Setting up F5 Advanced WAF (TRG-BIG-AWF-SU1)

ID TRG-BIG-AWF-SU1 **Preis** US $ 1'100.– (exkl. MwSt.) **Dauer** 1 Tage

Zielgruppe

Dieser Kurs richtet sich an Sicherheits- und Netzwerkadministratoren, die für den Einsatz der F5 Advanced Web Application Firewall zum Schutz der Webanwendungen vor häufig auftretenden Sicherheitslücken und Denial-of-Service-Angriffen verantwortlich sind.

Voraussetzungen

Für diesen Kurs sind keine spezifischen Kenntnisse der F5-Technologie erforderlich. Für Teilnehmer mit begrenzter BIG-IP-Administrations- und Konfigurationserfahrung wäre es jedoch sehr hilfreich, die folgenden Kurse vor der Teilnahme an diesem Kurs zu absolvieren:

- Präsenzkurs zur Verwaltung von BIG-IP

oder

- F5-zertifizierter BIG-IP-Administrator

Die folgenden kostenlosen, webbasierten Schulungskurse sind zwar freiwillig, aber sehr hilfreich für alle Teilnehmer mit begrenzter BIG-IP-Administrations- und Konfigurationserfahrung.

- Erste Schritte mit BIG-IP
- Erste Schritte mit dem BIG-IP Application Security Manager (ASM)

Die folgenden allgemeinen Kenntnisse und Erfahrungen auf dem Gebiet der Netzwerktechnologie werden vor der Teilnahme an einem Präsenzkurs von F5 Global Training Services empfohlen:

- OSI-Modell-Kapselung
- Routing und Switching
- Ethernet und ARP
- TCP/IP-Konzepte
- IP-Adressen und Subnetze
- NAT und private IP-Adressen
- Standard-Gateway
- Netzwerk-Firewalls
- LAN vs. WAN

Kursziele

- Bereitstellung der Module Application Security Manager und Fraud Protection Service
- Festlegen einer Web Application Firewall
- Bereitstellung von F5 Advanced WAF unter Verwendung der geführten Konfiguration für die Anwendungssicherheit
- Festlegen von Lern-, Alarm- und Blockierungseinstellungen, wie sie für die Konfiguration von F5 Advanced WAF erforderlich sind
- Festlegen von Angriffssignaturen mitsamt Erklärung, warum das Staging von Angriffssignaturen wichtig ist
- Vergleich der Umsetzung positiver und negativer Sicherheitsrichtlinien und Erläuterung der einzelnen Vorteile
- Manuelle Abstimmung einer Richtlinie durch Prüfung von Lernvorschlägen
- Durchführen einer Bedrohungskampagne
- Abwehr von Credential-Stuffing-Angriffen
- Sicherung einer URL mithilfe der DataSafe-Verschlüsselungs- und -Verschleierungsoptionen zum Schutz vor betrügerischen Aktionen auf Client-Seite
- Bereitstellung von F5 Advanced WAF unter Verwendung der geführten Konfiguration für die Denial-of-Service-Abwehr auf Layer7
- Verwenden der automatischen, verhaltensgesteuerten Denial-of-Service-Abwehr auf Layer7, um DoS-Angriffe zu erkennen und abzuwehren

Kursinhalt

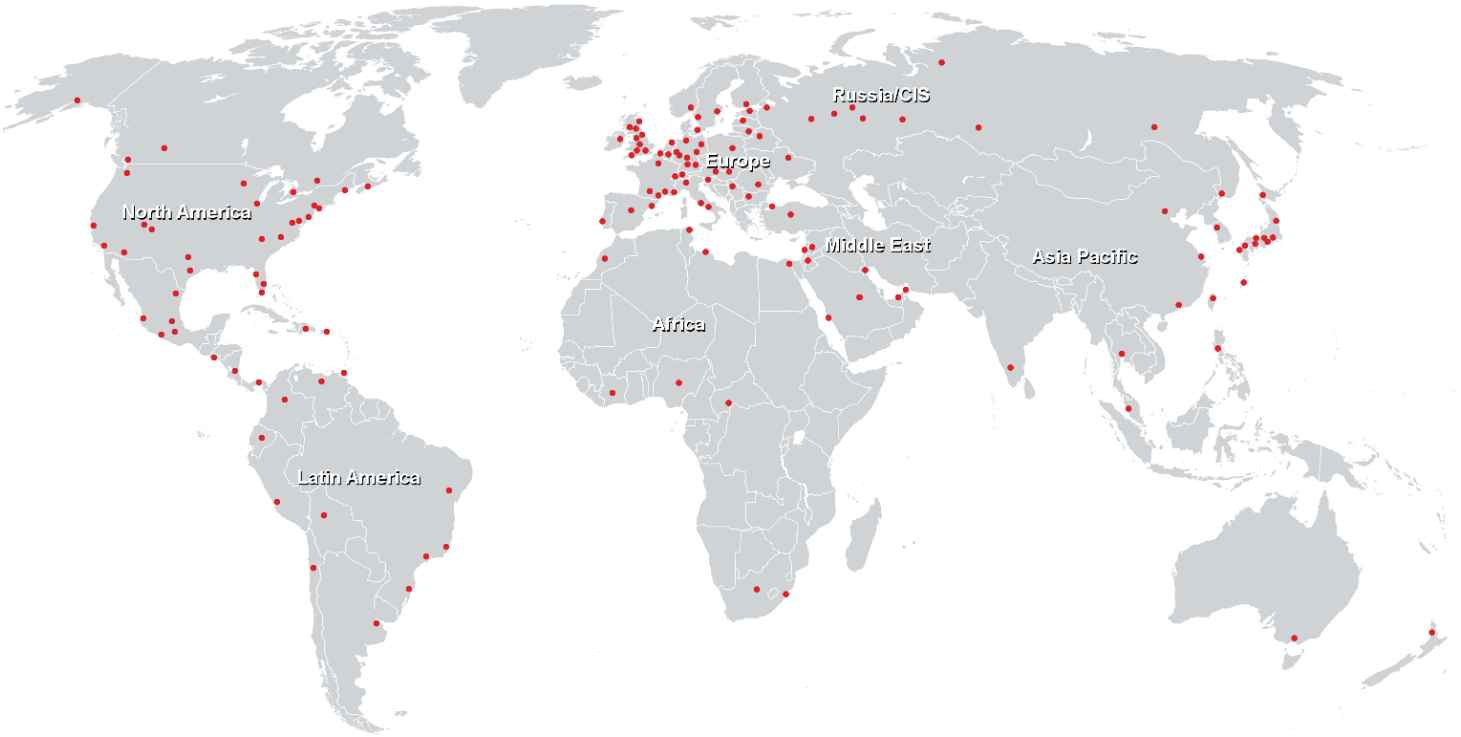
- Unterscheidung zwischen clientseitigen und anwendungsseitigen Web-Schwachstellen
- Kategorisierung von Angriffstechniken
- Verwenden der geführten Konfiguration, um eine Sicherheitsrichtlinie für Webanwendungen zu implementieren
- Definition der wichtigsten Teile einer Webanwendungs-Sicherheitsrichtlinie
- Erklärung der Optionen zur Protokollierung von Anfragen
- Identifizieren von HTTP-Headern und -Methoden
- Festlegen von Angriffssignaturen, des Stagings von Angriffssignaturen und entsprechenden Verletzungen

Setting up F5 Advanced WAF (TRG-BIG-AWF-SU1)

- Überblick über die OWASP Top 10
- Prüfen von Lernvorschlägen und grundlegenden Richtlinienabstimmungen
- Durchführen einer Bedrohungskampagne
- Abwehr von Credential-Stuffing
- Sicherung einer URL mithilfe der DataSafe-Verschlüsselungs- und -Verschleierungsoptionen zum Schutz vor betrügerischen Aktionen auf Client-Seite
- Verwenden der automatischen, verhaltensgesteuerten Denial-of-Service-Abwehr auf Layer7, um DoS-Angriffe zu erkennen und abzuwehren

Setting up F5 Advanced WAF (TRG-BIG-AWF-SU1)

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