Venha aprender como se aplica análise comportamental a redes e dispositivos para prevenir, detectar e combater ameaças de segurança cibernética.

CySA+ (parceria oficial CompTIA) (EaD)

O CompTIA Cybersecurity Analyst (CySA+) foi desenhado para praticantes de ciber segurança que desempenham funções relacionadas a proteção de sistemas da informação assegurando sua disponibilidade, integridade, autenticação, confidencialidade e não-repudiação. Esse curso foca no conhecimento, habilidades e prática necessária para fornecer defesa a tais sistemas de informação em um contexto de ciber segurança incluindo proteção, detecção, análise, investigação e processos de respostas a incidentes.

Este curso foi desenvolvido para estudantes que estão se preparando par fazer o exame de certificação CompTIA CySA+ CSO-001.

Características

- 5 (cinco) semanas de duração, com 2 (dois) encontros online por semana (total de 10 encontros);
- Os encontros serão ao vivo com tutor e terão 2 (duas) horas de duração;
- Para o auto estudo, o material de apoio será disponibilizado no AVA: livro do curso, materiais extras, indicação de leituras, atividades;
- Sugerimos que antes de iniciar o curso, o aluno verifique o seu acesso à internet;
- Para acompanhamento do curso, sugerimos que o aluno acesse por um computador utilizando, de preferência, o navegador Firefox;
- **Para conclusão do curso é necessário que o aluno responda aos questionários e realize 75% das atividades propostas dentro dos prazos estabelecidos.**

Competências desenvolvidas

- Gestão de Ameaças;
- Arquitetura de Segurança e Conjuntos de Ferramentas;
- Gestão de Vulnerabilidades;
- Resposta ao Ciber-Incidente.

Conhecimentos prévios

Para garantir o sucesso nesse curso, você deve ter pelo menos 2 anos de experiência em Segurança de Redes de TI, e mais:

Escola Superior de Redes RNP
esr.rnp.br

RNP

- A habilidade de reconhecer vulnerabilidades e ameaças de segurança da informação no contexto de gestão de risco;
- Habilidades operacionais de nível básico de sistemas operacionais mais comuns;
- Conhecimento básico dos conceitos e framework de políticas de segurança da informação de redes e dispositivos;
- Entendimento básico sobre conceito de redes mais comuns;
- Conhecimento básico dos principais protocolos TCP/IP;
- Inglês básico (apenas leitura).

Investimento

- R$ 4.500,00

Programa do curso

- Lição 1:
- Avaliando os Riscos de Segurança da Informação: Identificando a Importância da Gestão de Riscos • Avaliando Riscos • Mitigando Riscos • Integrando Documentação na Gestão de Riscos
- Lição 2:
- Analisando as Ameaças de Reconhecimento aos Ambientes de Redes e TI: Avaliando o Impacto do Incidentes de Reconhecimento • Avaliando o Impacto da Engenharia Social
- Lição 3:
- Analisando Ataques em Ambientes de Redes e Computacionais: Avaliando o Impacto Ataques de Hacking de Sistemas • Avaliando o Impacto de Ataques baseados em Web • Avaliando o Impacto de Malwares • Avaliando o Impacto de Ataques de Impersonificação e Sequestro • Avaliando o Impacto de Incidentes de DoS • Avaliando o Impacto de Ameaças à Segurança Mobile • Avaliando o Impacto das Ameaças à Segurança da Nuvem
- Lição 4:
- Analisando Técnicas Pós-Ataques: Avaliando as Técnicas de Controle e Comando • Técnicas de Acesso Persistente • Avaliando Técnicas de Movimentação Lateral e Pivoteamento • Avaliando Técnicas de Exfiltração de Dados • Avaliando Técnicas Anti-Forense
- Lição 5:
- Gerenciando Vulnerabilidades na Organização: Implementando um Plano de Gestão de Vulnerabilidades • Avaliando as Vulnerabilidades Comuns • Conduzindo Varredura de Vulnerabilidades • Conduzindo Testes de Penetração em Ativos de Redes
- Lição 6:
- Coletando Inteligência de Ciber Segurança: Lançando uma Plataforma de Coleta e Análise de Segurança da Informação • Coletando Dados de Fontes de Inteligência baseados em Rede • Coletando Dados de Fontes de Inteligência baseados em Host
- Lição 7:
- Analisando os Dados de Log: Usando Ferramentas Comuns de Análise de Logs • Usando a Ferramenta SIEM para Análise
- Lição 8:
- Performando Análise Ativa de Ativos e Rede: Analisando Incidentes com Ferramentas baseadas em Windows • Analisando Incidentes com Ferramentas

Escola Superior de Redes RNP

esr.rnp.br

RNP

baseadas em Linux • Analisando Malware • Analisando os Índices de Comprometimento

- Lição 9:
- Respondendo a Incidentes de Ciber Segurança: Lançando uma Arquitetura de Manuseio e Resposta a Incidentes • Mitigando Incidentes • Preparando para Investigação Forense como um CSIRT
- Lição 10:
- Investigando os Incidentes de Ciber Segurança: Aplicando um Plano de Investigação Forense • Coletando e Analisando Seguramente Evidências Eletrônicas • Follow Up nos Resultados de uma Investigação
- Lição 11: Abordando Questões de Arquitetura de Segurança: Remediando Gestão de Acesso e Identidade

Escola Superior de Redes RNP

esr.rnp.br

RNP