Free Questions for SCS-C02 by actualtestdumps

Shared by Cox on 09-08-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An application has been built with Amazon EC2 instances that retrieve messages from Amazon SQS. Recently, IAM changes were made and the instances can no longer retrieve messages.

What actions should be taken to troubleshoot the issue while maintaining least privilege? (Select TWO.)

Options:

A- Configure and assign an MFA device to the role used by the instances.

B- Verify that the SQS resource policy does not explicitly deny access to the role used by the instances.

C- Verify that the access key attached to the role used by the instances is active.

D- Attach the AmazonSQSFullAccest. managed policy to the role used by the instances.

E- Verify that the role attached to the instances contains policies that allow access to the queue

Answer:

B, E

Explanation:

The correct answer is B and E. To troubleshoot the issue, the security engineer should verify that the SQS resource policy does not explicitly deny access to the role used by the instances, and that the role attached to the instances contains policies that allow access to the queue. These actions will ensure that the instances have the necessary permissions to retrieve messages from Amazon SQS, while maintaining the principle of least privilege.

The other options are incorrect because they are either unnecessary or overly permissive. Option A is incorrect because configuring and assigning an MFA device to the role used by the instances is not required to access Amazon SQS.MFA is an optional security feature that adds an extra layer of protection on top of the user name and password1. Option C is incorrect because verifying that the access key attached to the role used by the instances is active is not relevant to the issue.Access keys are used to make programmatic requests to AWS services, not to retrieve messages from Amazon SQS2. Option D is incorrect because attaching the AmazonSQSFullAccess managed policy to the role used by the instances is overly permissive and violates the principle of least privilege.This policy grants full access to all Amazon SQS actions and resources, which may expose the instances to unnecessary risks3.

Question 2

Question Type: **MultipleChoice**

A company is using an Amazon CloudFront distribution to deliver content from two origins. One origin is a dynamic application that is hosted on Amazon EC2 instances. The other origin is an Amazon S3 bucket for static assets.

A security analysis shows that HTTPS responses from the application do not comply with a security requirement to provide an X-Frame-Options HTTP header to prevent frame-related cross-site scripting attacks. A security engineer must ipake the full stack compliant by adding the missing HTTP header to the responses.

Which solution will meet these requirements?

Options:

A- Create a Lambda@Edge function. Include code to add the X-Frame-Options header to the response. Configure the function to run in response to the CloudFront origin response event.

B- Create a Lambda@Edge function. Include code to add the X-Frame-Options header to the response. Configure the function to run in response to the CloudFront viewer request event.

C- Update the CloudFront distribution by adding X-Frame-Options to custom headers in the origin settings.

D- Customize the EC2 hosted application to add the X-Frame-Options header to the responses that are returned to CloudFront.

Answer:

A

Explanation:

The correct answer is A because it allows the security engineer to add the X-Frame-Options header to the HTTPS responses from the application origin without modifying the origin itself. A Lambda@Edge function is a Lambda function that runs in response to CloudFront events, such as viewer request, origin request, origin response, or viewer response.By configuring the function to run in response to the origin response event, the security engineer can modify the response headers that CloudFront receives from the origin before sending them to the viewer1.The function can include code to add the X-Frame-Options header with the desired value, such as DENY or

SAMEORIGIN, to prevent frame-related cross-site scripting attacks2.

The other options are incorrect because they are either less efficient or less secure than option A) Option B is incorrect because configuring the Lambda@Edge function to run in response to the viewer request event is not optimal, as it adds latency to the request processing and does not modify the response headers that CloudFront receives from the origin. Option C is incorrect because adding X-Frame-Options to custom headers in the origin settings does not affect the response headers that CloudFront sends to the viewer.Custom headers are only used to send additional information to the origin when CloudFront forwards a request3. Option D is incorrect because customizing the EC2 hosted application to add the X-Frame-Options header to the responses requires changing the origin code, which may not be feasible or desirable for the security engineer.

Question 3

Question Type: MultipleChoice

An Amazon API Gateway API invokes an AWS Lambda function that needs to interact with a software-as-a-service (SaaS) platform. A unique client token is generated in the SaaS platform to grant access to the Lambda function. A security engineer needs to design a solution to encrypt the access token at rest and pass the token to the Lambda function at runtime.

Which solution will meet these requirements MOST cost-effectively?

Options:

A- Store the client token as a secret in AWS Secrets Manager. Use th^AWS SDK to retneve the secret in the Lambda function.

B- Configure a token-based Lambda authorizer in API Gateway.

C- Store the client token as a SecureString parameter in AWS Systems Manager Parameter Store. Use the AWS SDK to retrieve the value of the SecureString parameter in the Lambda function.

D- Use AWS Key Management Service (AWS KMS) to encrypt the client token. Pass the token to the Lambda function at runtime through an environment variable.

Answer:

C

Question 4

Question Type: MultipleChoice

A security analyst attempted to troubleshoot the monitoring of suspicious security group changes. The analyst was told that there is an Amazon CloudWatch alarm in place for these AWS CloudTrail log events. The analyst tested the monitoring setup by making a configuration change to the security group but did not receive any alerts.

Which of the following troubleshooting steps should the analyst perform?

Options:

A- Ensure that CloudTrail and S3 bucket access logging is enabled for the analyst's AWS account.

B- Verify that a metric filter was created and then mapped to an alarm. Check the alarm notification action.

C- Check the CloudWatch dashboards to ensure that there is a metric configured with an appropriate dimension for security group changes.

D- Verify that the analyst's account is mapped to an IAM policy that includes permissions for cloudwatch:GetMetricStatistics and cloudwatch:ListMetrics.

Answer:

B

Explanation:

The correct answer is B because it checks the configuration of the CloudWatch alarm that is supposed to monitor the CloudTrail log events. The analyst should verify that a metric filter was created to extract the relevant information from the log events, such as the event name, source, and user identity.The analyst should also verify that the metric filter was mapped to an alarm that triggers when a certain threshold is reached, and that the alarm notification action is set up correctly to send alerts to the analyst1.

The other options are incorrect because they do not address the issue of the CloudWatch alarm not working as expected. Option A is incorrect because CloudTrail and S3 bucket access logging are not related to the monitoring of security group changes.CloudTrail logs the API calls made to AWS services, and S3 bucket access logging records the requests made to the bucket2.Option C is incorrect because CloudWatch dashboards are used to display metrics and alarms in a graphical way, but they do not affect the functionality of

the alarm3. Option D is incorrect because the IAM policy permissions for cloudwatch:GetMetricStatistics and cloudwatch:ListMetrics are not required to monitor the CloudTrail log events.These permissions are used to retrieve the statistics and list of metrics for a given namespace4.

Question 5

Question Type: MultipleChoice

A company suspects that an attacker has exploited an overly permissive role to export credentials from Amazon EC2 instance metadat

a. The company uses Amazon GuardDuty and AWS Audit Manager. The company has enabled AWS CloudTrail logging and Amazon CloudWatch logging for all of its AWS accounts.

A security engineer must determine if the credentials were used to access the company's resources from an external account.

Which solution will provide this information?

Options:

A- Review GuardDuty findings to find InstanceCredentialExfiltration events.

B- Review assessment reports in the Audit Manager console to find InstanceCredentialExfiltration events.

C- Review CloudTrail logs for GetSessionToken API calls to AWS Security Token Service (AWS STS) that come from an acount ID from outside the company.

D- Review CloudWatch logs for GetSessionToken API calls to AWS Security Token Service (AWS STS) that come from an account ID from outside the company.

Answer:

A

Explanation:

The correct answer is A because GuardDuty can detect and alert on EC2 instance credential exfiltration events.These events indicate that the credentials obtained from the EC2 instance metadata service are being used from an IP address that is owned by a different AWS account than the one that owns the instance1.GuardDuty can also provide details such as the source and destination IP addresses, the AWS account ID of the attacker, and the API calls made using the exfiltrated credentials2.

The other options are incorrect because they do not provide the information needed to determine if the credentials were used to access the company's resources from an external account. Option B is incorrect because Audit Manager does not generate InstanceCredentialExfiltration events.Audit Manager is a service that helps you continuously audit your AWS usage to simplify how you assess risk and compliance with regulations and industry standards3. Option C is incorrect because CloudTrail logs do not show the account ID of the caller for GetSessionToken API calls to AWS STS.CloudTrail logs show the account ID of the identity whose credentials were used to call the API4. Option D is incorrect because CloudWatch logs do not show the GetSessionToken API calls to AWS STS by default.CloudWatch logs can show the API calls made by AWS Lambda functions, Amazon API Gateway, and other AWS services that integrate with CloudWatch5.

Question 6

Question Type: MultipleChoice

A company hosts an application on Amazon EC2 instances. The application also uses Amazon S3 and Amazon Simple Queue Service (Amazon SQS). The application is behind an Application Load Balancer (ALB) and scales with AWS Auto Scaling.

The company's security policy requires the use of least privilege access, which has been applied to all existing AWS resources. A security engineer needs to implement private connectivity to AWS services.

Which combination of steps should the security engineer take to meet this requirement? (Select THREE.)

Options:

A- Use an interface VPC endpoint for Amazon SQS

B- Configure a connection to Amazon S3 through AWS Transit Gateway.

C- Use a gateway VPC endpoint for Amazon S3.

D- Modify the 1AM role applied to the EC2 instances in the Auto Scaling group to allow outbound traffic to the interface endpoints.

E- Modify the endpoint policies on all VPC endpoints. Specify the SQS and S3 resources that the application uses

F- Configure a connection to Amazon S3 through AWS Firewall Manager

Answer:

A, C, E

Explanation:

The correct answer is A, C, and E because they provide the most secure and efficient way to implement private connectivity to AWS services. Using interface VPC endpoints for Amazon SQS and gateway VPC endpoints for Amazon S3 allows the application to access these services without using public IP addresses or internet gateways. Modifying the endpoint policies on all VPC endpoints enables the security engineer to specify the SQS and S3 resources that the application uses and restrict access to other resources.

The other options are incorrect because they do not provide private connectivity to AWS services or they introduce unnecessary complexity or cost. Option B is incorrect because AWS Transit Gateway is used to connect multiple VPCs and on-premises networks, not to connect to AWS services. Option D is incorrect because modifying the IAM role applied to the EC2 instances is not sufficient to allow outbound traffic to the interface endpoints. The security group and route table associated with the interface endpoints also need to be configured. Option F is incorrect because AWS Firewall Manager is used to centrally manage firewall rules across multiple accounts and resources, not to connect to AWS services.

Question 7

Question Type: MultipleChoice

An AWS Lambda function was misused to alter data, and a security engineer must identify who invoked the function and what output was produced. The engineer cannot find any logs create^ by the Lambda function in Amazon CloudWatch Logs.

Which of the following explains why the logs are not available?

Options:

A- The execution role for the Lambda function did not grant permissions to write log data to CloudWatch Logs.

B- The Lambda function was invoked by using Amazon API Gateway, so the logs are not stored in CloudWatch Logs.

C- The execution role for the Lambda function did not grant permissions to write to the Amazon S3 bucket where CloudWatch Logs stores the logs.

D- The version of the Lambda function that was invoked was not current.

Answer:

A

Question 8

Question Type: MultipleChoice

A company has an application that runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances are in an Amazon EC2 Auto Scaling group and are attached to Amazon Elastic Blodfc Store (Amazon EBS) volumes.

A security engineer needs to preserve all forensic evidence from one of the instances.

Which order of steps should the security engineer use to meet this requirement?

Options:

A- Take an EBS volume snapshot of the instance and store the snapshot in an Amazon S3 bucket. Take a memory snapshot of the instance and store the snapshot in an S3 bucket. Detach the instance from the Auto Scaling group. Deregister the instance from the ALB. Stop the instance.

B- Take a memory snapshot of the instance and store the snapshot in an Amazon S3 bucket. Stop the instance. Take an EBS volume snapshot of the instance
and store the snapshot in an S3 bucket. Detach the instance from the Auto Scaling group. Deregister the instance from the ALB.

C- Detach the instance from the Auto Scaling group. Deregister the instance from the ALB. Take an EBS volume snapshot of the instance and store the snapshot
in an Amazon S3 bucket. Take a memory snapshot of the instance and store the snapshot in an S3 bucket. Stop the instance

D- Detach the instance from the Auto Scaling group Deregister the instance from the ALB. Stop the instance. Take a memory snapshot of the instance and store the snapshot in an Amazon S3 bucket. Take an EBS volume snapshot of the instance and store the snapshot in an S3 bucket.

Answer:

B

Explanation:

The correct answer is B because it preserves the forensic evidence from the instance in the correct order. The first step is to take a memory snapshot of the instance and store it in an S3 bucket, as memory data is volatile and can be lost when the instance is stopped. The second step is to stop the instance, which will prevent any further changes to the EBS volume. The third step is to take an EBS volume snapshot of the instance and store it in an S3 bucket, which will capture the disk state of the instance. The last two steps are to detach the instance from the Auto Scaling group and deregister it from the ALB, which will isolate the instance from the rest of the application.

The other options are incorrect because they do not preserve the forensic evidence in the correct order. Option A takes the EBS volume snapshot before the memory snapshot, which can result in inconsistent data. Option C detaches and deregisters the instance before taking any snapshots, which can affect the availability of the application. Option D stops the instance before taking the memory snapshot, which can cause the loss of memory data.