Executive Master

Pentesting e Red Team

MPRT

tech universidade tecnológica

tech universidade tecnológica

Executive Master
Pentesting e Red Team

- Modalidade: **online**
- Duração: **12 meses**
- Certificado: **TECH Universidade Tecnológica**
- Horário: **no seu próprio ritmo**
- Provas: **online**
- Dirigido a: **graduados que tenham concluído anteriormente qualquer curso nas áreas de Ciências Sociais, Jurídicas, Administrativas e Empresariais**

Acesso ao site: **www.techtitute.com/br/escola-de-negocios/executive-master/executive-master-pentesting-red-team**

Índice

01

Boas-vindas

Atualmente, os ataques cibernéticos ganharam destaque e força consideráveis, preocupando o público e as próprias empresas. Como resultado, as empresas sofreram exponencialmente com essas ameaças e tiveram que colocar em prática a máxima proteção para os bancos de dados e as informações confidenciais de seus clientes. Assim, esse setor está em constante busca de especialistas altamente qualificados em cibersegurança, razão pela qual a TECH elaborou esse programa acadêmico, com recursos tecnológicos e outros desenvolvimentos em torno das táticas, técnicas e procedimentos utilizados por agentes maliciosos. Tudo isso, por meio da metodologia *Relearning* e uma plataforma 100% online muito completa, que oferece flexibilidade de tempo.

Mestrado Próprio em Pentesting e Red Team
TECH Universidade Tecnológica

Graças a este programa 100% online, você se especializará na promoção de práticas éticas e legais na execução de ataques e testes em sistemas Windows"

02

Por que estudar na TECH?

A TECH é a maior escola de negócios 100% online do mundo. Trata-se de uma Escola de Negócios de elite, um modelo com os mais altos padrões acadêmicos. Um centro internacional de alto desempenho e de capacitação intensiva das habilidades de gestão.

A TECH é uma universidade na vanguarda da tecnologia, que coloca todos os seus recursos à disposição do aluno para ajudá-lo a alcançar o sucesso empresarial"

Na TECH Universidade Tecnológica

Inovação

A universidade oferece um modelo de aprendizagem online que combina a mais recente tecnologia educacional com o máximo rigor pedagógico. Um método único com alto reconhecimento internacional que proporcionará aos alunos o conhecimento necessário para se desenvolverem em um mundo dinâmico, onde a inovação deve ser a principal aposta de todo empresário.

"Caso de Sucesso Microsoft Europa" por incorporar aos cursos um inovador sistema interativo de multivídeo.

Máxima exigência

O critério de admissão da TECH não é econômico. Você não precisa fazer um grande investimento para estudar nesta universidade. No entanto, para concluir os cursos da TECH, os limites de inteligência e capacidade do aluno serão testados. O padrão acadêmico desta instituição é muito alto...

95% | **dos alunos da TECH finalizam seus estudos com sucesso.**

Networking

Os cursos da TECH são realizados por profissionais de todo o mundo, permitindo que os alunos possam criar uma ampla rede de contatos que será útil para seu futuro.

+100.000
gestores capacitados a cada ano

+200
nacionalidades diferentes

Empowerment

O aluno crescerá ao lado das melhores empresas e dos profissionais mais prestigiosos e influentes. A TECH desenvolveu parcerias estratégicas e uma valiosa rede de contatos com os principais agentes econômicos dos 7 continentes.

+500 | **Acordos de colaboração com as melhores empresas**

Talento

Este programa é uma proposta única para revelar o talento do aluno no mundo dos negócios. Uma oportunidade para demonstrar suas inquietudes e sua visão de negócio.

Ao concluir este programa, a TECH ajuda o aluno a mostrar ao mundo o seu talento.

Contexto Multicultural

Ao estudar na TECH, o aluno irá desfrutar de uma experiência única. Estudará em um contexto multicultural. Em um curso com visão global, através do qual poderá aprender sobre a forma de trabalhar em diferentes partes do mundo, reunindo as informações mais atuais que melhor se adaptam à sua ideia de negócio.

A TECH conta com alunos de mais de 200 nacionalidades.

Aprenda com os melhores

Em sala de aula, a equipe de professores da TECH explica o que os levou ao sucesso em suas empresas, trabalhando a partir de um contexto real, animado e dinâmico. Professores que se envolvem ao máximo para oferecer uma capacitação de qualidade, permitindo que o aluno cresça profissionalmente e se destaque no mundo dos negócios.

Professores de 20 nacionalidades diferentes.

Na TECH você terá acesso aos estudos de casos mais rigorosos e atuais do mundo acadêmico"

A TECH prima pela excelência e, para isso, conta com uma série de características que a tornam uma universidade única:

Análise

A TECH explora o lado crítico do aluno, sua capacidade de questionar as coisas, suas habilidades interpessoais e de resolução de problemas.

Excelência acadêmica

A TECH coloca à disposição do aluno a melhor metodologia de aprendizagem online. A universidade combina o método Relearning (a metodologia de aprendizagem de pós-graduação mais bem avaliada internacionalmente) com o Estudo de Caso. Tradição e vanguarda em um equilíbrio desafiador, com o itinerário acadêmico mais rigoroso.

Economia de escala

A TECH é a maior universidade online do mundo. Conta com um portfólio de mais de 10.000 cursos de pós-graduação. E na nova economia, **volume + tecnologia = preço disruptivo**. Dessa forma, garantimos que estudar não seja tão caro quanto em outra universidade.

03

Por que o nosso programa?

Fazer o programa de estudos da TECH significa multiplicar suas chances de alcançar o sucesso profissional na alta gestão empresarial.

É um desafio que requer esforço e dedicação, mas que abre as portas para um futuro promissor. O aluno irá aprender com a melhor equipe de professores e através da mais flexível e inovadora metodologia educacional.

Contamos com um corpo docente de prestígio e o conteúdo mais completo do mercado, o que nos permite oferecer a você uma capacitação do mais alto nível acadêmico”

Este curso irá proporcionar diversas vantagens profissionais e pessoais, entre elas:

01

Dar um impulso definitivo na carreira do aluno

Ao estudar na TECH, o aluno será capaz de assumir o controle do seu futuro e desenvolver todo o seu potencial. Ao concluir este programa, o aluno irá adquirir as habilidades necessárias para promover uma mudança positiva em sua carreira em um curto espaço de tempo.

70% dos participantes desta capacitação alcançam uma mudança profissional positiva em menos de 2 anos.

02

Desenvolver uma visão estratégica e global da empresa

A TECH oferece uma visão aprofundada sobre gestão geral, permitindo que o aluno entenda como cada decisão afeta as diferentes áreas funcionais da empresa.

Nossa visão global da empresa irá melhorar sua visão estratégica.

03

Consolidar o aluno na gestão empresarial

Estudar na TECH significa abrir as portas para um cenário profissional de grande importância, para que o aluno possa se posicionar como um gestor de alto nível, com uma ampla visão do ambiente internacional.

Você irá trabalhar mais de 100 casos reais de alta gestão.

04

Você irá assumir novas responsabilidades

Durante o programa de estudos, serão apresentadas as últimas tendências, avanços e estratégias, para que os alunos possam desenvolver seu trabalho profissional em um ambiente que está em constante mudança.

45% dos alunos são promovidos dentro da empresa que trabalham.

05

Acesso a uma poderosa rede de contatos

A TECH conecta seus alunos para maximizar as oportunidades. Alunos com as mesmas inquietudes e desejo de crescer. Assim, será possível compartilhar parceiros, clientes ou fornecedores.

Você irá encontrar uma rede de contatos essencial para o seu desenvolvimento profissional.

06

Desenvolver projetos empresariais de forma rigorosa

O aluno irá adquirir uma visão estratégica aprofundada que irá ajudá-lo a desenvolver seu próprio projeto, levando em conta as diferentes áreas da empresa.

20% dos nossos alunos desenvolvem sua própria ideia de negócio.

07

Melhorar *soft skills* e habilidades de gestão

A TECH ajuda o aluno a aplicar e desenvolver os conhecimentos adquiridos e melhorar suas habilidades interpessoais para se tornar um líder que faz a diferença.

Melhore as suas habilidades de comunicação e liderança e impulsione a sua carreira.

08

Fazer parte de uma comunidade exclusiva

O aluno fará parte de uma comunidade de gestores de elite, grandes empresas, renomadas instituições e profissionais qualificados procedentes das universidades mais prestigiadas do mundo: a comunidade TECH Universidade Tecnológica.

Oferecemos a você a oportunidade de se especializar com uma equipe de professores internacionalmente reconhecida.

04

Objetivos

Esta capacitação universitária fornecerá aos alunos atualizações inovadoras sobre regulamentos e conformidade em projetos de cibersegurança na área de *Pentesting*, agregando mais valor à sua carreira. Nesse sentido, a TECH fornecerá recursos didáticos ao longo do desenvolvimento do programa, aprimorando as habilidades relacionadas à detecção de anomalias e comportamentos suspeitos. Assim, ao final do programa, o aluno terá ampliado seus conhecimentos sobre *Pentesting e Red Team*. Tudo isso em 12 meses de capacitação online.

Após este Mestrado Próprio, você estará atualizado sobre a utilidade da Investigação Forense Digital (DFIR) para solucionar crimes cibernéticos"

A TECH torna os objetivos de seus alunos seus próprios Trabalhamos juntos para alcançá-los.

O **Executive Master em Pentesting e Red Team** capacitará o aluno para:

01 Estudar e compreender as táticas, técnicas e procedimentos usados por agentes mal-intencionados, permitindo a identificação e a simulação de ameaças

02 Aplicar os conhecimentos teóricos em cenários práticos e simulações, enfrentando desafios reais, a fim de fortalecer as habilidades de *Pentesting*

03 Aprender a alocar recursos de forma eficiente em uma equipe de cibersegurança, levando em conta as habilidades individuais e maximizando a produtividade do projeto

04 Aprimorar as habilidades de comunicação específicas de ambientes técnicos, facilitando a compreensão e a coordenação entre os membros da equipe

05 Aprender técnicas de monitoramento e controle de projetos, identificando desvios e tomando medidas corretivas conforme necessário

06 Desenvolver competências para avaliar e melhorar as configurações de segurança em sistemas Windows, garantindo a implementação de medidas eficazes

07 Promover práticas éticas e legais na execução de ataques e testes em sistemas Windows, considerando os princípios éticos da cibersegurança

08 Familiarizar o aluno com a avaliação da segurança em APIs e serviços da Web, identificando possíveis vulnerabilidades e reforçando a segurança em interfaces de programação

09 Promover a colaboração eficaz com as equipes de segurança, integrando estratégias e esforços para proteger a infraestrutura de rede

10 Promover práticas éticas e legais na análise e no desenvolvimento de malware, garantindo a integridade e a responsabilidade em todas as atividades

11 Aplicar o conhecimento teórico em ambientes simulados, participar de exercícios práticos para entender e combater ataques maliciosos

12 Adquirir uma sólida compreensão dos princípios fundamentais da Investigação Forense Digital (DFIR) e sua aplicação na resolução de incidentes cibernéticos

13 Aprender a preparar relatórios detalhados que documentem as descobertas, as metodologias usadas e as recomendações derivadas de *Red Team* avançados

14 Desenvolver habilidades para formular recomendações práticas e acionáveis destinadas a atenuar as vulnerabilidades e melhorar a postura de segurança

15 Familiarizar o aluno com as práticas recomendadas para relatórios executivos, adaptando informações técnicas para públicos não técnicos

05

Competências

Essa proposta acadêmica fornecerá ao aluno uma visão atual sobre o *Pentesting*. Isso lhe dará a oportunidade de aprimorar suas habilidades, assumindo funções gerenciais, lidando com situações desafiadoras e mutáveis e até mesmo trabalhando de forma eficaz com outras empresas do setor de TI. Dessa forma, o profissional terá à sua disposição várias ferramentas, como infográficos e vídeos, que apresentarão uma perspectiva mais prática sobre esse campo de estudo.

Capacite suas habilidades para a detecção e prevenção eficazes de malware, resolvendo as situações mais desafiadoras do setor de TI"

01 Adquirir habilidades de *coaching* para o desenvolvimento profissional dos membros da equipe, promovendo o crescimento e o aprimoramento

02 Desenvolver habilidades de tomada de decisões estratégicas em situações de cibersegurança, considerando o impacto de curto e longo prazo na segurança organizacional

03 Adquirir competências na identificação, avaliação e atenuação de riscos específicos de projetos de cibersegurança

04 Desenvolver habilidades para implementar medidas de defesa ativa, fortalecendo a segurança de sistemas e redes

05 Aprender técnicas de análise de tráfego da Web para identificar padrões e comportamentos anômalos, facilitando a detecção de possíveis ameaças

06 Adquirir habilidades em análise forense aplicada a ambientes de rede, permitindo a identificação e a resposta eficazes a incidentes cibernéticos

07 Aprender estratégias para detecção e prevenção eficazes de malware, incluindo a implementação de soluções avançadas de segurança

08 Desenvolver habilidades na identificação de indicadores de comprometimento (IoC) durante a investigação forense, facilitando a detecção e a resposta a incidentes

09 Adquirir habilidades para o planejamento estratégico de exercícios de *Red Team*, considerando objetivos, escopo, recursos e cenários realistas

10 Adquirir habilidades na identificação e priorização de vulnerabilidades, destacando aquelas que representam os maiores riscos à segurança

06

Estrutura e conteúdo

O programa em Pentesting e Red Team é um programa essencialmente voltado para que o aluno adquira as competências relacionadas à computação forense em cibersegurança. Dessa forma, essa qualificação acadêmica é voltada para uma estrutura teórico-prática, acompanhada da ampla experiência e do extenso histórico de uma equipe altamente especializada de especialistas.

Sem cronogramas predefinidos ou avaliações contínuas: a TECH lhe garante o acesso mais rápido e flexível ao seu conteúdo acadêmico"

Plano de estudos

Esta capacitação consiste em 1.500 horas de aprendizado contínuo por meio do ensino dos mais altos padrões, graças ao qual o aluno alcançará os melhores cargos no setor de TI e de negócios. Dessa forma, os alunos superarão os vários obstáculos impostos pelo ambiente de trabalho. Essa qualificação fornecerá várias habilidades que abordam técnicas avançadas em Kerberos, mitigações e proteções.

Por outro lado, a equipe de professores desenvolveu um programa de estudos exclusivo, que incorpora 10 módulos, com o objetivo de que o aluno adquira competências fundamentais relacionadas à avaliação da segurança em APIs e serviços da Web, identificando possíveis pontos de vulnerabilidade.

Além disso, ele se aprofundará em recomendações práticas e acionáveis destinadas a atenuar as vulnerabilidades e melhorar a postura de segurança. Nesse sentido, os alunos se tornarão especialistas importantes no campo de métodos de medição e prevenção de conflitos.

Para esse programa acadêmico, os empreendedores terão o apoio da metodologia exclusiva *Relearning*, por meio do qual eles poderão examinar conceitos complexos e assimilar sua aplicação cotidiana de forma fluente. Ao mesmo tempo, o curso será ministrado em uma plataforma inovadora de aprendizado 100% online, que não está sujeita a horários fixos ou cronogramas de avaliação contínua.

Este Executive Master é realizado em 12 meses e está dividido em 10 módulos:

Módulo 1	Segurança ofensiva
Módulo 2	Gerenciamento de Equipes de Cibersegurança
Módulo 3	Gestão de Projetos de Segurança
Módulo 4	Ataques a Redes e Sistemas Windows
Módulo 5	***Hacking Web*** Avançado
Módulo 6	Arquitetura e Segurança em Redes
Módulo 7	Análise e Desenvolvimento de ***Malware***
Módulo 8	Fundamentos forenses e DFIR
Módulo 9	Exercícios de ***Red Team*** Avançados
Módulo 10	Relatório técnico e executivo

Onde, quando e como é ensinado?

A TECH oferece a possibilidade de desenvolver este Mestrado em Pentesting e Rede Team totalmente online. Durante os 12 meses de capacitação, o aluno terá acesso a todo o conteúdo do curso a qualquer momento, o que lhe permitirá autogerenciar seu tempo de estudo.

Uma experiência de capacitação única, fundamental e decisiva para impulsionar seu crescimento profissional.

Módulo 1. Segurança ofensiva

1.1. Definição e contexto
1.1.1. Conceitos fundamentais de segurança ofensiva
1.1.2. A importância da cibersegurança na atualidade
1.1.3. Desafios e oportunidades na segurança ofensiva

1.2. Fundamentos da cibersegurança
1.2.1. Desafios iniciais e evolução das ameaças
1.2.2. Marcos tecnológicos e seu impacto na cibersegurança
1.2.3. Cibersegurança na era moderna

1.3. Base da segurança ofensiva
1.3.1. Principais conceitos e terminologia
1.3.2. *Think Outside the Box*
1.3.3. Diferenças entre hacking ofensivo e defensivo

1.4. Metodologias de segurança ofensivas
1.4.1. PTES (*Penetration Testing Execution Standard*)
1.4.2. OWASP (*Open Web Application Security Project*)
1.4.3. *Cyber Security Kill Chain*

1.5. Funções e responsabilidades na segurança ofensiva
1.5.1. Principais perfis
1.5.2. *Bug Bounty Hunters*
1.5.3. *Researching*: A arte da pesquisa

1.6. Arsenal do auditor ofensivo
1.6.1. Sistemas operacionais de *Hacking*
1.6.2. Introdução ao C2
1.6.3. *Metasploit*: Fundamentos e uso
1.6.4. Recursos úteis

1.7. OSINT Inteligência em Fontes Abertas
1.7.1. Fundamentos da OSINT
1.7.2. Técnicas e ferramentas de OSINT
1.7.3. Aplicativos OSINT em segurança ofensiva

1.8. *Scripting*: Introdução à automatização
1.8.1. Fundamentos de *scripting*
1.8.2. *Scripting* em Bash
1.8.3. *Scripting* em Python

1.9. Categorização de vulnerabilidades
1.9.1. CVE (*Common Vulnerabilities and Exposure*)
1.9.2. CWE (*Common Weakness Enumeration*)
1.9.3. CAPEC (*Common Attack Pattern Enumeration and Classification*)
1.9.4. CVSS (*Common Vulnerability Scoring System*)
1.9.5. MITRE ATT & CK

1.10. Ética e *hacking*
1.10.1. Princípios de ética *hacker*
1.10.2. A linha entre *hacking* ético e *hacking* malicioso
1.10.3. Implicações e consequências legais
1.10.4. Estudos de caso: Situações éticas na cibersegurança

Módulo 2. Gerenciamento de Equipes de Cibersegurança

2.1. Gestão de equipes
2.1.1. Quem é quem
2.1.2. O gestor
2.1.3. Conclusões

2.2. Funções e responsabilidades
2.2.1. Identificação de função
2.2.2. Delegação eficaz
2.2.3. Gestão de expectativas

2.3. Formação e desenvolvimento de equipes
2.3.1. Estágios da formação de equipes
2.3.2. Dinâmicas de grupo
2.3.3. Avaliação e retroalimentação

2.4. Gestão de Talentos
2.4.1. Identificação de talentos
2.4.2. Desenvolvimento de capacidades
2.4.3. Retenção de talentos

2.5. Liderança e motivação de equipes
2.5.1. Estilos de liderança
2.5.2. Teorias da motivação
2.5.3. Reconhecimento de conquistas

2.6. Comunicação e coordenação
2.6.1. Ferramentas de comunicação
2.6.2. Obstáculos à comunicação
2.6.3. Estratégias de coordenação

2.7. Planejamento estratégico de desenvolvimento de pessoal
2.7.1. Identificação das necessidades de capacitação
2.7.2. Planos de desenvolvimento individual
2.7.3. Monitoramento e avaliação

2.8. Resolução de conflitos
2.8.1. Identificação de conflitos
2.8.2. Métodos de medição
2.8.3. Prevenção de conflitos

2.9. Gestão de qualidade e melhoria contínua
2.9.1. Princípios de qualidade
2.9.2. Técnicas de aprimoramento contínuo
2.9.3. *Feedback* e retroalimentação

2.10. Ferramentas e tecnologias
2.10.1. Plataformas colaborativas
2.10.2. Gerenciamento de projetos
2.10.3. Conclusões

Módulo 3. Gestão de Projetos de Segurança

3.1. Gestão de projetos de segurança
3.1.1. Definição e propósito da gestão de projetos de cibersegurança
3.1.2. Principais desafios
3.1.3. Considerações

3.2. Ciclo de vida de um projeto de segurança
3.2.1. Estágios iniciais e definição de objetivos
3.2.2. Implementação e execução
3.2.3. Avaliação e revisão

3.3. Planejamento e estimativa de recursos
3.3.1. Conceitos básicos de gestão econômica
3.3.2. Determinação de recursos humanos e e técnicos
3.3.3. Orçamento e custos associados

3.4. Implementação e monitoramento de projetos
3.4.1. Monitoramento e acompanhamento
3.4.2. Adaptação e mudanças no projeto
3.4.3. Avaliação intermediária e revisões

3.5. Comunicação e relatórios do projeto
3.5.1. Estratégias efetivas de comunicação
3.5.2. Preparação de relatórios e apresentações
3.5.3. Comunicação com o cliente e a gestão

3.6. Ferramentas e tecnologias
3.6.1. Ferramentas de planejamento e organização
3.6.2. Ferramentas de colaboração e comunicação
3.6.3. Ferramentas de documentação e armazenamento

3.7. Documentação e protocolos
3.7.1. Estruturação e criação de documentação
3.7.2. Protocolos de ação
3.7.3. Guias

3.8. Regulamentos e conformidade em projetos de cibersegurança
3.8.1. Leis e regulamentos internacionais
3.8.2. Conformidade
3.8.3. Auditorias

3.9. Gerenciamento de risco do projeto de segurança
3.9.1. Identificação e análise de riscos
3.9.2. Estratégias de mitigação
3.9.3. Monitoramento e revisão de riscos

3.10. Encerramento do projeto
3.10.1. Revisão e avaliação
3.10.2. Documentação final
3.10.3. *Feedback*

Módulo 4. Ataques a Redes e Sistemas Windows

4.1. Windows e Diretório Ativo
4.1.1. História e evolução do Windows
4.1.2. Noções básicas sobre o Diretório Ativo
4.1.3. Funções e serviços do Diretório Ativo
4.1.4. Arquitetura geral do Diretório Ativo

4.2. Redes em ambientes de Diretório Ativo
4.2.1. Protocolos de rede no Windows
4.2.2. DNS e seu funcionamento no Diretório Ativo
4.2.3. Ferramentas de diagnóstico de rede
4.2.4. Implementação de redes no Diretório Ativo

4.3. Autenticação e autorização no Diretório Ativo
4.3.1. Processo e fluxo de autenticação
4.3.2. Tipos de credenciais
4.3.3. Armazenamento e gestão de credenciais
4.3.4. Segurança de autenticação

4.4. Permissões e políticas no Diretório Ativo
4.4.1. GPOs
4.4.2. Implementação e gestão de GPOs
4.4.3. Gestão de licenças no Diretório Ativo
4.4.4. Vulnerabilidades e mitigações em licenças

4.5. Noções básicas do Kerberos
4.5.1. O que é o Kerberos?
4.5.2. Componentes e funcionamento
4.5.3. Tickets no Kerberos
4.5.4. Kerberos no contexto do Diretório Ativo

4.6. Técnicas avançadas do Kerberos
4.6.1. Ataques comuns do Kerberos
4.6.2. Mitigações e proteções
4.6.3. Monitoramento de tráfego Kerberos
4.6.4. Ataques avançados do Kerberos

4.7. *Active Directory Certificate Services* (ADCS)
4.7.1. Noções básicas de PKI
4.7.2. Funções e componentes do ADCS
4.7.3. Configuração e implantação do ADCS
4.7.4. Segurança em ADCS

4.8. Ataques e defesas em Active Directori Certificate Services (ADCS)
4.8.1. Vulnerabilidades comuns no ADCS
4.8.2. Ataques e técnicas de exploração
4.8.3. Defesas e mitigações
4.8.4. Monitoramento e auditoria de ADCS

4.9. Auditoria do Diretório Ativo
4.9.1. Importância da auditoria no Diretório Ativo
4.9.2. Ferramentas de auditoria
4.9.3. Detecção de anomalias e comportamentos suspeitos
4.9.4. Resposta a incidentes e recuperação

4.10. Azure AD.
4.10.1. Fundamentos do Azure AD
4.10.2. Sincronização com o diretório ativo local
4.10.3. Gestão de identidades no Azure AD
4.10.4. Integração com aplicativos e serviços

Módulo 5. *Hacking* Web Avançado

5.1. Funcionamento de um site
5.1.1. O URL e suas partes
5.1.2. Métodos HTTP
5.1.3. Os cabeçalhos
5.1.4. Como visualizar solicitações da Web com o Burp Suite

5.2. Sessões
5.2.1. Os *cookies*
5.2.2. *Tokens* JWT
5.2.3. Ataques de sequestro de sessão
5.2.4. Ataques a JWT

5.3. *Cross Site Scripting* (XSS)
5.3.1. O que é um XSS
5.3.2. Tipos de XSS
5.3.3. Exploração de um XSS
5.3.4. Introdução ao *XSLeaks*

5.4. Injeções de banco de dados
5.4.1. O que é um SQL *Injection*
5.4.2. Extração de informações com SQLi
5.4.3. SQLi Blind, Time-Based e Error-Based
5.4.4. Injeções de NoSQLi

5.5. *Path Traversal e Local File Inclusion*
5.5.1. O que são e suas diferenças
5.5.2. Filtros comuns e como contorná-los
5.5.3. *Log Poisoning*
5.5.4. LFIs em PHP

5.6. *Broken Authentication*
5.6.1. *User Enumeration*
5.6.2. *Password Bruteforce*
5.6.3. 2FA Bypass
5.6.4. *Cookies* com informações sensíveis e modificáveis

5.7. *Remote Command Execution*
5.7.1. *Command Injection*
5.7.2. *Blind Command Injection*
5.7.3. *Insecure Deserialization* PHP
5.7.4. *Insecure Deserialization* Java

5.8. *File Uploads*
5.8.1. RCE mediante *webshells*
5.8.2. XSS em uploads de arquivos
5.8.3. XML *External Entity* (XXE) *Injection*
5.8.4. *Path traversal* em uploads de arquivos

5.9. *Broken Acess Control*
5.9.1. Acesso aos painéis sem restrição
5.9.2. *Insecure Direct Object References* (IDOR)
5.9.3. *Bypass* de filtros
5.9.4. Métodos de autorização insuficientes

5.10. Vulnerabilidades do DOM e ataques mais avançados
5.10.1. *Regex Denial of Service*
5.10.2. DOM *Clobbering*
5.10.3. *Prototype Pollution*
5.10.4. HTTP *Request Smuggling*

Módulo 6. Arquitetura e Segurança em Redes

6.1. Redes de computadores
6.1.1. Conceitos básicos Protocolos LAN, WAN, CP, CC
6.1.2. Modelo OSI TCP/IP
6.1.3. *Switching:* Conceitos básicos
6.1.4. *Routing:* Conceitos básicos

6.2. *Switching:*
6.2.1. Introdução às VLANs
6.2.2. STP
6.2.3. *EtherChannel*
6.2.4. Ataques à camada 2

6.3. VLAN´s
6.3.1. Importância das VLANs
6.3.2. Vulnerabilidades em VLANs
6.3.3. Ataques comuns a VLANs
6.3.4. Mitigações

6.4. *Routing*
6.4.1. Endereçamento IP - IPv4 e IPv6
6.4.2. Roteamento: Conceitos fundamentais
6.4.3. Roteamento estático
6.4.4. Roteamento dinâmico: Introdução

6.5. Protocolos IGP
6.5.1. RIP
6.5.2. OSPF
6.5.3. RIP vs OSPF
6.5.4. Análise das necessidades de topologia

6.6. Proteção do perímetro
6.6.1. DMZs
6.6.2. *Firewalls*
6.6.3. Arquiteturas comuns
6.6.4. *Zero Trust Network Access*

6.7. IDS e IPS
6.7.1. Características
6.7.2. Implementação
6.7.3. SIEM e SIEM CLOUDS
6.7.4. Detecção baseada em *HoneyPots*

6.8. TLS e VPN´s
6.8.1. SSL/ TLS
6.8.2. TLS: Ataques comuns
6.8.3. VPNs com TLS
6.8.4. VPNs com IPSEC

6.9. Segurança em redes sem fio
6.9.1. Introdução às redes sem fio
6.9.2. Protocolos
6.9.3. Elementos fundamentais
6.9.4. Ataques comuns

6.10. Redes empresariais e como lidar com elas
6.10.1. Segmentação lógica
6.10.2. Segmentação física
6.10.3. Controle de acesso
6.10.4. Outras considerações

Módulo 7. Análise e Desenvolvimento de *Malware*

7.1. Análise e Desenvolvimento de *Malware*
7.1.1. História e evolução do *malware*
7.1.2. Classificação e tipos de *Malware*
7.1.3. Análises de *malware*
7.1.4. Desenvolvimento de *malware*

7.2. Preparação do ambiente
7.2.1. Configuração de máquina virtual e *Snapshots*
7.2.2. Ferramentas de análise de *malware*
7.2.3. Ferramentas de desenvolvimento de *malware*

7.3. Fundamentos do Windows
7.3.1. Formato do arquivo PE (*Portable Executable*)
7.3.2. Processos e *Threads*
7.3.3. Sistema de arquivos e registro
7.3.4. *Windows Defender*

7.4. Técnicas de *Malware* básicas
7.4.1. Geração de *shellcode*
7.4.2. Execução de *shellcode* no disco
7.4.3. Disco vs memória
7.4.4. Execução de *shellcode* na memória

7.5. Técnicas de malware intermediárias
7.5.1. Persistência no Windows
7.5.2. Pasta inicial
7.5.3. Chaves de registro
7.5.4. Protetores de tela

7.6. Técnicas de *malware* avançadas
7.6.1. Cifrado de *shellcode* (XOR)
7.6.2. Cifrado de *shellcode* (RSA)
7.6.3. Ofuscação de *strings*
7.6.4. Injeção de processos

7.7. Análise estática de *malware*
7.7.1. Analisando *packers* com DIE (*Detect It Easy*)
7.7.2. Analisando seções com o PE-Bear
7.7.3. Descompilação com Ghidra

7.8. Análise dinâmica de *malware*
7.8.1. Observando o comportamento com o Process Hacker
7.8.2. Análise de chamadas com o API Monitor
7.8.3. Análise de alterações no registro com o Regshot
7.8.4. Observação de solicitações de rede com o TCPView

7.9. Análise em .NET
7.9.1. Introdução ao .NET
7.9.2. Descompilação com o dnSpy
7.9.3. Depuração com o dnSpy

7.10. Analizando um *malware* real
7.10.1. Preparação do ambiente
7.10.2. Análise estática do *malware*
7.10.3. Análise dinâmica do *malware*
7.10.4. Criação de regras YARA

Módulo 8. Fundamentos forenses e DFIR

8.1. Forense digital
8.1.1. História e evolução da computação forense
8.1.2. Importância da computação forense na cibersegurança
8.1.3. História e evolução da computação forense

8.2. Fundamentos de informática forense
8.2.1. Cadeia de custódia e sua implementação
8.2.2. Tipos de evidência digital
8.2.3. Processos de aquisição de evidências

8.3. Sistemas de arquivos e estrutura de dados
8.3.1. Principais sistemas de arquivos
8.3.2. Métodos de ocultação de dados
8.3.3. Análise de metadados e atributos de arquivos

8.4. Análise de sistemas operacionais
8.4.1. Análise forense de sistemas Windows
8.4.2. Análise forense de sistemas Linux
8.4.3. Análise forense de sistemas macOS

8.5. Recuperação de dados e análise de disco
8.5.1. Recuperação de dados de mídias danificadas
8.5.2. Ferramentas de análise de disco
8.5.3. Interpretação de tabelas de alocação de arquivos

8.6. Análise de rede e tráfego
8.6.1. Captura e análise de pacotes de rede
8.6.2. Análise de registros de *firewall*
8.6.3. Detecção de intrusão de rede

8.7. *Malware* e análise de código malicioso
8.7.1. Classificação de *Malware* e suas características
8.7.2. Análise estática e dinâmica de *malware*
8.7.3. Técnicas de desmontagem e depuração

8.8. Análise de registros e eventos
8.8.1. Tipos de registros em sistemas e aplicativos
8.8.2. Interpretação de eventos relevantes
8.8.3. Ferramentas de análise de registros

8.9. Resposta a incidentes de segurança
8.9.1. Processo de resposta a incidentes
8.9.2. Criação de um plano de resposta a incidentes
8.9.3. Coordenação com equipes de segurança

8.10. Apresentação de evidências e questões legais
8.10.1. Regras de evidência digital no campo jurídico
8.10.2. Preparação de relatórios forenses
8.10.3. Comparecimento ao julgamento como testemunha especializada

Módulo 9. Exercícios de *Rede Team* Avançados

9.1. Técnicas avançadas de reconhecimento
9.1.1. Enumeração avançada de subdomínios
9.1.2. *Google Dorking* avançado
9.1.3. Redes Sociais e theHarvester

9.2. Campanhas de *phishing* avançadas
9.2.1. O que é *Reverse-Proxy Phishing*
9.2.2. *2FA Bypass* com Evilginx
9.2.3. Exfiltração de dados

9.3. Técnicas avançadas de persistência
9.3.1. *Golden Tickets*
9.3.2. *Silver Tickets*
9.3.3. Técnica *DCShadow*

9.4. Técnicas avançadas de evasão
9.4.1. *Bypass* de AMSI
9.4.2. Modificação de ferramentas existentes
9.4.3. Ofuscação de *Powershell*

9.5. Técnicas avançadas de movimento lateral
9.5.1. *Pass-the-Ticket* (PtT)
9.5.2. *Overpass-the-Hash* (Pass-the-Key)
9.5.3. NTLM Relay

9.6. Técnicas avançadas de pós-exploração
9.6.1. *Dump* de LSASS
9.6.2. *Dump* de SAM
9.6.3. Ataque *DCSync*

9.7. Técnicas avançadas de *pivoting*
9.7.1. O que él *pivoting*
9.7.2. Túneis com SSH
9.7.3. *Pivoting* com Chisel

9.8. Intrusões físicas
9.8.1. Vigilância e reconhecimento
9.8.2. *Tailgating e Piggybacking*
9.8.3. *Lock-Picking*

9.9. Ataques *Wi-Fi*
9.9.1. Ataques a WPA/WPA2 PSK
9.9.2. Ataques de Rogue AP
9.9.3. Ataques a WPA2 *Enterprise*

9.10. Ataques RFID
9.10.1. Leitura de cartões RFID
9.10.2. Manuseio de cartões RFID
9.10.3. Criação de cartões clonados

Módulo 10. Relatório técnico e executivo

10.1. Processo de relatório
10.1.1. Estrutura de um relatório
10.1.2. Processo de relatório
10.1.3. Conceitos fundamentais
10.1.4. Executivo x Técnico

10.2. Guias
10.2.1. Introdução
10.2.2. Tipos de guias
10.2.3. Guias nacionais
10.2.4. Casos de uso

10.3. Metodologias
10.3.1. Avaliação
10.3.2. *Pentesting*
10.3.3. Revisão de metodologias comuns
10.3.4. Introdução às metodologias nacionais

10.4. Abordagem técnica para a fase de relatório
10.4.1. Entendendo os limites do *pentester*
10.4.2. Uso e dicas de linguagem
10.4.3. Apresentação de informações
10.4.4. Erros mais comuns

10.5. Abordagem executiva para a fase de relatório
10.5.1. Ajustando o relatório ao contexto
10.5.2. Uso e dicas de linguagem
10.5.3. Padronização
10.5.4. Erros mais comuns

10.6. OSSTMM
10.6.1. Entendendo a metodologia
10.6.2. Reconhecimento
10.6.3. Documentação
10.6.4. Elaboração do relatório

10.7. LINCE
10.7.1. Entendendo a metodologia
10.7.2. Reconhecimento
10.7.3. Documentação
10.7.4. Elaboração do relatório

10.8. Relatório de vulnerabilidades
10.8.1. Conceitos fundamentais
10.8.2. Quantificação do escopo
10.8.3. Vulnerabilidades e evidências
10.8.4. Erros mais comuns

10.9. Focando o relatório no cliente
10.9.1. Importância da evidência do trabalho
10.9.2. Soluções e mitigações
10.9.3. Dados sensíveis e relevantes
10.9.4. Exemplos práticos e casos

10.10. Reportando *retakes*
10.10.1. Conceitos fundamentais
10.10.2. Compreensão das informações legadas
10.10.3. Verificação de erros
10.10.4. Adicionando informações

07

Metodologia

Este curso oferece uma maneira diferente de aprender. Nossa metodologia é desenvolvida através de um modo de aprendizagem cíclico: ***o Relearning***. Este sistema de ensino é utilizado, por exemplo, nas faculdades de medicina mais prestigiadas do mundo e foi considerado um dos mais eficazes pelas principais publicações científicas, como o ***New England Journal of Medicine.***

Descubra o Relearning, um sistema que abandona a aprendizagem linear convencional para realizá-la através de sistemas de ensino cíclicos: uma forma de aprendizagem que se mostrou extremamente eficaz, especialmente em disciplinas que requerem memorização"

A Escola de Negócios da TECH utiliza o Estudo de Caso para contextualizar todo o conteúdo

Nosso programa oferece um método revolucionário para desenvolver as habilidades e o conhecimento. Nosso objetivo é fortalecer as competências em um contexto de mudança, competitivo e altamente exigente.

Com a TECH você irá experimentar uma forma de aprender que está revolucionando as bases das universidades tradicionais em todo o mundo"

Nosso programa prepara você para enfrentar novos desafios em ambientes incertos e alcançar o sucesso em sua carreira.

Nosso programa prepara você para enfrentar novos desafios em ambientes incertos e alcançar o sucesso em sua carreira.

Um método de aprendizagem inovador e diferente

Este curso da TECH é um programa de ensino intensivo, criado do zero, que propõe ao gerente os desafios e as decisões mais exigentes nesta área, em âmbito nacional ou internacional. Através desta metodologia, o crescimento pessoal e profissional é impulsionado, sendo este um passo decisivo para alcançar o sucesso. O método do caso, técnica que forma a base deste conteúdo, garante que a realidade econômica, social e empresarial mais atual seja seguida.

> *Você aprenderá, através de atividades de colaboração e casos reais, a resolver situações complexas em ambientes reais de negócios"*

O método do caso é o sistema de aprendizagem mais utilizado nas principais escolas de negócios do mundo, desde que elas existem. Desenvolvido em 1912 para que os estudantes de Direito não aprendessem a lei apenas com base no conteúdo teórico, o método do caso consistia em apresentar-lhes situações realmente complexas para que tomassem decisões conscientes e julgassem a melhor forma de resolvê-las. Em 1924 foi estabelecido como o método de ensino padrão em Harvard.

Em uma determinada situação, o que um profissional deveria fazer? Esta é a pergunta que abordamos no método do caso, um método de aprendizagem orientado para a ação. Ao longo do programa, os alunos irão se deparar com diversos casos reais. Terão que integrar todo o seu conhecimento, pesquisar, argumentar e defender suas ideias e decisões.

Metodologia Relearning

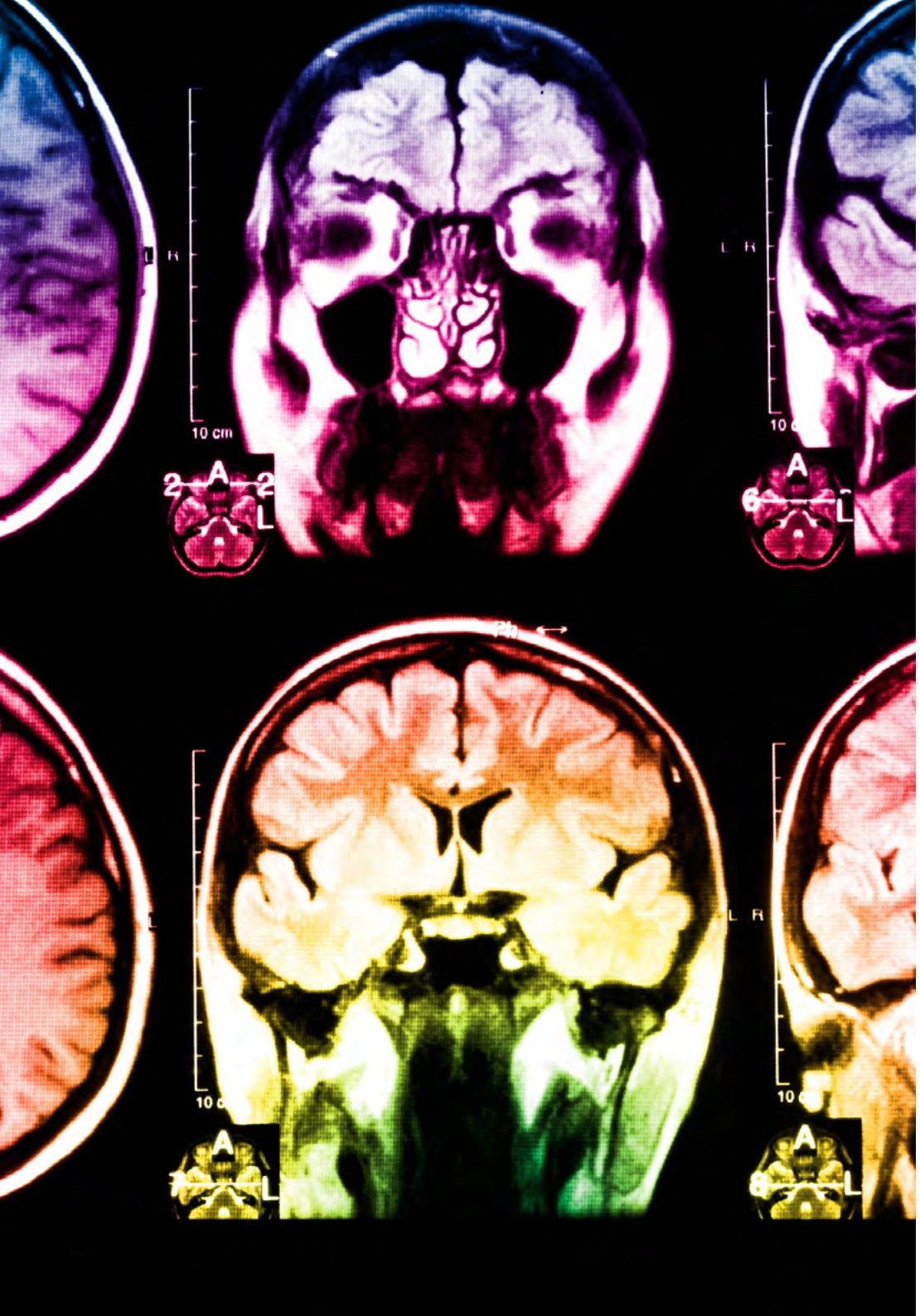
A TECH utiliza de maneira eficaz a metodologia do estudo de caso com um sistema de aprendizagem 100% online, baseado na repetição, combinando elementos didáticos diferentes em cada aula.

Potencializamos o Estudo de Caso com o melhor método de ensino 100% online: o Relearning.

> *Nosso sistema online lhe permitirá organizar seu tempo e ritmo de aprendizagem, adaptando-os ao seu horário. Você poderá acessar o conteúdo a partir de qualquer dispositivo, fixo ou móvel, com conexão à Internet.*

Na TECH você aprenderá através de uma metodologia de vanguarda, desenvolvida para capacitar os profissionais do futuro. Este método, na vanguarda da pedagogia mundial, se chama Relearning.

Nossa escola de negócios é uma das únicas que possui a licença para usar este método de sucesso. Em 2019 conseguimos melhorar os níveis de satisfação geral de nossos alunos (qualidade de ensino, qualidade dos materiais, estrutura dos cursos, objetivos, entre outros) com relação aos indicadores da melhor universidade online.



No nosso programa, a aprendizagem não é um processo linear, ela acontece em espiral (aprender, desaprender, esquecer e reaprender). Portanto, combinamos cada um desses elementos de forma concêntrica. Esta metodologia já capacitou mais de 650 mil graduados universitários com um sucesso sem precedentes em áreas tão diversas como bioquímica, genética, cirurgia, direito internacional, habilidades gerenciais, ciências do esporte, filosofia, direito, engenharia, jornalismo, história ou mercados e instrumentos financeiros. Tudo isso em um ambiente altamente exigente, com um corpo discente com um perfil socioeconômico médio-alto e uma média de idade de 43,5 anos.

O Relearning permitirá uma aprendizagem com menos esforço e mais desempenho, fazendo com que você se envolva mais em sua especialização, desenvolvendo o espírito crítico e sua capacidade de defender argumentos e contrastar opiniões: uma equação de sucesso.

A partir das últimas evidências científicas no campo da neurociência, sabemos como organizar informações, ideias, imagens, memórias, mas sabemos também que o lugar e o contexto onde aprendemos algo é fundamental para nossa capacidade de lembrá-lo e armazená-lo no hipocampo, para mantê-lo em nossa memória a longo prazo.

Desta forma, no que se denomina Neurocognitive context-dependent e-learning, os diferentes elementos do nosso programa estão ligados ao contexto onde o aluno desenvolve sua prática profissional.

Neste programa, oferecemos o melhor material educacional, preparado especialmente para os profissionais:

Material de estudo

Todo o conteúdo foi criado especialmente para o curso pelos especialistas que irão ministrá-lo, o que faz com que o desenvolvimento didático seja realmente específico e concreto.

Posteriormente, esse conteúdo é adaptado ao formato audiovisual, para criar o método de trabalho online da TECH. Tudo isso, com as técnicas mais inovadoras que proporcionam alta qualidade em todo o material que é colocado à disposição do aluno.

Masterclasses

Há evidências científicas sobre a utilidade da observação de terceiros especialistas.

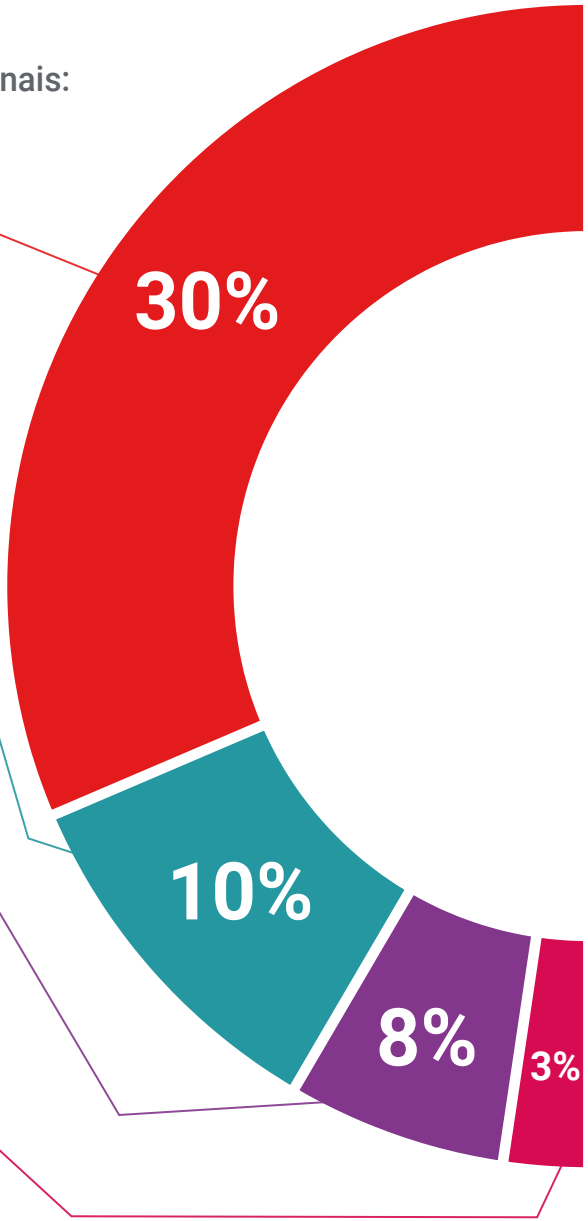
O "Learning from an expert" fortalece o conhecimento e a memória, além de gerar segurança para a tomada de decisões difíceis no futuro

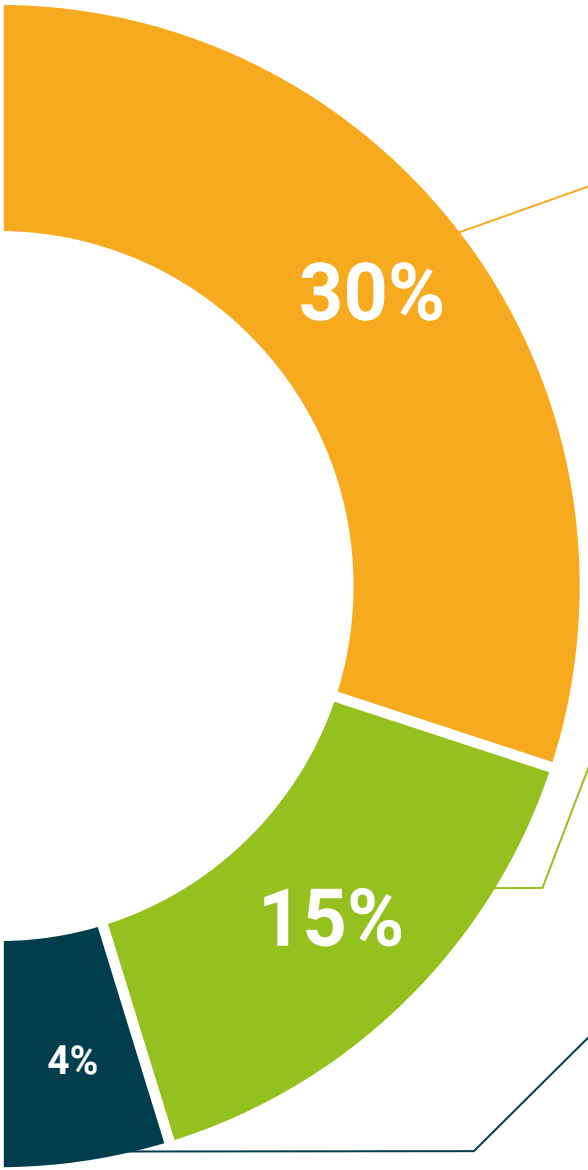
Práticas de habilidades gerenciais

Serão realizadas atividades para desenvolver as competências gerenciais específicas em cada área temática. Práticas e dinâmicas para adquirir e ampliar as competências e habilidades que um gestor precisa desenvolver no contexto globalizado em que vivemos.

Leituras complementares

Artigos recentes, documentos de consenso e diretrizes internacionais, entre outros. Na biblioteca virtual da TECH o aluno terá acesso a tudo o que for necessário para complementar a sua capacitação.





Estudos de caso

Os alunos irão completar uma seleção dos melhores estudos de caso escolhidos especialmente para esta capacitação. Casos apresentados, analisados e orientados pelos melhores especialistas da alta gestão do cenário internacional.

Resumos interativos

A equipe da TECH apresenta o conteúdo de forma atraente e dinâmica através de pílulas multimídia que incluem áudios, vídeos, imagens, gráficos e mapas conceituais para consolidar o conhecimento.

Este sistema exclusivo de capacitação por meio da apresentação de conteúdo multimídia foi premiado pela Microsoft como "Caso de sucesso na Europa"

Testing & Retesting

Avaliamos e reavaliamos periodicamente o conhecimento do aluno ao longo do programa, através de atividades e exercícios de avaliação e autoavaliação, para que possa comprovar que está alcançando seus objetivos.

08

Perfil dos nossos alunos

O Programa está destinado a graduados universitários que tenham concluído anteriormente qualquer curso na área das ciências sociais e jurídicas, administrativas e econômicas.

A diversidade de participantes com diferentes perfis acadêmicos e de múltiplas nacionalidades compõe a abordagem multidisciplinar deste programa.

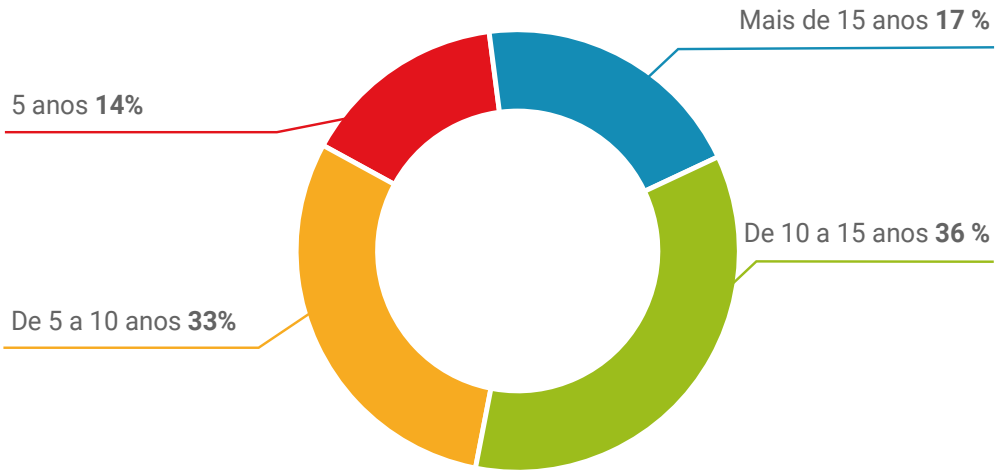
O programa também pode ser estudado por profissionais que, sendo graduados universitários em qualquer área, tenham dois anos de experiência de trabalho no campo de TI.

Se você tem experiência em Pentesting e Red Team e está procurando um aprimoramento interessante em sua carreira enquanto continua trabalhando, este é o programa para você"

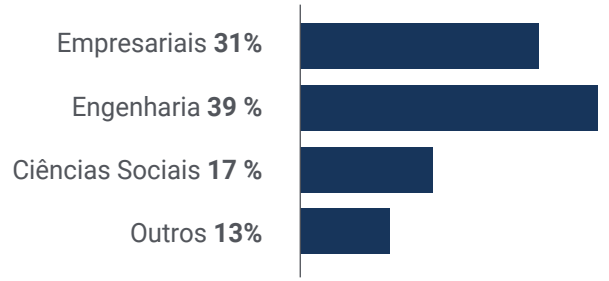
Média de idade

Entre **35** e **45** anos

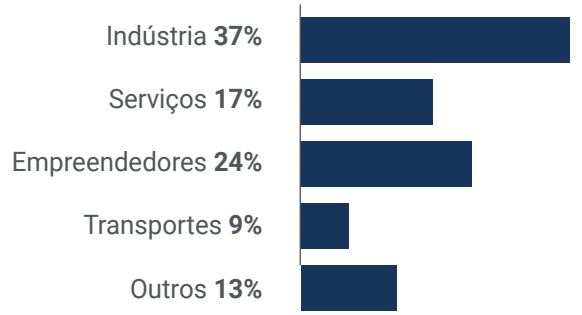
Anos de experiência



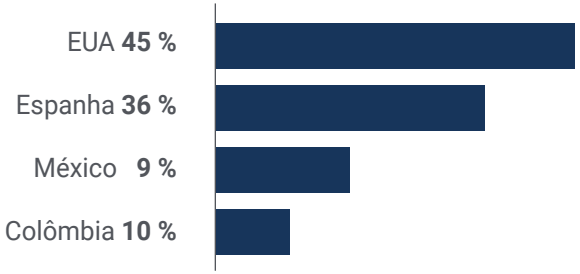
Formação



Perfil acadêmico



Distribuição geográfica



Salomón Galvis

Analista de segurança da informação

"Com esse curso, destaco que pude aprofundar minha compreensão da importância de avaliações regulares e de como é essencial medir a segurança cibernética. Um grande investimento que se refletirá no futuro, graças às ferramentas essenciais que a equipe de professores implementa no desenvolvimento do programa"

09

Direção do curso

Este Executive Master tem à sua disposição uma equipe docente de grande reconhecimento internacional e com importantes conhecimentos especializados em Software e Tecnologias da Sociedade da Informação e Cibersegurança em Integração Tecnológica Empresarial. Assim, a educação de elite se reflete em uma abordagem dinâmica e inovadora do plano de estudos, implementando as últimas tendências em cibersegurança. Dessa forma, os casos simulados são combinados com a análise de situações reais para que os alunos obtenham uma prática de alto nível permitindo que eles assumam os diferentes desafios profissionais no ambiente de trabalho.

Os principais especialistas em Pentesting e Red Team apresentarão esse programa inovador e ambicioso"

Direção

Sr. Carlos Gómez Pintado

- Gerente de cibersegurança e Red Team Cipherbit no Grupo Oesía
- Gerente *Advisor & Investor* na Wesson App
- Formado em Engenharia de Software e Tecnologias da Sociedade da Informação pela Universidade Politécnica de Madri
- Colaboração com instituições educacionais para o desenvolvimento de ciclos de formação de nível superior em cibersegurança

Professores

Sr. Marcelino Siles Rubia

- Cibersecurity Engineer
- Engenharia de Cibersegurança na Universidade Rey Juan Carlos
- Conhecimentos Programação competitiva, *Hacking Web, Active Directory e Malware Development*
- Vencedor do concurso AdaByron

Sr. Marcos González Sanz

- Cybersecurity Consultant-Red Teamer Cipherbit no Grupo Oesía
- Engenheiro de Software pela Universidade Politécnica de Madri
- Especialista em *Cybersecurity Tutor* e Core *Dumped*

Sr. Pablo Redondo Castro

- Pentester no Grupo Oesía
- Engenheiro de cibersegurança, Universidade Rey Juan Carlos, Madri
- Ampla experiência como *Cibersecurity Evaluator Traineev*
- Ele acumula experiência de ensino, ministrando capacitações relacionadas a torneios de Capture The Flag

Sr. Alejandro Gallego Sánchez

- Pentester no Grupo Oesia
- Consultor de Cibersegurança na Integración Tecnológica Empresarial, S.L.
- Técnico Audiovisual na Ingeniería Audiovisual S.A.
- Formado em Engenharia de Cibersegurança pela Universidade Rey Juan Carlos

Sr. Sergio Mora Navas

- Consultor de Cibersegurança no Grupo Oesía
- Engenheiro em Cibersegurança pela Universidad Rey Juan Carlos
- Engenheiro da Computação pela Universidade de Burgos

Sr. Yuba González Parrilla

- Coordenador da linha de segurança ofensiva e red team
- Especialista em gestão de projetos *Predictive* no Project Management Institute
- Especialista em *SmartDefense*
- Especialista em *Web Application Penetration Tester* no eLearnSecurity
- *Junior Penetration Tester* no eLearnSecurity
- Graduado em Engenharia da Computação pela Universidade Politécnica de Madri

Uma experiência de capacitação única, fundamental e decisiva para impulsionar seu crescimento profissional"

10

Impacto para a sua carreira

Esse programa universitário foi criado com a intenção de orientar o aluno sobre os conhecimentos que o levarão a enfrentar qualquer situação no campo da cibersegurança. Dessa forma, a TECH se concentrará especificamente no ensino da mais alta qualidade, buscando a eficiência em cada um de seus cursos. Dessa forma, o profissional terá a garantia de um aprendizado especializado em *Pentesting* e *Red Team*.

A Red Team e outros aspectos de TI da cibersegurança podem ser integrados ao Pentesting por meio desse curso intensivo"

Técnicas avançadas de pivotamento são algumas das habilidades que você terá em suas mãos após este abrangente Executive Master de 12 meses.

Você está pronto para crescer profissionalmente? Uma excelente capacitação profissional espera por você.

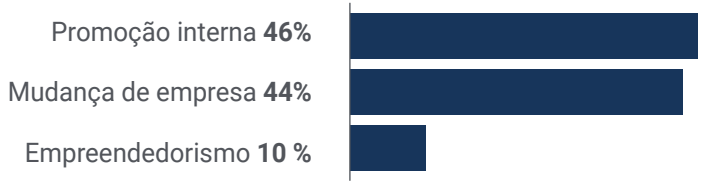
O Executive Master em Pentesting e Red Team da TECH é um programa intensivo que lhe prepara para enfrentar desafios e decisões de negócios na área de TI. Seu principal objetivo é promover seu crescimento pessoal e profissional. Ajudando você a obter sucesso.

Se você quer se superar, realizar uma mudança profissional positiva e se relacionar com os melhores, este é o lugar certo para você.

Aproveite essa oportunidade de expandir suas habilidades em Pentesting por meio da TECH, a melhor universidade online do mundo de acordo com a Forbes.

Momento da mudança

Tipo de mudança



Melhoria salarial

A conclusão deste programa pode representar um aumento salarial anual de mais de 25,55% para nossos alunos.

11

Benefícios para a sua empresa

Esse programa ajuda a elevar o talento da organização ao seu potencial máximo por meio da capacitação de líderes de alto nível.

Além disso, participar dessa opção universitária é uma oportunidade única de acessar uma poderosa rede de contatos para encontrar futuros parceiros profissionais, clientes ou fornecedores.

Na era digital, os gestores precisam integrar novos processos e estratégias que geram mudanças significativas e desenvolvimento organizacional. Isso só é possível por meio de capacitação e atualização universitária"

Desenvolver e reter o talento nas empresas é o melhor investimento a longo prazo.

01

Crescimento do talento e do capital intelectual

O profissional irá proporcionar à empresa novos conceitos, estratégias e perspectivas que poderão gerar mudanças relevantes na organização.

02

Retenção de gestores de alto potencial para evitar a evasão de talentos

Esse programa fortalece o vínculo entre empresa e profissional e abre novos caminhos para o crescimento profissional dentro da companhia.

03

Construindo agentes de mudança

Ser capaz de tomar decisões em tempos de incerteza e crise, ajudando a organização a superar obstáculos.

04

Maiores possibilidades de expansão internacional

Graças a este programa, a empresa entrará em contato com os principais mercados da economia mundial.

05

Desenvolvimento de projetos próprios

O profissional poderá trabalhar em um projeto real ou desenvolver novos projetos na área de P&D ou desenvolvimento de negócio da sua empresa.

06

Aumento da competitividade

Este programa proporcionará aos profissionais as habilidades necessárias para assumir novos desafios e impulsionar a empresa.

12

Certificado

O Executive Master em Pentesting e Red Team garante, além da capacitação mais rigorosa e atualizada, o acesso a um título de Mestrado Próprio emitido pela TECH Universidade Tecnológica.

Conclua este programa de estudos com sucesso e receba o seu certificado sem sair de casa e sem burocracias”

Este **Executive Master em Pentesting e Red Team** conta com o conteúdo mais completo e atualizado do mercado.

Uma vez aprovadas as avaliações, o aluno receberá por correio o certificado* do **Executive Master** emitido pela **TECH Universidade Tecnológica.**

O certificado emitido pela **TECH Universidade Tecnológica** expressará a qualificação obtida no Executive Master, atendendo aos requisitos normalmente exigidos pelas bolsas de empregos, concursos públicos e avaliação de carreira profissional.

Título: **Executive Master em Pentesting e Red Team**

Modalidade: **online**

Duração: **12 meses**


tech universidade tecnológica

Outorga o presente

CERTIFICADO

a

Sr./Sra. _____, com documento de identidade nº_____

por ter concluído e aprovado com sucesso o programa de

EXECUTIVE MASTER

em

Pentesting e Red Team

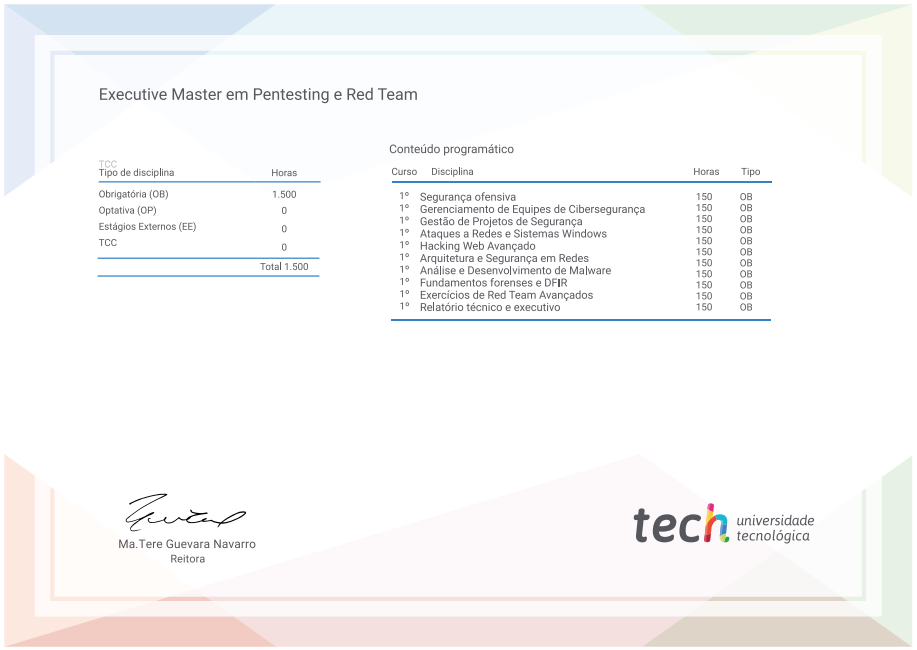
Este é um curso próprio desta Universidade, com duração de 1.500 horas, com data de início dd/mm/aaaa e data final dd/mm/aaaaa.

A TECH é uma Instituição Privada de Ensino Superior reconhecida pelo Ministério da Educação Pública em 28 de junho de 2018.

Em 17 de junho de 2020

Ma.Tere Guevara Navarro
Reitora

código único TECH: AFWOR23S techtitute.com/titulos


Executive Master em Pentesting e Red Team

TCC

Tipo de disciplina	Horas
Obrigatória (OB)	1.500
Optativa (OP)	0
Estágios Externos (EE)	0
TCC	0
	Total 1.500

Conteúdo programático

Curso	Disciplina	Horas	Tipo
1º	Segurança ofensiva	150	OB
1º	Gerenciamento de Equipes de Cibersegurança	150	OB
1º	Gestão de Projetos de Segurança	150	OB
1º	Ataques a Redes e Sistemas Windows	150	OB
1º	Hacking Web Avançado	150	OB
1º	Arquitetura e Segurança em Redes	150	OB
1º	Análise e Desenvolvimento de Malware	150	OB
1º	Fundamentos forenses e DFIR	150	OB
1º	Exercícios de Red Team Avançados	150	OB
1º	Relatório técnico e executivo	150	OB

Ma.Tere Guevara Navarro
Reitora

tech universidade tecnológica

*Apostila de Haia: Caso o aluno solicite que seu certificado seja apostilado, a TECH EDUCATION providenciará a obtenção do mesmo a um custo adicional.

tech universidade tecnológica

Executive Master
Pentesting e Red Team

- Modalidade: **online**
- Duração: **12 meses**
- Certificado: **TECH Universidade Tecnológica**
- Horário: **no seu próprio ritmo**
- Provas: **online**

Executive Master

Pentesting e Red Team

tech universidade tecnológica