SCS-C02 Best Preparation Materials, SCS-C02 Relevant Exam Dumps

P.S. Free & New SCS-C02 dumps are available on Google Drive shared by ValidBraindumps: https://drive.google.com/open?id=1Sx68etfqaA8NMYEwucVAF_BCUFPQT7Mu

These days the ValidBraindumps is providing you online Amazon SCS-C02 exam questions to crack the Amazon SCS-C02 certification exam which means you don't need to be physically present anywhere except the chair at your home. You need a laptop and an active internet connection to access the ValidBraindumps Amazon SCS-C02 Exam Questions and practice exam.

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	• 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 3	• 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.
Topic 4	• 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.

>> SCS-C02 Best Preparation Materials <<

SCS-C02 Best Preparation Materials - High Pass-Rate Amazon AWS Certified Security - Specialty - SCS-C02 Relevant Exam Dumps

You will be able to assess your shortcomings and improve gradually without having anything to lose in the actual AWS Certified Security - Specialty exam. You will sit through mock exams and solve actual Amazon SCS-C02 dumps. In the end, you will get results that'll improve each time you progress and grasp the concepts of your syllabus. The desktop-based Amazon SCS-C02 Practice Exam software is only compatible with Windows.

Amazon AWS Certified Security - Specialty Sample Questions (Q358-Q363):

NEW QUESTION # 358
A company needs to delect unauthenticated access to its Amazon Elastic Kubernetes Service (Amazon EKS) clusters. The company needs a solution that requires no additional configuration ot the existing EKS deployment.
Which solution will meet these requirements with the LEAST operational effort?

- A. Install an Amazon EKS add-on from a security vendor.
- B. Monitor Amazon CloudWatch Container Insights metrics for Amazon EKS.
- C. Enable Amazon GuardDuty Use EKS Audit Log Monitoring.
- D. Enable AWS Security Hub Monitor the Kubernetes findings

Answer: C

Explanation:
* Enable GuardDuty:
* GuardDuty provides monitoring for EKS clusters by analyzing EKS audit logs.
* Automatic Configuration:
* No additional setup for the EKS deployment is needed. GuardDuty directly monitors API calls to detect suspicious or unauthenticated access.
* Advantages:
* Minimal Effort: No operational overhead for configuration.
* Proactive Detection: Alerts for unauthorized or suspicious activity in near-real-time.
Amazon GuardDuty for EKS
EKS Audit Log Monitoring

NEW QUESTION # 359
A company has a new partnership with a vendor. The vendor will process data from the company's customers. The company will upload data files as objects into an Amazon S3 bucket. The vendor will download the objects to perform data processing. The objects will contain sensi-tive data.
A security engineer must implement a solution that prevents objects from resid-ing in the S3 bucket for longer than 72 hours.
Which solution will meet these requirements?

- A. Use the S3 Intelligent-Tiering storage class for all objects that are up-loaded to the S3 bucket. Use S3 Intelligent-Tiering to expire objects that have been in the S3 bucket for 72 hours.
- B. Use Amazon Macie to scan the S3 bucket for sensitive data every 72 hours. Configure Macie to delete the objects that contain sensitive data when they are discovered.
- C. Configure an S3 Lifecycle rule on the S3 bucket to expire objects that have been in the S3 bucket for 72 hours.
- D. Create an Amazon EventBridge scheduled rule that invokes an AWS Lambda function every day. Program the Lambda function to remove any objects that have been in the S3 bucket for 72 hours.

Answer: C

NEW QUESTION # 360
A company has implemented IAM WAF and Amazon CloudFront for an application. The application runs on Amazon EC2 instances that are part of an Auto Scaling group. The Auto Scaling group is behind an Application Load Balancer (ALB).

The IAM WAF web ACL uses an IAM Managed Rules rule group and is associated with the CloudFront distribution. CloudFront receives the request from IAM WAF and then uses the ALB as the distribution's origin.
During a security review, a security engineer discovers that the infrastructure is susceptible to a large, layer 7 DDoS attack.
How can the security engineer improve the security at the edge of the solution to defend against this type of attack?

- A. Configure the IAM WAF web ACL so that the web ACL has more capacity units to process all IAM WAF rules faster.
- B. Configure IAM WAF with a rate-based rule that imposes a rate limit that automatically blocks requests when the rate limit is exceeded.
- C. Configure the CloudFront distribution to use IAM WAF as its origin instead of the ALB.
- D. Configure the CloudFront distribution to use the Lambda@Edge feature. Create an IAM Lambda function that imposes a rate limit on CloudFront viewer requests. Block the request if the rate limit is exceeded.

Answer: B

Explanation:
To improve the security at the edge of the solution to defend against a large, layer 7 DDoS attack, the security engineer should do the following:
Configure AWS WAF with a rate-based rule that imposes a rate limit that automatically blocks requests when the rate limit is exceeded. This allows the security engineer to use a rule that tracks the number of requests from a single IP address and blocks subsequent requests if they exceed a specified threshold within a specified time period.

NEW QUESTION # 361
A company has an organization with SCPs in AWS Organizations. The root SCP for the organization is as follows:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsAllActions",
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
        },
        {
            "Sid": "DenySES",
            "Effect": "Deny",
            "Action": "ses:*",
            "Resource": "*"
        }
    ]
}
```


The company's developers are members of a group that has an IAM policy that allows access to Amazon Simple Email Service (Amazon SES) by allowing ses:* actions. The account is a child to an OU that has an SCP that allows Amazon SES. The developers are receiving a not-authorized error when they try to access Amazon SES through the AWS Management Console.
Which change must a security engineer implement so that the developers can access Amazon SES?

- A. Remove the AWS Control Tower control (guardrail) that restricts access to Amazon SES.
- B. Add a resource policy that allows "Principal": {"AWS": "arn:aws:iam::account-number:group/Dev"}.
- C. Remove Amazon SES from the root SCP.
- D. Add a resource policy that allows each member of the group to access Amazon SES.

Answer: C

Explanation:
The correct answer is D. Remove Amazon SES from the root SCP.
This answer is correct because the root SCP is the most restrictive policy that applies to all accounts in the organization. The root SCP explicitly denies access to Amazon SES by using the NotAction element, which means that any action that is not listed in the element is denied. Therefore, removing Amazon SES from the root SCP will allow the developers to access it, as long as there are no other SCPs or IAM policies that deny it.
The other options are incorrect because:
* A.Adding a resource policy that allows each member of the group to access Amazon SES is not a solution, because resource policies are not supported by Amazon SES1.Resource policies are policies that are attached to AWS resources, suchas S3 buckets or SNS topics, to control access to those resources2. Amazon SES does not have any resources that can have resource policies attached to them.
* B.Adding a resource policy that allows "Principal": {"AWS": "arn:aws:iam::account-number:group /Dev"} is not a solution, because resource policies do not support IAM groups asprincipals3.Principals are entities that can perform actions on AWS resources, such as IAM users, roles, or AWSaccounts4.
IAM groups are not principals, but collections of IAM users that share the same permissions5.
* C.Removing the AWS Control Tower control (guardrail) that restricts access to Amazon SES is not a solution, because AWS Control Tower does not have any guardrails that restrict access to Amazon SES6.Guardrails are high-level rules that govern the overall behavior of an organization's accounts7.
AWS Control Tower provides a set of predefined guardrails that cover security, compliance, and operations domains8.
References:
1: Amazon Simple Email Service endpoints and quotas2: Resource-based policies and IAM policies3: Specifying a principal in a policy4: Policy elements: Principal5: IAM groups6: AWS Control Tower guardrails reference7: AWS Control Tower concepts8: AWS Control Tower guardrails

NEW QUESTION # 362
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 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.
- B. 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.
- C. In Amazon CloudWatch, create a metric filter that matches active IAM Access Analyzer findings and invokes AWS Batch for resolution.
- D. In Amazon EventBridge, create an event rule that matches active IAM Access Analyzer findings and invokes AWS Step Functions for resolution.
- E. 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.
- 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,D,E

Explanation:
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.
References:
AWS Step Functions
AWS Batch
Amazon EventBridge
Amazon CloudWatch
Amazon SQS
Amazon SNS

NEW QUESTION # 363
.....

One of the most important functions of our SCS-C02 preparation questions are that can support almost all electronic equipment, including the computer, mobile phone and so on. If you want to prepare for your exam by the computer, you can buy the Software and APP online versions of our SCS-C02 training quiz, because these two versions can work well by the computer. Moreover, the APP online version of our SCS-C02 learning materials can also apply the IPAD, phone, laptop and so on.

www.pdfvce.com □☀□ for ➠ SCS-C02 □ to obtain exam materials for free download □SCS-C02 Latest Test Question

- SCS-C02 Latest Test Question □ SCS-C02 Reliable Exam Testking □ SCS-C02 Exam Simulations □ Immediately open 「 www.examdiscuss.com 」 and search for ⇛ SCS-C02 ⇚ to obtain a free download □Reliable SCS-C02 Practice Materials
- SCS-C02 Latest Test Question □ SCS-C02 Exam Paper Pdf □ Reliable SCS-C02 Exam Vce □ Open website （ www.pdfvce.com ） and search for ➤ SCS-C02 □ for free download □Certification SCS-C02 Test Answers
- SCS-C02 Reliable Test Topics □ SCS-C02 Latest Test Question □ Reliable SCS-C02 Practice Materials □ Search for 《 SCS-C02 》 and easily obtain a free download on ➠ www.exam4pdf.com □ □SCS-C02 Latest Mock Exam
- marb45.com, www.stes.tyc.edu.tw, rdcvw.q711.myverydz.cn, royaaacademy.com.au, bloomingcareerss.com, 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, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, theapra.org, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, kareyed271.dailyhitblog.com, Disposable vapes

BONUS!!! Download part of ValidBraindumps SCS-C02 dumps for free: https://drive.google.com/open?id=1Sx68etfqaA8NMYEwucVAF_BCUFPQT7Mu