Free Questions for SCS-C02 by dumpshq

Shared by Dudley on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A company has a VPC that has no internet access and has the private DNS hostnames option enabled. An Amazon Aurora database is running inside the VPC. A security engineer wants to use AWS Secrets Manager to automatically rotate the credentials for the Aurora database The security engineer configures the Secrets Manager default AWS Lambda rotation function to run inside the same VPC that the Aurora database uses. However, the security engineer determines that the password cannot be rotated properly because the Lambda function cannot communicate with the Secrets Manager endpoint.

What is the MOST secure way that the security engineer can give the Lambda function the ability to communicate with the Secrets Manager endpoint?

Options:

A- Add a NAT gateway to the VPC to allow access to the Secrets Manager endpoint.

B- Add a gateway VPC endpoint to the VPC to allow access to the Secrets Manager endpoint.

C- Add an interface VPC endpoint to the VPC to allow access to the Secrets Manager endpoint.

D- Add an internet gateway for the VPC to allow access to the Secrets Manager endpoint.

Answer:

C

Explanation:

In an AWS environment where a VPC has no internet access and requires communication with AWS services such as Secrets Manager, the most secure method is to use an interface VPC endpoint (AWS PrivateLink). This allows private connectivity to services like Secrets Manager, enabling AWS Lambda functions and other resources within the VPC to access Secrets Manager without requiring an internet gateway, NAT gateway, or VPN connection. Interface VPC endpoints are powered by AWS PrivateLink, a technology that enables private connectivity between AWS services using Elastic Network Interfaces (ENI) with private IPs in your VPCs. This option is more secure than creating a NAT gateway because it doesn't expose the resources to the internet and adheres to the principle of least privilege by providing direct access to only the required service.

Question 2

Question Type: MultipleChoice

A company has AWS accounts that are in an organization in AWS Organizations. A security engineer needs to set up AWS Security Hub in a dedicated account for security monitoring.

The security engineer must ensure that Security Hub automatically manages all existing accounts and all new accounts that are added to the organization. Security Hub also must receive findings from all AWS Regions.

Which combination of actions will meet these requirements with the LEAST operational overhead? (Select TWO.)

Options:

A- Configure a finding aggregation Region for Security Hub. Link the other Regions to the aggregation Region.

B- Create an AWS Lambda function that routes events from other Regions to the dedicated Security Hub account. Create an Amazon EventBridge rule to invoke the Lambda function.

C- Turn on the option to automatically enable accounts for Security Hub.

D- Create an SCP that denies the securityhub DisableSecurityHub permission. Attach the SCP to the organization's root account.

E- Configure services in other Regions to write events to an AWS CloudTrail organization trail. Configure Security Hub to read events from the trail.

Answer:

A, C

Explanation:

To set up AWS Security Hub for centralized security monitoring across all accounts in an AWS Organization with the least operational overhead, the best actions to take are:

Solution A: Configure a finding aggregation Region for Security Hub. This allows Security Hub to aggregate findings from multiple regions into a single designated region, simplifying monitoring and analysis. By centralizing findings, the security team can have a unified view of security alerts and compliance statuses across all accounts and regions, enhancing the efficiency of security operations.

Solution C: Turn on the option to automatically enable accounts for Security Hub within the AWS Organization. This ensures that as new accounts are created and added to the organization, they are automatically enrolled in Security Hub, and their findings are included in the centralized monitoring. This automation reduces the manual effort required to manage account enrollment and ensures comprehensive coverage of security monitoring across the organization.

These actions collectively ensure that Security Hub is effectively configured to manage security findings across all accounts and regions, providing a comprehensive and automated approach to security monitoring with minimal manual intervention.

Question 3

Question Type: **MultipleChoice**

A company has secured the AWS account root user for its AWS account by following AWS best practices. The company also has enabled AWS CloudTrail, which is sending its logs to Amazon S3. A security engineer wants to receive notification in near-real time if a user uses the AWS account root user credentials to sign in to the AWS Management Console.

Which solutions will provide this notification? (Select TWO.)

Options:

A- Use AWS Trusted Advisor and its security evaluations for the root account. Configure an Amazon EventBridge event rule that is invoked by the Trusted Advisor API. Configure the rule to target an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe any required endpoints to the SNS topic so that these endpoints can receive notification.

B- Use AWS IAM Access Analyzer. Create an Amazon CloudWatch Logs metric filter to evaluate log entries from Access Analyzer that detect a successful root account login. Create an Amazon CloudWatch alarm that monitors whether a root login has occurred. Configure the CloudWatch alarm to notify an Amazon Simple Notification Service (Amazon SNS) topic when the alarm enters the ALARM state. Subscribe any required endpoints to this SNS topic so that these endpoints can receive notification.

C- Configure AWS CloudTrail to send its logs to Amazon CloudWatch Logs. Configure a metric filter on the CloudWatch Logs log group used by CloudTrail to evaluate log entries for successful root account logins. Create an Amazon CloudWatch alarm that monitors whether a root login has occurred Configure the CloudWatch alarm to notify an Amazon Simple Notification Service (Amazon SNS) topic when the alarm enters the ALARM state. Subscribe any required endpoints to this SNS topic so that these endpoints can receive notification.

D- Configure AWS CloudTrail to send log notifications to an Amazon Simple Notification Service (Amazon SNS) topic. Create an AWS Lambda function that parses the CloudTrail notification for root login activity and notifies a separate SNS topic that contains the endpoints that should receive notification. Subscribe the Lambda function to the SNS topic that is receiving log notifications from CloudTrail.

E- Configure an Amazon EventBridge event rule that runs when Amazon CloudWatch API calls are recorded for a successful root login. Configure the rule to target an Amazon Simple Notification Service (Amazon SNS) topic. Subscribe any required endpoints to the SNS topic so that these endpoints can receive notification.

Answer:

C, E

Explanation:

To receive near-real-time notifications of AWS account root user sign-ins, the most effective solutions involve the use of AWS CloudTrail logs, Amazon CloudWatch Logs, and Amazon EventBridge.

Solution C involves configuring AWS CloudTrail to send logs to Amazon CloudWatch Logs and then setting up a CloudWatch Logs metric filter to detect successful root account logins. When such logins are detected, a CloudWatch alarm can be configured to trigger and notify an Amazon Simple Notification Service (Amazon SNS) topic, which in turn can send notifications to the required endpoints. This solution provides an efficient way to monitor and alert on root account usage without requiring custom parsing or handling of log data.

Solution E uses Amazon EventBridge to monitor for specific AWS API calls, such as SignIn events that indicate a successful root account login. By configuring an EventBridge rule to trigger on these events, notifications can be sent directly to an SNS topic, which then distributes the alerts to the necessary endpoints. This approach leverages native AWS event patterns and provides a streamlined mechanism for detecting and alerting on root account activity.

Both solutions offer automation, scalability, and the ability to integrate with other AWS services, ensuring that stakeholders are promptly alerted to critical security events involving the root user.

Question 4

Question Type: MultipleChoice

A company wants to implement host-based security for Amazon EC2 instances and containers in Amazon Elastic Container Registry (Amazon ECR). The company has deployed AWS Systems Manager Agent (SSM Agent) on the EC2 instances. All the company's AWS accounts are in one organization in AWS Organizations. The company will analyze the workloads for software vulnerabilities and unintended network exposure. The company will push any findings to AWS Security Hub. which the company has configured for the organization.

The company must deploy the solution to all member accounts, including pew accounts, automatically. When new workloads come online, the solution must scan the workloads.

Which solution will meet these requirements?

Options:

A- Use SCPs to configure scanning of EC2 instances and ECR containers for all accounts in the organization.

B- Configure a delegated administrator for Amazon GuardDuty for the organization. Create an Amazon EventBridge rule to initiate analysis of ECR containers

C- Configure a delegated administrator for Amazon Inspector for the organization. Configure automatic scanning for new member accounts.

D- Configure a delegated administrator for Amazon Inspector for the organization. Create an AWS Config rule to initiate analysis of ECR containers

Answer:

C

Explanation:

To implement host-based security for Amazon EC2 instances and containers in Amazon ECR with minimal operational overhead and ensure automatic deployment and scanning for new workloads, the recommended solution is to configure a delegated administrator for Amazon Inspector within the AWS Organizations structure. By enabling Amazon Inspector for the organization and configuring it to automatically scan new member accounts, the company can ensure that all EC2 instances and ECR containers are analyzed for software vulnerabilities and unintended network exposure. Amazon Inspector will automatically assess the workloads and push findings to AWS Security Hub, providing centralized security monitoring and compliance checking. This approach ensures that as new accounts or workloads are added, they are automatically included in the security assessments, maintaining a consistent security posture across the organization with minimal manual intervention.

Question 5

Question Type: MultipleChoice

A company deployed an Amazon EC2 instance to a VPC on AWS. A recent alert indicates that the EC2 instance is receiving a suspicious number of requests over an open TCP port from an external source. The TCP port remains open for long periods of time.

The company's security team needs to stop all activity to this port from the external source to ensure that the EC2 instance is not being compromised. The application must remain available to other users.

Which solution will mefet these requirements?

Options:

A- Update the network ACL that is attached to the subnet that is associated with the EC2 instance. Add a Deny statement for the port and the source IP addresses.

B- Update the elastic network interface security group that is attached to the EC2 instance to remove the port from theinbound rule list.

C- Update the elastic network interface security group that is attached to the EC2 instance by adding a Deny entry in the inbound list for the port and the source
IP addresses.

D- Create a new network ACL for the subnet. Deny all traffic from the EC2 instance to prevent data from being removed.

Answer:

A

Explanation:

To address the issue of an Amazon EC2 instance receiving suspicious requests over an open TCP port, the most effective solution is to update the Network Access Control List (NACL) associated with the subnet where the EC2 instance resides. By adding a deny rule for the specific TCP port and source IP addresses involved in the suspicious activity, the security team can effectively block unwanted traffic at the subnet level. NACLs act as a stateless firewall for controlling traffic in and out of subnets, allowing for broad-based traffic filtering. This measure ensures that only legitimate traffic can reach the EC2 instance, thereby enhancing security without affecting the application's availability to other users. It's a more granular and immediate way to block specific traffic compared to modifying security

group rules, which are stateful and apply at the instance level.

Question 6

Question Type: MultipleChoice

A company wants to receive automated email notifications when AWS access keys from developer AWS accounts are detected on code repository sites.

Which solution will provide the required email notifications?

Options:

A- Create an Amazon EventBridge rule to send Amazon Simple Notification Service (Amazon SNS) email notifications for Amazon GuardDuty UnauthorizedAccesslAMUser/lnstanceCredentialExfiltration OutsideAWS findings.

B- Change the AWS account contact information for the Operations type to a separate email address. Periodically poll this email address for notifications.

C- Create an Amazon EventBridge rule that reacts to AWS Health events that have a value of Risk for the service category Configure email notifications by using Amazon Simple Notification Service (Amazon SNS).

D- Implement new anomaly detection software. Ingest AWS CloudTrail logs. Configure monitoring for ConsoleLogin events in the AWS

Management Console. Configure email notifications from the anomaly detection software.

Answer:

A

Explanation:

The solution to receiving automated email notifications when AWS access keys are detected on code repository sites is to use Amazon EventBridge with Amazon GuardDuty findings. Specifically, creating an EventBridge rule that targets Amazon GuardDuty findings, particularly the UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration finding type, allows for the detection of potential unauthorized use or exposure of AWS credentials. When such a finding is detected, EventBridge can then trigger an action to send a notification via Amazon Simple Notification Service (Amazon SNS). By configuring an SNS topic to send emails, stakeholders can be promptly informed of such security incidents. This approach leverages AWS's native security and monitoring services to provide timely alerts with minimal operational overhead, ensuring that the company can respond quickly to potential security breaches involving exposed AWS credentials.

Question 7

Question Type: MultipleChoice

A company has two AWS accounts: Account A and Account B. Account A has an IAM role that IAM users in Account B assume when they need to upload sensitive documents to Amazon S3 buckets in Account A.

A new requirement mandates that users can assume the role only if they are authenticated with multi-factor authentication (MFA). A security engineer must recommend a solution that meets this requirement with minimum risk and effort.

Which solution should the security engineer recommend?

Options:

A- Add an aws:MultiFactorAuthPresent condition to therole's permissions policy.

B- Add an aws:MultiFactorAuthPresent condition to therole's trust policy.

C- Add an aws:MultiFactorAuthPresent condition to thesession policy.

D- Add an aws:MultiFactorAuthPresent condition to theS3 bucket policies.

Answer:

B

Explanation:

To ensure that IAM users in Account B can only assume a role in Account A if they are authenticated with Multi-Factor Authentication (MFA), the recommended solution is to add an aws:MultiFactorAuthPresent condition to the role's trust policy in Account A. The trust policy defines which principals (users, applications, services) can assume the role and under what conditions. By adding the

aws:MultiFactorAuthPresent condition, the policy explicitly requires MFA to be present for the assume role action to succeed. This ensures that only authenticated users with MFA can assume the role, enhancing the security posture with minimal operational overhead and without modifying permissions or session policies, which could affect the role's intended capabilities.

Question 8

Question Type: MultipleChoice

A company runs an online game on AWS. When players sign up for the game, their username and password credentials are stored in an Amazon Aurora database.

The number of users has grown to hundreds of thousands of players. The number of requests for password resets and login assistance has become a burden for the company's customer service team.

The company needs to implement a solution to give players another way to log in to the game. The solution must remove the burden of password resets and login assistance while securely protecting each player's credentials.

Which solution will meet these requirements?

Options:

A- When a new player signs up, use an AWS Lambda function to automatically create an 1AM access key and a secret access key.

Program the Lambda function to store the credentials on the player's device. Create 1AM keys for existing players.

B- Migrate the player credentials from the Aurora database to AWS Secrets Manager. When a new player signs up. create a key-value pair in Secrets Manager for the player's user ID and password.

C- Configure Amazon Cognito user pools to federate access to the game with third-party identity providers (IdPs), such as social IdPs Migrate the game's authentication mechanism to Cognito.

D- Instead of using usernames and passwords for authentication, issue API keys to new and existing players. Create an Amazon API Gateway API to give the game client access to the game's functionality.

Answer:

C

Explanation:

The best solution to meet the company's requirements of offering an alternative login method while securely protecting player credentials and reducing the burden of password resets is to use Amazon Cognito with user pools. Amazon Cognito provides a fully managed service that facilitates the authentication, authorization, and user management for web and mobile applications. By configuring Amazon Cognito user pools to federate access with third-party Identity Providers (IdPs), such as social media platforms or Google, the company can allow users to sign in through these external IdPs, thereby eliminating the need for traditional username and password logins. This not only enhances user convenience but also offloads the responsibility of managing user credentials and the associated challenges like password resets to Amazon Cognito, thereby reducing the burden on the company's customer service team. Additionally, Amazon Cognito integrates seamlessly with other AWS services and follows best practices for security and compliance, ensuring that the player's credentials are protected.