Analista de Segurança

Segurança Informática

Com certificação

- **Nível:** Intermédio
- **Duração:** 126h

Sobre o curso

Este percurso irá fornecer-lhe as competências técnicas necessárias para construir uma carreira sustentada na área da Segurança de Informação. Formar profissionais capazes de utilizar de técnicas inovadoras de monitorização, investigação, análise, prevenção e resposta a incidentes e recuperação de desastres, para que possam ter assim os conhecimentos necessário tanto para uma Red Team como para uma Blue Team.

Esta é a segunda carreira o de um conjunto de três, que compõem a carreira mais longa, a Cyber Security.

Inclui as Certificações:

- Certified Ethical Hacker
- CompTIA Cybersecurity Analyst+

Condições Financeiras

- Taxa de inscrição: 220€, dedutível no valor total.
- Possibilidade de pagamento faseado para particulares, **até 10 prestações, sem juros**.
- Os valores apresentados não incluem IVA. Isenção do valor do IVA a particulares.
- Para informações completas sobre os requisitos e condições financeiras disponíveis, contacte-nos através de info@galileu.pt ou do botão Saber +.

Campanha de Natal

- Oferta de 10% de desconto sobre o valor da inscrição.
- Campanha válida para as 5 primeiras inscrições até 31 de janeiro de 2020.
- Para todas as edições das Carreiras Profissionais a iniciar no 1º semestre de 2020.
- Acumulável com 5% de desconto por pronto pagamento.

Destinatários

- Arquitetos de Redes;
- Administradores de Redes;
- Administradores de Sistemas Seniores;
- Profissionais que pretendam investir ou mudar de carreira.

Saídas Profissionais:

- Administrador de Segurança da Informação
- Consultor de Segurança da Informação
- Penetration Test Engineer
- Cyber Security Analyst

Pré-requisitos

- Conhecimentos de Inglês técnico: é aconselhável que o formando seja capaz de compreender manuais técnicos na língua inglesa
- Privilegiam-se conhecimentos técnicos de informática e redes, ao nível dos conhecimentos que se adquirem na Carreira Profissional Técnico de Informática ou Técnico de Segurança
- Não apresenta quaisquer pré-requisitos a nível de habilitações académicas ou experiência profissional

---

Metodologia

Constituído por 5 módulos de formação, integrados numa ótica de sessões mistas de teoria e prática. Cada módulo é constituído por um período de formação presencial e acompanhamento permanente e personalizado por parte de um formador. Serão elaborados exercícios e simulações de situações

práticas com resolução individualizada garantindo uma aprendizagem mais eficaz. Os conteúdos ministrados durante o percurso foram desenvolvidos pela GALILEU e Entidades parceiras, e são devidamente acompanhados por manuais, distribuídos aos Participantes.

Composição:

- 119 Horas de Formação
- 4 Ações de Formação TI
- 1 Modulo e-Learning
- 1 Ação de Formação Complementar
- 2 Ações de Preparação para Exame
- 2 Exames de Certificação

Exame

Conheça os **prazos limite para realização do exame de certificação**.

Contacte-nos, caso tenha alguma específica sobre os exames.

Programa

- Fundamentos Kali Linux (e-Learning)
- Ethical Hacking and Countermeasures
- Offensive Penetration Testing Services
- Ação de Preparação para Exame CEH
- Noções básicas de direito + Lei do Cibercrime
- Monitorização, Deteção e Prevenção de Intrusões
- Resposta a Incidentes com Técnicas Forenses
- Ação de Preparação para Exame CompTIA CySA+

Fundamentos Kali Linux (e-Learning)

Dotar os formandos de conhecimentos essencial em Kali Linux e utiliza-lo como ferramenta em testes de intrusão e de defesa a eventuais ataques.

Conteúdos:

- 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

Dotar os formandos com os conceitos e técnicas de Ethical Hacking para poder defender de futuros possíveis ataques, aprendendo a verificar, testar Hackar e proteger os seus próprios sistemas. Aprenderá ainda a cinco fases do Ethical Hacking (Gaining Access, Enumeration, Maintaining Access, and covering your tracks).

Conteúdos:

- 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

Num curso completamente prático, irá ser permitido aos formandos com acompanhamento do formador,

explorar e utilizar algumas das ferramentas mais utilizadas em Ethical Hacking por forma a terem um pleno conhecimento ao nível do que é feito em Red Teams.

Conteúdos:

- 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

Tem como objetivo preparar os formandos o exame CEH da Ec-Council que permitirá alcançar a certificação de Ethical Hacking (CEH).

Noções básicas de direito + Lei do Cibercrime

Monitorização, Deteção e Prevenção de Intrusões

Capacitar os formandos para deteção e monitorização de anomalias que possam indicar comportamentos anómalos e de como uma análise pró-ativa através de uma contante monitorização, análise e prevenção poderá prever e evitar o ataque informático por completo.

Conteúdos:

- 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

Dotar os formandos com os conhecimentos em ferramentas para que possam fazer uma eficaz a deteção, resolução e prevenção de incidentes de segurança.

Conteúdos:

- 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 CySA+

Tem como objetivo preparar os formandos o exame CS0-001 que permitirá alcançar a certificação CompTIA Cybersecurity Analyst (CySA+).