Cybersecurity Analyst

Infrastructure - Cibersegurança

Com certificação

- **Nível:** Intermédio
- **Duração:** 119h

Sobre o curso

Esta Academia foi projetada para formar profissionais capazes de utilizar de técnicas inovadoras de monitorização, investigação, análise, prevenção e resposta a incidentes e recuperação de desastres.

Os formandos vão poder adquirir conhecimentos nas principais das tendências atuais que afetam o dia a dia dos analistas de segurança. Assim como desenvolverem competências para monitorizar e detectar proativamente atividades maliciosas utilizando os métodos e ferramentas atuais, como threat intelligence, sistemas de informação e gestão de eventos de segurança (SIEM) e resposta orquestrada a ameaças e automatização (SOAR).

Razões para frequentar esta Academia?

- Os melhores profissionais certificados do mercado como formadores
- Formação qualificada, através da Rumos, uma das empresas líderes na área da formação e distinguida "Marca n.º 1 na Escolha dos Profissionais" pela ConsumerChoice
- Acesso ao Employability Hub, um serviço dedicado a apoiar a integração e a progressão de carreira dos formandos das Academias da Rumos. Oferecemos um acompanhamento personalizado, focado na maximização do teu posicionamento no mercado de trabalho.

Inclui a Certificação:

- **CompTIA Cybersecurity Analyst (CySA+)**
  Esta certificação valida a capacidade dos profissionais para detetar, analisar e responder proativamente a ameaças de segurança, com base em monitorização contínua e análise de dados. Inclui áreas como operações de segurança, gestão de vulnerabilidades, resposta a incidentes e comunicação eficaz em ambientes cloud, aplicações web e dispositivos móveis.

Saídas Profissionais:

- Analista de Cibersegurança
- Especialista de Cibersegurança
- Arquiteto de cibersegurança

Diagnóstico de Conhecimentos:

- Faça a nossa avaliação gratuita para verificar se detém os conhecimentos base para garantir uma boa aprendizagem neste curso

---

Destinatários

- Profissionais de cibersegurança
- Arquitetos e administradores de redes
- Administradores de sistemas seniores

Objetivos

- **Análise avançada de ameaças cibernéticas:**
  Desenvolver competências avançadas em análise de ameaças, capacitando os formandos a identificarem e avaliarem eficientemente possíveis ataques, bem como a responder de forma proativa a incidentes de segurança.
- **Implementação de estratégias de defesa:**
  Capacitar os profissionais a projetar e implementar estratégias robustas de defesa cibernética. Isso inclui a compreensão detalhada das melhores práticas de segurança, políticas de controle de acesso, monitoramento de rede e utilização eficaz de ferramentas de segurança.
- **Resposta a incidentes e recuperação de dados:**
  Fornecer conhecimentos especializados em resposta a incidentes cibernéticos, preparando os formandos para lidar com situações de emergência de maneira eficaz. Isso envolve a identificação rápida de ameaças, contenção, erradicação e recuperação de sistemas comprometidos.
- **Desenvolvimento de competências em ferramentas analíticas e tecnologias emergentes:**
  Proporcionar uma compreensão aprofundada e prática de ferramentas analíticas e tecnologias emergentes no campo da segurança cibernética. Isso inclui o uso eficaz de inteligência artificial, machine learning e análise de big data para aprimorar a detecção de ameaças e fortalecer as defesas digitais.

Ao atingir estes objetivos, os participantes da Academia Cybersecurity Analyst estarão preparados para desempenhar papéis cruciais na proteção de sistemas e dados, contribuindo para a segurança global da informação em ambientes corporativos e organizacionais.

Condições

- Taxa de inscrição: 290€, dedutível no valor total do curso.
- Formandos não residentes no território nacional, terão de efetuar um pagamento de 50% do valor total da propina no momento da inscrição.
- Inscrições a título particular de pessoas que se encontrem em situação de desemprego, beneficiam de um desconto de 10%, mediante apresentação de comprovativo da situação atual (não acumulável com outras campanhas em vigor).
- Condições especiais para Alumni de Academias ou Pós-graduações GALILEU.
- Os valores apresentados não incluem IVA. Isenção do valor do IVA a particulares.

Modalidades de Pagamento

- Pronto pagamento: Liquide o valor total do curso no momento da inscrição e beneficie de um desconto adicional de 5%.
- Pagamento faseado sem juros: Liquide a taxa de inscrição e divida o valor restante em até 4 mensalidades diretamente connosco, sem juros ou custos associados.

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;
- Conhecimentos técnicos em ethical hacking e testes de penetração equivalentes ao que são abordados na Academia Penetration Testing;
- O percurso não apresenta quaisquer pré-requisitos a nível de habilitações académicas ou experiência profissional.

Metodologia

- Constituído por módulos de formação, integrados numa ótica de sessões mistas de teoria e prática.
- Serão elaborados exercícios e simulações de situações práticas garantindo uma aprendizagem mais eficaz.
- Os conteúdos ministrados durante o percurso foram desenvolvidos pela Rumos, em consulta a organizações parceiras, e são devidamente acompanhados por material didáctico, distribuídos aos participantes.
- Existem ainda, ao longo da Academia, momentos de autoestudo onde serão facultados guiões, ou materiais, que servirão como um roteiro valioso durante a jornada individual de aprendizagem do formando.

Composição:

- 119 Horas de Formação
- 2 Ações de Formação TI
- 2 Hands-on-Labs
- 1 Ação de Preparação para Exame
- 1 Exame de Certificação: CS0-003
- Momento de auto-estudo

Exame de Certificação:

- O exame de certificação deverá preferencialmente ser realizado no final do respetivo módulo de formação;
- A data é sugerida 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;
- O exame tem de ser realizado até 6 meses após a data de fim da formação.

Programa

- Autoestudo dedicado a Fundamentos de Python
- Segurança no Desenvolvimento de Software
- Wi-Fi Best Practices
- Cloud Security
- Offensive Penetration Testing Services
- CompTIA Cybersecurity Analyst + CertPrep (CySA+)
- Hand-on-Labs: SIEM and SOAR
- Try to Hack Me - Security Analyst (Hands-on Lab)
- Ação de Preparação para Exame CySA+

Autoestudo dedicado a Fundamentos de Python

Neste módulo de autoestudo, os formandos terão uma introdução à programação em Python, explorando conceitos básicos, estruturas de controlo, funções e bibliotecas úteis para tarefas de automação.

Competências desenvolvidas:

- Compreensão dos conceitos fundamentais de Python
- Aplicação de estruturas básicas de programação

Programa:

- O ambiente de desenvolvimento Python
- Python crash course
- Python collections
- Python function

Segurança no Desenvolvimento de Software (17,5h)

Neste módulo, os formandos irão explorar ameaças comuns no desenvolvimento de aplicações, tais como injeções de código, XSS e exposição de dados sensíveis. Serão analisadas técnicas de mitigação, como validação de dados, encriptação e boas práticas de codificação. O conteúdo inclui ainda a integração da segurança no ciclo de vida do desenvolvimento e a aplicação de testes de segurança.

Competências desenvolvidas:

- Identificação de ameaças e vulnerabilidades comuns em software
- Aplicação de boas práticas de desenvolvimento seguro
- Integração de segurança em pipelines de desenvolvimento contínuo

Programa:

- Understanding Key Security Concepts and Common Threats:
    - Explore fundamental security concepts and the most prevalent types of threats.
    - Identify various attack vectors such as injection attacks, cross-site scripting (XSS), and sensitive data exposure.
- Recognizing Defense Techniques and Risk Mitigation:
    - Learn techniques to defend against security threats and mitigate risks in software development.
    - Understand practices like input validation, secure coding guidelines, and encryption to enhance application security.
- Understanding the Software Development Lifecycle and Security:
    - Gain insight into the software development lifecycle and the pivotal role of security at each phase.
    - Explore secure coding practices, security testing, and continuous security integration within the software development process.
- Identifying Challenges in Building Secure Applications:
    - Identify common pitfalls and challenges faced in creating secure applications.
    - Discuss real-world examples of security vulnerabilities in applications and explore strategies to address these issues effectively.

Wi-Fi Best Practices (3,5 h)

Este módulo aborda as principais medidas de proteção aplicadas a redes Wi-Fi, dispositivos Bluetooth e tecnologias NFC. Serão exploradas técnicas de configuração segura, utilização de protocolos de encriptação robustos, emparelhamento seguro e mitigação de riscos associados à utilização destas tecnologias em espaços públicos.

Competências desenvolvidas:

- Configuração segura de redes sem fios
- Aplicação de medidas de proteção em comunicações Bluetooth e NFC
- Identificação de riscos e boas práticas em ambientes públicos

Programa:

- Wireless Network Security Best Practices
- Bluetooth Security Measures
- NFC (Near Field Communication) Security Protocols
- Securing Wireless Communication in Public Spaces

Cloud Security (10,5h)

Este módulo aborda os conceitos fundamentais de Cloud Computing e os principais serviços disponíveis no mercado. Serão explorados os modelos de responsabilidade partilhada entre fornecedores e utilizadores, os benefícios e os riscos da adoção da Cloud, bem como os principais frameworks e boas práticas de cibersegurança aplicados a este contexto.

Competências desenvolvidas:

- Compreensão de modelos e serviços em Cloud
- Identificação de riscos e responsabilidades de segurança
- Aplicação de frameworks e medidas de proteção em ambientes Cloud

Programa

- Cloud Computing Definition and Concepts
- Main Cloud Services and Technologies Landscape
- Shared Responsibility in the Cloud
- Security Benefits of Cloud Computing
- Risks of Cloud Computing
- Cloud Cybersecurity Frameworks and Best Practices

Offensive Penetration Testing Services (17,5h)

Neste módulo prático, os formandos irão utilizar ferramentas como Metasploit e técnicas especializadas para executar ataques simulados em diferentes camadas — redes, aplicações, clientes e sistemas. O foco é desenvolver competências avançadas de exploração, pós-exploração, engenharia social e análise de tráfego.

Competências desenvolvidas:

- Execução de ataques simulados com ferramentas avançadas
- Realização de testes a aplicações web e redes wireless
- Capacidade de análise de tráfego e injeção de pacotes

Programa:

- Using the Metasploit Framework
- Information Gathering

- Finding Vulnerabilities
- Exploitation
- Password Attacks
- Client-Side Exploitation
- Social Engineering
- Post Exploitation
- Web Application Testing
- Wireless Attack
- Lab: Packet capture
- Lab Packet Injection
- Lab: Rogue Access Point

CompTIA Cybersecurity Analyst+ CertPrep (CySA+) (35h)

Este módulo foca-se na deteção de ameaças através da análise de comportamento de redes e sistemas. Os formandos vão aprender a realizar atividades de threat hunting, gestão de vulnerabilidades, operações de segurança e resposta a incidentes. Inclui ainda conteúdos de conformidade, monitorização e aplicação de boas práticas organizacionais.

Competências desenvolvidas:

- Aplicação de técnicas de threat hunting e análise de malware
- Gestão de vulnerabilidades e resposta a incidentes
- Preparação para a certificação CompTIA CySA+

Programa:

- Understanding Vulnerability Response, Handling, and Management
- Exploring Threat Intelligence and Threat Hunting Concepts
- Explaining Important System and Network Architecture Concepts
- Understanding Process Improvement in Security Operations
- Implementing Vulnerability Scanning Methods
- Performing Vulnerability Analysis
- Demonstrating Incident Response Communication
- Applying Tools to Identify Malicious Activity
- Analysing Potentially Malicious Activity
- Understanding Application Vulnerability Assessment
- Exploring Scripting Tools and Analysis Concepts
- Understanding Application Security and Attack Mitigation Best Practices

SIEM and SOAR (Hands-on Lab) (14h)

Através de um conjunto de exercícios práticos, os formandos vão configurar e utilizar ferramentas SIEM e SOAR para recolher, analisar e correlacionar eventos de segurança. Será também abordada a resposta automática a

incidentes e a integração entre diferentes sistemas.

Competências desenvolvidas:

- Configuração básica e avançada de soluções SIEM
- Implementação de fluxos automatizados com SOAR
- Análise de eventos e resposta a incidentes

Programa

- SIEM Overview
- Basic SIEM Configuration
- Hands-on Lab: Initial SIEM Setup
- Advanced Analysis with SIEM
- Introduction to SOAR
- Hands-on Lab: SIEM and SOAR Integration
- Automated Response with SOAR
- Best Practices and Case Studies

Try to Hack Me – Security Analyst (Hands-on Lab) (14h)

Neste laboratório, os formandos serão desafiados a aplicar metodologias de deteção, análise e mitigação de ameaças em ambientes simulados. Através da plataforma “Try to Hack Me”, serão recriados cenários reais de ciberataques, nos quais os formandos devem atuar como analistas de segurança.

Competências desenvolvidas:

- Deteção e análise de ameaças em tempo real
- Aplicação de medidas defensivas em ambientes simulados
- Fortalecimento das competências de um analista de SOC

Ação de Preparação para Exame CompTIA CySA+ (7h)

Esta sessão é dedicada à revisão dos tópicos mais relevantes do exame CySA+ (CS0-003). Serão abordadas estratégias de resolução de questões, técnicas de gestão de tempo e reforço de áreas críticas, proporcionando maior confiança e preparação para a certificação.

Competências desenvolvidas:

- Revisão focada de tópicos chave
- Estratégias práticas para resolução do exame
- Preparação direcionada para obtenção da certificação