paloalto

CYBERSECURITY ACADEMY

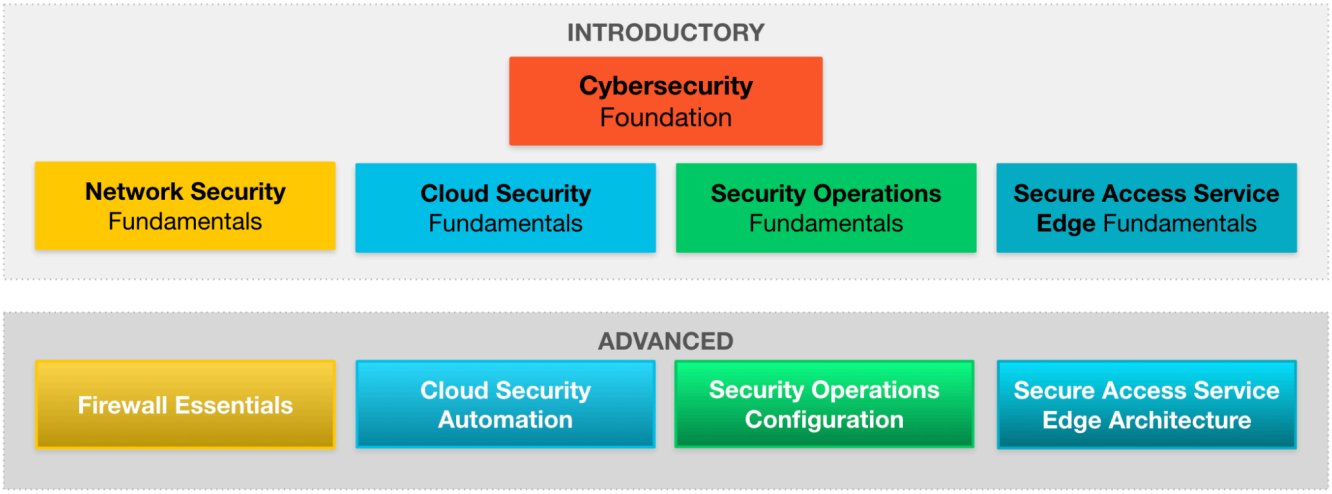
Cybersecurity Academy Curriculum Overview

The Palo Alto Networks Cybersecurity Academy program offers comprehensive courses and technology to address the educational needs of academic learning institutions globally, including universities, colleges, and high schools.

Academy curriculum is aligned with the U.S. National Initiative for Cybersecurity Education (NICE) framework and cybersecurity work roles.

The academic curriculum delivered by our Academy partner institutions helps provide the knowledge and expertise that prepare their students to be successful as they pursue higher education and/or cyber careers. Our trusted certifications validate their knowledge of Palo Alto Networks technology, as well as their ability to prevent cyberattacks and safely enable applications.

Academic Curriculum



Note: All academic courses align to the U.S. National Initiative for Cybersecurity Education (NICE) framework and Cybersecurity Work Roles.

Cybersecurity Survival Guide

The Cybersecurity Survival Guide, a free PDF e-book, presents information to support the entry-level, fundamentals courses listed below, as well as a glossary of terms and list of figures. This tool is vital in preparing for the PCCET certification exam (see Certifications section coming up).

Fundamentals Courses

Cybersecurity Foundation

Students will learn fundamental principles associated with the current cybersecurity landscape, and concepts required to recognize and potentially mitigate attacks against enterprise networks and mission-critical infrastructure. Students will also learn how to set up and configure interfaces, security zones, authentication, and policies on a NextGeneration firewall. Ideal for entry-level candidates in the cybersecurity workforce, and anyone who participates in internet activities.

NIST/NICE Alignment and Work Roles

- Technical Support Specialist (OM-STS-001)
- Work roles: Technical Support Associate; Help Desk Associate

Course Objectives:

- Discover modern computing trends and application threat vectors.
- Configure a network interface and test for connectivity.
- Identify cloud computing and software-as-a-service (SaaS) application challenges.
- Review cybersecurity industry regulations and standards.
- Explore recent cyberattacks and their impact on business.
- Review attacker profiles, motivations, and the Cyberattack Lifecycle.
- Recognize high-profile cybersecurity attacks and Advanced Persistent Threats.
- Identify malware types, vulnerabilities, exploits, spamming, and phishing attacks.
- Configure and test a malware analysis security profile.
- Describe how bots and botnets are used to attack enterprise networks.
- Explore Zero Trust design principles, architecture, capabilities, and implementation.
- Review perimeter network security strategies, policies, models, and trust boundaries.
- Setup and configure inside, outside, and DMZ security zones on a NGFW.
- Create and test an authentication policy on a Next- Generation firewall.
- Review capabilities of the Security Operating Platform and components.
- Explore how to secure the enterprise with NGFW and Cortex® XDR endpoint protection.
- Discover how to secure the cloud with Prisma® Access, SaaS, and Cloud.
- Apply two-factor authentication on the Next-Generation firewall (NGFW).
- Configure the NGFW to allow only trusted applications.

Network Security Fundamentals

Students will gain an understanding of the fundamental tenets of network security, and review the general concepts involved in maintaining a secure network computing environment. Upon successful completion of this course, students will be able to describe general network security concepts and implement basic network security configuration techniques. Ideal for entry-level candidates in the cybersecurity work- force, and anyone who participates in internet activities.

NIST/NICE Alignment and Work Roles

- Technical Support Specialist (OM-STS-001)
- Network Operations Specialist (OM-NET-001)
- Work roles: Technical Support Associate; Help Desk Associate; Network Operations Specialist

Course Objectives:

- Identify common enterprise network devices.
- Differentiate between routed and routing protocols.
- Recognize various types of area networks and topologies.
- Describe the Domain Name System DNS, FQDN, and IoT.
- Recognize decimal, binary, and hexadecimal conversion methods.
- Describe the structure and fields of IP header, IPV4 and IPV6 addresses.
- Subnet an IPV4 Class C addressing scheme and configure IP address on the firewall.
- Review the four DHCP process messages and Network Address Translation (NAT).
- Setup the firewall as a DHCP server and test the DHCP client.
- Recognize packet encapsulation and the lifecycle process.
- Identify protocols and define the OSI and TCP model layers.
- Review the transport layer protocols, ports and packet- filtering procedures.
- Create and analyze packet captures using Wireshark.
- Identify common network security encryption algorithms and key management concepts.
- Recognize symmetric/asymmetric key rotation techniques and PKI.
- Generate a self-signed root certificate authority (CA) certificate.
- Create a decryption policy on the firewall to decrypt SSH traffic and SSL traffic.
- Describe the benefits of the Next-Generation firewall single-pass architecture.
- Identify the NGFW App-ID™, User-ID™, Content-ID™ and deployment options.
- Explore the five steps required to implement an NGFW Zero Trust environment.
- Configure the NGFW to monitor, forward, and backup system logs (Syslog).

Modules	Scope	Prerequisites
Module 1: The Connected Globe **Module 2:** IP Addressing **Module 3:** Packet Encapsulation **Module 4:** Network and Endpoint Security **Module 5:** Network Security Principles	**Level:** Introductory **Duration:** 3 credits - 45 contact hours **Format:** Instructor-Led or Self-Paced	Successful completion of the Cybersecurity Foundation course or comparable experience. Students are expected to have basic internet and application software skills.

Cloud Security Fundamentals

Students will learn basic principles associated with securing the cloud and SaaS-based applications through Secure Access Service Edge (SASE) architecture and understand how to recognize and potentially mitigate attacks against traditional and hybrid data centers and mission-critical infrastructure. Students will also learn how to set up and configure containers on a Docker bridge network and test the container security through the use of vulnerability scans and reports. Ideal for entry-level candidates in the cybersecurity workforce, and anyone who participates in internet activities.

NIST/NICE Alignment and Work Roles

- Technical Support Specialist (OM-STS-001)
- Network Services (OM-NET-001)
- Work roles: Technical Support Associate; Help Desk Associate; Network Operations Specialist

Course Objectives:

- Define cloud computing service, deployment, and shared responsibility models.
- Describe cloud native technologies including virtual machines, containers and orchestration, and serverless computing.
- Identify cloud native security, including Kubernetes® security, DevOps, and DevSecOps, visibility, governance, and compliance challenges.
- Create and run Docker bridge network containers in detached and interactive mode.
- Summarize hybrid data center security design concepts.
- Configure and test containers with vulnerability scanning.
- Review traditional data center security solution weaknesses.
- Investigate east-west and north-south traffic protection methods.
- Recognize the four pillars of Prisma Cloud.
- Describe the layers and capabilities in a Secure Access Service Edge (SASE).
- Review the layers in a Prisma Access architecture solution.
- Demonstrate an understanding of unique SaaS-based security risks.
- Understand how Prisma SaaS protects SaaS-based applications and data.

Modules	Scope	Prerequisites
Module 1: Cloud, Virtualization, Storage **Module 2: Cloud Native Security** **Module 3: Cloud and Data Center Security** **Module 4: Mobile and Cloud Security** **Module 5: Secure the Cloud (Prisma)**	**Level:** Introductory **Duration:** 2 credits - 30 contact hours **Format:** Instructor-Led or Self-Paced	Successful completion of the Network Security Fundamentals course or comparable experience. Students are expected to have basic internet and application software skills.

Security Operations Fundamentals

Students will gain an understanding of Security Operations (SecOps) and the role it plays in protecting our digital way of life for businesses and customers. Students will learn continuous improvement processes to collect high-fidelity intelligence, contextual data, and automated prevention workflows that quickly identify and respond to fast-evolving threats. They will also learn how to leverage automation to reduce strain on analysts and execute the Security Operation Center (SOC) mission to identify, investigate, and mitigate threats. Ideal for entry-level candidates in the cybersecurity work- force, and anyone who participates in internet activities.

NIST/NICE Alignment and Work Roles

- Threat/Warning Analyst (AN-TWA-001)
- All-Source Analyst (AN-ASA-001)
- Work roles: Cyber Threat Analyst; Data Analyst

Course Objectives:

- Identify key elements of SecOps and describe processes.
- Configure and test log forwarding for traffic analysis investigation and response.
- Describe SecOps infrastructure, including security information and event management (SIEM), analysis tools, and SOC engineering.
- Define security orchestration, automation and response (SOAR) for SecOps.
- Recognize the major components of the Cortex XDR deployment architecture and explain how it protects end-points from malware and exploits.
- Review how Cortex XSOAR automates security response actions.
- Explain how SOC teams can leverage Cortex Data Lake to collect, integrate, and normalize enterprise security data with advanced artificial intelligence (AI) and machine learning.
- Outline how AutoFocus™ delivers contextual threat intelligence to SOC teams to enable actionable insight into real-world attacks.
- Configure MineMeld™ for threat intelligence gathering and response.

Modules	Scope	Prerequisites
Module 1: Elements and Process of SOC **Module 2: CSOC Infrastructure and Automation** **Module 3: Advanced Endpoint Protection** **Module 4: Threat Prevention and Intelligence** **Module 5: Secure the Future (Cortex)**	**Level:** Introductory **Duration:** 2 credits - 30 contact hours **Format:** Instructor-Led or Self-Paced	Successful completion of the Cloud Security Fundamentals course or comparable experience. Students are expected to have basic internet and application software skills.

Secure Access Service Edge – SASE Fundamentals

This course is designed to introduce students to the fundamental concepts associated with security convergence through a review of security access service edge (SASE) technologies incorporated with zero-trust network access (ZTNA) and software defined wide area networking (SD-WAN). Students will learn user and application centric converged capabilities, managed from the cloud infrastructure, and enforced when and where an enterprise needs them through dynamically created, policy-based SASE. Students will also learn how zero trust networking models are used to replace implicit trust with continuously assessed risk and trust levels.

NIST/NICE Alignment and Work Roles

- Technical Support Specialist (OM-STS-001)
- Network Services (OM-NET-001)
- Systems Administration (OM-ADM-001)
- Work roles: Tech Support Associate; Help Desk Associate; Network Operations; Systems Administrator

Course Objectives:

- Define SASE, and describe important SASE features and functions.
- Explain 10 or more benefits of a successful SASE implementation.
- Describe the 10 tenets (tools and services) of an effective SASE solution.
- Understand the basic concepts of Zero Trust and Zero Trust Network Access - ZTNA.
- Explain how the Kipling Model of Zero Trust is used to communicate the security value of Zero Trust Network Access for business audiences.
- Understand the basic concepts and values of Software-Defined WAN - SDWAN.
- Explain how a Secure-Autonomous SD-WAN solution such as Prisma SD-WAN delivers better performance, increased speed, and cost savings relative to traditional WAN approaches.
- Describe the functionality of Prisma SASE as a application-centric cloud-based security solution.
- Review how Prisma SASE addresses the security challenges for users, application and data in the hybrid workplace.
- Explain the integrated components of a Prisma Access SASE solution.

Modules	Scope	Prerequisites
Module 1: Introduction to SASE **Module 2:** Basics of Zero Trust **Module 3:** Basics of Software-Defined Wide Area Network - SD-WAN **Module 4:** Secure the Cloud with Prisma SASE	**Level:** Intermediate **Duration:** 2 credits - 30 contact hours **Format:** Instructor-Led or Self-Paced	Successful completion of the Cybersecurity Foundation course or comparable experience. Students are expected to have basic internet and application software skills.

Advanced Courses

Enterprise Security Deployment

Students will gain a general understanding of how to install, configure, and deploy firewalls for the defense of enterprise network architecture. Students will learn the configuration and deployment steps for setting up App-ID, WildFire, User-ID, decryption, and logging procedures on next generation firewall technologies.

NIST/NICE Alignment and Work Roles

- Systems Architecture (SP-ARC-002)
- Systems Analysis (OM-ANA-001)
- Cybersecurity Defense Analysis (PR-CDA-001)
- Cloud Security Management (OV-MGT-001)
- Executive Cyber Leadership (OV-EXL-001)
- Work roles: Security Architect; Systems Security Analyst; Cyber Defense Analyst; Info Systems Security Manager; Executive Cyber Leader

Course Objectives:

- Identify how App-ID reduces the attack surface and configure App-ID based policy rules
- Describe and configure security, file blocking, and DoS protection profiles to mitigate attacks.
- Configure the firewall to block traffic from malicious IP addresses, domains, and URLs.
- Describe WildFire deployment options and configure WildFire updates.
- Identify the main components of User-ID and configure user to group name mapping.
- Describe and configure SSL/TLS forward proxy and inbound inspection decryption.
- Monitor threat and traffic information using logs, reports and the firewall ACC.

Modules	Scope	Prerequisites
Module 1: Identify Applications **Module 2:** Deploy Security Profiles **Module 3:** Configure URL Filters **Module 4:** Contain Malware with WildFire **Module 5:** Control Access with User-ID **Module 6:** Block Encrypted Traffic Threats **Module 7:** Monitor Logs and Develop Reports	**Level:** Intermediate **Duration:** 2 credits - 30 contact hours **Format:** Instructor-Led or Self-Paced	Successful completion of the Enterprise Security Management course or comparable experience with Next Generation Firewall configurations. Students are expected to have basic internet and application software skills.

Enterprise Security Management

The ESM course provides the student with a general understanding of how to install, configure, and manage firewalls for defense of enterprise security network architecture. Students will learn the configuration and management steps for setting up the security, networking, accounts, zones, and security policies of next generation firewall technologies.

NIST/NICE Alignment and Work Roles

- Systems Architecture (SP-ARC-002)
- Systems Analysis (OM-ANA-001)
- Cybersecurity Defense Analysis (PR-CDA-001)
- Cloud Security Management (OV-MGT-001)
- Executive Cyber Leadership (OV-EXL-001)
- Work roles: Security Architect; Systems Security Analyst; Cyber Defense Analyst; Info Systems Security Manager; Executive Cyber Leader

Course Objectives:

- 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, and security zones.
- Analyze security policy administrative concepts related to source and destination network address translation.
- Configure and manage virtual routing, filtering, licensing, service routes, software updates, and policy-based forwarding on next generation firewalls.
- Outline and construct security policies to identify known and unknown application software running on the service network

Modules	Scope	Prerequisites
Module 1: Security Architecture Planning **Module 2:** Configuring and Managing Firewall Interfaces **Module 3:** Managing Firewall Administrator Accounts **Module 4:** Configure and Manage Firewall Security Zones **Module 5:** Creating and Managing Security Policies **Module 6:** Creating and Managing NAT Policy Rules	**Level:** Intermediate **Duration:** 2 credits - 30 contact hours **Format:** Instructor-Led or Self-Paced	Fundamental understanding of networking and firewall technologies. Students are expected to have basic internet and application software skills.

Cloud Security Automation

Students will gain an understanding of securing cloud computing technologies using an enterprise suite of services such as Prisma Cloud Compute, with an emphasis on cloud container configurations that provide visibility and control over the risks associated with cloud and data center deployment. Ideal for intermediate-level candidates in the cybersecurity workforce, and anyone who participates in internet activities.

NIST/NICE Alignment and Work Roles

- Systems Administration (OM-ADM-001)
- Work roles: Systems Administrator

Course Objectives:

- Evaluate how cloud-based machine learning aids with anomaly detection.
- Explain how cloud security services analyze data security policies and apply classification.
- Identify container security deployment models and DevOps pipeline.
- Compare container vulnerability and compliance
- Examine the security enhancements provided by identity- based microsegmentation.
- Review and analyze Identity and Access Management (IAM) - cloud security services.
- Discover container compliance status through scans for Amazon Web Services (AWS®) cloud accounts.
- Describe container monitoring and runtime behavior.

management procedures.
- Evaluate container installation guides and upgrade procedures.
- Discover single and cluster container defender installation procedures.
- Describe methods used to monitor containers for vulnerabilities through image scanning.
- Review and analyze the container CVE details and top 10 vulnerability list.
- Design protection and security best practices for serverless applications.
- Describe container model machine learning, patterns, learning states, and drips.
- Analyze container model details processes, networking, and trust audit details.
- List the steps required to develop a new container runtime rule.
- Investigate an incident through compliance, image, snap- shots, and audit details.
- Evaluate challenges associated with cloud-based identity and privileged access management.

Modules	Scope	Prerequisites
Module 1: Cloud Security Overview **Module 2:** Monitoring Vulnerabilities **Module 3:** Monitoring Behavior **Module 4:** Maintaining Compliance **Module 5:** Incident Management	**Level:** Intermediate **Duration:** 2 credits - 30 contact hours **Format:** Instructor-Led or Self-Paced	Successful completion of the Cloud Security Fundamentals course or comparable experience. Students are expected to have basic internet and application software skills.

Security Operations Configuration

This course provides the student with an understanding of Development Security Operations (DevSecOps), Security Orchestration and Response (SOAR) and Threat Intelligence including the roles they play in configuring the SOC for automated protection of enterprise networks and critical infrastructure. Students will implement continuous improvement processes designed to collect high-fidelity intelligence and contextual data, and to apply automated prevention workflows that quickly identify and respond to fast evolving and dangerous cyber threats They will also learn how to leverage automation to reduce strain on analysts and configure the Security Operation Center (SOC) to effectively hunt for, identify, and mitigate threats that circumvent traditional defense mechanisms.

NIST/NICE Alignment and Work Roles

- Threat Analysis (AN-TWA-001)
- All-Source Analyst (AN-ASA-001)
- Cyber Operational Planning (CO-OPL-002)
- Work roles: Threat Analyst; Data Analyst; Cyber Ops Planner
- Info Systems Security Manager; Executive Cyber Leader

Course Objectives:

- Identify and summarize the key elements of Development, Security, and Operations (DevSecOps).
- Discover the Three Pillars of Security Automation: People, Processes, and Technology.
- Examine how security orchestration, automation, and response (SOAR) methods use automation to improve end-to-end business operations cyber posture.
- Identify and review Security Orchestration and Response Use Cases.
- Explain the benefits of Security Operations Configuration and Implementation.
- Explore Phishing Playbooks that execute repeatable tasks to identify false positives.
- Investigate Endpoint Malware Infection and Failed User Login Playbooks.
- Examine SSL Certificate, Vulnerability, and Endpoint Diagnostics Playbooks.
- Investigate how Cortex XSOAR automates security response actions.
- Review how Cortex XSOAR automates responses to ransomware and phishing attacks.
- Identify how to streamline the aggregation and sharing of threat intelligence.
- Examine the top ransomware variant threats across the cybersecurity landscape.
- For each stage of the Cyber Attack Life Cycle describe how threat intelligence and adversarial playbooks are utilized to deploy automated controls and mitigate attacks.

Modules	Scope	Prerequisites
Module 1: Security Operations (SecOps) Overview **Module 2:** Security Orchestration and Response (SOAR) **Module 3:** XSOAR Threat Intelligence Playbooks **Module 4:** Threat Hunting and Intelligence Sharing	**Level:** Intermediate **Duration:** 2 credits - 30 contact hours **Format:** Instructor-Led or Self-Paced	Successful completion of the Security Operations Fundamentals course or comparable experience. Students are expected to have basic internet and application software skills.

Secure Access Service Edge – SASE Architecture

The SASE Architecture course begins with a quick review of SASE Fundamentals and then focuses on a deeper technical understanding of SASE technologies including Zero Trust Operations Technology and Information Technology, SD-WAN Instant-ON device integration, Next-Gen Cloud Access Security Brokers - CASB, Cloud Secure Web Gateway - CSWG, and Autonomous Digital Experience Management - ADEM services

NIST/NICE Alignment and Work Roles

- Threat Analysis (AN-TWA-001)
- All-Source Analyst (AN-ASA-001)
- Cyber Operational Planning (CO-OPL-002)
- Work roles: Threat Analyst; Data Analyst; Cyber Ops Planner
- Info Systems Security Manager; Executive Cyber Leader

Course Objectives:

- Identify the ten tenets of an effective SASE solution.
- Examine the functions of Zero Trust, including Zero Trust Operations
- Technology and Information Technology.
- Explain the features and components of Prisma SD-WAN architecture, including Instant-ON device integration.
- Analyze the benefits and value proposition for implementing SASE Edge Security
- Evaluate the criteria and processes for securely architecting SASE
- Networks, Users, Internet, Application Design and Application Deployment.
- Explain how Cloud Access Security Broker services help the organization to identify risks and comply with regulations.
- Identify how Next-Gen CASB identifies SaaS/IaaS/web app usage, encryption/tokenization, and SaaS misconfiguration.
- Analyze how Next-Gen CASB implements real time Machine Learning- Based App-ID to secure newly deployed or modified applications.
- Identify how SASE architecture integrates a Secure Web Gateway along with other security services such as FWaaS, DNS Security, Threat Prevention, DLP, and CASB.
- Discover how SaaS Security Posture Management - SSPM - assesses the security risk and manages the security posture of SaaS applications.
- Explain why a converged cloud-delivered Secure Web Gateway / Secure Access Service Edge implementation is a critical forward-facing requirement for network security.
- Explain how the Autonomous Digital Experience Management add-on for Prisma Access provides end-to-end visibility and insights for SASE.
- Describe how ADEM observes connections and collects information from endpoints.
- Understand how ADEM can remediate end-user digital experience issues and complications.
- Evaluate how ADEM 'Synthetic Test' processes measure availability, loss, latency, and jitter.

Modules	Scope	Prerequisites
Module 1: SASE Review **Module 2: Cloud Access Security Broker (CASB)** **Module 3: Cloud Secure Web Gateway (CSWG)** **Module 4: Autonomous Digital Experience Management (ADEM)**	**Level:** Intermediate **Duration:** 2 credits - 30 contact hours **Format:** Instructor-Led or Self-Paced	Successful completion of the Security Operations Fundamentals course or comparable experience. Students are expected to have basic internet and application software skills.

Certifications

Our industry-leading courseware and professional certifications help validate technical competencies and knowledge of the Palo Alto Networks product portfolio. Exams are proctored by the third-party testing company Pearson VUE.

- Four Cybersecurity Academy Fundamentals courses - Cybersecurity Foundation, Network Security Fundamentals, Cloud Security Fundamentals and Secure Operations Fundamentals - help the candidate prepare for the Palo Alto Networks Certified Cyber-security Entry-Level Technician (PCCET) certification. Individuals who pass this exam possess knowledge of the cutting-edge technology available today to manage the cyberthreats of tomorrow.
- Cybersecurity Academy intermediate level courses help prepare for the Palo Alto Networks Certified Network Security Administrator (PCNSA) certification. Individuals who pass this exam can operate Palo Alto Networks Next-Generation Firewalls to protect networks from cutting-edge cyber- threats.
- There are dozens of other certifications from Palo Alto Networks at more advanced levels. Learn more here

How to Get Started with the Cybersecurity Academy Courses

To start incorporating the Cybersecurity Academy courses and technology into your own curriculum, complete and accept the Application and Agreement. Once your Application is accepted, you will receive an email with the Curriculum Onboarding Course

.Email any questions you may have to the Academy team at academy@paloaltonetworks.com.

paloalto NETWORKS

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