Free Questions for SCS-C02

Shared by Mosley on 04-10-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A company uses Amazon EC2 instances to host frontend services behind an Application Load Balancer. Amazon Elastic Block Store (Amazon EBS) volumes are attached to the EC2 instances. The company uses Amazon S3 buckets to store large files for images and music.

The company has implemented a security architecture oit>AWS to prevent, identify, and isolate potential ransomware attacks. The company now wants to further reduce risk.

A security engineer must develop a disaster recovery solution that can recover to normal operations if an attacker bypasses preventive and detective controls. The solution must meet an RPO of 1 hour.

Which solution will meet these requirements?

Options:

A- Use AWS Backup to create backups of the EC2 instances and S3 buckets every hour. Create AWS CloudFormation templates that replicate existing architecture components. Use AWS CodeCommit to store the CloudFormation templates alongside application configuration code.

B- Use AWS Backup to create backups of the EBS volumes and S3 objects every day. Use Amazon Security Lake to create a centralized data lake for AWS CloudTrail logs and VPC flow logs. Use the logs for automated response.

C- Use Amazon Security Lake to create a centralized data lake for AWS CloudTrail logs and VPC flow logs. Use the logs for automated response Enable AWS Security Hub to establish a single location for recovery procedures. Create AWS CloudFormation templates that replicate existing architecture components. Use AWS CodeCommit to store the CloudFormation templates alongside application configuration code.

D- Create EBS snapshots every 4 hours Enable Amazon GuardDuty Malware Protection. Create automation to immediately restore the most recent snapshot for any EC2 instances that produce an Execution:EC2/MaliciousFile finding in GuardDuty.

Answer:

A

Explanation:

The correct answer is A because it meets the RPO of 1 hour by creating backups of the EC2 instances and S3 buckets every hour. It also uses AWS CloudFormation templates to replicate the existing architecture components and AWS CodeCommit to store the templates and the application configuration code. This way, the security engineer can quickly restore the environment in case of a ransomware attack.

The other options are incorrect because they do not meet the RPO of 1 hour or they do not provide a complete disaster recovery solution. Option B only creates backups of the EBS volumes and S3 objects every day, which is not frequent enough to meet the RPO. Option C does not create any backups of the EC2 instances or the S3 buckets, which are essential for the frontend services. Option D only creates EBS snapshots every 4 hours, which is also not frequent enough to meet the RPO. Additionally, option D relies on Amazon GuardDuty to detect and respond to ransomware attacks, which may not be effective if the attacker bypasses the preventive and detective controls.

Question 2

Question Type: **MultipleChoice**

A company is running an application on Amazon EC2 instances in an Auto Scaling group. The application stores logs locally. A security engineer noticed that logs were lost after a scale-in event. The security engineer needs to recommend a solution to ensure the durability and availability of log data All logs must be kept for a minimum of 1 year for auditing purposes. What should the security engineer recommend?

Options:

A- Within the Auto Scaling lifecycle, add a hook to create and attach an Amazon Elastic Block Store (Amazon EBS) log volume each time an EC2 instance is created. When the instance is terminated, the EBS volume can be reattached to another instance for log review.

B- Create an Amazon Elastic File System (Amazon EFS) file system and add a command in the user data section of the Auto Scaling launch template to mount the EFS file system during EC2 instance creation. Configure a process on the instance to copy the logs once a day from an instance Amazon Elastic Block Store (Amazon EBS) volume to a directory in the EFS file system.

C- Add an Amazon CloudWatch agent into the AMI used in the Auto Scaling group. Configure the CloudWatch agent to send the logs to Amazon CloudWatch Logs for review,

D- Within the Auto Scaling lifecycle, add a lifecycle hook at the terminating state transition and alert the engineering team by using a lifecycle notification to Amazon Simple Notification Service (Amazon SNS). Configure the hook to remain in the Terminating:Wait state for 1 hour to allow manual review of the security logs prior to instance termination.

Answer:

C

Explanation:

Option C is the best solution to ensure the durability and availability of log data from EC2 instances in an Auto Scaling group. By using an Amazon CloudWatch agent, the logs can be sent to Amazon CloudWatch Logs, which is a fully managed service that can store, monitor, and analyze log dat

a. CloudWatch Logs also allows you to set retention policies for your log groups, so you can keep the logs for a minimum of 1 year for auditing purposes.CloudWatch Logs also supports encryption, access control, and compliance features to protect your log data12

Question 3

Question Type: MultipleChoice

A company that uses AWS Organizations is using AWS 1AM Identity Center (AWS Single Sign-On) to administer access to AWS accounts. A security engineer is creating a custom permission set in 1AM Identity Center. The company will use the permission set across multiple accounts. An AWS managed policy and a customer managed policy are attached to the permission set. The security engineer has full administrative permissions and is operating in the management account.

When the security engineer attempts to assign the permission set to an 1AM Identity Center user who has access to multiple accounts, the assignment fails.

What should the security engineer do to resolve this failure?

Options:

A- Create the customer managed policy in every account where the permission set is assigned. Give the customer managed policy the same name and same permissions in each account.

B- Remove either the AWS managed policy or the customer managed policy from the permission set. Create a second permission set that includes the removed policy. Apply the permission sets separately to the user.

C- Evaluate the logic of the AWS managed policy and the customer managed policy. Resolve any policy conflicts in the permission set before deployment.

D- Do not add the new permission set to the user. Instead, edit the user's existing permission set to include the AWS managed policy and the customer managed policy.

Answer:

A

Explanation:

https://docs.aws.amazon.com/singlesignon/latest/userguide/howtocmp.html

'Before you assign your permission set with IAM policies, you must prepare your member account. The name of an IAM policy in your member account must be a case-sensitive match to name of the policy in your management account. IAM Identity Center fails to assign the permission set if the policy doesn't exist in your member account.'

Question 4

Question Type: **MultipleChoice**

A company that operates in a hybrid cloud environment must meet strict compliance requirements. The company wants to create a report that includes evidence from on-premises workloads alongside evidence from AWS resources. A security engineer must implement a solution to collect, review, and manage the evidence to demonstrate compliance with company policy.'

Which solution will meet these requirements?

Options:

A- Create an assessment in AWS Audit Manager from a prebuilt framework or a custom framework. Upload manual evidence from the on-premises workloads. Add the evidence to the assessment. Generate an assessment report after Audit Manager collects the necessary evidence from the AWS resources.

B- Install the Amazon CloudWatch agent on the on-premises workloads. Use AWS Config to deploy a conformance pack from a sample conformance pack template or a custom YAML template. Generate an assessment report after AWS Config identifies noncompliant workloads and resources.

C- Set up the appropriate security standard in AWS Security Hub. Upload manual evidence from the on-premises workloads. Wait for Security Hub to collect the evidence from the AWS resources. Download the list of controls as a .csv file.

D- Install the Amazon CloudWatch agent on the on-premises workloads. Create a CloudWatch dashboard to monitor the on-premises workloads and the AWS resources. Run a query on the workloads and resources. Download the results.

Answer:

A

Explanation:

The reason is that this solution will meet the requirements of collecting, reviewing, and managing the evidence from both on-premises and AWS resources to demonstrate compliance with company policy.According to the web search results12, "AWS Audit Manager helps you continuously audit your AWS usage to simplify how you manage risk and compliance with regulations and industry standards.AWS Audit Manager makes it easier to evaluate whether your policies, procedures, and activities---also known as controls---are operating as intended." The results1also state that "In addition to the evidence that Audit Manager collects from your AWS environment, you can also upload and centrally manage evidence from your on-premises or multicloud environment." Therefore, by creating an assessment in AWS Audit Manager, the security engineer can use a prebuilt or custom framework that contains the relevant controls for the company policy, upload manual evidence from the on-premises workloads, and add the evidence to the assessment. After Audit Manager collects the necessary evidence from the AWS resources, the security engineer can generate an assessment report that includes all the evidence from both sources.

The other options are incorrect because:

B) Install the Amazon CloudWatch agent on the on-premises workloads. Use AWS Config to deploy a conformance pack from a sample conformance pack template or a custom YAML template. Generate an assessment report after AWS Config identifies noncompliant workloads and resources. This option is not sufficient to meet the requirements, because it does not collect or manage the evidence from both sources. It only monitors and evaluates the configuration compliance of the workloads and resources using AWS Config rules.According to the web search results3, "A conformance pack is a collection of AWS Config rules and remediation actions that can be easily deployed as a single entity in an account and a Region or across an organization in AWS Organizations." However, a conformance pack does not provide a way to upload or include manual evidence from the on-premises workloads, nor does it generate an assessment report that contains all the evidence.

C) Set up the appropriate security standard in AWS Security Hub. Upload manual evidence from the on-premises workloads. Wait for Security Hub to collect the evidence from the AWS resources. Download the list of controls as a .csv file. This option is not optimal to meet the requirements, because it does not provide a comprehensive or audit-ready report that contains all the evidence. It only provides a list of controls and their compliance status in a .csv file format.According to the web search results4, "Security Hub provides you with a comprehensive view of your security state within AWS and helps you check your environment against security industry standards and best practices." However, Security Hub does not provide a way to upload or include manual evidence from the on-premises workloads, nor does it generate an assessment report that contains all the evidence.

D) Install the Amazon CloudWatch agent on the on-premises workloads. Create a CloudWatch dashboard to monitor the on-premises workloads and the AWS resources. Run a query on the workloads and resources. Download the results. This option is not sufficient to meet the requirements, because it does not collect or manage the evidence from both sources. It only monitors and analyzes the metrics and logs of the workloads and resources using CloudWatch. According to the web search results, "Amazon CloudWatch is a monitoring and observability service built for DevOps engineers, developers, site reliability engineers (SREs), and IT managers." However, CloudWatch does not provide a way to upload or include manual evidence from the on-premises workloads, nor does it generate an assessment report that contains all the evidence.

Question 5

Question Type: MultipleChoice

A company's data scientists want to create artificial intelligence and machine learning (AI/ML) training models by using Amazon SageMaker. The training models will use large datasets in an Amazon S3 bucket. The datasets contain sensitive information.

On average. the data scientists need 30 days to train models. The S3 bucket has been secured appropriately The companfs data retention policy states that all data that is older than 45 days must be removed from the S3 bucket.

Which action should a security engineer take to enforce this data retention policy?

Options:

A- Configure an S3 Lifecycle rule on the S3 bucket to delete objects after 45 days.

B- Create an AWS Lambda function to check the last-modified date of the S3 objects and delete objects that are older than 45 days. Create an S3 event notification to invoke the Lambda function for each PutObject operation.

C- Create an AWS Lambda function to check the last-modified date of the S3 objects and delete objects that are older than 45 days. Create an Amazon EventBridge rule to invoke the Lambda function each month.

D- Configure S3 Intelligent-Ttering on the S3 bucket to automatically transition objects to another storage class.

Answer:

A

Explanation:

The correct answer is A. Configure an S3 Lifecycle rule on the S3 bucket to delete objects after 45 days.

The reason is that this is the simplest and most effective way to enforce the data retention policy. According to the AWS documentation1, "To manage your objects so that they are stored cost effectively throughout their lifecycle, configure their Amazon S3 Lifecycle. An S3 Lifecycle configuration is a set of rules that define actions that Amazon S3 applies to a group of objects. There are two types of actions: Transition actions and Expiration actions." The documentation1 also states that "Expiration actions define when objects expire. Amazon S3 deletes expired objects on your behalf." Therefore, by configuring an S3 Lifecycle rule on the S3 bucket to delete objects after 45 days, the security engineer can ensure that the data is removed from the S3 bucket according to the company's policy.

The other options are incorrect because:

B) Create an AWS Lambda function to check the last-modified date of the S3 objects and delete objects that are older than 45 days. Create an S3 event notification to invoke the Lambda function for each PutObject operation. This option is not optimal because it requires deploying and maintaining a Lambda function, which adds complexity and cost. Moreover, it does not guarantee that the data is deleted exactly after 45 days, since the Lambda function is triggered only when a new object is put into the S3 bucket. If there are no new objects for a long period of time, the Lambda function will not run and the data will not be deleted.

C) Create an AWS Lambda function to check the last-modified date of the S3 objects and delete objects that are older than 45 days. Create an Amazon EventBridge rule to invoke the Lambda function each month. This option is not optimal because it requires deploying and maintaining a Lambda function, which adds complexity and cost. Moreover, it does not guarantee that the data is deleted exactly after 45 days, since the Lambda function is triggered only once a month. If the data is older than 45 days but less than a month, it will not be deleted until the next month.

D) Configure S3 Intelligent-Tiering on the S3 bucket to automatically transition objects to another storage class. This option is not sufficient to enforce the data retention policy, because it does not delete the data from the S3 bucket. It only moves the data to a less expensive storage class based on access patterns. According to the AWS documentation2, ''S3 Intelligent-Tiering optimizes storage costs by automatically moving data between two access tiers, frequent access and infrequent access, when access patterns change.'' However, this feature does not expire or delete the data after a certain period of time.

Question 6

Question Type: **MultipleChoice**

A company manages multiple AWS accounts using AWS Organizations. The company's security team notices that some member accounts are not sending AWS CloudTrail logs to a centralized Amazon S3 logging bucket. The security team wants to ensure there is at least one trail configured for all existing accounts and for any account that is created in the future.

Which set of actions should the security team implement to accomplish this?

Options:

A- Create a new trail and configure it to send CloudTrail logs to Amazon S3. Use Amazon EventBridge to send notification if a trail is deleted or stopped.

B- Deploy an AWS Lambda function in every account to check if there is an existing trail and create a new trail, if needed.

C- Edit the existing trail in the Organizations management account and apply it to the organization.

D- Create an SCP to deny the cloudtrail:Delete* and cloudtrail:Stop* actbns. Apply the SCP to all accounts.

Answer:

C

Explanation:

The correct answer is C. Edit the existing trail in the Organizations management account and apply it to the organization.

The reason is that this is the simplest and most effective way to ensure that there is at least one trail configured for all existing accounts and for any account that is created in the future. According to the AWS documentation1, "If you have created an organization in AWS Organizations, you can create a trail that logs all events for all AWS accounts in that organization. This is sometimes called an organization trail." The documentation1 also states that "The management account for the organization can edit an existing trail in their account, and apply it to an organization, making it an organization trail. Organization trails log events for the management account and all member accounts in the organization." Therefore, by editing the existing trail in the management account and applying it to the organization, the security team can ensure that all accounts are sending CloudTrail logs to a centralized S3 logging bucket.

The other options are incorrect because:

A) Create a new trail and configure it to send CloudTrail logs to Amazon S3. Use Amazon EventBridge to send notification if a trail is deleted or stopped. This option is not sufficient to ensure that there is at least one trail configured for all accounts, because it does not prevent users from deleting or stopping the trail in their accounts. Even if EventBridge sends a notification, the security team would have to manually restore or restart the trail, which is not efficient or scalable.

B) Deploy an AWS Lambda function in every account to check if there is an existing trail and create a new trail, if needed. This option is not optimal because it requires deploying and maintaining a Lambda function in every account, which adds complexity and cost. Moreover, it does not prevent users from deleting or stopping the trail after it is created by the Lambda function.

D) Create an SCP to deny the cloudtrail:Delete and cloudtrail:Stop actions. Apply the SCP to all accounts. This option is not sufficient to ensure that there is at least one trail configured for all accounts, because it does not create or apply a trail in the first place. It only prevents users from deleting or stopping an existing trail, but it does not guarantee that a trail exists in every account.

Question 7

Question Type: **MultipleChoice**

A company hosts a web application on an Apache web server. The application runs on Amazon EC2 instances that are in an Auto Scaling group. The company configured the EC2 instances to send the Apache web server logs to an Amazon CloudWatch Logs group that the company has configured to expire after 1 year.

Recently, the company discovered in the Apache web server logs that a specific IP address is sending suspicious requests to the web application. A security engineer wants to analyze the past week of Apache web server logs to determine how many requests that the IP address sent and the corresponding URLs that the IP address requested.

What should the security engineer do to meet these requirements with the LEAST effort?

Options:

A- Export the CloudWatch Logs group data to Amazon S3. Use Amazon Macie to query the logs for the specific IP address and the requested URLs.

B- Configure a CloudWatch Logs subscription to stream the log group to an Am-azon OpenSearch Service cluster. Use OpenSearch Service to analyze the logs for the specific IP address and the requested URLs.

C- Use CloudWatch Logs Insights and a custom query syntax to analyze the CloudWatch logs for the specific IP address and the requested URLs.

D- Export the CloudWatch Logs group data to Amazon S3. Use AWS Glue to crawl the S3 bucket for only the log entries that contain the specific IP ad-dress. Use AWS Glue to view the results.

Answer:

C

Question 8

Question Type: **MultipleChoice**

A company is using AWS Organizations to manage multiple AWS accounts for its hu-man resources, finance, software development, and production departments. All the company's developers are part of the software development AWS account.

The company discovers that developers have launched Amazon EC2 instances that were preconfigured with software that the company has not approved for use. The company wants to implement a solution to ensure that developers can launch EC2 instances with only approved software applications and only in the software de-velopment AWS account.

Which solution will meet these requirements?

Options:

A- In the software development account, create AMIS of preconfigured instanc-es that include only approved software. Include the AMI IDs in the condi-tion section of an AWS CloudFormation template to launch the appropriate AMI based on the AWS Region. Provide the developers with the CloudFor-mation template to launch EC2 instances in the software development ac-count.

B- Create an Amazon EventBridge rule that runs when any EC2 RunInstances API event occurs in the software development account. Specify AWS Systems Man-ager Run Command as a target of the rule. Configure Run Command to run a script that will install all approved software onto the instances that the developers launch.

C- Use an AWS Service Catalog portfolio that contains EC2 products with ap-propriate AMIS that include only approved software. Grant the developers permission to portfolio access only the Service Catalog to launch a prod-uct in the software development account.

D- In the management account, create AMIS of preconfigured instances that in-clude only approved software. Use AWS CloudFormation StackSets to launch the AMIS across any AWS account in the organization. Grant the developers permission to launch the stack sets within the management account.

Answer:

C

Question 9

Question Type: MultipleChoice

A company is running internal microservices on Amazon Elastic Container Service (Amazon ECS) with the Amazon EC2 launch type. The company is using Amazon Elastic Container Registry (Amazon ECR) private repositories.

A security engineer needs to encrypt the private repositories by using AWS Key Management Service (AWS KMS). The security engineer also needs to analyze the container images for any common vulnerabilities and exposures (CVEs).

Which solution will meet these requirements?

Options:

A- Enable KMS encryption on the existing ECR repositories. Install Amazon Inspector Agent from the ECS container instances' user data. Run an assessment with the CVE rules.

B- Recreate the ECR repositories with KMS encryption and ECR scanning enabled. Analyze the scan report after the next push of images.

C- Recreate the ECR repositories with KMS encryption and ECR scanning enabled. Install AWS Systems Manager Agent on the ECS container instances. Run an inventory report.

D- Enable KMS encryption on the existing ECR repositories. Use AWS Trusted Advisor to check the ECS container instances and to verily the findings against a list of current CVEs.

Answer:

B

Question 10

Question Type: **MultipleChoice**

What are the MOST secure ways to protect the AWS account root user of a recently opened AWS account? (Select TWO.)

Options:

A- Use the AWS account root user access keys instead of the AWS Management Console.

B- Enable multi-factor authentication for the AWS IAM users with the Adminis-tratorAccess managed policy attached to them.

C- Enable multi-factor authentication for the AWS account root user.

D- Use AWS KMS to encrypt all AWS account root user and AWS IAM access keys and set automatic rotation to 30 days.

E- Do not create access keys for the AWS account root user; instead, create AWS IAM users.

Answer:

C, E

Question 11

Question Type: **MultipleChoice**

A company has a web server in the AWS Cloud. The company will store the content for the web server in an Amazon S3 bucket. A security engineer must use an Amazon CloudFront distribution to speed up delivery of the content. None of the files can be publicly accessible from the S3 bucket direct.

Which solution will meet these requirements?

Options:

A- Configure the permissions on the individual files in the S3 bucket so that only the CloudFront distribution has access to them.

B- Create an origin access identity (OAI). Associate the OAI with the CloudFront distribution. Configure the S3 bucket permissions so that only the OAI can access the files in the S3 bucket.

C- Create an S3 role in AWS Identity and Access Management (IAM). Allow only the CloudFront distribution to assume the role to access the files in the S3 bucket.

D- Create an S3 bucket policy that uses only the CloudFront distribution ID as the principal and the Amazon Resource Name (ARN) as the target.

Answer:

B