
CYBER
ACADEMY
FEBRABAN

MÓDULO 11

Carreira em Cyber

A cibersegurança tornou-se um pilar fundamental para as empresas em um mundo cada vez mais digitalizado. Com o aumento da dependência de sistemas e dados online, as ameaças cibernéticas se tornaram mais sofisticadas e frequentes. Nesse contexto, o papel do profissional de cibersegurança é crucial para proteger as organizações contra-ataques, vazamentos de dados e outras violações de segurança.

Por que os profissionais de cibersegurança são tão importantes?

• Proteção de Dados: Os profissionais de cibersegurança são responsáveis por proteger os dados confidenciais das empresas e de seus clientes, evitando vazamentos que podem causar danos financeiros e reputacionais.
• Prevenção de Ataques: Eles implementam medidas de segurança para prevenir ataques cibernéticos, como phishing, Ransomware e ataques DDoS, que podem paralisar as operações de uma empresa.
• Conformidade com Regulamentações: As empresas precisam cumprir diversas leis e regulamentações de proteção de dados, e os profissionais de cibersegurança garantem que as organizações estejam em conformidade.
• Continuidade dos Negócios: Um incidente de segurança cibernética pode causar interrupções significativas nas operações de uma empresa. Os profissionais de cibersegurança trabalham para minimizar o impacto desses incidentes e garantir a continuidade dos negócios.

Quais Profissionais de Cibersegurança são Mais Procurados?

O mercado de trabalho para profissionais de cibersegurança está em constante crescimento, e algumas especializações são particularmente demandadas:

• Analista de Segurança da Informação: Responsável por identificar e avaliar vulnerabilidades em sistemas e redes, além de implementar medidas de segurança para protegê-los.

• Engenheiro de Segurança: Projeta e implementa soluções de segurança para proteger infraestruturas de TI.
• Especialista em Segurança de Redes: Foca na segurança de redes de computadores, incluindo firewalls, sistemas de detecção de intrusão e VPNs.
• Especialista em Segurança de Aplicativos: Responsável por garantir a segurança de aplicativos web e móveis.
• Especialista em Resposta a Incidentes: Lidam com incidentes de segurança, como ataques cibernéticos e vazamentos de dados, realizando as ações necessárias para minimizar os danos.
• Especialista em Governança de Risco e Conformidade: Garantem que a empresa esteja em conformidade com as leis e regulamentações de proteção de dados, além de gerenciar os riscos de segurança.

Habilidades Essenciais para um Profissional de Cibersegurança

• Conhecimento técnico: É fundamental ter conhecimento em redes, sistemas operacionais, segurança de aplicativos e ferramentas de segurança.
• Pensamento crítico: A capacidade de analisar situações complexas e identificar possíveis ameaças é essencial.
• Capacidade de resolução de problemas: Os profissionais de cibersegurança precisam ser capazes de encontrar soluções para problemas de segurança de forma rápida e eficiente.
• Adaptabilidade: O cenário de ameaças cibernéticas está em constante evolução, por isso é importante ser capaz de se adaptar às novas tecnologias e tendências.

Equipes Especializadas em Cibersegurança

Com o aumento das ameaças cibernéticas e cada vez mais poder computacional, o mercado precisou criar equipes especializadas em cibersegurança, a fim de garantir a segurança de seus sistemas e dados, e por conta disso, surgiram equipes chamadas Red Team, Blue Team, White Team, Purple Team, CSIRT e DFIR. Vamos falar um pouco de cada uma delas, abordando seus objetivos e funções específicas:

1. Red Team

Objetivo:
Simular ataques cibernéticos para identificar vulnerabilidades nos sistemas e processos da empresa.

Funções:
• Pentesting: Realiza testes de penetração para encontrar falhas na segurança.
• Engenharia Social: Simula ataques de engenharia social para avaliar a conscientização dos funcionários.

• Ataques direcionados: Simula ataques específicos, como Ransomware ou phishing, para testar a resposta da empresa.
• Perfil: Profissionais com habilidades avançadas em hacking ético, conhecimento profundo em sistemas operacionais, redes e programação.

2. Blue Team

Objetivo:
Defender os sistemas e dados da empresa contra-ataques cibernéticos.

Funções:
• Monitoramento: Monitora continuamente os sistemas em busca de atividades suspeitas.
• Incident Response: Responde a incidentes de segurança, contendo a ameaça e restaurando os sistemas.
• Análise forense: Analisa os incidentes para identificar a causa raiz e prevenir futuros ataques.
• Perfil: Profissionais com conhecimento em análise de malware, segurança de redes, sistemas de detecção de intrusão e análise forense.

3. White Team

Objetivo:
Arbitrar e mediar entre o Red Team e o Blue Team, garantindo que os testes sejam realizados de forma ética e segura.

Funções:
• Definição de escopo: Define o escopo dos testes, garantindo que não haja danos aos sistemas da empresa.
• Revisão de resultados: Analisa os resultados dos testes e fornece feedback para o Red Team e o Blue Team.
• Gerenciamento de riscos: Avalia os riscos associados aos testes e implementa medidas de mitigação.
• Perfil: Profissionais com experiência em gestão de projetos, segurança da informação e resolução de conflitos.

4. Purple Team

Objetivo:
Integrar as atividades do Red Team e do Blue Team para melhorar a postura de segurança da empresa de forma contínua.

Funções:

- Planejamento conjunto: Planeja e executa testes de penetração em conjunto com o Blue Team.
- Melhoria contínua: Utiliza os resultados dos testes para melhorar os processos de segurança da empresa.
- Automatização: Automatiza os processos de teste e resposta a incidentes.
- Perfil: Profissionais com habilidades tanto em ataque quanto em defesa, além de conhecimento em automação e orquestração de segurança.

CSIRT (Computer Security Incident Response Team)

Objetivo:
Responder a incidentes de segurança de forma rápida e eficiente, minimizando os danos à empresa.

Funções:

- Detecção: Detecta e investiga incidentes de segurança.
- Contenção: Contém a ameaça e impede sua propagação.
- Erradicação: Remove a ameaça dos sistemas.
- Recuperação: Restaura os sistemas afetados e implementa medidas para evitar a recorrência do incidente.
- Perfil: Profissionais com experiência em resposta a incidentes, análise forense e comunicação.

DFIR (Digital Forensics and Incident Response)

Objetivo:
Investigar incidentes de segurança para identificar a causa raiz, coletar evidências e auxiliar em processos legais.

Funções:

- Aquisição de evidências: Coleta e preserva evidências digitais de forma forense.
- Análise: Analisa as evidências para identificar a natureza e o escopo do incidente.
- Relatório: Elabora relatórios detalhados sobre os resultados da investigação.
- Perfil: Profissionais com conhecimento em análise forense digital, leis e regulamentações relacionadas à cibersegurança.

Certificações voltadas às equipes especializadas em Cibersegurança

Apresentamos abaixo, uma coletânea de certificações relacionadas a cada área de especialidade acima abordada, que atualmente são bem-vistas pelas empresas, no sentido de validar a expertise e aumentar a confiança das empresas na contratação e desenvolvimento de suas equipes.

Red Team:

- Pentest: CEH (Certified Ethical Hacker), OSCP (Offensive Security Certified Professional), CPT (Certified Penetration Tester).
- Engenharia Social: CHFI (Certified Hacking Forensic Investigator).
- Ataques direcionados: GCIH (GIAC Certified Incident Handler).

Blue Team:

- Monitoramento: GCIH (GIAC Certified Incident Handler), Security+, CISSP (Certified Information Systems Security Professional).
- Incident Response: GCIH, CSSP.
- Análise forense: CHFI, EnCE (EnCase Certified Examiner).

White Team:

- Gestão de Projetos: PMP (Project Management Professional), CSM (Certified ScrumMaster).
- Segurança da Informação: CISSP, CISM (Certified Information Security Manager).

Purple Team:

- Combinação de habilidades: CEH, OSCP, GCIH, CISSP.
- Automação: CCSP (Certified Cloud Security Professional).

CSIRT:

- Gerenciamento de Incidentes: GCIH, CSSP.
- Análise Forense: CHFI.

DFIR:

- Análise Forense: CHFI, EnCE.
- Investigação: CFCE (Certified Forensic Computer Examiner).

Certificações Gerais de Cibersegurança

Além das certificações específicas para cada equipe, algumas certificações gerais são altamente valorizadas pelas empresas, como:

- CISSP: A certificação mais abrangente em segurança da informação. Certificação de nível avançado que abrange uma ampla gama de tópicos de segurança, incluindo gerenciamento de risco, segurança de rede, criptografia e segurança de software.
- CISM: Certificação focada em gestão de segurança da informação, abordando aspectos como governança, gerenciamento de riscos e programas de conformidade.
- CISA: Certificação para auditores de sistemas de informação.
- CompTIA Security+: Certificação de nível intermediário em segurança cibernética e muito bem-vista pelas empresas na hora da contratação, além de ser uma certificação intermediária em nível de dificuldade, frente a certificações como CISM ou CISSP.

Alguns fatores a serem considerados ao escolher uma certificação:

- Alinhamento com o cargo: Escolha certificações que correspondam às suas responsabilidades e aos requisitos do seu trabalho.
- Nível de experiência: Algumas certificações exigem mais experiência do que outras.
- Interesses: Escolha certificações que abrangem áreas que você considera mais interessantes.
- Reconhecimento do mercado: Verifique quais certificações são mais valorizadas pelas empresas do seu setor.
- Também vale salientar algumas informações úteis para quem vai buscar treinamentos e certificações:

Organizações certificadoras conhecidas

- ISC2
- CompTIA
- EC-Council
- GIAC

Exemplos de plataformas de treinamento

- Udemy
- Coursera
- Cybrary

Referências Bibliográficas:

Capeletti, Lucas. Fundamentos de Gestão de Acesso e Identidade (IAM) (Portuguese Edition).
Lisboa Melo, Jefferson; Vieira de Oliveira, Alexandre; Mauser, Daniel. Do Iniciante ao Profissional em Segurança Cibernética. SF Editorial e AcademiaTI.
Fernandes, Victor. Inteligência Artificial para Leigos (Portuguese Edition).
Wendt, Emerson; Jorge, Higor Vinicius Nogueira. Crimes Cibernéticos 3a edição: Ameaças e procedimentos de investigação (Portuguese Edition). BRASPORT.
Baars, Hans; Hintzbergen, Kees; Hintzbergen, Jule; Smulders, André. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002 (Portuguese Edition). BRASPORT.
R., Raphael. Segurança Cibernética: Protegendo Infraestruturas e Dados (Portuguese Edition).

CYBER
ACADEMY

FEBRABAN