

PÚBLICO

Este curso é destinado a profissionais de SecOps responsáveis pela implementação, pelo ajuste e pela manutenção diária do F5 Advanced WAF. Os participantes adquirirão um nível funcional de conhecimento sobre o F5 Advanced WAF, incluindo configuração abrangente de políticas e perfis de segurança, avaliação de clientes e aplicação dos tipos adequados de mitigação.

PRÉ-REQUISITOS

Recomenda-se que o participante possua conhecimentos e experiência em tecnologias gerais de redes antes de frequentar qualquer curso conduzido por instrutor da F5 Global Training Services, incluindo:

- Encapsulamento no modelo OSI
- Roteamento e switching
- Ethernet e ARP
- Conceitos de TCP/IP
- Endereçamento IP e subnetting
- NAT e endereçamento IP privado
- Gateway padrão
- Firewalls de rede
- Diferenças entre LAN e WAN

VISÃO

Esse treinamento é destinado a administradores de segurança de aplicações responsáveis pela implementação do F5 Advanced Web Application Firewall para proteger aplicações web contra vulnerabilidades comuns e ataques de negação de serviço.

Os tópicos abordam a identificação e a mitigação de vulnerabilidades em aplicações web, considerando tanto o lado do cliente quanto o lado da aplicação no espectro de ameaças. As áreas de estudo incluem fundamentos do Advanced WAF, mitigação de vulnerabilidades, defesa contra bots e outros ataques automatizados, além de cenários adicionais de implementação.

As habilidades são desenvolvidas por meio de uma combinação de apresentações em vídeo e demonstrações práticas de laboratório, acompanhadas de materiais de apoio que fornecem exemplos de configuração.

Capítulo 1: Introdução ao Sistema BIG-IP

Configuração Inicial do Sistema BIG-IP

Arquivamento da Configuração do BIG-IP

Utilização dos Recursos e Ferramentas de Suporte da F5

Capítulo 2: Processamento de Tráfego com o BIG-IP

Identificação dos Objetos de Processamento de Tráfego do BIG-IP

Compreensão dos Perfis

Visão Geral das Políticas de Tráfego Local

Visualização do Fluxo de Requisições HTTP

Capítulo 3: Visão Geral do Processamento de Aplicações Web

Web Application Firewall: Proteção de Camada 7

Verificações de Segurança da Camada 7

Visão Geral dos Elementos de Comunicação Web

Visão Geral da Estrutura de uma Requisição HTTP

Análise das Respostas HTTP

Como o F5 Advanced WAF Analisa Tipos de Arquivo, URLs e Parâmetros

Utilização do Proxy HTTP Fiddler

Capítulo 4: Visão Geral das Vulnerabilidades em Aplicações Web

Uma Taxonomia de Ataques: o Cenário de Ameaças

Explorações Comuns contra Aplicações Web

Capítulo 5: Implementação de Políticas de Segurança — Conceitos e Terminologia

Definição de Aprendizado

Comparação entre Modelos de Segurança Positivo e Negativo

Fluxo de Trabalho de Implementação

Atribuição de Política ao Servidor Virtual

Fluxo de Trabalho de Implementação: Uso de Configurações Avançadas

Configuração das Tecnologias de Servidor

Definição de Assinaturas de Ataque

Visualização de Requisições

Verificações de Segurança Oferecidas pelo Rapid Deployment

Capítulo 6: Ajuste de Políticas e Violações

Processamento de Tráfego após a Implementação

Como as Violações são Categorizadas

Classificação de Violações: uma Escala de Ameaças

Definição de Staging e Enforcement

Definição do Modo de Enforcement

Definição do Período de Preparação para Enforcement

Revisão da Definição de Aprendizado

Definição de Sugestões de Aprendizado

Escolha entre Aprendizado Automático ou Manual

Definição das Configurações Learn, Alarm e Block

Interpretação do Resumo de Preparação para Enforcement

Configuração da Página de Resposta de Bloqueio

Capítulo 7: Utilização de Assinaturas de Ataque e Campanhas de Ameaças

Definição de Assinaturas de Ataque

Fundamentos das Assinaturas de Ataque

Criação de Assinaturas de Ataque Personalizadas

Definição dos Modos de Edição Simples e Avançado

Definição de Conjuntos de Assinaturas de Ataque

Definição de Pools de Assinaturas de Ataque

Compreensão das Assinaturas de Ataque e do Staging

Atualização das Assinaturas de Ataque

Definição de Campanhas de Ameaças

Implementação de Campanhas de Ameaças

Capítulo 8: Construção de Políticas de Segurança Positiva

Definição e Aprendizado dos Componentes da Política de Segurança

Definição de Wildcard

Definição do Ciclo de Vida das Entidades

Escolha do Esquema de Aprendizado

Como Aprender: Never — Somente Wildcard

Como Aprender: Always

Como Aprender: Selective

Revisão do Período de Preparação para Enforcement: Entidades

Visualização das Sugestões de Aprendizado e do Status de Staging

Definição da Pontuação de Aprendizado

Definição de Endereços IP Confiáveis e Não Confiáveis

Como Aprender: Compact

Capítulo 9: Proteção de Cookies e Outros Tópicos Relacionados a Cabeçalhos

Finalidade dos Cookies do F5 Advanced WAF

Definição de Cookies Permitidos e Obrigatórios

Proteção de Cabeçalhos HTTP

Capítulo 10: Relatórios Visuais e Logs

Visualização dos Dados de Resumo de Segurança da Aplicação

Relatórios: Criação de uma Visualização Personalizada

Relatórios: Gráficos Baseados em Filtros

Estatísticas de Ataques de Força Bruta e Web Scraping

Visualização de Relatórios de Recursos

Conformidade PCI: PCI-DSS 3.0

Análise de Requisições

Recursos e Destinos de Logs Locais

Visualização de Logs no Utilitário de Configuração

Definição do Perfil de Logging

Configuração do Logging de Respostas

Capítulo 11: Projeto de Laboratório 1

Capítulo 12: Tratamento Avançado de Parâmetros

Definição de Tipos de Parâmetros

Definição de Parâmetros Estáticos

Definição de Parâmetros Dinâmicos

Definição de Níveis de Parâmetros

Outras Considerações sobre Parâmetros

Capítulo 13: Construção Automática de Políticas

Definição de Templates que Automatizam o Aprendizado

Definição de Flexibilização de Políticas

Definição de Restrição de Políticas

Definição da Velocidade de Aprendizado: Amostragem de Tráfego

Definição do Rastreamento de Alterações no Site

Capítulo 14: Integração com Scanners de Vulnerabilidades de Aplicações Web

Integração da Saída do Scanner

Importação de Vulnerabilidades

Correção de Vulnerabilidades
Utilização do Arquivo XSD do Scanner XML Genérico

Capítulo 15: Implementação de Políticas em Camadas
Definição de uma Política Pai
Definição de Herança
Casos de Uso para Implementação de Políticas Pai

Capítulo 16: Controle de Login e Mitigação de Ataques de Força Bruta
Definição de Páginas de Login para Controle de Fluxo
Configuração da Detecção Automática de Páginas de Login
Definição de Ataques de Força Bruta
Configuração da Proteção contra Força Bruta
Mitigações de Força Bruta Baseadas na Origem
Definição de Credential Stuffing
Mitigação de Credential Stuffing

Capítulo 17: Reconhecimento com Rastreamento de Sessão
Definição de Rastreamento de Sessão
Configuração de Ações após a Detecção de Violações

Capítulo 18: Mitigação de Negação de Serviço na Camada 7
Definição de Ataques de Negação de Serviço
Definição do Perfil de Proteção contra DoS
Visão Geral da Proteção contra DoS Baseada em TPS
Criação de um Perfil de Logging de DoS
Aplicação de Mitigações Baseadas em TPS
Definição de Detecção Comportamental e Baseada em Estresse

Capítulo 19: Proteção Avançada contra Bots
Classificação de Clientes com o Perfil de Bot Defense
Definição de Assinaturas de Bots
Definição de Fingerprinting da F5
Definição de Templates de Perfil de Bot Defense
Definição de Proteção para Microsserviços

Capítulo 20: Projetos Finais



Próximas turmas

03/11/2026

Carga horária	32 horas
Modalidade	Online
Horário	09:00 às 18:00

Prevista

24/11/2026

Carga horária	32 horas
Modalidade	Online
Horário	09:00 às 18:00

Prevista

08/12/2026

Carga horária 32 horas

Modalidade Presencial/São Paulo

Horário 09:00 às 18:00

Confirmado

14/12/2026

Carga horária 32 horas

Modalidade Online

Horário 08:00 às 12:00

Prevista

Fale com a InLearn

Acompanhe nossos canais e fale com a nossa equipe para saber mais sobre cursos, próximas turmas e soluções de capacitação.

WhatsApp: +55 (11) 92058-5393

[Site](#) · [LinkedIn](#) · [Instagram](#) · [Facebook](#) · [YouTube](#)

www.inlearn.com.br

Avenida Ipanema, 165, Dezoito do Forte Empresarial/Alphaville, Barueri
- SP, 06472-002

Documento gerado automaticamente a partir do
catálogo InLearn.