Amazon-Web-Services

Exam Questions SCS-C03

AWS Certified Security - Specialty

NEW QUESTION 1
A company stores sensitive data in an Amazon S3 bucket. The company encrypts the data at rest by using server-side encryption with Amazon S3 managed keys (SSE-S3). A security engineer must prevent any modifications to the data in the S3 bucket.
Which solution will meet this requirement?

A. Configure S3 bucket policies to deny DELETE and PUT object permissions.
B. Configure S3 Object Lock in compliance mode with S3 bucket versioning enabled.
C. Change the encryption on the S3 bucket to use AWS Key Management Service (AWS KMS) customer managed keys.
D. Configure the S3 bucket with multi-factor authentication (MFA) delete protection.

Answer: B

NEW QUESTION 2
A company needs to identify the root cause of security findings and investigate IAM roles involved in those findings. The company has enabled VPC Flow Logs, Amazon GuardDuty, and AWS CloudTrail.
Which solution will meet these requirements?

A. Use Amazon Detective to investigate IAM roles and visualize findings.
B. Use Amazon Inspector and CloudWatch dashboards.
C. Export GuardDuty findings to S3 and analyze with Athena.
D. Use Security Hub custom actions to investigate IAM roles.

Answer: A

NEW QUESTION 3
A company has decided to move its fleet of Linux-based web server instances to an Amazon EC2 Auto Scaling group. Currently, the instances are static and are launched manually. When an administrator needs to view log files, the administrator uses SSH to establish a connection to the instances and retrieves the logs manually.
The company often needs to query the logs to produce results about application sessions and user issues. The company does not want its new automatically scaling architecture to result in the loss of any log files when instances are scaled in.
Which combination of steps should a security engineer take to meet these requirements MOST cost-effectively? (Select TWO.)

A. Configure a cron job on the instances to forward the log files to Amazon S3 periodically.
B. Configure AWS Glue and Amazon Athena to query the log files.
C. Configure the Amazon CloudWatch agent on the instances to forward the logs to Amazon CloudWatch Logs.
D. Configure Amazon CloudWatch Logs Insights to query the log files.
E. Configure the instances to write the logs to an Amazon Elastic File System (Amazon EFS) volume.

Answer: CD

NEW QUESTION 4
A company runs an application on an Amazon EC2 instance. The application generates invoices and stores them in an Amazon S3 bucket. The instance profile that is attached to the instance has appropriate access to the S3 bucket. The company needs to share each invoice with multiple clients that do not have AWS credentials. Each client must be able to download only the client's own invoices. Clients must download their invoices within 1 hour of invoice creation. Clients must use only temporary credentials to access the company's AWS resources.
Which additional step will meet these requirements?

A. Update the S3 bucket policy to ensure that clients that use pre-signed URLs have the S3:Get* permission and the S3:List* permission to access S3 objects in the bucket.
B. Add a StringEquals condition to the IAM role policy for the EC2 instance profil
C. Configure the policy condition to restrict access based on the s3:ResourceTag/ClientId tag of each invoic
D. Tag each generated invoice with the ID of its corresponding client.
E. Update the script to use AWS Security Token Service (AWS STS) to obtain new credentials each time the script runs by assuming a new role that has S3:GetObject permission
F. Use the credentials to generate the pre-signed URLs.
G. Generate an access key and a secret key for an IAM user that has S3:GetObject permissions on the S3 bucke
H. Embed the keys into the scrip
I. Use the keys to generate the pre-signed URLs.

Answer: B

NEW QUESTION 5
A security engineer has designed a VPC to segment private traffic from public traffic. The VPC includes two Availability Zones. Each Availability Zone contains one public subnet and one private subnet. Three route tables exist: one for the public subnets and one for each private subnet.
The security engineer discovers that all four subnets are routing traffic through the internet gateway that is attached to the VPC.
Which combination of steps should the security engineer take to remediate this scenario? (Select TWO.)

A. Verify that a NAT gateway has been provisioned in the public subnet in each Availability Zone.
B. Verify that a NAT gateway has been provisioned in the private subnet in each Availability Zone.
C. Modify the route tables for the public subnets to add a local route to the VPC CIDR range.
D. Modify the route tables for the private subnets to route 0.0.0.0/0 to the NAT gateway in the public subnet of the same Availability Zone.
E. Modify the route tables for the private subnets to route 0.0.0.0/0 to the internet gateway.

Answer: AD

NEW QUESTION 6

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 7
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 8
A company is building a secure solution that relies on an AWS Key Management Service (AWS KMS) customer managed key. The company wants to allow AWS Lambda to use the KMS key. However, the company wants to prevent Amazon EC2 from using the key.
Which solution will meet these requirements?

A. Use IAM explicit deny for EC2 instance profiles and allow for Lambda roles.
B. Use a KMS key policy with kms:ViaService conditions to allow Lambda usage and deny EC2 usage.
C. Use aws:SourceIp and aws:AuthorizedService condition keys in the KMS key policy.
D. Use an SCP to deny EC2 and allow Lambda.

Answer: B

NEW QUESTION 9
A security administrator is setting up a new AWS account. The security administrator wants to secure the data that a company stores in an Amazon S3 bucket. The security administrator also wants to reduce the chance of unintended data exposure and the potential for misconfiguration of objects that are in the S3 bucket.
Which solution will meet these requirements with the LEAST operational overhead?

A. Configure the S3 Block Public Access feature for the AWS account.
B. Configure the S3 Block Public Access feature for all objects that are in the bucket.
C. Deactivate ACLs for objects that are in the bucket.
D. Use AWS PrivateLink for Amazon S3 to access the bucket.

Answer: A

NEW QUESTION 10
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 10
A company has an encrypted Amazon Aurora DB cluster in the us-east-1 Region that uses an AWS KMS customer managed key. The company must copy a DB snapshot to the us- west-1 Region but cannot access the encryption key across Regions.
What should the company do to properly encrypt the snapshot in us-west-1?

A. Store the customer managed key in AWS Secrets Manager in us-west-1.
B. Create a new customer managed key in us-west-1 and use it to encrypt the snapshot.

C. Create an IAM policy to allow access to the key in us-east-1 from us-west-1.
D. Create an IAM policy that allows RDS in us-west-1 to access the key in us-east-1.

Answer: B

NEW QUESTION 14
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 17
A company has security requirements for Amazon Aurora MySQL databases regarding encryption, deletion protection, public access, and audit logging. The company needs continuous monitoring and real-time visibility into compliance status.
Which solution will meet these requirements?

A. Use AWS Audit Manager with a custom framework.
B. Enable AWS Config and use managed rules to monitor Aurora MySQL compliance.
C. Use AWS Security Hub configuration policies.
D. Use EventBridge and Lambda with custom metrics.

Answer: B

NEW QUESTION 22
A company??s data scientists use Amazon SageMaker with datasets stored in Amazon S3. Data older than 45 days must be removed according to policy.
Which action should enforce this policy?

A. Configure an S3 Lifecycle rule to delete objects after 45 days.
B. Create a Lambda function triggered on object upload to delete old data.
C. Create a scheduled Lambda function to delete old objects monthly.
D. Configure S3 Intelligent-Tiering.

Answer: A

NEW QUESTION 25
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 29
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 31
A security engineer discovers that a company's user passwords have no required minimum length. The company uses the following identity providers (IdPs):
• AWS Identity and Access Management (IAM) federated with on-premises Active Directory
• Amazon Cognito user pools that contain the user database for an AWS Cloud application Which combination of actions should the security engineer take to implement a required minimum password length? (Select TWO.)

A. Update the password length policy in the IAM configuration.
B. Update the password length policy in the Amazon Cognito configuration.
C. Update the password length policy in the on-premises Active Directory configuration.

D. Create an SCP in AWS Organizations to enforce minimum password length.
E. Create an IAM policy with a minimum password length condition.

Answer: BC

NEW QUESTION 36
A consultant agency needs to perform a security audit for a company's production AWS account. Several consultants need access to the account. The consultant agency already has its own AWS account. The company requires multi-factor authentication (MFA) for all access to its production account. The company also forbids the use of long-term credentials.
Which solution will provide the consultant agency with access that meets these requirements?

A. Create an IAM grou
B. Create an IAM user for each consultan
C. Add each user to the grou
D. Turn on MFA for each consultant.
E. Configure Amazon Cognito on the company??s production account to authenticate against the consultant agency's identity provider (IdP). Add MFA to a Cognito user pool.
F. Create an IAM role in the consultant agency's AWS accoun
G. Define a trust policy that requires MF
H. In the trust policy, specify the company's production account as the principa
I. Attach the trust policy to the role.
J. Create an IAM role in the company??s production accoun
K. Define a trust policy that requires MF
L. In the trust policy, specify the consultant agency's AWS account as the principa
M. Attach the trust policy to the role.

Answer: D

NEW QUESTION 41
A company is planning to deploy a new log analysis environment. The company needs to analyze logs from multiple AWS services in near real time. The solution must provide the ability to search the logs and must send alerts to an existing Amazon Simple Notification
Service (Amazon SNS) topic when specific logs match detection rules. Which solution will meet these requirements?

A. Analyze the logs by using Amazon OpenSearch Servic
B. Search the logs from the OpenSearch AP
C. Use OpenSearch Service Security Analytics to match logs with detection rules and to send alerts to the SNS topic.
D. Analyze the logs by using AWS Security Hu
E. Search the logs from the Findings page in Security Hu
F. Create custom actions to match logs with detection rules and to send alerts to the SNS topic.
G. Analyze the logs by using Amazon CloudWatch Log
H. Use a subscription filter to match logs with detection rules and to send alerts to the SNS topi
I. Search the logs manually by using CloudWatch Logs Insights.
J. Analyze the logs by using Amazon QuickSigh
K. Search the logs by listing the query results in a dashboar
L. Run queries to match logs with detection rules and to send alerts to the SNS topic.

Answer: A

NEW QUESTION 43
CloudFormation stack deployments fail for some users due to permission inconsistencies.
Which combination of steps will ensure consistent deployments MOST securely? (Select THREE.)

A. Create a composite principal service role.
B. Create a service role with cloudformation.amazonaws.com as the principal.
C. Attach scoped policies to the service role.
D. Attach service ARNs in policy resources.
E. Update each stack to use the service role.
F. Allow iam:PassRole to the service role.

Answer: BEF

NEW QUESTION 47
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 48
A company needs to scan all AWS Lambda functions for code vulnerabilities.

A. Use Amazon Macie.
B. Enable Amazon Inspector Lambda scanning.
C. Use GuardDuty and Security Hub.
D. Use GuardDuty Lambda Protection.

Answer: B

NEW QUESTION 51
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 53
A company requires a specific software application to be installed on all new and existing Amazon EC2 instances across an AWS Organization. SSM Agent is installed and active.
How can the company continuously monitor deployment status of the software application?

A. Use AWS Config organization-wide with the ec2-managedinstance-applications-required managed rule and specify the application name.
B. Use approved AMIs rule organization-wide.
C. Use Distributor package and review output.
D. Use Systems Manager Application Manager inventory filtering.

Answer: A

NEW QUESTION 54
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 59
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 60
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 62
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 67
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 68
A company runs a global ecommerce website using Amazon CloudFront. The company must block traffic from specific countries to comply with data regulations.
Which solution will meet these requirements MOST cost-effectively?

A. Use AWS WAF IP match rules.
B. Use AWS WAF geo match rules.
C. Use CloudFront geo restriction to deny the countries.
D. Use geolocation headers in CloudFront.

Answer: C

NEW QUESTION 72
A company must immediately disable compromised IAM users across all AWS accounts and collect all actions performed by the user in the last 7 days.
Which solution will meet these requirements?

A. Disable the IAM user and query CloudTrail logs in Amazon S3 using Athena.
B. Remove IAM policies and query logs in Security Hub.
C. Remove permission sets and query logs using CloudWatch Logs Insights.
D. Disable the user in IAM Identity Center and query the organizational event data store.

Answer: D

NEW QUESTION 75
A company sends Apache logs from EC2 Auto Scaling instances to a CloudWatch Logs log group with 1-year retention. A suspicious IP address appears in logs. A security engineer needs to analyze the past week of logs to count requests from that IP and list requested URLs.
What should the engineer do with the LEAST effort?

A. Export to S3 and use Macie.
B. Stream to OpenSearch and analyze.
C. Use CloudWatch Logs Insights with queries.
D. Export to S3 and use AWS Glue.

Answer: C

NEW QUESTION 78
A company runs ECS services behind an internet-facing ALB that is the origin for CloudFront. An AWS WAF web ACL is associated with CloudFront, but clients can bypass it by accessing the ALB directly.
Which solution will prevent direct access to the ALB?

A. Use AWS PrivateLink with the ALB.
B. Replace the ALB with an internal ALB.
C. Restrict ALB listener rules to CloudFront IP ranges.
D. Require a custom header from CloudFront and validate it at the ALB.

Answer: D

NEW QUESTION 79
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 83
A company uploads data files as objects into an Amazon S3 bucket. A vendor downloads the objects to perform data processing.
A security engineer must implement a solution that prevents objects from residing in the S3 bucket for longer than 72 hours.

A. Configure S3 Versioning to expire object versions that have been in the bucket for 72 hours.
B. Configure an S3 Lifecycle configuration rule on the bucket to expire objects after 72 hours.
C. Use the S3 Intelligent-Tiering storage class and configure expiration after 72 hours.
D. Generate presigned URLs that expire after 72 hours.

Answer: B

NEW QUESTION 86
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 87
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 90

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

SCS-C03 Practice Exam Features:

* SCS-C03 Questions and Answers Updated Frequently

* SCS-C03 Practice Questions Verified by Expert Senior Certified Staff

* SCS-C03 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SCS-C03 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The SCS-C03 Practice Test Here