PALO ALTO NETWORKS® TRAPS™ ADVANCED ENDPOINT PROTECTION (PAN-EDU-281)

DURATION: 2 DAY

COURSE 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 Wild Fire™ product.

TARGET AUDIENCE

Firewall administrators, network security administrators, and technical professionals

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.

COURSE CONTENT

Mod 0: Introduction

Mod 1: Threat Landscape

1. Advanced Persistent Threats
2. Data Breaches and Tactics
3. Threat Management
4. Strategies
5. Mod 2: Integrated
6. Approach to Threat
7. Protection
8. Integrated Approach to
9. Protection

10. Next-Generation Firewall
11. Advanced Endpoint
12. ProtectionMod 3: Network Visibility
13. Zero Trust Model
14. SSL Decryption
15. Decryption Policy

Mod 4: Reducing the

1. Attack Surface
2. App-ID to Reduce
3. Attack Surface
4. Control Advanced Vectors
5. Handling Drive-By
6. Downloads
7. DoS Protection

Mod 5: Handling Known

1. Threats
2. Control Threat Enablers
3. Security Profiles

Mod 6: Dealing with

1. Zero-Day Attacks
2. Wild Fire
3. Researching Threat Events
4. Identifying Unknown
5. Applications

Mod 7: Investigating

1. Attacks
2. Indicators of Compromise
3. Logs and Reports
4. Log Correlation
5. Using App Scope

Mod 8: Custom Signatures

1. Creating Custom App-IDs
2. Threat Signatures

COURSE PREREQUISITES

Students must complete the Firewall Essentials I (PANEDU-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.