PÓS GRADUAÇÃO

UMA NOVA VERSÃO DA PÓS-GRADUAÇÃO

REDES E CIBERSEGURANÇA

FUNDAMENTOS FORENSES, GOVERNANÇA, ARQUITETURA, SOC & ETHICAL HACKING

PÓS GRADUAÇÃO

A PÓS-GRADUAÇÃO

Um novo plano real de formação para um mercado que exige os melhores.

A área de cibersegurança vive um *boom*.

Empresas estão desesperadas por **profissionais capazes de operar SOCs modernos,** entender ameaças em tempo real e criar arquiteturas resilientes.

Pensando no seu desenvolvimento profissional,

a nossa pós-graduação foi repensada e agora entrega uma formação que dialoga diretamente com as reais necessidades do mercado.

Você terá uma jornada desde o alicerce — redes, fundamentos e arquitetura...

...até o domínio de ferramentas como SIEM, SOAR, Firewall, EDR e resposta a incidentes, com projetos reais, simulações de alertas e SOC moderno.

Não é uma atualização. É uma nova geração de especialistas.

PÓS GRADUAÇÃO

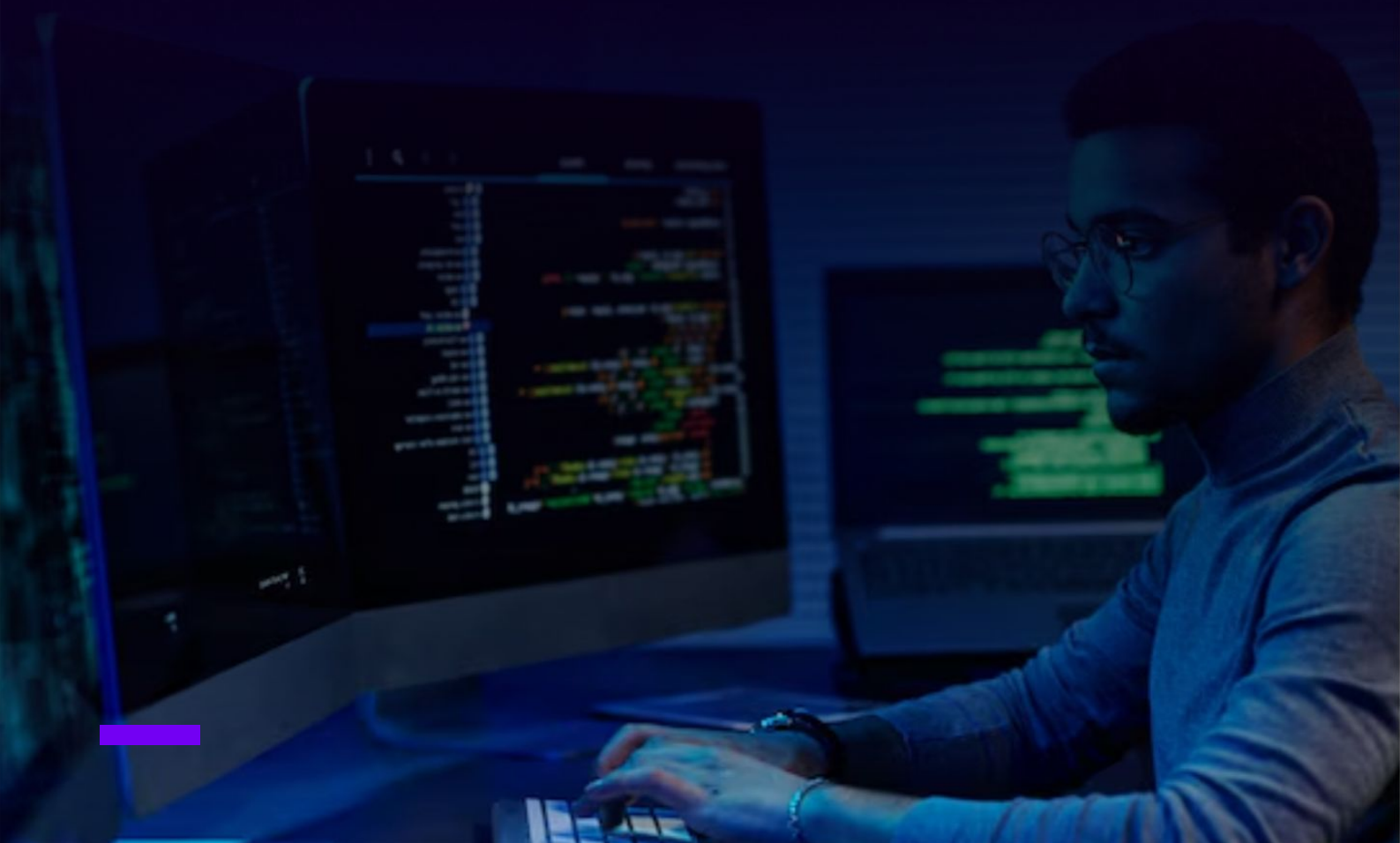
PRÉ-REQUISITOS PARA SE MATRICULAR

Não é necessário ter experiência prévia nem graduação para se matricular.

Basta ter curiosidade, vontade de aprender e uma verdadeira sede de conhecimento por SOC, redes e cibersegurança.

Este é o seu ponto de partida para mergulhar nesse universo!

FALAR COM UM CONSULTOR



PÓS GRADUAÇÃO

ESTRUTURA DO CURSO

DURAÇÃO

12 meses

CERTIFICADO

Lato sensu chancelado pelo MEC

ESPECIALIZAÇÕES

RedTeam e BlueTeam

CONTEÚDO COMPLEMENTAR

Preparatório para certificações

CAPACITAÇÃO EXTRA

IA para Infraestrutura

FORMATO

Aulas gravadas e ao vivo

PÓS GRADUAÇÃO

SEUS OBJETIVOS ALCANÇADOS

Com a pós Hackone, você vai:

✔️ Aprimorar habilidades técnicas estratégicas para enfrentar desafios reais.

✔️ Impulsionar sua carreira, assumindo projetos de infraestrutura e proteção de dados.

✔️ Garantir valorização no mercado, com melhores salários e retorno financeiro.

✔️ Se tornar referência em gestão de riscos e análise de ameaças.

PÓS GRADUAÇÃO

POR QUE A PÓS DA HACKONE É DIFERENTE?

Nossos experts **respiram o campo de batalha todos os dias** e estão preparados para te ensinar o que realmente funciona.

Joabe Kachorrosky

Alexandre Sabino

Carlos Silva

Bruno Marangoni

Lucas Palma

Juliano Schmitz

PÓS GRADUAÇÃO

METODOLOGIA

Um conteúdo completo através de **uma jornada com início, meio e fim**, passando pelos conteúdos que você realmente precisa dominar.

PÓS GRADUAÇÃO

ALICERCE/CERTIFICAÇÕES

Fundamentos de Redes (CCNA)

- ✔ Componentes de Rede
- ✔ Camada OSI
- ✔ Topologias de Rede
- ✔ IPv4, IPv6, TCP e UDP
- ✔ Binário & Decimal
- ✔ SSID e Criptografia
- ✔ Virtualização
- ✔ Conceitos de Switch e Ethernet
- ✔ Introdução ao IOS

Fortinet FCP Network Security

FCP Fortigate Administrator

- ✔ Introdução
- ✔ FortiGate Security
- ✔ Fortigate Infrastructure
- ✔ Prova de Certificação
- ✔ Simulados

FCP FortiAnalyzer

- ✔ Introdução, Modos de Operação e Configuração de Rede
- ✔ Administração, Segurança e Domínios Administrativos
- ✔ RAID e HA
- ✔ Gerenciamento de Dispositivos e Troubleshooting
- ✔ Logs e Gerenciamento de Reports

PÓS GRADUAÇÃO

IA PARA INFRAESTRUTURA

- ✔ Conceitos fundamentais de inteligência artificial
- ✔ Tipos de inteligência artificial
- ✔ Frameworks e Ecossistema
- ✔ Inteligência artificial aplicada a cyber

- ✔ Ameaças contra sistemas de inteligência artificial
- ✔ Preparando o Ambiente de laboratorio pratico
- ✔ Detecção de problemas de redes de computadores
- ✔ Detecção de malware na rede

PÓS GRADUAÇÃO

DISCIPLINAS OFICIAIS

Design & Arquitetura de Redes

- ✔ Fundamentos
- ✔ Arquitetura
- ✔ Virtualização
- ✔ Automação
- ✔ Oficina de projetos

Fundamentos de Cibersegurança

- ✔ Introdução a Cibersegurança
- ✔ Tecnologia, Inovação e Segurança
- ✔ Governança e Estratégia em Cibersegurança
- ✔ Oficina de Projetos

Tecnologias em Cibersegurança

- ✔ Segurança de Infraestrutura
- ✔ Cloud Computing Security, DevOps e DevSecOps
- ✔ Ethical Hacking – Penetration Test
- ✔ Prevenção contra Perda de Dados (DLP)
- ✔ Defesa Cibernética
- ✔ Inteligência Artificial & Machine Learning
- ✔ Segurança para Infraestrutura Crítica

PÓS GRADUAÇÃO

DISCIPLINA CORE

Next Generation SOC

- ✔ Os 12 pilares do NG-SOC
- ✔ SOC (Security Operations Center) + Componentes
- ✔ Instalação e aprofundamento de ferramentas do SOC
- ✔ SIEM + SOAR + DIFIR
- ✔ Estudos de caso

ESPECIALIZAÇÕES

Especialização BLUE TEAM

- ✔ Usando Linux para Cibersecurity
- ✔ Crypto
- ✔ Esteganografi
- ✔ Aprofundamento ao Hash
- ✔ Perícia Forense Computacional
- ✔ Engenharia Social
- ✔ Programação Neurolinguística

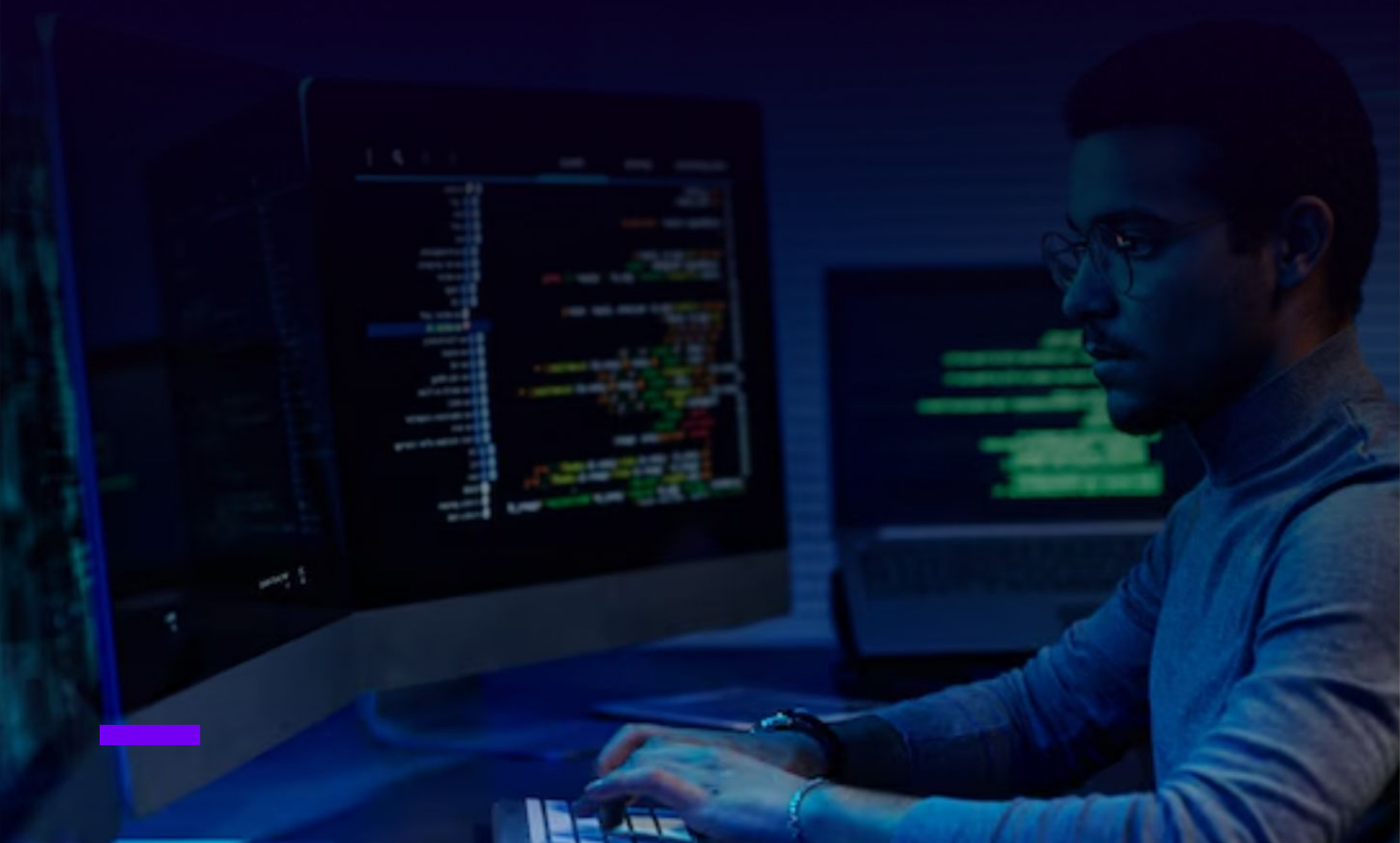
Especialização RED TEAM

- ✔ Fundamentos
- ✔ Engenharia Social
- ✔ Anomização
- ✔ Testes de Intrusão
- ✔ Exploitation
- ✔ Malware
- ✔ Web Security

PÓS GRADUAÇÃO

PROJETO INTEGRADO FINAL

- ✔ Definindo arquitetura de um produto
- ✔ Entendimento do escopo, orçamento e prazos
- ✔ Análise de Risco, Desafios e Oportunidades
- ✔ Decisão de Tecnologias e Meios de Integração
- ✔ Como lidar com imprevistos e mudanças
- ✔ Desenho da Solução Definitiva
- ✔ Pitch da Solução



PÓS GRADUAÇÃO

ESTRUTURA

O PROGRAMA CONTA COM UMA DURAÇÃO TOTAL DE 12 MESES.

ELE PODE, NO ENTANTO, PODE SER COMPLETADO NO TEMPO MÍNIMO DE 6 MESES.

CONTEÚDO AO VIVO

- ✔ Imersão mensal ao vivo com os mentores e professores.
- ✔ Aulas ao vivo realizadas sempre aos sábados, das 9h às 12h (horário de brasília).
- ✔ Elas também estarão disponíveis para acesso posterior.

PÓS GRADUAÇÃO

DISCIPLINAS OFICIAIS

- **DESIGN & ARQUITETURA DE REDES**
- **FUNDAMENTOS DE CIBERSEGURANÇA**
- **TECNOLOGIAS EM CIBERSEGURANÇA**

Nas nossas disciplinas oficiais, você terá acesso a um conjunto de conteúdos que mergulha na criação e proteção de ambientes de rede modernos. Você desenvolverá habilidades em design e arquitetura de redes, dominando virtualização, automação e práticas de projeto. Na área de cibersegurança, aprenderá desde fundamentos estratégicos até tecnologias avançadas, incluindo DevSecOps, pentests e proteção de dados. A integração entre infraestrutura crítica e IA reforça a defesa cibernética inteligente. Tudo é complementado por oficinas práticas, preparando você para atuar de forma eficaz e inovadora no setor de redes e segurança.

PÓS GRADUAÇÃO

MÓDULOS → DESIGN & ARQUITETURA DE REDES

MÓDULO 1 – FUNDAMENTOS

MÓDULO 2 – ARQUITETURA

MÓDULO 3 – VIRTUALIZAÇÃO

MÓDULO 4 – OFICINA DE PROJETOS

DURAÇÃO: +7 HORAS

MÓDULO 1 - FUNDAMENTOS

➡️ Camada OSI ➡️ Componentes de rede ➡️ Topologia de Rede
➡️ Endereço MAC ➡️ Endereçamento IP

MÓDULO 2 - ARQUITETURA

➡️ O que é arquitetura de redes ➡️ Concepcão de projetos
➡️ Capacity planning (Parte 1) ➡️ Capacity planning (Parte 2)
➡️ Ambiente de laboratório (Parte 1) ➡️ Ambiente de laboratório (Parte 2)
➡️ Network Design (Parte 1 de 5) ➡️ Network Design (Parte 2 de 5)
➡️ Network Design (Parte 3 de 5) ➡️ Network Design (Parte 4 de 5)
➡️ Network Design (Parte 5 de 5) ➡️ Implementação de projetos ➡️ Cook Book
➡️ Suporte ➡️ Ferramentas para automação de rede

MÓDULO 3 - VIRTUALIZAÇÃO

➡️ O que é virtualização
➡️ GRE, VRF, DMVPN, Virtual Switching, L3VPN
➡️ Soluções de virtualização para LAN (SD-ACCESS)
➡️ SD-ACCESS na rede Hackone
➡️ Soluções de virtualização para WAN (SD-WAN)

MÓDULO 4 - OFICINA DE PROJETOS

➡️ Estudo de caso

PÓS GRADUAÇÃO

MÓDULOS → FUNDAMENTOS DE CIBERSEGURANÇA

MÓDULO 1 – INTRODUÇÃO À CIBERSEGURANÇA

MÓDULO 2 – TECNOLOGIA E SEGURANÇA

MÓDULO 3 – GOVERNANÇA EM CIBER

DURAÇÃO: +5 HORAS

MÓDULO 1 - INTRODUÇÃO À CIBERSEGURANÇA

- ➡ O que é Cibersegurança?
- ➡ O que fazer quando for invadido?
- ➡ Definições sobre cibersegurança
- ➡ Segurança da Informação vs Cibersegurança
- ➡ Riscos, Vulnerabilidades e Ameaças à Segurança da Informação
- ➡ Ataques e Vetores de Ataques
- ➡ Ataques por força bruta
- ➡ Ataques por Negação de Serviço
- ➡ Ataques por Malware
- ➡ Ataques Web
- ➡ Controle para mitigação de Riscos

MÓDULO 2 - TECNOLOGIA E SEGURANÇA

- ➡ Introdução ao direito digital
- ➡ Crimes Digitais
- ➡ Deep Web
- ➡ Agentes da Web
- ➡ Monitorando a Segurança
- ➡ Dispositivos Pessoais
- ➡ Como você protege sua privacidade
- ➡ LGPD - A lei que vigia os seus dados
- ➡ LGPD - Quais as responsabilidades da TI?

MÓDULO 3 - GOVERNANÇA EM CIBER

- ➡ Governança Corporativa
- ➡ O que é Governança em TI?
- ➡ Motivadores da Governança
- ➡ Gestão de Vulnerabilidades
- ➡ Fases do processo de invasão em sistemas
- ➡ Busca e Exploração de Vulnerabilidades
- ➡ Invasão e Eliminação de Rastros
- ➡ Riscos
- ➡ Conceituação de Risco
- ➡ Vazamentos de Dados
- ➡ Riscos e Tipos de Ataques em Segurança
- ➡ Riscos em Dispositivos Móveis
- ➡ Princípios da Gestão de Riscos
- ➡ Plano de Ação e Estratégia
- ➡ ISO 27001
- ➡ ISO 27002
- ➡ PCI DSS

PÓS GRADUAÇÃO

MÓDULOS → TECNOLOGIAS EM CIBERSEGURANÇA

MÓDULO 1 – SEGURANÇA DE INFRAESTRUTURA

MÓDULO 2 – CLOUD SECURITY, DEVOPS E DEVSECOPS

MÓDULO 3 – DLP | **MÓDULO 4** – SEGURANÇA PARA INFRA CRÍTICA

MÓDULO 5 – INTELIGÊNCIA ARTIFICIAL E ML

DURAÇÃO: +11 HORAS

MÓDULO 1 - SEGURANÇA DE INFRAESTRUTURA

➡️ A base para a Segurança Corporativa ➡️ Risco Corporativo e Criminalidade Cibernética
➡️ Navegação Segura ➡️ Navegação Segura ➡️ Proteção contra DDoS ➡️ Proteção de email

MÓDULO 2 - CLOUD SECURITY, DEVOPS E DEVSECOPS

➡️ O que é DevOps e CI/CD ➡️ Pipeline de Integração Contínua - Jenkins
➡️ Pipeline de Integração Contínua - Jenkins - Estudo de Caso
➡️ Iniciando os testes na esteira CI/CD ➡️ Iniciando os testes na esteira CI/DI - Estudo de Caso
➡️ Provisionamento de Infraestrutura - IAC - Terraform
➡️ Prov. de Infra - IAC - Terraform - Estudo de Caso
➡️ Implementação e Gestão de Configuração - Ansible
➡️ Implementação e Gestão de Config. - Ansible - Estudo de Caso

MÓDULO 3 - DLP

➡️ O que é uma solução de DLP?
➡️ Quais são os benefícios de adotar um DLP?
➡️ Formas de detecção de ameaças de conteúdo

MÓDULO 4 - SEGURANÇA PARA INFRA CRÍTICA

➡️ Segurança de Infraestruturas Críticas (SIC)
➡️ O que é PNSIC?

MÓDULO 5 - INTELIGÊNCIA ARTIFICIAL E ML

➡️ O que é IA e ML ➡️ Algoritmos de busca e suas aplicações em Ciber ➡️Tipos de Algoritmos
➡️ Algoritmos de Heurística Gulosa ➡️ Algoritmos A* ➡️ ML Algoritmo Supervisionado e não supervisionado ➡️ ML Deep Learning ➡️ Conclusão Pipeline ML

PÓS GRADUAÇÃO

MÓDULOS

→ ESPECIALIZAÇÃO BLUE TEAM E RED TEAM

Nossa trilha de especialização em Blue Team e Red Team mergulha nos dois lados da cibersegurança: defesa e ataque. No Blue Team, você dominará ferramentas de proteção como Linux, criptografia, esteganografia, análise forense e até técnicas de engenharia social e programação neurolinguística. Já no Red Team, o foco é entender como os atacantes pensam, com temas como anonimização, testes de intrusão, exploração de falhas, malware e segurança web. A dualidade dos conteúdos prepara você para antecipar ameaças e agir com precisão. Uma formação completa para quem quer estar à frente no combate cibernético.

DURAÇÃO: +11 HORAS

PÓS GRADUAÇÃO

ESPECIALIZAÇÃO BLUE TEAM

- Introdução - Blue Team
- O que é virtualização
- Baixando e instalando o VirtualBox
- Baixando o Kali e Criando uma VM
- Ajustando seu Kali
- Atualizando seu Kali
- Exportando e Importando seu Kali
- Introdução ao Diretório Linux
- Conhecendo o Diretório Bin
- Conhecendo o Diretório Boot
- Conhecendo o Diretório Dev
- Conhecendo o Diretório Etc
- Conhecendo os diretórios Home, Media e demais
- Permissões
- Permissões comando chmod
- Permissões comando chown
- O que é Script
- Iniciando um Script
- Dando permissão de execução para um script
- Saída do Script
- Executando comando de sistema no script
- Shell Script - Comentários e Variáveis
- Shell Script - Entradas
- Shell Script - Condição IF
- Shell Script - Condição ELSE
- Shell Script - Condição Elif
- Shell Script - Exercício
- Shell Script - Resolução
- Shell Script - Case
- Shell Script - For
- Shell Script - While
- Shell Script - Comandos Linux
- Conhecendo a Plataforma de Laboratório
- Conhecendo o SSH
- Preparando VPN TryHackMe
- Conectando a VPN TryHackMe
- Fechando VPN
- SSH
- HASH
- Wireshark
- Investigação
- Investigação - BRIM
- Investigação - Análise

PÓS GRADUAÇÃO

ESPECIALIZAÇÃO RED TEAM

- Introdução a Pentest e Cibersegurança
- Recomendações e Relatórios de Pentest
- Engenharia Social Pentest
- Laboratório Pentest
- OSINT / Coleta de Informações
- Cyber Kill Chain
- MITRE ATT&CK
- Reconhecimento
- Shodan
- Reconhecimento Ativo
- Reconhecimento NMAP
- Baixando e instalando Metasploitable
- Reconhecimento NMAP - Parte 2
- Enumeração de informações e serviços
- Enumerando Serviços
- Atacando FTP
- Quebrando a Autenticação FTP
- Analisando Vulnerabilidade FTP
- Explorando FTP com Metasploit
- Varrendo e Explorando
- Introdução ao Python
- IDE Python
- Script Simples
- Entrada de dados
- Argumentos Python
- Estruturas Python
- Introdução a Web Security
- Web Security: Servidores Web
- Web Security: Falhas e Vulnerabilidades
- Web Security: Como proteger a aplicação Web
- Web Security: Como desenvolver uma aplicação Web de forma segura (DevSec)

PÓS GRADUAÇÃO

MÓDULOS

→ NEXT GENERATION SOC

Nossa disciplina CORE mergulha nas operações modernas de segurança com foco em Next Generation SOC. Você vai conhecer os 12 pilares essenciais para estruturar um SOC eficaz, explorando seus componentes, ferramentas e práticas avançadas. O curso inclui implementação aprofundada de soluções como SIEM, SOAR e DIFIR, que automatizam e potencializam a resposta a incidentes. Além disso, estudos de caso reais ajudam a contextualizar a teoria com desafios práticos. É uma formação estratégica para dominar os bastidores da segurança cibernética corporativa.

PÓS GRADUAÇÃO

MÓDULOS → NEXT GENERATION SOC

MÓDULO 1 – INTRODUÇÃO A SOC
MÓDULO 2 – O QUE É UM SOC + COMPONENTES
MÓDULO 3 – INSTALAÇÃO E APROFUNDAMENTO DE FERRAMENTAS DO SOC
MÓDULO 4 – OPERAÇÃO E AUTOMAÇÃO NO SOC

MÓDULO 1 - INTRODUÇÃO A SOC

➡ Segurança da Informação (Triade CIA, ameaças e vulnerabilidades)
➡ Eventos vs Incidentes ➡ Resposta a Incidentes (IR – Incident Response)
➡ Políticas de Segurança ➡ Gestão de Vulnerabilidades ➡ Controle de Acessos
➡ Inventário de Ativos ➡ Backups ➡ Awareness (Awareness)

MÓDULO 2 - O QUE É UM SOC + COMPONENTES

➡ O que é um SOC ➡ O que é um SIEM ➡ EDR/XDR ➡ NGFW (Next-Generation Firewall)
➡ O que é um SOAR ➡ DFIR (Digital Forensics and Response) ➡ CTI (Cyber Threat Intelligence)
➡ IDS/IPS (Intrusion Detection System/Intrusion Prevention System)
➡ NTA/NDR (Network Traffic Analysis/Network Detection and Response)
➡ DLP (Data Loss Prevention)

MÓDULO 3 - INSTALAÇÃO E APROFUNDAMENTO DE FERRAMENTAS DO SOC

➡ Instalação do sistema operacional ➡ Instalação do Wazuh
➡ Instalação do Wazuh agent + navegação pela ferramenta ➡ Instalação do docker + Iris + navegação
➡ Integração do Iris com Wazuh ➡ Integração do Iris com Virus Total + case
➡ Instalação do Shuffle ➡ Integração Shuffle com Discord ➡ Integração Shuffle com VirusTotal

MÓDULO 4 - OPERAÇÃO E AUTOMAÇÃO NO SOC

➡ Anatomia de um Incidente: da Detecção à Resposta ➡ Análise e investigação com o Wazuh
➡ Casos no Iris: boas práticas, artefatos e enriquecimento
➡ Integrações úteis no Shuffle: Discord, Slack, VirusTotal
➡ Cenário de Incidente Integrado (Mini CTF SOC)

PÓS GRADUAÇÃO

MÓDULOS

→ IA PARA INFRAESTRUTURA

Um curso especial que explora as bases da inteligência artificial, desde seus conceitos fundamentais até os diferentes tipos e ecossistemas tecnológicos. Ele mostra como a IA pode ser aplicada à segurança cibernética, ajudando a detectar problemas em redes e identificar malwares de forma inteligente. Você conhecerá ameaças direcionadas a sistemas de IA e como protegê-los. Também aprenderá a configurar um ambiente prático de laboratório para aplicar tudo isso com simulações reais. Ideal para quem quer unir automação, cibersegurança e redes em um só caminho de especialização.

PÓS GRADUAÇÃO

MÓDULOS → IA PARA INFRAESTRUTURA

MÓDULO 1 – CONCEITOS FUNDAMENTAIS DE INTELIGÊNCIA ARTIFICIAL

MÓDULO 2 – TIPOS DE INTELIGÊNCIA ARTIFICIAL

MÓDULO 3 – FRAMEWORKS E ECOSSISTEMA

MÓDULO 4 – INTELIGÊNCIA ARTIFICIAL APLICADA A CYBER

MÓDULO 5 – AMEAÇAS CONTRA SISTEMAS DE INTELIGÊNCIA ARTIFICIAL

MÓDULO 6 – PREPARANDO O AMBIENTE DE LABORATÓRIO PRÁTICO

MÓDULO 7 – CONSTRUINDO MODELO: DETECÇÃO DE PROBLEMAS DE REDES DE COMPUTADORES

MÓDULO 8 – CONSTRUINDO MODELO: DETECÇÃO DE MALWARE NA REDE

DURAÇÃO: +10 HORAS

MÓDULO 1 - CONCEITOS FUNDAMENTAIS DE INTELIGÊNCIA ARTIFICIAL

➡️ O que é IA? Histórico e evolução ➡️ Aplicações práticas da IA no cotidiano e na segurança
➡️ Diferença entre algoritmos tradicionais e modelos de IA
➡️ Principais algoritmos de ML (Árvore de decisão, KNN, SVM, redes neurais)
➡️ Ética e impacto social da IA

MÓDULO 2 - TIPOS DE INTELIGÊNCIA ARTIFICIAL

➡️ ANI – Inteligência Artificial Fraca ou Limitada ➡️ AGI – Inteligência Artificial Geral
➡️ ASI – Superinteligência Artificial

MÓDULO 3 - FRAMEWORKS E ECOSSISTEMA

➡️ Ecossistema: OpenAI, LangChain, Ollama, HuggingFace
➡️ Ambientes Python para IA: Scikit-learn, TensorFlow, PyTorch
➡️ Introdução a LLMs (Large Language Models)
➡️ Fundamentos de RAG (Retrieval-Augmented Generation)
➡️ Agentes inteligentes e arquiteturas autônomas
➡️ Conceito de MCP (Modelo Cognitivo de Percepção)

PÓS GRADUAÇÃO

MÓDULOS → IA PARA INFRAESTRUTURA

MÓDULO 4 - INTELIGÊNCIA ARTIFICIAL APLICADA A CYBER

- ➡ IA defensiva: detecção de ameaças, SIEM, SOAR
- ➡ IA ofensiva: fuzzing, evasão de antivírus e geração de payloads
- ➡ Cibercrime e o uso malicioso de inteligência artificial

MÓDULO 5 - AMEAÇAS CONTRA SISTEMAS DE INTELIGÊNCIA ARTIFICIAL

➡ Vulnerabilidades de LLMs ➡ Prompt Injection ➡ Model Stealing e Data Poisoning

MÓDULO 6 - PREPARANDO O AMBIENTE DE LABORATÓRIO PRÁTICO

- ➡ Instalação do Python, Jupyter Notebook e bibliotecas ➡ Introdução ao Google Colab
- ➡ Fontes de dados: CICIDS, CTU-13, datasets do Kaggle
- ➡ Importação e pré-processamento de datasets

MÓDULO 7 - CONSTRUINDO MODELO: DETECÇÃO DE PROBLEMAS DE REDES DE COMPUTADORES

- ➡ Apresentação do problema a ser resolvido
- ➡ Análise exploratória de dados de rede (PCAP)
- ➡ Aplicação de algoritmos de ML ao cenário
- ➡ Desenvolvimento e avaliação do modelo

MÓDULO 8 - CONSTRUINDO MODELO: DETECÇÃO DE MALWARE NA REDE

- ➡ Apresentação do problema a ser resolvido
- ➡ Análise dos dados e identificação de comportamentos maliciosos
- ➡ Algoritmos de classificação e detecção
- ➡ Treinamento e validação do modelo

PÓS GRADUAÇÃO

MÓDULOS

→ PROJETO INTEGRADO FINAL

O Projeto Integrado Final coloca em prática todos os aprendizados ao conduzir o desenvolvimento completo de uma solução tecnológica. Você vai definir a arquitetura do produto, entender profundamente o escopo, orçamento e cronograma, além de analisar riscos e oportunidades. O curso orienta na escolha das tecnologias certas e estratégias de integração, lidando com imprevistos com visão adaptativa. Tudo culmina na criação e apresentação do pitch da solução definitiva — uma experiência realista para preparar você para desafios do mercado.

MÓDULO 1 – DEFININDO ARQUITETURA DE UM PRODUTO
MÓDULO 2 – ENTENDIMENTO DE UM ESCOPO, ORÇAMENTO E PRAZOS
MÓDULO 3 – ANÁLISE DE RISCO, DESAFIOS E OPORTUNIDADES
MÓDULO 4 – DECISÃO DE TECNOLOGIAS E MEIOS DE INTEGRAÇÃO
MÓDULO 5 – COMO LIDAR COM IMPREVISTOS E MUDANÇAS
MÓDULO 6 – DESENHO DA SOLUÇÃO DEFINITIVA
MÓDULO 7 – PITCH DA SOLUÇÃO

PÓS GRADUAÇÃO

MÓDULOS → BÔNUS - MENTORIA DE CARREIRAS

MÓDULO 1 – O MAIOR MERCADO DO MUNDO
MÓDULO 2 – DESENVOLVIMENTO PESSOAL
MÓDULO 3 – O RH E SUA JORNADA PROFISSIONAL
MÓDULO 4 – MISSÃO EMPREGO NOVO: O SEU SUPERPODER
MÓDULO 5 – MISSÃO EMPREGO NOVO: TUDO SOBRE CURRÍCULO
MÓDULO 6 – MISSÃO EMPREGO NOVO: O LINKEDIN QUE ENGAJA
MÓDULO 7 – MISSÃO EMPREGO NOVO: BOOTCAMP DA ENTREVISTA

MÓDULO 1 - O MAIOR MERCADO DO MUNDO

➡️ Vertentes da área de tecnologia - Carreira T e Y
➡️ Exponencializando a carreira no mercado de tecnologia ➡️ Criando o seu plano de carreira

MÓDULO 2 - DESENVOLVIMENTO PESSOAL

➡️ Desenvolvimento pessoal e profissional ➡️ RH de A a Z ➡️ Mentoria e Coaching
➡️ Soft Skill e inteligência emocional ➡️ Diversidade e inclusão no ambiente de trabalho
➡️ Comunicação assertiva ➡️ Motivação ➡️ Jargão Técnico ➡️ Liderança (SMART)
➡️ Trabalho em Equipe ➡️ Intraempreendedorismo
➡️ Entenda o DISC - Perfil comportamental ➡️ Mapeando o seu perfil DISC - Parte 1
➡️ Mapeando o seu perfil DISC - Parte 2 ➡️ Aplicando o DISC em seu plano de carreira

MÓDULO 3 - O RH E SUA JORNADA PROFISSIONAL

➡️ Mentoria com o Recrutamento e Seleção
➡️ Como funciona o processo seletivo em empresas de tecnologia de A a Z
➡️ Potencializando a sua busca por oportunidades no mercado de tecnologia
➡️ Construindo o currículo da nova geração
➡️ Como entrar em contato com o RH e/ou o gestor da vaga
➡️ Como entrar em contato com o RH e/ou o gestor da vaga pelo LinkedIn
➡️ Estruturando o seu LinkedIn - Parte 1 ➡️ Estruturando o seu LinkedIn - Parte 2
➡️ Entrevista com o RH ➡️ Bootcamp entrevista em Inglês (ft. Danilo Torlai)

PÓS GRADUAÇÃO

MÓDULOS → BÔNUS - MENTORIA DE CARREIRAS

MÓDULO 4 - MISSÃO EMPREGO NOVO: O SEU SUPERPODER

➡️ Metodologia ➡️ O seu super poder ➡️ Identificando o seu super poder
➡️ A importância do objetivo ➡️ Definindo o objetivo profissional
➡️ Criando lista de Keywords ➡️ O Seu super poder: Revisão

MÓDULO 5 - MISSÃO EMPREGO NOVO: TUDO SOBRE CURRÍCULO

➡️ Introdução ao CV Supremo ➡️ O CV SUPREMO - Passo 1: Objetivo e Keywords
➡️ O CV SUPREMO - Passo 2: Dados Pessoais ➡️ O CV SUPREMO - Passo 3: Definindo o OBJETIVO
➡️ O CV SUPREMO - Passo 3.1: Definindo o OBJETIVO (Estudante)
➡️ O CV SUPREMO - Passo 3.2: Definindo o OBJETIVO (Recém Formado)
➡️ O CV SUPREMO - Passo 3.3 Definindo o OBJETIVO (Profissional Experiente)
➡️ O CV SUPREMO - Passo 3.4: Definindo o OBJETIVO (Migração de Carreira)
➡️ O CV SUPREMO - Passo 3.5: Definindo o OBJETIVO (Profissional Certificado)
➡️ O CV SUPREMO - Passo 4: Resumo Profissional
➡️ O CV SUPREMO - Passo 5: Certificações e treinamento
➡️ O CV SUPREMO - Passo 6: Experiência Profissional
➡️ CV SUPREMO - Passo 7: Formação Acadêmica ➡️ O CV SUPREMO - Passo 8: IDIOMAS

MÓDULO 6 - MISSÃO EMPREGO NOVO: O LINKEDIN QUE ENGAJA

➡️A linguagem do Linkedin ➡️Os 3 Públicos do Linkedin ➡️Busca de emprego ativa
➡️A Vitrine Magnética ➡️A Vitrine Magnética - Foto Do Perfil ➡️A Vitrine Magnética - Foto De Capa
➡️A Vitrine Magnética - Título ➡️Configurações avançadas Linkedin
➡️Engajando com o campo "Sobre" ➡️Experiências Profissionais ➡️Competências
➡️Inserindo Certificações ➡️Dica para gerar dados e engajamento no Linkedin

MÓDULO 7 - MISSÃO EMPREGO NOVO: BOOTCAMP DA ENTREVISTA

➡️ Introdução ➡️ Tipos de Entrevista ➡️ Conversa com Recrutador ➡️ Conversa com o RH
➡️ Conversa com o Gestor ➡️ Bate Papo com o Diretor / CEO / Dono
➡️ Combatendo o Vilão - A Falta de Autoconfiança ➡️ Preparo para Entrevistas
➡️ Entendendo a mente do gestor que contrata
➡️ Bootcamp MCT 360 - O Preparo definitivo para entrevistas
➡️ Bootcamp MCT - A Prática Leva a Perfeição ➡️ Resumo Bootcamp MCT 360

PÓS GRADUAÇÃO

Excelência reconhecida pelo MEC

RECONHECIDO PELO MEC

OUTROS BENEFÍCIOS

hackone FORTINET

ACADEMIA OFICIAL FORTINET

Sendo nosso aluno, você ganha **acesso aos laboratórios oficiais Fortinet e vouchers para certificações**.

Você sai com a base em redes, se aprofunda em cibersegurança e termina certificado internacionalmente, **economizando mais de R$ 4.500 em certificações**.

PÓS GRADUAÇÃO

OUTROS BENEFÍCIOS

ACESSO COMPLETO À Hackone PRO

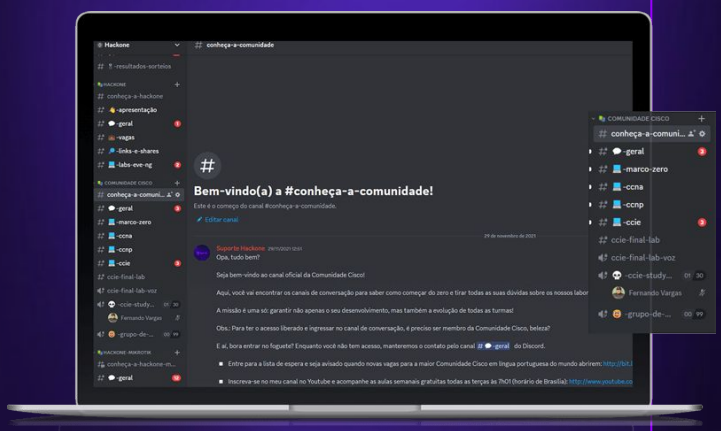
Formamos especialistas prontos para conquistar as melhores oportunidades no mercado de infraestrutura.

Conte com conteúdos práticos e atualizados, alinhados às demandas reais da profissão.

OUTROS BENEFÍCIOS

FÓRUM EXCLUSIVO NO DISCORD

Conecte-se com experts da área e expanda suas oportunidades no mundo da cibersegurança com acompanhamento e suporte.



Entre em contato com nossos consultores e faça a sua matrícula para a próxima turma!

FALAR COM UM CONSULTOR

PÓS
GRADUAÇÃO