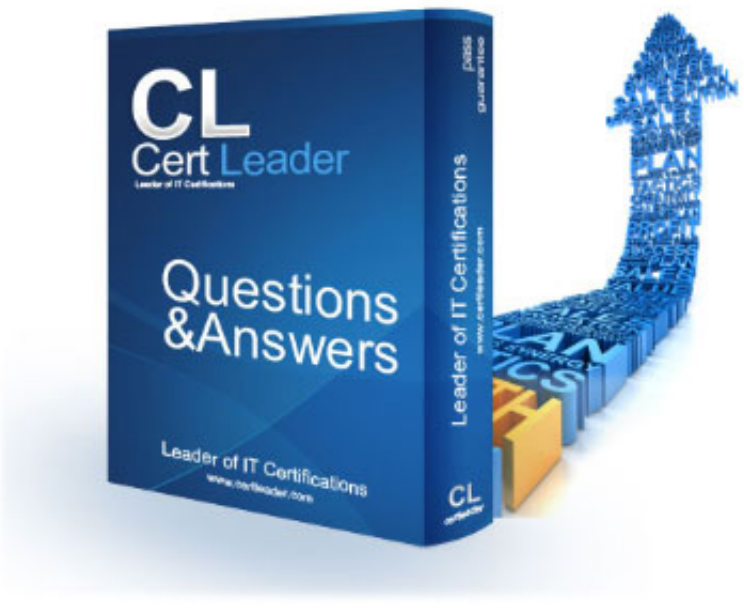
SCS-C03 Dumps

AWS Certified Security - Specialty

https://www.certleader.com/SCS-C03-dumps.html



NEW QUESTION 1
AWS Config cannot deliver configuration snapshots to Amazon S3. Which TWO actions will remediate this issue?

A. Verify the S3 bucket policy allows config.amazonaws.com.
B. Verify the IAM role has s3:GetBucketAcl and s3:PutObject permissions.
C. Verify the S3 bucket can assume the IAM role.
D. Verify IAM policy allows AWS Config to write logs.
E. Modify AWS Config API permissions.

Answer: AB

NEW QUESTION 2
A company uses AWS Organizations to manage an organization that consists of three workload OUs: Production, Development, and Testing. The company uses AWS CloudFormation templates to define and deploy workload infrastructure in AWS accounts that are associated with the OUs. Different SCPs are attached to each workload OU.
The company successfully deployed a CloudFormation stack update to workloads in the Development OU and the Testing OU. When the company uses the same CloudFormation template to deploy the stack update in an account in the Production OU, the update fails.
The error message reports insufficient IAM permissions.
What is the FIRST step that a security engineer should take to troubleshoot this issue?

A. Review the AWS CloudTrail logs in the account in the Production O
B. Search for any failed API calls from CloudFormation during the deployment attempt.
C. Remove all the SCPs that are attached to the Production O
D. Rerun the CloudFormation stack update to determine if the SCPs were preventing the CloudFormation API calls.
E. Confirm that the role used by CloudFormation has sufficient permissions to create, update, and delete the resources that are referenced in the CloudFormation template.
F. Make all the SCPs that are attached to the Production OU the same as the SCPs that are attached to the Testing OU.

Answer: A

NEW QUESTION 3
A company has a web application that reads from and writes to an Amazon S3 bucket. The company needs to use AWS credentials to authenticate all S3 API calls to the S3 bucket. Which solution will provide the application with AWS credentials to make S3 API calls?

A. Integrate with Cognito identity pools and use GetId to obtain AWS credentials.
B. Integrate with Cognito identity pools and use AssumeRoleWithWebIdentity to obtain AWS credentials.
C. Integrate with Cognito user pools and use the ID token to obtain AWS credentials.
D. Integrate with Cognito user pools and use the access token to obtain AWS credentials.

Answer: B

NEW QUESTION 4
A company hosts its public website on Amazon EC2 instances behind an Application Load Balancer (ALB). The website is experiencing a global DDoS attack from a specific IoT device brand that uses a unique user agent. A security engineer is creating an AWS WAF web ACL and will associate it with the ALB.
Which rule statement will mitigate the current attack and future attacks from these IoT devices without blocking legitimate customers?

A. Use an IP set match rule statement.
B. Use a geographic match rule statement.
C. Use a rate-based rule statement.
D. Use a string match rule statement on the user agent.

Answer: D

NEW QUESTION 5
A company??s developers are using AWS Lambda function URLs to invoke functions directly. The company must ensure that developers cannot configure or deploy unauthenticated functions inproduction accounts. The company wants to meet this requirement by using AWS Organizations. The solution must not require additional work for the developers.
Which solution will meet these requirements?

A. Require the developers to configure all function URLs to support cross-origin resource sharing (CORS) when the functions are called from a different domain.
B. Use an AWS WAF delegated administrator account to view and block unauthenticated access to function URLs in production accounts, based on the OU of accounts that are using the functions.
C. Use SCPs to allow all lambda:CreateFunctionUrlConfig and lambda:UpdateFunctionUrlConfig actions that have a lambda:FunctionUrlAuthType condition key value of AWS_IAM.
D. Use SCPs to deny all lambda:CreateFunctionUrlConfig and lambda:UpdateFunctionUrlConfig actions that have a lambda:FunctionUrlAuthType condition key value of NONE.

Answer: D

NEW QUESTION 6
A company??s application team needs a new AWS Key Management Service (AWS KMS) customer managed key to use with Amazon S3. The company??s security policy requires separate keys for different AWS services to limit security exposure.
How can a security engineer limit the KMS customer managed key to work with only Amazon S3?

A. Configure the key policy to allow only Amazon S3 to perform the kms:Encrypt action.
B. Configure the key policy to allow KMS actions only when the value for the kms:ViaService condition key matches the Amazon S3 service name.

C. Configure the application??s IAM role policy to allow Amazon S3 to perform the iam:PassRole action.
D. Configure the application??s IAM role policy to allow only S3 operations when the operations are combined with the KMS customer managed key.

Answer: B

NEW QUESTION 7
A company's security team wants to receive near-real-time email notifications about AWS abuse reports related to DoS attacks. An Amazon SNS topic already exists and is subscribed to by the security team.
What should the security engineer do next?

A. Poll Trusted Advisor for abuse notifications by using a Lambda function.
B. Create an Amazon EventBridge rule that matches AWS Health events for AWS_ABUSE_DOS_REPORT and publishes to SNS.
C. Poll the AWS Support API for abuse cases by using a Lambda function.
D. Detect abuse reports by using CloudTrail logs and CloudWatch alarms.

Answer: B

NEW QUESTION 8
A company's security engineer receives an abuse notification from AWS indicating that malware is being hosted from the company??s AWS account. The security engineer discovers that an IAM user created a new Amazon S3 bucket without authorization.
Which combination of steps should the security engineer take to MINIMIZE the consequences of this compromise? (Select THREE.)

A. Encrypt all AWS CloudTrail logs.
B. Turn on Amazon GuardDuty.
C. Change the password for all IAM users.
D. Rotate or delete all AWS access keys.
E. Take snapshots of all Amazon Elastic Block Store (Amazon EBS) volumes.
F. Delete any resources that are unrecognized or unauthorized.

Answer: BDF

NEW QUESTION 9
A security engineer wants to forward custom application-security logs from an Amazon EC2 instance to Amazon CloudWatch. The security engineer installs the CloudWatch agent on the EC2 instance and adds the path of the logs to the CloudWatch configuration file.
However, CloudWatch does not receive the logs. The security engineer verifies that the awslogs service is running on the EC2 instance.
What should the security engineer do next to resolve the issue?

A. Add AWS CloudTrail to the trust policy of the EC2 instanc
B. Send the custom logs to CloudTrail instead of CloudWatch.
C. Add Amazon S3 to the trust policy of the EC2 instanc
D. Configure the application to write the custom logs to an S3 bucket that CloudWatch can use to ingest the logs.
E. Add Amazon Inspector to the trust policy of the EC2 instanc
F. Use Amazon Inspector instead of the CloudWatch agent to collect the custom logs.
G. Attach the CloudWatchAgentServerPolicy AWS managed policy to the EC2 instance role.

Answer: D

NEW QUESTION 10
An application is running on an Amazon EC2 instance that has an IAM role attached. The IAM role provides access to an AWS Key Management Service (AWS KMS) customer managed key and an Amazon S3 bucket. The key is used to access 2 TB of sensitive data that is stored in the S3 bucket. A security engineer discovers a potential vulnerability on the EC2 instance that could result in the compromise of the sensitive data. Due to other critical operations, the security engineer cannot immediately shut down the EC2 instance for vulnerability patching.
What is the FASTEST way to prevent the sensitive data from being exposed?

A. Download the data from the existing S3 bucket to a new EC2 instanc
B. Then delete the data from the S3 bucke
C. Re-encrypt the data with a client-based ke
D. Upload the data to a new S3 bucket.
E. Block access to the public range of S3 endpoint IP addresses by using a host-based firewal
F. Ensure that internet-bound traffic from the affected EC2 instance is routed through the host-based firewall.
G. Revoke the IAM role??s active session permission
H. Update the S3 bucket policy to deny access to the IAM rol
I. Remove the IAM role from the EC2 instance profile.
J. Disable the current ke
K. Create a new KMS key that the IAM role does not have access to, and re-encrypt all the data with the new ke
L. Schedule the compromised key for deletion.

Answer: C

NEW QUESTION 10
A company uses AWS IAM Identity Center to manage access to its AWS accounts. The accounts are in an organization in AWS Organizations. A security engineer needs to set up delegated administration of IAM Identity Center in the organization??s management account.
Which combination of steps should the security engineer perform in IAM Identity Center before configuring delegated administration? (Select THREE.)

A. Grant least privilege access to the organization's management account.
B. Create a new IAM Identity Center directory in the organization's management account.
C. Set up a second AWS Region in the organization??s management account.
D. Create permission sets for use only in the organization's management account.

E. Create IAM users for use only in the organization's management account.
F. Create user assignments only in the organization's management account.

Answer: BDF

NEW QUESTION 11
A company is running its application on AWS. The company has a multi-environment setup, and each environment is isolated in a separate AWS account. The company has an organization in AWS Organizations to manage the accounts. There is a single dedicated security account for the organization. The company must create an inventory of all sensitive data that is stored in Amazon S3 buckets across the organization's accounts. The findings must be visible from a single location.
Which solution will meet these requirements?

A. Set the security account as the delegated administrator for Amazon Macie and AWS Security Hu
B. Enable and configure Macie to publish sensitive data findings to Security Hub.
C. Set the security account as the delegated administrator for AWS Security Hu
D. In each account, configure Amazon Inspector to scan the S3 buckets for sensitive dat
E. Publish sensitive data findings to Security Hub.
F. In each account, configure Amazon Inspector to scan the S3 buckets for sensitive dat
G. Enable Amazon Inspector integration with AWS Trusted Adviso
H. Publish sensitive data findings to Trusted Advisor.
I. In each account, enable and configure Amazon Macie to detect sensitive dat
J. Enable Macie integration with AWS Trusted Adviso
K. Publish sensitive data findings to Trusted Advisor.

Answer: A

NEW QUESTION 15
A company needs to build a code-signing solution using an AWS KMS asymmetric key and must store immutable evidence of key creation and usage for compliance and audit purposes.
Which solution meets these requirements?

A. Create an Amazon S3 bucket with S3 Object Lock enable
B. Create an AWS CloudTrail trail with log file validation enabled for KMS event
C. Store logs in the bucket and grant auditors access.
D. Log application events to Amazon CloudWatch Logs and export them.
E. Capture KMS API calls using EventBridge and store them in DynamoDB.
F. Track KMS usage with CloudWatch metrics and dashboards.

Answer: A

NEW QUESTION 20
A company uses AWS IAM Identity Center with SAML 2.0 federation. The company decides to change its federation source from one identity provider (IdP) to another. The underlying directory for both IdPs is Active Directory.
Which solution will meet this requirement?

A. Disable all existing users and groups within IAM Identity Center that were part of thefederation with the original IdP.
B. Modify the attribute mappings within the IAM Identity Center trust relationship to match information that the new IdP sends.
C. Reconfigure all existing IAM roles in the company's AWS accounts to explicitly trust the new IdP as the principal.
D. Confirm that the Network Time Protocol (NTP) clock skew is correctly set between IAM Identity Center and the new IdP endpoints.

Answer: B

NEW QUESTION 25
A company runs an internet-accessible application on several Amazon EC2 instances that run Windows Server. The company used an instance profile to configure the EC2 instances. A security team currently accesses the VPC that hosts the EC2 instances by using an AWS Site-to-Site VPN tunnel from an on-premises office. The security team issues a policy that requires all external access to the VPC to be blocked in the event of a security incident. However, during an incident, the security team must be able to access the EC2 instances to obtain forensic information on the instances.
Which solution will meet these requirements?

A. Install EC2 Instance Connect on the EC2 instance
B. Update the IAM policy for the IAM role to grant the required permission
C. Use the AWS CLI to open a tunnel to connect to the instances.
D. Install EC2 Instance Connect on the EC2 instance
E. Configure the instances to permit access to the ec2-instance-connect command use
F. Use the AWS Management Console to connect to the EC2 instances.
G. Create an EC2 Instance Connect endpoint in the VP
H. Configure an appropriate security group to allow access between the EC2 instances and the endpoin
I. Use the AWS CLI to open a tunnel to connect to the instances.
J. Create an EC2 Instance Connect endpoint in the VP
K. Configure an appropriate security group to allow access between the EC2 instances and the endpoin
L. Use the AWS Management Console to connect to the EC2 instances.

Answer: D

NEW QUESTION 29
A company creates AWS Lambda functions from container images that are stored in Amazon Elastic Container Registry (Amazon ECR). The company needs to identify any software vulnerabilities in the container images and any code vulnerabilities in the Lambda functions.
Which solution will meet these requirements?

A. Enable Amazon GuardDut
B. Configure Amazon ECR scanning and Lambda code scanning in GuardDuty.
C. Enable Amazon GuardDut
D. Configure Runtime Monitoring and Lambda Protection in GuardDuty.
E. Enable Amazon Inspecto
F. Configure Amazon ECR enhanced scanning and Lambda code scanning in Amazon Inspector.
G. Enable AWS Security Hu
H. Configure Runtime Monitoring and Lambda Protection in Security Hub.

Answer: C

NEW QUESTION 34
A company has a single AWS account and uses an Amazon EC2 instance to test application code. The company recently discovered that the instance was compromised and was serving malware. Analysis showed that the instance was compromised 35 days ago. A security engineer must implement a continuous monitoring solution that automatically notifies the security team by email for high severity findings as soon as possible.
Which combination of steps should the security engineer take to meet these requirements? (Select THREE.)

A. Enable AWS Security Hub in the AWS account.
B. Enable Amazon GuardDuty in the AWS account.
C. Create an Amazon Simple Notification Service (Amazon SNS) topi
D. Subscribe the security team's email distribution list to the topic.
E. Create an Amazon Simple Queue Service (Amazon SQS) queu
F. Subscribe the security team's email distribution list to the queue.
G. Create an Amazon EventBridge rule for GuardDuty findings of high severit
H. Configure the rule to publish a message to the topic.
I. Create an Amazon EventBridge rule for Security Hub findings of high severit
J. Configure the rule to publish a message to the queue.

Answer: BCE

NEW QUESTION 37
A security engineer needs to prepare Amazon EC2 instances for quarantine during a security incident. AWS Systems Manager Agent (SSM Agent) is installed, and a script exists to install and update forensic tools.
Which solution will quarantine EC2 instances during a security incident?

A. Track SSM Agent versions with AWS Config.
B. Configure Session Manager to deny external connections.
C. Store the script in Amazon S3 and grant read access.
D. Configure IAM permissions for the SSM Agent to run the script as a Systems Manager Run Command document.

Answer: D

NEW QUESTION 40
A company uses AWS to run a web application that manages ticket sales in several countries. The company recently migrated the application to an architecture that includes Amazon API Gateway, AWS Lambda, and Amazon Aurora Serverless. The company needs the application to comply with Payment Card Industry Data Security Standard (PCI DSS) v4.0. A security engineer must generate a report that shows the effectiveness of the PCI DSS v4.0 controls that apply to the application. The company's compliance team must be able to add manual evidence to the report.
Which solution will meet these requirements?

A. Enable AWS Trusted Adviso
B. Configure all the Trusted Advisor check
C. Manually map the checks against the PCI DSS v4.0 standard to generate the report.
D. Enable and configure AWS Confi
E. Deploy the Operational Best Practices for PCI DSS conformance pack in AWS Confi
F. Use AWS Config to generate the report.
G. Enable AWS Security Hu
H. Enable the Security Hub PCI DSS security standar
I. Use the AWS Management Console to download the report from the security standard.
J. Create an AWS Audit Manager assessment that uses the AWS managed PCI DSS v4.0 standard framewor
K. Add all evidence to the assessmen
L. Generate the report in Audit Manager for download.

Answer: D

NEW QUESTION 41
A company runs a web application on a fleet of Amazon EC2 instances in an Auto Scaling group. Amazon GuardDuty and AWS Security Hub are enabled. The security engineer needs an automated response to anomalous traffic that follows AWS best practices and minimizes application disruption.
Which solution will meet these requirements?

A. Use EventBridge to disable the instance profile access keys.
B. Use EventBridge to invoke a Lambda function that removes the affected instance from the Auto Scaling group and isolates it with a restricted security group.
C. Use Security Hub to update the subnet network ACL to block traffic.
D. Send GuardDuty findings to Amazon SNS for email notification.

Answer: B

NEW QUESTION 44
A company??s security engineer receives an alert that indicates that an unexpected principal is accessing a company-owned Amazon Simple Queue Service

(Amazon SQS) queue. All the company??s accounts are within an organization in AWS Organizations. The security engineer must implement a mitigation solution that minimizes compliance violations and investment in tools outside of AWS.
What should the security engineer do to meet these requirements?

A. Create security groups and attach them to all SQS queues.
B. Modify network ACLs in all VPCs to restrict inbound traffic.
C. Create interface VPC endpoints for Amazon SQ
D. Restrict access using aws:SourceVpce and aws:PrincipalOrgId conditions.
E. Use a third-party cloud access security broker (CASB).

Answer: C

NEW QUESTION 47
A company has an AWS account that hosts a production application. The company receives an email notification that Amazon GuardDuty has detected an Impact:IAMUser/AnomalousBehavior finding in the account. A security engineer needs to run the investigation playbook for this security incident and must collect and analyze the information without affecting the application.
Which solution will meet these requirements MOST quickly?

A. Log in to the AWS account by using read-only credential
B. Review the GuardDuty finding for details about the IAM credentials that were use
C. Use the IAM console to add a DenyAll policy to the IAM principal.
D. Log in to the AWS account by using read-only credential
E. Review the GuardDuty finding to determine which API calls initiated the findin
F. Use Amazon Detective to review the API calls in context.
G. Log in to the AWS account by using administrator credential
H. Review the GuardDuty finding for details about the IAM credentials that were use
I. Use the IAM console to add a DenyAll policy to the IAM principal.
J. Log in to the AWS account by using read-only credential
K. Review the GuardDuty finding to determine which API calls initiated the findin
L. Use AWS CloudTrail Insights and AWS CloudTrail Lake to review the API calls in context.

Answer: B

NEW QUESTION 50
A company is using AWS CloudTrail and Amazon CloudWatch to monitor resources in an AWS account. The company??s developers have been using an IAM role in the account for the last 3 months.
A security engineer needs to refine the customer managed IAM policy attached to the role to ensure that the role provides least privilege access.
Which solution will meet this requirement with the LEAST effort?

A. Implement AWS IAM Access Analyzer policy generation on the role.
B. Implement AWS IAM Access Analyzer policy validation on the role.
C. Search CloudWatch logs to determine the actions the role invoked and to evaluate the permissions.
D. Use AWS Trusted Advisor to compare the policies assigned to the role against AWS best practices.

Answer: A

NEW QUESTION 55
A company detects bot activity targeting Amazon Cognito user pool endpoints. The solution must block malicious requests while maintaining access for legitimate users.
Which solution meets these requirements?

A. Enable Amazon Cognito threat protection.
B. Restrict access to authenticated users only.
C. Associate AWS WAF with the Cognito user pool.
D. Monitor requests with CloudWatch.

Answer: A

NEW QUESTION 56
A company is planning to migrate its applications to AWS in a single AWS Region. The company??s applications will use a combination of Amazon EC2 instances, Elastic Load Balancing (ELB) load balancers, and Amazon S3 buckets. The company wants to complete the migration as quickly as possible. All the applications must meet the following requirements:
• Data must be encrypted at rest.
• Data must be encrypted in transit.
• Endpoints must be monitored for anomalous network traffic.
Which combination of steps should a security engineer take to meet these requirements with the LEAST effort? (Select THREE.)

A. Install the Amazon Inspector agent on EC2 instances by using AWS Systems Manager Automation.
B. Enable Amazon GuardDuty in all AWS accounts.
C. Create VPC endpoints for Amazon EC2 and Amazon S3. Update VPC route tables to use only the secure VPC endpoints.
D. Configure AWS Certificate Manager (ACM). Configure the load balancers to use certificates from ACM.
E. Use AWS Key Management Service (AWS KMS) for key managemen
F. Create an S3 bucket policy to deny any PutObject command with a condition for x-amz-meta-side- encryption.
G. Use AWS Key Management Service (AWS KMS) for key managemen
H. Create an S3 bucket policy to deny any PutObject command with a condition for x-amz-server-side- encryption.

Answer: BDF

NEW QUESTION 59
A company is using AWS Organizations with nested OUs to manage AWS accounts. The company has a custom compliance monitoring service for the accounts. The monitoring service runs as an AWS Lambda function and is invoked by Amazon EventBridge Scheduler.
The company needs to deploy the monitoring service in all existing and future accounts in the organization. The company must avoid using the organization's management account when the management account is not required.
Which solution will meet these requirements?

A. Create a CloudFormation stack set in the organization's management account andmanually add new accounts.
B. Configure a delegated administrator account for AWS CloudFormatio
C. Create a CloudFormation StackSet in the delegated administrator account targeting the organization root with automatic deployment enabled.
D. Use Systems Manager delegated administration and Automation to deploy the Lambda function and schedule.
E. Create a Systems Manager Automation runbook in the management account and share it to accounts.

Answer: B

NEW QUESTION 64
A company needs centralized log monitoring with automatic detection across hundreds of AWS accounts.
Which solution meets these requirements with the LEAST operational effort?

A. Designate a GuardDuty administrator account and enable protections.
B. Centralize CloudWatch logs and use Inspector.
C. Centralize CloudTrail logs and query with Athena.
D. Stream logs to Kinesis and process with Lambda.

Answer: A

NEW QUESTION 67
A company is implementing new compliance requirements to meet customer needs. According to the new requirements, the company must not use any Amazon RDS DB instances or DB clusters that lack encryption of the underlying storage. The company needs a solution that will generate an email alert when an unencrypted DB instance or DB cluster is created. The solution also must terminate the unencrypted DB instance or DB cluster.
Which solution will meet these requirements in the MOST operationally efficient manner?

A. Create an AWS Config managed rule to detect unencrypted RDS storag
B. Configure an automatic remediation action to publish messages to an Amazon Simple Notification Service (Amazon SNS) topic that includes an AWS Lambda function and an email delivery target as subscriber
C. Configure the Lambda function to delete the unencrypted resource.
D. Create an AWS Config managed rule to detect unencrypted RDS storag
E. Configure a manual remediation action to invoke an AWS Lambda functio
F. Configure the Lambda function to publish messages to an Amazon Simple Notification Service (Amazon SNS) topic and to delete the unencrypted resource.
G. Create an Amazon EventBridge rule that evaluates RDS event patterns and is initiated by the creation of DB instances or DB cluster
H. Configure the rule to publish messages to an Amazon Simple Notification Service (Amazon SNS) topic that includes an AWS Lambda function and an email delivery target as subscriber
I. Configure the Lambda function to delete the unencrypted resource.
J. Create an Amazon EventBridge rule that evaluates RDS event patterns and is initiated by the creation of DB instances or DB cluster
K. Configure the rule to invoke an AWS Lambda functio
L. Configure the Lambda function to publish messages to an Amazon Simple Notification Service (Amazon SNS) topic and to delete the unencrypted resource.

Answer: A

NEW QUESTION 70
A company is running a new workload across accounts in an organization in AWS Organizations. All running resources must have a tag of CostCenter, and the tag must have one of three approved values. The company must enforce this policy and must prevent any changes of the CostCenter tag to a non-approved value.
Which solution will meet these requirements?

A. Use AWS Config custom policy rule and an SCP to deny non-approved aws:RequestTag/CostCenter values.
B. Use CloudTrail + EventBridge + Lambda to block creation.
C. Enable tag policies, define allowed values, enforce noncompliant operations, and use an SCP to deny creation when aws:RequestTag/CostCenter is null.
D. Enable tag policies and use EventBridge + Lambda to block changes.

Answer: C

NEW QUESTION 74
A security engineer needs to implement a solution to identify any sensitive data that is stored in an Amazon S3 bucket. The solution must report on sensitive data in the S3 bucket by using an existing Amazon Simple Notification Service (Amazon SNS) topic.
Which solution will meet these requirements with the LEAST implementation effort?

A. Enable AWS Confi
B. Configure AWS Config to monitor for sensitive data in the S3 bucket and to send notifications to the SNS topic.
C. Create an AWS Lambda function to scan the S3 bucket for sensitive data that matches a patter
D. Program the Lambda function to send notifications to the SNS topic.
E. Configure Amazon Macie to use managed data identifiers to identify and categorize sensitive dat
F. Create an Amazon EventBridge rule to send notifications to the SNS topic.
G. Enable Amazon GuardDut
H. Configure AWS CloudTrail S3 data event
I. Create an Amazon CloudWatch alarm that reacts to GuardDuty findings and sends notifications to the SNS topic.

Answer: C

NEW QUESTION 75
A company needs a cloud-based, managed desktop solution for its workforce of remote employees. The company wants to ensure that the employees can access the desktops only by using company-provided devices. A security engineer must design a solution that will minimize cost and management overhead.
Which solution will meet these requirements?

A. Deploy a custom virtual desktop infrastructure (VDI) solution with a restriction policy to allow access only from corporate devices.
B. Deploy a fleet of Amazon EC2 instance
C. Assign an instance to each employee with certificate-based device authentication that uses Windows Active Directory.
D. Deploy Amazon WorkSpace
E. Set up a trusted device policy with IP blocking on the authentication gateway by using AWS Identity and Access Management (IAM).
F. Deploy Amazon WorkSpace
G. Create client certificates, and deploy them to trusted device
H. Enable restricted access at the directory level.

Answer: D

NEW QUESTION 80
A company is operating an open-source software platform that is internet facing. The legacy software platform no longer receives security updates. The software platform operates using Amazon Route 53 weighted load balancing to send traffic to two Amazon EC2 instances that connect to an Amazon RDS cluster. A recent report suggests this software platform is vulnerable to SQL injection attacks, with samples of attacks provided. The company's security engineer must secure this system against SQL injection attacks within 24 hours. The solution must involve the least amount of effort and maintain normal operations during implementation.
What should the security engineer do to meet these requirements?

A. Create an Application Load Balancer with the existing EC2 instances as a target grou
B. Create an AWS WAF web ACL containing rules that protect the application from this attack, then apply it to the AL
C. Test to ensure the vulnerability has been mitigated, then redirect the Route 53 records to point to the AL
D. Update security groups on the EC2 instances to prevent direct access from the internet.
E. Create an Amazon CloudFront distribution specifying one EC2 instance as an origi
F. Create an AWS WAF web ACL containing rules that protect the application from this attack, then apply it to the distributio
G. Test to ensure the vulnerability has been mitigated, then redirect the Route 53 records to point to CloudFront.
H. Obtain the latest source code for the platform and make the necessary update
I. Test the updated code to ensure that the vulnerability has been mitigated, then deploy the patched version of the platform to the EC2 instances.
J. Update the security group that is attached to the EC2 instances, removing access from the internet to the TCP port used by the SQL databas
K. Create an AWS WAF web ACL containing rules that protect the application from this attack, then apply it to the EC2 instances.

Answer: A

NEW QUESTION 82
A company that uses AWS Organizations is using AWS IAM Identity Center to administer access to AWS accounts. A security engineer is creating a custom permission set in IAM 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 IAM Identity Center user who has access to multiple accounts, the assignment fails.
What should the security engineer do to resolve this failure?

A. Create the customer managed policy in every account where the permission set is assigne
B. Give the customer managed policy the same name and same permissions in each account.
C. Remove either the AWS managed policy or the customer managed policy from the permission se
D. Create a second permission set that includes the removed polic
E. Apply the permission sets separately to the user.
F. Evaluate the logic of the AWS managed policy and the customer managed polic
G. Resolve any policy conflicts in the permission set before deployment.
H. Do not add the new permission set to the use
I. Instead, edit the user's existing permission set to include the AWS managed policy and the customer managed policy.

Answer: A

NEW QUESTION 87
A company recently experienced a malicious attack on its cloud-based environment. The company successfully contained and eradicated the attack. A security engineer is performing incident response work. The security engineer needs to recover an Amazon RDS database cluster to the last known good version. The database cluster is configured to generate automated backups with a retention period of 14 days. The initial attack occurred 5 days ago at exactly 3:15 PM.
Which solution will meet this requirement?

A. Identify the Regional cluster ARN for the databas
B. Use the ARN to restore the Regional cluster by using the restore to point in time featur
C. Set a target time 5 days ago at 3:14 PM.
D. Identify the Regional cluster ARN for the databas
E. List snapshots that have been taken of the cluste
F. Restore the database by using the snapshot that has a creation time that is closest to 5 days ago at 3:14 PM.
G. List all snapshots that have been taken of all the company's RDS database
H. Identify the snapshot that was taken closest to 5 days ago at 3:14 PM and restore it.
I. Identify the Regional cluster ARN for the databas
J. Use the ARN to restore the Regional cluster by using the restore to point in time featur
K. Set a target time 14 days ago.

Answer: A

NEW QUESTION 92
A company uses AWS Organizations and has an SCP at the root that prevents sharing resources with external accounts. The company now needs to allow only the marketing account to share resources externally while preventing all other accounts from doing so. All accounts are in the same OU.

Which solution will meet these requirements?

A. Create a new SCP in the marketing account to explicitly allow sharing.
B. Edit the existing SCP to add a condition that excludes the marketing account.
C. Edit the SCP to include an Allow statement for the marketing account.
D. Use a permissions boundary in the marketing account.

Answer: B

NEW QUESTION 96
A security engineer receives a notice about suspicious activity from a Linux-based Amazon EC2 instance that uses Amazon Elastic Block Store (Amazon EBS)-based storage. The instance is making connections to known malicious addresses.
The instance is in a development account within a VPC that is in the us-east-1 Region. The VPC contains an internet gateway and has a subnet in us-east-1a and us-east-1b. Each subnet is associated with a route table that uses the internet gateway as a default route. Each subnet also uses the default network ACL. The suspicious EC2 instance runs within the us-east-1b subnet. During an initial investigation, a security engineer discovers that the suspicious instance is the only instance that runs in the subnet.
Which response will immediately mitigate the attack and help investigate the root cause?

A. Log in to the suspicious instance and use the netstat command to identify remote connection
B. Use the IP addresses from these remote connections to create deny rules in the security group of the instanc
C. Install diagnostic tools on the instance for investigatio
D. Update the outbound network ACL for the subnet in us-east-1b to explicitly deny all connections as the first rule during the investigation of the instance.
E. Update the outbound network ACL for the subnet in us-east-1b to explicitly deny all connections as the first rul
F. Replace the security group with a new security group that allows connections only from a diagnostics security grou
G. Update the outbound network ACL for the us-east-1b subnet to remove the deny all rul
H. Launch a new EC2 instance that has diagnostic tool
I. Assign the new security group to the new EC2 instanc
J. Use the new EC2 instance to investigate the suspicious instance.
K. Ensure that the Amazon Elastic Block Store (Amazon EBS) volumes that are attached to the suspicious EC2 instance will not delete upon terminatio
L. Terminate the instanc
M. Launch a new EC2 instance in us-east-1a that has diagnostic tool
N. Mount the EBS volumes from the terminated instance for investigation.
O. Create an AWS WAF web ACL that denies traffic to and from the suspicious instanc
P. Attach the AWS WAF web ACL to the instance to mitigate the attac
Q. Log in to the instance and install diagnostic tools to investigate the instance.

Answer: C

NEW QUESTION 97
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your SCS-C03 Exam with Our Prep Materials Via below:

https://www.certleader.com/SCS-C03-dumps.html