paloalto

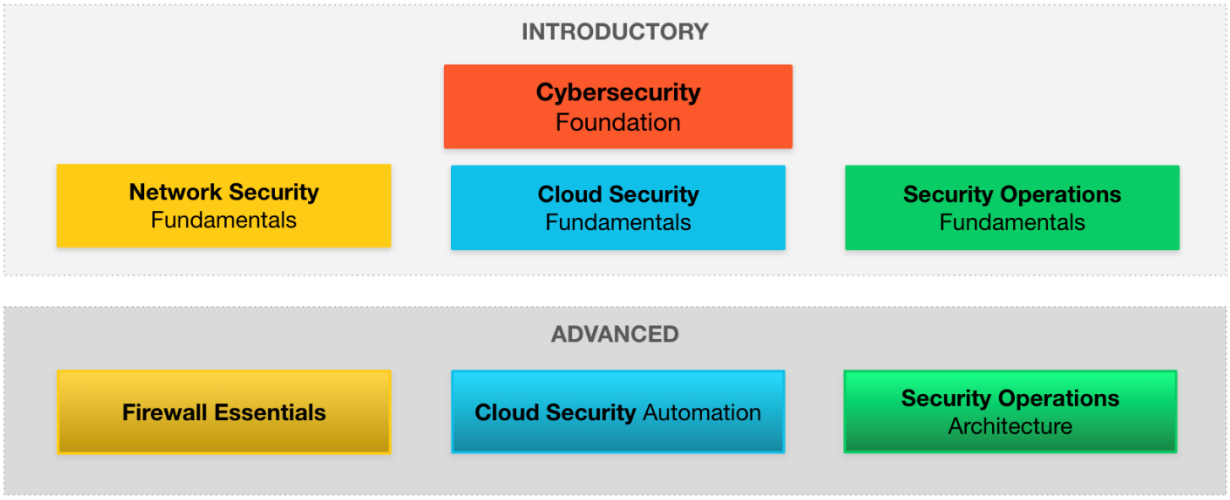
CYBERSECURITY ACADEMY

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.

The academic curriculum delivered by our Academy partners help provide the knowledge and expertise that prepare their students to be successful as they pursue higher education and/or cybersecurity industry careers. Our trusted certifications validate their knowledge of the general cybersecurity landscape and Palo Alto Networks technology, as well as their ability to detect and prevent cyberattacks.

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 Cybersecurity Apprentice and Practitioner certification exams available through Pearson Vue. (see the Certifications section at the end of this document). Cybersecurity Survival Guide

Cybersecurity Academy Fundamentals Courses

Cybersecurity Foundation

Course Description:

In this course students will learn fundamental principles associated with the current cybersecurity landscape and identify concepts required to recognize and potentially mitigate attacks against enterprise networks as well as mission critical infrastructure. Students will also learn how to initially setup and configure security zones, authentication, and policies on a next generation firewall. Additionally, students are introduced to artificial intelligence and the role it plays in cybersecurity today.

NIST/NICE Alignment and Work Roles:

- Implementation and Operation - Technical Support (IO-WRL-007)
- Potential Job 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 and software-as-a-service (SaaS) application challenges.
- Explore Zero Trust principles, architecture, capabilities, and implementation.
- Review perimeter security strategies, policies, models, and trust boundaries.
- Setup and configure inside, outside and DMZ security zones on a NGFW.

- Review cybersecurity industry regulations and standards.
- Explore recent cyberattacks and their impact on business.
- Review attacker profiles, motivations and the Cyber-Attack 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.
- Create and test an authentication policy on a next generation firewall.
- Review capabilities of the Security Operating Platform and components.
- 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.
- Identify and examine artificial intelligence (AI) as it relates to cybersecurity.
- Examine cybersecurity machine learning and large language models with AI.

Course Modules:	Course Prerequisites:	Course Scope:	Hands-On Labs:
• Cybersecurity Landscape • Cybersecurity Threats • Cybersecurity Attacks and Techniques • Cybersecurity Models and Design Principles • Artificial Intelligence in Cybersecurity • Security Operating Platform	Students are expected to have basic internet and application software skills.	**Level:** Introductory **Duration:** 3 credits - 45 contact hours **Format:** Instructor-Led or Self-Paced	• Configuring TCP/IP and a Virtual Router • Exploring Malware Analysis • Creating a Zero Trust Environment • Configuring NGFW Authentication • Applying Two-Factor Authentication to Secure the Firewall • Allowing Only Trusted Applications through the NGFW • Denying International Attackers • Preventing Internet Threats with File Blocking

Network Security Fundamentals

Course Description:

This course provides the student with an understanding of the fundamental tenets of network security 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 describe general network security fundamentals as well as implement basic network security platform configuration techniques.

NIST/NICE Alignment and Work Roles:

- Implementation and Operation - Technical Support (IO-WRL-007)
- Implementation and Operation - Network Operations (IO-WRL-004)
- Potential Job Roles: Technical Support Associate; Help Desk Associate; Network
- Operations Specialist; Network Admin Associate; Cybersecurity Specialist

Course Objectives:

- Identify the most common enterprise network devices.
- Differentiate between routed and routing protocols.
- Recognize the 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 an IP header, IPV4, and IPV6 addresses.
- Subnet IPV4 address schemes and configure an IP address on the firewall.
- Review 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.
- Classify various endpoint and network security technologies.
- Identify common security encryption algorithms and key management concepts.
- 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 a NGFW zero-trust environment.
- Configure the NGFW to monitor, forward, and backup system logs (Syslog)
- Define SASE and describe SASE features and functions.
- Understand the concepts and values of Software-Defined WAN - SDWAN

Course Modules:	Course Prerequisites:	Course Scope:	Hands-On Labs:
• The Inter-connected Globe • Physical and Logical Addressing • Packet Encapsulation and Lifecycle • Network and Endpoint Security • Networking Concepts and Security Principles • Zero Trust Network Access • Network Security Platform - SASE	Successful completion of the Cybersecurity Foundation course or comparable experience. 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 DHCP • Configuring Virtual IP Addresses • Creating Packet Captures • Analyzing Packet Captures • Managing Certificates • Decrypting SSH Traffic • Decrypting SSL Inbound Traffic • Backing up Firewall Logs • Configuring HIP for Global Protect

Cloud Security Fundamentals

Course Description:

In this course, students will learn basic principles associated with securing the cloud and SaaS-based applications through Secure Access Service Edge architecture and identify concepts required to recognize and potentially mitigate attacks against traditional and hybrid datacenters as well as mission critical infrastructure. Students will also learn how to initially setup and configure containers on a docker bridge network and test the container security through vulnerability scans and reports.

NIST/NICE Alignment and Work Roles:

- Implementation and Operation - Technical Support (IO-WRL-007)
- Implementation and Operation - Network Operations (IO-WRL-004)
- Potential Job Roles: Technical Support Associate; Help Desk Associate; Network
- Operations Specialist; Network Admin Associate; Cybersecurity Specialist

Course Objectives:

- Define cloud computing service, deployment, and shared responsibility models.
- Describe cloud native technologies including virtual machines, containers and orchestration, as well as serverless computing.
- Identify cloud native security Kubernetes, Microservices, and DevSecOps.
- Create a Container to run services on virtual machines.
- Examine Docker Volumes, Networking, and Host Port Mapping.
- 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.
- Configure the NGFW to deny International Attackers.
- Recognize the four pillars of Prisma Cloud.
- Review the layers of a Prisma Access architecture solution.
- Demonstrate an understanding of unique SaaS-based security risks.
- Review how Cloud Native Protection Platforms protect SaaS-based applications and data.
- Describe the layers and capabilities in a Secure Access Service Edge (SASE).
- Describe the integrated components of a Prisma Access SASE.

Course Modules:	Course Prerequisites:	Course Scope:	Hands-On Labs:
• Cloud Computing Models • Cloud-Native Technologies • Cloud-Native Security • Data Center Security • Code-To-Cloud Platform – Prisma • Secure Access Service Edge (SASE)	Successful completion of the Network Security Fundamentals course or comparable experience. Students are expected to have basic internet and application software skills.	**Level:** Introductory **Duration:** 3 credits - 45 contact hours **Format:** Instructor-Led or Self-Paced	• Exploring Container Fundamentals • Introduction to Docker I • Introduction to Docker II • Protecting Sensitive Data • Configuring Container Security • Scanning Container Vulnerabilities

Security Operations Fundamentals

Course Description:

This course provides the student with 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 playbook workflows that quickly identify and respond to fast-evolving threats. Students will also learn how to leverage artificial intelligence driven automation used to facilitate the Security Operation Center's (SOC) mission to identify, investigate and mitigate threats.

NIST/NICE Alignment and Work Roles:

- Cyberspace Intelligence – All Source Analysis (CI-WRL-001)
- Protection and Defense – Vulnerability Analysis (PD-WRL-007)
- Potential Job Roles: Cyber Threat Analyst; Vulnerability Analyst; Incident and Intrusion Analyst

Course Objectives:

- Identify the key Security Operations elements and processes.
- Discover the Pillars of Automation: People, Processes, and Technology.
- Configure and test log forwarding for traffic analysis investigation and response.
- Describe Security Information and Event Management (SIEM).
- Investigate Security Operations Center engineering and analysis process.
- Define security orchestration, automation, and response (SOAR) for SecOps.
- Configure the Next Generation Firewall to stop Reconnaissance Attacks.
- Recognize the major components of the Cortex XDR deployment architecture.
- Configure the Next Generation Firewall with endpoint Vulnerability Profiles.
- Identify how to streamline the aggregation and sharing of threat intelligence.
- Configure the Next Generation Firewall to use Dynamic Block Lists.
- Explain how AI/ML collects, integrates, and normalizes enterprise security data.
- Discover how AI facilitates the automation of cybersecurity defense strategies.
- Explore AI-driven Security Operations (SecOps) platform technologies.

Course Modules:	Course Prerequisites:	Course Scope:	Hands-On Labs:
• Security Operations (SecOps) Overview • Security Operations Center (SOC) Elements and Processes • SOC Infrastructure and Automation • SOC Advanced Endpoint Protection • SOC Threat Prevention and Intelligence • AI-Driven Security Operations Platform	Successful completion of the Cloud Security Fundamentals course or comparable experience. Students are expected to have basic internet and application software skills.	**Level:** Introductory **Duration:** 3 credits - 45 contact hours **Format:** Instructor-Led or Self-Paced	• Network Traffic Analysis • Finding Threats with Application Command Center • Analyzing Firewall Threat Logs • Configuring Log Forwarding • Stopping Reconnaissance Attacks • Securing Endpoints using Vulnerability Profiles • Collecting Threat Intelligence • Using Dynamic Block Lists

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

Cloud Security Automation

Course Description:

Cyber-attacks against cloud network operations are increasing with intensity and have the potential to inflict wide-spread damage to business production and organization's reputation. It is now more important than ever for security practitioners to understand the magnitude of the problem and employ solutions to defend cloud-based networks as well as to maintain trust with customers, partners, and shareholders. This course is designed to enhance student's understanding of securing Cloud Computing technologies using an enterprise suite of services such as Cloud Native Application Protection Platform, with an emphasis on cloud container configurations that provide visibility of risks associated with deployment in public cloud and private data centers.

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:

- Evaluate how Cloud-based machine learning aids with anomaly detection.
- Explain how Cloud security services deploy and analyze data security policies.
- Identify container security deployment models and DevOps pipeline.
- Compare container vulnerability and compliance management procedures.
- Evaluate container installation guides and upgrade procedures.
- Examine Cloud-based Infrastructure as Code.
- Review and analyze Identity and Access Management Cloud security services.
- Discover the container compliance status through scans for AWS cloud accounts.
- Describe container monitoring and runtime behavior.
- Describe container model machine learning, patterns, learning states and drips.
- Analyze container model details processes, networking and Trust Audit details.

- Discover single and cluster container defender installation procedures.
- Describe methods used to monitor containers for vulnerabilities.
- Review and analyze the top 10 container vulnerability list.
- Search for and evaluate the container CVE details information.
- Design protection and security best practices for Serverless applications
- Examine the security enhancements provided by Identity-Based Micro-segmentation.
- List the steps required to develop a new container runtime rule.
- Investigate an incident through compliance, image, snapshots and audit details.
- Evaluate the challenges associated with Cloud Identity and Access Management.
- Identify how SASE architecture integrates Secure Web Gateway, FWAAS, and CASB.
- Discover how Security Posture Management assesses risk of SaaS applications.
- Examine the network security requirement for a Secure Web Gateway SASE solution.

Course Modules:	Course Prerequisites:	Course Scope:	Hands-On Labs:
• Cloud and Container Security Overview • Cloud Defender - Monitoring Vulnerabilities • Cloud Assessment - Monitoring Behavior • Maintaining Compliance and Identity Access Management • Cloud Incident Management - Runtime Defense	Successful completion of the Cloud Security Fundamentals course or comparable experience. Students are expected to have basic internet and application software skills.	**Level:** Introductory **Duration:** 3 credits – 45 contact hours **Format:** Instructor-Led or Self-Paced	• Introduction to Kubernetes • Configuring Kubernetes: Persistent Storage and YAML Files • Configuring Kubernetes: Microservices and DevSecOps • Reviewing CNAPP Compute Console I • Reviewing CNAPP Compute Console II • Running CNAPP Compute Defense I • Running CNAPP Compute Defense II

Security Operations Architecture

Course Description:

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

NIST/NICE Alignment and Work Roles:

- Protection and Defense - Threat Analysis (PD-WRL-006)
- Protection and Defense – Insider Threat Analysis (PD-WRL-005)
- Protection and Defense – Defensive Cybersecurity (PD-WRL-001)
- Potential Job Roles: Threat Analyst; Security Analyst; Cyber Defense Associate; Incident and Intrusion Analyst

Course Objectives:

- Examine how security orchestration, automation, and response (SOAR) methods use automation to improve end-to-end business operations cybersecurity posture.
- Identify and review Security Orchestration and Response Use Cases.
- Explain the benefits of Security Operations Architecture 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 attacks.
- Identify how to streamline the aggregation and sharing of threat intelligence.
- Examine the top ransomware variant threats across the cybersecurity landscape.
- Describe how threat intelligence and adversarial playbooks are utilized to deploy automated controls and mitigation for each stage of the Cyber Attack Life Cycle
- Explore how to resolve unknown exposures with Cortex XPANSE Automation.
- Investigate how Cortex XPANSE can actively discover, learn about, and respond to unknown risks in all connected systems and exposed services.
- Identify and Review Attack Surface Management Use Cases.
- Review how Cortex XSIAM automates security response actions.
- Discover how Cortex XSIAM unites SOC capabilities that include XDR, SOAR, SIEM, ASM and others into a single SecOps platform.

Course Modules:	Course Prerequisites:	Course Scope:	Hands-On Labs:
• Security Orchestration and Response (SOAR) • Advanced Endpoint Protection – Cortex XDR • Threat Intelligence Playbooks – Cortex XSOAR • Attack Surface Management – Cortex XPANSE • Secure the Future - Cortex XSIAM	Successful completion of the Security Operations Fundamentals course or comparable experience. Students are expected to have basic internet and application software skills.	**Level:** Introductory **Duration:** 3 credits – 45 contact hours **Format:** Instructor-Led or Self-Paced	

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.

The Cybersecurity Academy Fundamentals course series - Cybersecurity Foundation, Network Security Fundamentals, Cloud Security Fundamentals and Secure Operations Fundamentals - help the candidate prepare for the Palo Alto Networks Certified Cybersecurity Apprentice and Practitioner certification exams. Individuals who pass these exams possess knowledge of the latest and most advanced cutting-edge technology available to manage the cyberthreats of today and the future.

The Cybersecurity Academy advanced courses help prepare students for the Palo Alto Networks Certified Network Security Generalist and NGFW Engineer certifications. Individuals who pass these exams can operate Palo Alto Networks Next-Generation Firewalls to protect networks from cutting-edge cyber threats.
Learn more about the Palo Alto Networks certification program here:
https://www.paloaltonetworks.com/services/education/certification

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. When your application is accepted, you will receive an email with the Curriculum Onboard ing Course.

Learn more about how to partner with the Cybersecurity Academy here:

https://www.paloaltonetworks.com/services/education/academy

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