Curso: Academia Cybersecurity Analyst

Duração: 119h
Área formativa: Cursos

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).

Porque quero frequentar esta Academia?

:: Os melhores profissionais certificados do mercado como formadores.

:: 1 Certificação reconhecida internacionalmente.

:: Formação qualificada, através da Rumos. Uma das empresas lideres na área da formação.

:: Acesso ao **Employability Hub**, um serviço dedicado a apoiar a integração e a progressão de carreira dos formandos das Academias da FLAG. Oferecemos um acompanhamento personalizado, focado na maximização do teu posicionamento no mercado de trabalho. Descobre mais sobre o Employability Hub aqui.

Que certificação vou obter?

:: CompTIA Cybersecurity Analyst+

Que profissões me esperam?

:: Analista de Cibersegurança

:: Especialista de Cibersegurança

:: Arquiteto de cibersegurança

Objectivos

:: 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.

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

:: 6 Ações de Formação TI

:: 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.

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 Tester;

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

Diagnóstico de Conhecimentos
Faça a nossa avaliação gratuita para verificar se detém os conhecimentos base para garantir uma boa aprendizagem neste curso.

Destinatários

A Academia Cybersecurity Analist destina-se a:

:: Profissionais de cibersegurança

:: Arquitetos e administradores de redes

:: Administradores de sistemas seniores

Programa

Autoestudo dedicado a Fundamentos de Python

Neste momento de autoestudo, os formandos vão ter a oportunidade de aprender os fundamentos da linguagem Python.

Segurança no desenvolvimento de Software (17,5h)

Este módulo irá proporcionar uma compreensão ao nível do desenvolvimento seguro de software através de uma análise do ciclo de vida do desenvolvimento de software, integrando práticas seguras de codificação, testes de segurança e integração contínua de segurança. Adicionalmente, serão identificados e discutidos desafios comuns na construção de aplicações seguras.

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 (3,5h)

Neste módulo vamos realçar as boas práticas essenciais para proteger redes sem fios e comunicações Bluetooth e NFC. Vamos começar com as configurações seguras de redes Wi-Fi, destacando a importância da criptografia robusta e senhas seguras. Em seguida, exploraremos técnicas de emparelhamento seguro para dispositivos Bluetooth e protocolos de segurança NFC, garantindo transações seguras. Abordaremos também o uso seguro dessas tecnologias em espaços públicos, realçando os riscos e as medidas preventivas necessárias.

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)

Neste módulo serão explorados os princípios fundamentais relacionados com Cloud Computing, abrangendo conceitos e definições essenciais. Este módulo tem como objetivo dar a conhecer os principais serviços Cloud disponíveis no mercado, explicar os modelos de responsabilidade partilhada entre fornecedores e utilizadores de serviços Cloud, bem como analisar os benefícios e riscos inerentes a estas tecnologias. Adicionalmente, serão abordados os frameworks e as melhores práticas de cibersegurança para a Cloud, capacitando os formandos a tomar decisões informadas e implementar medidas de segurança eficazes 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 (24,5h)

Neste módulo inteiramente prático, com o acompanhamento do formador, os formandos vão explorar e utilizar algumas das ferramentas avançadas mais utilizadas em Ethical Hacking de forma a terem um pleno conhecimento ao nível do que é feito em Red Teams.

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 está focado na análise comportamental às redes para melhorar o estado geral da segurança, identificando e combatendo malware e ameaças persistentes avançadas (APTs),

resultando numa visibilidade aprimorada das ameaças numa superfície de ataque alargada. Contribuirá para capacitar um profissional de TI na defensa proactivamente e melhorar continuamente a segurança de uma organização.

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
- Communicating Vulnerability Information
- Explaining Incident Response Activities
- Demonstrating Incident Response Communication
- Applying Tools to Identify Malicious Activity
- Analyzing Potentially Malicious Activity
- Understanding Application Vulnerability Assessment
- Exploring Scripting Tools and Analysis Concepts
- Understanding Application Security and Attack Mitigation Best Practices

Hand-on Labs: SIEM and SOAR (14h)

Neste módulo, os formandos vão trabalhar num conjunto de exercícios para proporcionar uma compreensão abrangente dos Sistemas de Informação e Gestão de Eventos de Segurança (SIEM) e Resposta Orquestrada a Ameaças e Automatizada (SOAR).

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

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

Esta sessão tem como objetivo preparar os formandos no esclarecimento de dúvidas para o exame CS0-003 que permitirá alcançar a certificação CompTIA Cybersecurity Analyst (CySA+).

Capture the Flag – CTF (7h)

Desafio prático de grupo que servirá para testar os conhecimentos e raciocínio lógico dos formandos, enquanto permite que os mesmos apliquem Técnicas e Conceitos adquiridos nos módulos anteriores,

tanto a nível de Red Team como a nível de Blue Team.