PassQueen
a.k.a dumpsqueen.com

Palo Alto Certified Cybersecurity Practitioner ()

Palo Alto Networks PCCP

Version Demo

Total Demo Questions: 9

Total Premium Questions: 92

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Cybersecurity Fundamentals	28
Topic 2, Security Infrastructure and Security Operations	4
Topic 3, Network Security	14
Topic 4, Cloud Security	20
Topic 5, Security Operations	26
Total	92

QUESTION NO: 1

Which Palo Alto Networks solution has replaced legacy IPS solutions?

A. Advanced DNS Security

B. Advanced WildFire

C. Advanced Threat Prevention

D. Advanced URL Filtering

ANSWER: C

Explanation:

Advanced Threat Prevention is correct because it is Palo Alto Networks' modern evolution of traditional intrusion prevention capabilities. Rather than relying solely on conventional signatures, it combines inline prevention with cloud-delivered threat intelligence, advanced inspection, and machine-learning-based protections. This approach is designed to identify and block exploits, command-and-control activity, malware-related traffic, and evasive threats as sessions traverse the next-generation firewall. Advanced Threat Prevention delivers prevention in real time, helping organizations protect applications and users against both known threats and emerging attack techniques while reducing exposure to threats that can bypass legacy IPS controls. Palo Alto Networks positions this capability as part of its network security platform's threat-prevention services, extending the inspection and blocking capabilities expected of an IPS with protections intended for modern, sophisticated attacks. See Palo Alto Networks' Advanced Threat Prevention overview and its Advanced Threat Prevention documentation for product details and deployment guidance.

QUESTION NO: 2

Which tool automates remediation of a confirmed cybersecurity breach?

A. SIEM

B. EDR

C. SOAR

D. ISIM

ANSWER: C

Explanation:

SOAR is designed to orchestrate and automate incident-response actions after security teams confirm an incident or breach. A SOAR platform uses predefined playbooks to coordinate tasks across security tools and infrastructure, such as enriching alerts with threat intelligence, opening and updating cases, notifying stakeholders, disabling compromised accounts, blocking malicious indicators, or isolating affected endpoints. By executing repeatable workflows automatically or with analyst approval at defined checkpoints, SOAR reduces manual effort, speeds containment and remediation, and helps teams apply response procedures consistently. Palo Alto Networks Cortex XSOAR is a SOAR platform that centralizes incident management and automates security operations through playbooks and integrations. Palo Alto Networks describes Cortex XSOAR as providing security orchestration, case management, real-time collaboration, and threat-intelligence management to improve and automate incident response. See the Palo Alto Networks Cortex XSOAR overview and the Cortex XSOAR playbook automation documentation.

QUESTION NO: 3

What are two advantages of security orchestration, automation, and response (SOAR)? (Choose two.)

A. Completely isolated system

B. Scripting of manual tasks

C. Consistent incident handling

D. Long-term retention of logs

ANSWER: B C

Explanation:

Scripting of manual tasks is an advantage of SOAR because SOAR platforms use integrations, workflows, playbooks, and automation scripts to perform repetitive analyst activities. For example, a playbook can enrich an alert with threat-intelligence data, collect contextual information from security tools, open or update a case, and initiate approved containment actions. Automating these repeatable steps reduces the time analysts spend on routine work and enables faster, more scalable incident response.

Consistent incident handling is also an advantage because playbooks document and execute standardized response procedures. Each relevant alert or incident can follow the same defined investigation, escalation, approval, and remediation workflow. This supports reliable outcomes across shifts and analysts, reduces the likelihood that important response steps are missed, and helps teams demonstrate that incident processes are being applied consistently. Palo Alto Networks describes Cortex XSOAR as a platform for orchestrating security tools and automating incident-response processes through playbooks. See the Cortex XSOAR overview and the Cortex XSOAR documentation.

QUESTION NO: 4

A cloud team deploys infrastructure by using templates in a CI/CD pipeline. The security team wants to prevent publicly exposed storage and overly permissive identity policies before the resources are created.

Which two practices support this goal? (Choose two.)

A. Scanning infrastructure-as-code templates

B. Applying policy checks in the CI/CD pipeline

C. Isolating endpoints after suspicious execution

D. Analyzing packets with a network sandbox

ANSWER: A B

Explanation:

Scanning infrastructure-as-code templates identifies insecure cloud configurations before deployment. **Applying policy checks in the CI/CD pipeline** can prevent builds or deployments that violate the organization's security requirements. Runtime workload protection and post-deployment monitoring remain important controls, but they identify or mitigate risk after the insecure resource could already exist.

QUESTION NO: 5

Which service is encompassed by serverless architecture?

A. Infrastructure as a Service (IaaS)

B. Function as a Service (FaaS)

C. Security as a Service (SaaS)

D. Authentication as a Service

ANSWER: B

Explanation:

Function as a Service (FaaS) is encompassed by serverless architecture. With FaaS, developers package application logic as discrete functions and deploy them to a cloud platform without provisioning, administering, or maintaining the servers that execute the code. The cloud provider manages the underlying compute infrastructure, including capacity provisioning, availability, patching, and automatic scaling. Functions are commonly invoked in response to events, such as an HTTP request, a file upload, a database change, or a message arriving in a queue. This model lets teams focus on writing business logic while consumption is generally based on the time and resources used during each function invocation. Serverless can also include managed backend services, but FaaS is the core compute service model most directly associated with serverless architecture. Palo Alto Networks discusses how serverless environments use functions and event-driven execution, creating a distinct security model that requires visibility into function code, permissions, dependencies, and runtime behavior. See Palo Alto Networks' serverless security overview and AWS's AWS Lambda documentation for further details.

QUESTION NO: 6

Which two statements apply to SaaS financial botnets? (Choose two.)

A. They are largerthan spammingor 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 commonly associated with a criminal service model in which malware or botnet capabilities are packaged for purchase, rental, or licensing. Therefore, "They are sold as kits that allow attackers to license the code." accurately describes how financial-malware operators can make tooling available to other criminals without those customers needing to develop the full malware platform themselves. Such kits may include the malicious code, configuration resources, administration panels, and operational support needed to conduct credential theft, banking fraud, or other financially motivated activity.

"They are used by attackers to build their own botnets." is also correct because purchasers or subscribers can deploy the provided malware to compromise endpoints and enroll them into an attacker-controlled network. This model lowers the technical and financial barrier to operating a targeted botnet while allowing the service provider and the customer to play distinct roles in the attack lifecycle. Palo Alto Networks describes botnets as networks of compromised devices controlled by an attacker and notes their use in malicious activities. Its explanation of malware-as-a-service also outlines the broader commercialization of malicious capabilities that supports this type of ecosystem. See Palo Alto Networks: What Is a Botnet? and Palo Alto Networks: What Is Malware as a Service?.

QUESTION NO: 7

What are two examples of an attacker using social engineering? (Choose two.)

A. Convincing an employee that they are also an employee

B. Leveraging open-source intelligence to gather information about a high-level executive

C. Acting as a company representative and asking for personal information not relevant to the reason for their call

D. Compromising a website and configuring it to automatically install malicious files onto systems that visit the page

ANSWER: A C

Explanation:

“Convincing an employee that they are also an employee” describes an attacker establishing a false shared identity or trusted relationship with a target. By posing as an insider, the attacker exploits the employee’s trust and familiarity with coworkers to make a request for information, credentials, access, or another action seem legitimate. This form of deception is central to social engineering because the attacker targets human judgment rather than attempting to exploit a technical vulnerability directly.

“Acting as a company representative and asking for personal information not relevant to the reason for their call” is also social engineering. The attacker impersonates an authoritative or trusted organization and uses a plausible pretext to persuade the victim to disclose sensitive information. This tactic can occur by phone, email, text message, or other communication channels and commonly supports phishing, vishing, identity theft, and credential compromise. Palo Alto Networks describes social engineering as manipulating people into providing confidential information or performing actions that enable an attack. Effective defenses include verifying identities through independent channels, limiting disclosure of sensitive data, and reporting suspicious requests. See Palo Alto Networks’ social engineering overview and phishing overview.

QUESTION NO: 8

Which component of the AAA framework verifies user identities so they may access the network?

A. Allowance

B. Authorization

C. Accounting

D. Authentication

ANSWER: D

Explanation:

Authentication is the AAA component that verifies a user’s identity before granting access to a network or protected resource. It answers the question, “Who is this user?” by validating supplied credentials, such as a username and password, certificate, one-time passcode, biometric factor, or another approved identity factor. In a Palo Alto Networks environment, authentication can be performed against local firewall accounts or external identity services such as LDAP, RADIUS, TACACS+, Kerberos, or SAML-based identity providers. After the identity is successfully verified, the authenticated username can be used by security policy and other controls to apply appropriate access decisions and provide visibility into user activity. Palo Alto Networks describes authentication profiles as a way to define the authentication service and login criteria used to verify users, including for GlobalProtect and captive portal workflows. This identity-verification role is the foundational first stage of the AAA model. For implementation details, see the Palo Alto Networks Authentication Profiles documentation and the PAN-OS Authentication documentation.

QUESTION NO: 9

Which capability does Cloud Security Posture Management (CSPM) provide for threat detection within Prisma Cloud?

A. Real-time protection from threats

B. Alerts for new code introduction

C. Integration with threat feeds

D. Continuous monitoring of resources

ANSWER: D

Explanation:

Continuous monitoring of resources is correct because Prisma Cloud CSPM continuously assesses cloud environments to maintain visibility into the security posture of cloud assets and configurations. It monitors cloud resources across connected

accounts and services, evaluates them against security policies and compliance standards, and identifies conditions that introduce risk, such as insecure configurations, excessive permissions, or exposed services. This ongoing assessment is essential for threat detection because cloud environments are dynamic: resources, identities, network settings, and configurations can change frequently. By detecting and alerting on posture changes and policy violations, CSPM helps security teams investigate and remediate risks before they can be exploited. Prisma Cloud's capabilities are designed to provide this continuous visibility across multicloud environments, rather than relying only on periodic, manual reviews. Palo Alto Networks describes Prisma Cloud as delivering continuous security and compliance monitoring for cloud environments, including detection of configuration risks and policy violations. For additional details, see the Prisma Cloud documentation and Palo Alto Networks' Cloud Security Posture Management overview.