Curso: Percurso Cyber Security

Duração: 350h
Área formativa: Outros

Sobre o curso

Este percurso fornecer-lhe as competências técnicas necessárias para construir uma carreira sustentada na área da Segurança de Informação.
Ao longo do percurso as matérias, e respetivo nível, vão evoluindo. O percurso inicia com as temáticas da identificação de ameaças e vulnerabilidades de segurança, configuração de soluções que permitam reduzir a superfície de ataque de variados tipos de sistemas informáticos, bem como a implementação de diferentes tipos de metodologias de hardening. Culmina de forma a proporcionar a experiência e credibilidade para projetar, implementar e gerir um programa de segurança da informação para proteger as organizações de crescentes ataques sofisticados.

Este curso tem como objetivos:

Munir os participantes com os conhecimentos e experiência em configuração de equipamentos de networking e segurança (Switches, Firewalls, VPNs, IPS e Load Balancers) bem como a implementação soluções que permitam reduzir a superfície de ataque de servidores, clientes, dispositivos de rede, sistemas industriais e dispositivos moveis (AV, HIDS, SIEM, Threat Analytics, …).

Preparar Analistas de Segurança para desenhar e implementar soluções de monitorização, análise, prevenção de intrusões, firewalls, controle de acesso e alarmística. Lidar com sistemas críticos e criar planos de resposta a incidentes e recuperação de desastres. Desenvolver competências na resposta a novas ameaças. Realizar análise de vulnerabilidades e testes de intrusão de forma a testar as soluções implementadas.

Preparar auditores para realização de testes de intrusão a ambientes com elevado nível de segurança, adotando a perspetiva de um adversário avançado como modo de operação, permitindo uma melhor identificação, quantificação e gestão do risco, melhorando os conhecimentos necessários para conduzir auditorias de acordo com os requisitos e normas existentes.

O Percurso Cyber Security inclui 6 exames de certificação:

- MTA Security Fundamentals (98-367)
- CompTIA S+ (SY0-501)
- Ethical Hacking (CEH)
- Comptia CSA+ (CS0-001)
- ISO 27001

- MoR

E confere as seguintes certificações:

- MTA Security Fundamentals
- CompTIA Security+
- Ethical Hacking
- CompTIA Cybersecurity Analyst
- ISO/IEC 27001
- M_o_R (Management of Risk) Certification
- Certificação Rumos Expert (CRE): Auditor de Segurança

Os exames de certificação deverão ser realizados no final dos respetivos módulos de formação. As datas para a realização dos exames de certificação são sugeridas pela Rumos, no entanto, a marcação é feita pelo formando no momento em que se sentir preparado para tal.
A marcação deve ser efetuada com 4 dias úteis de antecedência à data pretendida e o resultado do exame é conhecido aquando da finalização do mesmo.
Os exames têm a validade de 6 meses a contar da data de fim da formação.

Destinatários

Destina-se a todos os interessados em aprofundar conhecimentos e desenvolver competências na área de Segurança de Redes e Sistemas, para consolidar uma carreira especializada em Segurança de Informação.

Pré-requisitos

Conhecimentos de Inglês técnico: é aconselhável que o formando seja capaz de compreender manuais técnicos na língua inglesa.

Valorizam-se conhecimentos técnicos Informática ao nível de redes e sistemas

O percurso não apresenta quaisquer pré-requisitos a nível de habilitações académicas ou experiência profissional

---

Metodologia

Presencial.

Programa

- Fundamentos de Segurança e Informática (31,5h)

- Security Fundamentals (e-Learning)
- CompTIA Security+ (31,5h)
- Ação de Preparação para Exame MTA (3,5h)
- Seminário: Powershell and Scripting (7h)
- Hardening de Sistemas (31,5 h)
- Segurança no desenvolvimento de Software (17,5h)
- Ação de Preparação para Exame Comptia S+ (3,5h)
- Marketing Pessoal e Comunicação (3,5h)
- Fundamentos Kali Linux (e-Learning)
- Ethical Hacking and Countermeasures (31,5h)
- Offensive Penetration Testing Services (21 h)
- Ação de Preparação para Exame CEH (3,5h)
- Noções básicas de direito + Lei do Cibercrime (7h)
- Monitorização, Deteção e Prevenção de Intrusões (28h)
- Resposta a Incidentes com Técnicas Forenses (24,5h)
- Ação de Preparação para Exame CompTIA CSA+ (3,5h)
- Information Security Management ISO/IEC 27001/27002 (28h)
- Ação de Preparação para Exame EXIN ISO/IEC 27001 (3,5h)
- Risk Management (31,5h)
- Ação de Preparação para Exame MoR (3,5h)
- Proteção de Dados - RGPD (7h)
- Information Systems Security - Domains of knowledge – Part 1 (e-Learning)
- Information Systems Security - Domains of knowledge – Part 2 (17,5h)
- Certificação Rumos Expert (CRE): Auditor de Segurança (14 h)

Fundamentos de Segurança e Informática

- Introdução à temática da segurança
- Evolução e antecedentes históricos
- Panorâmica geral sobre a situação atual
- Hardware
- Sistemas Operativos
- Virtualização e Cloud Computing
- Criação de máquinas virtuais em Hyper-V e VBox
- Utilização prática dos dois hipervisores
- Criptografia
- Passwords
- Redes de computadores

Security Fundamentals (e-Learning)

- Understanding Security Layers
- Authentication, Authorization, and Accounting
- Understanding Security Policies
- Understanding Network Security
- Protecting the Server and Client

CompTIA Security+

- Security Fundamentals
- Data Security
- Application Security

- Hosts and Devices Protection
- Internal Network Protection
- Perimeter Network Protection
- Physical Security
- Compliance and Operational Security
- Threats

Ação de Preparação para Exame MTA

Seminário: Powershell and Scripting

Hardening de Sistemas

- Introduction
- Hardening
- Standards
- DISA STIGs
- Windows 7 Hardening
- Windows 10 Hardening
- Linux Hardening
- Windows Server 2012 Hardening
- Windows & Linux Hardening
- OpenVas

Segurança no desenvolvimento de Software

- Ciclo de vida de desenvolvimento de software
- Conceitos básicos da programação
- Desenho de código seguro
- Testes de segurança de software

Ação de Preparação para Exame Comptia S+

Marketing Pessoal e Comunicação

- Marketing Pessoal: definição e exploração do conceito
- Identificação da importância do Marketing Pessoal no crescimento pessoal e profissional
- A análise Swot aplicada aos objetivos pessoais e profissionais
- Abordagem ativa ao mercado de trabalho

Fundamentos Kali Linux (e-Learning)

- About Kali Linux
- Getting Started with Kali Linux
- Linux Fundamental
- Installing Kali Linux
- Configuring Kali Linux
- Helping Yourself and Getting Help
- Securing and Monitoring Kali Linux
- Debian Package Management
- Advanced Usage
- Kali Linux in the Enterprise
- Introduction to Security Assessments

Ethical Hacking and Countermeasures

- Introduction to Ethical Hacking
- Footprinting and Reconnaissance
- Scanning Networks
- Enumeration
- Vulnerability Analysis
- System Hacking
- Malware Threats
- Sniffing
- Social Engineering
- Denial-of-Service
- Session Hijacking
- Evading IDS, Firewalls, and Honeypots
- Hacking Web Servers
- Hacking Web Applications
- SQL Injection
- Hacking Wireless Networks
- Hacking Mobile Platforms
- IoT Hacking
- Cloud Computing
- Cryptography

Offensive Penetration Testing Services

- Using the Metasploit Framework
- Information Gathering
- Finding Vulnerabilities
- Capturing Traffic
- Exploitation
- Password Attacks
- Client-Side Exploitation
- Social Engineering
- Bypassing Antivirus Applications
- Post Exploitation
- Web Application Testing
- Wireless Attacks

Ação de Preparação para Exame CEH

Noções básicas de direito + Lei do Cibercrime

Monitorização, Deteção e Prevenção de Intrusões

- Policy and Compliance
- Evaluating Security Risks
- Defensible Security Architecture
- Defensible Endpoint Security Architecture
- Traditional Attack Techniques
- Network Security Monitoring (NSM)
- Identity and Access Management Security
- Designing a Vulnerability Management Program

- Analyzing Vulnerability Scans
- Monitoring Logs
- Monitoring Critical Events

Resposta a Incidentes com Técnicas Forenses

- Preparação para o Incidente
- Deteção e caracterização de incidente
- Recolha de Evidências/Dados
- Análises de Dados
- Contenção e Remediação
- Erradicação
- Documentação e Conclusões

Ação de Preparação para Exame CompTIA CSA+

Information Security Management ISO/IEC 27001/27002 (28h)

- Introduction to the ISO 27000 standards family Introduction to management systems and the process approach
- General requirements of ISO/IEC 27002
- Implementation phases of the ISO/IEC 27002 framework
- Introduction to risk management according to ISO 27005
- Continual improvement of information security
- Conducting an ISO/IEC 27002 certification audit

Ação de Preparação para Exame EXIN ISO/IEC 27001 (3,5h)

Risk Management (31,5h)

- Explain the terminology that is used within M_o_R
- Understand the principles for the development of good risk management practices
- Design an approach to risk management to improve performance
- Identify and assess risks, then plan and implement risk responses
- Establish current practices using M_o_R healthcheck and maturity model
- Identify opportunities and ways to improve Risk management
- Understand the importance of Risk Specialisms

Ação de Preparação para Exame MoR (3,5h)

Proteção de Dados – RGPD (7h)

Information Systems Security – Domains of knowledge – Part 1 (e-Learning)

- Segurança e Gestão de Riscos;
- Segurança de Ativos;
- Engenharia de Segurança;
- Comunicações e Segurança de Redes;
- Gestão de Identidades e Acessos;
- Avaliação de Segurança e Testes;
- Operações de Segurança;
- Segurança em Desenvolvimento de Software

Information Systems Security – Domains of knowledge – Part 2

- Segurança e Gestão de Riscos;
- Segurança de Ativos;
- Engenharia de Segurança;
- Comunicações e Segurança de Redes;
- Gestão de Identidades e Acessos;
- Avaliação de Segurança e Testes;
- Operações de Segurança;
- Segurança em Desenvolvimento de Software

Certificação Rumos Expert (CRE): Auditor de Segurança