Segurança Ofensiva e Inteligência Cibernética – 360 h

Essa Especialização Lato Sensu tem como público alvo, profissionais que queiram se aperfeiçoar na área de Segurança da Informação, Segurança Cibernética e Segurança Ofensiva (OffSec).Essas são áreas com expressivo crescimento, só o Brasil foi alvo de mais de 3,2 bilhões de tentativas de ataque no primeiro trimestre de 2021 e a tendência é de que esses números continuem aumentando, e com isso a demanda por serviços de segurança e profissionais capacitados também cresce.

Disciplinas:

- Ethical Hacking - Técnicas e Ferramentas
    - Ethical Hacking – Fundamentos
    - Preparando seu ambiente de testes
    - Técnicas de Ethical Hacking
    - Ferramentas na prática
    - Segurança em ambiente Web

- Engenharia Social e Phishing
    - Introdução ao No-Tech Hacking
    - Ciência do comportamento
    - Linguagem corporal
    - Introdução à Engenharia Social
    - Análise de Caos
    - Phishing

- Detecção de Intrusão, Configuração de Perímetro e Análise de Logs
    - Segurança da Informação
    - Pilares da Segurança da Informação
    - Governança de Tecnologia em Segurança da Informação
    - Incidente de Segurança da Informação
    - Sistemas de Detecção de Intrusão
    - Pós-detecção
    - Exemplos e sistemas de detecção de intrusão

- Malware Hunting
    - O que é uma Threat (Ameaça)?
    - Malwares, Vulnerabilidades e Exploits
    - Cenário Atual
    - Entendendo alguns ataques
    - Ameaças Avançadas Persistentes (APTs)
    - DNA de uma APT
    - Etapas de uma APT
    - Sandbox
    - Threat Hunting
    - Qual time eu deveria ter
    - Empoderando meu SOC
    - Incidentes de Segurança
    - Monitoramento de Segurança em Camadas

    - Gerenciamento de Incidentes
    - Encodings

- Criptografia e Criptoanálise, privacidade e comunicações digitais
    - Esteganografia
    - Criptografia clássica
    - Criptografia Moderna Simétrica
    - Criptografia Assimétrica
    - Criptografia assimétrica com PGP
    - Hash
    - Brute Force em senhas Hash
    - Criptografia Quântica

- Gestão de Segurança da Informação
    - Pilares da Segurança da Informação
    - Nomes e Padrões em Segurança da Informação (ISO / NIST / PCI)
    - Ameaças, vulnerabilidades, Riscos e tipos de ataques em segurança
    - Política e Conscientização em Segurança da Informação
    - Segurança em Internet das Coisas, Ciberataques e Ransomware
    - Segurança em Cloud Computing e segurança em dispositivos móveis

- Gerenciamento de Projeto de Redes de Computadores
    - Arquitetura de Camadas
    - Ciclo de Vida de uma Rede
    - Preparação
    - Planejamento de Rede de Computadores
    - Projeto de Rede de Computadores
    - Implantação
    - Operação e otimização de Redes
    - Conectores de Cabos e Guias de Identificação

- Equipamentos e Configurações
    - Redes de Computadores e seus componentes
    - Protocolo TCP/IP
    - Endereçamento IP e suas sub-redes
    - Equipamentos utilizados em Redes
    - Roteamento

- Teste de Invasão em Redes e Sistemas
    - Introdução ao Teste de Invasão
    - Metodologias
    - Nmap
    - Metasploit
    - Nessus
    - Burp Suite
    - Common Vulnerability Scoring System (CVSS)

- Segurança ofensiva em Sistemas Web
    - Sistemas web
    - Damn Vulnerable Web Application (DVWA)
    - Explorando falhas na DVWA
    - Ataque de Força Bruta
    - OWASP