Cybersecurity Prevention and Countermeasures

The Prevention and Countermeasures course covers advanced information about the installation, configuration, and management of firewalls for the defense of enterprise network architecture.

Students will learn the theory and extended configuration features necessary for setting up traffic handling, advanced content and user identification, quality of service, GlobalProtect, monitoring and reporting, and high availability of Next-Generation Firewalls.

Using Palo Alto Networks Next-Generation Firewalls, students will learn how to:

- Apply firewall certificate management policies.
- Identify unknown malware, zero-day exploits, and advanced persistent threats.
- Configure and deploy zones, agents, and security policies.
- Differentiate and apply mobile device protection.
- Implement and configure Application Command Center (ACC) log forwarding and report monitoring.
- Apply and monitor active/passive and active/active security device high availability.

NIST/NICE Course Mapping—Work Role

- Protect and Defend: Cyber Defense Analyst – PR-CDA-001

Course Structure

Module 1: Decryption and Certificate Management

Learn to decrypt and screen traffic as it passes through the firewall.

Module 2: Virus Analysis and Mitigation

Integrate WildFire within a security architecture, examining file contents and building virus signature databases.

Module 3: End User Identification

Understand Next-Generation Firewall setup and authentication of User-ID as well as monitoring and logging of User-ID-to-device mapping.

Module 4: Remote Access Security

Explore and configure firewall authentication certificates, security profiles, and client agents.

Module 5: Security Monitoring and Reporting

Configure the Next-Generation Firewall dashboard and filters to refine widget display results, interacting with the ACC.

Module 6: Security Device High Availability

Configure Next-Generation Firewall port assignments for high availability control, management, and data link connections, as well as monitoring of heartbeat notifications.