Cyber Security

Infrastructure - Cibersegurança

Live Training (também disponível em presencial)

Com certificação

- **Localidade:**
- **Data:** 25 Sep 2024
- **Preço:** 6820 € (POSSIBILIDADE DE PAGAMENTO FASEADO ATÉ 12 MENSALIDADES
  Os valores apresentados não incluem IVA. Oferta de IVA a particulares.)
- **Horário:** Pós-Laboral das 2ª, 4ª e 6ª feiras das 18h45 às 22h15
- **Nível:** Intermédio
- **Duração:** 350h

Sobre o curso

A Academia Cybersecurity está desenhada para desenvolver competências técnicas avançadas em cibersegurança, ao formar e certificar os formandos numa das áreas mais críticas e maior crescimento a nível mundial.

Com uma abordagem imersiva e uma forte componente prática nos principais domínios de ataque e defesa em cibersegurança, o programa deste percurso de formação é constituído por vários módulos que vão explorar diferentes especializações e verticalidades da área da segurança informática aplicadas à realidade do mercado profissional.

Os formandos vão poder consolidar as principais frameworks de segurança informática e evoluírem passo a passo aplicando diferentes técnicas avançadas e abordagens tais como: Ethical hacking, testes de penetração e vulnerabilidade, análise e auditoria da conformidade dos sistemas de informação, entre muitos outros desafios.

Através de laboratórios *hands-on* e outros desafios práticos, os formandos vão poder adquirir as principais competências críticas que as organizações procuram na atualidade e poderem assim integrar equipas e projetos de cibersegurança.

Razões para frequentar esta Academia?

- Formação imersiva e com forte componente prática nos principais domínios de ataque e defesa em cibersegurança
- 3 Certificações reconhecidas internacionalmente

- Os melhores profissionais certificados do mercado como formadores
- Possibilidade de estágio no final da formação
- Formação qualificada

Inclui as Certificações:

- **CompTIA PenTest+**
  Esta acreditação reconhece profissionais de cibersegurança com competências práticas para identificar, mitigar e reportar vulnerabilidades em sistemas. Abrange todas as fases dos testes de penetração em diferentes superfícies de ataque, incluindo cloud, aplicações web, APIs e dispositivos IoT.
- **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.
- **ISO/IEC 27001**
  Reconhecida como uma das normas mais importantes na segurança da informação, a certificação ISO/IEC 27001 da PECB valida competências para implementar, gerir e melhorar um Sistema de Gestão da Segurança da Informação (SGSI). Baseada numa abordagem de gestão de risco, permite assegurar a confidencialidade, integridade e disponibilidade da informação, promovendo a melhoria contínua dos processos organizacionais.
- **Certificação Rumos Expert (CRE): CyberSecurity Engineer**
  Através da realização de um projeto prático baseado em cenários reais e tarefas do dia-a-dia, esta certificação prática valida a aplicação das competências técnicas e o desempenho no terreno de um CyberSecurity Engineer.

Saídas Profissionais:

- Especialista de Cibersegurança
- Consultor de Cibersegurança
- Administrador de Segurança Informática
- Penetration & Vulnerability Tester
- Analista de Cibersegurança
- Cyber Security Engineer
- Auditor de Segurança da Informação
- Chief Information Security Officer (CISO)

Estágio:

Esta Academia inclui a possibilidade de estágio, após a conclusão da formação mediante a realização dos exames de Certificação com aproveitamento.

Destinatários

Destina-se a todos os interessados em aprofundar os seus conhecimentos de redes e sistemas com especialização em cibersegurança.

Objetivos

- Preparar profissionais de cibersegurança capazes de dominar as principais ferramentas, técnicas de análise e de conformidade na segurança dos sistemas de informação.
- Dotar os formandos com conhecimentos de implementação de soluções de monitorização, análise e prevenção de intrusões. Lidar com sistemas críticos e criar planos de resposta a incidentes e recuperação de desastres. Desenvolver competências na resposta a novas ameaças. Realizar análises de vulnerabilidades e testes de intrusão. Compreender e dominar as estratégias de ataque e defesa de diferentes ângulos ao imitar as estratégias de ataque de hackers maliciosos.
- Desenvolver e capacitar os formandos com conhecimentos sólidos nas principais práticas de codificação em testes de segurança e integração contínua para o desenvolvimento de software. Configuração e proteção de redes Wi-Fi com técnicas robustas e seguras. Implementação de medidas de segurança eficazes em ambientes Cloud. Utilizar ferramentas avançadas em testes de penetração ofensiva. Utilizar ferramentas de Inteligência Artificial (IA) aplicadas à cibersegurança.
- Compreender Sistemas de Informação e Gestão de Eventos de Segurança (SIEM) e Resposta Orquestrada a Ameaças e Automatizada (SOAR). Capacitar os participantes para a análise de ameaças e vulnerabilidades em redes e sistemas e na defesa proativa da segurança de uma organização.
- Desenvolver competências na implementação de frameworks internacionais e das principais normas de conformidade para segurança de informação: DevSecOps, Normas ISO/IEC 27001/27002, Regulamento Geral de Proteção de Dados (RGPD), Digital Operational Resilience Act – DORA, Network and Information Security Directive 2 – NIS2 e Cyber Resilience Act (CRA).
- Criar oportunidades de networking para os formandos construírem uma rede de contatos estratégica com outros formandos e profissionais especialistas em cibersegurança, fomentando colaborações futuras e oportunidades de carreira.
- Certificar as competências técnicas adquiridas através da obtenção de certificações internacionais.

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 12 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;
- São ainda requeridos conhecimentos técnicos de informática e redes, ao nível dos conhecimentos que se adquirem na Academia Técnico de Informática;
- 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. Cada módulo é constituído por um período de formação síncrono e acompanhamento permanente e personalizado por parte de um formador.
- 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 didático, 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:

- 14 Ações de Formação TI
- 3 Módulos de conhecimento complementar

- 3 Ações de Preparação para Exame
- 3 Exames de Certificação Internacional
- 1 Exame de Certificação Rumos
- 5 Hands-on-Labs
- 3 Momentos de auto-estudo

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 das certificações CompTIA e ISO/IEC 27001 têm de ser realizados até 6 meses após a data de fim da Academia.

Certificação Rumos

Baseada em casos práticos da vida real dos profissionais, esta certificação permite demonstrar a detenção de conhecimentos e competências autênticos. Para isso, o formando é sujeito à realização de um projeto que é espelho das tarefas realizadas pelos profissionais no seu dia-a-dia.

O formando é presente a um exame prático sobre as matérias lecionadas e com avaliação presencial. Após avaliação positiva, este obterá um Certificado Rumos que atesta as competências na respetiva área.

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

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

Programa

- NIST Cybersecurity Framework
- Autoestudo dedicado a Fundamentos de PowerShell e Scripting
- Systems Hardening
- Noções básicas de direito + Lei do Cibercrime
- Autoestudo dedicado a Linux for Ethical Hackers
- CompTIA PenTest+ CertPrep
- Ethical Hacking for Mobile
- Try to Hack Me - Penetration Tester (Hands-on Lab)
- Ação de Preparação para Exame PenTest+
- Autoestudo dedicado a Fundamentos de Pyhton
- 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+
- AI in Cybersecurity
- DevSecOps Foundation
- ISO/IEC 27001 Foundation
- Ação de Preparação para Exame ISO/IEC 27001
- Fundamentos de Proteção de Dados - RGPD
- Network and Information Security Directive 2 - NIS2
- Seminário: Digital Operational Resilience Act - DORA
- Cyber Resilience Act - CRA
- Try to Hack Me - Security Engineer (Hands-on Lab)
- Certificação Rumos Expert (CRE): Cyber Security Engineer

Apresentação

Sessão de boas-vindas para esclarecimento de todos os processos e procedimentos existentes.

NIST: Cybersecurity Framework (21h)

A primeira etapa para quem está a iniciar-se ou a especializar-se em cibersegurança, é conhecer as boas práticas reconhecidamente eficazes pelos profissionais.

Este módulo estabelece os alicerces para a compreensão estruturada da cibersegurança, através do estudo do NIST Cybersecurity Framework. Desenvolvido pelo National Institute of Standards and Technology (NIST), este referencial tem como objetivo auxiliar organizações a identificar, proteger, detetar, responder e recuperar de incidentes de segurança. Os formandos irão explorar os cinco pilares do framework e a sua aplicabilidade prática, bem como outros referenciais relevantes.

Competências desenvolvidas:

- Compreensão dos componentes e objetivos do NIST Framework
- Capacidade de aplicar o modelo às operações de segurança de uma organização
- Conhecimento das interligações entre o NIST e outras normas e frameworks

Programa:

- What is the NIST Cybersecurity Framework, and how can it be used by an organization.
- History and Creation of the Framework
- Uses and Benefits of the Framework
- Cybersecurity Framework Components
- The Five Functions of the Framwork
    - Identify
    - Protect
    - Detect
    - Respond
    - Recover

- Other related frameworks and standards

Autoestudo dedicado a Fundamentos de PowerShell e Scripting

Neste momento de autoestudo, os formandos serão introduzidos ao ambiente PowerShell, explorando os conceitos básicos de scripting e a execução de tarefas automatizadas. Este conhecimento é particularmente útil para administradores de sistemas e profissionais de segurança que operam em ambientes Microsoft, nomeadamente em contextos de análise, auditoria e exploração de sistemas.

Competências desenvolvidas:

- Execução de comandos em PowerShell
- Criação e execução de scripts simples
- Aplicação prática em tarefas de administração e segurança

Programa:

- Introduction to PowerShell
- Introduction to scripting in PowerShell
- Create and run scripts by using Windows PowerShell

Systems Hardening (28h)

Neste módulo serão abordadas práticas e ferramentas destinadas à proteção proativa de sistemas, com foco na eliminação de vulnerabilidades e na aplicação de políticas de segurança robustas. Serão exploradas estratégias de hardening aplicadas a vários níveis — desde aplicações e sistemas operativos, até bases de dados, redes e endpoints. O módulo inclui ainda a utilização de ferramentas para avaliação e medição da conformidade com baselines de segurança.

Competências desenvolvidas:

- Compreensão dos conceitos e objetivos do hardening
- Aplicação de medidas práticas de endurecimento de sistemas
- Utilização de ferramentas de avaliação de segurança e benchmarks

Programa:

- Introduction to Systems Hardening
- Security Baselines
- Security Protocols and Specifications
- Vulnerability Assessment Tools
- Tools for assessment, measurement, and enforcement of security baselines
- Systems Hardening
- Application hardening
- Operating system hardening
- Endpoint hardening
- Server hardening
- Database hardening

- Network hardening

Noções básicas de direito + Lei do Cibercrime (7h)

Este módulo tem como finalidade sensibilizar os formandos para o enquadramento legal da cibersegurança, nomeadamente através da introdução a conceitos básicos de direito e ao estudo da Lei do Cibercrime. Serão analisados os principais tipos legais, responsabilidades individuais e institucionais, bem como as implicações do incumprimento legal.

Competências desenvolvidas:

- Conhecimento do enquadramento jurídico da cibersegurança
- Compreensão da Lei do Cibercrime e das suas aplicações
- Consciência das responsabilidades legais na área da segurança da informação

Programa:

- Noções básicas de direito
- Lei do Cibercrime

Autoestudo dedicado a Linux for Ethical Hackers

Neste momento de autoestudo, os formandos serão introduzidos à utilização do Kali Linux, uma distribuição amplamente utilizada em testes de intrusão. O conteúdo inclui instalação, navegação no sistema de ficheiros, gestão de utilizadores e serviços, comandos de rede e introdução ao scripting em Bash.

Competências desenvolvidas:

- Familiarização com o ambiente Kali Linux
- Execução de comandos básicos de administração e redes
- Introdução ao desenvolvimento de scripts em Bash

Programa:

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

CompTIA PenTest+ CertPrep (35h)

Neste módulo são abordadas as principais fases de um teste de intrusão: planeamento, reconhecimento, análise de vulnerabilidades, exploração e report. Os formandos vão utilizar ferramentas e técnicas modernas de Ethical Hacking, com o objetivo de compreender como os ataques ocorrem e como mitigá-los. É também dado ênfase à

preparação para o exame CompTIA PenTest+ (PT0-003).

Competências desenvolvidas:

- Planeamento e execução de testes de penetração
- Exploração de vulnerabilidades em redes, aplicações e sistemas
- Elaboração de relatórios técnicos e comunicação de resultados

Programa:

- Introduction
- Penetration Testing
- Planning and Scoping Penetration Tests
- Information Gathering
- Vulnerability Scanning
- Analyzing Vulnerability Scans
- Exploit and Pivot
- Exploiting Network Vulnerabilities
- Exploiting Physical and Social Vulnerabilities
- Exploiting Application Vulnerabilities
- Exploiting Host Vulnerabilities
- Reporting and Communication
- Scripting for Penetration Testing

Ethical Hacking for Mobile (14h)

Este módulo aborda as particularidades da segurança em plataformas móveis, com especial enfoque no sistema operativo Android. Serão exploradas vulnerabilidades comuns em aplicações móveis, bem como técnicas de engenharia reversa, modificação de aplicações e análise estática e dinâmica. Os formandos irão preparar ambientes de teste realistas, utilizando dispositivos físicos e virtuais, e aplicar ferramentas como APKTool, MobSF e Burp Suite para identificar e explorar falhas de segurança.

Competências desenvolvidas:

- Identificação de vulnerabilidades e falhas de segurança em aplicações móveis
- Aplicação de técnicas de engenharia reversa e modificação de aplicações Android
- Utilização de ferramentas de análise estática e dinâmica em ambiente controlado

Programa:

- Preparação do ambiente para testes de aplicações móveis
- Utilização de dispositivos Android físicos e virtuais (AVDs)
- Arquitetura e componentes do sistema Android (Dalvik, ART, JNI)
- Modelo de permissões e segurança do Android
- Utilização da linha de comandos (CLI) para interação com o sistema
- Anatomia e estrutura de um pacote APK
- Engenharia reversa de aplicações Android
- Modificação, recompilação e assinatura de aplicações

- Ferramentas de engenharia reversa: APKTool, SMALI, Dex2jar, JD-GUI, apksigner
- Técnicas de bypass de controlos de segurança
- Análise automatizada com QARK e MobSF
- Instalação e configuração do Android Studio e Android Virtual Devices
- Integração do Burp Suite para análise dinâmica de tráfego
- Estudo de caso prático: identificação e exploração de vulnerabilidades em app simulada

Try to Hack Me – Penetration Tester (Hands-on Lab) (14h)

Este laboratório prático permite aos formandos aplicar técnicas e ferramentas utilizadas por equipas Red Team, através de desafios reais na plataforma "Try to Hack Me". O foco está na exploração de vulnerabilidades, escalada de privilégios e reporte de falhas de segurança.

Competências desenvolvidas:

- Aplicação de técnicas de Ethical Hacking em ambiente simulado mas próximos dos reais
- Utilização prática de ferramentas de ataque
- Capacidade de análise e exploração de vulnerabilidades

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

Durante esta ação, serão revistos os conteúdos principais do exame, esclarecidas dúvidas e abordadas boas práticas para a realização da prova. Serão ainda partilhadas estratégias de gestão de tempo e de abordagem a questões típicas.

Competências desenvolvidas:

- Consolidação dos conhecimentos essenciais para o exame
- Identificação de áreas críticas a reforçar
- Preparação estratégica para certificação CompTIA PenTest+

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

AI in Cybersecurity (7h)

Este módulo aborda o impacto crescente da Inteligência Artificial na cibersegurança, explorando tanto o seu potencial defensivo como os riscos associados à sua utilização maliciosa. Os formandos irão analisar o papel da IA na deteção e resposta a ameaças, as ferramentas e técnicas baseadas em modelos de machine learning e linguagem natural, e as implicações legais e éticas do seu uso. O módulo inclui ainda um conjunto de casos práticos e ferramentas aplicadas em contextos reais de segurança.

Competências desenvolvidas:

- Identificação de aplicações práticas e riscos da utilização de IA em cibersegurança
- Utilização de ferramentas e modelos de IA para apoio à análise e resposta a ameaças
- Interpretação de regulamentações e desafios éticos associados à IA

Programa:

- Fundamentos e Cenário de Ameaças
- Introdução Estratégica à IA na Cibersegurança

    - Desmistificar a IA: Diferenças práticas entre IA, Machine Learning e Deep Learning, com analogias para públicos não técnicos.
    - A natureza dual da IA: Introdução ao paradigma “IA para Defesa vs. IA para Ataque” desde o início.
- O Ecossistema de Risco da IA
    - Categoria de Risco 1: IA como Arma
    - Categoria de Risco 2: Ataques à IA (IA Adversária)
    - Categoria de Risco 3: Riscos Operacionais e de Governance
- Governança, Ferramentas e Conformidade
- Panorama de Ferramentas e Aplicações Práticas
    - Aplicação da IA em SIEM, SOAR, EDR/XDR, Segurança de Rede, UEBA, e Threat Intelligence
    - Como avaliar uma ferramenta com “IA”
- Ética, Legislação e Conformidade
    - Desafios Éticos enquanto Risco Empresarial: Responsabilização, transparência e equidade
    - EU AI Act
    - Modelos de Governance
    - O papel das autoridades
    - Passos para a conformidade

DevSecOps Foundation (17,5h)

Este módulo fornece uma visão abrangente das práticas DevSecOps, destacando a importância da segurança desde o início do desenvolvimento até à operação. Serão abordadas ferramentas e processos como threat modeling, secure code review, integração contínua (CI/CD) e análise de vulnerabilidades. Os formandos irão ainda compreender como promover a colaboração entre equipas de desenvolvimento, operações e segurança.

Competências desenvolvidas:

- Aplicação de práticas seguras em pipelines CI/CD
- Identificação e mitigação de vulnerabilidades desde o desenvolvimento
- Promoção da cultura DevSecOps nas organizações

Programa:

- AppSec Fundamentals
- The history behind software development practices and how they’ve evolved over the years
- The importance of this field and the concepts of what makes DevSecOps
- DevSecOps culture and as a discipline
- Introdution Threat Modeling
- Introdution
- Why Threat Model?
- Process overview
- Models
- Deep dive of threats (STRIDE)
- Tools
- Introdution Secure Code Review
- Code Review

- Phylosophy
- Methodology
- Perform Secure Code Review
- Tools
- CI-CD integration life-cycle
- Introdution to GitHub Actions
- Secret Scanning
- SAST
- SCA
- IAC
- DAST
- How to perform hardening images
- How to perform a gap analyses
- Review Owasp top 10 CI-CD Attacks
- CI-CD arquitecture implementation.

ISO/IEC 27001 Foundation – PECB (14h)

Os formandos irão conhecer os elementos essenciais para a implementação e gestão de um SGSI, com base na norma ISO/IEC 27001. Serão explorados temas como políticas de segurança, controlos, auditoria interna e melhoria contínua. O módulo prepara também os participantes para o exame de certificação ISO/IEC 27001 Foundation.

Competências desenvolvidas:

- Compreensão dos requisitos da norma ISO/IEC 27001
- Conhecimento de controlos e objetivos de segurança da informação
- Preparação para a certificação ISO/IEC 27001 Foundation

Programa:

- Introdução, contexto e definições
- Principais publicações
- Liderança e suporte ao SGSI
- Planeamento e operação do SGSI
- Objetivos de controlo e controlos de segurança da informação (Parte 1)
- Objetivos de controlo e controlos de segurança da informação (Parte 2)
- Obtenção da Certificação ISO/IEC 27001

Ação de Preparação para Exame PECB ISO/IEC 27001:2022 Foundation (7h)

Durante esta ação de preparação, serão abordados os conteúdos mais relevantes da norma ISO/IEC 27001, com esclarecimento de dúvidas, simulação de questões e estratégias práticas para maximizar o sucesso no exame.

Competências desenvolvidas:

- Consolidação dos principais tópicos da norma
- Prática de resolução de questões de exame

- Planeamento estratégico para a obtenção da certificação

Fundamentos de Proteção de Dados – RGPD (7h)

Neste módulo serão analisadas as bases legais do RGPD, os direitos dos titulares dos dados, o papel do Encarregado de Proteção de Dados (DPO), as obrigações das organizações e as consequências de incumprimento. O objetivo é dotar os formandos de conhecimento prático para aplicar o regulamento em ambientes reais.

Competências desenvolvidas:

- Interpretação dos princípios do RGPD
- Identificação de responsabilidades e obrigações legais
- Aplicação prática de medidas de conformidade

Programa:

- European Legislative Process
- Essential Definitions – Personal Data and Privacy concepts and principles
- Responsibilities
- Data Subject Rights
- Data Protection Officer (DPO) role
- Data Breach Management
- Sanctions, Fines, and Administrative Procedures
- Privacy by Design vs. Privacy by Default

Network and Information Security Directive 2 – NIS2 (14h)

Este módulo aborda a estrutura e os requisitos da diretiva NIS2, com foco nos operadores de serviços essenciais e prestadores de serviços digitais. Serão exploradas políticas, gestão de riscos, continuidade de negócio, tratamento de incidentes e aspetos éticos e legais relacionados com a segurança das redes e da informação.

Competências desenvolvidas:

- Interpretação dos requisitos da NIS2
- Planeamento de medidas de conformidade
- Aplicação de boas práticas em cibersegurança organizacional

Programa:

- Introduction to the Network and Information Security Directive 2 (NIS2)
- Structure and requirements
- Essential Service Operators and Digital service Providers
- Policies
- Risk analysis and Incident handling
- Business continuity and crisis management
- Best practices in Cybersecurity
- Ethical and Legal Aspects of NIS2

Seminário: Digital Operational Resilience Act – DORA (3,5h)

Neste seminário serão apresentados os objetivos e pilares do DORA, a sua articulação com outras regulamentações da UE, os desafios da sua implementação e as entidades afetadas. Os formandos terão uma visão clara sobre as exigências de gestão de incidentes, governança e terceiros prestadores de serviços.

Competências desenvolvidas:

- Compreensão dos principais elementos do DORA
- Identificação de entidades abrangidas e obrigações
- Avaliação dos desafios de implementação

Programa:

- DORA introduction
    - Main objectives and obligations
    - EU Context
    - Timeline and application
- Entities Affected by DORA
- DORA obligations
    - Key pillars
    - Incident Management
    - Governance
    - Third parties' management
- Challenges in DORA Implementation
    - Best practices
    - Deliverables
- Main Challenges

Cyber Resilience Act – CRA (7h)

Os formandos irão analisar o enquadramento legal do CRA, os requisitos de segurança, as obrigações de notificação e as melhores práticas para assegurar a conformidade. O módulo permite compreender o impacto transversal desta legislação na cadeia de fornecimento digital e na proteção do consumidor.

Competências desenvolvidas:

- Compreensão das exigências legais do CRA
- Aplicação de práticas de conformidade em produtos digitais
- Interpretação de implicações para fabricantes e utilizadores

Programa:

- Understanding the Cyber Resilience Act (CRA)
- Framework and regulatory landscape
- Requirements and main objectives
- Impacts on manufacturers and user
- Notification requirements

- Best practices for compliance and implementation
- Cross-Border perspectives
- Enhancing Consumer Protection

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

Neste laboratório prático, os formandos irão trabalhar em cenários avançados de defesa de infraestruturas, com foco na identificação de vulnerabilidades, aplicação de medidas corretivas e monitorização de sistemas. Utilizando a plataforma "Try to Hack Me", terão contacto com tarefas típicas do dia a dia de um Security Engineer.

Competências desenvolvidas:

- Implementação de medidas de proteção de sistemas e redes
- Monitorização de infraestruturas e resposta a ameaças
- Prática de defesa em ambientes simulados

Certificação Rumos Expert (CRE): Cyber Security Engineer (14h)

A Certificação Rumos Expert (CRE) consiste na resolução de um caso prático inspirado em desafios reais do setor. Os formandos aplicam os conhecimentos desenvolvidos em contextos técnicos e normativos, sendo avaliados por um júri. Esta certificação atesta o domínio técnico e a preparação para funções como Cyber Security Engineer.

Competências desenvolvidas:

- Integração de conhecimentos técnicos e normativos
- Capacidade de resolver desafios práticos de segurança
- Validação final das competências profissionais

Sessão de Encerramento

Esta sessão marca o final do percurso formativo, promovendo a partilha de experiências entre formandos e equipa pedagógica. São apresentados os principais destaques da Academia, feedback recolhido, resultados obtidos e oportunidades de progressão profissional no setor da cibersegurança.

Objetivos:

- Reflexão sobre a aprendizagem e evolução individual
- Reforço da rede de contactos profissionais
- Planeamento de próximos passos na carreira em cibersegurança