SCS-C01 Q&As

AWS Certified Security - Specialty (SCS-C01)

Pass Amazon SCS-C01 Exam with 100% Guarantee

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

https://www.leads4pass.com/aws-certified-security-specialty.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

Your company looks at the gaming domain and hosts several Ec2 Instances as game servers. The servers each experience user loads in the thousands. There is a concern of DDos attacks on the EC2 Instances which could cause a huge revenue loss to the company. Which of the following can help mitigate this security concern and also ensure minimum downtime for the servers.

Please select:

A. Use VPC Flow logs to monitor the VPC and then implement NACL\\'s to mitigate attacks

B. Use AWS Shield Advanced to protect the EC2 Instances

C. Use AWS Inspector to protect the EC2 Instances

D. Use AWS Trusted Advisor to protect the EC2 Instances

Correct Answer: B

Below is an excerpt from the AWS Documentation on some of the use cases for AWS Shield

VPN Connections

You can connect your Amazon VPC to remote networks by using a VPN connection. The following are some of the connectivity options available to you.

VPN connectivity option	Description
AWS managed VPN	You can create an IPsec VPN connection between your VPC and your remote network. On the AWS side of the VPN connection, a *virtual private gateway* provides two VPN endpoints (tunnels) for automatic failover. You configure your *customer gateway* on the remote side of the VPN connection. For more information, see AWS Managed VPN Connections, and the Amazon VPC Network Administrator Guide.
AWS VPN CloudHub	If you have more than one remote network (for example, multiple branch offices), you can create multiple AWS managed VPN connections via your virtual private gateway to enable communication between these networks. For more information, see Providing Secure Communication Between Sites Using VPN CloudHub.
Third party software VPN appliance	You can create a VPN connection to your remote network by using an Amazon EC2 instance in your VPC that's running a third party software VPN appliance. AWS does not provide or maintain third party software VPN appliances; however, you can choose from a range of products provided by partners and open source communities. Find third party software VPN appliances on the AWS Marketplace.

You can also use AWS Direct Connect to create a dedicated private connection from a remote network to your VPC. You can combine this connection with an AWS managed VPN connection to create an IPsec-encrypted connection. For more information, see What is AWS Direct Connect? in the *AWS Direct Connect User Guide*. For more information about the different VPC and VPN connectivity options, see the Amazon Virtual Private Cloud Connectivity Options whitepaper.

QUESTION 2

A company has a legacy application that runs on a single Amazon EC2 instance. A security audit shows that the application has been using an IAM access key within its code to access an Amazon S3 bucket that is named DOC-EXAMPLEBUCKET1 in the same AWS account. This access key pair has the s3:GetObject permission to all objects in only this S3 bucket. The company takes the application offline because the application is not compliant with the company\\'s security policies for accessing other AWS resources from Amazon EC2.

A security engineer validates that AWS CloudTrail is turned on in all AWS Regions. CloudTrail is sending logs to an S3 bucket that is named DOC-EXAMPLE-BUCKET2. This S3 bucket is in the same AWS account as DOC-EXAMPLEBUCKET1. However, CloudTrail has not been configured to send logs to Amazon CloudWatch Logs.

The company wants to know if any objects in DOC-EXAMPLE-BUCKET1 were accessed with the IAM access key in the

past 60 days. If any objects were accessed, the company wants to know if any of the objects that are text files (.txt extension) contained personally identifiable information (PII).

Which combination of steps should the security engineer take to gather this information? (Choose two.)

A. Configure Amazon Macie to identify any objects in DOC-EXAMPLE-BUCKET1 that contain PII and that were available to the access key.

B. Use Amazon CloudWatch Logs Insights to identify any objects in DOC-EXAMPLE-BUCKET1 that contain PII and that were available to the access key.

C. Use Amazon OpenSearch Service (Amazon Elasticsearch Service) to query the CloudTrail logs in DOC-EXAMPLE-BUCKET2 for API calls that used the access key to access an object that contained PII.

D. Use Amazon Athena to query the CloudTrail logs in DOC-EXAMPLE-BUCKET2 for any API calls that used the access key to access an object that contained PII.

E. Use AWS Identity and Access Management Access Analyzer to identify any API calls that used the access key to access objects that contained PII in DOC-EXAMPLE-BUCKET1.

Correct Answer: DE

QUESTION 3

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?

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.

Correct Answer: B

MetricFilter:

Type: \\'AWS::Logs::MetricFilter\\'

Properties:

LogGroupName: \\'\\'

FilterPattern: >{ ($.eventName = AuthorizeSecurityGroupIngress) || ($.eventName = AuthorizeSecurityGroupEgress) || ($.eventName =

RevokeSecurityGroupIngress) || ($.eventName = RevokeSecurityGroupEgress) || ($.eventName = CreateSecurityGroup) || ($.eventName = DeleteSecurityGroup) } MetricTransformations:

-MetricValue: \\'1\\' MetricNamespace: CloudTrailMetrics MetricName: SecurityGroupEventCount

QUESTION 4

You need to have a requirement to store objects in an S3 bucket with a key that is automatically managed and rotated. Which of the following can be used for this purpose?

Please select:

A. AWS KMS

B. AWS S3 Server side encryption

C. AWS Customer Keys

D. AWS Cloud HSM

Correct Answer: B

The AWS Documentation mentions the following Server-side encryption protects data at rest. Server-side encryption with Amazon S3- managed encryption keys (SSE-S3) uses strong multi-factor encryption. Amazon S3 encrypts each object

with a unique key. As an additional safeguard, it encrypts the key itself with a master key that it rotates regularly. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard

(AES- 256), to encrypt your data.

All other options are invalid since here you need to ensure the keys are manually rotated since you manage the entire key set Using AWS S3 Server side encryption, AWS will manage the rotation of keys automatically.

For more information on Server side encryption, please visit the following URL:

https://docs.aws.amazon.com/AmazonS3/latest/dev/UsineServerSideEncryption.htmll The correct answer is: AWS S3 Server side encryption

QUESTION 5

A water utility company uses a number of Amazon EC2 instances to manage updates to a fleet of 2,000 Internet of Things (IoT) field devices that monitor water quality. These devices each have unique access credentials.

An operational safety policy requires that access to specific credentials is independently auditable.

What is the MOST cost-effective way to manage the storage of credentials?

A. Use AWS Systems Manager to store the credentials as Secure Strings Parameters.Secure by using an AWS KMS key.

B. Use AWS Key Management System to store a master key, which is used to encrypt the credentials. The encrypted

credentials are stored in an Amazon RDS instance.

C. Use AWS Secrets Manager to store the credentials.

D. Store the credentials in a JSON file on Amazon S3 with server-side encryption.

Correct Answer: A

https://docs.aws.amazon.com/systems-manager/latest/userguide/parameter-store-advanced-parameters.html