Analista de Segurança

Infrastructure - Cibersegurança

Com certificação

- **Nível:** Avançado
- **Duração:** 119h

Sobre o curso

A **Academia Analista de Segurança** 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.

Razões para frequentar esta Academia:

- Os melhores profissionais certificados do mercado como formadores.
- 2 Certificações reconhecidas Internacionalmente.
- Formação qualificada

Inclui as Certificações:

- Certified Ethical Hacker
- CompTIA Cybersecurity Analyst+

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

Condições

- Taxa de inscrição: 220€, dedutível no valor total.
- Possibilidade de pagamento faseado para particulares, **até 10 prestações, sem juros**.
- Estudantes não residentes no território nacional, terão de efetuar um pagamento de 50% do valor total da propina no momento da inscrição.
- 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 +

O exame EC-Council incluido no valor do curso deve ser obrigatoriamente realizado presencialmente, num dos centros de Exames GALILEU/Rumos.

Caso não tenha disponibilidade ou não pretenda realizar o exame de forma presencial e prefira uma solução remota acresce uma taxa de 75€ ao valor do curso.

Desconto – Profissionais em situação de desemprego

- **10% de desconto** válido **para inscrições a título particular de pessoas que se encontrem em situação de desemprego**, para o efeito, será solicitado **documento comprovativo da situação atual –** Não acumulável com outras campanhas em vigor.

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 Academia Técnico de Segurança
- A Academia 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 live training 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
- 3 Ações de Formação TI
- 1 Ação de Formação Complementar
- 1 CTF
- 2 Ações de Preparação para Exame
- 2 Exames de Certificação
- Momentos de auto-estudo

Exames de Certificação:

- 2 exames de certificação;
- Os exames de certificação deverão ser realizados no final dos respetivos módulos de formação;
- As datas 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 10 dias úteis de antecedência à data pretendida;
- Os exames têm de ser realizados até 6 meses após a data de fim da formação;
- Modalidades dos exames:
  - Exame para certificação CompTIA Cybersecurity Analyst+: poderá optar por realizar em presencial ou remotamente
  - Exame para certificação CEH: na Academia está incluído o exame na modalidade presencial. Caso opte pela modalidade remota terá um custo adicional de 75€ + IVA (Isenção do valor do IVA a particulares)

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

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

Programa

- Auto-estudo dedicado a Linux para Ethical Hackers
- Ethical Hacking and Countermeasures
- Offensive Penetration Testing Services
- Ação de Preparação para Exame CEH

- Case Event Analyst
- Capture The Flag – CTF
- Ação de Preparação para Exame CySA+

Auto-estudo dedicado a Linux para Ethical Hackers

Neste momento de auto-estudo ser-te-ão facultados guiões, ou materiais, que servirão como um roteiro valioso durante a tua jornada individual de aprendizagem e que serão focados nestes tópicos:

- Installing VMWare / Kali Linux
- Kali Linux Overview
- Navigating the File System
- Users and Privileges
- Common Network Commands
- Viewing, Creating, and Editing Files
- Starting and Stopping Services
- Installing and Updating Tools
- Scripting with Bash

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
- Post Exploitation
- Web Application Testing
- Wireless Attacks
  - Lab: Packet capture
  - Lab: Packet Injection
  - Lab: Rogue Access Point

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).

Case Event Analyst

Capacitar os formandos para deteção, monitorização e resposta 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

- Threat and Vulnerability Management
- Software and Systems Security
- Security Operations and Monitoring
- Incident Response
- Compliance and Assessment

Capture the Flag – CTF

Desafio prático de grupo que servirá para testar os conhecimentos e raciocínio lógico dos formandos, ao mesmo tempo que permite que os mesmos apliquem Técnicas e Conceitos adquiridos nos módulos anteriores, tanto a nível de Red Team como a nível de Blue Team.

Ação de Preparação para Exame CompTIA CySA+

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