CYBERSECURITY ACADEMY CURRICULUM

Palo Alto Networks Cybersecurity Academy provides a comprehensive offering of course content that matches the educational needs of high school and university students. Academy curriculum is aligned with the U.S. National Initiative for Cybersecurity Education, or NICE, framework and cybersecurity work roles.

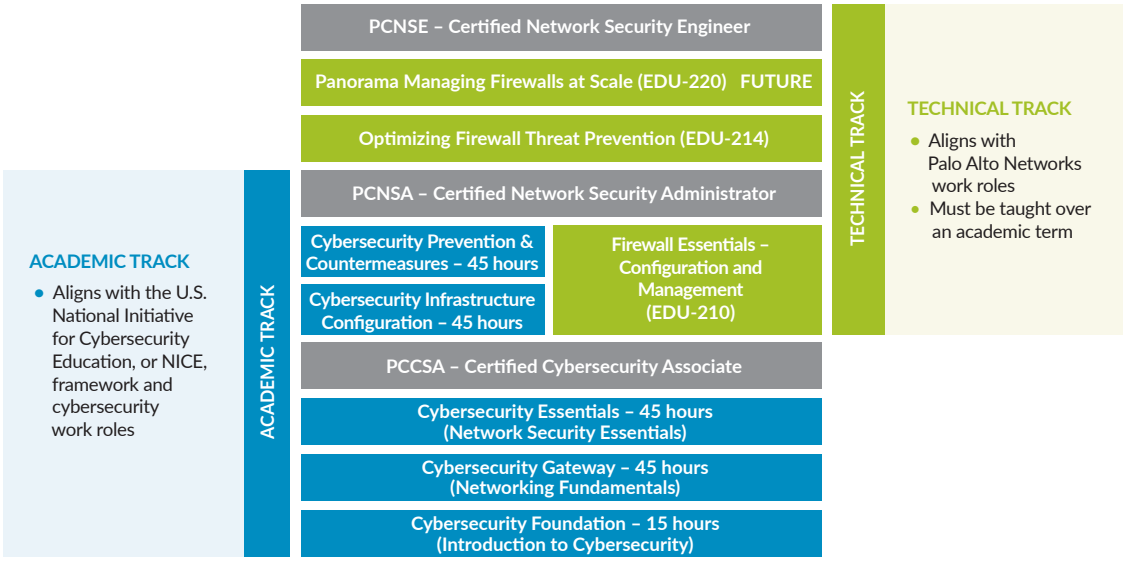

Figure 1: Course and certification roadmap

Cybersecurity Foundation

The Foundation course introduces students to the fundamentals of cybersecurity and the concepts they must understand to be able to recognize and mitigate attacks against networks and mission-critical infrastructure.

Students will learn:

- The nature and scope of today's cybersecurity challenges.
- Strategies for network defense.
- Detailed information about next-generation cybersecurity approaches.
- Security methodologies, technologies and concepts used to implement a secure network environment.

Course Structure

Module 1: Cyber Landscape

Summarize the vulnerabilities and risks associated with modern computing trends, such as Web 2.0/enterprise, cloud, and integrated apps and services.

Module 2: Cyberthreats

Identify common attacker profiles and categorize a typical attack into seven identifiable stages.

Module 3: Malware and Spamming

Explore different attacker utilizations of bots and botnets, including command and control, spamming, and distributed denial-of-service, aka DDoS, implementations.

Module 4: Wi-Fi and Advanced Threats

Evaluate various cyberattack types and techniques employed in DDoS attacks, Wi-Fi exploits and advanced threat actions.

Module 5: Network Security Models

Learn the relationships and differences between regulatory compliance and security.

Module 6: Cloud and Data Center Security

Define virtual data center architectures and their data communication pathways.

Module 7: Best Practice and Principles

Recognize endpoint security anti-malware strategies, including signature-based, container-based, application whitelisting and anomaly-based techniques.

Supporting Materials

The Cybersecurity Survival Guide e-book, a downloadable PDF, presents information included in the Foundation, Gateway and Essentials courses. It also includes a glossary of terms and a list of figures.

Cybersecurity Gateway

The Gateway course presents the fundamental tenets of networking and covers the general concepts involved in maintaining a secure network computing environment.

Upon successful completion of this course, students will be able to examine and implement basic networking configuration techniques and describe general networking fundamentals.

Students will learn to:

- Demonstrate knowledge of interconnected technologies.
- Examine threat vectors, vulnerabilities and risks.
- Apply subnet mask schemes for physical, logical and virtual networks.
- Fully identify the functions of specific layers in the TCP/IP model.
- Accurately explain cloud and virtual storage, backup, and recovery procedures.
- Plan, design, implement and troubleshoot network infrastructure environments.

Course Structure

Module 1: The Connected Globe

Demonstrate service desk, networking, and systems maintenance knowledge as well as cybersecurity best practices.

Module 2: Physical, Logical and Virtual Addressing

Diagnose network connectivity problems, including subnetting, using commonly available tools.

Module 3: Packet Encapsulation and Lifecycle

Analyze network traffic flows, capacities and performance using packet-level analysis.

Module 4: Cybersecurity Landscape and Threats

Recognize vulnerabilities and associated cyberthreats.

Module 5: Cloud, Virtualization, and Storage Security

Develop and implement network backup and recovery procedures that align with disaster recovery, contingency and continuity operations plans.

Module 6: Networking Principles

Use appropriate tools to analyze and optimize network throughput.

Supporting Materials

The Cybersecurity Survival Guide e-book, a downloadable PDF, presents information included in the Foundation, Gateway and Essentials courses. It also includes a glossary of terms and a list of figures.

Final Assessment

The Gateway course's final assignment, the Palo Alto Networks Cybersecurity Gateway Assessment, or PCGA, exam, is available through the Learning Center at no cost.

NIST/NICE Course Mappings – Cybersecurity Gateway and PCIA Work Roles

- Customer Service and Technical Support: Technical Support Specialist – OM-TS-001
- Network Services: Network Operations Specialist – OM-NET-001

Cybersecurity Essentials

In the Essentials course, students will evaluate cybersecurity principles and demonstrate how to secure a network computing environment through the application of security controls. Students will learn the nature and scope of today's cybersecurity challenges, strategies for network defense and detailed information about next-generation cybersecurity. Students will also deploy a variety of security methodologies, along with technologies used for implementing secure network environments.

Using Palo Alto Networks next-generation firewalls, students will learn to:

- Formulate an industry-standard design to protect infrastructure against cybersecurity threats.
- Apply advanced filtering methodologies, such as user, application and content identification, to protect against all known and unknown attack vectors.
- Describe the basics of cryptography, including synchronous and asynchronous encryption, public key infrastructure and certificates.
- Assess and harden endpoints based on security policies.
- Describe the uses of advanced malware research and analysis that provide enhanced protection for enterprise networks.
- Examine mobile- and cloud-based connection technologies.

Course Structure

Module 1: Cybersecurity Design Principles

Evaluate different cybersecurity fundamentals, designs and concepts, with specific focus on the principles of perimeter-based and Zero Trust models.

Module 2: Next-Generation Firewalls

Study the functions and features of next-generation firewall technology, specifically the configuration and administration of Palo Alto Networks next-generation firewalls and PAN-OS® software.

Module 3: Cryptography, PKI and Certificate Protection

Reinforce understanding of cryptographic encoding and decoding, certificate management, and secure traffic analysis.

Module 4: Advanced Endpoint Protection

Secure client devices with the goals of hardening, patching and analyzing malware risks, using Palo Alto Networks Traps™ advanced endpoint protection and WildFire® malware prevention service.

Module 5: Threat Prevention and Intelligence

Focus on risk analysis via in-depth examination of WildFire and next-generation firewall application services.

Module 6: Mobile Device and Cloud Security

Apply the most advanced security features of Palo Alto Networks next-generation firewalls: App-ID™ and User-ID™ technology, and GlobalProtect™ network security for endpoints.

Supporting Materials

The Cybersecurity Survival Guide e-book, a downloadable PDF, presents information included in the Foundation, Gateway and Essentials courses. It also includes a glossary of terms and a list of figures.

NIST/NICE Course Mapping – Cybersecurity Essentials and PCIA Work Role

Systems Analysis: Systems Security Analyst – OM-AN-001

Cybersecurity Infrastructure Configuration

Students will gain a general understanding of how to install, configure and manage firewalls for the defense of enterprise network architecture. Students will also learn the theory and steps for setting up the security, networking, threat prevention, logging and reporting features of next-generation firewalls.

Using Palo Alto Networks next-generation firewalls, students will learn to:

- Compare industry-leading firewall platforms, architecture and defense capability related to Zero Trust security approaches and public cloud security.
- Demonstrate and apply configuration of firewall initial access, interfaces, security zones, routing, etc.
- Analyze security policy administrative concepts related to source and destination network address translation, or NAT.
- Outline and construct security policies to identify known and unknown application software.
- Differentiate, configure and deploy filtering technologies such as antivirus, anti-spyware and file blocking.
- Construct and deploy URL profiles for attachment to next-generation firewall security policies.

Course Structure

Module 1: Security Architecture Planning

Review Palo Alto Networks next-generation firewalls, both hardware and software offerings.

Module 2: Infrastructure Device Configuration

Examine Palo Alto Networks next-generation firewall flow logic and participate in several tutorials for initial configuration of a next-generation firewall.

Module 3: Cybersecurity Policy

Analyze security policy and NAT concepts, along with firewall configurations.

Module 4: Application Software Identification

Configure application properties and write firewall rules to permit or deny running of specific applications.

Module 5: Antivirus, Anti-Spyware and File Blocking

Set up malware content identification through antivirus and anti-spyware security policies for next-generation firewalls.

Module 6: Uniform Resource Locator Filtering

Manage access to URL web addresses and content.

Final Assessment

The Infrastructure Configuration course's final assignment, the Palo Alto Networks Cybersecurity Infrastructure Assessment, or PCIA, exam, is available through the Learning Center at no cost.

NIST/NICE Course Mapping – Cybersecurity Infrastructure Configuration and PCIA Work Roles

Cyber Defense Analysis: Cyber Defense Analyst – PR-CDA-001

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 log forwarding and report monitoring.
- Apply and monitor active/passive and active/active security device high availability.

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 Application Command Center.

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.

NIST/NICE Course Mappings – Cybersecurity Prevention and Countermeasures, and PCIA Work Roles

- Systems Administration: Systems Administrator – OM-ADM-001
- Cyber Defense Infrastructure Support: Cyber Defense Infrastructure Support Specialist – PR-INF-001

Certification

Our industry-leading courseware and professional certifications help validate technical competencies and knowledge of the Palo Alto Networks Security Operating Platform. The exams are proctored by the third-party testing company Pearson VUE.

- A Palo Alto Networks Certified Cybersecurity Associate, or PCCSA, possesses knowledge of cutting-edge technology available today to manage the cyberthreats of tomorrow.
- A Palo Alto Networks Certified Network Security Engineer, or PCNSE, is capable of designing, deploying, configuring, maintaining and troubleshooting the vast majority of Palo Alto Networks Security Operating Platform implementations.
- COMING SOON: A Palo Alto Networks Certified Network Security Administrator, or PCNSA, can operate Palo Alto Networks next-generation firewalls to protect networks from cutting-edge cyberthreats.

How to Become a Cybersecurity Academy

To start incorporating the Cybersecurity Academy curriculum and technology into your own curriculum, sign and return our Cybersecurity Academy Agreement, which can be found at www.paloaltonetworks.com/academy. For any questions about the Palo Alto Networks Cybersecurity Academy, email the Cybersecurity Academy team at academy@paloaltonetworks.com.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

cybersecurity-academy-curriculum-ds-010319