Starting Point de Cibersegurança

Starting Points

- **Nível:** Entrada
- **Duração:** 24h

Sobre o curso

O curso Starting Point de Cibersegurança é ideal para quem deseja iniciar uma carreira em segurança informática ou consolidar competências de base em proteção de sistemas e dados.

A formação permite desenvolver, de forma prática, competências essenciais em sistemas operativos (Windows e Linux), redes e protocolos, gestão de dados, resposta a incidentes e automação de tarefas de segurança, proporcionando uma base sólida para quem pretende evoluir para áreas de cybersecurity operations, suporte técnico ou administração de sistemas.

Durante o curso, os participantes terão acesso aos materiais oficiais CompTIA, que incluem um assessment online. Quem concluir com sucesso este assessment, poderá obter o badge oficial “CompTIA A+ Cyber”, emitido pela CompTIA.

Destinatários

O curso destina-se a:

- Profissionais em início de carreira em Tecnologias de Informação que pretendam adquirir fundamentos de cibersegurança.
- Estudantes ou recém-formados que queiram construir uma base prática para ingressar no setor.
- Técnicos de suporte, helpdesk ou administração de sistemas que desejem evoluir para funções de segurança informática.
- Qualquer profissional que, não tendo experiência avançada em segurança, necessite de compreender os princípios fundamentais para funções de proteção de sistemas e dados.

Objetivos

- Compreender os principais papéis e responsabilidades no domínio da cibersegurança.
- Administrar e proteger sistemas Windows e Linux em contexto organizacional.
- Configurar e proteger redes locais, clientes e infraestruturas empresariais.

- Identificar e mitigar ameaças, vulnerabilidades e riscos de segurança.
- Implementar práticas de backup, gestão de dados e privacidade da informação.
- Explorar protocolos de comunicação, serviços cloud e dispositivos IoT em segurança.
- Aplicar controlos de segurança, responder a incidentes e reforçar a resiliência operacional.
- Utilizar ferramentas de análise de rede e automação básica para apoio a tarefas de segurança.

Pré-requisitos

- Conhecimentos básicos de informática na ótica do utilizador.
- Conhecimentos de Inglês técnico: é aconselhável que o formando seja capaz de compreender manuais técnicos na língua inglesa.
- Recomenda-se familiaridade geral com ambientes Windows e noções elementares de redes informáticas.
- Não é exigida experiência prévia em programação ou administração de sistemas.

Metodologia

Este curso b-learning é constituído por módulos de formação síncronos (online em tempo real) e assíncronos (e-learning):

- Formação síncrona com formador em sala online, para a realização de Technical Labs
- Formação autónoma em autoestudo com acesso a recursos e-learning

---

Programa

- Introdução à Cibersegurança e Funções de Suporte
- Administração de Windows I (Computadores e Contas)
- Administração de Windows II (Aplicações, Armazenamento e Gestão de Dados)
- Fundamentos de Redes I (Clientes e Navegação Segura)
- Fundamentos de Redes II (Infraestrutura Empresarial e Segurança)
- Fundamentos de Redes III (Aplicações, Cloud e IoT)
- Controlo e Automação em Ciber

Introdução à Cibersegurança e Funções de Suporte

Neste módulo, os formandos obtêm uma visão global da cibersegurança, dos principais papéis numa equipa e da forma como lidam com ameaças, vulnerabilidades e riscos. Os formandos irão aprender o funcionamento de um "SOC" (Security Operations Center), a classificar diferentes tipos de ameaças e a reconhecer a importância do trabalho em equipa.

Módulo e-learning

- Funções de suporte em cibersegurança
- Ameaças de segurança, vulnerabilidades e riscos

Technical Lab – 3h

- Identificar diferentes funções numa equipa de cibersegurança e mapear responsabilidades.
- Analisar e classificar ameaças reais ou simuladas (Who, Why, How, What).
- Avaliar riscos básicos em cenários práticos e propor medidas de mitigação.
- Simular o funcionamento de um Security Operations Center (SOC) em resposta a alertas.

Administração de Windows I (Computadores e Contas)

Neste módulo, os formandos aprendem competências de administração básica em sistemas Windows, nomeadamente na configuração, gestão e proteção de computadores e contas de utilizador. Este módulo fornece os fundamentos para compreender a gestão de sistemas operativos, essenciais para garantir ambientes seguros e estáveis em qualquer organização.

Módulo e-learning

- Gerir computadores Windows

Technical Lab – 3h

- Configurar e gerir computadores Windows em ambiente organizacional.
- Utilizar ferramentas de administração (GUI e CLI) para tarefas de gestão.
- Configurar contas de utilizador e aplicar políticas de segurança.
- Implementar boas práticas de segurança e realizar troubleshooting básico.

Administração de Windows II (Aplicações, Armazenamento e Gestão de Dados)

Neste módulo, são exploradas as competências para gerir aplicações, armazenamento e dados em ambiente Windows, com foco em monitorização de desempenho, configuração de dispositivos de armazenamento e implementação de políticas de backup e privacidade. Este módulo introduz ainda os princípios de segurança e gestão de dados.

Módulo e-learning

- Gerir aplicações Windows
- Instalar e configurar dispositivos de armazenamento
- Descrever os fundamentos de armazenamento de dados
- Descrever os fundamentos de gestão de dados

Technical Lab – 3h

- Monitorizar desempenho de sistemas e aplicações em Windows.
- Configurar dispositivos de armazenamento e interpretar o processo de boot.
- Implementar políticas de backup e recuperação de dados.
- Aplicar boas práticas de segurança, privacidade e ciclo de vida dos dados.

Fundamentos de Redes I (Clientes e Navegação Segura)

Este módulo introduz os conceitos fundamentais de redes, desde protocolos e modelos até à configuração de

clientes e redes SOHO, incluindo mecanismos básicos de firewall e práticas de navegação segura. Os formandos adquirem competências práticas para configurar e proteger ligações de rede.

Módulo e-learning

- Descrever protocolos de rede
- Configurar clientes de rede
- Configurar redes SOHO
- Navegar na web de forma segura

Technical Lab – 3h

- Configurar clientes de rede com endereços IP e conectividade.
- Implementar e validar configurações de redes SOHO, incluindo firewalls básicas.
- Configurar definições de segurança em browsers.
- Reconhecer e responder a tentativas de engenharia social em cenários simulados.

Fundamentos de Redes II (Infraestrutura Empresarial e Segurança)

Neste módulo, os formandos conhecem o que são redes empresariais e os principais mecanismos de segurança associados, como firewalls, proxies, criptografia e autenticação (AAA). Este módulo prepara os formandos para mapear e proteger infraestruturas de rede em contexto corporativo.

Módulo e-learning

- Descrever redes empresariais/campus

Technical Lab – 3h

- Mapear a infraestrutura de uma rede empresarial (switches, routers, APs).
- Configurar e validar regras básicas de firewall em ambiente simulado.
- Implementar mecanismos de autenticação e autorização (AAA).
- Aplicar conceitos de defesa em profundidade em cenários práticos.

Fundamentos de Redes III (Aplicações, Cloud e IoT)

Neste módulo, os participantes aprendem os protocolos de aplicação, redes WAN e VPNs, serviços em cloud e dispositivos IoT, destacando riscos e medidas de proteção. Este módulo permite aos formandos compreender os principais vetores tecnológicos atuais e emergentes, essenciais para responder a desafios modernos em cibersegurança.

Módulo e-learning

- Explicar a utilização de protocolos de aplicação
- Descrever o papel das WAN, da cloud e da IoT

Technical Lab – 3h

- Configurar e testar protocolos de rede (HTTP, FTP, SMTP, TLS).
- Implementar e validar uma ligação VPN.

- Criar e configurar uma máquina virtual em ambiente cloud (Azure).
- Identificar riscos e aplicar medidas de segurança em dispositivos IoT.

Controlo e Automação em Cibersegurança

Neste módulo, os formandos adquirem competências em controlos de segurança, gestão de incidentes e resiliência operacional, utilizando ferramentas como Nmap e Wireshark. O módulo introduz ainda fundamentos de scripting e automação para suportar processos de deteção e resposta.

Módulo e-learning

- Explicar procedimentos operacionais de rede
- Explicar resiliência em cibersegurança
- Explicar controlos de cibersegurança
- Descrever fundamentos de scripting
- Desenvolver scripts

Technical Lab – 3h

- Executar análises de rede com Nmap e Wireshark.
- Criar e aplicar um plano básico de resposta a incidentes.
- Configurar estratégias de backup e recuperação em ambiente de simulação.
- Desenvolver scripts simples (PowerShell/Bash) para automatizar tarefas de administração.

Fundamentos de Linux

Neste módulo, os formandos aprendem administração Linux, incluindo comandos básicos, gestão de utilizadores, permissões, pacotes e serviços. O módulo permite aos formandos compreender e operar em sistemas críticos para a área de cybersecurity, uma vez que grande parte da infraestrutura de servidores e ferramentas de segurança assenta neste sistema operativo.

Módulo e-learning

- Operar computadores Linux
- Gerir servidores Linux
- Gerir aplicações Linux

Technical Lab – 3h

- Utilizar comandos básicos em Linux para administração de sistemas.
- Configurar permissões de ficheiros e gerir utilizadores e grupos.
- Estabelecer ligações remotas seguras via SSH.
- Gerir pacotes, processos e serviços em ambiente Linux.