Palo Alto Networks.PCCET.by.David.85q

Number: PCCET
Passing Score: 800
Time Limit: 120
File Version: 5.0

Exam Code: PCCET
Exam Name: Palo Alto Networks Certified Cybersecurity Entry-level Technician

Exam A

QUESTION 1
Which two pieces of information are considered personally identifiable information (PII)? (Choose two.)

A. Birthplace
B. Login 10
C. Profession
D. Name

Correct Answer: A, D
Section:
Explanation:
Personally identifiable information (PII) is any data that can be used to identify someone.All information that directly or indirectly links to a person is considered PII1. Among PII, some pieces of information are more sensitive than others.Sensitive PII is sensitive information that directly identifies an individual and could cause significant harm if leaked or stolen2.Birthplace and name are examples of sensitive PII, as they can be used to distinguish or trace an individual's identity, either alone or when combined with other information3. Login 10 and profession are not considered sensitive PII, as they are not unique to a person and do not reveal their identity.Login 10 is a non-sensitive PII that is easily accessible from public sources, while profession is not a PII at all, as it does not link to a specific individual4.Reference:
1: What is PII (personally identifiable information)? - Cloudflare
2: What is Personally Identifiable Information (PII)? | IBM
3: personally identifiable information - Glossary | CSRC
4: What Is Personally Identifiable Information (PII)? Types and Examples

QUESTION 2
TCP is the protocol of which layer of the OSI model?

A. Transport
B. Session
C. Data Link
D. Application

Correct Answer: A
Section:
Explanation:
TCP stands for Transmission Control Protocol, and it is one of the main protocols used in the internet.TCP provides reliable, ordered, and error-free delivery of data between applications1. In terms of the OSI model, TCP is a transport-layer protocol.The transport layer is the fourth layer of the OSI model, and it is responsible for establishing end-to-end connections, segmenting data into packets, and ensuring reliable and efficient data transfer2.The transport layer also provides flow control, congestion control, and error detection and correction mechanisms2.TCP is not the only transport-layer protocol; another common one is UDP (User Datagram Protocol), which is faster but less reliable than TCP3.Reference:1: TCP/IP TCP, UDP, and IP protocols - IBM2: Transport Layer | Layer 4 | The OSI-Model3: TCP/IP Model vs. OSI Model | Similarities and Differences - Fortinet

QUESTION 3
What is the purpose of SIEM?

A. Securing cloud-based applications
B. Automating the security team's incident response
C. Real-time monitoring and analysis of security events
D. Filtering webpages employees are allowed to access

Correct Answer: C
Section:
Explanation:
SIEM stands for security information and event management. It is a technology that collects, analyzes, and reports on security-related data from various sources within an organization's network. The purpose of SIEM is to provide real-time monitoring and analysis of security events, such as user logins, file access, and changes to critical system files. SIEM helps security teams to detect and respond to potential threats, as well as to meet compliance requirements and improve their cybersecurity posture.Reference:What Is Security Information and Event Management (SIEM)? - Palo Alto Networks,What is a SIEM Solution? - Palo Alto Networks,Integrate IoT Security with SIEM - Palo Alto Networks

QUESTION 4
Which network firewall primarily filters traffic based on source and destination IP address?

A. Proxy
B. Stateful
C. Stateless
D. Application

Correct Answer: C
Section:
Explanation:
A stateless firewall is a network firewall that primarily filters traffic based on source and destination IP address, as well as port numbers and protocols. A stateless firewall does not keep track of the state or context of network connections, and only inspects packet headers. A stateless firewall is faster and simpler than a stateful firewall, but it is less secure and flexible. A stateless firewall cannot block complex attacks or inspect packet contents for malicious payloads.Reference:What Is a Packet Filtering Firewall? - Palo Alto Networks,Common IP Filtering Techniques -- APNIC,What is IP filtering? - Secure Network Traffic Management

QUESTION 5
Which capability of a Zero Trust network security architecture leverages the combination of application, user, and content identification to prevent unauthorized access?

A. Cyber threat protection
B. Inspection of all traffic
C. Least privileges access control
D. Network segmentation

Correct Answer: C
Section:
Explanation:
Least privileges access control is the capability of a Zero Trust network security architecture that leverages the combination of application, user, and content identification to prevent unauthorized access. Least privileges access control means that users and devices are only granted the permissions they need to perform their tasks, and nothing more. This helps reduce the attack surface and makes it more difficult for attackers to gain access to sensitive data or resources. Least privileges access control is based on the principle of Zero Trust, which assumes that there are attackers both within and outside of the network, so no users or devices should be automatically trusted. Zero Trust verifies user identity and privileges as well as device identity and security, and requires end-to-end encryption. Least privileges access control also involves careful management of user permissions and network segmentation, which limit the amount of information and length of time people can access something, and contain the damage if someone does get unauthorized access.Reference:What Is Zero Trust Architecture? | Microsoft Security,Zero Trust security | What is a Zero Trust network? | Cloudflare,What is Zero Trust Architecture? | SANS Institute,What Is a Zero Trust Architecture? | Zscaler,What is Zero Trust Architecture (ZTA)? - CrowdStrike.

QUESTION 6
Which security component can detect command-and-control traffic sent from multiple endpoints within a corporate data center?

A. Personal endpoint firewall
B. Port-based firewall
C. Next-generation firewall

D. Stateless firewall

Correct Answer: C
Section:
Explanation:
A next-generation firewall (NGFW) is a security component that can detect command-and-control (C2) traffic sent from multiple endpoints within a corporate data center. A NGFW is a network device that combines traditional firewall capabilities with advanced features such as application awareness, intrusion prevention, threat intelligence, and cloud-based analysis. A NGFW can identify and block C2 traffic by inspecting the application layer protocols, signatures, and behaviors of the network traffic, as well as correlating the traffic with external sources of threat intelligence. A NGFW can also leverage inline cloud analysis to detect and prevent zero-day C2 threats in real-time. A NGFW can provide granular visibility and control over the network traffic, as well as generate alerts and reports on the C2 activity.Reference:
Palo Alto Networks Certified Cybersecurity Entry-level Technician (PCCET)
Command and Control, Tactic TA0011 - Enterprise | MITRE ATT&CK
Advanced Threat Prevention: Inline Cloud Analysis - Palo Alto Networks

QUESTION 7
Identify a weakness of a perimeter-based network security strategy to protect an organization's endpoint systems.

A. It cannot identify command-and-control traffic
B. It assumes that all internal devices are untrusted
C. It assumes that every internal endpoint can be trusted
D. It cannot monitor all potential network ports

Correct Answer: C
Section:
Explanation:
A perimeter-based network security strategy relies on firewalls, routers, and other devices to create a boundary between the internal network and the external network. This strategy assumes that every internal endpoint can be trusted, and that any threat comes from outside the network. However, this assumption is flawed, as internal endpoints can also be compromised by malware, phishing, insider attacks, or other methods. Once an attacker gains access to an internal endpoint, they can use it to move laterally within the network, bypassing the perimeter defenses. Therefore, a perimeter-based network security strategy is not sufficient to protect an organization's endpoint systems, and a more comprehensive approach, such as Zero Trust, is needed.Reference:
Palo Alto Networks Certified Cybersecurity Entry-level Technician (PCCET)
Traditional perimeter-based network defense is obsolete---transform to a Zero Trust model
What is Network Perimeter Security? Definition and Components | Acalvio

QUESTION 8
What is the recommended method for collecting security logs from multiple endpoints?

A. Leverage an EDR solution to request the logs from endpoints.
B. Connect to the endpoints remotely and download the logs.
C. Configure endpoints to forward logs to a SIEM.
D. Build a script that pulls down the logs from all endpoints.

Correct Answer: C
Section:
Explanation:
A SIEM (Security Information and Event Management) is a system that collects, analyzes, and correlates security logs from multiple sources, such as endpoints, firewalls, servers, etc. A SIEM can provide a centralized and comprehensive view of the security posture of an organization, as well as detect and respond to threats. Configuring endpoints to forward logs to a SIEM is the recommended method for collecting security logs from multiple endpoints, as it reduces the network bandwidth and storage requirements, simplifies the log management process, and enables faster and more effective security analysis. Leveraging an EDR (Endpoint Detection and Response) solution to request the logs from endpoints is not recommended, as it may cause performance issues on the endpoints, increase the network traffic, and create a dependency on the EDR solution. Connecting to the endpoints remotely and downloading the logs is not recommended, as it is a manual and time-consuming process, prone to errors and inconsistencies, and may expose the endpoints to unauthorized access. Building a script that pulls down the logs from all endpoints is not recommended, as it requires technical skills and maintenance, may not be compatible with different endpoint platforms, and may introduce security risks if the script is

compromised or misconfigured.Reference:
Palo Alto Networks Certified Cybersecurity Entry-level Technician (PCCET) - Palo Alto Networks
Fundamentals of Security Operations Center (SOC)
10 Palo Alto Networks PCCET Exam Practice Questions - CBT Nuggets

QUESTION 9
What does ''forensics'' refer to in a Security Operations process?

A. Collecting raw data needed to complete the detailed analysis of an investigation
B. Validating cyber analysts' backgrounds before hiring
C. Reviewing information about a broad range of activities
D. Analyzing new IDS/IPS platforms for an enterprise

Correct Answer: A
Section:
Explanation:
Forensics in a Security Operations process refers to collecting raw data needed to complete the detailed analysis of an investigation. Forensic analysis is a crucial step in identifying, investigating, and documenting the cause, course, and consequences of a security incident or violation. Forensic analysis involves various techniques and tools to extract, preserve, analyze, and present evidence in a structured and acceptable format. Forensic analysis can be used for legal compliance, auditing, incident response, and threat intelligence purposes.Reference:
Cyber Forensics Explained: Reasons, Phases & Challenges of Cyber Forensics
SOC Processes, Operations, Challenges, and Best Practices
What is Digital Forensics | Phases of Digital Forensics | EC-Council

QUESTION 10
If an endpoint does not know how to reach its destination, what path will it take to get there?

A. The endpoint will broadcast to all connected network devices.
B. The endpoint will not send the traffic until a path is clarified.
C. The endpoint will send data to the specified default gateway.
D. The endpoint will forward data to another endpoint to send instead.

Correct Answer: C
Section:
Explanation:
If an endpoint does not know how to reach its destination, it will send data to the specified default gateway. A default gateway is a device that routes traffic from a local network to other networks or the internet. The endpoint will use the default gateway's IP address as the next hop for packets that are destined for unknown or remote networks. The default gateway will then forward the packets to the appropriate destination or another gateway, based on its routing table.Reference:
Fundamentals of Network Security, Module 2: Networking Concepts, Lesson 2: IP Addressing and Routing1
PCCET Study Guide, Section 2.2: Describe IP Addressing and Routing2

QUESTION 11
A user is given access to a service that gives them access to cloud-hosted physical and virtual servers, storage, and networking.
Which NIST cloud service model is this?

A. IaaS
B. SaaS
C. PaaS
D. CaaS

Correct Answer: A
Section:
Explanation:
According to the NIST definition of cloud computing, Infrastructure as a Service (IaaS) is a cloud service model that provides ''the capability to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications''1.The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls)1.In other words, IaaS gives the user access to cloud-hosted physical and virtual servers, storage, and networking, as stated in the question.Reference:1: SP 800-145, The NIST Definition of Cloud Computing | CSRC2

QUESTION 12
Which native Windows application can be used to inspect actions taken at a specific time?

A. Event Viewer
B. Timeline inspector
C. Task Manager
D. Task Scheduler

Correct Answer: A
Section:
Explanation:
Event Viewer is a native Windows application that can be used to inspect actions taken at a specific time. Event Viewer displays detailed information about significant events on your computer, such as application, security, system, and setup events. You can use Event Viewer to monitor and troubleshoot problems with your computer, such as hardware failures, software errors, security breaches, network issues, etc. Event Viewer allows you to filter, sort, and search events by various criteria, such as date and time, event level, event source, event ID, etc. You can also view the event properties, which provide more details about the event, such as the event description, user name, computer name, event data, etc. Event Viewer can help you identify the root cause of a problem, or provide evidence of a malicious activity, by inspecting the actions taken at a specific time on your computer.Reference:
Palo Alto Networks Certified Cybersecurity Entry-level Technician (PCCET) - Palo Alto Networks
WinAppDriver and Desktop UI Test Automation - Microsoft Tech Community
Palo Alto Networks PCCET Quiz 1 Topic 14 Questions 1-5 - Buddy4Exam
Paloalto Networks Exam PCCET Questions and Answers - DumpsMate
Event Viewer - Windows 10 - Microsoft Docs

QUESTION 13
Which of the following is a Routed Protocol?

A. Routing Information Protocol (RIP)
B. Transmission Control Protocol (TCP)
C. Internet Protocol (IP)
D. Domain Name Service (DNS)

Correct Answer: C
Section:
Explanation:
A routed protocol is a protocol by which data can be routed. It provides appropriate addressing information in its internet layer or network layer to allow a packet to be forwarded from one network to another network. Examples of routed protocols are the Internet Protocol (IP) and Internetwork Packet Exchange (IPX). IP is the most widely used routed protocol on the Internet and other networks. It assigns a unique logical address to each device and enables data to be fragmented, reassembled, and routed across multiple networks.Reference:
Routing v/s Routed Protocols in Computer Network
Routing protocol - Wikipedia
CCNA Certification: Routed Protocols vs Routing Protocols
What is the difference between Routing Protocols and Routed Protocols

QUESTION 14
What are the two most prominent characteristics of the malware type rootkit? (Choose two.)

A. It encrypts user data.
B. It cannot be detected by antivirus because of its masking techniques.
C. It takes control of the operating system.
D. It steals personal information.

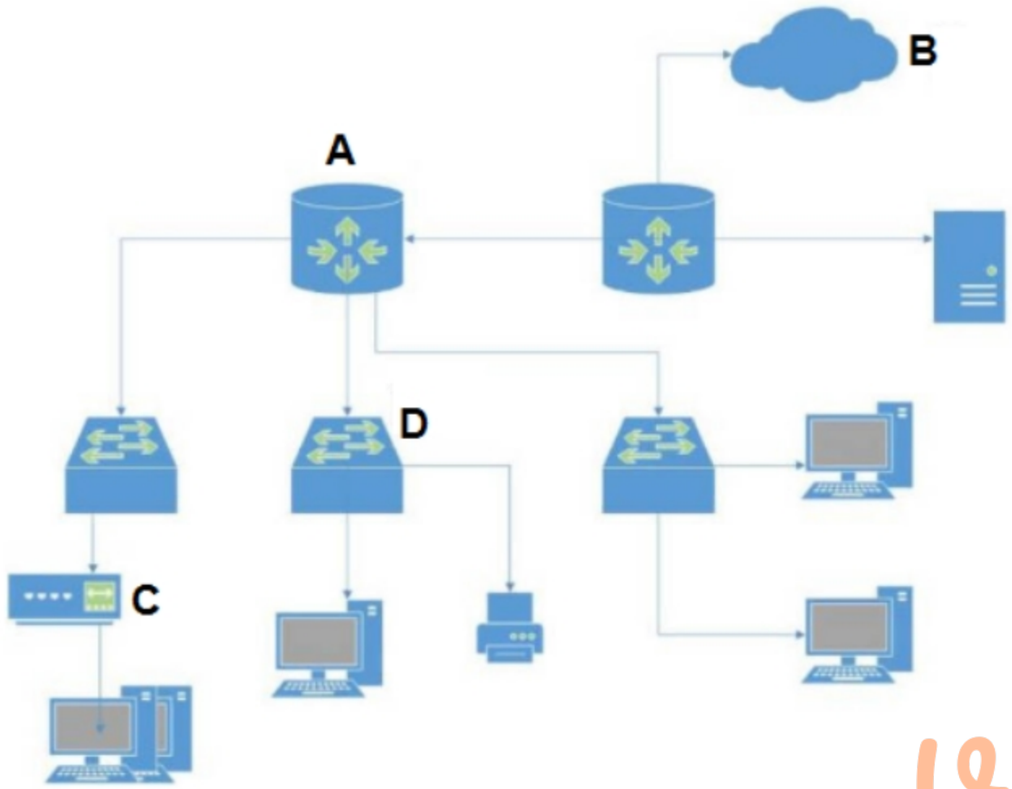
Correct Answer: B, C
Section:
Explanation:
A rootkit is a type of malware that enables cyber criminals to gain access to and infiltrate data from machines without being detected.It covers software toolboxes designed to infect computers, give the attacker remote control, and remain hidden for a long period of time1One of the most prominent characteristics of a rootkit is that it cannot be detected by antivirus because of its masking techniques.A rootkit may be able to subvert the software that is intended to find it, such as by hooking system calls, modifying kernel objects, or tampering with the registry2Another prominent characteristic of a rootkit is that it takes control of the operating system. A rootkit may install itself in the kernel or the firmware of the device, giving it the highest level of privilege and access. A rootkit may also replace the bootloader or the BIOS of the machine, making it difficult to remove.A rootkit can use its control over the operating system to launch other malware, such as ransomware, bots, keyloggers, or trojans34Reference:
1: What Is a Rootkit? How to Defend and Stop Them? | Fortinet
2: Rootkit - Wikipedia
3: What Is a Rootkit? -- Microsoft 365
4: What is Rootkit? Attack Definition & Examples - CrowdStrike

QUESTION 15
What is a key method used to secure sensitive data in Software-as-a-Service (SaaS) applications?

A. Allow downloads to managed devices but block them from unmanaged devices.
B. Allow downloads to both managed and unmanaged devices.
C. Leave data security in the hands of the cloud service provider.
D. Allow users to choose their own applications to access data.

Correct Answer: A
Section:
Explanation:
One of the best practices for securing sensitive data in SaaS applications is to control the access and usage of data based on the device type. Managed devices are those that are enrolled and monitored by the organization's IT department, and have security policies and controls applied to them. Unmanaged devices are those that are not under the organization's control, such as personal laptops or mobile phones. Allowing downloads to managed devices but blocking them from unmanaged devices prevents data leakage and unauthorized access to sensitive data.This can be achieved by using a cloud access security broker (CASB) solution, such as Prisma SaaS from Palo Alto Networks, which can enforce granular policies based on device posture, user identity, and data sensitivity12.Reference:1: Securing SaaS applications on the cloud is a critical aspect of protecting sensitive data and maintaining the trust of customers.By implementing best practices, such as enhanced authentication, data encryption, Break Glass, and oversight, organizations can mitigate the security risks associated with SaaS applications2: Prisma SaaS - Palo Alto Networks

QUESTION 16
In the network diagram below, which device is the router?



A. A
B. C
C. D
D. B

Correct Answer: D
Section:
Explanation:
In the given network diagram, device D is depicted as a cloud symbol, which is commonly used to represent the internet in network diagrams. The router is typically connected to the internet and acts as a gateway for internal network devices to access external networks. Therefore, device D is the router in this context.Reference:Virtual Router Overview - Palo Alto Networks | TechDocs,Networking (UDRs) in Azure: Inserting the VM-Series into an Azure ...,Setting Up the PA-200 for Home and Small Office - Palo Alto Networks ...

QUESTION 17
Which SOAR feature coordinates across technologies, security teams, and external users for centralized data visibility and action?

A. Case management
B. Integrations
C. Ticketing system
D. Playbooks

Correct Answer: D
Section:

Explanation:
Playbooks are collections of workflows that automate and orchestrate tasks, alerts, and responses to incidents. Playbooks are triggered by rules or incidents and can coordinate across technologies, security teams, and external users for centralized data visibility and action. Playbooks can help improve the efficiency and effectiveness of security operations by reducing manual work, streamlining processes, and enhancing collaboration.Reference:What Is SOAR? - Palo Alto Networks,What Is SOAR? Technology and Solutions | Microsoft Security,How SecOps can help solve these 6 key MSSP conundrums - Google Cloud

QUESTION 18
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

Correct Answer: A
Section:
Explanation:
Dynamic analysis is a method of malware analysis that executes the malware in a controlled environment and observes its behavior and effects. Dynamic analysis can reveal the malware's network activity, file system changes, registry modifications, and other indicators of compromise. Dynamic analysis is performed by Palo Alto Networks WildFire, a cloud-based service that analyzes unknown files and links from various sources, such as email attachments, web downloads, and firewall traffic. WildFire uses a custom-built, evasion-resistant virtual environment to detonate the submissions and generate detailed reports and verdicts. WildFire can also share the threat intelligence with other Palo Alto Networks products and partners to prevent future attacks.Reference:WildFire Overview,WildFire Features,WildFire Dynamic Analysis

QUESTION 19
What is required for a SIEM to operate correctly to ensure a translated flow 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

Correct Answer: A
Section:
Explanation:
Connectors and interfaces are the components that enable a SIEM to collect, process, and analyze data from various sources, such as Microsoft 365 services and applications1, cloud platforms, network devices, and security solutions. Connectors are responsible for extracting and transforming data from the source systems, while interfaces are responsible for sending and receiving data to and from the SIEM server. Without connectors and interfaces, a SIEM cannot operate correctly and ensure a translated flow from the system of interest to the SIEM data lake.Reference:
SIEM server integration with Microsoft 365 services and applications
What Is SIEM Integration? 2024 Comprehensive Guide - SelectHub
SIEM Connector - docs.metallic.io
SIEM Connector

QUESTION 20
Which type of Wi-Fi attack depends on the victim initiating the connection?

A. Evil twin
B. Jasager
C. Parager
D. Mirai

Correct Answer: A
Section:
Explanation:
An evil twin is a type of Wi-Fi attack that involves setting up a fake malicious Wi-Fi hotspot with the same name as a legitimate network to trick users into connecting to it. The attacker can then intercept the user's data, such as passwords, credit card numbers, or personal information. The victim initiates the connection by choosing the fake network from the list of available Wi-Fi networks, thinking it is the real one. The attacker can also use a deauthentication attack to disconnect the user from the legitimate network and force them to reconnect to the fake one.Reference:
Types of Wi-Fi Attacks You Need to Guard Your Business Against - TechGenix
Types of Wireless and Mobile Device Attacks - GeeksforGeeks
The 5 most dangerous Wi-Fi attacks, and how to fight them
What are Wi-Fi Attacks & How to Fight - Tech Resider

QUESTION 21
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 traffic
B. Intrazone traffic
C. East-West traffic
D. Interzone traffic

Correct Answer: A
Section:
Explanation:
North-South traffic refers to the data packets that move between the virtualized environment and the external network, such as the internet or a traditional data center. This traffic typically involves requests from clients to access applications or services hosted on virtual machines (VMs) or containers, or responses from those VMs or containers to the clients. North-South traffic can also include management or monitoring traffic from external devices to the virtualized environment.Reference:Fundamentals of Cloud Security,East-West and North-South Traffic Security,What is the meaning / origin of the terms north-south and east-west traffic?

QUESTION 22
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

Correct Answer: B
Section:
Explanation:
SecOps is the organizational function that is responsible for security automation and eventual vetting of the solution to help ensure consistency through machine-driven responses to security issues. SecOps is a collaboration between security and operations teams that aims to align their goals, processes, and tools to improve security posture and efficiency. SecOps can leverage automation to simplify and accelerate security tasks, such as threat detection, incident response, vulnerability management, compliance enforcement, and more. Security automation can also reduce human errors, enhance scalability, and free up resources for more strategic initiatives.Reference:
SecOpsfrom Palo Alto Networks
What is security automation?from Red Hat
What is Security Automation?from Check Point Software

QUESTION 23
On an endpoint, which method should you use to secure applications against exploits?

A. endpoint-based firewall
B. strong user passwords
C. full-disk encryption
D. software patches

Correct Answer: D
Section:
Explanation:
Software patches are updates that fix bugs, vulnerabilities, or performance issues in applications. Applying software patches regularly is one of the best practices to secure applications against exploits, as it prevents attackers from taking advantage of known flaws in the software. Software patches can also improve the functionality and compatibility of applications, as well as address any security gaps that may arise from changes in the operating system or other software components. Endpoint security solutions, such as Cortex XDR, can help organizations automate and streamline the patch management process, ensuring that all endpoints are up to date and protected from exploits.Reference:
Endpoint Protection - Palo Alto Networks
Endpoint Security - Palo Alto Networks
Patch Management - Palo Alto Networks

QUESTION 24
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

Correct Answer: B
Section:
Explanation:
MITRE is a not-for-profit organization that operates research and development centers sponsored by the federal government. MITRE maintains the Common Vulnerabilities and Exposures (CVE) catalog, which is a dictionary of common names for publicly known cybersecurity vulnerabilities.CVE's common identifiers, called CVE Identifiers, make it easier to share data across separate network security databases and tools, and provide a baseline for evaluating the coverage of an organization's security tools12.Reference:
Common Vulnerabilities and Exposures (CVE)
CVE - CVE

QUESTION 25
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

Correct Answer: D
Section:
Explanation:
Cortex XDR is a security analytics platform that converges logs from network, identity, endpoint, application, and other security relevant sources to generate high-fidelity behavioral alerts and facilitate rapid incident analysis, investigation, and response1.Cortex XDR uses machine learning algorithms to automate data analysis and apply modeling in real time, helping organizations to reduce analyst workloads and improve security1.Cortex XDR also integrates with Palo Alto Networks next-generation firewalls and other security tools to streamline and speed network security response2.Reference:Security Analytics - Palo Alto Networks,Network Security Automation - Palo Alto Networks

QUESTION 26
Which endpoint product from Palo Alto Networks can help with SOC visibility?

A. STIX
B. Cortex XDR
C. WildFire
D. AutoFocus

Correct Answer: B
Section:
Explanation:
Cortex XDR is an endpoint product from Palo Alto Networks that can help with SOC visibility by allowing you to rapidly detect and respond to threats across your networks, endpoints, and clouds. It assists SOC analysts by allowing them to view all the alerts from all Palo Alto Networks products in one place, and to perform root cause analysis and automated response actions.Cortex XDR also integrates with other Palo Alto Networks products, such as WildFire, AutoFocus, and Cortex Data Lake, to provide comprehensive threat intelligence and data enrichment12.Reference:
SOC Services - Palo Alto Networks
Endpoint Protection - Palo Alto Networks
Security Operations | Palo Alto Networks
Cortex - Palo Alto Networks

QUESTION 27
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

Correct Answer: B
Section:
Explanation:
Port hopping is a technique that changes protocols at random during a session to evade detection and analysis by security devices. Port hopping can be used by malware or attackers to communicate with command and control servers or to exfiltrate data. Port hopping makes it difficult to identify and block malicious traffic based on port numbers or signatures.Reference:Port Hopping,Ports Used for Management Functions,Adding a Custom Application/Ports to Security Policy

QUESTION 28
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 sysvol 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

Correct Answer: D
Section:
Explanation:
page 211 'Consolidating servers within trust levels: Organizations often consolidate servers within the same trust level into a single virtual computing environment: ... ... This virtual systems capability enables a single physical device to be used to simultaneously meet the unique requirements of multiple VMs or groups of VMs. Control and protection of inter-host traffic with physical network security appliances that are properly positioned and configured is the primary security focus.'

QUESTION 29
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

Correct Answer: C
Section:
Explanation:
page 173 'AutoFocus makes over a billion samples and sessions, including billions of artifacts, immediately actionable for security analysis and response efforts. AutoFocus extends the product portfolio with the global threat intelligence and attack context needed to accelerate analysis, forensics, and hunting workflows. Together, the platform and AutoFocus move security teams away from legacy manual approaches that rely on aggregating a growing number of detectionbased alerts and post-event mitigation, to preventing sophisticated attacks and enabling proactive hunting activities.'

QUESTION 30
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.

Correct Answer: B
Section:
Explanation:
'In serverless apps, the developer uploads only the app package itself, without a full container image or any OS components. The platform dynamically packages it into an image, runs the image in a container, and (if needed) instantiates the underlying host OS and VM and the hardware required to run them.'

QUESTION 31
Which key component is used to configure a static route?

A. router ID
B. enable setting
C. routing protocol
D. next hop IP address

Correct Answer: D
Section:
Explanation:
A static route is a manually configured route that specifies the destination network and the next hop IP address or interface to reach it. A static route does not depend on any routing protocol and remains in the routing table until it is removed or overridden. Static routes are useful for defining default routes, reaching stub networks, or providing backup routes in case of link failures. To configure a static route in a virtual router on a Palo Alto Networks firewall, you need to specify the name, destination, interface, and next hop IP address or virtual router of the route.Reference:Configure a Static Route in Virtual Routers,Palo Alto Networks Certified Cybersecurity Entry-level Technician (PCCET),FREE Cybersecurity Education Courses

QUESTION 32
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

Correct Answer: D
Section:
Explanation:
Type 1 (native or bare metal). Runs directly on the host computer's hardware
Type 2 (hosted). Runs within an operating system environment

QUESTION 33
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

Correct Answer: A
Section:
Explanation:
SOAR tools ingest aggregated alerts from detection sources (such as SIEMs, network security tools, and mailboxes) before executing automatable, process-driven playbooks to enrich and respond to these alerts.
https://www.paloaltonetworks.com/cortex/security-operations-automation

QUESTION 34
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

Correct Answer: B
Section:
Explanation:
Local organization security policies are the rules and guidelines that define how a SaaS application can be used by the employees, contractors, and partners of an organization. These policies cover aspects such as authentication, authorization, data access, data protection, data sharing, and compliance.Local organization security policies aim to ensure that the SaaS application is used in a secure, ethical, and legal manner, and that the organization's data and assets are not compromised or misused123.Reference:
Securing SaaS tools for your organisation - GOV.UK
SaaS Security: A Complete Best Practices Guide - BetterCloud
Security policy document examples for B2B SaaS apps

QUESTION 35
Which option is a Prisma Access security service?

A. Compute Security
B. Firewall as a Service (FWaaS)

C. Virtual Private Networks (VPNs)
D. Software-defined wide-area networks (SD-WANs)

Correct Answer: B
Section:
Explanation:
Prisma Access provides firewall as a service (FWaaS) that protects branch offices from threats while also providing the security services expected from a next-generation firewall. The full spectrum of FWaaS includes threat prevention, URL filtering, sandboxing, and more.

QUESTION 36
Which pillar of Prisma Cloud application security addresses ensuring that your cloud resources and SaaS applications are correctly configured?

A. visibility, governance, and compliance
B. network protection
C. dynamic computing
D. compute security

Correct Answer: A
Section:
Explanation:
Ensuring that your cloud resources and SaaS applications are correctly configured and adhere to your organization's security standards from day one is essential to prevent successful attacks. Also, making sure that these applications, and the data they collect and store, are properly protected and compliant is critical to avoid costly fines, a tarnished image, and loss of customer trust. Meeting security standards and maintaining compliant environments at scale, and across SaaS applications, is the new expectation for security teams.

QUESTION 37
Which item accurately describes a security weakness that is caused by implementing a ''ports first'' data security solution in a traditional data center?

A. You may have to use port numbers greater than 1024 for your business-critical applications.
B. You may have to open up multiple ports and these ports could also be used to gain unauthorized entry into your datacenter.
C. You may not be able to assign the correct port to your business-critical applications.
D. You may not be able to open up enough ports for your business-critical applications which will increase the attack surface area.

Correct Answer: B
Section:
Explanation:
A ''ports first'' data security solution is a traditional approach that relies on port numbers to identify and filter network traffic.This approach has several limitations and security weaknesses, such as12:
Port numbers are not reliable indicators of the type or content of network traffic, as they can be easily spoofed or changed by malicious actors.
Port numbers do not provide any visibility into the application layer, where most of the attacks occur.
Port numbers do not account for the dynamic and complex nature of modern applications, which often use multiple ports or protocols to communicate.
Port numbers do not support granular and flexible policies based on user identity, device context, or application behavior. One of the security weaknesses that is caused by implementing a ''ports first'' data security solution in a traditional data center is that you may have to open up multiple ports and these ports could also be used to gain unauthorized entry into your datacenter. For example, if you have a web server that runs on port 80, you may have to open up port 80 on your firewall to allow incoming traffic. However, this also means that any other service or application that uses port 80 can also access your datacenter, potentially exposing it to attacks.Moreover, opening up multiple ports increases the attack surface area of your network, as it creates more entry points for attackers to exploit34.Reference:Common Open Port Vulnerabilities List - Netwrix,Optimize security with Azure Firewall solution for Azure Sentinel | Microsoft Security Blog,Which item accurately describes a security weakness that is caused by ...,Which item accurately describes a security weakness ... - Exam4Training

QUESTION 38
Which statement describes DevOps?

A. DevOps is its own separate team
B. DevOps is a set of tools that assists the Development and Operations teams throughout the software delivery process
C. DevOps is a combination of the Development and Operations teams
D. DevOps is a culture that unites the Development and Operations teams throughout the software delivery process

Correct Answer: D
Section:
Explanation:
DevOps is not:
A combination of the Dev and Ops teams: There still are two teams; they just operate in a communicative, collaborative way.
Its own separate team: There is no such thing as a ''DevOps engineer.'' Although some companies may appoint a ''DevOps team'' as a pilot when trying to transition to a DevOps culture, DevOps refers to a culture where developers, testers, and operations personnel cooperate throughout the entire software delivery lifecycle.
A tool or set of tools: Although there are tools that work well with a DevOps model or help promote DevOps culture, DevOps ultimately is a strategy, not a tool.
Automation: Although automation is very important for a DevOps culture, it alone does not define DevOps.

QUESTION 39
Which product from Palo Alto Networks enables organizations to prevent successful cyberattacks as well as simplify and strengthen security processes?

A. Expedition
B. AutoFocus
C. MineMeld
D. Cortex XDR

Correct Answer: D
Section:
Explanation:
From a business perspective, XDR platforms enable organizations to prevent successful cyberattacks as well as simplify and strengthen security processes.

QUESTION 40
Which network firewall operates up to Layer 4 (Transport layer) of the OSI model and maintains information about the communication sessions which have been established between hosts on trusted and untrusted networks?

A. Group policy
B. Stateless
C. Stateful
D. Static packet-filter

Correct Answer: C
Section:
Explanation:
Stateful packet inspection firewalls Second-generation stateful packet inspection (also known as dynamic packet filtering) firewalls have the following characteristics:
They operate up to Layer 4 (Transport layer) of the OSI model and maintain state information about the communication sessions that have been established between hosts on the trusted and untrusted networks.
They inspect individual packet headers to determine source and destination IP address, protocol (TCP, UDP, and ICMP), and port number (during session establishment only) to determine whether the session should be allowed, blocked, or dropped based on configured firewall rules.
After a permitted connection is established between two hosts, the firewall creates and deletes firewall rules for individual connections as needed, thus effectively creating a tunnel that allows traffic to flow between the two hosts without further inspection of individual packets during the session.
This type of firewall is very fast, but it is port-based and it is highly dependent on the trustworthiness of the two hosts because individual packets aren't inspected after the connection is established.

QUESTION 41
Which subnet does the host 192.168.19.36/27 belong?

A. 192.168.19.0
B. 192.168.19.16
C. 192.168.19.64
D. 192.168.19.32

Correct Answer: B
Section:
Explanation:
To find the subnet that the host 192.168.19.36/27 belongs to, we need to convert the IP address and the subnet mask to binary form and perform a logical AND operation. The /27 notation means that the subnet mask has 27 bits of ones and 5 bits of zeros. In decimal form, the subnet mask is 255.255.255.224. The binary form of the IP address and the subnet mask are:
IP address: 11000000.10101000.00010011.00100100 Subnet mask: 11111111.11111111.11111111.11100000
The logical AND operation gives us the network prefix:
Network prefix: 11000000.10101000.00010011.00100000
To get the subnet address, we convert the network prefix back to decimal form:
Subnet address: 192.168.19.32
The subnet address is the first address in the subnet range. To find the last address in the subnet range, we flip the bits of the subnet mask and perform a logical OR operation with the network prefix:
Flipped subnet mask: 00000000.00000000.00000000.00011111 Logical OR: 11000000.10101000.00010011.00111111
The last address in the subnet range is:
Last address: 192.168.19.63
The subnet range is from 192.168.19.32 to 192.168.19.63. The host 192.168.19.36 belongs to this subnet. Therefore, the correct answer is B. 192.168.19.16, which is the second address in the subnet range.
IP Subnet Calculator
Subnet Calculator - IP and CIDR
Which subnet does the host 192.168.19.36/27 belong? - VCEguide.com

QUESTION 42
Order the OSI model with Layer7 at the top and Layer1 at the bottom.

A. Layer 1
B. Layer 2
C. Layer 3
D. Layer 7

Correct Answer: A, D
Section:

QUESTION 43
How does Prisma SaaS provide protection for Sanctioned SaaS applications?

A. Prisma SaaS connects to an organizations internal print and file sharing services to provide protection and sharing visibility
B. Prisma SaaS does not provide protection for Sanctioned SaaS applications because they are secure
C. Prisma access uses Uniform Resource Locator (URL) Web categorization to provide protection and sharing visibility
D. Prisma SaaS connects directly to sanctioned external service providers SaaS application service to provide protection and sharing visibility

Correct Answer: D
Section:

Explanation:
Prisma SaaS connects directly to the applications themselves, therefore providing continuous silent monitoring of the risks within the sanctioned SaaS applications, with detailed visibility that is not possible with traditional security solutions.

QUESTION 44
Which type of Software as a Service (SaaS) application provides business benefits, is fast to deploy, requires minimal cost and is infinitely scalable?

A. Benign
B. Tolerated
C. Sanctioned
D. Secure

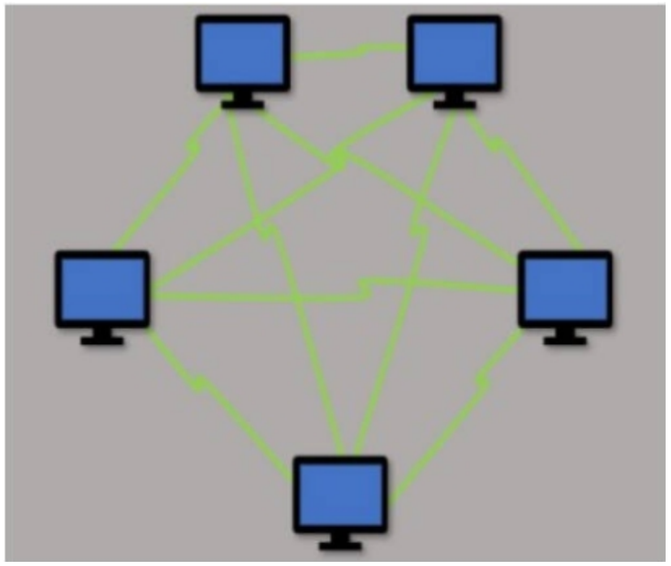
Correct Answer: C
Section:
Explanation:
Sanctioned SaaS applications are those that are approved and supported by the organization's IT department. They provide business benefits such as increased productivity, collaboration, and efficiency. They are fast to deploy because they do not require installation or maintenance on the user's device. They require minimal cost because they are usually paid on a subscription or usage basis, and they do not incur hardware or software expenses.They are infinitely scalable because they can adjust to the changing needs and demands of the organization without affecting performance or availability12.Reference:8 Types of SaaS Solutions You Must Know About in 2024,What is SaaS (Software as a Service)? | SaaS Types | CDW,Palo Alto Networks Certified Cybersecurity Entry-level Technician

QUESTION 45
How does DevSecOps improve the Continuous Integration/Continuous Deployment (CI/CD) pipeline?

A. DevSecOps improves pipeline security by assigning the security team as the lead team for continuous deployment
B. DevSecOps ensures the pipeline has horizontal intersections for application code deployment
C. DevSecOps unites the Security team with the Development and Operations teams to integrate security into the CI/CD pipeline
D. DevSecOps does security checking after the application code has been processed through the CI/CD pipeline

Correct Answer: C
Section:
Explanation:
DevSecOps takes the concept behind DevOps that developers and IT teams should work together closely, instead of separately, throughout software delivery and extends it to include security and integrate automated checks into the full CI/CD pipeline. The integration of the CI/CD pipeline takes care of the problem of security seeming like an outside force and instead allows developers to maintain their usual speed without compromising data security

QUESTION 46
Which type of LAN technology is being displayed in the diagram?



A. Star Topology
B. Spine Leaf Topology
C. Mesh Topology
D. Bus Topology

Correct Answer: C
Section:
Explanation:
The diagram displays a mesh topology, where each device is connected to every other device in the network. This topology is characterized by the multiple connections each node has, ensuring there is no single point of failure and providing redundant paths for data transmission, enhancing the reliability and resilience of the network.Mesh topology is one of the types of LAN technology that uses ethernet or Wi-Fi to connect devices12.Reference:
What Is Local Area Network (LAN)? Definition, Types, Architecture, and Best Practicesfrom Spiceworks
Types of LAN | Introduction and Classification of LANfrom EDUCBA

QUESTION 47
What does SOAR technology use to automate and coordinate workflows?

A. algorithms
B. Cloud Access Security Broker
C. Security Incident and Event Management
D. playbooks

Correct Answer: D
Section:
Explanation:
SOAR tools ingest aggregated alerts from detection sources (such as SIEMs, network security tools, and mailboxes) before executing automatable, process-driven playbooks to enrich and respond to these alerts.

QUESTION 48
In a traditional data center what is one result of sequential traffic analysis?

A. simplifies security policy management
B. reduces network latency
C. causes security policies to be complex
D. improves security policy application ID enforcement

Correct Answer: C
Section:
Explanation:
Multiple policies, no policy reconciliation tools: Sequential traffic analysis (stateful inspection, application control, intrusion prevention system (IPS), anti-malware, etc.) in traditional data center security solutions requires a corresponding security policy or profile, often using multiple management tools. The result is that your security policies become convoluted as you build and manage a firewall policy with source, destination, user, port, and action; an application control policy with similar rules; and any other threat prevention rules required. Multiple security policies that mix positive (firewall) and negative (application control, IPS, and anti-malware) control models can cause security holes by missing traffic and/or not identifying

QUESTION 49
Which three services are part of Prisma SaaS? (Choose three.)

A. Data Loss Prevention
B. DevOps
C. Denial of Service
D. Data Exposure Control
E. Threat Prevention

Correct Answer: A, D, E
Section:
Explanation:
Prisma SaaS is a cloud access security broker (CASB) solution that helps secure and manage SaaS applications.It provides advanced capabilities in risk discovery, data loss prevention, compliance assurance, data governance, user behavior monitoring, and advanced threat prevention12. The three services that are part of Prisma SaaS are:
Data Loss Prevention: This service helps prevent the leakage or exposure of sensitive data stored in SaaS applications.It allows you to define data patterns, policies, and actions to protect your data from unauthorized access or sharing3.
Data Exposure Control: This service helps identify and remediate data exposure risks in SaaS applications. It scans your data at rest and classifies it based on its sensitivity and exposure level.It also provides recommendations and remediation actions to reduce the risk of data breaches4.
Threat Prevention: This service helps detect and block malicious activities and threats in SaaS applications. It leverages the WildFire and AutoFocus threat intelligence services to analyze user and file activity and identify indicators of compromise.It also provides alerts and response actions to mitigate the impact of threats5.
Prisma SaaS Overview
Prisma SaaS - Palo Alto Networks
Data Loss Prevention
Data Exposure Control
Threat Prevention

QUESTION 50
In which phase of the cyberattack lifecycle do attackers establish encrypted communication channels back to servers across the internet so that they can modify their attack objectives and methods?

A. exploitation
B. actions on the objective
C. command and control
D. installation

Correct Answer: C

Section:
Explanation:
Command and Control: Attackers establish encrypted communication channels back to command-and-control (C2) servers across the internet so that they can modify their attack objectives and methods as additional targets of opportunity are identified within the victim network, or to evade any new security countermeasures that the organization may attempt to deploy if attack artifacts are discovered.

QUESTION 51
Which of the following is an AWS serverless service?

A. Beta
B. Kappa
C. Delta
D. Lambda

Correct Answer: D
Section:
Explanation:
Examples of serverless environments include Amazon Lambda and Azure Functions. Many PaaS offerings, such as Pivotal Cloud Foundry, also are effectively serverless even if they have not historically been marketed as such. Although serverless may appear to lack the container-specific, cloud native attribute, containers are extensively used in the underlying implementations, even if those implementations are not exposed to end users directly.

QUESTION 52
In which situation would a dynamic routing protocol be the quickest way to configure routes on a router?

A. the network is large
B. the network is small
C. the network has low bandwidth requirements
D. the network needs backup routes

Correct Answer: A
Section:
Explanation:
A static routing protocol requires that routes be created and updated manually on a router or other network device. If a static route is down, traffic can't be automatically rerouted unless an alternate route has been configured. Also, if the route is congested, traffic can't be automatically rerouted over the less congested alternate route. Static routing is practical only in very small networks or for very limited, special-case routing scenarios (for example, a destination that's used as a backup route or is reachable only via a single router). However, static routing has low bandwidth requirements (routing information isn't broadcast across the network) and some built-in security (users can route only to destinations that are specified in statically defined routes).

QUESTION 53
Which three layers of the OSI model correspond to the Application Layer (L4) of the TCP/IP model?

A. Session, Transport, Network
B. Application, Presentation, and Session
C. Physical, Data Link, Network
D. Data Link, Session, Transport

Correct Answer: B
Section:
Explanation:
Application (Layer 4 or L4): This layer loosely corresponds to Layers 5 through 7 of the OSI model.
Transport (Layer 3 or L3): This layer corresponds to Layer 4 of the OSI model.

Internet (Layer 2 or L2): This layer corresponds to Layer 3 of the OSI model.
Network Access (Layer 1 or L1): This layer corresponds to Layers 1 and 2 of the OSI model

QUESTION 54
A user is provided access over the internet to an application running on a cloud infrastructure. The servers, databases, and code of that application are hosted and maintained by the vendor.
Which NIST cloud service model is this?

A. IaaS
B. SaaS
C. PaaS
D. CaaS

Correct Answer: B
Section:
Explanation:
According to the NIST definition of cloud computing1, there are three service models for cloud computing: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). In the SaaS model, the cloud provider delivers the software applications over the internet, and the users access them from various devices through a web browser or a program interface. The cloud provider manages the underlying infrastructure, including the servers, databases, and code of the applications. The users do not need to install, update, or maintain the software, and they only pay for the service they use. The scenario described in the question is an example of the SaaS model, as the user is provided access over the internet to an application running on a cloud infrastructure, and the vendor hosts and maintains the servers, databases, and code of that application.Reference:
SP 800-145, The NIST Definition of Cloud Computing | CSRC
Final Version of NIST Cloud Computing Definition Published
NIST Cloud Computing Program - NCCP | NIST
SaaS - User responsible for only the data, vendor responsible for rest

QUESTION 55
Which type of malware replicates itself to spread rapidly through a computer network?

A. ransomware
B. Trojan horse
C. virus
D. worm

Correct Answer: D
Section:
Explanation:
A worm is a type of malware that replicates itself to spread rapidly through a computer network. Unlike a virus, a worm does not need a host program or human interaction to infect other devices.A worm can consume network bandwidth, slow down the system performance, or deliver a malicious payload, such as ransomware or a backdoor123.Reference:Types of Malware & Malware Examples - Kaspersky,10 types of malware + how to prevent malware from the start,Computer worm - Wikipedia
A worm replicates through the network while a virus replicates, not necessarily to spread through the network.

QUESTION 56
From which resource does Palo Alto Networks AutoFocus correlate and gain URL filtering intelligence?

A. Unit 52
B. PAN-DB
C. BrightCloud
D. MineMeld

Correct Answer: B
Section:
Explanation:
When you enable URL Filtering, all web traffic is compared against the URL Filtering database, PAN-DB, which contains millions of URLs that have been grouped into about 65 categories.

QUESTION 57
Which of the following is a service that allows you to control permissions assigned to users in order for them to access and utilize cloud resources?

A. User-ID
B. Lightweight Directory Access Protocol (LDAP)
C. User and Entity Behavior Analytics (UEBA)
D. Identity and Access Management (IAM)

Correct Answer: D
Section:
Explanation:
Identity and access management (IAM) is a software service or framework that allows organizations to define user or group identities within software environments, then associate permissions with them. The identities and permissions are usually spelled out in a text file, which is referred to as an IAM policy.

QUESTION 58
Which pillar of Prisma Cloud application security does vulnerability management fall under?

A. dynamic computing
B. identity security
C. compute security
D. network protection

Correct Answer: C
Section:
Explanation:
Prisma Cloud comprises four pillars:
Visibility, governance, and compliance. Gain deep visibility into the security posture of multicloud environments. Track everything that gets deployed with an automated asset inventory, and maintain compliance with out-of-the-box governance policies that enforce good behavior across your environments.
Compute security. Secure hosts, containers, and serverless workloads throughout the application lifecycle. Detect and prevent risks by integrating vulnerability intelligence into your integrated development environment (IDE), software configuration management
(SCM), and CI/CD workflows. Enforce machine learning-based runtime protection to protect applications and workloads in real time.
Network protection. Continuously monitor network activity for anomalous behavior, enforce microservice-aware micro-segmentation, and implement industry-leading firewall protection. Protect the network perimeter and the connectivity between containers and hosts.
Identity security. Monitor and leverage user and entity behavior analytics (UEBA) across your environments to detect and block malicious actions. Gain visibility into and enforce governance p

QUESTION 59
What is used to orchestrate, coordinate, and control clusters of containers?

A. Kubernetes
B. Prisma Saas
C. Docker
D. CN-Series

Correct Answer: A
Section:
Explanation:
As containers grew in popularity and used diversified orchestrators such as Kubernetes (and its derivatives, such as OpenShift), Mesos, and Docker Swarm, it became increasingly important to deploy and operate containers at scale.
https://www.dynatrace.com/news/blog/kubernetes-vs-docker/

QUESTION 60
Under which category does an application that is approved by the IT department, such as Office 365, fall?

A. unsanctioned
B. prohibited
C. tolerated
D. sanctioned

Correct Answer: D
Section:
Explanation:
A sanctioned application is an application that is approved by the IT department and meets the security and compliance requirements of the organization. Sanctioned applications are allowed to access the organization's network and data and are monitored and protected by the IT department. Examples of sanctioned applications are Office 365, Salesforce, and Zoom. Sanctioned applications are different from unsanctioned, prohibited, and tolerated applications, which are not approved by the IT department and may pose security risks to the organization. Unsanctioned applications are applications that are used by the employees without the IT department's knowledge or consent, such as Dropbox, Gmail, or Facebook. Prohibited applications are applications that are explicitly forbidden by the IT department, such as BitTorrent, Tor, or malware. Tolerated applications are applications that are not approved by the IT department, but are not blocked or restricted, such as Skype, Spotify, or YouTube.Reference:Palo Alto Networks Certified Cybersecurity Entry-level Technician (PCCET),Cloud Security Fundamentals - Module 4: Cloud Security Best Practices,Application Visibility and Control

QUESTION 61
What are three benefits of SD-WAN infrastructure? (Choose three.)

A. Improving performance of SaaS applications by requiring all traffic to be back-hauled through the corporate headquarters network
B. Promoting simplicity through the utilization of a centralized management structure
C. Utilizing zero-touch provisioning for automated deployments
D. Leveraging remote site routing technical support by relying on MPLS
E. Improving performance by allowing efficient access to cloud-based resources without requiring back-haul traffic to a centralized location

Correct Answer: B, C, E
Section:
Explanation:
Simplicity: Because each device is centrally managed, with routing based on application policies, WAN managers can create and update security rules in real time as network requirements change. Also, when SD-WAN is combined with zero-touch provisioning, a feature that helps automate the deployment and configuration processes, organizations can further reduce the complexity, resources, and operating expenses required to spin up new sites. Improved performance: By allowing efficient access to cloud-based resources without the need to backhaul traffic to centralized locations, organizations can provide a better user experience.

QUESTION 62
Which security component should you configure to block viruses not seen and blocked by the perimeter firewall?

A. endpoint antivirus software
B. strong endpoint passwords
C. endpoint disk encryption
D. endpoint NIC ACLs

Correct Answer: A
Section:
Explanation:
Endpoint antivirus software is a type of software designed to help detect, prevent, and eliminate malware on devices, such as laptops, desktops, smartphones, and tablets. Endpoint antivirus software can block viruses that are not seen and blocked by the perimeter firewall, which is a network security device that monitors and controls incoming and outgoing network traffic based on predefined security rules. Perimeter firewall can block some known viruses, but it may not be able to detect and stop new or unknown viruses that use advanced techniques to evade detection.Endpoint antivirus software can provide an additional layer of protection by scanning the files and processes on the devices and using various methods, such as signatures, heuristics, behavior analysis, and cloud-based analysis, to identify and remove malicious code123.Reference:
What Is Endpoint Antivirus? Key Features & Solutions Explained - Trellix
Microsoft Defender for Endpoint | Microsoft Security
Download ESET Endpoint Antivirus | ESET

QUESTION 63
A doctor receives an email about her upcoming holiday in France. When she clicks the URL website link in the email, the connection is blocked by her office firewall because it's a known malware website. Which type of attack includes a link to a malware website in an email?

A. whaling
B. phishing
C. pharming
D. spam

Correct Answer: B
Section:
Explanation:
Phishing is a type of attack that involves sending fraudulent emails that appear to be from legitimate sources, such as banks, companies, or individuals, in order to trick recipients into clicking on malicious links, opening malicious attachments, or providing sensitive information12.The link to a malware website in the email is an example of a malicious link, which may lead to the installation of malware, ransomware, spyware, or other malicious software on the user's device, or the redirection to a fake website that mimics a legitimate one, where the user may be asked to enter their credentials, personal information, or financial details34.Phishing emails often use social engineering techniques, such as creating a sense of urgency, curiosity, or fear, to persuade the user to click on the link or attachment, or to reply to the email5.Phishing emails may also spoof the sender's address, domain, or logo, to make them look more authentic and trustworthy6.
Whaling, pharming, and spam are not the correct answers for this question.Whaling is a specific type of phishing that targets high-profile individuals, such as executives, celebrities, or politicians, with the aim of stealing their confidential information or influencing their decisions7. Pharming is a type of attack that involves redirecting the user's web browser to a fake website, even if they enter the correct URL, by modifying the DNS server or the user's hosts file. Spam is the unsolicited or unwanted electronic messages, such as emails, texts, or instant messages, that are sent in bulk to a large number of recipients, usually for advertising, marketing, or scamming purposes.Reference:
What is phishing? | Malwarebytes
Phishing - Wikipedia
Don't Panic! Here's What To Do If You Clicked On A Phishing Link
How can Malware spread through Email and How to Protect
What is phishing? How this cyber attack works and how to prevent it ...
Identifying Illegitimate Email Links | Division of Information Technology
What is whaling? | NortonLifeLock
[What is pharming? | NortonLifeLock]
[What is spam? | NortonLifeLock]

QUESTION 64
With regard to cloud-native security in layers, what is the correct order of the four C's from the top (surface) layer to the bottom (base) layer?

A. container, code, cluster, cloud
B. code, container, cluster, cloud
C. code, container, cloud, cluster
D. container, code, cloud, cluster

Correct Answer: B
Section:
Explanation:
Cloud-native security is the integration of security strategies into applications and systems designed to be deployed and to run in cloud environments. It involves a layered approach that considers security at every level of the cloud-native application architecture.The four C's of cloud-native security are123:
Code: This layer refers to the application code and its dependencies. Security at this layer involves ensuring the code is free of vulnerabilities, using secure coding practices, and implementing encryption, authentication, and authorization mechanisms.
Container: This layer refers to the lightweight, isolated units that encapsulate the application and its dependencies. Security at this layer involves scanning and verifying the container images, enforcing policies and rules for container deployment and runtime, and isolating and protecting the containers from unauthorized access.
Cluster: This layer refers to the group of nodes that host the containers and provide orchestration and management capabilities. Security at this layer involves securing the communication between the nodes and the containers, monitoring and auditing the cluster activity, and applying security patches and updates to the cluster components.
Cloud: This layer refers to the underlying infrastructure and services that support the cloud-native applications. Security at this layer involves configuring and hardening the cloud resources, implementing identity and access management, and complying with the cloud provider's security standards and best practices.
The correct order of the four C's from the top (surface) layer to the bottom (base) layer iscode, container, cluster, cloud, as each layer depends on the security of the next outermost layer.Reference:What Is Cloud-Native Security? - Palo Alto Networks,What is Cloud-Native Security? An Introduction | Splunk,The 4C's of Cloud Native Kubernetes security - Medium

QUESTION 65
Which protocol is used by both internet service providers (ISPs) and network service providers (NSPs)?

A. Routing Information Protocol (RIP)
B. Border Gateway Protocol (BGP)
C. Open Shortest Path First (OSPF)
D. Split horizon

Correct Answer: B
Section:
Explanation:
Border Gateway Protocol (BGP) is a protocol that enables ISPs and NSPs to exchange routing information among themselves. BGP is used to determine the best path for sending data packets across the Internet. BGP is also known as the protocol of the Internet backbone, as it connects different autonomous systems (ASes) that form the Internet. BGP is not used by end systems or local networks, but only by routers that operate at the border of ASes. BGP is a complex and dynamic protocol that can handle changes in network topology, traffic load, and policy requirements.BGP is also a scalable protocol that can support the growth of the Internet1234Reference:
1: Internet service provider - Wikipedia
2: 1.8: Internet Backbones, NAPs, and ISPs - cs.huji.ac.il
3: Lecture Notes -- Unit 2 How does the Internet work?
4: Border Gateway Protocol - Wikipedia

QUESTION 66
Which attacker profile acts independently or as part of an unlawful organization?

A. cybercriminal
B. cyberterrorist
C. state-affiliated group
D. hacktivist

Correct Answer: A
Section:
Explanation:
Cybercriminals are attackers who act independently or as part of an unlawful organization, such as a crime syndicate or a hacker group. Their main motivation is to make money by exploiting vulnerabilities in systems, networks, or applications. They use various methods, such as ransomware, phishing, identity theft, fraud, or botnets, to steal data, extort victims, or disrupt services. Cybercriminals often target individuals, businesses, or institutions that have valuable or sensitive information, such as financial, personal, or health data. Cybercriminals are constantly evolving their techniques and tools to evade detection and countermeasures. They may also

collaborate with other cybercriminals or hire hackers to perform specific tasks.Reference:
Cybersecurity Threats: Cybercriminals
Attackers Profile

QUESTION 67
At which layer of the OSI model are routing protocols defined?

A. Network
B. Physical
C. Transport
D. Data Link

Correct Answer: A
Section:
Explanation:
Routing protocols are defined at the network layer (Layer 3) of the OSI model. The network layer is responsible for routing packets across different networks using logical addresses (IP addresses). Routing protocols are used to exchange routing information between routers and to determine the best path for data delivery. Some examples of routing protocols are BGP, OSPF, RIP, and EIGRP. Palo Alto Networks devices support advanced routing features using the Advanced Routing Engine1.
Reference: Advanced Routing - Palo Alto Networks | TechDocs, What Is Layer 7? - Palo Alto Networks, How to Configure Routing Information Protocol (RIP)

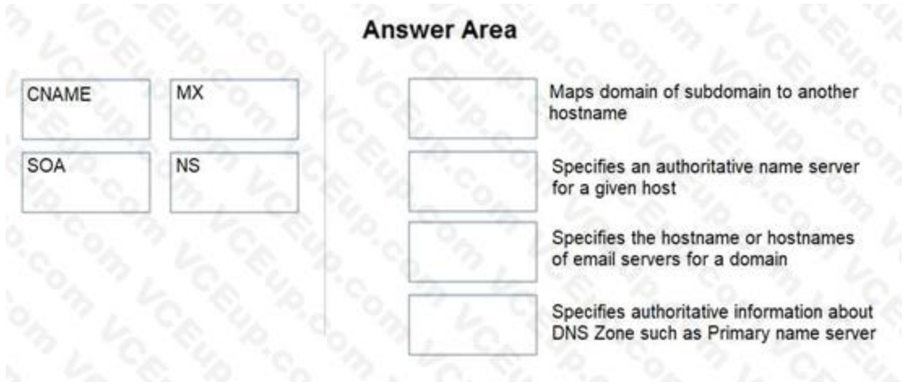
QUESTION 68
Organizations that transmit, process, or store payment-card information must comply with what standard?

A. HIPAA
B. CISA
C. GDPR
D. PCI DSS

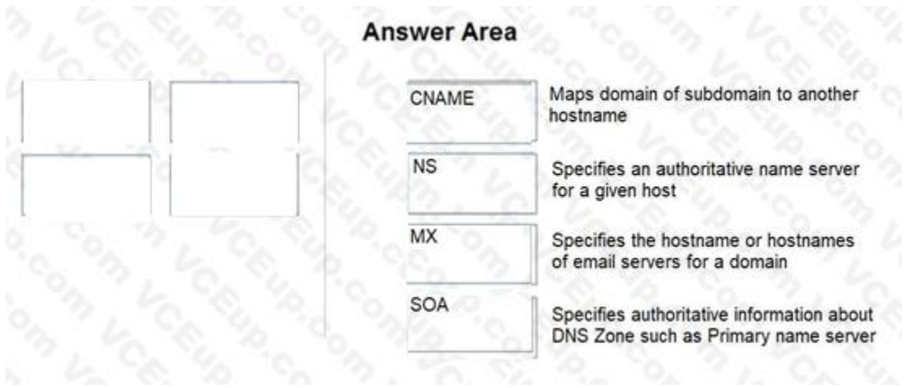
Correct Answer: D
Section:
Explanation:
PCI DSS stands for Payment Card Industry Data Security Standard, which is a set of requirements intended to ensure that all companies that process, store, or transmit credit card information maintain a secure environment1. The standard is administered by the Payment Card Industry Security Standards Council, and its use is mandated by the major card brands2. PCI DSS covers 12 requirements for compliance, organized into six control objectives, such as building and maintaining a secure network and systems, protecting cardholder data, and implementing strong access control measures3.
Reference: Payment Card Industry Security Standards, PCI Security Standards Council -- Protect Payment Data with Industry-driven Security Standards, Training, and Programs, What is PCI Compliance? 12 Requirements & More - Digital Guardian

QUESTION 69
DRAG DROP
Match the DNS record type to its function within DNS.

Select and Place:



Correct Answer:



Section:

Explanation:

The basic DNS record types are as follows:

• A (IPv4) or AAAA (IPv6) (Address): Maps a domain or subdomain to an IP address or multiple IP addresses • CNAME (Canonical Name): Maps a domain or subdomain to another hostname • MX (Mail Exchanger): Specifies the hostname or hostnames of email servers for a domain • PTR (Pointer): Points to a CNAME; commonly used for reverse DNS lookups that map an IP address to a host in a domain or subdomain • SOA (Start of Authority): Specifies authoritative information about a DNS zone such as primary name server, email address of the domain administrator, and domain serial number • NS (Name Server): The NS record specifies aan authoritative name server for a given host.

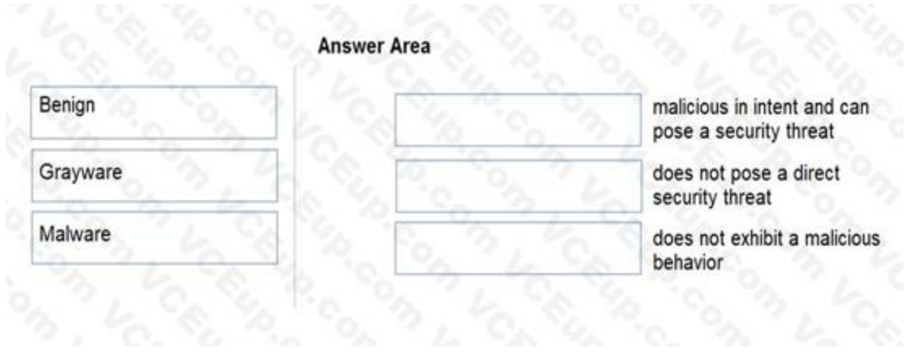
• TXT (Text): Stores text-based information

QUESTION 70

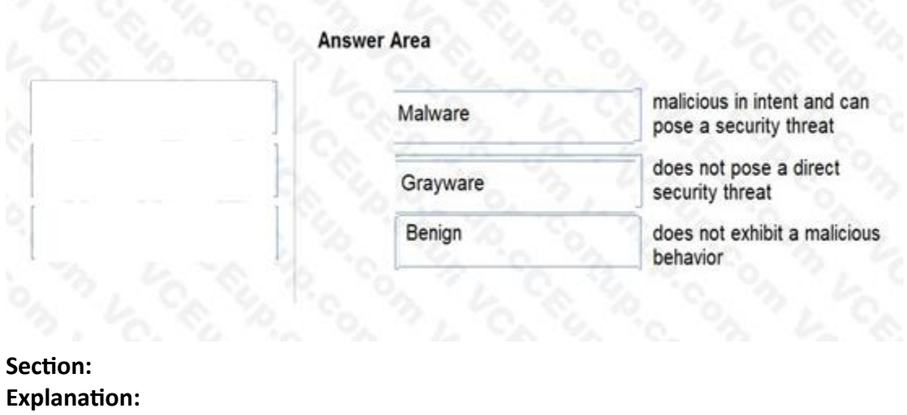
DRAG DROP

Match the Palo Alto Networks WildFire analysis verdict with its definition.

Select and Place:



Correct Answer:



Section:

Explanation:

• Benign: Safe and does not exhibit malicious behavior

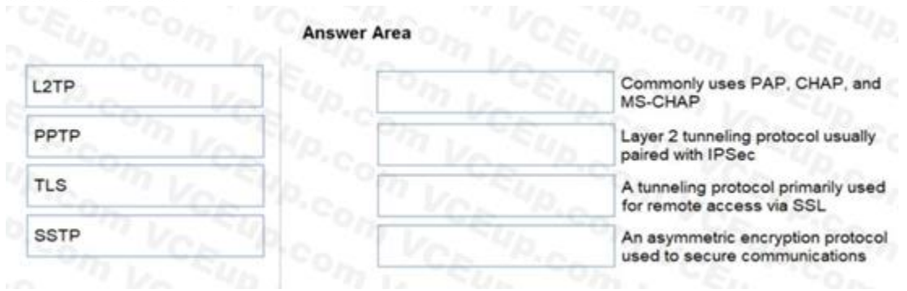
• Grayware: No security risk but might display obtrusive behavior (for example, adware, spyware, and browser helper objects) • Malware: Malicious in nature and intent and can pose a security threat (for example, viruses, worms, trojans, root kits, botnets, and remote-access toolkits) • Phishing: Malicious attempt to trick the recipient into revealing sensitive data

QUESTION 71

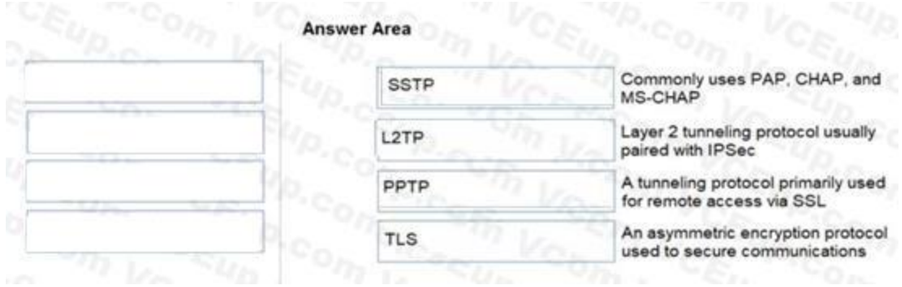
DRAG DROP

Match each tunneling protocol to its definition.

Select and Place:



Correct Answer:



Section:
Explanation:

QUESTION 72
Which two statements are true about servers in a demilitarized zone (DMZ)? (Choose two.)

A. They can be accessed by traffic from the internet.
B. They are located in the internal network.
C. They can expose servers in the internal network to attacks.
D. They are isolated from the internal network.

Correct Answer: A, D
Section:
Explanation:
A demilitarized zone (DMZ) is a portion of an enterprise network that sits behind a firewall but outside of or segmented from the internal network1.The DMZ typically hosts public services, such as web, mail, and domain servers, that can be accessed by traffic from the internet1.However, the DMZ is isolated from the internal network by another firewall or security gateway, which prevents unauthorized access to the private network2. Therefore, statements A and D are true about servers in a DMZ, while statements B and C are false.Reference:
What is a Demilitarized Zone (DMZ)? | F5
Demilitarized Zones (DMZs) - Secure Network Architecture - CompTIA ...

QUESTION 73
Which statement is true about advanced persistent threats?

A. They use script kiddies to carry out their attacks.
B. They have the skills and resources to launch additional attacks.
C. They lack the financial resources to fund their activities.
D. They typically attack only once.

Correct Answer: B
Section:
Explanation:
An advanced persistent threat (APT) is a sophisticated, sustained cyberattack in which an intruder establishes an undetected presence in a network in order to steal sensitive data over a prolonged period of time. APTs are usually carried out by well-funded, experienced teams of cybercriminals that target high-value organizations, such as governments, military, or corporations. APTs have the skills and resources to launch additional attacks, as they often use advanced techniques to evade detection, move laterally within the network, and establish multiple entry points and backdoors. APTs are not interested in causing immediate damage or disruption, but rather in achieving long-term goals, such as espionage, sabotage, or theft of intellectual property.Therefore, option B is the correct answer among the given choices123Reference:
1: Palo Alto Networks Certified Cybersecurity Entry-level Technician - Palo Alto Networks
2: 10 Palo Alto Networks PCCET Exam Practice Questions - CBT Nuggets
3: What Is an Advanced Persistent Threat (APT)? - Cisco
4: What is an Advanced Persistent Threat (APT)? - CrowdStrike

5: What Is an Advanced Persistent Threat (APT)? - Kaspersky

QUESTION 74
You have been invited to a public cloud design and architecture session to help deliver secure east west flows and secure Kubernetes workloads.
What deployment options do you have available? (Choose two.)

A. PA-Series
B. VM-Series
C. Panorama
D. CN-Series

Correct Answer: B, D
Section:
Explanation:
To deliver secure east-west flows and secure Kubernetes workloads in a public cloud environment, you have two deployment options available: VM-Series and CN-Series.
VM-Seriesis a virtualized form factor of the Palo Alto Networks next-generation firewall that can be deployed in public cloud platforms such as AWS, Azure, Google Cloud, and Oracle Cloud. VM-Series provides comprehensive network security and threat prevention capabilities for protecting your cloud workloads and applications from cyberattacks. VM-Series can also integrate with native cloud services and third-party tools to enable automation, orchestration, and visibility across your cloud environment.VM-Series supports various deployment scenarios, such as securing internet-facing applications, protecting hybrid connectivity, segmenting internal networks, and enabling secure DevOps12.
CN-Seriesis a containerized form factor of the Palo Alto Networks next-generation firewall that can be deployed in Kubernetes environments. CN-Series provides granular network security and threat prevention capabilities for protecting your Kubernetes pods and namespaces from cyberattacks. CN-Series can also integrate with Kubernetes network plugins and services to enable dynamic policy enforcement, service discovery, and visibility across your Kubernetes clusters.CN-Series supports various deployment scenarios, such as securing ingress and egress traffic, enforcing microsegmentation, and enabling secure DevSecOps34.
VM-Series in Public Cloud
VM-Series Deployment Guide
CN-Series in Kubernetes
CN-Series Deployment Guide

QUESTION 75
What is the definition of a zero-day threat?

A. The amount of time it takes to discover a vulnerability and release a security fix
B. The period between the discovery of a vulnerability and development and release of a patch
C. The day a software vendor becomes aware of an exploit and prevents any further hacking
D. A specific day during which zero threats occurred

Correct Answer: B
Section:
Explanation:
A zero-day threat is an attack that takes advantage of a security vulnerability that does not have a fix in place. It is referred to as a ''zero-day'' threat because once the flaw is eventually discovered, the developer or organization has ''zero days'' to then come up with a solution. A zero-day threat can compromise a system or network by exploiting the unknown vulnerability, and can cause data loss, unauthorized access, or other damages. Zero-day threats are difficult to detect and prevent, and require advanced security solutions and practices to mitigate them.Reference:
Palo Alto Networks Certified Cybersecurity Entry-level Technician (PCCET)
Zero-day (computing) - Wikipedia
What is a zero-day exploit? | Zero-day threats | Cloudflare

QUESTION 76
Which of the following is a CI/CD platform?

A. Github
B. Jira
C. Atom.io
D. Jenkins

Correct Answer: D
Section:
Explanation:
A CI/CD platform is a comprehensive set of tools that help developers, engineers, and DevOps practitioners package and deliver software to the end users. A CI/CD platform automates the process of software testing and deployment, and enables faster and more reliable software releases. Jenkins is a popular open source CI/CD platform that supports a wide range of plugins and integrations to build, test, and deploy various types of applications. Jenkins can be configured to run on different platforms, such as Linux, Windows, or Docker, and can work with various version control systems, such as Git, SVN, or Mercurial. Jenkins can also orchestrate complex workflows, such as parallel or sequential execution, conditional branching, or parameterized triggering, using a graphical interface or a declarative syntax. Jenkins can help developers and DevOps teams achieve continuous integration and continuous delivery/deployment, by providing features such as:
* Pipeline as code: Jenkins allows users to define and manage their pipelines as code, using a domain-specific language (DSL) called Jenkinsfile. This enables users to store, version, and reuse their pipeline configurations, and to apply best practices such as code review and testing.
* Distributed builds: Jenkins can scale up or down to meet the demand of concurrent builds, by distributing the workload across multiple agents or nodes. This improves the performance and efficiency of the CI/CD process, and allows users to leverage different environments and resources for different stages of the pipeline.
* Plugin ecosystem: Jenkins has a rich and active community that contributes to its plugin ecosystem, which extends its functionality and compatibility with various tools and technologies. Users can find and install plugins from the Jenkins Plugin Manager, or create their own custom plugins using Java or Groovy.
* Blue Ocean: Jenkins offers a modern and user-friendly web interface called Blue Ocean, which simplifies the creation and visualization of pipelines. Blue Ocean provides features such as real-time feedback, interactive editing, branch and pull request support, and integration with popular chat platforms, such as Slack or Microsoft Teams.
* Palo Alto Networks Certified Cybersecurity Entry-level Technician (PCCET) - Palo Alto Networks
* What Is a CI/CD Platform and Why Should I Care? | Harness
* What is CI/CD? - Red Hat
* Jenkins Documentation

QUESTION 77
What differentiates knowledge-based systems from behavior-based systems?

A. Behavior-based systems find the data that knowledge-based systems store.
B. Knowledge-based systems pull from a previously stored database that distinguishes ''bad''. C. Knowledge-based systems try to find new, distinct traits to find ''bad'' things.
C. Behavior-based systems pull from a previously stored database that distinguishes ''bad''.

Correct Answer: B
Section:
Explanation:
Knowledge-based systems and behavior-based systems are two types of artificial intelligence systems that can be used for security purposes. Knowledge-based systems use a predefined database of rules, facts, and patterns that distinguish ''bad'' or malicious activities from normal ones. They compare the incoming data with the stored knowledge and flag any anomalies or matches. Behavior-based systems, on the other hand, learn from the observed data and establish a baseline of normal behavior. They then monitor the data for any deviations or changes from the baseline and alert on any suspicious or abnormal activities.
Reference:
* Types of Knowledge-Based Systems - Springer
* Difference between Knowledge-based IDS and behavior-based IDS
* Behaviour-based Knowledge Systems: An Epigenetic Path from Behaviour to ...

QUESTION 78
How can local systems eliminate vulnerabilities?

A. Patch systems and software effectively and continuously.

B. Create preventative memory-corruption techniques.
C. Perform an attack on local systems.
D. Test and deploy patches on a focused set of systems.

Correct Answer: A
Section:
Explanation:
Local systems can eliminate vulnerabilities by patching systems and software effectively and continuously. Patching is the process of applying updates or fixes to software or hardware components that have known vulnerabilities or bugs. Patching can prevent attackers from exploiting these vulnerabilities and compromising the security or functionality of the systems. Patching should be done regularly and promptly, as new vulnerabilities are constantly discovered and exploited by cybercriminals. Patching should also be done effectively, meaning that the patches are tested and verified before deployment, and that they do not introduce new vulnerabilities or issues. Patching should also be done continuously, meaning that the systems are monitored for new vulnerabilities and patches are applied as soon as they are available. Continuous patching can reduce the window of opportunity for attackers to exploit unpatched vulnerabilities and cause damage or data breaches.
Reference:
* 1: What is Patch Management? | Palo Alto Networks
* 2: Patch Management Best Practices: How to Keep Your Systems Secure | Snyk
* 3: Vulnerability Remediation Process - 4 Steps to Remediation | Snyk

QUESTION 79
How does Cortex XSOAR Threat Intelligence Management (TIM) provide relevant threat data to analysts?

A. It creates an encrypted connection to the company's data center.
B. It performs SSL decryption to give visibility into user traffic.
C. II prevents sensitive data from leaving the network.
D. II automates the ingestion and aggregation of indicators.

Correct Answer: D
Section:
Explanation:
Cortex XSOAR Threat Intelligence Management (TIM) is a platform that enables security teams to manage the lifecycle of threat intelligence, from aggregation to action. One of the key features of Cortex XSOAR TIM is that it automates the ingestion and aggregation of indicators from various sources, such as threat feeds, open-source intelligence, internal data, and third-party integrations 1. Indicators are pieces of information that can be used to identify malicious activity, such as IP addresses, domains, URLs, hashes, etc. By automating the ingestion and aggregation of indicators, Cortex XSOAR TIM reduces the manual effort and time required to collect, validate, and prioritize threat data. It also enables analysts to have a unified view of the global threat landscape and the impact of threats on their network 1.
Reference: 1: Threat Intelligence Management - Palo Alto Networks 2

QUESTION 80
Which VM-Series virtual firewall cloud deployment use case reduces your environment's attack surface?

A. O Multicloud
B. O 5G -
C. Micro-segmentation
D. DevOps

Correct Answer: C
Section:
Explanation:
Micro-segmentation is a VM-Series virtual firewall cloud deployment use case that reduces your environment's attack surface. Micro-segmentation is the process of dividing a network into smaller segments, each with its own security policies and controls. This helps to isolate and protect workloads from lateral movement and unauthorized access, as well as to enforce granular trust zones and application dependencies. Micro-segmentation can be applied to virtualized data centers, private clouds, and public clouds, using software-defined solutions such as VMware NSX, Cisco ACI, and Azure Virtual WAN.

Reference: Micro-Segmentation - Palo Alto Networks, VM-Series Deployment Guide - Palo Alto Networks, VM-Series on VMware NSX - Palo Alto Networks, VM-Series on Cisco ACI - Palo Alto Networks, VM-Series on Azure Virtual WAN - Palo Alto Networks

QUESTION 81
Which two statements describe the Jasager attack? (Choose two.)

A. The victim must manually choose the attacker s access point
B. It actively responds to beacon reguests.
C. It tries to get victims to conned at random.
D. The attacker needs to be wilhin close proximity of the victim.

Correct Answer: B, D
Section:
Explanation:
A Jasager attack is a type of wireless man-in-the-middle attack that exploits the way mobile devices search for known wireless networks. A Jasager device will respond to any beacon request from a mobile device by saying ''Yes, I'm here'', pretending to be one of the preferred networks. This way, the Jasager device can trick the mobile device into connecting to it, without the user's knowledge or consent. The Jasager device can then intercept, modify, or redirect the traffic of the victim. For this attack to work, the attacker needs to be within close proximity of the victim, and the victim must have at least one known network in their preferred list. The victim does not need to manually choose the attacker's access point, nor does the attacker try to get victims to connect at random.
Reference: Wireless Man in the Middle - Palo Alto Networks, Man-in-the-middle attacks with malicious & rogue Wi-Fi access points - Privacy Guides

QUESTION 82
What is the ptrpose of automation in SOAR?

A. To provide consistency in response to security issues
B. To give only administrators the ability to view logs
C. To allow easy manual entry of changes to security templates
D. To complicate programming for system administration -

Correct Answer: A
Section:
Explanation:
Automation in SOAR (Security Orchestration, Automation, and Response) is the process of programming tasks, alerts, and responses to security incidents so that they can be executed without human intervention. Automation in SOAR helps security teams to handle the huge amount of information generated by various security tools, analyze it through machine learning processes, and take appropriate actions based on predefined rules and workflows. Automation in SOAR also reduces the manual effort and time required for security operations, improves the accuracy and efficiency of threat detection and response, and provides consistency in handling security issues across different environments and scenarios.
Reference: What is SOAR (security orchestration, automation and response)? | IBM, What Is SOAR? Technology and Solutions | Microsoft Security, Security orchestration - Wikipedia.

QUESTION 83
The seventy of an attack needs to be escalated.
What needs to be in place in order for the security operations team to properly inform various units within the enterprise of the issue?

A. Interface Agreement
B. FAO Incident Site ---
C. Corporate Executive Listserv
D. Security Breach Blog

Correct Answer: A
Section:

QUESTION 84
What type of address translation does a NAT perform?

A. Private to public
B. Logical to physical
C. Physical Io logical
D. Public to private

Correct Answer: A
Section:
Explanation:
NAT stands for Network Address Translation, which is a process that allows devices on a private network to communicate with devices on a public network, such as the Internet. NAT translates the private IP addresses of the devices on the private network to public IP addresses that can be routed on the public network. This way, multiple devices on the private network can share a single public IP address and access the Internet. NAT also provides security benefits, as it hides the internal network structure and IP addresses from the outside world.
Reference: Palo Alto Networks Certified Cybersecurity Entry-level Technician (PCCET), Fundamentals of Network Security, Network Address Translation (NAT)

QUESTION 85
Which action must Secunty Operations take when dealing with a known attack?

A. Document, monitor, and track the incident.
B. Limit the scope of who knows about the incident.
C. Increase the granularity of the application firewall.
D. Disclose details of lhe attack in accordance with regulatory standards.

Correct Answer: A
Section:
Explanation:
Security Operations (SecOps) is the process of coordinating and aligning security teams and IT teams to improve the security posture of an organization. SecOps involves implementing and maintaining security controls, technologies, policies, and procedures to protect the organization from cyber threats and incidents. When dealing with a known attack, SecOps must take the following action: document, monitor, and track the incident. This action is important because it helps SecOps to:
* Record the details of the attack, such as the source, target, impact, timeline, and response actions.
* Monitor the status and progress of the incident response and recovery efforts, as well as the ongoing threat activity and indicators of compromise.
* Track the performance and effectiveness of the security controls and technologies, as well as the lessons learned and improvement opportunities.
Reference:
* Palo Alto Networks Certified Cybersecurity Entry-level Technician (PCCET)
* 6 Incident Response Steps to Take After a Security Event - Exabeam
* Dealing with Cyber Attacks--Steps You Need to Know | NIST