Number: 156-560
Passing Score: 800
Time Limit: 120
File Version: 34.0

Exam Code: 156-560
Exam Name: Check Point Certified Cloud Specialist

Exam A

QUESTION 1
How does the Cloud Security Posture Management (CSPM) service deliver intelligence threat feeds, enforce compliance policies, and apply security enhancement to the environment.

A. The Cloud Security Posture Management (CSPM) does this by using the SOAP protocol and XML
B. The Cloud Security Posture Management (CSPM) does this by .usingSSH and microagents
C. The Cloud Security Posture Management (CSPM) does this by using REST APIs
D. The Cloud Security Posture Management (CSPM) does this by using SIC connections on the cloud

Correct Answer: D
Section:

QUESTION 2
Cloud Security Posture Management uses CloudBots to assist with_____.

A. cloud account configurations and data flows
B. securing IAM account credentials.
C. identifying where the organization's security posture need:
D. automatic compliance remediation

Correct Answer: D
Section:

QUESTION 3
Which CloudGuard security platform enables organizations to view and access their security posture, find cloud misconfigurations, and enforce best practices?

A. CloudGuard laaS Private Cloud Solution
B. CloudGuard SaaS
C. CloudGuard Security Posture Management
D. CloudGuard laaS Public Cloud Solution

Correct Answer: C
Section:

QUESTION 4
Which solution delivers a software platform for public cloud security and compliance orchestration?

A. CloudGuard Network Public
B. CloudGuard Network Private
C. CloudGuard SaaS
D. Cloud Security Posture Management

Correct Answer: D

Section:

QUESTION 5
Which language can be used by users of Cloud Security Posture Management to create custom Security Policies?

A. eXtensible Markup Language (XML)
B. Posture Management Language (PML)
C. Governance Specific Language (GSL)
D. JavaScript Object Notation (JSON)

Correct Answer: C
Section:

QUESTION 6
When using Data Center Objects in a policy and the objects are not updating, what are two steps we can check?

A. 1. Verify process is running with 'cloudguard on' and 2. restart the api process with 'api restart'
B. 1. Verify process is running with 'cloudguard on' and 2. 'test communication' button the Data Center Server object
C. 1. Reboot the Security Management Server and 2. restart the cloudguard process with 'cloudguard on'
D. 1. Reboot the Security Management Server and 2. restart the api process with 'api restart'

Correct Answer: B
Section:

QUESTION 7
When Cloud Security Posture Management discovers non- compliant cloud resources, CloudBot applications perform automated remediation's to correct any violations. How true is this statement?

A. This is true, however it requires Full Protection access to the Cloud Account to perform automated remediation
B. This is not true, Cloud Security Posture Management (CSPIU) can only report non-compliance and cannot remediate by itself
C. This is partially true, however the automated remediation is not done by CloudBot applications but it is done by the Security Management Server
D. This is not true because CloudBot applications are used to provide chat service to respond to noncompliance alerts

Correct Answer: A
Section:

QUESTION 8
Once the Deployment finishes, Cloud Security Posture Management applies default network security posture that does what?

A. Minimizes the risk of external threats by blocking access to high risk sites and external users
B. Minimizes the risk of external threats by blocking accessed to the internet
C. Minimizes the risk of external threats by blocking access to all internal resources
D. Minimizes the risks of external threats by blocking access to services and ports

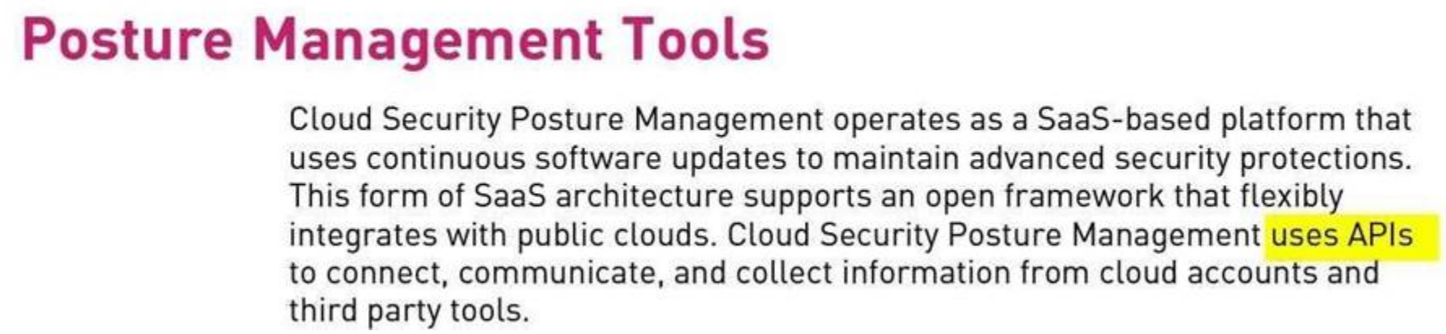
Correct Answer: D
Section:

QUESTION 9

Introduction to Cloud Security Posture Management uses which of the following to connect, communicate, and collect information from cloud accounts and third party tools?

A. SmartConsole
B. HTML
C. CLI
D. APIs

Correct Answer: D
Section:
Explanation:



QUESTION 10
Cloud Security Posture Management (CSPM) operates as which type of service based platform?

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

Correct Answer: D
Section:

QUESTION 11
The framework for cloud security consists of five basic components, or pillars Making small, reversible changes is a design principle of which of these five pillars

A. Reliability
B. Performance Efficiency
C. Cost Optimization
D. Operational Excellence

Correct Answer: D
Section:
Explanation:
There are five design principles for operational excellence in the cloud:
Perform operations as code
Make frequent, small, reversible changes
Refine operations procedures frequently

Anticipate failure
Learn from all operational failures

QUESTION 12
The Administrators ability to protect data, systems, and assets While taking advantage of cloud technologies is commonly called

A. Cost Optimization
B. Security
C. Operational Excellence
D. Performance Efficiency

Correct Answer: B
Section:
Explanation:
The security pillar encompasses the ability to protect data, systems, and assets to take advantage of cloud technologies to improve your security.

QUESTION 13
What is Operational Excellence?

A. The ability of a Workload to function correctly and consistently in all expected
B. In terms of the cloud, security is about architecting every workload to prevent
C. The ability to use cloud resources efficiently for meeting system requirements, and maintaining that efficiency as demand changes and technologies evolve
D. The ability to support development and run workloads effectively

Correct Answer: D
Section:
Explanation:
The Operational Excellence pillar includes the ability to support development and run workloads effectively, gain insight into their operation, and continuously improve supporting processes and procedures to delivery business value.

QUESTION 14
What is Reliability according to the Five Pillars?

A. The ability to use cloud resources efficiently for meeting system requirements, and maintaining that efficiency as demand changes and technologies evolve
B. The ability of a Workload to function correctly and consistently in all expected.
C. The ability to support development and run workload effectively
D. In terms of the cloud, security is about architecting every workload to prevent.

Correct Answer: B
Section:
Explanation:
The Reliability pillar encompasses the ability of a workload to perform its intended function correctly and consistently when it’s expected to. This includes the ability to operate and test the workload through its total lifecycle. You can find prescriptive guidance on implementation in the Reliability Pillar whitepaper.

QUESTION 15
Which is not a Pillar of the Framework for the Cloud?

A. Performance Efficiency

B. Cost Optimization
C. Scalability
D. Reliability

Correct Answer: C
Section:
Explanation:
https://emergencetek.com/aws-five-pillars-of-a-well-architectedframework/#:~:text=AWS%20and%20their%20partners%20use,performance%20efficiency%2C%20and%20cost%20optimization.

QUESTION 16
What is Performance Efficiency?

A. The ability to use cloud resources efficiently for meeting system requirements, and maintaining that efficiency as demand changes and technologies evolve
B. The ability to support development and run workloads effectively
C. In terms of the cloud, security is about architecting every workload to prevent
D. The ability of a Workload to function correctly and consistently in all expected

Correct Answer: A
Section:
Explanation:
The Performance Efficiency pillar includes the ability to use computing resources efficiently to meet system requirements, and to maintain that efficiency as demand changes and technologies evolve. You can find prescriptive guidance on implementation in the Performance Efficiency Pillar whitepaper.

QUESTION 17
What is Cloud Security according to the Five Pillars?

A. The ability to support development and run workloads effectively
B. The ability of a Workload to function correctly and consistently in all expected
C. The ability to use cloud resources efficiently for meeting system requirements, and maintaining that efficiency as demands changes and technologies evolve
D. In terms of tie cloud, security is about architecting every workload to prevent

Correct Answer: D
Section:

QUESTION 18
In a CloudGuard deployment, what does the acronym IAM stand for?

A. Information and Adaptability Measures
B. IP Address Management
C. Identity and Access Management
D. Instant Access Management

Correct Answer: C
Section:

QUESTION 19
Which cloud components specify the Workloads associated with traffic and tell load balancers which Workloads are members of the same group?

A. Target Groups
B. Listening Rules
C. Dynamic assignment
D. Health Checks

Correct Answer: A
Section:

QUESTION 20
Which pricing model gives administrators the ability to deploy devices as needed without the need to purchase blocks of vCore licenses?

A. Pay As You Go
B. Bring Your Own License
C. Central licensing
D. Local licensing

Correct Answer: A
Section:

QUESTION 21
The integration of cloud resources into the Security Policy requires establishing a secure connection between_____

A. The SDDC, CloudGuard Security Gateways, and the Security Management Server
B. The SDDC and CloudGuard Security Gateways.
C. The SDDC and the Security Management Server
D. CloudGuard Security Gateways and the Security Management Server

Correct Answer: A
Section:

QUESTION 22
What is vertical scaling?

A. Tunes the environment up and down according to the resource capacity needs
B. Tunes the environment by automatically adding or removing resource to the SDN
C. Tunes the environment by manually adding or removing resource to an SDDC
D. Scaling method that does not require a system shutdown to add or remove resources.

Correct Answer: A
Section:

QUESTION 23
Which software blade provides forensic analysis tools?

A. Logging Blade
B. Identity Awareness Blade

C. Monitoring Blade
D. SmartEvent Blade

Correct Answer: B
Section:

QUESTION 24
Adaptive Security Policies allow the deployment of new cloud based resources without

A. Changing the cloud environment
B. Paying for new resources
C. Installing New Policies
D. Installing New Applications

Correct Answer: C
Section:

QUESTION 25
Adding new Security Gateways as system load increases is an example of _____

A. Vertical Scaling
B. Network Scaling
C. Horizontal Scaling
D. System Scaling

Correct Answer: C
Section:

QUESTION 26
Which autoscaling method requires the VM to temporarily shut down while it processes system modification?

A. Both Vertical and Horizontal Scaling
B. Vertical Scaling
C. Horizontal Scaling
D. Neither autoscaling method requires the VM to}

Correct Answer: B
Section:

QUESTION 27
Which function do Load Balancers perform?

A. Trigger capacity on security gateways
B. To secure balance between private and public cloud
C. Direct internet traffic to spoke networks
D. Restrict traffic loads between servers

Correct Answer: B
Section:

QUESTION 28
A utility that allows integration between SMS, the CloudGuard Network Solution, and CSPs, allowing the SMS to monitor and control scaling solutions in their associated cloud environments is called

A. CloudGuard Management Extension (CME)
B. CloudGuard Controller and Enforcer (CCE)
C. CloudGuard Scanner and Enforcer (CSE)
D. CloudGuard Controller (CC)

Correct Answer: A
Section:

QUESTION 29
CloudGuard uses several management tools to create and manage Security Policies. Which is NOT one of those tools?

A. Gaia Portal
B. CloudGuard Controller
C. SmartConsole
D. CLI

Correct Answer: D
Section:

QUESTION 30
Which Security Gateway function inspects cloud applications and workload resources for malicious activity?

A. Application Control
B. Threat Prevention
C. Identity Awareness
D. Access Control

Correct Answer: B
Section:

QUESTION 31
Which of these Cloud Platforms support User Defined Route (UDR) to force traffic destined for spoke networks to go through a network virtual appliance

A. Amazon AWS
B. Google Cloud Platform
C. Amazon AWS and Google Cloud Platform
D. Microsoft Azure

Correct Answer: D
Section:

QUESTION 32
The best practice for CloudGuard Network deployments utilizes the Hub and Spokes Model. Which of these statements is the most correct for this model.

A. All the security components including SMS, Northbound and Southbound Security Gateways and East-West VPN Gateways will be deployed in one Hub.
B. A Spoke can ONLY consist of a single virtual machine in a dedicated subnet shared between the VM and the Hub.
C. All traffic that enters and exits each spoke must travel through a hub
D. The Hub and Spoke model is applicable ONLY to multi-cloud environments. The Hub includes all the Security Gateways in all cloud environment. Each Spoke includes all resources of a Data Center in a single Cloud Environment.

Correct Answer: A
Section:

QUESTION 33
Check Point's Public Cloud model is described as the following

A. A Security Matrix Model
B. A Hub and Spoke Model
C. An Advanced Threat Tunnel Model
D. A Borderless Model

Correct Answer: B
Section:

QUESTION 34
Which is not a deployment method for CloudGuard solutions using

A. Terraform
B. Shell
C. CLI
D. CPS Portal

Correct Answer: A
Section:

QUESTION 35
What is an alternative method to double NAT in Azure?

A. Scaling
B. System Routes
C. Peering
D. User Defined Routes

Correct Answer: C
Section:

QUESTION 36
To travel between spokes, non-transitive traffic uses _____ to allow Ipv4 and IPv6 traffic to reach a spoke network

A. a VTI
B. the Northbound hub
C. the Southbound hub
D. Peering

Correct Answer: D
Section:

QUESTION 37
One of the limitations in deploying Check Point CloudGuard Cluster High Availability is that:

A. State synchronization is required and must be done ONLY on a dedicated link
B. High Availability configurations support only two Security Gateway Members
C. High Availability configurations support only three Security Gateway members
D. VMAC mode is mandatory for all cluster interfaces

Correct Answer: B
Section:

QUESTION 38
Which APIs are used by Public clouds and Hybrid clouds to support the interactions between cloud resources, on- premises equipment, scripts, orchestration playbooks and CloudGuard Network cloud resources, on- premise equipment, scripts.

A. CloudGuard Management Extension API (CME-API)
B. CloudGuard Controller API (CG-API)
C. Representational State Transfer (REST) APIs
D. Cloud Security Posture Management (CSPM)

Correct Answer: A
Section:

QUESTION 39
Which scripting language is used by CloudGuard to develop templates that automate Security Gateway deployments?

A. Perl
B. C++
C. JSON
D. Python

Correct Answer: C
Section:

QUESTION 40
REST is an acronym for the following

A. Representation of Security Traffic

B. Really Efficient Security Template
C. Representational State Transfer
D. Real Security Threat

Correct Answer: C
Section:
Explanation:
The abbreviation REST stands for "Representational State Transfer" and refers to a software architectural style. It is based on six principles that describe how networked resources are defined and addressed on the web, for example in a cloud.

QUESTION 41
Which one of the following is part of the Orchestration Playbook process for creating a new spoke and an automated Security Gateway?

A. Transfer of resources to a VPN
B. An event trigger
C. Vertical scaling
D. Communication with the OS

Correct Answer: A
Section:

QUESTION 42
What are the Automation tools?

A. API. CLI Scripts. Shells and Templates
B. Terraform and Ansible
C. AMIs
D. CloudFormation

Correct Answer: A
Section:

QUESTION 43
Which of these is true of the CloudGuard Controller?

A. CloudGuard Controller manually updates SmartConsole security tads and API connections
B. CloudGuard Controller only displays cloud-based Security Gateway objects
C. CloudGuard Controller maintains visibility of the protected cloud environment
D. CoudGuard Control statically .denies Cloud resources created within a single cloud or a multicloud environment.

Correct Answer: D
Section:

QUESTION 44
What does the Adaptive Security Policy involve to import the Data Center Objects?

A. CloudGuard API

B. CloudGuard Controller
C. CloudGuard Access Control
D. CloudGuard Gateway

Correct Answer: B
Section:
Explanation:

CloudGuard Controller

The CloudGuard Controller, a sub-component of the Security Management Server, maintains visibility of protected cloud environments to carry out automation and adaptive security. This mechanism dynamically identifies cloud resources created within a single cloud or a multi-cloud environment.

In SmartConsole, the CloudGuard Controller displays cloud-based objects such as Security Gateways, virtual machines, and other Workload resources to define the Security Policy with an identity-based context. When Workloads expand/contract, the CloudGuard Controller tracks any modifications of

QUESTION 45
Logging Implied rules, enabling Hit Count and defining advanced VPN functions are all settings that are applied as

A. Inline Layer
B. Global Properties
C. Policy Settings
D. Gateway Properties

Correct Answer: B
Section:

QUESTION 46
What are two basic rules Check Point recommends for building an effective policy?

A. Cleanup and Stealth Rule
B. VPN and Admin Rules
C. Implicit and Explicit Rules
D. Access and Identity Rules

Correct Answer: A
Section:
Explanation:

Cleanup and Stealth Rules

There are two basic rules that Check Point recommends for building an effective Security Policy: the Cleanup rule and the Stealth rule. Both the Cleanup and Stealth rules are important for creating basic security measures and tracking important information.

- Cleanup Rule — A Cleanup rule is recommended to determine how to handle connections not matched by the rules above it in the Rulebase. It is also necessary for logging this traffic. Cleanup rules can be configured to allow or drop the connection. It should always be placed at the bottom of the Rulebase.
- Stealth Rule — A stealth rule is a rule that should be located as early in your policy as possible, typically immediately after any Management rules. The purpose of this is to drop any traffic destined for the Firewall that is not otherwise explicitly allowed.

In most cases, the Stealth rule should be placed above all other rules. Placing the Stealth rule among the first rules protects the gateway from port scanning, spoofing, and other types of direct attacks. Connections that need to be made directly to the gateway, such as Client Authentication, encryption, and Content Vectoring Protocol (CVP) rules, always go above the Stealth rule.

QUESTION 47
What is the key component in securing and managing any environment?

A. Security Management Server
B. Security Gateway
C. Security Policy
D. Security Access

Correct Answer: A
Section:

QUESTION 48
What can Data Center Objects represent?

A. vNets. VPCs or Network Security Groups
B. Compute. Regions or Availability Zones
C. Public IP. Private IP NAT or IAM roles
D. Cloud Data Center. Tags, subnets, or hosts

Correct Answer: C
Section:

QUESTION 49
An organization is using an adaptive security policy where a Data Center Object was imported and used in some rules. When the cloud resource represented by this object changes it's IP address, how will the change be effected on the Security Gateway

A. If CloudGuard Controller is enabled on the Security Gateway, the gateway will connect with the Cloud account and synchronize all the Data Center Objects used on
B. With a property functioning configuration, the change will automatically be done on the Security Gateway without any action required by the administrator
C. The Data Center Object needs to be refreshed in the SmartCansoIe and then a policy install will be required
D. The change is automatically updated to the Security Management Server and so only a policy install from SmartConsole or with API will be required

Correct Answer: B
Section:
Explanation:

protected cloud resources by automatically updating SmartConsole, security logs, and API connections to cloud accounts.

The CloudGuard Controller dynamically learns about objects and attributes in Workloads, such as changes in subnets, security groups, virtual machines, IP addresses ,and tags. After using the vendor's API to establish a trust relationship with a datacenter, CloudGuard Controller regularly polls the connected environments for changes in objects and object attributes used in the Security Policy. Changes are automatically pushed to the security gateway.

Dynamic environments present a large challenge to security professionals. The number of subnets, machines, and IP addresses changes quickly. The legacy model of manual updates to the security policy and Security Gateways every two or three days is too slow for such environments.

In most organizations, personnel from several different departments have permission to add or remove assets in Workloads. This kind of overlap creates a concern about the security and maintenance of assets in the data center. The solution to manual updates is to protect the security and maintenance of the assets - automatically. This is where the CloudGuard Controller comes in to assist. With the CloudGuard Controller, the Security Operation Center (SOC) can configure the security policy to automatically detect changes in Workloads, and push these changes directly to the Gateway.

QUESTION 50

What can a Security Admin do in a situation where collecting additional log file information to examine a CloudGuard Controller issue is required?

A. Execute a debug on the SMS
B. Set the operation to TRACE to collect more data.
C. Verify connectivity between the SMS and the SDDC.
D. Search for the information in the objects database.

Correct Answer: C
Section:

QUESTION 51
Deployment of a Security Gateway was initiated on AWS using a CloudFormation Template available through sk111013. The deployment process, after a while failed and rolled back. What could be the probable cause of this failure and roll back?

A. The Security Management Server that will be managing the Security Gateway had a lower version
B. The specific software being deployed was not subscribed to in the AWS Marketplace Subscriptions
C. The template used was for some cloud platform other than AWS
D. The web browser used to run the template was not compatible

Correct Answer: C
Section:

QUESTION 52
To troubleshoot CloudGuard Controller, administrators can execute the following command:

A. cloudguard troubleshoot
B. cloudguard security
C. cloudguard off
D. cloudguard on

Correct Answer: D
Section:

QUESTION 53
Where are the api logs found on the Security Management Server?

A. $FWDIR/log/api.elg
B. /var/tmp/api.elg
C. /var/log/api.elg
D. /opt/log/api.elg

Correct Answer: A
Section:

QUESTION 54
Which command will enable the CloudGuard Controller services on the Security Management Server

A. set cgcontroller state on
B. controller on
C. set cgcontroller on
D. cloudguard on

Correct Answer: D
Section:

QUESTION 55
The Security Administrator needs to reconfigure the API server, which command would need to be ran?

A. api reboot
B. api reconf
C. api restart
D. api reconfig

Correct Answer: D
Section:

QUESTION 56
What platform provides continuous compliance and governance assessments that evaluate public infrastructure according to industry to industry standards and best practices?

A. Cloud Security Posture Management
B. CloudGuard IaaS Public Cloud
C. CloudGuard SaaS
D. CloudGuard IaaS Private Cloud

Correct Answer: B
Section:

QUESTION 57
After the cloud acquisition process finishes. Cloud Security Posture Security module secures access to cloud environments by performing controls access to cloud environments by performing the following tasks: Visualizes Security Policies in cloud environments, control access to protected cloud assets with short-term dynamic access leases, and_____.

A. Automatically Installs Policies
B. Deploys new management resources
C. Manages Network Security Groups
D. Deploys new internal cloud resources

Correct Answer: B
Section:

QUESTION 58
What is the CloudGuard solution?

A. Check Point solution for private and public cloud
B. Check Point solution for public cloud

C. Check Point solution for private cloud
D. Check Point virtual gateway

Correct Answer: A
Section:

QUESTION 59
When using system routes and user defined routes in Azure, which takes precedent?

A. The user defined route takes precedent
B. The system route always takes precedent
C. The most specific route takes precedent
D. The newest route takes precedent

Correct Answer: C
Section:

QUESTION 60
When choosing PAYG (Pay As You Go) licensing in AWS, it is provided:

A. Via specific dedicated channels
B. Directly with Check Point
C. At the marketplace
D. Through the regular Check Point channels

Correct Answer: C
Section:

QUESTION 61
Which log file should an administrator gather to expedite the diagnosis of a CloudGuard Controller issue?

A. $CPDIR/logs/cloud.elg
B. $DADIR/logs/controller_proxy.elg
C. $FWDIR/logs/cloud_controller.elg
D. $FWDIR/logs/cloud_proxy.elg

Correct Answer: D
Section:

QUESTION 62
Which hub serves as the front end of the Workload that permits inbound web communications such as HTTP traffic from the Internet to reach spoke Workloads?

A. Web Hub
B. Southbound Hub
C. East-West Hub
D. Northbound Hub

Correct Answer: D
Section:
Explanation:
https://www.checkpoint.com/downloads/products/check-point-secure-cloud-blueprint-azurewhitepaper.pdf p.6