Cybersecurity Academy Advanced Courses

Firewall Essentials

Course Description:

This course introduces students to general defense strategies for enterprise security network architecture. Students will learn about the processes used for setting up security, networking, accounts, zones, and security policies of next generation firewalls. Students will also learn about technologies such as App-ID, WildFire, User-ID, decryption, and logging procedures used to fortify and supplement the platform approach to enterprise network defense. Finally, students will learn about Secure Access Service Edge (SASE) technologies and services including Zero Trust Operations and Information Technology, SD-WAN Instant-ON device integration, Cloud Access Security Brokers (CASB), Cloud Secure Web Gateway (CSWG), and Autonomous Digital Experience Management (ADEM).

NIST/NICE Alignment and Work Roles:

- Implementation and Operation – Systems Administration (IO-WRL-005)
- Implementation and Operation – Systems Security Analysis (IO-WRL-006)
- Protection and Defense – Infrastructure Support (PD-WRL-004)
- Potential Job Roles: Systems Administrator; Security Architect; Systems Security Analyst; Cyber Defense Analyst

Course Objectives:

- Review industry leading firewall platforms, architecture, and defense capability.
- Demonstrate and apply configuration of firewall interfaces, and security zones.
- Configure and manage virtual routing and filtering on next generation firewalls.
- Analyze security policy admin concepts related to network address translation.
- Outline and construct security policies to identify unknown application software.
- Identify how to configure App-ID to reduce the attack surface.
- Describe and configure security, file blocking, and DoS protection profiles.
- Configure the firewall to block traffic from malicious domains, and URLs.
- Describe WildFire deployment options and configure WildFire updates.
- Identify the main components of User-ID and configure user to group names.
- Configure SSL/TLS forward proxy and inbound inspection decryption.
- Monitor threat and traffic information using logs, reports and the firewall ACC.
- Examine the functionality of Zero Trust, including Zero Trust Operations.
- Explain the features and components of Prisma SD-WAN architecture.
- Analyze the value proposition for implementing SASE Edge Security.
- Evaluate the criteria and processes for securely architecting SASE Networks.
- Explain how Cloud Access Security Broker services help identify risks.
- Identify how Next-Gen CASB identifies SaaS/IaaS/web application usage.
- Analyze how Next-Gen CASB implements Machine Learning-Based App-ID.
- Describe how ADEM observes connections and collects endpoint information.

Course Modules:	Course Prerequisites:	Course Scope:	Hands-On Labs:
• Platforms, Architecture and Initial FW Configuration • Firewall Configuration and Admin Accounts • Configuring Security Zones, Policies, and NAT • Application Identification and User-ID • Security Profiles and URL Filtering • Wildfire Malware Protection • Encrypted Traffic, Logs, and Reports • SASE Overview and Architecture • Cloud Access Security Broker • Autonomous Digital Experience Management	Fundamental understanding of Network Security, Cloud, Security Operations, and Firewall technologies. Students are expected to have basic internet and application software skills.	**Level:** Introductory **Duration:** 4 credits - 60 contact hours **Format:** Instructor-Led or Self-Paced	• Configuring Initial Firewall Settings • Managing Firewall Configurations • Managing Firewall Admin Accounts • Configuring Security Zones • Creating Security and NAT Policy Rules • Controlling Application Usage with App-ID • Configuring Security Profiles • Blocking Web Traffic with URL Filtering • Blocking Unknown Threats with WildFire • Controlling Access to Resources with User-ID • Using Decryption to Block Threats • Locating Information with Logs and Reports