Configuring F5 Advanced WAF (previously licensed as ASM) (TRG-BIG-AWF-CFG)

ID TRG-BIG-AWF-CFG **Preis** US $ 5'280.– (exkl. MwSt.) **Dauer** 4 Tage

Zielgruppe

Dieser Kurs richtet sich an SecOps-Experten, die für die Bereitstellung, Anpassung und tägliche Wartung von F5 Advanced WAF verantwortlich sind. Die Teilnehmer erhalten ein funktionelles Mass an Fachwissen zu F5 Advanced WAF, darunter die umfassende Konfiguration von Sicherheitsrichtlinien und -profilen, Client-Beurteilungen und geeignete Arten der Angriffsabwehr.

- Erfahrung mit LTM ist nicht erforderlich.
- Vorkenntnisse zu WAF sind nicht erforderlich.
- Dieser Kurs steht auf der Liste der genehmigten Studienressourcen für die F5-ASM-303-Zertifizierungsprüfung.

Voraussetzungen

Sie müssen mindestens einen Punkt der folgenden Voraussetzungen erfüllen, um am Advanced WAF Training teilzunehmen:

- Bestehen der F5 Big-IP Zertifizierung (201)
- Bestehen der Admin Equivalence Prüfung (mind. 70%)
- oder Teilnahme am Administering BIG-IP (TRG-BIG-OP-ADMIN)

Die folgenden allgemeinen Kenntnisse und Erfahrungen im Bereich der Netzwerktechnologie werden vor der Teilnahme an einem von F5 Global Training Services geleiteten Kurs empfohlen:

- OSI-Modell Verkapselung
- Routing und Switching
- Ethernet und ARP
- TCP/IP-Konzepte
- IP-Adressierung und Subnetting
- NAT und private IP-Adressierung
- Standard-Gateway
- Netzwerk-Firewalls
- LAN vs. WAN

Kursziele

- Beschreibung der Rolle des BIG-IP-Systems als Vollproxy-Lösung in einem Anwendungsbereitstellungsnetzwerk
- Bereitstellung der F5 Advanced Web Application Firewall
- Festlegen einer Web Application Firewall
- Beschreibung des Schutzes von Webanwendungen durch die Sicherung von Dateitypen, URLs und Parametern mithilfe der F5 Advanced Web Application Firewall
- Bereitstellung der F5 Advanced Web Application Firewall unter Verwendung der Vorlage zur schnellen Bereitstellung (und anderer Vorlagen) und Definition der einzelnen Sicherheitsprüfungen
- Festlegen von Lern-, Alarm- und Blockierungseinstellungen, wie sie für die Konfiguration der F5 Advanced Web Application Firewall erforderlich sind
- Festlegen von Angriffssignaturen mitsamt Erklärung, warum das Staging von Angriffssignaturen wichtig ist
- Durchführen von Bedrohungskampagnen zum Schutz vor CVE-Bedrohungen
- Vergleich der Umsetzung positiver und negativer Sicherheitsrichtlinien und Erläuterung der einzelnen Vorteile
- Konfiguration der Sicherheitsverarbeitung auf der Parameterebene einer Webanwendung
- Integration der F5 Advanced Web Application Firewall mit dem Automatic Policy Builder
- Manuelle Anpassung einer Richtlinie oder Zulassung einer automatischen Richtlinienerstellung
- Integration der Informationen eines Anwendungsschwachstellen-Scanners von Drittanbietern in eine Sicherheitsrichtlinie
- Konfiguration der Anmeldungsdurchsetzung zur Kontrolle des Datenverkehrs
- Abwehr von Credential-Stuffing
- Konfiguration der Schutzmassnahmen gegen Brute-Force-Angriffe
- Bereitstellung einer erweiterten Bot-Abwehr gegen Web-Scraper, alle bekannten Bots und andere automatisierte Agents
- Bereitstellung von DataSafe zum Schutz clientseitiger Daten

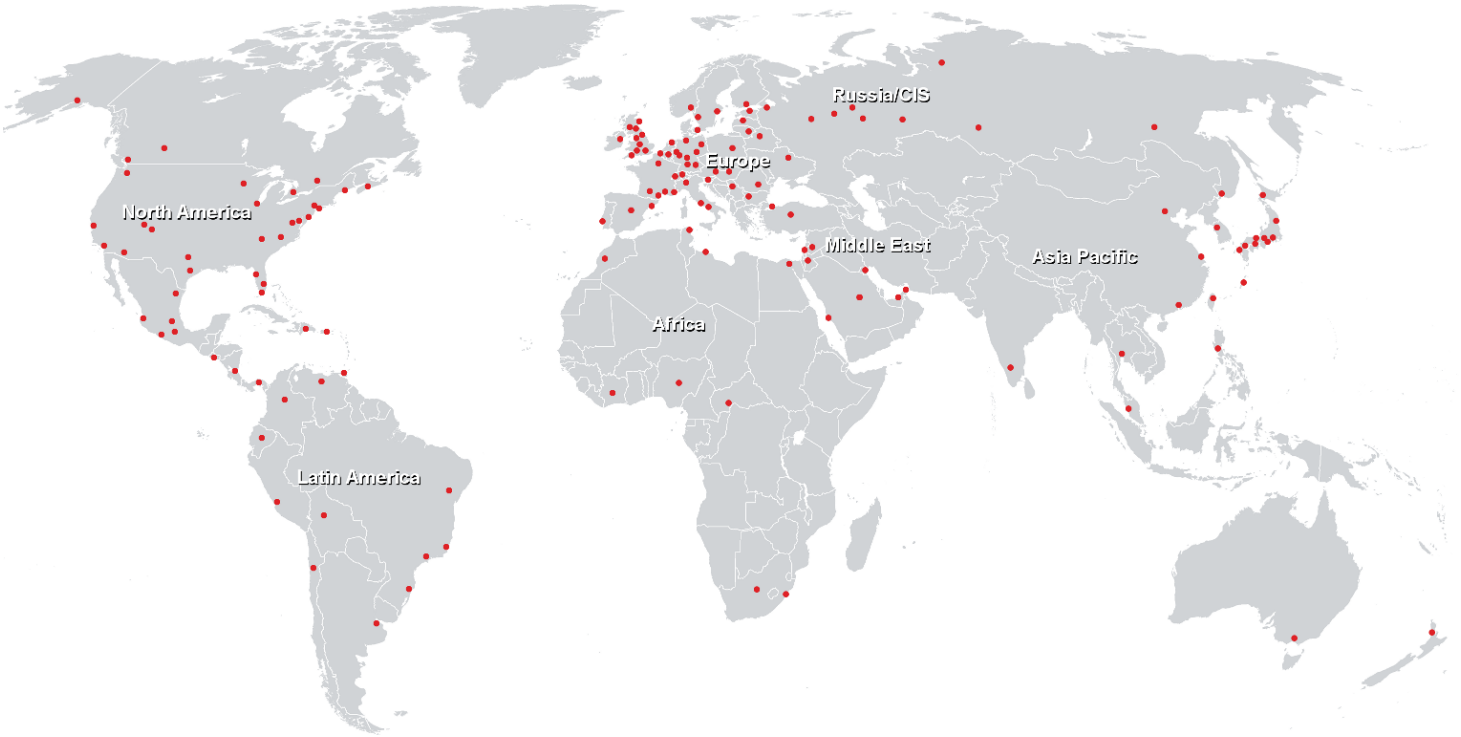
Kursinhalt

Configuring F5 Advanced WAF (previously licensed as ASM) (TRG-BIG-AWF-CFG)

- Ressourcenbereitstellung für die F5 Advanced Web Application Firewall
- Verarbeitung des Datenverkehrs mit dem BIG-IP Local Traffic Manager (LTM)
- Konzepte von Webanwendungen
- Verteidigung gegen die OWASP Top 10 und andere Sicherheitslücken
- Bereitstellung von Sicherheitsrichtlinien
- Anpassung von Sicherheitsrichtlinien
- Bereitstellung von Angriffssignaturen und Bedrohungskampagnen
- Positives Sicherheitsmodell
- Sichern von Cookies und anderen Headern
- Berichterstattung und Protokollierung
- Erweiterte Parameteroptionen
- Verwenden des Automatic Policy Builder
- Integration mit Webschwachstellen-Scannern
- Anmeldungsdurchsetzung zur Kontrolle des Datenverkehrs
- Abwehr von Brute-Force- und Credential-Stuffing-Angriffen
- Sitzungsverfolgung zur Client-Aufklärung
- Verwenden von über- und untergeordneten Richtlinien
- Schutz vor DoS-Angriffen auf Layer 7
    - DoS-Schutz auf Basis der Transaktionen pro Sekunde
    - Schutz vor verhaltensbasierten DoS-Angriffen auf Layer 7
- Konfiguration der erweiterten Bot-Abwehr
    - Schutz vor Web-Scraping und anderen Mikrodiensten
    - Arbeiten mit Bot-Signaturen
- Verwenden von DataSafe zum Schutz des Dokument-Objektmodells auf Client-Seite

Configuring F5 Advanced WAF (previously licensed as ASM) (TRG-BIG-AWF-CFG)

Weltweite Trainingscenter



Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch