

# **FIREWALL 8.1: OPTIMIZING FIREWALL THREAT PREVENTION (EDU-214)**

**DURATION: 4 DAYS**

## **COURSE OVERVIEW**

Successful completion of this four-day, instructor-led course will enhance the student's understanding of how to better configure, manage, and monitor PAN-OS® threat prevention features. The student will get hands-on experience configuring, managing, and monitoring threat prevention features in a lab environment.

## **TARGET AUDIENCE**

Security Engineers, Security Administrators, Security Operations Specialists, Security Analysts, Network Engineers, and Support Staff

## **COURSE OBJECTIVES**

**After completing this course, you should be able to:**

1. Describe the cyber-attack lifecycle and recognize common forms of attack
2. Describe PAN-OS® threat prevention capabilities
3. Use firewall logs and reports to make better configuration decisions
4. Configure the firewall to detect, block, and record threats

## **COURSE CONTENT**

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

## 11. Module 11: Viewing Threat and Traffic Information

### **COURSE PREREQUISITES**

Participants must complete the Firewall 8.1 Essentials: Configuration and Management course, or have equivalent experience. Students must have a basic familiarity with networking concepts including routing, switching, and IP addressing.