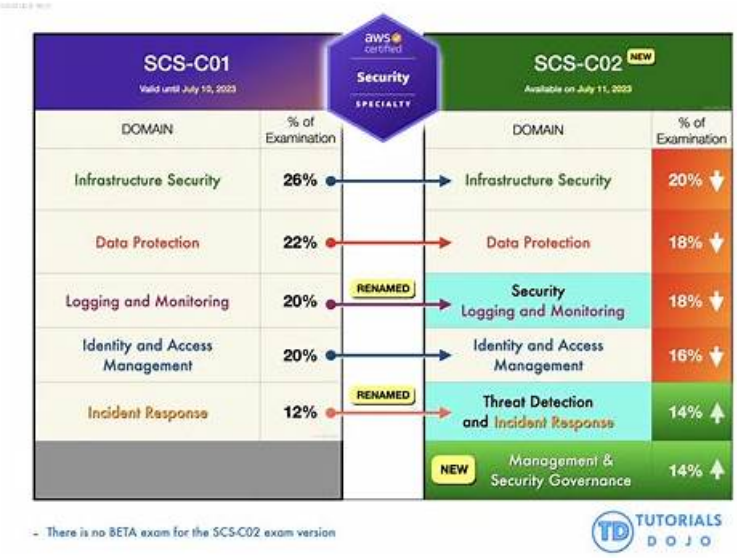
Salient Features of Desktop SCS-C02 AWS Certified Security - Specialty Practice Tests Software



P.S. Free & New SCS-C02 dumps are available on Google Drive shared by PDFTorrent: https://drive.google.com/open?id=1ZJ2YNMS2pARIctQr0Y2Dnj562wRluB0f

Thus you can study Amazon SCS-C02 on your preferred smart device such as your smartphone or in hard copy format. Once downloaded from the website, you can easily study from the Amazon SCS-C02 Exam Questions compiled by our highly experienced professionals as directed by the Amazon exam syllabus.

Amazon SCS-C02 Exam Syllabus Topics:

Topic	Details
Topic 1	• Management and Security Governance: This topic teaches AWS Security specialists to develop centralized strategies for AWS account management and secure resource deployment. It includes evaluating compliance and identifying security gaps through architectural reviews and cost analysis, essential for implementing governance aligned with certification standards.
Topic 2	• Security Logging and Monitoring: This topic prepares AWS Security specialists to design and implement robust monitoring and alerting systems for addressing security events. It emphasizes troubleshooting logging solutions and analyzing logs to enhance threat visibility.
Topic 3	• Identity and Access Management: The topic equips AWS Security specialists with skills to design, implement, and troubleshoot authentication and authorization mechanisms for AWS resources. By emphasizing secure identity management practices, this area addresses foundational competencies required for effective access control, a vital aspect of the certification exam.
Topic 4	• Infrastructure Security: Aspiring AWS Security specialists are trained to implement and troubleshoot security controls for edge services, networks, and compute workloads under this topic. Emphasis is placed on ensuring resilience and mitigating risks across AWS infrastructure. This section aligns closely with the exam's focus on safeguarding critical AWS services and environments.

>> Reliable SCS-C02 Test Testking <<

Free PDF Quiz Valid Amazon - SCS-C02 - Reliable AWS Certified Security -

Specialty Test Testking

Before you purchase our product you can have a free download and tryout of our SCS-C02 study tool. We provide the demo on our pages of our product on the websites and thus you have an understanding of part of our titles and the form of our SCS-C02 test torrent. We guarantee to you if you fail in we will refund you in full immediately and the process is simple. If only you provide us the screenshot or the scanning copy of the SCS-C02 failure marks we will refund you immediately. If you have doubts or other questions please contact us by emails or contact the online customer service and we will reply you and solve your problem as quickly as we can. So feel relieved when you buy our SCS-C02 guide torrent.

Amazon AWS Certified Security - Specialty Sample Questions (Q88-Q93):

NEW QUESTION # 88
A company needs to improve its ability to identify and prevent IAM policies that grant public access or cross-account access to resources. The company has implemented AWS Organizations and has started using AWS Identity and Access Management Access Analyzer to refine overly broad access to accounts in the organization.
A security engineer must automate a response in the company's organization for any newly created policies that are overly permissive. The automation must remediate external access and must notify the company's security team.
Which combination of steps should the security engineer take to meet these requirements? (Select THREE.)

- A. Create an Amazon Simple Notification Service (Amazon SNS) topic for external or cross-account access notices. Subscribe the security team's email addresses to the topic.
- B. Create an AWS Step Functions state machine that checks the resource type in the finding and adds an explicit Deny statement in the trust policy for the IAM role. Configure the state machine to publish a notification to an Amazon SimpleNotification Service (Amazon SNS) topic.
- C. In Amazon EventBridge, create an event rule that matches active IAM Access Analyzer findings and invokes AWS Step Functions for resolution.
- D. Create an AWS Batch job that forwards any resource type findings to an AWS Lambda function. Configure the Lambda function to add an explicit Deny statement in the trust policy for the IAM role. Configure the AWS Batch job to publish a notification to an Amazon Simple Notification Service (Amazon SNS) topic.
- E. In Amazon CloudWatch, create a metric filter that matches active IAM Access Analyzer findings and invokes AWS Batch for resolution.
- F. Create an Amazon Simple Queue Service (Amazon SQS) queue. Configure the queue to forward a notification to the security team that an external principal has been granted access to the specific IAM role and has been blocked.

Answer: A,B,C

Explanation:
The correct answer is A, C, and F.
To automate a response for any newly created policies that are overly permissive, the security engineer needs to use a combination of services that can monitor, analyze, remediate, and notify the security incidents.
Option A is correct because creating an AWS Step Functions state machine that checks the resource type in the finding and adds an explicit Deny statement in the trust policy for the IAM role is a valid way to remediate external access. AWS Step Functions is a service that allows you to coordinate multiple AWS services into serverless workflows. You can use Step Functions to invoke AWS Lambda functions, which can modify the IAM policies programmatically. You can also use Step Functions to publish a notification to an Amazon SNS topic, which can send messages to subscribers such as email addresses.
Option B is incorrect because creating an AWS Batch job that forwards any resource type findings to an AWS Lambda function is not a suitable way to automate a response. AWS Batch is a service that enables you to run batch computing workloads on AWS. Batch is designed for large-scale and long-running jobs that can benefit from parallelization and dynamic provisioning of compute resources. Batch is not intended for event-driven and real-time workflows that require immediate response.
Option C is correct because creating an Amazon EventBridge event rule that matches active IAM Access Analyzer findings and invokes AWS Step Functions for resolution is a valid way to monitor and analyze the security incidents. Amazon EventBridge is a serverless event bus service that allows you to connect your applications with data from various sources. EventBridge can use rules to match events and route them to targets for processing. You can use EventBridge to invoke AWS Step Functions state machines from the IAM Access Analyzer findings.
Option D is incorrect because creating an Amazon CloudWatch metric filter that matches active IAM Access Analyzer findings and invokes AWS Batch for resolution is not a suitable way to monitor and analyze the security incidents. Amazon CloudWatch is a service that provides monitoring and observability for your AWS resources and applications. CloudWatch can collect metrics, logs, and events from various sources and perform actions based on alarms or filters. However, CloudWatch cannot directly invoke AWS Batch jobs from the IAM Access Analyzer findings. You would need to use another service such as EventBridge or SNS to trigger the Batch job.
Option E is incorrect because creating an Amazon SQS queue that forwards a notification to the security team that an external

principal has been granted access to the specific IAM role and has been blocked is not a valid way to notify the security incidents. Amazon SQS is a fully managed message queue service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SQS can deliver messages to consumers that poll the queue for messages. However, SQS cannot directly forward a notification to the security team's email addresses. You would need to use another service such as SNS or SES to send email notifications.
Option F is correct because creating an Amazon SNS topic for external or cross-account access notices and subscribing the security team's email addresses to the topic is a valid way to notify the security incidents. Amazon SNS is a fully managed messaging service that enables you to decouple and scale microservices, distributed systems, and serverless applications. SNS can deliver messages to a variety of endpoints, such as email, SMS, or HTTP. You can use SNS to send email notifications to the security team when a critical security finding is detected.
Reference:
AWS Step Functions
AWS Batch
Amazon EventBridge
Amazon CloudWatch
Amazon SQS
Amazon SNS

NEW QUESTION # 89
A company is using Amazon Elastic Container Service (Amazon ECS) to run its container-based application on AWS. The company needs to ensure that the container images contain no severe vulnerabilities. The company also must ensure that only specific IAM roles and specific AWS accounts can access the container images.
Which solution will meet these requirements with the LEAST management overhead?

- A. Pull images from the public container registry. Publish the images to AWS CodeArtifact repositories in a centralized AWS account. Use a CI/CD pipeline to deploy the images to different AWS accounts. Use repository policies and identity-based policies to restrict access to which IAM principals and accounts can access the images.
- B. Pull images from the public container registry. Publish the images to Amazon Elastic Container Registry (Amazon ECR) repositories with scan on push configured in a centralized AWS account. Use a CI/CD pipeline to deploy the images to different AWS accounts. Use identity-based policies to restrict access to which IAM principals can access the images.
- C. Pull images from the public container registry. Publish the images to Amazon Elastic Container Registry (Amazon ECR) repositories with scan on push configured in a centralized AWS account. Use a CI/CD pipeline to deploy the images to different AWS accounts. Use repository policies and identity-based policies to restrict access to which IAM principals and accounts can access the images.
- D. Pull images from the public container registry. Publish the images to a private container registry that is hosted on Amazon EC2 instances in a centralized AWS account. Deploy host-based container scanning tools to EC2 instances that run Amazon ECS. Restrict access to the container images by using basic authentication over HTTPS.

Answer: C

Explanation:
The correct answer is C. Pull images from the public container registry. Publish the images to Amazon Elastic Container Registry (Amazon ECR) repositories with scan on push configured in a centralized AWS account.
Use a CI/CD pipeline to deploy the images to different AWS accounts. Use repository policies and identity-based policies to restrict access to which IAM principals and accounts can access the images.
This solution meets the requirements because:
* Amazon ECR is a fully managed container registry service that supports Docker and OCI images and artifacts1. It integrates with Amazon ECS and other AWS services to simplify the development and deployment of container-based applications.
* Amazon ECR provides image scanning on push, which uses the Common Vulnerabilities and Exposures (CVEs) database from the open-source Clair project to detect software vulnerabilities in container images2. The scan results are available in the AWS Management Console, AWS CLI, or AWS SDKs2.
* Amazon ECR supports cross-account access to repositories, which allows sharing images across
* multiple AWS accounts3. This can be achieved by using repository policies, which are resource-based policies that specify which IAM principals and accounts can access the repositories and what actions they can perform4. Additionally, identity-based policies can be used to control which IAM roles in each account can access the repositories5.
The other options are incorrect because:
* A. This option does not use repository policies to restrict cross-account access to the images, which is a requirement. Identity-based policies alone are not sufficient to control access to Amazon ECR repositories5.
* B. This option does not use Amazon ECR, which is a fully managed service that provides image scanning and cross-account access features. Hosting a private container registry on EC2 instances would require more management overhead and additional

security measures.
* D. This option uses AWS CodeArtifact, which is a fully managed artifact repository service that supports Maven, npm, NuGet, PyPI, and generic package formats6. However, AWS CodeArtifact does not support Docker or OCI container images, which are required for Amazon ECS applications.

NEW QUESTION # 90
A company is undergoing a layer 3 and layer 4 DDoS attack on its web servers running on AWS.
Which combination of AWS services and features will provide protection in this scenario?
(Choose three.)

- A. AWS Shield
- B. Amazon S3
- C. Amazon Route 53
- D. AWS Certificate Manager (ACM)
- E. Network Load Balancer
- F. Amazon GuardDuty

Answer: A,C,E

NEW QUESTION # 91
A development team is attempting to encrypt and decode a secure string parameter from the IAM Systems Manager Parameter Store using an IAM Key Management Service (IAM KMS) CMK. However, each attempt results in an error message being sent to the development team.
Which CMK-related problems possibly account for the error? (Select two.)

- A. The CMK is used in the attempt needs to be rotated.
- B. The CMK is used in the attempt does not exist.
- C. The CMK is used in the attempt is using an alias.
- D. The CMK is used in the attempt is using the CMKs key ID instead of the CMK ARN.
- E. The CMK is used in the attempt is not enabled.

Answer: B,E

Explanation:
Explanation
https://docs.IAM.amazon.com/kms/latest/developerguide/services-parameter-store.html#parameter-store-cmk-fa

NEW QUESTION # 92
A security team is developing an application on an Amazon EC2 instance to get objects from an Amazon S3 bucket. All objects in the S3 bucket are encrypted with an AWS Key Management Service (AWS KMS) customer managed key. All network traffic for requests that are made within the VPC is restricted to the AWS infrastructure. This traffic does not traverse the public internet.
The security team is unable to get objects from the S3 bucket
Which factors could cause this issue? (Select THREE.)

- A. The I AM instance profile that is attached to the EC2 instance does not allow the s3 ListParts action to the S3; bucket in the AWS accounts.
- B. The KMS key policy that encrypts the object in the S3 bucket does not allow the kms Decrypt action to the EC2 instance profile ARN.
- C. The security group that is attached to the EC2 instance is missing an outbound rule to the S3 managed prefix list over port 443.
- D. The KMS key policy that encrypts the object in the S3 bucket does not allow the kms; ListKeys action to the EC2 instance profile ARN.
- E. The IAM instance profile that is attached to the EC2 instance does not allow the s3 ListBucket action to the S3: bucket in the AWS accounts.
- F. The security group that is attached to the EC2 instance is missing an inbound rule from the S3 managed prefix list over port 443.

Answer: B,C,E

Explanation:
https://docs.aws.amazon.com/vpc/latest/userguide/security-group-rules.html To get objects from an S3 bucket that are encrypted with a KMS customer managed key, the security team needs to have the following factors in place:
The IAM instance profile that is attached to the EC2 instance must allow the s3:GetObject action to the S3 bucket or object in the AWS account. This permission is required to read the object from S3. Option A is incorrect because it specifies the s3:ListBucket action, which is only required to list the objects in the bucket, not to get them.
The KMS key policy that encrypts the object in the S3 bucket must allow the kms:Decrypt action to the EC2 instance profile ARN. This permission is required to decrypt the object using the KMS key. Option D is correct.
The security group that is attached to the EC2 instance must have an outbound rule to the S3 managed prefix list over port 443. This rule is required to allow HTTPS traffic from the EC2 instance to S3 within the AWS infrastructure. Option E is correct. Option B is incorrect because it specifies the s3:ListParts action, which is only required for multipart uploads, not for getting objects. Option C is incorrect because it specifies the kms:ListKeys action, which is not required for getting objects. Option F is incorrect because it specifies an inbound rule from the S3 managed prefix list, which is not required for getting objects. Verified Reference:
https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingKMSEncryption.html
https://docs.aws.amazon.com/kms/latest/developerguide/control-access.html
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints-s3.html

NEW QUESTION # 93
.....

Our SCS-C02 test prep embrace latest information, up-to-date knowledge and fresh ideas, encouraging the practice of thinking out of box rather than treading the same old path following a beaten track. As the industry has been developing more rapidly, our SCS-C02 exam dumps have to be updated at irregular intervals in case of keeping pace with changes. To give you a better using environment, our experts have specialized in the technology with the system upgraded to offer you the latest SCS-C02 Exam practices. And you can enjoy free updates of our SCS-C02 learning prep for one year.

SCS-C02 Reliable Exam Cram: https://www.pdftorrent.com/SCS-C02-exam-prep-dumps.html

- New SCS-C02 Test Duration □ SCS-C02 Braindump Free □ SCS-C02 Sample Exam □ ▹ www.vce4dumps.com ◃ is best website to obtain { SCS-C02 } for free download □SCS-C02 Dumps Free
- SCS-C02 Dumps Free □ SCS-C02 Dumps Free □ New SCS-C02 Exam Testking □ Search for { SCS-C02 } and easily obtain a free download on " www.pdfvce.com " □SCS-C02 Answers Real Questions
- SCS-C02 Dumps Free □ Exam SCS-C02 Collection Pdf □ SCS-C02 Braindump Free □ Copy URL " www.validtorrent.com " open and search for □ SCS-C02 □ to download for free □SCS-C02 New Question
- 100% Pass 2026 Amazon Fantastic SCS-C02: Reliable AWS Certified Security - Specialty Test Testking □ Open ⇛ www.pdfvce.com ⇚ enter " SCS-C02 " and obtain a free download □Valid Dumps SCS-C02 Ebook
- SCS-C02 Sample Exam □ SCS-C02 Reliable Test Review □ Valid Dumps SCS-C02 Ebook □ Go to website □ www.prepawayete.com □ open and search for □ SCS-C02 □ to download for free □SCS-C02 Sample Exam
- 100% Pass 2026 Amazon Fantastic SCS-C02: Reliable AWS Certified Security - Specialty Test Testking □ Search on （ www.pdfvce.com ） for 【 SCS-C02 】 to obtain exam materials for free download □SCS-C02 New Question
- Realistic Reliable SCS-C02 Test Testking - Easy and Guaranteed SCS-C02 Exam Success □ Search for □ SCS-C02 □ and download it for free on □ www.examcollectionpass.com □ website □SCS-C02 Latest Exam Pattern
- SCS-C02 Reliable Test Review □ SCS-C02 Latest Exam Pattern □ SCS-C02 Sample Exam □ Easily obtain □ SCS-C02 □ for free download through 「 www.pdfvce.com 」 □SCS-C02 New Dumps
- Pass Guaranteed SCS-C02 - AWS Certified Security - Specialty Newest Reliable Test Testking □ Enter ➽ www.vce4dumps.com □ and search for ✔ SCS-C02 □✔□ to download for free □SCS-C02 Dumps Free
- New SCS-C02 Exam Testking □ New SCS-C02 Test Duration □ Relevant SCS-C02 Exam Dumps □ Search for " SCS-C02 " on " www.pdfvce.com " immediately to obtain a free download □Relevant SCS-C02 Exam Dumps
- SCS-C02 practice questions - SCS-C02 latest torrent - SCS-C02 training material □ Easily obtain free download of 《 SCS-C02 》 by searching on ➽ www.examcollectionpass.com □ □SCS-C02 Latest Exam Pattern
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, Disposable vapes

BONUS!!! Download part of PDFTorrent SCS-C02 dumps for free: https://drive.google.com/open?id=1ZJ2YNMS2pARIctQr0Y2Dnj562wRluB0f