# Segurança Defensiva: Blue Team Operations – 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:

- Analista de SOC (Security Operation Center)
    - Introdução ao SOC
    - SIEM
    - Criando um SOC
    - Frameworks e Acesso Físico
    - Plano de comunicação e Threat Intelligence

- Estratégias de Segurança Cibernéticas
    - Introdução à Segurança Computacional
    - Introdução à Privacidade e Proteção dos Dados
    - Governança
    - Ataques e suas características
    - Ferramentas e Processos

- Segurança Defensiva e Resposta a Incidentes
    - Introdução a segurança defensiva
    - Quem é o inimigo e Como hackers atuam
    - Mitre & Attack
    - Exploit Database
    - APTs
    - Malwares
    - Processo de Contratação de ferramentas
    - Gestão de ferramentas de segurança
    - Conhecendo uma rede corporativa de grande porte
    - Proteção contra malwares
    - Windows Internals
    - AMSI bypass
    - UAC Bypass
    - Sysmon Bypass
    - ETW bypass
    - Análise Heurística de ameaças
    - EDR x AV convencional
    - MSS
    - Firewall Next Generation x Firewalls convencionais
    - Ferramentas de detecção de Ameaças
    - Machine Learn em defesa cibernética
    - Micro Segmentação

        - Nano Segmentação
        - Publicação segura de serviços e recursos
        - WAF - Web Application Firewall
        - Vazamento de dados
        - DLP e CASB
        - Proteção de Domínio
        - Phishing e Spear Phishing
        - Security Awareness
        - DevSecOps e APP sec
        - Correlação de eventos
        - SIEM
        - SOAR
        - IDS/IPS
        - IOCs
        - Threat Intelligence
        - Análise de Malware
        - Maldoc
        - Introdução a engenharia reversa
        - Resposta a Incidentes
        - Cadeia de Custódia
        - First responder
        - Como a memória ram funciona
        - Dump de Memória
        - FTK-Imager
        - Análise de Memória
        - IPED - Polícia Federal

- 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

- Exploração de Software
    - Sistemas Computacionais, Arquitetura de Von Neumann e sistemas numéricos
    - Representação de dados: ASCII, BCD e Ponto Flutuante
    - Riscos, Vulnerabilidades e Ameaças
    - Exploits e Payloads
    - Metasploit
    - Armitage
    - SEToolKit
    - Metasploitable2
    - Apache Tomcat
    - Samba
    - NFS

    - Programação com Python

- Análise Forense Aplicada a Sistemas Linux
    - Introdução à Forense
    - Fases de Investigação
    - Análise de um incidente
    - Documentação
    - Análise Forense
    - Análise de arquivos de log
    - Coletando hashes
    - Dump de memória RAM
    - Criando e montando imagens
    - Sistema de Arquivos, Análise de Memória e Volatility
    - Criando um perfil no Volatility
    - Malware e Além
    - Comandos úteis

- Tópicos especiais em redes de computadores
    - WANET, MANET e Roteamento em redes Ad hoc
    - Resiliência, multicast e protocolos P2P
    - Redes e protocolos VPN
    - Segurança em Redes sem fio
    - Qualidade de Serviço em redes de computadores

- Gerenciamento de Riscos
    - Comportamento em Relação aos Riscos
    - Identificação dos Riscos
    - Estrutura Analítica de Riscos
    - Brainstorming
    - Análise de SWOT
    - Delphi
    - Análise dos Riscos
    - Processo de Análise Qualitativa
    - Planejamento de Respostas
    - Controle dos Riscos
    - Documentação dos Riscos e Fechamento do Projeto

- Fundamentos da Computação em Nuvem
    - Entendendo a mudança de paradigma que é a computação em nuvem
    - Arquitetura de Computação em Nuvem
    - Modelos de Deploy
    - Os aplicativos da Nuvem
    - O gerenciamento da Nuvem
    - O papel da conectividade de rede na Nuvem
    - Estratégias para Computação em Nuvem
    - OnDemand versus OnPremises
    - Os quatro pilares da computação em Nuvem

- Análise Forense Computacional
    - O Perito Forense
    - Análise
    - Coleta
    - Análise Forense em Windows