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

Voraussetzungen

Die folgenden kostenlosen Kurse im Rahmen des „Self-Directed Training“ (SDT) sind zwar optional, aber für alle Teilnehmer hilfreich, die nur über begrenzte Erfahrung in der Verwaltung und Konfiguration von BIG-IP verfügen:

- Erste Schritte mit BIG-IP
- Erste Schritte mit Local Traffic Manager (LTM)
- Erste Schritte mit F5 Advanced WAF

Vor der Teilnahme an einem von F5 Global Training Services angebotenen Präsenzkurs werden allgemeine Kenntnisse und Erfahrungen im Bereich Netzwerktechnik empfohlen, darunter Kapselung nach dem OSI-Modell, Routing und Switching, Ethernet und ARP, TCP/IP-Konzepte, IP-Adressierung und Subnetzbildung, NAT und private IP-Adressierung, Standard-Gateway, Netzwerk-Firewalls sowie LAN im Vergleich zu WAN.

Kursziele

- Die Studierenden sollten in der Lage sein:
- Beschreiben Sie die Rolle des BIG-IP-Systems als vollwertiges Proxy-Gerät in einem Application Delivery Network.
- Bereitstellung der F5 Advanced Web Application Firewall
- Eine Webanwendungs-Firewall definieren
- Beschreiben Sie, wie die F5 Advanced Web Application Firewall eine Webanwendung schützt, indem sie Dateitypen, URLs und Parameter absichert.
- Stellen Sie die F5 Advanced Web Application Firewall mithilfe der Rapid-Deployment-Vorlage (und anderer Vorlagen) bereit und legen Sie die in den einzelnen Vorlagen enthaltenen Sicherheitsprüfungen fest
- Definieren Sie die Einstellungen für „Learn“, „Alarm“ und „Block“ im Zusammenhang mit der Konfiguration der F5 Advanced Web Application Firewall
- Definieren Sie Angriffssignaturen und erläutern Sie, warum die Einstufung von Angriffssignaturen wichtig ist
- Setzen Sie Bedrohungskampagnen ein, um sich vor CVE-Bedrohungen zu schützen
- Vergleichen Sie die Umsetzung positiver und negativer Sicherheitsmassnahmen und erläutern Sie die jeweiligen Vorteile.
- Konfigurieren der Sicherheitsverarbeitung auf Parameterebene einer Webanwendung
- Bereitstellung der F5 Advanced Web Application Firewall mithilfe des Automatic Policy Builder
- Eine Richtlinie manuell anpassen oder die automatische Erstellung von Richtlinien zulassen
- Die Ergebnisse von Schwachstellenscannern von Drittanbietern in eine Sicherheitsrichtlinie integrieren
- Anmeldungszwang für die Flusssteuerung konfigurieren
- Risiken durch Credential Stuffing mindern
- Schutz vor Brute-Force-Angriffen konfigurieren
- Setzen Sie „Advanced Bot Defense“ gegen Web-Scraper, alle bekannten Bots und andere automatisierte Programme ein
- Setzen Sie DataSafe ein, um clientseitige Daten zu schützen

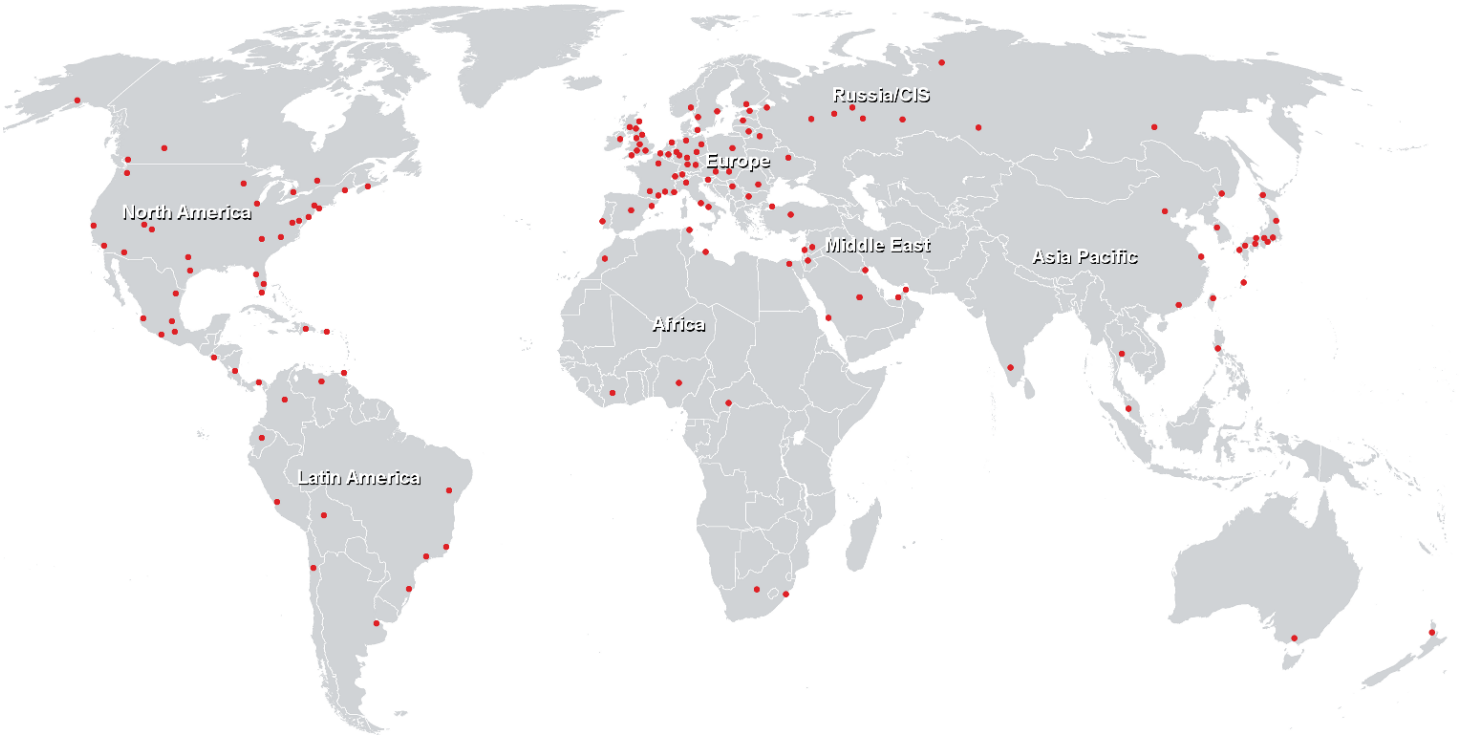
Kursinhalt

- Vorstellung des BIG-IP-Systems
- Datenverkehrsverarbeitung mit BIG-IP
- Überblick über die Verarbeitung von Webanwendungen
- Überblick über Sicherheitslücken in Webanwendungen
- Implementierung von Sicherheitsrichtlinien: Konzepte und Fachbegriffe
- Anpassung von Richtlinien und Verstösse
- Verwendung von Angriffssignaturen und Bedrohungskampagnen
- Entwicklung einer positiven Sicherheitspolitik
- Sicherheit von Cookies und andere Header-Themen
- Visuelle Berichterstellung und Protokollierung
- Laborprojekt 1
- Erweiterte Parameterverwaltung
- Automatische Richtlinienerstellung
- Integration mit Scannern zur Erkennung von Schwachstellen in Webanwendungen
- Bereitstellung mehrstufiger Richtlinien
- Durchsetzung der Anmeldevorschriften und Abwehr von Brute-Force-Angriffen
- Erkundung mit Sitzungsverfolgung
- Massnahmen zur Abwehr von Denial-of-Service-Angriffen auf Schicht 7

- Erweiterter Bot-Schutz
- Abschlussarbeiten

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