CYBERSECURITY ACADEMY

Protecting life in the digital age one student at a time

WASTC 2019 Faculty Development Weeks

Palo Alto Networks Faculty Training: Admin I & II

Dates: In Person, June 24-28, 2019, Coastline Community College, Garden Grove, CA

Target Audience: This course is for you if …

- Have a basic familiarity with networking concepts including routing, switching, and IP addressing..
- Be familiar with basic security concepts. Experience with other security technologies (IPS, proxy, and content filtering) is a plus

Workshop Overview:
This faculty training will prepare you to teach the Cybersecurity Infrastructure Configuration (CIC) and Cybersecurity Prevention & Countermeasures (CPC) courses offered through participating in the Palo Alto Networks Cybersecurity Academy program. It will provide hands-on experience to do the course labs. Further it prepares faculty to become Palo Alto Networks Certified Network Security Administrator (PCNSA).

Cybersecurity Infrastructure Configuration (CIC)
This course provides you with a general understanding of how to install, configure, and manage firewalls for defense of enterprise network architecture. You will learn the theory and configuration steps for setting up the security, networking, threat prevention, logging, and reporting features of next generation firewall technologies. Upon successful completion of this course, you should be able to:

Cybersecurity Prevention & Countermeasures (CPC)
This course provides you with advanced information for how to install, configure, and manage firewalls for defense of enterprise network architecture. You will learn the theory and extended configuration features necessary for setting up traffic handling, advanced content/user identification, quality of service, global protect, monitoring/reporting and high availability of next generation firewall technologies.
Upon completion of this course, you will be able to:

Instructor: John Cone, Trainer, PCNSE, CISSP, CISA, CISM, ICND1, MCT, MCSE, MCSA, MCTS, MCITP SA/EA, MCDST, CTT+, Security+, Net +, A+. John is a Palo Alto Networks Cybersecurity Academy Technical Engineer; his duties include: academic and technical training, supporting new academies and managing the ticketing system.

John graduated from Sam Houston State University in Huntsville, TX in 1989 and 1991 in Secondary Education. He has a total of thirty years teaching/training experience. He was a staff instructor for Southern Methodist University as well as Heald College in Fresno, CA. He has been involved in several capacities in the training industry: instructor, courseware development, train the trainer, and consultant. John's background as a degreed educator gives him insight into the following: the lesson cycle, questioning techniques, creative learning strategies and outcome-based education.

Sponsored by:

Class Description/Objectives:

Cybersecurity Infrastructure Configuration (CIC)
This course provides you with a general understanding of how to install, configure, and manage firewalls for defense of enterprise network architecture. You will learn the theory and configuration steps for setting up the security, networking, threat prevention, logging, and reporting features of next generation firewall technologies. Upon successful completion of this course, you should be able to:

- Review industry leading firewall platforms, architecture, and defense capability related to zero trust security models and public cloud security.
- Demonstrate and apply configuration of firewall initial access, interfaces, security zones, virtual routing, filtering, licensing, service routes, software updates, and policy-based forwarding.
- Analyze security policy administrative concepts related to source and destination network address translation.
- Outline and construct security policies to identify known and unknown application software running on the service network.
- Differentiate, configure, and deploy filtering technologies such as anti-virus, antispyware, and file blocking, to protect against telemetry induced attack vectors.
- Construct and deploy uniform resource locator profiles for attachment to next generation firewall security policies.

Cybersecurity Prevention & Countermeasures (CPC)
This course provides you with advanced information for how to install, configure, and manage firewalls for defense of enterprise network architecture. You will learn the theory and extended configuration features necessary for setting up traffic handling, advanced content/user identification, quality of service, global protect, monitoring/reporting and high availability of next generation firewall technologies.
Upon completion of this course, you will be able to:

- Identify and apply firewall certificate management policy including configuration of inbound and outbound secure socket layer decryption.
- Identify unknown malware, zero-day exploits, and advanced persistent threats through static and dynamic analysis in a scalable, virtual environment.
- Configure and deploy zones, agents, and security policies related to UserID mapping and redistribution.
- Differentiate and apply mobile device protection topologies, gateways, portals, agents, IPsec tunnels, and Virtual Private Networks.
- Implement and configure Application Command Center log forwarding and report monitor for email, syslog, zone protection and Simple Network Management Protocol.
- Demonstrate, apply, and monitor active/passive and active/active security device high availability.

Course Access: Participants will be provided Moodle course links to self-enroll prior to the start of the course. Faculty who successfully complete all course labs (submission of screen shots required), pass all chapter assessments (quizzes and final exams) at 80+%, final assignment and course survey will receive the authorized faculty certificates to begin teaching the courses.

Prerequisite Knowledge: To understand the content and successfully complete this course, you should have knowledge and skills associated with the following:

- Have a basic familiarity with networking concepts including routing, switching, and IP addressing.
- Be familiar with basic security concepts. Experience with other security technologies (IPS, proxy, and content filtering) is a plus.

Prerequisite Course: Cybersecurity Academy Orientation (AO)
Participants will be provided with the AO Moodle course link to self-enroll prior to the start of the course.

Textbook: None; course content will be delivered via Moodle.

Course Labs: The following labs that will be taught to support the CIC and CPC courses are:

Cybersecurity Infrastructure Configuration (CIC)

- Module 2.1: Initial Configuration
- Module 2.2: Interface Configuration
- Module 3: Security and NAT Polices
- Module 4: Application ID
- Module 5: Content ID
- Module 6: URL Filtering

Cybersecurity Prevention & Countermeasures (CPC)

- Module 1: Decryption
- Module 2: Wildfire
- Module 3: User-ID
- Module 4.1: Global Protect
- Module 4.2: Site-to-Site VPN
- Module 5: Monitor and Report
- Module 6: High Availability