FIREWALL 7.1: MANAGE CYBERTHREATS (EDU-231)

Overview

This two-day, instructor-led course teaches strategies in defense against cyberthreats. Successful completion of this course enables administrators to better understand the threat landscape. Students will learn the use of Palo Alto Networks® next-generation firewalls, including the WildFire™ product.

SESSIONS:

Mod 1: Threat Landscape
- Advanced Persistent Threats
- Data Breaches and Tactics
- Threat Management Strategies

Mod 2: Integrated Approach to Threat Protection
- Integrated Approach to Protection
- Next-Generation Firewall
- Advanced Endpoint Protection

Mod 3: Network Visibility
- Zero Trust Model
- SSL Decryption
- Decryption Policy

Mod 4: Reducing the Attack Surface
- App-ID to Reduce Attack Surface
- Control Advanced Vectors
- Handling Drive-By Downloads
- DoS Protection

Mod 5: Handling Known Threats
- WildFire Analysis
- Security Profiles

Mod 6: Handling Unknown Traffic and Zero-Day Exploits
- WildFire
- Researching Threat Events
- Identifying Unknown Applications

Mod 7: Investigating Breaches
- Identify IOCs Using App-Scope
- Log Correlation
- Finding Infected Host

Mod 8: Using Custom Signatures
- Creating Custom App-IDs
- Threat Signatures

Course Objectives

The Firewall 7.1: Manage Cyberthreats course is for students who want to understand cyberthreats and their characteristics. Students will learn how to manage cyberthreats using security policies, profiles, and signatures to protect their network against emerging threats.

Scope

- **Course level:** Intermediate
- **Course duration:** 2 days
- **Course format:** Combines lecture with hands-on labs
- **Platform supported:** All Palo Alto Networks next-generation firewall models running the PAN-OS® operating system

Target Audience

Firewall Administrators, Network Security Administrators, and Technical Professionals

Prerequisites

Students must complete the Firewall 7.1: Install, Configure, and Manage (EDU-201) course and have an understanding of network concepts, including routing, switching, and IP addressing. They also will need in-depth knowledge of port-based security and security technologies such as IPS, proxy, and content filtering

Course Outline

Firewall 7.1: Manage Cyberthreats

PART NUMBER: EDU-231

4401 Great America Parkway
Santa Clara, CA 95054
Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087
www.paloaltonetworks.com