Claranet University - Academias relGNITE

Cyber Security Academy

Integradas na oferta de formação tecnológica Claranet University, as Academias relGNITE apostam nas profissões do futuro e no desenvolvimento de competências técnicas e conhecimento especializado, com elevada procura.

Estes percursos formativos com certificações oficiais proporcionam aos profissionais uma atualização tecnológica constante, bem como a aquisição de competências para responder às necessidades de novas funções ou projetos.

As Academias relGNITE acompanham os rodmaps completos de cursos oficiais made by Claranet e dirigem-se a profissionais de TI com experiência, ou com conhecimentos para cumprir os pré-requisitos de cada projeto de formação em que pretendam participar.

Num contexto em que a procura por profissionais de cibersegurança é cada vez maior, a Academia de Cyber Security da Claranet pretende responder a esse desafio global, fornecendo o know-how e as competências técnicas para os profissionais construírem uma carreira na área da Segurança de Informação.

Esta academia visa dotar os profissionais com as competências necessárias para identificar ameaças e vulnerabilidades de segurança, através de uma oferta de formação abrangente, que inclui regulamentos e boas práticas, e que no final permitirá aos participantes implementar e gerir, nas suas organizações, um programa de segurança da informação.

NOME DA FORMAÇÃO — **Cyber Security Academy**

FORMATO — **Live Training**

CERTIFICAÇÕES OFICIAIS

- Integrada na oferta de Academias relGNITE, a Academia de Cyber Security é composta por seis módulos de formação que abrangem tópicos essenciais para uma ação eficaz enquanto profissional na área da Segurança de Informação.
- O percurso formativo da Academia de Cyber Security inclui três certificações - o CompTIA A+, o CompTIA Securiy + e o ISO 27001.
- A componente de hacking é garantida pelos cursos da Not So Secure.

PRÉ-REQUISITOS

- Os participantes devem ter conhecimentos técnicos de informática e redes.
- Os participantes devem igualmente ter bons conhecimentos de língua inglesa, atendendo ao facto de os manuais entregues durante a formação estarem neste idioma e dos dois últimos módulos serem ministrados em inglês.

OBJETIVOS GERAIS

- Identificar regulamentos, normas e práticas de cibersegurança, permitindo implementar e gerir um programa de segurança da informação.

PROGRAMA

MATERIAIS

- Todos os materiais sobre os conteúdos dos módulos serão entregues aos participantes em língua inglesa e formato digital.

Módulo 1
Comptia A + (30 Horas)

Additional information:
CompTIA A+ is the preferred qualifying credential for technical support and IT operational roles. CompTIA A+ certified professionals are proven problem solvers. They support today's core technologies from security zto cloud to data management and more.

CompTIA A+ is the industry standard for launching IT careers in today's digital world.

To receive the CompTIA A+ certification, learners must pass two exams: Core 1 (220-1001) and Core 2 (220-1002)

- Supporting Operating Systems
- Installing and Configuring PC Components
- Installing, Configuring, and Troubleshooting Display and Multimedia Devices
- Installing, Configuring, and Troubleshooting Storage Devices
- Installing, Configuring, and Troubleshooting Internal System Components
- Installing, Configuring, and Maintaining Operating Systems
- Maintaining and Troubleshooting Microsoft Windows
- Network Infrastructure Concepts
- Configuring and Troubleshooting Networks
- Managing Users, Workstations, and Shared Resources
- Implementing Client Virtualization and Cloud Computing
- Security Concepts
- Securing Workstations and Data
- Troubleshooting Workstation Security Issues
- Supporting and Troubleshooting Laptops
- Supporting and Troubleshooting Mobile Devices
- Installing, Configuring, and Troubleshooting Print Devices
- Implementing Operational Procedures

Módulo 2
CompTIA Security + (30 Horas)

Additional information:
The Official CompTIA Security+ Instructor and Student Guides (SY0-601) have been developed by CompTIA for the CompTIA certification candidate.

Rigorously evaluated to validate coverage of the CompTIA Security+ (SY0-601) exam objectives, The Official CompTIA Security+ Instructor and Student Guides teach students the knowledge and skills required to:

- Assess the security posture of an enterprise environment and recommend and implement appropriate security solutions.
- Monitor and secure hybrid environments, including cloud, mobile, and IoT.
- Operate with an awareness of applicable laws and policies, including principles of governance, risk, and compliance.
- Identify, analyze, and respond to security events and incidents.

- Comparing and Contrasting Attacks
- Comparing and Contrasting Security Controls
- Using Security Assessment Tools
- Comparing and Contrasting Basic Concepts of Cryptography
- Implementing Public Key Infrastructure
- Implementing Identity and Access Management Controls
- Managing Access Services and Accounts
- Implementing Secure Network Architecture Concepts
- Installing and Configuring Security Appliances
- Installing and Configuring Wireless and Physical Access Security
- Deploying Secure Host, Embedded, and Mobile Systems
- Implementing Secure Network Access Protocols
- Implementing Secure Network Applications
- Explaining Risk Management and Disaster Recovery Concepts
- Summarizing Secure Application Development Concepts
- Explaining Organizational Security Concepts

Módulo 3
ISO/IEC27001 Foundation (18 Horas)

Additional information:
ISO/IEC 27001 Foundation training allows you to learn the basic elements to implement and manage an Information Security Management System as specified in ISO/IEC 27001.

During this training course, you will be able to understand the different modules of ISMS, including ISMS policy, procedures, performance measurements, management commitment, internal audit, management review and continual improvement.

- The scope and purpose of ISO/IEC 27001 and how it can be used,
- The key terms and definitions used in the ISO/IEC 27000 series
- The fundamental requirements for an ISMS in ISO/IEC 27001 and the need for continual improvement.
- The processes, their objectives, and high-level requirements.
- Applicability and scope definition requirements.
- Use of controls to mitigate IS risks.
- The purpose of internal audits and external certification audits, their operation, and the associated terminology.
- The relationship with best practices and with other related International
- Standards: ISO 9001 and ISO/IEC 20000.

Módulo 4
GDPR - General Data Protection Regulation (6 Horas)

- Introducing to Personal Data Concept.
- Legitimacy and purpose limitations.
- Responsibilities in data processing.
- Requirements for personal data processing.
- The Sensitive Data concept.
- Privacy by Design & Privacy by Default.
- Data Protection on Companies.
- IAPP professional certifications.
- Right to be forgotten (RTBF), access to information, portability, correction and elimination.
- “Data breach” and notifications to controller entity and citizens.
- Personal data transfer to third countries.
- The regulatory bodies.
- The Information Technologies in supporting of GDPR.

Módulo 5
Basic Infrastructure Hacking (21 Horas)

- The Art of Port Scanning
- The Art of Online Password Attacks
- The Art of Hacking Databases
- Mestasploit Basics
- Password Cracking
- Hacking UNIX
- Hacking Application Servers on UNIX
- Hacking Third Party CMS Software
- Windows Enumeration
- Client-Side Attacks
- Privilege Escalation on Windows
- Hacking Application Servers on Windows
- Post Exploitation
- Hacking Windows Domains

Módulo 6
Basic Web Hacking (14 Horas)

- Understanding the HTTP Protocol
- Information Gathering
- Username Enumeration & Faulty Password Reset
- Issues with SSL/TLS
- Authorization Bypass
- Cross Site Scripting (XSS)
- Cross Site Request Forgery (CSRF)
- SQL Injection
- External Entity (XXE) Attacks
- Insecure File Uploads
- Deserialization Vulnerabilities

MATERIAIS

- Todos os materiais sobre os conteúdos dos módulos serão entregues aos participantes em língua inglesa e formato digital.