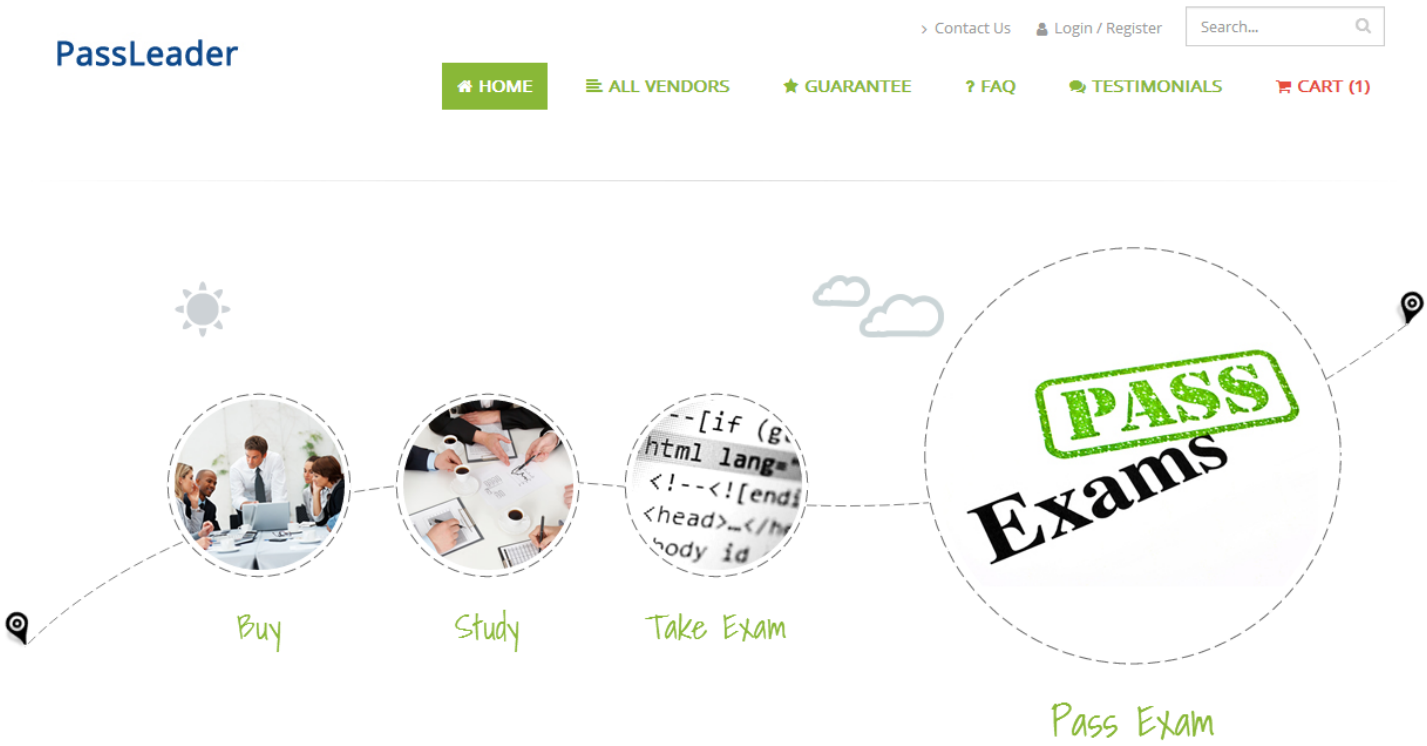
PassLeader



Try **PDF Demo** before you buy

We're not the only ones **happy** about PassLeader Practice Material ...

63159+ customers in 100+ countries use PassLeader Test Engine. Meet our customers.

VOREED GetCustom JET ORANGE iCompany Paradoxx iMessenger

http://www.passleader.top/

Latest Exam Guide & Learning Materials

Exam : **PCCP**

Title : Palo Alto Networks Certified Cybersecurity Practitioner

Vendor : Palo Alto Networks

Version : DEMO

NO.1 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 -
Answer: A
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. References: What is SOAR (security orchestration, automation and response)? | IBM, What Is SOAR? Technology and Solutions | Microsoft Security, Security orchestration - Wikipedia.

NO.2 Which action is unique to the security orchestration, automation, and response (SOAR) platforms?
A. Prioritizing alerts
B. Enhancing data collection
C. Using predefined workflows
D. Correlating incident data
Answer: C
Explanation:
SOAR platforms are unique in their ability to automate incident response through the use of predefined workflows. These workflows allow repetitive security tasks to be executed automatically, improving response speed and efficiency.

NO.3 What are two capabilities of identity threat detection and response (ITDR)? (Choose two.)
A. Matching risks to signatures
B. Securing individual devices
C. Analyzing access management logs
D. Scanning for excessive logins
Answer: C,D

NO.4 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

Answer: C
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.

NO.5 What are two limitations of signature-based anti-malware software? (Choose two.)
A. It is unable to detect polymorphic malware.
B. It requires samples lo be buffered
C. It uses a static file for comparing potential threats.
D. It only uses packet header information.
Answer: A C
Explanation:
Signature-based systems struggle with polymorphic or obfuscated malware, which changes its code to avoid detection. Signature-based detection relies on static databases of known threat signatures, limiting its ability to identify new or unknown threats.

NO.6 Which of the Cloud-Delivered Security Services (CDSS) will detect zero-day malware by using inline cloud machine learning (ML) and sandboxing?
A. DNS security
B. Advanced WildFire
C. IoT security
D. Advanced Threat Prevention
Answer: B
Explanation:
Advanced WildFire is a Cloud-Delivered Security Service (CDSS) that detects zero-day malware using inline cloud machine learning (ML) and sandboxing techniques. It analyzes unknown files in real-time to identify and block new threats before they can cause harm.

NO.7 In an IDS/IPS, which type of alarm occurs when legitimate traffic is improperly identified as malicious traffic?
A. False-positive
B. True-negative
C. False-negative
D. True-positive
Answer: A
Explanation:
In anti-malware, a false positive incorrectly identifies a legitimate file or application as malware. A false negative incorrectly identifies malware as a legitimate file or application. In intrusion detection, a false positive incorrectly identifies legitimate traffic as a threat, and a false negative incorrectly identifies a threat as legitimate traffic.

NO.8 When signature-based antivirus software detects malware, what three things does it do to

provide protection?
(Choose three.)
A. decrypt the infected file using base64
B. alert system administrators
C. quarantine the infected file
D. delete the infected file
E. remove the infected file's extension
Answer: B C D
Explanation:
Signature-based antivirus software is a type of security software that uses signatures to identify malware.
Signatures are bits of code that are unique to a specific piece of malware. When signature-based antivirus software detects a piece of malware, it compares the signature to its database of known signatures12. If a match is found, the software can do three things to provide protection:
* Alert system administrators: The software can notify the system administrators or the users about the malware detection, and provide information such as the name, type, location, and severity of the malware. This can help the administrators or the users to take appropriate actions to prevent further damage or infection3.
* Quarantine the infected file: The software can isolate the infected file from the rest of the system, and prevent it from accessing or modifying any other files or processes. This can help to contain the malware and limit its impact on the system4.
* Delete the infected file: The software can remove the infected file from the system, and prevent it from running or spreading. This can help to eliminate the malware and restore the system to a clean state4.
What is a signature-based antivirus? - Info Exchange
What is a Signature and How Can I detect it? - Sophos
How Does Heuristic Analysis Antivirus Software Work?
What Is Signature-based Malware Detection? | RiskXchange

NO.9 Which two statements apply to SaaS financial botnets? (Choose two.)
A. They are larger than spamming or DDoS botnets.
B. They are sold as kits that allow attackers to license the code.
C. They are a defense against spam attacks.
D. They are used by attackers to build their own botnets.
Answer: B D
Explanation:
SaaS financial botnets are often sold as kits, enabling attackers to license and reuse the malicious code easily.
These kits allow attackers to build and operate their own botnets, often targeting financial data or systems.
Financial botnets are typically smaller but more targeted than spamming or DDoS botnets. Botnets are not a defense mechanism, but rather a threat.

NO.10 How does adopting a serverless model impact application development?
A. costs more to develop application code because it uses more compute resources

B. slows down the deployment of application code, but it improves the quality of code development
C. reduces the operational overhead necessary to deploy application code
D. prevents developers from focusing on just the application code because you need to provision the underlying infrastructure to run the code
Answer: C
Explanation:
List three advantages of serverless computing over
CaaS: - Reduce costs - Increase agility - Reduce operational overhead

NO.11 At which layer of the OSI model are routing protocols defined?
A. Network
B. Physical
C. Transport
D. Data Link
Answer: A
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.
References: Advanced Routing - Palo Alto Networks | TechDocs, What Is Layer 7? - Palo Alto Networks , How to Configure Routing Information Protocol (RIP)

NO.12 Which Palo Alto Networks tool is used to prevent endpoint systems from running malware executables such as viruses, trojans, and rootkits?
A. Expedition
B. Cortex XDR
C. AutoFocus
D. App-ID
Answer: B
Explanation:
Cortex XDR is a cloud-based, advanced endpoint protection solution that combines multiple methods of prevention against known and unknown malware, ransomware, and exploits. Cortex XDR uses behavioral threat protection, exploit prevention, and local analysis to stop the execution of malicious programs before an endpoint can be compromised. Cortex XDR also enables remediation on the endpoint following an alert or investigation, giving administrators the option to isolate, terminate, block, or quarantine malicious files or processes. Cortex XDR is part of the Cortex platform, which provides unified visibility and detection across the network, endpoint, and cloud. References:
* Cortex XDR - Palo Alto Networks
* Endpoint Protection - Palo Alto Networks
* Endpoint Security - Palo Alto Networks
* Preventing Malware and Ransomware With Traps - Palo Alto Networks

NO.13 Anthem server breaches disclosed Personally Identifiable Information (PII) from a number of

its servers. The infiltration by hackers was attributed to which type of vulnerability?

A. an intranet-accessed contractor's system that was compromised

B. exploitation of an unpatched security vulnerability

C. access by using a third-party vendor's password

D. a phishing scheme that captured a database administrator's password

Answer: D

Explanation:

The Anthem data breach of 2015 was caused by a phishing scheme that captured a database administrator's password. According to the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR), hackers sent phishing emails to an Anthem subsidiary. At least one employee responded. Attackers were able to plant malware on the company's system and gain remote access to confidential information1. The breach exposed the electronic protected health information of almost 79 million people, including names, Social Security numbers, medical identification numbers, addresses, dates of birth, email addresses, and employment information2.

References:

* Anthem Pays OCR $16 Million in Record HIPAA Settlement Following Largest U.S. Health Data Breach
* How Anthem Data Breach Exposed Personnel Records - IDStrong

NO.14 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

Answer: B D

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-Series is 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-Series is 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

NO.15 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

Answer: C

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.
References: 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

NO.16 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.

Answer: A

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. References:
*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

NO.17 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.

Answer: D

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. References: 1: Threat Intelligence Management - Palo Alto Networks 2

NO.18 Which key component is used to configure a static route?

A. router ID

B. enable setting

C. routing protocol

D. next hop IP address

Answer: D

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. References: Configure a Static Route in Virtual Routers, Palo Alto Networks Certified Cybersecurity Entry-level Technician (PCCET), FREE Cybersecurity Education Courses

NO.19 What is used to orchestrate, coordinate, and control clusters of containers?

A. Kubernetes

B. Prisma Saas

C. Docker

D. CN-Series

Answer: A

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/

NO.20 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)
Answer: D
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.

NO.21 What is an event-driven snippet of code that runs on managed infrastructure?
A. API
B. Serverless function
C. Hypervisor
D. Docker container
Answer: B
Explanation:
A serverless function is an event-driven snippet of code that runs on managed infrastructure, typically as part of a Function as a Service (FaaS) model. It is executed in response to events such as HTTP requests or database changes, and the cloud provider handles the underlying infrastructure.

NO.22 Which option would be an example of PII that you need to prevent from leaving your enterprise network?
A. Credit card number
B. Trade secret
C. National security information
D. A symmetric encryption key
Answer: A
Explanation:
A credit card number is an example of PII that you need to prevent from leaving your enterprise network. PII, or personally identifiable information, is any information that can be used to identify an individual, either alone or in combination with other data. PII can be sensitive or non-sensitive, depending on the level of protection required and the potential harm if exposed. Sensitive PII includes data that can directly identify an individual and cause significant harm if leaked or stolen, such as financial information, medical records, or government-issued ID numbers. Non-sensitive PII includes data that is easily accessible from public sources and does not pose a high risk of identity theft, such as zip code, race, or gender. A credit card number is a sensitive PII because it can be used to access the cardholder's account, make fraudulent transactions, or steal their identity. Therefore, it is important to prevent credit card numbers from leaving the enterprise network, where they could

be intercepted by hackers, malicious insiders, or third parties. To protect credit card numbers and other sensitive PII, enterprises should implement data security measures such as encryption, tokenization, masking, access control, auditing, and monitoring. Additionally, enterprises should comply with data privacy laws and standards that regulate the collection, use, and protection of PII, such as the Payment Card Industry Data Security Standard (PCI DSS), the General Data Protection Regulation (GDPR), or the California Consumer Privacy Act (CCPA). References:
* What is PII? Examples, laws, and standards | CSO Online
* What is Personally Identifiable Information (PII)? | IBM
* What Is Personally Identifiable Information (PII)? Types and Examples
* What is PII (personally identifiable information)? - Cloudflare
* What is Personally Identifiable Information (PII)? - Data Privacy Manager

NO.23 Which option is an example of a North-South traffic flow?
A. Lateral movement within a cloud or data center
B. An internal three-tier application
C. Client-server interactions that cross the edge perimeter
D. Traffic between an internal server and internal user
Answer: C
Explanation:
North-south refers to data packets that move in and out of the virtualized environment from the host network or a corresponding traditional data center. North-south traffic is secured by one or more physical form factor perimeter edge firewalls.