Configuring F5 Advanced WAF

Kód kurzu: F5_AWF

Cílem tohoto 4 denního školení je seznámit síťové a bezpečnostní specialisty či vlastníky webových aplikací s produktem F5 BIG-IP Advanced Web Application Firewall (dříve ASM) od základní konfigurace přes pokročilé techniky zabezpečení webových aplikací. V průběhu školení jsou diskutovány základní koncepce webových aplikací, jejich zranitelnosti a způsoby jak webovou aplikaci chránit před kybernetickými útoky prostřednictvím F5 Advanced WAF, a to včetně několika desítek labů k získání praktické zkušenosti. Kurz je zároveň schváleným a doporučeným zdrojem informací a znalostí pro složení certifikace F5 ASM 303.

Pro koho je kurz určen

Kurz určen síťovým, systémovým a bezpečnostním administrátorům či vývojářům nebo vlastníkům webových aplikací zodpovědným za ochranu webových aplikací vůči kybernetickým útokům.

Co Vás naučíme

Cílem tohoto 4 denního školení je seznámit síťové a bezpečnostní specialisty či vlastníky webových aplikací s produktem F5 BIG-IP Advanced Web Application Firewall (dříve ASM) od základní konfigurace přes pokročilé techniky zabezpečení webových aplikací. V průběhu školení jsou diskutovány základní koncepce webových aplikací, jejich zranitelnosti a způsoby jak webovou aplikaci chránit před kybernetickými útoky prostřednictvím F5 Advanced WAF, a to včetně několika desítek labů k získání praktické zkušenosti. Kurz je zároveň schváleným a doporučeným zdrojem informací a znalostí pro složení certifikace F5 ASM 303.

Požadované vstupní znalosti

Základní znalost http protokolu a koncepcí webových aplikací, základní znalost bezpečnostních koncepcí, všeobecnou síťovou terminologii

Osnova kurzu

- Základní nastavení F5 Advanced Web Application Firewall
- Koncepty zabezpečení webové aplikace
- Koncepce http protokolu
- Nejčastější chyby v zabezpečení webových aplikací a způsoby jak tyto chyby zneužít
- Tvorba bezpečnostní politiky
- Práce s nástrojem pro stavbu a ladění bezpečnostních politik
- Konfigurace a správa signatur
- Konfigurace a správa ochrany detekce kampaní kybernetických útoků
- Reporting a monitoring
- Pozitivní bezpeční politika
- Ochrana cookies, headrů, URL a parametrů
- Integrace s VAT (Vulnerability Assement Tool)
- Session/Username tracking
- L7 DoS ochrana
- Detekce a ochrana proti robotickým útokům
- Ochrana webové aplikace pomocí DataSafe

GOPAS Praha
Na Strži 2097/63
140 00 Praha 4 - Krč
Tel.: +420 226 201 390
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 530 513 590
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 902 903 132
info@gopas.sk

Copyright © 2026 GOPAS, a.s.,
All rights reserved