

Palo Alto Networks Certified Cybersecurity Entry-level Technician

1. Which analysis detonates previously unknown submissions in a custom-built, evasion-resistant virtual environment to determine real-world effects and behavior?

A. Dynamic

B. Pre-exploit protection

C. Bare-metal

D. Static

Answer(s): A

2. What is required for a SIEM to operate correctly to ensure a translated ow from the system of interest to the SIEM data lake?

A. connectors and interfaces

B. infrastructure and containers

C. containers and developers

D. data center and UPS

Answer(s): A

3. Which type of Wi-Fi attack depends on the victim initiating the connection?

A. Evil twin

B. Jasager

C. Parager

D. Mirai

Answer(s): A

4. Which term describes data packets that move in and out of the virtualized environment from the host network or a corresponding traditional data center?

A. North-South tra c

B. Intrazone tra c

C. East-West tra c

D. Interzone tra c

Answer(s): A

5. Which organizational function is responsible for security automation and eventual vetting of the solution to help ensure consistency through machine-driven responses to security issues?

A. NetOps

B. SecOps

C. SecDevOps

D. DevOps

Answer(s): B

6. DRAG DROP (Drag and Drop is not supported).

Given the graphic, match each stage of the cyber-attack lifecycle to its description.



Select and Place:

reconnaissance		attacker will plan the cyber-attack
weaponization		attacker will determine which method to use to compromise an endpoint
delivery		attacker will distribute their weaponized payload to an endpoint
exploitation		attacker will trigger a weaponized payload
installation		escalate privileges on a compromised endpoint
command and control		establish secure communication channel to servers across the internet to reshape attack objectives

A. See Explanation section for answer.

Answer(s): A

7. DRAG DROP (Drag and Drop is not supported).

Match the Identity and Access Management (IAM) security control with the appropriate definition.

Select and Place:

IAM security		Ensuring least-privileged access to cloud resources and infrastructure
Machine Identity		Discovering threats by identifying activity that deviates from a normal baseline
User Entity Behavior Analytics		Securing and managing the relationships between users and cloud resources
Access Management		Decoupling workload identity from IP addresses

A. See Explanation section for answer.

Answer(s): A

8. On an endpoint, which method should you use to secure applications against exploits?

A. endpoint-based rewall

B. strong user passwords

C. full-disk encryption

D. software patches

Answer(s): D

9. Which not-for-profit organization maintains the common vulnerability exposure catalog that is available through their public website?

A. Department of Homeland Security

B. MITRE

C. Office of Cyber Security and Information Assurance

D. Cybersecurity Vulnerability Research Center

Answer(s): B

10. Which Palo Alto Networks tools enable a proactive, prevention-based approach to network automation that accelerates security analysis?

A. MineMeld

B. AutoFocus

C. WildFire

D. Cortex XDR

Answer(s): D

11. Which endpoint product from Palo Alto Networks can help with SOC visibility?

A. STIX

B. Cortex XDR

C. WildFire

D. AutoFocus

Answer(s): B

12. Which technique changes protocols at random during a session?

A. use of non-standard ports

B. port hopping

C. hiding within SSL encryption

D. tunneling within commonly used services

Answer(s): B

13. What is the primary security focus after consolidating data center hypervisor hosts within trust levels?

A. control and protect inter-host traffic using routers configured to use the Border Gateway Protocol (BGP) dynamic routing protocol

B. control and protect inter-host traffic by exporting all your traffic logs to a syslog log server using the User Datagram Protocol (UDP)

C. control and protect inter-host traffic by using IPv4 addressing

D. control and protect inter-host traffic using physical network security appliances

Answer(s): D

14. Which product from Palo Alto Networks extends the Security Operating Platform with the global threat intelligence and attack context needed to accelerate analysis, forensics, and hunting workflows?

A. Global Protect

B. WildFire

C. AutoFocus

D. STIX

Answer(s): C

15. DRAG DROP (Drag and Drop is not supported).

Match the description with the VPN technology.

Select and Place:

Primarily used for secure remote client VPN rather than for site-to-site VPN tunnels.		Generic Routing Encapsulation
Supported by most operating systems and provides no encryption by itself.		Layer 2 Tunneling Protocol
A tunneling protocol developed by Cisco Systems that can various network layer protocols inside point-to-point links.		Internet Protocol Security
A tunneling protocol that uses the Internet Key Exchange (IKE) to start a connection		Secure Socket Tunneling Protocol

A. See Explanation section for answer.

Answer(s): A

16. Which characteristic of serverless computing enables developers to quickly deploy application code?

A. Uploading cloud service autoscaling services to deploy more virtual machines to run their application code based on user demand

B. Uploading the application code itself, without having to provision a full container image or any OS virtual machine components

C. Using cloud service spot pricing to reduce the cost of using virtual machines to run their application code

D. Using Container as a Service (CaaS) to deploy application containers to run their code.

Answer(s): A

17. Which key component is used to configure a static route?

A. router ID

B. enable setting

C. routing protocol

D. next hop IP address

Answer(s): D

18. A native hypervisor runs:

A. with extreme demands on network throughput

B. only on certain platforms

C. within an operating system's environment

D. directly on the host computer's hardware

Answer(s): D

19. Which Palo Alto Networks product provides playbooks with 300+ multivendor integrations that help solve any security use case?

A. Cortex XSOAR

B. Prisma Cloud

C. AutoFocus

D. Cortex XDR

Answer(s): A

20. Which activities do local organization security policies cover for a SaaS application?

A. how the data is backed up in one or more locations

B. how the application can be used

C. how the application processes the data

D. how the application can transit the Internet

Answer(s): B
