GUIA DO CANDIDATO – SFDE

Security Fundamentals Defensive Engineer

---

1. Apresentação

A certificação SFDE (Security Fundamentals Defensive Engineer) é destinada a profissionais que atuam ou desejam atuar no campo da engenharia defensiva em segurança da informação, com foco em arquitetura segura, detecção, monitoramento, mitigação e resposta a incidentes. Ela atesta o domínio de competências fundamentais para proteger sistemas, redes e dados contra ameaças cibernéticas.

O exame é realizado uma vez ao ano, e o direito de participação só pode ser adquirido por meio da nossa loja oficial. A compra do direito de certificação garante o acesso às instruções do exame, aos recursos necessários para a realização e à data oficial, que é informada após a aquisição. A compra não garante a certificação, apenas o direito de realizar a prova.

A loja oficial também oferece cursos preparatórios voltados à capacitação dos candidatos, abordando os temas cobrados na certificação.

---

2. Estrutura da Avaliação

A certificação SFDE é composta por duas etapas eliminatórias:

- Prova Teórica: 30 questões de múltipla escolha, com foco na avaliação de conceitos e conhecimentos fundamentais.
- Prova Prática (CTF): Simulação de 24 horas com foco em detecção, resposta e mitigação de incidentes de segurança.

A aprovação em ambas as etapas é obrigatória para a obtenção da certificação. A prova prática será disponibilizada em uma máquina virtual (VM) que simula um ambiente corporativo com incidentes ativos. O candidato deverá realizar monitoramento, análise e resposta a ataques, documentando evidências e propondo contra-medidas.

---

3. Conteúdos Abordados

Os temas cobrados na certificação SFDE incluem, mas não se limitam a:

- Conceitos fundamentais de segurança da informação
- Fundamentos de protocolos de rede
- Criptografia aplicada à segurança de redes
- Sistemas de detecção e prevenção de intrusos (IDS/IPS)
- Monitoramento e análise de logs
- Resposta a incidentes e análise forense básica
- Reconhecimento de padrões de ataque
- Firewall e hardening de sistemas
- Arquitetura de rede segura
- Detecção de anomalias e análise de comportamento
- Segurança de endpoints
- Gestão de vulnerabilidades
- SIEM (Security Information and Event Management)
- Engenharia de segurança defensiva
- Vulnerabilidades em redes wireless e medidas preventivas
- Simulação de ataques para validação de segurança (purple teaming)

---

4. Requisitos Técnicos

O candidato deverá:

- Ter conhecimento intermediário de sistemas Linux e Windows.
- Ter familiaridade com ferramentas de monitoramento e análise.
- Estar apto a importar uma VM no VirtualBox.

- Ser capaz de trabalhar com captura e análise de pacotes, logs, alertas e relatórios.

---

5. Avaliação

- Nota mínima para aprovação: 70% na prova teórica e desempenho satisfatório na prática (conforme critérios de correção).
- Formato da prova prática: CTF (Capture The Flag) com foco em monitoramento, identificação e mitigação de incidentes.
- Duração da prova prática: 24 horas corridas.
- Entrega: Relatório detalhado de evidências, análise e proposta de contra-medidas.

---

6. Considerações Finais

- Os candidatos aprovados receberão certificado oficial, número de registro e selo digital verificável.
- O candidato é responsável por sua preparação, sendo os cursos oficiais recomendados, mas não obrigatórios.
- Dúvidas e informações adicionais podem ser consultadas diretamente no portal ou através do nosso canal de atendimento.

Loja oficial: https://securityforge.org/loja/