

## Firewall:

# OPTIMIZING FIREWALL THREAT PREVENTION (EDU-214)

## ÜBERBLICK

Der Kurs Palo Alto Networks Firewall Essentials: Optimizing Firewall Threat Prevention (EDU-214) ist ein viertägiges Training, welches Sie in die Lage versetzt:

- den Cyber-Attack-Lifecycle zu beschreiben und gängige Angriffsformen zu erkennen
- die PAN-OS Threat Prevention Funktionen anzuwenden
- Firewall-Logs und Berichte zur Verbesserung von Konfigurationen zu verwenden
- Firewalls zur Erkennung, Blockierung und Protokollierung von Bedrohungen zu konfigurieren

## PALO ALTO NETWORKS AUSBILDUNG

Trainings von Palo Alto Networks und Palo Alto Networks Authorized Trainings Centern vermitteln das Know-how und die Expertise, die Lebensweise in Zeiten des digitalen Wandels zu schützen. Mit den anerkannten Security-Zertifizierungen erhalten Teilnehmer das nötige Wissen rund um die Next Generation Security-Plattformen, um Cyber-Angriffe erfolgreich abzuwehren und Applikationen sicher bereit zu stellen.

## KURSZIELE

Nach dem erfolgreichen Abschluss des viertägigen Trainings haben Teilnehmer das Verständnis, wie die PAN-OS-Funktionen zur Gefahrenabwehr besser konfiguriert, verwaltet und überwacht werden können. Die Kursteilnehmer erhalten praktische Erfahrung beim konfigurieren, verwalten und überwachen von Threat Prevention-Funktionen in einer Laborumgebung.

## UMFANG

Level: Fortgeschrittene

Dauer: 5 Tage

Format: Vorträge mit Hands-on Labs

Plattformen: Alle Palo Alto Networks Next-Generation Firewall Modelle, die unter PAN-OS laufen

## ZIELGRUPPE

Security Engineers, Security Administratoren, Security Operations Spezialisten, Security Analysten, Network Engineers und IT-Support

## VORAUSSETZUNGEN

Kursteilnehmer sollten Grundkenntnisse zu Netzwerk-Konzepten inklusive Routing, Switching sowie IP Addressing haben und außerdem mit Security-Konzepten vertraut sein. Erfahrung mit weiteren Security-Technologien wie IPS, Proxy und Content Filtering sind von Vorteil.

## INHALTE

- Module 1: The Cyber-Attack Lifecycle
- Module 2: Blocking Packet- and Protocol-Based Attacks
- Module 3: Blocking Threats from Known-Bad Sources
- Module 4: Blocking Threats Using AppID
- Module 5: Blocking Threats Using Custom Signatures
- Module 6: Creating Custom Threat Signatures
- Module 7: Blocking Threats in Encrypted Traffic
- Module 8: Blocking Threats in Allowed Traffic
- Module 9: Authenticating Firewall User Accounts
- Module 10: Blocking Threats from Phishing and Stolen Credentials
- Module 11: Viewing Threat and Traffic Information

*Hinweis: DTS führt die Palo Alto Networks Schulungen in Zusammenarbeit mit Consigas als autorisiertem Schulungspartner durch.*