, Security Operations, and Software Development Security.

Key Learning Objectives

- Understand the Eight Domains of the Common Body of Knowledge (CBK)
- Develop an understanding of the underlying principles and processes involved in information security, such as access control, authentication, cryptography, network security, and physical security.
- Gain the skills needed to effectively assess risk, develop security strategies, and audit security policies.
- Understand the various threats to information systems and how to identify, monitor, and prevent them.
- Understand the importance of incident response, data protection, and business continuity planning.
- Acquire the skills necessary to perform security assessments, audits, and investigations.
- Develop the skills required to pass the CISSP certification exam.

Delivery and Certification

With over 85% completion rates, we understand how important it is to feel safe and secure when you're improving yourself. You will learn virtually on our online learning platform at your own pace. This give you the freedom and comfort of learning from your own home at your own pace, unimpeded. Once completed with the course, you will receive a certificate of completion.

EVIARE

Programme Highlights

Programme Duration: 6 months

1-2 hours per week

Learning Experience

The programme content is flexible and accessible on multiple devices. The programme flexibility can be utilised by working professionals to manage their schedules and access the content from anywhere and anytime. The programme includes various instruments in addition to its core curriculum to provide you a superior learning experience:

Self-paced videos

Discussions

Assignments

Quizzes