DUMPSBOSS.

AWS Certified Security - Specialty (SCS-C01)

Amazon AWS AWS-Certified-Security-Specialty-SCS-C01

Version Demo

Total Demo Questions: 20

Total Premium Questions: 820

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

A Systems Engineer is troubleshooting the connectivity of a test environment that includes a virtual security appliance deployed inline. In addition to using the virtual security appliance, the Development team wants to use security groups and network ACLs to accomplish various security requirements in the environment.

What configuration is necessary to allow the virtual security appliance to route the traffic?

A. Disable network ACLs.

B. Configure the security appliance's elastic network interface for promiscuous mode.

C. Disable the Network Source/Destination check on the security appliance's elastic network interface

D. Place the security appliance in the public subnet with the internet gateway

ANSWER: C

Explanation:

Each EC2 instance performs source/destination checks by default. This means that the instance must be the source or destination of any traffic it sends or receives. In this case virtual security appliance instance must be able to send and receive traffic when the source or destination is not itself. Therefore, you must disable source/destination checks on the NAT instance."

QUESTION NO: 2

A company uses Amazon API Gateway to present REST APIs to users. An API developer wants to analyze API access patterns without the need to parse the log files.

Which combination of steps will meet these requirements with the LEAST effort? (Select TWO.)

A. Configure access logging for the required API stage.

B. Configure an AWS CloudTrail trail destination for API Gateway events. Configure filters on the userIdentity, userAgent, and sourceIPAddress fields.

C. Configure an Amazon S3 destination for API Gateway logs. Run Amazon Athena queries to analyze API access information.

D. Use Amazon CloudWatch Logs Insights to analyze API access information.

E. Select the Enable Detailed CloudWatch Metrics option on the required API stage.

ANSWER: C D

QUESTION NO: 3

You have just received an email from IAM Support stating that your IAM account might have been compromised. Which of the following steps would you look to carry out immediately. Choose 3 answers from the options below.

Please select:

A. Change the root account password.

B. Rotate all IAM access keys

C. Keep all resources running to avoid disruption

D. Change the password for all IAM users.

ANSWER: A B D

Explanation:

One of the articles from IAM mentions what should be done in such a scenario

If you suspect that your account has been compromised, or if you have received a notification from IAM that the account has been compromised, perform the following tasks:

Change your IAM root account password and the passwords of any IAM users.

Delete or rotate all root and IAM Identity and Access Management (IAM) access keys.

Delete any resources on your account you didn't create, especially running EC2 instances, EC2 spot bids, or IAM users.

Respond to any notifications you received from IAM Support through the IAM Support Center.

Option C is invalid because there could be compromised instances or resources running on your environment. They should be shutdown or stopped immediately.

For more information on the article, please visit the below URL:

https://IAM.amazon.com/premiumsupport/knowledee-center/potential-account-compromise>

The correct answers are: Change the root account password. Rotate all IAM access keys. Change the password for all IAM users. Submit your Feedback/Queries to our Experts

QUESTION NO: 4

You want to launch an EC2 Instance with your own key pair in IAM. How can you achieve this? Choose 3 answers from the options given below.

Please select:

A. Use a third party tool to create the Key pair

B. Create a new key pair using the IAM CLI

C. Import the public key into EC2

D. Import the private key into EC2

ANSWER: A B C

Explanation:

This is given in the IAM Documentation Creating a Key Pair

You can use Amazon EC2 to create your key pair. For more information, see Creating a Key Pair Using Amazon EC2.

Alternatively, you could use a third-party tool and then import the public key to Amazon EC2. For more information, see Importing Your Own Public Key to Amazon EC2.

Option B is Correct, because you can use the IAM CLI to create a new key pair 1
https://docs.IAM.amazon.com/cli/latest/userguide/cli-ec2-keypairs.html

Option D is invalid because the public key needs to be stored in the EC2 Instance For more information on EC2 Key pairs, please visit the below URL:

* https://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/ec2-key-pairs

The correct answers are: Use a third party tool to create the Key pair. Create a new key pair using the IAM CLI, Import the public key into EC2

Submit your Feedback/Queries to our Experts

QUESTION NO: 5

A company wants to have an Intrusion detection system available for their VPC in IAM. They want to have complete control over the system. Which of the following would be ideal to implement?

Please select:

A. Use IAM WAF to catch all intrusions occurring on the systems in the VPC

B. Use a custom solution available in the IAM Marketplace

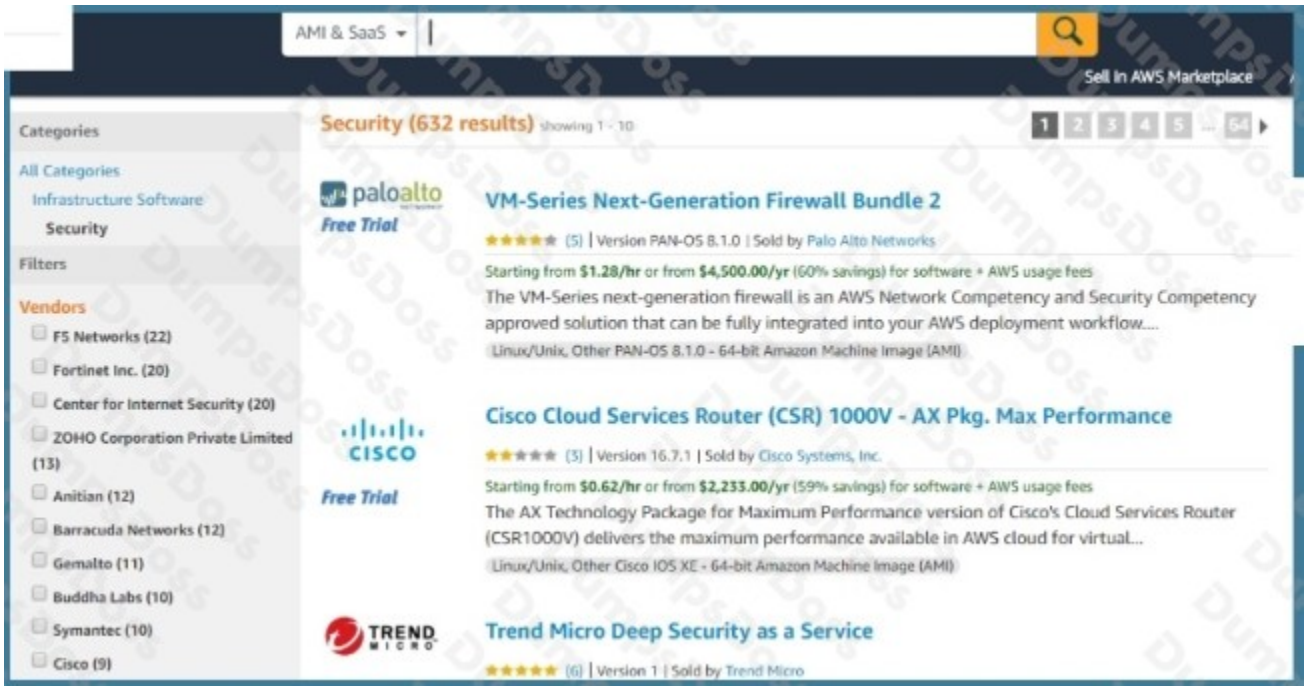
C. Use VPC Flow logs to detect the issues and flag them accordingly.

D. Use IAM Cloudwatch to monitor all traffic

ANSWER: B

Explanation:

Sometimes companies want to have custom solutions in place for monitoring Intrusions to their systems. In such a case, you can use the IAM Marketplace for looking at custom solutions.



Option A.C and D are all invalid because they cannot be used to conduct intrusion detection or prevention.

For more information on using custom security solutions please visit the below URL

https://d1.IAMstatic.com/Marketplace/security/IAMMP_Security_Solution%200verview.pdf

For more information on using custom security solutions please visit the below URL:

https://d1 .IAMstatic.com/Marketplace/security/IAMMP Security Solution%20Overview.pd1

The correct answer is: Use a custom solution available in the IAM Marketplace Submit your Feedback/Queries to our Experts

QUESTION NO: 6

A Security Engineer launches two Amazon EC2 instances in the same Amazon VPC but in separate Availability Zones. Each instance has a public IP address and is able to connect to external hosts on the internet. The two instances are able to communicate with each other by using their private IP addresses, but they are not able to communicate with each other when using their public IP addresses.

Which action should the Security Engineer take to allow communication over the public IP addresses?

A. Associate the instances to the same security groups.

B. Add 0.0.0.0/0 to the egress rules of the instance security groups.

C. Add the instance IDs to the ingress rules of the instance security groups.

D. Add the public IP addresses to the ingress rules of the instance security groups.

ANSWER: D

Explanation:

https://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/security-group-rules-reference.html#sg-rules-other-instances

QUESTION NO: 7

A security engineer needs to build a solution to turn IAM CloudTrail back on in multiple IAM Regions in case it is ever turned off.

What is the MOST efficient way to implement this solution?

A. Use IAM Config with a managed rule to trigger the IAM-EnableCloudTrail remediation.

B. Create an Amazon EventBridge (Amazon CloudWatch Events) event with a cloudtrail.amazonIAM.com event source and a StartLogging event name to trigger an IAM Lambda function to call the StartLogging API.

C. Create an Amazon CloudWatch alarm with a cloudtrail.amazonIAM.com event source and a StopLogging event name to trigger an IAM Lambda function to call the StartLogging API.

D. Monitor IAM Trusted Advisor to ensure CloudTrail logging is enabled.

ANSWER: B

QUESTION NO: 8

A company is using Amazon Elastic Container Service (Amazon ECS) to deploy an application that deals with sensitive data During a recent security audit, the company identified a security issue in which Amazon RDS credentials were stored with the application code In the company's source code repository

A security engineer needs to develop a solution to ensure that database credentials are stored securely and rotated periodically. The credentials should be accessible to the application only The engineer also needs to prevent database administrators from sharing database credentials as plaintext with other teammates. The solution must also minimize administrate overhead

Which solution meets these requirements?

A. Use the IAM Systems Manager Parameter Store to generate database credentials. Use an IAM profile for ECS tasks to restrict access to database credentials to specific containers only.

B. Use IAM Secrets Manager to store database credentials. Use an IAM inline policy for ECS tasks to restrict access to database credentials to specific containers only.

C. Use the IAM Systems Manager Parameter Store to store database credentials. Use IAM roles for ECS tasks to restrict access to database credentials lo specific containers only

D. Use IAM Secrets Manager to store database credentials. Use IAM roles for ECS tasks to restrict access to database credentials to specific containers only.

ANSWER: D

QUESTION NO: 9

A company has an application that uses an Amazon RDS PostgreSQL database. The company is developing an application feature that will store sensitive information for an individual in the database.

During a security review of the environment, the company discovers that the RDS DB instance is not encrypting data at rest. The company needs a solution that will provide encryption at rest for all the existing data and for any new data that is entered for an individual.

Which combination of options can the company use to meet these requirements? (Select TWO.)

A. Create a snapshot of the DB instance. Copy the snapshot to a new snapshot, and enable encryption for the copy process. Use the new snapshot to restore the DB instance.

B. Modify the configuration of the DB instance by enabling encryption. Create a snapshot of the DB instance. Use the snapshot to restore the DB instance.

C. Use IAM Key Management Service (IAM KMS) to create a new default IAM managed awa/rds key. Select this key as the encryption key for operations with Amazon RDS.

D. Use IAM Key Management Service (IAM KMS] to create a new CMK. Select this key as the encryption key for operations with Amazon RDS.

E. Create a snapshot of the DB instance. Enable encryption on the snapshoVUse the snapshot to restore the DB instance.

ANSWER: C E

QUESTION NO: 10

A company needs its Amazon Elastic Block Store (Amazon EBS) volumes to be encrypted at all times. During a security incident, EBS snapshots of suspicious instances are shared to a forensics account for analysis. A security engineer attempting to share a suspicious EBS snapshot to the forensics account receives the following error:

“Unable to share snapshot. An error occurred (OperationNotPermitted) when calling the ModifySnapshotAttribute operation: Encrypted snapshots with EBS default key cannot be shared” Which combination of steps should the security engineer take in the incident account to complete the sharing operation? (Choose three.)

A. Create a customer managed CMK. Copy the EBS snapshot encrypting the destination snapshot using the new CMK.

B. Allow forensics accounting principals to use the CMK by modifying its policy.

C. Create an Amazon EC2 instance. Attach the encrypted and suspicious EBS volume. Copy data from the suspicious volume to an unencrypted volume. Snapshot the unencrypted volume.

D. Copy the EBS snapshot to the new decrypted snapshot.

E. Restore a volume from the suspicious EBS snapshot. Create an unencrypted EBS volume of the same size.

F. Share the target EBS snapshot with the forensics account.

ANSWER: C D E

QUESTION NO: 11

An IAM user with fill EC2 permissions could bot start an Amazon EC2 instance after it was stopped for a maintenance task. Upon starting the instance, the instance state would change to “Pending”, but after a few seconds, it would switch back to “Stopped”.

An inspection revealed that the instance has attached Amazon EBS volumes that were encrypted by using a Customer Master Key (CMK). When these encrypted volumes were detached, the IAM user was able to start the EC2 instances.

The IAM user policy is as follows:

```
{
     "Version": "2012-10-17",
     "Statement": [
          {
               "Effect": "Allow",
               "Action": [
               <Action>
               ],
               "Resource": [
                   "arn:aws:kms:us-east-1:012345678910:key/ebs-encryption-key"
               ]
               <CONDITION>
          }
     ]
}
```

What additional items need to be added to the IAM user policy? (Choose two.)

A. kms:GenerateDataKey

B. kms:Decrypt

C. kms:CreateGrant

D. “Condition”: {“Bool”: {“kms:ViaService”: “ec2.us-west-2.amazonIAM.com”}}

E. “Condition”: {“Bool”: {“kms:GrantIsForIAMResource”: true}}

ANSWER: C E

Explanation:

The EBS which is IAM resource service is encrypted with CMK and to allow EC2 to decrypt , the IAM user should create a grant (action) and a boolean condition for the IAM resource . This link explains how IAM keys works.
https://docs.IAM.amazon.com/kms/latest/developerguide/key-policies.html

QUESTION NO: 12

A company has several production IAM accounts and a central security IAM account. The security account is used for centralized monitoring and has IAM privileges to all resources in every corporate account. All of the company's Amazon S3 buckets are tagged with a value denoting the data classification of their contents.

A Security Engineer is deploying a monitoring solution in the security account that will enforce bucket policy compliance. The system must monitor S3 buckets in all production accounts and confirm that any policy change is in accordance with the bucket's data classification. If any change is out of compliance; the Security team must be notified quickly.

Which combination of actions would build the required solution? (Choose three.)

A. Configure Amazon CloudWatch Events in the production accounts to send all S3 events to the security account event bus.

B. Enable Amazon GuardDuty in the security account. and join the production accounts as members.

C. Configure an Amazon CloudWatch Events rule in the security account to detect S3 bucket creation or modification events.

D. Enable IAM Trusted Advisor and activate email notifications for an email address assigned to the security contact.

E. Invoke an IAM Lambda function in the security account to analyze S3 bucket settings in response to S3 events, and send non-compliance notifications to the Security team.

F. Configure event notifications on S3 buckets for PUT; POST, and DELETE events.

ANSWER: D E F

QUESTION NO: 13

A company uses AWS CodePipeline for its software builds. Company policy mandates that code must be deployed to the staging environment before it is deployed to the production environment. The company needs to implement monitoring and alerting to detect when a CodePipeline pipeline is used to deploy code to production without the code first being deployed to staging.

What should a security engineer do to meet these requirements?

A. Enable Amazon GuardDuty to monitor AWS CloudTrail for CodePipeline. Configure findings through AWS Security Hub, and create a custom action in Security Hub to send to Amazon Simple Notification Service (Amazon SNS).

B. Use the AWS Cloud Development Kit (AWS CDK) to model reference-architecture CodePipeline pipeline that deploys application code through the staging environment and then the production environment.

C. Turn on AWS Config recording. Use a custom AWS Config rule to examine each CodePipeline pipeline for compliance. Configure an Amazon Simple Notification Service (Amazon SNS) notification on any change that is not in compliance with the rule. Add the desired receiver of the notification as a subscriber to the SNS topic.

D. Use Amazon Inspector to conduct an assessment of the CodePipeline pipelines and send a notification upon the discovery of a pipeline that is not in compliance. Add the desired receiver of the notification as a subscriber to the Amazon Simple Notification Service (Amazon SNS) topic.

ANSWER: A

QUESTION NO: 14

A Developer signed in to a new account within an AWS Organizations organizational unit (OU) containing multiple accounts. Access to the Amazon S3 service is restricted with the following SCP:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "s3:*",
            "Resource": "*"
        }
    ]
}
```

How can the Security Engineer provide the Developer with Amazon S3 access without affecting other accounts?

A. Move the SCP to the root OU of Organizations to remove the restriction to access Amazon S3.

B. Add an IAM policy for the Developer, which grants S3 access.

C. Create a new OU without applying the SCP restricting S3 access. Move the Developer account to this new OU.

D. Add an allow list for the Developer account for the S3 service.

ANSWER: C

QUESTION NO: 15

A developer at a company uses an SSH key to access multiple Amazon EC2 instances. The company discovers that the SSH key has been posted on a public GitHub repository. A security engineer verifies that the key has not been used recently.

How should the security engineer prevent unauthorized access to the EC2 instances?

A. Delete the key pair from the EC2 console. Create a new key pair.

B. Use the ModifyInstanceAttribute API operation to change the key on any EC2 instance that is using the key.

C. Restrict SSH access in the security group to only known corporate IP addresses.

D. Update the key pair in any AMI that is used to launch the EC2 instances. Restart the EC2 instances.

ANSWER: C

QUESTION NO: 16

An Amazon S3 bucket is encrypted using an AWS KMS CMK. An IAM user is unable to download objects from the S3 bucket using the AWS Management Console; however, other users can download objects from the S3 bucket.

Which policies should the Security Engineer review and modify to resolve this issue? (Choose three.)

A. The CMK policy

B. The VPC endpoint policy

C. The S3 bucket policy

D. The S3 ACL

E. The IAM policy

ANSWER: A C E

Explanation:

Reference: https://aws.amazon.com/premiumsupport/knowledge-center/decrypt-kms-encrypted-objects-s3/

QUESTION NO: 17

A security alert has been raised for an Amazon EC2 instance in a customer account that is exhibiting strange behavior. The Security Engineer must first isolate the EC2 instance and then use tools for further investigation.

What should the Security Engineer use to isolate and research this event? (Choose three.)

A. IAM CloudTrail

B. Amazon Athena

C. IAM Key Management Service (IAM KMS)

D. VPC Flow Logs

E. IAM Firewall Manager

F. Security groups

ANSWER: A D F

Explanation:

https://github.com/IAMlabs/aws-well-architected-labs/blob/master/Security/300_Incident_Response_with_IAM_Console_and_CLI/Lab_Guide.md

QUESTION NO: 18

Which of the following is used as a secure way to log into an EC2 Linux Instance?

Please select:

A. IAM User name and password

B. Key pairs

C. IAM Access keys

D. IAM SDK keys

ANSWER: B

Explanation:

The IAM Documentation mentions the following

Key pairs consist of a public key and a private key. You use the private key to create a digital signature, and then IAM uses the corresponding public key to validate the signature. Key pairs are used only for Amazon EC2 and Amazon CloudFront.

Option A.C and D are all wrong because these are not used to log into EC2 Linux Instances

For more information on IAM Security credentials, please visit the below URL:

https://docs.IAM.amazon.com/eeneral/latest/er/IAM-sec-cred-types.html

The correct answer is: Key pairs

Submit your Feedback/Queries to our Experts

QUESTION NO: 19

Your IT Security department has mandated that all data on EBS volumes created for underlying EC2 Instances need to be encrypted. Which of the following can help achieve this?

Please select:

A. IAM KMS API

B. IAM Certificate Manager

C. API Gateway with STS

D. IAM Access Key

ANSWER: A

Explanation:

The IAM Documentation mentions the following on IAM KMS

IAM Key Management Service (IAM KMS) is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data. IAM KMS is integrated with other IAM services including Amazon Elastic Block Store (Amazon EBS), Amazon Simple Storage Service (Amazon S3), Amazon Redshift Amazon Elastic Transcoder, Amazon WorkMail, Amazon Relational Database Service (Amazon RDS), and others to make it simple to encrypt your data with encryption keys that you manage

Option B is incorrect - The IAM Certificate manager can be used to generate SSL certificates that can be used to encrypt traffic transit, but not at rest

Option C is incorrect is again used for issuing tokens when using API gateway for traffic in transit.

Option D is used for secure access to EC2 Instances

For more information on IAM KMS, please visit the following URL:

https://docs.IAM.amazon.com/kms/latest/developereuide/overview.htmll

The correct answer is: IAM KMS API

Submit your Feedback/Queries to our Experts

QUESTION NO: 20

Users report intermittent availability of a web application hosted on AWS. Monitoring systems report an excess of abnormal network traffic followed by high CPU utilization on the application web tier. Which of the following techniques will improve the availability of the application? (Choose two.)

A. Deploy AWS WAF to block all unsecured web applications from accessing the internet.

B. Deploy an Intrusion Detection/Prevention Systems (IDS/IPS) to monitor or block unusual incoming network traffic.

C. Configure security groups to allow outgoing network traffic only from hosts that are protected with up-to-date antivirus software.

D. Create Amazon CloudFront distribution and configure AWS WAF rules to protect the web applications from malicious traffic.

E. Use the default Amazon VPC for external-facing systems to allow AWS to actively block malicious network traffic affecting Amazon EC2 instances.

ANSWER: A B