ADVANCED THREAT MANAGEMENT

Overview

This instructor-led course teaches strategies in defense against advanced threats. 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:

Day 1

Mod 0: **Introduction**

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

Day 2

Mod 5: **Handling Known Threats**
- Control Threat Enablers
- Security Profiles

Mod 6: **Dealing with Zero-Day Attacks**
- WildFire
- Researching Threat Events
- Identifying Unknown Applications

Mod 7: **Investigating Attacks**
- Indicators of Compromise
- Logs and Reports
- Log Correlation
- Using AppScope

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

Course Objectives

The Threat Management Course is for students who want to understand advanced threats and their characteristics. Students will learn how to manage advanced threats 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 (models running PAN-OS 7.0)

Target Audience

- Firewall administrators, network security administrators, and technical professionals

Prerequisite

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

Palo Alto Networkss Advanced Threat Management Datasheet

PART NUMBER: PAN-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