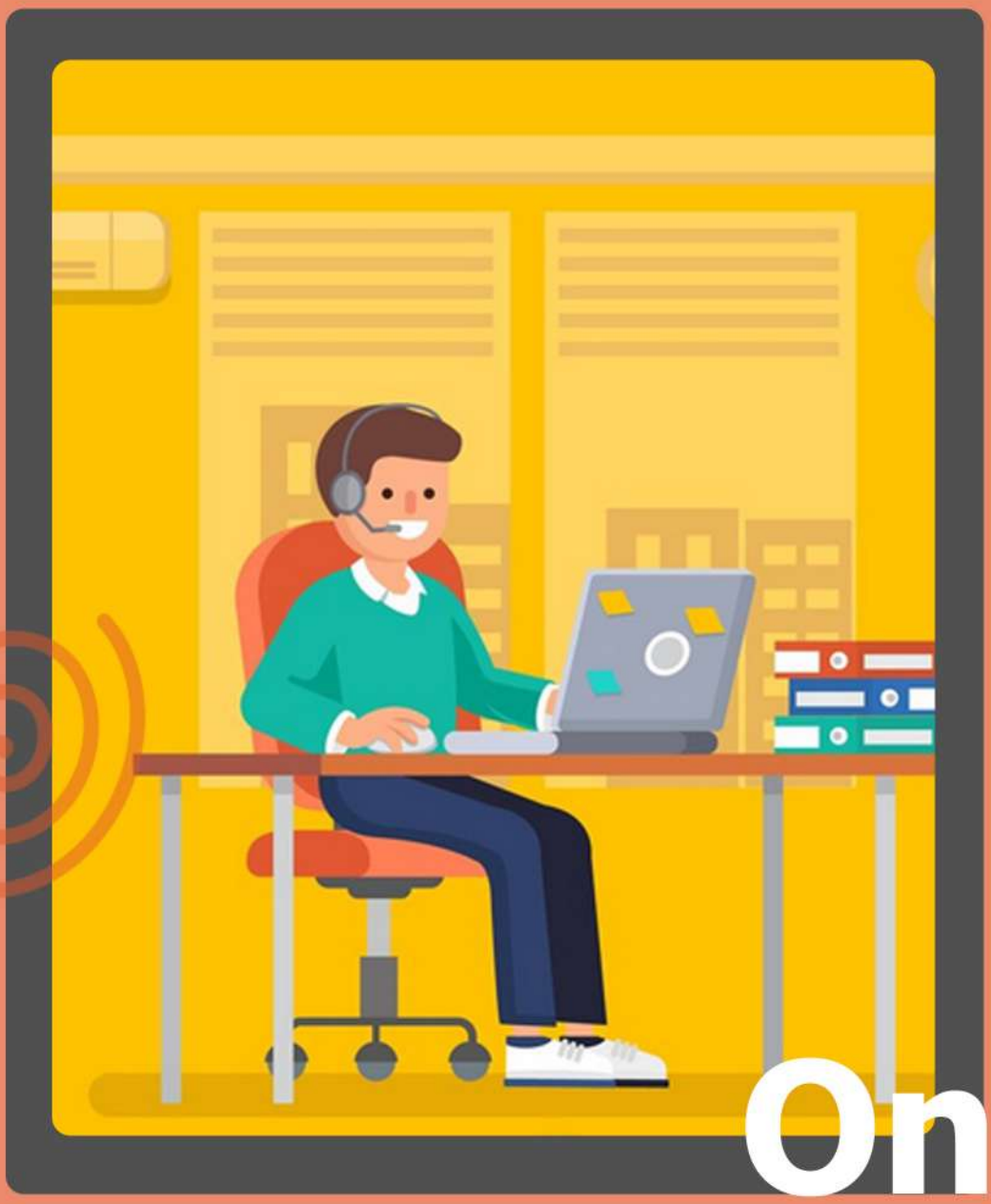
Palo Alto Networks Certificated Cybersecurity Entry-Level Technician

Zetlan Technologies



Online Course

ZETLAN TECHNOLOGIES
www.zetlantech.com

Palo Alto Networks Certificated Cybersecurity Entry-Level Technician

Course Modules

1. **Fundamentals of Cybersecurity**

- Distinguish between Web 2.0 and 3.0 applications and services
- Describe port-scanning methodologies and their impact
  - Nonstandard ports
  - Identify applications by their port number
- Recognize applications used to circumvent port-based firewalls
- Differentiate between common cloud computing service models
  - SaaS
  - PaaS
  - IaaS
- Describe the business processes of supply-chain management
- Describe the vulnerabilities associated with data being stored
  - Describe roles within a SaaS environment
  - Describe security controls for SaaS applications
- Describe the impact of governance, regulation, and compliance
  - Differentiate between compliance and security
  - Identify major cybersecurity laws and their implications
- Describe the tactics of the MITRE ATT&CK framework
- Identify a leading indicator of a compromise
  - Describe how to use CVE
  - Describe how to use CVS

Palo Alto Networks Certificated Cybersecurity Entry-Level Technician

- Identify the different attacker profiles and motivations
  - Dscb the diff value levels of the info that needs to be protected
- Describe the differt phases and events of the cyberattack lifecycle
  - Describe the purpose of command and control (C2)
- Identify the characteristics, capabilities, and appropriate actions
- Differentiate between vulnerabilities and exploits
  - Differentiate between various business email compromise attacks
  - Identify different methodologies for social engineering
  - Identify the chain of events that result from social engineering
- Identify what chain of events follows an attack
- Differentiate between the functional aspects of bots and botnets
  - Describe the type of IoT devices that are part of a botnet attack
- Differentiate the TCP/IP roles in DDoS attacks
  - Differentiate between DoS and DDoS
- Describe advanced persistent threats
- Describe risks with Wi-Fi networks
  - Differentiate between common types of Wi-Fi attacks
  - Describe how to monitor your Wi-Fi network
- Describe perimeter-based network security
  - Identify the types of devices used in perimeter de
- Describe the Demilitarized Zone (DMZ)

Palo Alto Networks Certificated Cybersecurity Entry-Level Technician

- Describ the transitn from a trusted netwrk to an untrusted network
  - Differentiate between North-South and East-West zones
- Describe Zero Trust
  - Identify the benefits of the Zero Trust model
  - Identify the design principles for Zero Trust
  - Describe a microperimeter
  - Differentiate between Trust and Untrust zones
- Describe the integration of services for network, endpoint, & cloud
- Identify the capabilities of an effective Security Operating Platform
  - Describe the components of the Security Operating Platform

2. Network Security Components

- Differentiate between hubs, switches, and routers
  - Given a network diagram, Identify the icons for hubs, switches..
- Describe the use of VLANs
- Differentiate between routed and routing protocols
- Differentiate between static and dynamic routing protocols
  - Differentiate between link state and distance vector
- Identify the borders of collision and broadcast domains

Palo Alto Networks Certificated Cybersecurity Entry-Level Technician

- Differentiate between different types of area networks
  - WAN
  - LAN
- Describe the advantages of SD-WAN
- Describe the purpose of the Domain Name System (DNS)
  - Describe how DNS record types are used
  - Identify a fully qualified domain name (FQDN)
  - Describe the DNS hierarchy
- Differentiate between categories of IoT devices
  - Identify the known security risks and solutions associatd with IoT
- Identify IoT connectivity technologies
- Differentiate between IPv4 and IPv6 addresses
  - Describe binary-to-decimal conversion
  - Describe IPv4 CIDR notation
  - Describe IPv4 classful subnetting
  - Given a scenario, identify the proper subnet mask
  - Describe the purpose of subnetting
  - Describe the structure of IPv4 and IPv6
  - Describe the purpose of IPv4 and IPv6 addressing
- Describe the purpose of a default gateway
- Describe the role of NAT

Palo Alto Networks Certificated Cybersecurity Entry-Level Technician

- Describe OSI and TCP/IP models
  - Identify the order of the layers of both OSI and TCP/IP models
  - Compare the similarities of some OSI and TCP/IP layers
  - Identify the protocols and functions of each OSI layer
- Describe the data-encapsulation process
  - Describe the PDU format used at different layers
- Identify the characteristics of various types of network firewalls
  - Traditional firewalls
  - Next-generation firewalls
  - Differentiate between NGFWs and traditional firewalls
- Describe the application of NGFW deployment options
- Differentiate betwn intrusion detection systems & intrusion prevent
  - Differentiate betwn knowledge-based & behavior-based systems
- Describe virtual private networks
  - Describe when to use VPNs
- Differentiate between the different tunneling protocols
- Describe the purpose of data loss prevention
  - Classify different types of data (e.g., sensitive, inappropriate)
- Differentiate the various types of security functions

Palo Alto Networks Certificated Cybersecurity Entry-Level Technician

- Describe endpoint security standards
  - Describe the advantages of endpoint security
  - Describe host-based intrusion detection/prevention systems
  - Differentiat betwn signature-based & behavioral-based malware
  - Describe application block and allow listing
  - Describe the concepts of false-positive and false-negative alerts
  - Describe the purpose of anti-spyware software
- Identify differences in managing wireless devices compard to other
- Describe the purpose of identity and access management
  - Single- and multi-factor Authentication
  - Separation of duties and impact on privileges
  - RBAC, ABAC, DAC, and MAC
  - User profiles
- Integration of NGFWs with the cloud, networks, & endpoints
- Describe App-ID, User-ID, and Content-ID
- Describe Palo Alto Networks firewall subscription services
  - WildFire
  - URL Filtering
  - Threat Prevention
  - DNS Security
  - IoT Security
  - SD-WAN
  - Advanced Threat Prevention

- Advanced URL Filtering
- GlobalProtect
- Enterprise DLP
- SaaS Security Inline
- Virtual Systems

- Describe network security management
  - Identify the deployment modes of Panorama
  - Describe the three components of Best Practice Assessment

3. Cloud Technologies

- Describe the NIST cloud service and deployment models
- Recognize and list cloud security challenges
  - Describe the vulnerabilities in a shared community environment
  - Describe cloud security responsibilities
  - Describe cloud multitenancy
  - Differentiat between security tools in various cloud environments
  - Identity and access management controls for cloud resources
  - Describe different types of cloud security alerts and notifications
- Identify the 4 Cs of cloud native security
- Describe the purpose of virtualization in cloud computing
  - Describe the types of hypervisors
  - Describe characteristics of various cloud providers
  - Describe economic benefits of cloud computing and virtualization

Palo Alto Networks Certificated Cybersecurity Entry-Level Technician

- Describe the security implications of virtualization
- Explain the purpose of containers in application deployment
  - Differentiate containers versus virtual machines
  - Describe Container as a Service
  - Differentiate a hypervisor from a Docker Container
- Describe how serverless computing is used
- Describe DevOps
- Describe DevSecOps
- Illustrate the continuous integration/continuous delivery pipeline
- Governance & compliance related to deployment of SaaS apps
  - Describe security compliance to protect data
  - Describe privacy regulations globally
  - Describe security compliance betwn local policies and SaaS apps
- Describe the cost of maintaining a physical data center
- Difft betwee=n data-center security weaknesses of traditional solns
- Differentiate between east-west and north-south traffic patterns
- Describe the four phases of hybrid data-center security
- How data centers can transform their operatns incrementally
- Describe the cloud-native security platform
- Identify the four pillars of Prisma Cloud application security
- Describe the concept of SASE

- Describe the SASE layer
  - Describe sanctioned, tolerated, and unsanctioned SaaS apps
  - List how to control sanctioned SaaS usage
- Describe the network-as-a-service layer
- Describe how Prisma Access provides traffic protection
- Describe Prisma Cloud Security Posture Management (CSPM)

4. Elements of Security Operations

- Main elements included in the dvlopmnt of SOC business objectives
- Describe the components of SOC business management & operatns
- List the six essential elements of effective security operations
- Describe the four SecOps functions
  - Identify
  - Investigate
  - Mitigate
  - Improve

- Describe SIEM
- Purpose of security orchestration, automation, & response (SOAR)
- The analysis tools usd to detect evidence of a security compromise
- Describe how to collect security data for analysis
- Use of analysis tools within a security operations environment

Palo Alto Networks Certificated Cybersecurity Entry-Level Technician

For Enquiry: +91 8680961847

- The responsibilities of a security operations engineering team
- Cortex platform in a security operatns environment & the purpose
- How Cortex XSOAR improves security operations efficiency
- Describe how Cortex Data Lake improves security operatns visibility
- How XSIAM can be used to accelerate SOC threat response

Zetlan Technologies

LEARN REMOTELY!!

The efficiency of online learning in terms of time management, flexibility, and the ability to access resources anytime, anywhere can be compelling.

ZETLAN TECHNOLOGIES

www.zetlantech.com

For contact: +91 8680961847
+91 9600579474