SCS-C02 Q&As

AWS Certified Security - Specialty

Pass Amazon SCS-C02 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/scs-c02.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Amazon Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

A company\\'s Security Team received an email notification from the Amazon EC2 Abuse team that one or more of the company\\'s Amazon EC2 instances may have been compromised

Which combination of actions should the Security team take to respond to (be current modem? (Select TWO.)

A. Open a support case with the IAM Security team and ask them to remove the malicious code from the affected instance

B. Respond to the notification and list the actions that have been taken to address the incident

C. Delete all IAM users and resources in the account

D. Detach the internet gateway from the VPC remove aft rules that contain 0.0.0.0V0 from the security groups, and create a NACL rule to deny all traffic Inbound from the internet

E. Delete the identified compromised instances and delete any associated resources that the Security team did not create.

Correct Answer: DE

these are the recommended actions to take when you receive an abuse notice from AWS8. You should review the abuse notice to see what content or activity was reported and detach the internet gateway from the VPC to isolate the affected instances from the internet. You should also remove any rules that allow inbound traffic from 0.0.0.0/0 from the security groups and create a network access control list (NACL) rule to deny all traffic inbound from the internet. You should then delete the compromised instances and any associated resources that you did not create. The other options are either inappropriate or unnecessary for responding to the abuse notice.

QUESTION 2

A company has deployed Amazon GuardDuty and now wants to implement automation for potential threats. The company has decided to start with RDP brute force attacks that come from Amazon EC2 instances in the company\\'s AWS

environment. A security engineer needs to implement a solution that blocks the detected communication from a suspicious instance until investigation and potential remediation can occur.

Which solution will meet these requirements?

A. Configure GuardDuty to send the event to an Amazon Kinesis data stream. Process the event with an Amazon Kinesis Data Analytics for Apache Flink application that sends a notification to the company through Amazon Simple Notification Service (Amazon SNS). Add rules to the network ACL to block traffic to and from the suspicious instance.

B. Configure GuardDuty to send the event to Amazon EventBridge (Amazon CloudWatch Events). Deploy an AWS WAF web ACL. Process the event with an AWS Lambda function that sends a notification to the company through Amazon Simple Notification Service (Amazon SNS) and adds a web ACL rule to block traffic to and from the suspicious instance.

C. Enable AWS Security Hub to ingest GuardDuty findings and send the event to Amazon EventBridge (Amazon CloudWatch Events). Deploy AWS Network Firewall. Process the event with an AWS Lambda function that adds a rule to a Network Firewall firewall policy to block traffic to and from the suspicious instance.

D. Enable AWS Security Hub to ingest GuardDuty findings. Configure an Amazon Kinesis data stream as an event destination for Security Hub. Process the event with an AWS Lambda function that replaces the security group of the suspicious instance with a security group that does not allow any connections.

Correct Answer: C

https://aws.amazon.com/blogs/security/automatically-block-suspicious-traffic-with-aws-network-firewall-and-amazon-guardduty/

QUESTION 3

A company plans to create individual child accounts within an existing organization in IAM Organizations for each of its DevOps teams. IAM CloudTrail has been enabled and configured on all accounts to write audit logs to an Amazon S3 bucket in a centralized IAM account. A security engineer needs to ensure that DevOps team members are unable to modify or disable this configuration.

How can the security engineer meet these requirements?

A. Create an IAM policy that prohibits changes to the specific CloudTrail trail and apply the policy to the IAM account root user.

B. Create an S3 bucket policy in the specified destination account for the CloudTrail trail that prohibits configuration changes from the IAM account root user in the source account.

C. Create an SCP that prohibits changes to the specific CloudTrail trail and apply the SCP to the appropriate organizational unit or account in Organizations.

D. Create an IAM policy that prohibits changes to the specific CloudTrail trail and apply the policy to a new IAM group. Have team members use individual IAM accounts that are members of the new IAM group.

Correct Answer: D

QUESTION 4

A company finds that one of its Amazon EC2 instances suddenly has a high CPU usage. The company does not know whether the EC2 instance is compromised or whether the operating system is performing background cleanup.

Which combination of steps should a security engineer take before investigating the issue? (Select THREE.)

A. Disable termination protection for the EC2 instance if termination protection has not been disabled.

B. Enable termination protection for the EC2 instance if termination protection has not been enabled.

C. Take snapshots of the Amazon Elastic Block Store (Amazon EBS) data volumes that are attached to the EC2 instance.

D. Remove all snapshots of the Amazon Elastic Block Store (Amazon EBS) data volumes that are attached to the EC2 instance.

E. Capture the EC2 instance metadata, and then tag the EC2 instance as under quarantine.

F. Immediately remove any entries in the EC2 instance metadata that contain sensitive information.

Correct Answer: BCE

https://d1.awsstatic.com/WWPS/pdf/aws_security_incident_response.pdf

QUESTION 5

A company wants to monitor the deletion of customer managed CMKs A security engineer must create an alarm that will notify the company before a CMK is deleted The security engineer has configured the integration of IAM CloudTrail with Amazon CloudWatch

What should the security engineer do next to meet this requirement?

A. Use inbound rule 100 to allow traffic on TCP port 443 Use inbound rule 200 to deny traffic on TCP port 3306 Use outbound rule 100 to allow traffic on TCP port 443

B. Use inbound rule 100 to deny traffic on TCP port 3306. Use inbound rule 200 to allow traffic on TCP port range 1024-65535. Use outbound rule 100 to allow traffic on TCP port

C. Use inbound rule 100 to allow traffic on TCP port range 1024-65535 Use inbound rule 200 to deny traffic on TCP port 3306 Use outbound rule 100 to allow traffic on TCP port

D. Use inbound rule 100 to deny traffic on TCP port 3306 Use inbound rule 200 to allow traffic on TCP port 443 Use outbound rule 100 to allow traffic on TCP port 443

Correct Answer: A

QUESTION 6

An ecommerce company has a web application architecture that runs primarily on containers. The application containers are deployed on Amazon Elastic Container Service (Amazon ECS). The container images for the application are stored

in Amazon Elastic Container Registry (Amazon ECR).

The company\\'s security team is performing an audit of components of the application architecture.

The security team identifies issues with some container images that are stored in the container repositories.

The security team wants to address these issues by implementing continual scanning and on-push scanning of the container images.

The security team needs to implement a solution that makes any findings from these scans visible in a centralized dashboard.

The security team plans to use the dashboard to view these findings along with other security-related findings that they intend to generate in the future.

There are specific repositories that the security team needs to exclude from the scanning process.

Which solution will meet these requirements?

A. Use Amazon Inspector. Create inclusion rules in Amazon ECR to match repos-itories that need to be scanned. Push Amazon Inspector findings to AWS Se-curity Hub.

B. Use ECR basic scanning of container images. Create inclusion rules in Ama-zon ECR to match repositories that need to be scanned. Push findings to AWS Security Hub.

C. Use ECR basic scanning of container images. Create inclusion rules in Ama-zon ECR to match repositories that need to be scanned. Push findings to Amazon Inspector.

D. Use Amazon Inspector. Create inclusion rules in Amazon Inspector to match repositories that need to be scanned. Push Amazon Inspector findings to AWS Config.

Correct Answer: A

QUESTION 7

A company has multiple accounts in the AWS Cloud. Users in the developer account need to have access to specific resources in the production account. What is the MOST secure way to provide this access?

A. Create one IAM user in the production account. Grant the appropriate permissions to the resources that are needed. Share the password only with the users that need access.

B. Create cross-account access with an IAM role in the developer account. Grant the appropriate permissions to this role. Allow users in the developer account to assume this role to access the production resources.

C. Create cross-account access with an IAM user account in the production account. Grant the appropriate permissions to this user account. Allow users in the developer account to use this user account to access the production resources.

D. Create cross-account access with an IAM role in the production account. Grant the appropriate permissions to this role. Allow users in the developer account to assume this role to access the production resources.

Correct Answer: D

https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html

QUESTION 8

A security engineer is creating an AWS Lambda function. The Lambda function needs to use a role that is named LambdaAuditRole to assume a role that is named AcmeAuditFactoryRole in a different AWS account.

When the code is processed, the following error message appears: "An error oc-curred (AccessDenied) when calling the AssumeRole operation."

Which combination of steps should the security engineer take to resolve this er-ror? (Select TWO.)

A. Ensure that LambdaAuditRole has the sts:AssumeRole permission for Ac-meAuditFactoryRole.

B. Ensure that LambdaAuditRole has the AWSLambdaBasicExecutionRole managed policy attached.

C. Ensure that the trust policy for AcmeAuditFactoryRole allows the sts:AssumeRole action from LambdaAuditRole.

D. Ensure that the trust policy for LambdaAuditRole allows the sts:AssumeRole action from the lambda.amazonaws.com service.

E. Ensure that the sts:AssumeRole API call is being issued to the us-east-I Region endpoint.

Correct Answer: AC

QUESTION 9

A company stores images for a website in an Amazon S3 bucket. The company is using Amazon CloudFront to serve the images to end users. The company recently discovered that the images are being accessed from countries where the company does not have a distribution license.

Which actions should the company take to secure the images to limit their distribution? (Select TWO.)

A. Update the S3 bucket policy to restrict access to a CloudFront origin access identity (OAI).

B. Update the website DNS record to use an Amazon Route 53 geolocation record deny list of countries where the company lacks a license.

C. Add a CloudFront geo restriction deny list of countries where the company lacks a license.

D. Update the S3 bucket policy with a deny list of countries where the company lacks a license.

E. Enable the Restrict Viewer Access option in CloudFront to create a deny list of countries where the company lacks a license.

Correct Answer: AC

To secure the images to limit their distribution, the company should take the following actions:

Update the S3 bucket policy to restrict access to a CloudFront origin access identity (OAI). This allows the company to use a special CloudFront user that can access objects in their S3 bucket, and prevent anyone else from accessing them

directly.

Add a CloudFront geo restriction deny list of countries where the company lacks a license. This allows the company to use a feature that controls access to their content based on the geographic location of their viewers, and block requests

from countries where they do not have a distribution license.

QUESTION 10

A company has developed a new Amazon RDS database application. The company must secure the ROS database credentials for encryption in transit and encryption at rest. The company also must rotate the credentials automatically on a regular basis.

Which solution meets these requirements?

A. Use IAM Systems Manager Parameter Store to store the database credentiais.Configure automatic rotation of the credentials.

B. Use IAM Secrets Manager to store the database credentials. Configure automat* rotation of the credentials

C. Store the database credentials in an Amazon S3 bucket that is configured with server-side encryption with S3 managed encryption keys (SSE-S3) Rotate the credentials with IAM database authentication.

D. Store the database credentials m Amazon S3 Glacier, and use S3 Glacier Vault Lock Configure an IAM Lambda function to rotate the credentials on a scheduled basts

Correct Answer: A

QUESTION 11

To meet regulatory requirements, a Security Engineer needs to implement an IAM policy that restricts the use of AWS services to the us-east-1 Region.

What policy should the Engineer implement?

A.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
          "Effect": "Allow",
          "Action": "*",
          "Resource": "*",
          "Condition":  {
              "StringEquals":  {
                  "aws:RequestedRegion": "us-east-1"
              }
          }
        }
    ]
}
```

B.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
          "Effect": "Allow",
          "Action": "*",
          "Resource": "*",
          "Condition":  {
              "StringEquals":  {
                  "ec2:Region": "us-east-1"
              }
          }
        }
    ]
}
```

C.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
          "Effect": "Deny",
          "Action": "*",
          "Resource": "*",
          "Condition":  {
              "StringNotEquals":  {
                  "aws:RequestedRegion": "us-east-1"
              }
          }
        }
    ]
}
```

D.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
          "Effect": "Deny",
          "NotAction": "*",
          "Resource": "*",
          "Condition":  {
              "StringEquals":  {
                  "aws:RequestedRegion": "us-east-1"
              }
          }
        }
    ]
}
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: C

https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_examples_aws_deny-requested-region.html

QUESTION 12

A company\\'s application team wants to replace an internal application with a new IAM architecture that consists of Amazon EC2 instances, an IAM Lambda function, and an Amazon S3 bucket in a single IAM Region. After an architecture review, the security team mandates that no application network traffic can traverse the public internet at any point. The security team already has an SCP in place for the company\\'s organization in IAM Organizations to restrict the creation of internet gateways. NAT gateways, and egress-only gateways.

Which combination of steps should the application team take to meet these requirements? (Select THREE.)

A. Create an S3 endpoint that has a full-access policy for the application\\'s VPC.

B. Create an S3 access point for the S3 bucket. Include a policy that restricts the network origin to VPCs.

C. Launch the Lambda function. Enable the block public access configuration.

D. Create a security group that has an outbound rule over port 443 with a destination of the S3 endpomt. Associate the security group with the EC2 instances.

E. Create a security group that has an outbound rule over port 443 with a destination of the S3 access point. Associate the security group with the EC2 instances.

F. Launch the Lambda function in a VPC.

Correct Answer: ADF

QUESTION 13

A security engineer is defining the controls required to protect the IAM account root user credentials in an IAM Organizations hierarchy. The controls should also limit the impact in case these credentials have been compromised. Which combination of controls should the security engineer propose? (Select THREE.)

A. Apply the following SCP:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GRRESTRICTROOTUSER",
            "Effect": "Deny",
            "Action": "*",
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringLike": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::*:root"
                    ]
                }
            }
        }
    ]
}
```

B. Apply the following SCP:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GRRESTRICTROOTUSER",
            "Effect": "Deny",
            "Principal" : "arn:aws:iam::*:root"
            "Action": "*",
            "Resource": [
                "*"
            ]
        }
    ]
}
```

C. Enable multi-factor authentication (MFA) for the root user.

D. Set a strong randomized password and store it in a secure location.

E. Create an access key ID and secret access key, and store them in a secure location.

F. Apply the following permissions boundary to the toot user:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "GRRESTRICTROOTUSER",
            "Effect": "Deny",
            "Action": "*",
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringLike": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::*:root"
                    ]
                }
            }
        }
    ]
}
```

A. Option A

B. Option B

C. Option C

D. Option D

E. Option E

F. Option F

Correct Answer: ACE

QUESTION 14

A security engineer is configuring a new website that is named example.com. The security engineer wants to secure communications with the website by requiring users to connect to example.com through HTTPS.

Which of the following is a valid option for storing SSL/TLS certificates?

A. Custom SSL certificate that is stored in AWS Key Management Service (AWS KMS)

B. Default SSL certificate that is stored in Amazon CloudFront.

C. Custom SSL certificate that is stored in AWS Certificate Manager (ACM)

D. Default SSL certificate that is stored in Amazon S3

Correct Answer: C

QUESTION 15

A security engineer needs to run an AWS CloudFormation script. The CloudFormation script builds AWS infrastructure to support a stack that includes web servers and a MySQL database. The stack has been deployed in pre-production environments and is ready for production.

The production script must comply with the principle of least privilege. Additionally, separation of duties must exist between the security engineer\\'s IAM account and CloudFormation.

Which solution will meet these requirements?

A. Use IAM Access Analyzer policy generation to generate a policy that allows the CloudFormation script to run and manage the stack. Attach the policy to a new IAM role. Modify the security engineer\\'s IAM permissions to be able to pass the new role to CloudFormation.

B. Create an IAM policy that allows ec2:* and rds:* permissions. Attach the policy to a new IAM role. Modify the security engineer\\'s IAM permissions to be able to assume the new role.

C. Use IAM Access Analyzer policy generation to generate a policy that allows the CloudFormation script to run and manage the stack. Modify the security engineer\\'s IAM permissions to be able to run the CloudFormation script.

D. Create an IAM policy that allows ec2:* and rds:* permissions. Attach the policy to a new IAM role. Use the IAM policy

simulator to confirm that the policy allows the AWS API calls that are necessary to build the stack. Modify the security engineer\\'s IAM permissions to be able to pass the new role to CloudFormation.

Correct Answer: A

According to the AWS documentation, IAM Access Analyzer is a service that helps you identify the resources in your organization and accounts, such as Amazon S3 buckets or IAM roles, that are shared with an external entity. You can also use IAM Access Analyzer to generate fine-grained policies that grant least privilege access based on access activity and access attempts. To use IAM Access Analyzer policy generation, you need to enable IAM Access Analyzer in your account or organization. You can then use the IAM console or the AWS CLI to generate a policy for a resource based on its access activity or access attempts. You can review and edit the generated policy before applying it to the resource. To use IAM Access Analyzer policy generation with CloudFormation, you can follow these steps: Run the CloudFormation script in a pre-production environment and monitor its access activity or access attempts using IAM Access Analyzer. Use IAM Access Analyzer policy generation to generate a policy that allows the CloudFormation script to run and manage the stack. The policy will include only the permissions that are necessary for the script to function. Attach the policy to a new IAM role that has a trust relationship with CloudFormation. This will allow CloudFormation to assume the role and execute the script. Modify the security engineer\\'s IAM permissions to be able to pass the new role to CloudFormation. This will allow the security engineer to launch the stack using the role. Run the CloudFormation script in the production environment using the new role. This solution will meet the requirements of least privilege and separation of duties, as it will limit the permissions of both CloudFormation and the security engineer to only what is needed for running and managing the stack. Option B is incorrect because creating an IAM policy that allows ec2:* and rds:* permissions is not following the principle of least privilege, as it will grant more permissions than necessary for running and managing the stack. Moreover, modifying the security engineer\\'s IAM permissions to be able to assume the new role is not ensuring separation of duties, as it will allow the security engineer to bypass CloudFormation and directly access the resources. Option C is incorrect because modifying the security engineer\\'s IAM permissions to be able to run the CloudFormation script is not ensuring separation of duties, as it will allow the security engineer to execute the script without using CloudFormation. Option D is incorrect because creating an IAM policy that allows ec2:* and rds:* permissions is not following the principle of least privilege, as it will grant more permissions than necessary for running and managing the stack. Using the IAM policy simulator to confirm that the policy allows the AWS API calls that are necessary to build the stack is not sufficient, as it will not generate a fine-grained policy based on access activity or access attempts.