Amazon AWS Certified Security - Specialty

AWS Certified Security Specialty

Version: 5.1

QUESTION NO: 1

The Security team believes that a former employee may have gained unauthorized access to AWS resources sometime in the past 3 months by using an identified access key.

What approach would enable the Security team to find out what the former employee may have done within AWS?

A.
Use the AWS CloudTrail console to search for user activity.

B.
Use the Amazon CloudWatch Logs console to filter CloudTrail data by user.

C.
Use AWS Config to see what actions were taken by the user.

D.
Use Amazon Athena to query CloudTrail logs stored in Amazon S3.

Answer: A
Explanation:

QUESTION NO: 2

The Security Engineer implemented a new vault lock policy for 10TB of data and called initiate-vault-lock 12 hours ago. The Audit team identified a typo that is allowing incorrect access to the vault.

What is the MOST cost-effective way to correct this?

A.
Call the abort-vault-lock operation, fix the typo, and call the initiate-vault-lock again.

B.
Copy the vault data to Amazon S3, delete the vault, and create a new vault with the data.

C.
Update the policy, keeping the vault lock in place.

D.
Update the policy and call initiate-vault-lock again to apply the new policy.

Answer: A

Explanation:

QUESTION NO: 3

A company wants to control access to its AWS resources by using identities and groups that are defined in its existing Microsoft Active Directory.

What must the company create in its AWS account to map permissions for AWS services to Active Directory user attributes?

A.
AWS IAM groups

B.
AWS IAM users

C.
AWS IAM roles

D.
AWS IAM access keys

Answer: C
Reference: https://aws.amazon.com/blogs/security/how-to-connect-your-on-premises-active-directory-to-aws-using-ad-connector/

QUESTION NO: 4

A company has contracted with a third party to audit several AWS accounts. To enable the audit, cross-account IAM roles have been created in each account targeted for audit. The Auditor is having trouble accessing some of the accounts.

Which of the following may be causing this problem? (Choose three.)

A.
The external ID used by the Auditor is missing or incorrect.

B.
The Auditor is using the incorrect password.

C.
The Auditor has not been granted sts:AssumeRole for the role in the destination account.

D.
The Amazon EC2 role used by the Auditor must be set to the destination account role.

E.
The secret key used by the Auditor is missing or incorrect.

F.
The role ARN used by the Auditor is missing or incorrect.

Answer: C,E,F
Reference:

https://aws.amazon.com/blogs/security/how-to-use-external-id-when-granting-access-to-your-aws-resources/

QUESTION NO: 5

Compliance requirements state that all communications between company on-premises hosts and EC2 instances be encrypted in transit. Hosts use custom proprietary protocols for their communication, and EC2 instances need to be fronted by a load balancer for increased availability.

Which of the following solutions will meet these requirements?

A.
Offload SSL termination onto an SSL listener on a Classic Load Balancer, and use a TCP connection between the load balancer and the EC2 instances.

B.
Route all traffic through a TCP listener on a Classic Load Balancer, and terminate the TLS connection on the EC2 instances.

C.
Create an HTTPS listener using an Application Load Balancer, and route all of the communication through that load balancer.

D.
Offload SSL termination onto an SSL listener using an Application Load Balancer, and re-spawn and SSL connection between the load balancer and the EC2 instances.

Answer: C

Explanation:

QUESTION NO: 6

An application is currently secured using network access control lists and security groups. Web servers are located in public subnets behind an Application Load Balancer (ALB); application servers are located in private subnets.

How can edge security be enhanced to safeguard the Amazon EC2 instances against attack? (Choose two.)

A.
Configure the application's EC2 instances to use NAT gateways for all inbound traffic.

B.
Move the web servers to private subnets without public IP addresses.

C.
Configure AWS WAF to provide DDoS attack protection for the ALB.

D.
Require all inbound network traffic to route through a bastion host in the private subnet.

E.
Require all inbound and outbound network traffic to route through an AWS Direct Connect connection.

Answer: B,C
Explanation:

QUESTION NO: 7

A Security Administrator is restricting the capabilities of company root user accounts. The company uses AWS Organizations and has enabled it for all feature sets, including consolidated billing. The top-level account is used for billing and administrative purposes, not for operational AWS resource purposes.

How can the Administrator restrict usage of member root user accounts across the organization?

A.

Disable the use of the root user account at the organizational root. Enable multi-factor authentication of the root user account for each organizational member account.

B.
Configure IAM user policies to restrict root account capabilities for each Organizations member account.

C.
Create an organizational unit (OU) in Organizations with a service control policy that controls usage of the root user. Add all operational accounts to the new OU.

D.
Configure AWS CloudTrail to integrate with Amazon CloudWatch Logs and then create a metric filter for RootAccountUsage.

Answer: C
Reference:

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_about-scps.html

QUESTION NO: 8

A Systems Engineer has been tasked with configuring outbound mail through Simple Email Service (SES) and requires compliance with current TLS standards.

The mail application should be configured to connect to which of the following endpoints and corresponding ports?

A.
email.us-east-1.amazonaws.com over port 8080

B.
email-pop3.us-east-1.amazonaws.com over port 995

C.
email-smtp.us-east-1.amazonaws.com over port 587

D.
email-imap.us-east-1.amazonaws.com over port 993

Answer: C
Reference: https://docs.aws.amazon.com/ses/latest/DeveloperGuide/smtp-connect.html

QUESTION NO: 9

A threat assessment has identified a risk whereby an internal employee could exfiltrate sensitive data from production host running inside AWS (Account 1). The threat was documented as follows:

Threat description: A malicious actor could upload sensitive data from Server X by configuring credentials for an AWS account (Account 2) they control and uploading data to an Amazon S3 bucket within their control.

Server X has outbound internet access configured via a proxy server. Legitimate access to S3 is required so that the application can upload encrypted files to an S3 bucket. Server X is currently using an IAM instance role. The proxy server is not able to inspect any of the server communication due to TLS encryption.

Which of the following options will mitigate the threat? (Choose two.)

A.
Bypass the proxy and use an S3 VPC endpoint with a policy that whitelists only certain S3 buckets within Account 1.

B.
Block outbound access to public S3 endpoints on the proxy server.

C.
Configure Network ACLs on Server X to deny access to S3 endpoints.

D.
Modify the S3 bucket policy for the legitimate bucket to allow access only from the public IP addresses associated with the application server.

E.
Remove the IAM instance role from the application server and save API access keys in a trusted and encrypted application config file.

Answer: A,C
Explanation:

QUESTION NO: 10

A company will store sensitive documents in three Amazon S3 buckets based on a data

classification scheme of “Sensitive,” “Confidential,” and “Restricted.” The security solution must meet all of the following requirements:

Each object must be encrypted using a unique key.

Items that are stored in the “Restricted” bucket require two-factor authentication for decryption.

AWS KMS must automatically rotate encryption keys annually.

Which of the following meets these requirements?

A.
Create a Customer Master Key (CMK) for each data classification type, and enable the rotation of it annually. For the “Restricted” CMK, define the MFA policy within the key policy. Use S3 SSE-KMS to encrypt the objects.

B.
Create a CMK grant for each data classification type with EnableKeyRotation and MultiFactorAuthPresent set to true. S3 can then use the grants to encrypt each object with a unique CMK.

C.
Create a CMK for each data classification type, and within the CMK policy, enable rotation of it annually, and define the MFA policy. S3 can then create DEK grants to uniquely encrypt each object within the S3 bucket.

D.
Create a CMK with unique imported key material for each data classification type, and rotate them annually. For the “Restricted” key material, define the MFA policy in the key policy. Use S3 SSE-KMS to encrypt the objects.

Answer: A

Explanation:

QUESTION NO: 11

An organization wants to deploy a three-tier web application whereby the application servers run on Amazon EC2 instances. These EC2 instances need access to credentials that they will use to authenticate their SQL connections to an Amazon RDS DB instance. Also, AWS Lambda functions must issue queries to the RDS database by using the same database credentials.

The credentials must be stored so that the EC2 instances and the Lambda functions can access them. No other access is allowed. The access logs must record when the credentials were accessed and by whom.

What should the Security Engineer do to meet these requirements?

A.
Store the database credentials in AWS Key Management Service (AWS KMS). Create an IAM role with access to AWS KMS by using the EC2 and Lambda service principals in the role's trust policy. Add the role to an EC2 instance profile. Attach the instance profile to the EC2 instances. Set up Lambda to use the new role for execution.

B.
Store the database credentials in AWS KMS. Create an IAM role with access to KMS by using the EC2 and Lambda service principals in the role's trust policy. Add the role to an EC2 instance profile. Attach the instance profile to the EC2 instances and the Lambda function.

C.
Store the database credentials in AWS Secrets Manager. Create an IAM role with access to Secrets Manager by using the EC2 and Lambda service principals in the role's trust policy. Add the role to an EC2 instance profile. Attach the instance profile to the EC2 instances and the Lambda function.

D.
Store the database credentials in AWS Secrets Manager. Create an IAM role with access to Secrets Manager by using the EC2 and Lambda service principals in the role's trust policy. Add the role to an EC2 instance profile. Attach the instance profile to the EC2 instances. Set up Lambda to use the new role for execution.

Answer: D

Explanation:

QUESTION NO: 12

A company has a customer master key (CMK) with imported key materials. Company policy requires that all encryption keys must be rotated every year.

What can be done to implement the above policy?

A.
Enable automatic key rotation annually for the CMK.

B.
Use AWS Command Line Interface to create an AWS Lambda function to rotate the existing CMK annually.

C.
Import new key material to the existing CMK and manually rotate the CMK.

D.
Create a new CMK, import new key material to it, and point the key alias to the new CMK.

Answer: D
Explanation:

QUESTION NO: 13

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.

Answer: A
Explanation:

QUESTION NO: 14

An organization is using Amazon CloudWatch Logs with agents deployed on its Linux Amazon EC2 instances. The agent configuration files have been checked and the application log files to be pushed are configured correctly. A review has identified that logging from specific instances is missing.

Which steps should be taken to troubleshoot the issue? (Choose two.)

A.
Use an EC2 run command to confirm that the “awslogs” service is running on all instances.

B.
Verify that the permissions used by the agent allow creation of log groups/streams and to put log events.

C.
Check whether any application log entries were rejected because of invalid time stamps by reviewing /var/cwlogs/rejects.log.

D.
Check that the trust relationship grants the service “cwlogs.amazonaws.com” permission to write objects to the Amazon S3 staging bucket.

E.
Verify that the time zone on the application servers is in UTC.

Answer: B,C

Explanation:

QUESTION NO: 15

A Security Engineer must design a solution that enables the Incident Response team to audit for changes to a user’s IAM permissions in the case of a security incident.

How can this be accomplished?

A.
Use AWS Config to review the IAM policy assigned to users before and after the incident.

B.
Run the GenerateCredentialReport via the AWS CLI, and copy the output to Amazon S3 daily for auditing purposes.

C.
Copy AWS CloudFormation templates to S3, and audit for changes from the template.

D.
Use Amazon EC2 Systems Manager to deploy images, and review AWS CloudTrail logs for changes.

Answer: A

Explanation:

QUESTION NO: 16

A company has complex connectivity rules governing ingress, egress, and communications between Amazon EC2 instances. The rules are so complex that they cannot be implemented within the limits of the maximum number of security groups and network access control lists (network ACLs).

What mechanism will allow the company to implement all required network rules without incurring additional cost?

A.
Configure AWS WAF rules to implement the required rules.

B.
Use the operating system built-in, host-based firewall to implement the required rules.

C.
Use a NAT gateway to control ingress and egress according to the requirements.

D.
Launch an EC2-based firewall product from the AWS Marketplace, and implement the required rules in that product.

Answer: B

Explanation:

QUESTION NO: 17

An IAM user with fill EC2 permissions could bot start an Amazon EC2 instance after it was stopped for a maintenance task. Upon starting the instance, the instance state would change to “Pending”, but after a few seconds, it would switch back to “Stopped”.

An inspection revealed that the instance has attached Amazon EBS volumes that were encrypted by using a Customer Master Key (CMK). When these encrypted volumes were detached, the IAM user was able to start the EC2 instances.

The IAM user policy is as follows:

```
{
     "Version": "2012-10-17",
     "Statement": [
          {
               "Effect": "Allow",
               "Action": [
               <Action>
               ],
               "Resource": [
                    "arn:aws:kms:us-east-1:012345678910:key/ebs-encryption-key"
               ]
               <CONDITION>
          }
     ]
}
```


What additional items need to be added to the IAM user policy? (Choose two.)

A.
kms:GenerateDataKey

B.
kms:Decrypt

C.
kms:CreateGrant

D.
“Condition”: {

“Bool”: {

“kms:ViaService”: “ec2.us-west-2.amazonaws.com”

}

}

E.
“Condition”: {

“Bool”: {

“kms:GrantIsForAWSResource”: true

}

}

Answer: A,D

Explanation:

QUESTION NO: 18

A Security Administrator has a website hosted in Amazon S3. The Administrator has been given the following requirements:

Users may access the website by using an Amazon CloudFront distribution.

Users may not access the website directly by using an Amazon S3 URL.

Which configurations will support these requirements? (Choose two.)

A.
Associate an origin access identity with the CloudFront distribution.

B.
Implement a “Principal”: “cloudfront.amazonaws.com” condition in the S3 bucket policy.

C.
Modify the S3 bucket permissions so that only the origin access identity can access the bucket contents.

D.
Implement security groups so that the S3 bucket can be accessed only by using the intended CloudFront distribution.

E.
Configure the S3 bucket policy so that it is accessible only through VPC endpoints, and place the CloudFront distribution into the specified VPC.

Answer: A,C

Explanation:

QUESTION NO: 19

A Security Engineer has created an Amazon CloudWatch event that invokes an AWS Lambda function daily. The Lambda function runs an Amazon Athena query that checks AWS CloudTrail logs in Amazon S3 to detect whether any IAM user accounts or credentials have been created in the past 30 days. The results of the Athena query are created in the same S3 bucket. The Engineer runs a test execution of the Lambda function via the AWS Console, and the function runs successfully.

After several minutes, the Engineer finds that his Athena query has failed with the error message: “Insufficient Permissions”. The IAM permissions of the Security Engineer and the Lambda function are shown below:

Security Engineer

```
{
      "Version": "2012-10-17",
      "Statement": [
           {
                "Effect": "Allow",
                 "Action": [
                     "s3:*",
                     "iam:*",
                     "lambda:*",
                     "athena:Get*",
                     "athena:List*",
                     "cloudwatch:*"

                 ],
                 "Resource": "*"
           }
      ]
}
```

Lambda function execution role

```
{
      "Version": "2012-10-17",
      "Statement": [
           {
                "Effect": "Allow",
                 "Action": [
                     "athena:*",
                     "cloudwatch:*"
                 ],
                 "Resource": "*"
           }
      ]
}
```

What is causing the error?

A.
The Lambda function does not have permissions to start the Athena query execution.

B.
The Security Engineer does not have permissions to start the Athena query execution.

C.
The Athena service does not support invocation through Lambda.

D.
The Lambda function does not have permissions to access the CloudTrail S3 bucket.

Answer: B

Explanation:

QUESTION NO: 20

A company requires that IP packet data be inspected for invalid or malicious content.

Which of the following approaches achieve this requirement? (Choose two.)

A.
Configure a proxy solution on Amazon EC2 and route all outbound VPC traffic through it. Perform inspection within proxy software on the EC2 instance.

B.
Configure the host-based agent on each EC2 instance within the VPC. Perform inspection within the host-based agent.

C.
Enable VPC Flow Logs for all subnets in the VPC. Perform inspection from the Flow Log data within Amazon CloudWatch Logs.

D.
Configure Elastic Load Balancing (ELB) access logs. Perform inspection from the log data within the ELB access log files.

E.
Configure the CloudWatch Logs agent on each EC2 instance within the VPC. Perform inspection from the log data within CloudWatch Logs.

Answer: A,B

Explanation:

QUESTION NO: 21

An organization has a system in AWS that allows a large number of remote workers to submit data files. File sizes vary from a few kilobytes to several megabytes. A recent audit highlighted a concern that data files are not encrypted while in transit over untrusted networks.

Which solution would remediate the audit finding while minimizing the effort required?

A.
Upload an SSL certificate to IAM, and configure Amazon CloudFront with the passphrase for the private key.

B.
Call KMS.Encrypt() in the client, passing in the data file contents, and call KMS.Decrypt() server-side.

C.
Use AWS Certificate Manager to provision a certificate on an Elastic Load Balancing in front of the web service's servers.

D.
Create a new VPC with an Amazon VPC VPN endpoint, and update the web service's DNS record.

Answer: C
Explanation:

QUESTION NO: 22

Which option for the use of the AWS Key Management Service (KMS) supports key management best practices that focus on minimizing the potential scope of data exposed by a possible future key compromise?

A.
Use KMS automatic key rotation to replace the master key, and use this new master key for future encryption operations without re-encrypting previously encrypted data.

B.
Generate a new Customer Master Key (CMK), re-encrypt all existing data with the new CMK, and use it for all future encryption operations.

C.

Change the CMK alias every 90 days, and update key-calling applications with the new key alias.

D.
Change the CMK permissions to ensure that individuals who can provision keys are not the same individuals who can use the keys.

Answer: A

Explanation:

QUESTION NO: 23

A Security Engineer must enforce the use of only Amazon EC2, Amazon S3, Amazon RDS, Amazon DynamoDB, and AWS STS in specific accounts.

What is a scalable and efficient approach to meet this requirement?

A.
Set up an AWS Organizations hierarchy, and replace the FullAWSAccess policy with the following Service Control Policy for the governed organization units:

```
{
     "Version": "2012-10-17",
     "Statement": [
          {
               "Action": [
                    "dynamodb:*", "rds:*", "ec2:*",
"s3:*", "sts:*"
               ],
               "Effect": "Allow",
               "Resource": "*"
          }
     ]
}
```


B.
Create multiple IAM users for the regulated accounts, and attach the following policy statement to restrict services as required:

```
{
     "Version": "2012-10-17",
     "Statement": [
          {
               "Action": *
               "Effect": "Allow",
               "Resource": "*"
          }
{
               "NotAction": [
                    "dynamodb:*", "rds:*", "ec2:*",
"s3:*", "sts:*"
               ],
               "Effect": "Deny ",
               "Resource": "*"
          }
     ]
}
```


C.

Set up an Organizations hierarchy, replace the global FullAWSAccess with the following Service Control Policy at the top level:

```
{
     "Version": "2012-10-17",
     "Statement": [
          {
               "Action": [
                    "dynamodb:*", "rds:*", "ec2:*",
"s3:*", "sts:*"
               ],
               "Effect": "Allow",
               "Resource": "*"
          }
     ]
}
```


D.

Set up all users in the Active Directory for federated access to all accounts in the company. Associate Active Directory groups with IAM groups, and attach the following policy statement to restrict services as required:

```
{
     "Version": "2012-10-17",
     "Statement": [
          {
               "Action": *
               "Effect": "Allow",
               "Resource": "*"
          }
{
               "NotAction": [
                    "dynamodb:*", "rds:*", "ec2:*",
"s3:*", "sts:*"
               ],
               "Effect": "Deny ",
               "Resource": "*"
          }
     ]
}
```


Answer: A

Explanation:

QUESTION NO: 24

A company's database developer has just migrated an Amazon RDS database credential to be stored and managed by AWS Secrets Manager. The developer has also enabled rotation of the credential within the Secrets Manager console and set the rotation to change every 30 days.

After a short period of time, a number of existing applications have failed with authentication errors.

What is the MOST likely cause of the authentication errors?

A.
Migrating the credential to RDS requires that all access come through requests to the Secrets Manager.

B.
Enabling rotation in Secrets Manager causes the secret to rotate immediately, and the applications are using the earlier credential.

C.
The Secrets Manager IAM policy does not allow access to the RDS database.

D.
The Secrets Manager IAM policy does not allow access for the applications.

Answer: A
Explanation:

QUESTION NO: 25

A Security Engineer launches two Amazon EC2 instances in the same Amazon VPC but in separate Availability Zones. Each instance has a public IP address and is able to connect to external hosts on the internet. The two instances are able to communicate with each other by using their private IP addresses, but they are not able to communicate with each other when using their public IP addresses.

Which action should the Security Engineer take to allow communication over the public IP addresses?

A.
Associate the instances to the same security groups.

B.
Add 0.0.0.0/0 to the egress rules of the instance security groups.

C.
Add the instance IDs to the ingress rules of the instance security groups.

D.
Add the public IP addresses to the ingress rules of the instance security groups.

Answer: A
Explanation:

QUESTION NO: 26

The Security Engineer is managing a web application that processes highly sensitive personal information. The application runs on Amazon EC2. The application has strict compliance requirements, which instruct that all incoming traffic to the application is protected from common web exploits and that all outgoing traffic from the EC2 instances is restricted to specific whitelisted URLs.

Which architecture should the Security Engineer use to meet these requirements?

A.
Use AWS Shield to scan inbound traffic for web exploits. Use VPC Flow Logs and AWS Lambda to restrict egress traffic to specific whitelisted URLs.

B.
Use AWS Shield to scan inbound traffic for web exploits. Use a third-party AWS Marketplace solution to restrict egress traffic to specific whitelisted URLs.

C.
Use AWS WAF to scan inbound traffic for web exploits. Use VPC Flow Logs and AWS Lambda to restrict egress traffic to specific whitelisted URLs.

D.
Use AWS WAF to scan inbound traffic for web exploits. Use a third-party AWS Marketplace solution to restrict egress traffic to specific whitelisted URLs.

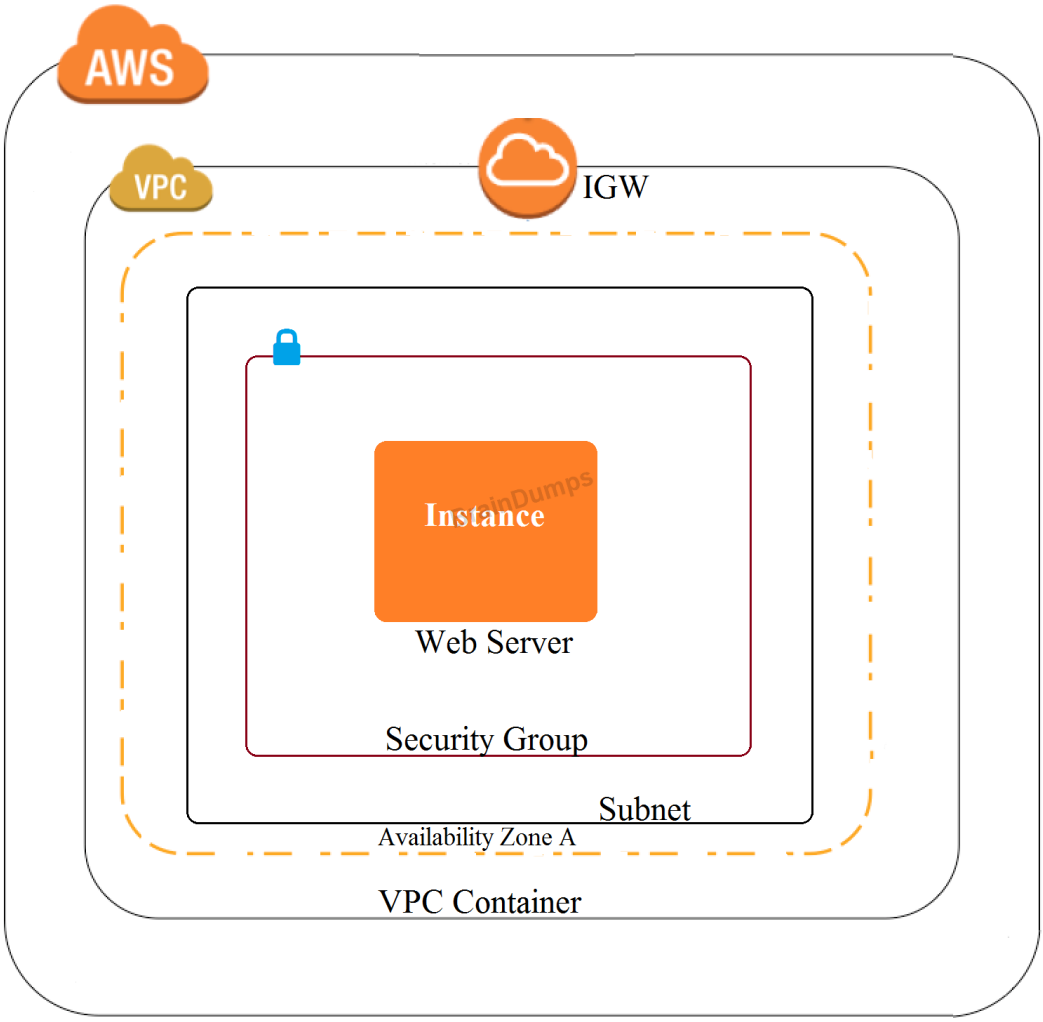
Answer: D

Explanation:

QUESTION NO: 27

A company recently experienced a DDoS attack that prevented its web server from serving content. The website is static and hosts only HTML, CSS, and PDF files that users download.

Based on the architecture shown in the image, what is the BEST way to protect the site against future attacks while minimizing the ongoing operational overhead?



A.
Move all the files to an Amazon S3 bucket. Have the web server serve the files from the S3 bucket.

B.
Launch a second Amazon EC2 instance in a new subnet. Launch an Application Load Balancer in front of both instances.

C.
Launch an Application Load Balancer in front of the EC2 instance. Create an Amazon CloudFront distribution in front of the Application Load Balancer.

D.
Move all the files to an Amazon S3 bucket. Create a CloudFront distribution in front of the bucket and terminate the web server.

Answer: A

Explanation:

QUESTION NO: 28

The Information Technology department has stopped using Classic Load Balancers and switched to Application Load Balancers to save costs. After the switch, some users on older devices are no longer able to connect to the website.

What is causing this situation?

A.
Application Load Balancers do not support older web browsers.

B.
The Perfect Forward Secrecy settings are not configured correctly.

C.
The intermediate certificate is installed within the Application Load Balancer.

D.
The cipher suites on the Application Load Balancers are blocking connections.

Answer: C
Explanation:

QUESTION NO: 29

A security team is responsible for reviewing AWS API call activity in the cloud environment for security violations. These events must be recorded and retained in a centralized location for both current and future AWS regions.

What is the SIMPLEST way to meet these requirements?

A.
Enable AWS Trusted Advisor security checks in the AWS Console, and report all security incidents for all regions.

B.
Enable AWS CloudTrail by creating individual trails for each region, and specify a single Amazon S3 bucket to receive log files for later analysis.

C.
Enable AWS CloudTrail by creating a new trail and applying the trail to all regions. Specify a single Amazon S3 bucket as the storage location.

D.
Enable Amazon CloudWatch logging for all AWS services across all regions, and aggregate them to a single Amazon S3 bucket for later analysis.

Answer: B
Reference: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-create-a-trail-using-the-console-first-time.html

QUESTION NO: 30

A Security Administrator is performing a log analysis as a result of a suspected AWS account compromise. The Administrator wants to analyze suspicious AWS CloudTrail log files but is overwhelmed by the volume of audit logs being generated.

What approach enables the Administrator to search through the logs MOST efficiently?

A.
Implement a “write-only” CloudTrail event filter to detect any modifications to the AWS account resources.

B.
Configure Amazon Macie to classify and discover sensitive data in the Amazon S3 bucket that contains the CloudTrail audit logs.

C.
Configure Amazon Athena to read from the CloudTrail S3 bucket and query the logs to examine account activities.

D.
Enable Amazon S3 event notifications to trigger an AWS Lambda function that sends an email alarm when there are new CloudTrail API entries.

Answer: C
Reference: https://docs.aws.amazon.com/athena/latest/ug/cloudtrail-logs.html

QUESTION NO: 31

During a recent security audit, it was discovered that multiple teams in a large organization have placed restricted data in multiple Amazon S3 buckets, and the data may have been exposed. The auditor has requested that the organization identify all possible objects that contain personally identifiable information (PII) and then determine whether this information has been accessed.

What solution will allow the Security team to complete this request?

A.
Using Amazon Athena, query the impacted S3 buckets by using the PII query identifier function. Then, create a new Amazon CloudWatch metric for Amazon S3 object access to alert when the objects are accessed.

B.
Enable Amazon Macie on the S3 buckets that were impacted, then perform data classification. For identified objects that contain PII, use the research function for auditing AWS CloudTrail logs and S3 bucket logs for GET operations.

C.
Enable Amazon GuardDuty and enable the PII rule set on the S3 buckets that were impacted, then perform data classification. Using the PII findings report from GuardDuty, query the S3 bucket logs by using Athena for GET operations.

D.
Enable Amazon Inspector on the S3 buckets that were impacted, then perform data classification. For identified objects that contain PII, query the S3 bucket logs by using Athena for GET operations.

Answer: B

Explanation:

QUESTION NO: 32

During a recent internal investigation, it was discovered that all API logging was disabled in a production account, and the root user had created new API keys that appear to have been used several times.

What could have been done to detect and automatically remediate the incident?

A.
Using Amazon Inspector, review all of the API calls and configure the inspector agent to leverage SNS topics to notify security of the change to AWS CloudTrail, and revoke the new API keys for the root user.

B.
Using AWS Config, create a config rule that detects when AWS CloudTrail is disabled, as well as any calls to the root user create-api-key. Then use a Lambda function to re-enable CloudTrail logs and deactivate the root API keys.

C.
Using Amazon CloudWatch, create a CloudWatch event that detects AWS CloudTrail deactivation and a separate Amazon Trusted Advisor check to automatically detect the creation of root API

keys. Then use a Lambda function to enable AWS CloudTrail and deactivate the root API keys.

D.
Using Amazon CloudTrail, create a new CloudTrail event that detects the deactivation of CloudTrail logs, and a separate CloudTrail event that detects the creation of root API keys. Then use a Lambda function to enable CloudTrail and deactivate the root API keys.

Answer: C
Explanation:

QUESTION NO: 33

An application has a requirement to be resilient across not only Availability Zones within the application's primary region but also be available within another region altogether.

Which of the following supports this requirement for AWS resources that are encrypted by AWS KMS?

A.
Copy the application's AWS KMS CMK from the source region to the target region so that it can be used to decrypt the resource after it is copied to the target region.

B.
Configure AWS KMS to automatically synchronize the CMK between regions so that it can be used to decrypt the resource in the target region.

C.
Use AWS services that replicate data across regions, and re-wrap the data encryption key created in the source region by using the CMK in the target region so that the target region's CMK can decrypt the database encryption key.

D.
Configure the target region's AWS service to communicate with the source region's AWS KMS so that it can decrypt the resource in the target region.

Answer: C
Explanation:

QUESTION NO: 34

An organization policy states that all encryption keys must be automatically rotated every 12

months.

Which AWS Key Management Service (KMS) key type should be used to meet this requirement?

A.
AWS managed Customer Master Key (CMK)

B.
Customer managed CMK with AWS generated key material

C.
Customer managed CMK with imported key material

D.
AWS managed data key

Answer: A
Reference: https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html

QUESTION NO: 35

A Security Engineer received an AWS Abuse Notice listing EC2 instance IDs that are reportedly abusing other hosts.

Which action should the Engineer take based on this situation? (Choose three.)

A.
Use AWS Artifact to capture an exact image of the state of each instance.

B.
Create EBS Snapshots of each of the volumes attached to the compromised instances.

C.
Capture a memory dump.

D.
Log in to each instance with administrative credentials to restart the instance.

E.
Revoke all network ingress and egress except for to/from a forensics workstation.

F.
Run Auto Recovery for Amazon EC2.

Answer: A,B,C

Explanation:

QUESTION NO: 36

A Security Administrator is configuring an Amazon S3 bucket and must meet the following security requirements:

Encryption in transit

Encryption at rest

Logging of all object retrievals in AWS CloudTrail

Which of the following meet these security requirements? (Choose three.)

A.
Specify “aws:SecureTransport”: “true” within a condition in the S3 bucket policy.

B.
Enable a security group for the S3 bucket that allows port 443, but not port 80.

C.
Set up default encryption for the S3 bucket.

D.
Enable Amazon CloudWatch Logs for the AWS account.

E.
Enable API logging of data events for all S3 objects.

F.
Enable S3 object versioning for the S3 bucket.

Answer: A,C,E
Reference:

https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/log-s3-data-events.html

QUESTION NO: 37

What is the function of the following AWS Key Management Service (KMS) key policy attached to

a customer master key (CMK)?

```
{
  "Effect": "Allow",
  "Principal": {
   "AWS": "arn:aws:iam::111122223333:user/ExampleUser"
  },
  "Action": [
   "kms:Encrypt",
   "kms:Decrypt",
   "kms: GenerateDataKey*",
   "kms:CreateGrant",
   "kms:ListGrants"

  ],
  "Resource": "*",
  "Condition": {
   "StringEquals": {
    "kms:ViaService": [
     "workmail.us-west-2.amazonaws.com",
     "ses.us-west-2.amazonaws.com"
    ]
   }
  }
 }
```


A.
The Amazon WorkMail and Amazon SES services have delegated KMS encrypt and decrypt permissions to the ExampleUser principal in the 111122223333 account.

B.
The ExampleUser principal can transparently encrypt and decrypt email exchanges specifically between ExampleUser and AWS.

C.
The CMK is to be used for encrypting and decrypting only when the principal is ExampleUser and the request comes from WorkMail or SES in the specified region.

D.
The key policy allows WorkMail or SES to encrypt or decrypt on behalf of the user for any CMK in the account.

Answer: C
Reference:

https://docs.aws.amazon.com/kms/latest/developerguide/policy-conditions.html#conditions-kms-via-service

QUESTION NO: 38

A Security Engineer who was reviewing AWS Key Management Service (AWS KMS) key policies found this statement in each key policy in the company AWS account.

```
{
      "Sid": "Enable IAM User Permissions",
      "Effect": "Allow",
      "Principal": {
           "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": "kms:*",
      "Resource": "*"
}
```


What does the statement allow?

A.
All principals from all AWS accounts to use the key.

B.
Only the root user from account 111122223333 to use the key.

C.
All principals from account 111122223333 to use the key but only on Amazon S3.

D.
Only principals from account 111122223333 that have an IAM policy applied that grants access to this key to use the key.

Answer: D
Reference: https://docs.aws.amazon.com/kms/latest/developerguide/key-policies.html

QUESTION NO: 39

A Software Engineer wrote a customized reporting service that will run on a fleet of Amazon EC2 instances. The company security policy states that application logs for the reporting service must be centrally collected.

What is the MOST efficient way to meet these requirements?

A.

Write an AWS Lambda function that logs into the EC2 instance to pull the application logs from the EC2 instance and persists them into an Amazon S3 bucket.

B.
Enable AWS CloudTrail logging for the AWS account, create a new Amazon S3 bucket, and then configure Amazon CloudWatch Logs to receive the application logs from CloudTrail.

C.
Create a simple cron job on the EC2 instances that synchronizes the application logs to an Amazon S3 bucket by using rsync.

D.
Install the Amazon CloudWatch Logs Agent on the EC2 instances, and configure it to send the application logs to CloudWatch Logs.

Answer: D
Reference:

https://aws.amazon.com/blogs/devops/new-how-to-better-monitor-your-custom-application-metrics-using-amazon-cloudwatch-agent/

QUESTION NO: 40

A Security Engineer is trying to determine whether the encryption keys used in an AWS service are in compliance with certain regulatory standards.

Which of the following actions should the Engineer perform to get further guidance?

A.
Read the AWS Customer Agreement.

B.
Use AWS Artifact to access AWS compliance reports.

C.
Post the question on the AWS Discussion Forums.

D.
Run AWS Config and evaluate the configuration outputs.

Answer: B
Explanation:

QUESTION NO: 41

The Development team receives an error message each time the team members attempt to encrypt or decrypt a Secure String parameter from the SSM Parameter Store by using an AWS KMS customer managed key (CMK).

Which CMK-related issues could be responsible? (Choose two.)

A.
The CMK specified in the application does not exist.

B.
The CMK specified in the application is currently in use.

C.
The CMK specified in the application is using the CMK KeyID instead of CMK Amazon Resource Name.

D.
The CMK specified in the application is not enabled.

E.
The CMK specified in the application is using an alias.

Answer: C,D
Reference: https://docs.aws.amazon.com/kms/latest/developerguide/services-parameter-store.html

QUESTION NO: 42

An application has been written that publishes custom metrics to Amazon CloudWatch. Recently, IAM changes have been made on the account and the metrics are no longer being reported.

Which of the following is the LEAST permissive solution that will allow the metrics to be delivered?

A.
Add a statement to the IAM policy used by the application to allow logs:putLogEvents and logs:createLogStream

B.
Modify the IAM role used by the application by adding the CloudWatchFullAccess managed policy.

C.
Add a statement to the IAM policy used by the application to allow cloudwatch:putMetricData.

D.
Add a trust relationship to the IAM role used by the application for cloudwatch.amazonaws.com.

Answer: C
Explanation:

QUESTION NO: 43

A Developer's laptop was stolen. The laptop was not encrypted, and it contained the SSH key used to access multiple Amazon EC2 instances. A Security Engineer has verified that the key has not been used, and has blocked port 22 to all EC2 instances while developing a response plan.

How can the Security Engineer further protect currently running instances?

A.
Delete the key-pair key from the EC2 console, then create a new key pair.

B.
Use the modify-instance-attribute API to change the key on any EC2 instance that is using the key.

C.
Use the EC2 RunCommand to modify the authorized_keys file on any EC2 instance that is using the key.

D.
Update the key pair in any AMI used to launch the EC2 instances, then restart the EC2 instances.

Answer: C
Reference: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html#delete-key-pair

QUESTION NO: 44

An organization has tens of applications deployed on thousands of Amazon EC2 instances. During testing, the Application team needs information to let them know whether the network access control lists (network ACLs) and security groups are working as expected.

How can the Application team’s requirements be met?

A.
Turn on VPC Flow Logs, send the logs to Amazon S3, and use Amazon Athena to query the logs.

B.
Install an Amazon Inspector agent on each EC2 instance, send the logs to Amazon S3, and use Amazon EMR to query the logs.

C.
Create an AWS Config rule for each network ACL and security group configuration, send the logs to Amazon S3, and use Amazon Athena to query the logs.

D.
Turn on AWS CloudTrail, send the trails to Amazon S3, and use AWS Lambda to query the trails.

Answer: A
Reference:

https://aws.amazon.com/blogs/aws/vpc-flow-logs-log-and-view-network-traffic-flows/

QUESTION NO: 45

An application outputs logs to a text file. The logs must be continuously monitored for security incidents.

Which design will meet the requirements with MINIMUM effort?

A.
Create a scheduled process to copy the component’s logs into Amazon S3. Use S3 events to trigger a Lambda function that updates Amazon CloudWatch metrics with the log data. Set up CloudWatch alerts based on the metrics.

B.
Install and configure the Amazon CloudWatch Logs agent on the application’s EC2 instance. Create a CloudWatch metric filter to monitor the application logs. Set up CloudWatch alerts based on the metrics.

C.
Create a scheduled process to copy the application log files to AWS CloudTrail. Use S3 events to trigger Lambda functions that update CloudWatch metrics with the log data. Set up CloudWatch alerts based on the metrics.

D.

Create a file watcher that copies data to Amazon Kinesis when the application writes to the log file. Have Kinesis trigger a Lambda function to update Amazon CloudWatch metrics with the log data. Set up CloudWatch alerts based on the metrics.

Answer: A

Explanation:

QUESTION NO: 46

The Security Engineer for a mobile game has to implement a method to authenticate users so that they can save their progress. Because most of the users are part of the same OpenID-Connect compatible social media website, the Security Engineer would like to use that as the identity provider.

Which solution is the SIMPLEST way to allow the authentication of users using their social media identities?

A.
Amazon Cognito

B.
AssumeRoleWithWebIdentity API

C.
Amazon Cloud Directory

D.
Active Directory (AD) Connector

Answer: A
Reference: https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-pools-identity-provider.html

QUESTION NO: 47

A Software Engineer is trying to figure out why network connectivity to an Amazon EC2 instance does not appear to be working correctly. Its security group allows inbound HTTP traffic from 0.0.0.0/0, and the outbound rules have not been modified from the default. A custom network ACL associated with its subnet allows inbound HTTP traffic from 0.0.0.0/0 and has no outbound rules.

What would resolve the connectivity issue?

A.
The outbound rules on the security group do not allow the response to be sent to the client on the ephemeral port range.

B.
The outbound rules on the security group do not allow the response to be sent to the client on the HTTP port.

C.
An outbound rule must be added to the network ACL to allow the response to be sent to the client on the ephemeral port range.

D.
An outbound rule must be added to the network ACL to allow the response to be sent to the client on the HTTP port.

Answer: D
Explanation:

QUESTION NO: 48

A Security Engineer has been asked to create an automated process to disable IAM user access keys that are more than three months old.

Which of the following options should the Security Engineer use?

A.
In the AWS Console, choose the IAM service and select “Users”. Review the “Access Key Age” column.

B.
Define an IAM policy that denies access if the key age is more than three months and apply to all users.

C.
Write a script that uses the GenerateCredentialReport, GetCredentialReport, and UpdateAccessKey APIs.

D.
Create an Amazon CloudWatch alarm to detect aged access keys and use an AWS Lambda function to disable the keys older than 90 days.

Answer: A
Reference: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html

QUESTION NO: 49

The InfoSec team has mandated that in the future only approved Amazon Machine Images (AMIs) can be used.

How can the InfoSec team ensure compliance with this mandate?

A.
Terminate all Amazon EC2 instances and relaunch them with approved AMIs.

B.
Patch all running instances by using AWS Systems Manager.

C.
Deploy AWS Config rules and check all running instances for compliance.

D.
Define a metric filter in Amazon CloudWatch Logs to verify compliance.

Answer: C
Explanation:

QUESTION NO: 50

A pharmaceutical company has digitized versions of historical prescriptions stored on premises. The company would like to move these prescriptions to AWS and perform analytics on the data in them. Any operation with this data requires that the data be encrypted in transit and at rest.

Which application flow would meet the data protection requirements on AWS?

A.
Digitized files -> Amazon Kinesis Data Analytics

B.
Digitized files -> Amazon Kinesis Data Firehose -> Amazon S3 -> Amazon Athena

C.
Digitized files -> Amazon Kinesis Data Streams -> Kinesis Client Library consumer -> Amazon S3

-> Athena

D.
Digitized files -> Amazon Kinesis Data Firehose -> Amazon Elasticsearch

Answer: A
Explanation:

QUESTION NO: 51

The Security Engineer created a new AWS Key Management Service (AWS KMS) key with the following key policy:

```
{
    "Effect": "Allow",
    "Principal": {"AWS": "arn:aws:iam::111122223333:root"),
    "Action": "kms:*";
    "Resource": "*"
}
```


What are the effects of the key policy? (Choose two.)

A.
The policy allows access for the AWS account 111122223333 to manage key access though IAM policies.

B.
The policy allows all IAM users in account 111122223333 to have full access to the KMS key.

C.
The policy allows the root user in account 111122223333 to have full access to the KMS key.

D.
The policy allows the KMS service-linked role in account 111122223333 to have full access to the KMS key.

E.
The policy allows all IAM roles in account 111122223333 to have full access to the KMS key.

Answer: A,B
Explanation:

QUESTION NO: 52

A company uses AWS Organization to manage 50 AWS accounts. The finance staff members log in as AWS IAM users in the FinanceDept AWS account. The staff members need to read the consolidated billing information in the MasterPayer AWS account. They should not be able to view any other resources in the MasterPayer AWS account. IAM access to billing has been enabled in the MasterPayer account.

Which of the following approaches grants the finance staff the permissions they require without granting any unnecessary permissions?

A.
Create an IAM group for the finance users in the FinanceDept account, then attach the AWS managed ReadOnlyAccess IAM policy to the group.

B.
Create an IAM group for the finance users in the MasterPayer account, then attach the AWS managed ReadOnlyAccess IAM policy to the group.

C.
Create an AWS IAM role in the FinanceDept account with the ViewBilling permission, then grant the finance users in the MasterPayer account the permission to assume that role.

D.
Create an AWS IAM role in the MasterPayer account with the ViewBilling permission, then grant the finance users in the FinanceDept account the permission to assume that role.

Answer: D

Explanation:

QUESTION NO: 53

A Solutions Architect is designing a web application that uses Amazon CloudFront, an Elastic Load Balancing Application Load Balancer, and an Auto Scaling group of Amazon EC2 instances. The load balancer and EC2 instances are in the US West (Oregon) region. It has been decided that encryption in transit is necessary by using a customer-branded domain name from the client to CloudFront and from CloudFront to the load balancer.

Assuming that AWS Certificate Manager is used, how many certificates will need to be generated?

A.
One in the US West (Oregon) region and one in the US East (Virginia) region.

B.
Two in the US West (Oregon) region and none in the US East (Virginia) region.

C.
One in the US West (Oregon) region and none in the US East (Virginia) region.

D.
Two in the US East (Virginia) region and none in the US West (Oregon) region.

Answer: A
Explanation:

QUESTION NO: 54

A Security Engineer has been asked to troubleshoot inbound connectivity to a web server. This single web server is not receiving inbound connections from the internet, whereas all other web servers are functioning properly.

The architecture includes network ACLs, security groups, and a virtual security appliance. In addition, the Development team has implemented Application Load Balancers (ALBs) to distribute the load across all web servers. It is a requirement that traffic between the web servers and the internet flow through the virtual security appliance.

The Security Engineer has verified the following:

1. The rule set in the Security Groups is correct

2. The rule set in the network ACLs is correct

3. The rule set in the virtual appliance is correct

Which of the following are other valid items to troubleshoot in this scenario? (Choose two.)

A.
Verify that the 0.0.0.0/0 route in the route table for the web server subnet points to a NAT gateway.

B.
Verify which Security Group is applied to the particular web server’s elastic network interface (ENI).

C.
Verify that the 0.0.0.0/0 route in the route table for the web server subnet points to the virtual security appliance.

D.
Verify the registered targets in the ALB.

E.
Verify that the 0.0.0.0/0 route in the public subnet points to a NAT gateway.

Answer: B,D

Explanation:

QUESTION NO: 55

Which approach will generate automated security alerts should too many unauthorized AWS API requests be identified?

A.
Create an Amazon CloudWatch metric filter that looks for API call error codes and then implement an alarm based on that metric's rate.

B.
Configure AWS CloudTrail to stream event data to Amazon Kinesis. Configure an AWS Lambda function on the stream to alarm when the threshold has been exceeded.

C.
Run an Amazon Athena SQL query against CloudTrail log files. Use Amazon QuickSight to create an operational dashboard.

D.
Use the Amazon Personal Health Dashboard to monitor the account's use of AWS services, and raise an alert if service error rates increase.

Answer: B

Explanation:

QUESTION NO: 56

A company has multiple production AWS accounts. Each account has AWS CloudTrail configured to log to a single Amazon S3 bucket in a central account. Two of the production accounts have trails that are not logging anything to the S3 bucket.

Which steps should be taken to troubleshoot the issue? (Choose three.)

A.
Verify that the log file prefix is set to the name of the S3 bucket where the logs should go.

B.
Verify that the S3 bucket policy allows access for CloudTrail from the production AWS account IDs.

C.
Create a new CloudTrail configuration in the account, and configure it to log to the account's S3 bucket.

D.
Confirm in the CloudTrail Console that each trail is active and healthy.

E.
Open the global CloudTrail configuration in the master account, and verify that the storage location is set to the correct S3 bucket.

F.
Confirm in the CloudTrail Console that the S3 bucket name is set correctly.

Answer: A,B,F

Explanation:

QUESTION NO: 57

Amazon CloudWatch Logs agent is successfully delivering logs to the CloudWatch Logs service. However, logs stop being delivered after the associated log stream has been active for a specific number of hours.

What steps are necessary to identify the cause of this phenomenon? (Choose two.)

A.
Ensure that file permissions for monitored files that allow the CloudWatch Logs agent to read the file have not been modified.

B.
Verify that the OS Log rotation rules are compatible with the configuration requirements for agent streaming.

C.
Configure an Amazon Kinesis producer to first put the logs into Amazon Kinesis Streams.

D.
Create a CloudWatch Logs metric to isolate a value that changes at least once during the period

before logging stops.

E.
Use AWS CloudFormation to dynamically create and maintain the configuration file for the CloudWatch Logs agent.

Answer: B,E
Explanation:

QUESTION NO: 58

A company has deployed a custom DNS server in AWS. The Security Engineer wants to ensure that Amazon EC2 instances cannot use the Amazon-provided DNS.

How can the Security Engineer block access to the Amazon-provided DNS in the VPC?

A.
Deny access to the Amazon DNS IP within all security groups.

B.
Add a rule to all network access control lists that deny access to the Amazon DNS IP.

C.
Add a route to all route tables that black holes traffic to the Amazon DNS IP.

D.
Disable DNS resolution within the VPC configuration.

Answer: D
Reference: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-dns.html

QUESTION NO: 59

An employee accidentally exposed an AWS access key and secret access key during a public presentation. The company Security Engineer immediately disabled the key.

How can the Engineer assess the impact of the key exposure and ensure that the credentials were not misused? (Choose two.)

A.

Analyze AWS CloudTrail for activity.

B.
Analyze Amazon CloudWatch Logs for activity.

C.
Download and analyze the IAM Use report from AWS Trusted Advisor.

D.
Analyze the resource inventory in AWS Config for IAM user activity.

E.
Download and analyze a credential report from IAM.

Answer: A,E
Explanation:

QUESTION NO: 60

Which of the following minimizes the potential attack surface for applications?

A.
Use security groups to provide stateful firewalls for Amazon EC2 instances at the hypervisor level.

B.
Use network ACLs to provide stateful firewalls at the VPC level to prevent access to any specific AWS resource.

C.
Use AWS Direct Connect for secure trusted connections between EC2 instances within private subnets.

D.
Design network security in a single layer within the perimeter network (also known as DMZ, demilitarized zone, and screened subnet) to facilitate quicker responses to threats.

Answer: B
Explanation:

QUESTION NO: 61

A distributed web application is installed across several EC2 instances in public subnets residing

in two Availability Zones. Apache logs show several intermittent brute-force attacks from hundreds of IP addresses at the layer 7 level over the past six months.

What would be the BEST way to reduce the potential impact of these attacks in the future?

A.
Use custom route tables to prevent malicious traffic from routing to the instances.

B.
Update security groups to deny traffic from the originating source IP addresses.

C.
Use network ACLs.

D.
Install intrusion prevention software (IPS) on each instance.

Answer: C
Explanation:

QUESTION NO: 62

A company plans to move most of its IT infrastructure to AWS. They want to leverage their existing on-premises Active Directory as an identity provider for AWS.

Which combination of steps should a Security Engineer take to federate the company's on-premises Active Directory with AWS? (Choose two.)

A.
Create IAM roles with permissions corresponding to each Active Directory group.

B.
Create IAM groups with permissions corresponding to each Active Directory group.

C.
Configure Amazon Cloud Directory to support a SAML provider.

D.
Configure Active Directory to add relying party trust between Active Directory and AWS.

E.
Configure Amazon Cognito to add relying party trust between Active Directory and AWS.

Answer: A,D
Reference:

https://aws.amazon.com/blogs/security/aws-federated-authentication-with-active-directory-federation-services-ad-fs/

QUESTION NO: 63

A security alert has been raised for an Amazon EC2 instance in a customer account that is exhibiting strange behavior. The Security Engineer must first isolate the EC2 instance and then use tools for further investigation.

What should the Security Engineer use to isolate and research this event? (Choose three.)

A.
AWS CloudTrail

B.
Amazon Athena

C.
AWS Key Management Service (AWS KMS)

D.
VPC Flow Logs

E.
AWS Firewall Manager

F.
Security groups

Answer: A,D,F
Explanation:

QUESTION NO: 64

A financial institution has the following security requirements:

Cloud-based users must be contained in a separate authentication domain.

Cloud-based users cannot access on-premises systems.

As part of standing up a cloud environment, the financial institution is creating a number of Amazon managed databases and Amazon EC2 instances. An Active Directory service exists on-premises that has all the administrator accounts, and these must be able to access the databases and instances.

How would the organization manage its resources in the MOST secure manner? (Choose two.)

A.
Configure an AWS Managed Microsoft AD to manage the cloud resources.

B.
Configure an additional on-premises Active Directory service to manage the cloud resources.

C.
Establish a one-way trust relationship from the existing Active Directory to the new Active Directory service.

D.
Establish a one-way trust relationship from the new Active Directory to the existing Active Directory service.

E.
Establish a two-way trust between the new and existing Active Directory services.

Answer: B,C

Explanation:

QUESTION NO: 65

An organization wants to be alerted when an unauthorized Amazon EC2 instance in its VPC performs a network port scan against other instances in the VPC. When the Security team performs its own internal tests in a separate account by using pre-approved third-party scanners from the AWS Marketplace, the Security team also then receives multiple Amazon GuardDuty events from Amazon CloudWatch alerting on its test activities.

How can the Security team suppress alerts about authorized security tests while still receiving alerts about the unauthorized activity?

A.
Use a filter in AWS CloudTrail to exclude the IP addresses of the Security team’s EC2 instances.

B.
Add the Elastic IP addresses of the Security team’s EC2 instances to a trusted IP list in Amazon

GuardDuty.

C.
Install the Amazon Inspector agent on the EC2 instances that the Security team uses.

D.
Grant the Security team's EC2 instances a role with permissions to call Amazon GuardDuty API operations.

Answer: C
Explanation:

QUESTION NO: 66

An organization is moving non-business-critical applications to AWS while maintaining a mission-critical application in an on-premises data center. An on-premises application must share limited confidential information with the applications in AWS. The internet performance is unpredictable.

Which configuration will ensure continued connectivity between sites MOST securely?

A.
VPN and a cached storage gateway

B.
AWS Snowball Edge

C.
VPN Gateway over AWS Direct Connect

D.
AWS Direct Connect

Answer: A
Explanation:

QUESTION NO: 67

An application has been built with Amazon EC2 instances that retrieve messages from Amazon SQS. Recently, IAM changes were made and the instances can no longer retrieve messages.

What actions should be taken to troubleshoot the issue while maintaining least privilege? (Choose two.)

A.
Configure and assign an MFA device to the role used by the instances.

B.
Verify that the SQS resource policy does not explicitly deny access to the role used by the instances.

C.
Verify that the access key attached to the role used by the instances is active.

D.
Attach the AmazonSQSFullAccess managed policy to the role used by the instances.

E.
Verify that the role attached to the instances contains policies that allow access to the queue.

Answer: B,E
Reference:

https://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-using-identity-based-policies.html

QUESTION NO: 68

A company has a forensic logging use case whereby several hundred applications running on Docker on EC2 need to send logs to a central location. The Security Engineer must create a logging solution that is able to perform real-time analytics on the log files, grants the ability to replay events, and persists data.

Which AWS Services, together, can satisfy this use case? (Choose two.)

A.
Amazon Elasticsearch

B.
Amazon Kinesis

C.
Amazon SQS

D.

Amazon CloudWatch

E.
Amazon Athena

Answer: B,D
Explanation:

QUESTION NO: 69

Which of the following is the most efficient way to automate the encryption of AWS CloudTrail logs using a Customer Master Key (CMK) in AWS KMS?

A.
Use the KMS direct encrypt function on the log data every time a CloudTrail log is generated.

B.
Use the default Amazon S3 server-side encryption with S3-managed keys to encrypt and decrypt the CloudTrail logs.

C.
Configure CloudTrail to use server-side encryption using KMS-managed keys to encrypt and decrypt CloudTrail logs.

D.
Use encrypted API endpoints so that all AWS API calls generate encrypted CloudTrail log entries using the TLS certificate from the encrypted API call.

Answer: C
Reference: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/encrypting-cloudtrail-log-files-with-aws-kms.html

QUESTION NO: 70

An organization is using AWS CloudTrail, Amazon CloudWatch Logs, and Amazon CloudWatch to send alerts when new access keys are created. However, the alerts are no longer appearing in the Security Operations mail box.

Which of the following actions would resolve this issue?

A.
In CloudTrail, verify that the trail logging bucket has a log prefix configured.

B.
In Amazon SNS, determine whether the “Account spend limit” has been reached for this alert.

C.
In SNS, ensure that the subscription used by these alerts has not been deleted.

D.
In CloudWatch, verify that the alarm threshold “consecutive periods” value is equal to, or greater than 1.

Answer: D
Explanation:

QUESTION NO: 71

A Security Engineer must add additional protection to a legacy web application by adding the following HTTP security headers:

-Content Security-Policy

-X-Frame-Options

-X-XSS-Protection

The Engineer does not have access to the source code of the legacy web application.

Which of the following approaches would meet this requirement?

A.
Configure an Amazon Route 53 routing policy to send all web traffic that does not include the required headers to a black hole.

B.
Implement an AWS Lambda@Edge origin response function that inserts the required headers.

C.
Migrate the legacy application to an Amazon S3 static website and front it with an Amazon CloudFront distribution.

D.
Construct an AWS WAF rule to replace existing HTTP headers with the required security headers

by using regular expressions.

Answer: B

Explanation:

QUESTION NO: 72

During a security event, it is discovered that some Amazon EC2 instances have not been sending Amazon CloudWatch logs.

Which steps can the Security Engineer take to troubleshoot this issue? (Choose two.)

A.
Connect to the EC2 instances that are not sending the appropriate logs and verify that the CloudWatch Logs agent is running.

B.
Log in to the AWS account and select CloudWatch Logs. Check for any monitored EC2 instances that are in the “Alerting” state and restart them using the EC2 console.

C.
Verify that the EC2 instances have a route to the public AWS API endpoints.

D.
Connect to the EC2 instances that are not sending logs. Use the command prompt to verify that the right permissions have been set for the Amazon SNS topic.

E.
Verify that the network access control lists and security groups of the EC2 instances have the access to send logs over SNMP.

Answer: A,B

Explanation:

QUESTION NO: 73

A Security Engineer discovers that developers have been adding rules to security groups that allow SSH and RDP traffic from 0.0.0.0/0 instead of the organization firewall IP.

What is the most efficient way to remediate the risk of this activity?

A.
Delete the internet gateway associated with the VPC.

B.
Use network access control lists to block source IP addresses matching 0.0.0.0/0.

C.
Use a host-based firewall to prevent access from all but the organization’s firewall IP.

D.
Use AWS Config rules to detect 0.0.0.0/0 and invoke an AWS Lambda function to update the security group with the organization's firewall IP.

Answer: B

Explanation:

QUESTION NO: 74

In response to the past DDoS attack experiences, a Security Engineer has set up an Amazon CloudFront distribution for an Amazon S3 bucket. There is concern that some users may bypass the CloudFront distribution and access the S3 bucket directly.

What must be done to prevent users from accessing the S3 objects directly by using URLs?

A.
Change the S3 bucket/object permission so that only the bucket owner has access.

B.
Set up a CloudFront origin access identity (OAI), and change the S3 bucket/object permission so that only the OAI has access.

C.
Create IAM roles for CloudFront, and change the S3 bucket/object permission so that only the IAM role has access.

D.
Redirect S3 bucket access to the corresponding CloudFront distribution.

Answer: B

Explanation:

QUESTION NO: 75

A company plans to move most of its IT infrastructure to AWS. The company wants to leverage its existing on-premises Active Directory as an identity provider for AWS.

Which steps should be taken to authenticate to AWS services using the company's on-premises Active Directory? (Choose three).

A.
Create IAM roles with permissions corresponding to each Active Directory group.

B.
Create IAM groups with permissions corresponding to each Active Directory group.

C.
Create a SAML provider with IAM.

D.
Create a SAML provider with Amazon Cloud Directory.

E.
Configure AWS as a trusted relying party for the Active Directory

F.
Configure IAM as a trusted relying party for Amazon Cloud Directory.

Answer: A,C,E
Reference: https://aws.amazon.com/blogs/security/aws-federated-authentication-with-active-directory-federation-services-ad-fs/

QUESTION NO: 76

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.

B.
Check the CloudWatch dashboards to ensure that there is a metric configured with an appropriate

dimension for security group changes.

C.
Verify that the Analyst's account is mapped to an IAM policy that includes permissions for cloudwatch: GetMetricStatistics and Cloudwatch: ListMetrics.

Answer: B

Explanation:

QUESTION NO: 77

Example.com hosts its internal document repository on Amazon EC2 instances. The application runs on EC2 instances and previously stored the documents on encrypted Amazon EBS volumes. To optimize the application for scale, example.com has moved the files to Amazon S3. The security team has mandated that all the files are securely deleted from the EBS volume, and it must certify that the data is unreadable before releasing the underlying disks.

Which of the following methods will ensure that the data is unreadable by anyone else?

A.
Change the volume encryption on the EBS volume to use a different encryption mechanism. Then, release the EBS volumes back to AWS.

B.
Release the volumes back to AWS. AWS immediately wipes the disk after it is deprovisioned.

C.
Delete the encryption key used to encrypt the EBS volume. Then, release the EBS volumes back to AWS.

D.
Delete the data by using the operating system delete commands. Run Quick Format on the drive and then release the EBS volumes back to AWS.

Answer: D

Explanation:

QUESTION NO: 78

A Systems Administrator has written the following Amazon S3 bucket policy designed to allow access to an S3 bucket for only an authorized AWS IAM user from the IP address range

10.10.10.0/24:

```
{
  “Version”: “2012-10-17”,
  “Id”: “S3Policy1”,
  “Statement”: [
  {
   “Sid”: [“OfficeAllowIP”],
   “Effect”: [“Allow”],
   “Principal”: [“*”],
   “Action”: [“s3:*”],
   “Resource”: [“arn:aws:s3:::Bucket”],
   “Condition”: {
     “IpAddress”: [
        {“aws: SourceIp”: “10.10.10.0/24”}
      ]
     }
  }]
}
```


When trying to download an object from the S3 bucket from 10.10.10.40, the IAM user receives an access denied message.

What does the Administrator need to change to grant access to the user?

A.
Change the “Resource” from “arn: aws:s3:::Bucket” to “arn:aws:s3:::Bucket/*”.

B.
Change the “Principal” from “*” to {AWS:”arn:aws:iam: : account-number: user/username”}

C.
Change the “Version” from “2012-10-17” to the last revised date of the policy

D.
Change the “Action” from [“s3:*”] to [“s3:GetObject”, “s3:ListBucket”]

Answer: A

Explanation:

QUESTION NO: 79

The Security Engineer has discovered that a new application that deals with highly sensitive data is storing Amazon S3 objects with the following key pattern, which itself contains highly sensitive data.

Pattern:

"randomID_datestamp_PII.csv"

Example:

"1234567_12302017_000-00-0000 csv"

The bucket where these objects are being stored is using server-side encryption (SSE).

Which solution is the most secure and cost-effective option to protect the sensitive data?

A.
Remove the sensitive data from the object name, and store the sensitive data using S3 user-defined metadata.

B.
Add an S3 bucket policy that denies the action s3:GetObject

C.
Use a random and unique S3 object key, and create an S3 metadata index in Amazon DynamoDB using client-side encrypted attributes.

D.
Store all sensitive objects in Binary Large Objects (BLOBS) in an encrypted Amazon RDS instance.

Answer: B
Explanation:

QUESTION NO: 80

AWS CloudTrail is being used to monitor API calls in an organization. An audit revealed that CloudTrail is failing to deliver events to Amazon S3 as expected.

What initial actions should be taken to allow delivery of CloudTrail events to S3? (Choose two.)

A.
Verify that the S3 bucket policy allow CloudTrail to write objects.

B.
Verify that the IAM role used by CloudTrail has access to write to Amazon CloudWatch Logs.

C.
Remove any lifecycle policies on the S3 bucket that are archiving objects to Amazon Glacier.

D.
Verify that the S3 bucket defined in CloudTrail exists.

E.
Verify that the log file prefix defined in CloudTrail exists in the S3 bucket.

Answer: D,E

Explanation:

QUESTION NO: 81

Due to new compliance requirements, a Security Engineer must enable encryption with customer-provided keys on corporate data that is stored in DynamoDB. The company wants to retain full control of the encryption keys.

Which DynamoDB feature should the Engineer use to achieve compliance'?

A.
Use AWS Certificate Manager to request a certificate. Use that certificate to encrypt data prior to uploading it to DynamoDB.

B.
Enable S3 server-side encryption with the customer-provided keys. Upload the data to Amazon S3, and then use S3Copy to move all data to DynamoDB

C.
Create a KMS master key. Generate per-record data keys and use them to encrypt data prior to uploading it to DynamoDS. Dispose of the cleartext and encrypted data keys after encryption without storing.

D.
Use the DynamoDB Java encryption client to encrypt data prior to uploading it to DynamoDB.

Answer: B

Explanation:

QUESTION NO: 82

A Security Engineer must design a system that can detect whether a file on an Amazon EC2 host has been modified. The system must then alert the Security Engineer of the modification.

What is the MOST efficient way to meet these requirements?

A.
Install antivirus software and ensure that signatures are up-to-date. Configure Amazon CloudWatch alarms to send alerts for security events.

B.
Install host-based IDS software to check for file integrity. Export the logs to Amazon CloudWatch Logs for monitoring and alerting.

C.
Export system log files to Amazon S3. Parse the log files using an AWS Lambda function that will send alerts of any unauthorized system login attempts through Amazon SNS.

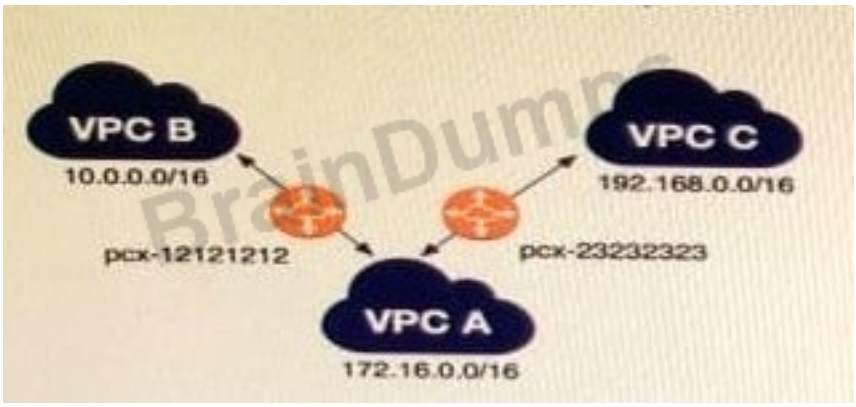
D.
Use Amazon CloudWatch Logs to detect file system changes. If a change is detected, automatically terminate and recreate the instance from the most recent AMI. Use Amazon SNS to send notification of the event.

Answer: D
Explanation:

QUESTION NO: 83

A company has multiple VPCs in their account that are peered, as shown in the diagram. A Security Engineer wants to perform penetration tests of the Amazon EC2 instances in all three VPCs.

How can this be accomplished? (Choose two.)



A.
Deploy a pre-authorized scanning engine from the AWS Marketplace into VPC B, and use it to scan instances in all three VPCs. Do not complete the penetration test request form.

B.
Deploy a pre-authorized scanning engine from the Marketplace into each VPC, and scan instances in each VPC from the scanning engine in that VPC. Do not complete the penetration test request form.

C.
Create a VPN connection from the data center to VPC A. Use an on-premises scanning engine to scan the instances in all three VPCs. Complete the penetration test request form for all three VPCs.

D.
Create a VPN connection from the data center to each of the three VPCs. Use an on-premises scanning engine to scan the instances in each VPC. Do not complete the penetration test request form.

E.
Create a VPN connection from the data center to each of the three VPCs. Use an on-premises scanning engine to scan the instances in each VPC. Complete the penetration test request form for all three VPCs.

Answer: C,E

Explanation:

QUESTION NO: 84

The Security Engineer is managing a traditional three-tier web application that is running on Amazon EC2 instances. The application has become the target of increasing numbers of malicious attacks from the Internet.

What steps should the Security Engineer take to check for known vulnerabilities and limit the attack surface? (Choose two.)

A.
Use AWS Certificate Manager to encrypt all traffic between the client and application servers.

B.
Review the application security groups to ensure that only the necessary ports are open.

C.
Use Elastic Load Balancing to offload Secure Sockets Layer encryption.

D.
Use Amazon Inspector to periodically scan the backend instances.

E.
Use AWS Key Management Services to encrypt all the traffic between the client and application servers.

Answer: B,D

Explanation:

QUESTION NO: 85

For compliance reasons, an organization limits the use of resources to three specific AWS regions. It wants to be alerted when any resources are launched in unapproved regions.

Which of the following approaches will provide alerts on any resources launched in an unapproved region?

A.
Develop an alerting mechanism based on processing AWS CloudTrail logs.

B.
Monitor Amazon S3 Event Notifications for objects stored in buckets in unapproved regions.

C.
Analyze Amazon CloudWatch Logs for activities in unapproved regions.

D.
Use AWS Trusted Advisor to alert on all resources being created.

Answer: A

Explanation:

QUESTION NO: 86

A company runs an application on AWS that needs to be accessed only by employees. Most employees work from the office, but others work remotely or travel.

How can the Security Engineer protect this workload so that only employees can access it?

A.
Add each employee’s home IP address to the security group for the application so that only those users can access the workload.

B.
Create a virtual gateway for VPN connectivity for each employee, and restrict access to the workload from within the VPC.

C.
Use a VPN appliance from the AWS Marketplace for users to connect to, and restrict workload access to traffic from that appliance.

D.
Route all traffic to the workload through AWS WAF. Add each employee’s home IP address into an AWS WAF rule, and block all other traffic.

Answer: B
Explanation:

QUESTION NO: 87

A Systems Engineer is troubleshooting the connectivity of a test environment that includes a virtual security appliance deployed inline. In addition to using the virtual security appliance, the Development team wants to use security groups and network ACLs to accomplish various security requirements in the environment.

What configuration is necessary to allow the virtual security appliance to route the traffic?

A.
Disable network ACLs.

B.
Configure the security appliance's elastic network interface for promiscuous mode.

C.
Disable the Network Source/Destination check on the security appliance's elastic network interface

D.
Place the security appliance in the public subnet with the internet gateway

Answer: D
Explanation:

QUESTION NO: 88

A Security Architect is evaluating managed solutions for storage of encryption keys. The requirements are:

-Storage is accessible by using only VPCs.

-Service has tamper-evident controls.

-Access logging is enabled.

-Storage has high availability.

Which of the following services meets these requirements?

A.
Amazon S3 with default encryption

B.
AWS CloudHSM

C.
Amazon DynamoDB with server-side encryption

D.
AWS Systems Manager Parameter Store

Answer: B
Reference: https://aws.amazon.com/blogs/aws/aws-cloud-hsm-secure-key-storage-and-cryptographic-operations/

QUESTION NO: 89

An AWS account includes two S3 buckets: bucket1 and bucket2. The bucket2 does not have a policy defined, but bucket1 has the following bucket policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam: : 123456789012: user/alice"},
       "Action": "s3:*",
       "Resource": ["arn:aws:s3: : :bucket1", "arn:aws:s3: : :bucket1/*"]
    }
  ]
}
```

In addition, the same account has an IAM User named "alice", with the following IAM policy.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "s3:*",
    "Resource": ["arn:aws:s3: : :bucket2", "arn:aws:s3: : :bucket2/*"]
    }
  ]
}
```

Which buckets can user "alice" access?

A.
Bucket1 only

B.
Bucket2 only

C.
Both bucket1 and bucket2

D.
Neither bucket1 nor bucket2

Answer: C

Explanation:

QUESTION NO: 90

An organization has three applications running on AWS, each accessing the same data on Amazon S3. The data on Amazon S3 is server-side encrypted by using an AWS KMS Customer Master Key (CMK).

What is the recommended method to ensure that each application has its own programmatic access control permissions on the KMS CMK?

A.
Change the key policy permissions associated with the KMS CMK for each application when it must access the data in Amazon S3.

B.
Have each application assume an IAM role that provides permissions to use the AWS Certificate Manager CMK.

C.
Have each application use a grant on the KMS CMK to add or remove specific access controls on the KMS CMK.

D.
Have each application use an IAM policy in a user context to have specific access permissions on the KMS CMK.

Answer: D
Explanation:

QUESTION NO: 91

The Security Engineer is given the following requirements for an application that is running on Amazon EC2 and managed by using AWS CloudFormation templates with EC2 Auto Scaling groups:

-Have the EC2 instances bootstrapped to connect to a backend database.

-Ensure that the database credentials are handled securely.

-Ensure that retrievals of database credentials are logged.

Which of the following is the MOST efficient way to meet these requirements?

A.
Pass databases credentials to EC2 by using CloudFormation stack parameters with the property set to true. Ensure that the instance is configured to log to Amazon CloudWatch Logs.

B.
Store database passwords in AWS Systems Manager Parameter Store by using SecureString parameters. Set the IAM role for the EC2 instance profile to allow access to the parameters.

C.
Create an AWS Lambda that ingests the database password and persists it to Amazon S3 with server-side encryption. Have the EC2 instances retrieve the S3 object on startup, and log all script invocations to syslog.

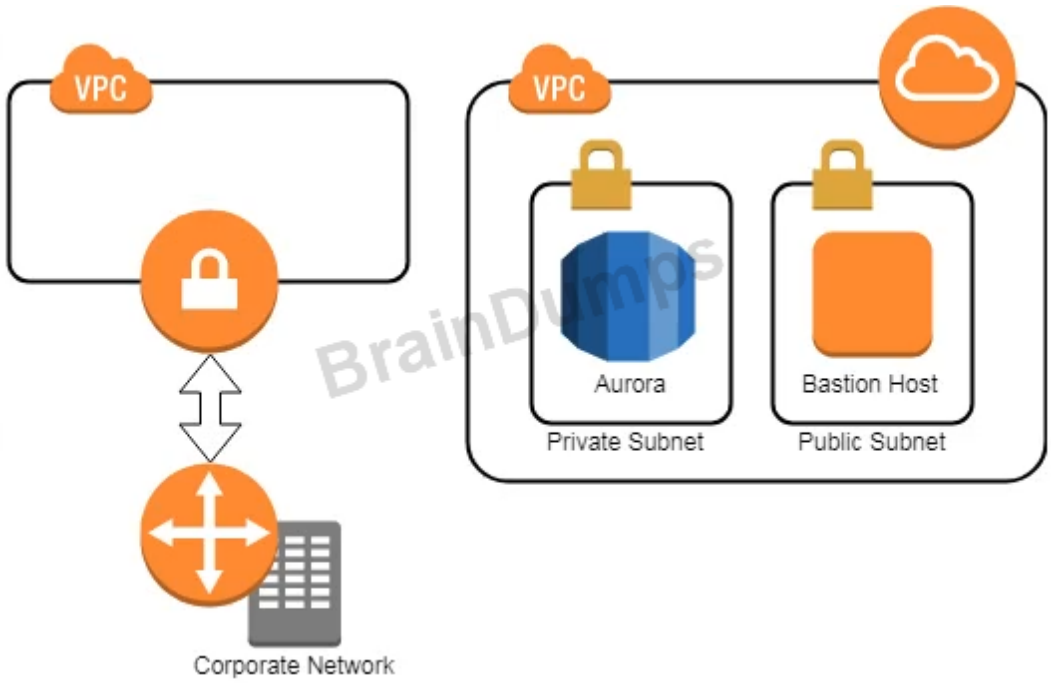
D.
Write a script that is passed in as UserData so that it is executed upon launch of the EC2 instance. Ensure that the instance is configured to log to Amazon CloudWatch Logs.

Answer: B

Explanation:

QUESTION NO: 92

A company has two AWS accounts, each containing one VPC. The first VPC has a VPN connection with its corporate network. The second VPC, without a VPN, hosts an Amazon Aurora database cluster in private subnets. Developers manage the Aurora database from a bastion host in a public subnet as shown in the image.



A security review has flagged this architecture as vulnerable, and a Security Engineer has been asked to make this design more secure. The company has a short deadline and a second VPN connection to the Aurora account is not possible.

How can a Security Engineer securely set up the bastion host?

A.
Move the bastion host to the VPC with VPN connectivity. Create a VPC peering relationship between the bastion host VPC and Aurora VPC.

B.
Create a SSH port forwarding tunnel on the Developer's workstation to the bastion host to ensure that only authorized SSH clients can access the bastion host.

C.
Move the bastion host to the VPC with VPN connectivity. Create a cross-account trust relationship between the bastion VPC and Aurora VPC, and update the Aurora security group for the relationship.

D.
Create an AWS Direct Connect connection between the corporate network and the Aurora account, and adjust the Aurora security group for this connection.

Answer: B
Explanation:

QUESTION NO: 93

An organization operates a web application that serves users globally. The application runs on Amazon EC2 instances behind an Application Load Balancer. There is an Amazon CloudFront distribution in front of the load balancer, and the organization uses AWS WAF. The application is currently experiencing a volumetric attack whereby the attacker is exploiting a bug in a popular mobile game.

The application is being flooded with HTTP requests from all over the world with the User-Agent set to the following string: Mozilla/5.0 (compatible; ExampleCorp; ExampleGame/1.22; Mobile/1.0)

What mitigation can be applied to block attacks resulting from this bug while continuing to service legitimate requests?

A.
Create a rule in AWS WAF rules with conditions that block requests based on the presence of ExampleGame/1.22 in the User-Agent header

B.
Create a geographic restriction on the CloudFront distribution to prevent access to the application from most geographic regions

C.
Create a rate-based rule in AWS WAF to limit the total number of requests that the web application services.

D.
Create an IP-based blacklist in AWS WAF to block the IP addresses that are originating from requests that contain ExampleGame/1.22 in the User-Agent header.

Answer: C

Explanation:

QUESTION NO: 94

Some highly sensitive analytics workloads are to be moved to Amazon EC2 hosts. Threat modeling has found that a risk exists where a subnet could be maliciously or accidentally exposed to the internet.

Which of the following mitigations should be recommended?

A.
Use AWS Config to detect whether an Internet Gateway is added and use an AWS Lambda function to provide auto-remediation.

B.
Within the Amazon VPC configuration, mark the VPC as private and disable Elastic IP addresses.

C.
Use IPv6 addressing exclusively on the EC2 hosts, as this prevents the hosts from being accessed from the internet.

D.
Move the workload to a Dedicated Host, as this provides additional network security controls and monitoring.

Answer: B

Explanation:

QUESTION NO: 95

A Developer who is following AWS best practices for secure code development requires an application to encrypt sensitive data to be stored at rest, locally in the application, using AWS KMS. What is the simplest and MOST secure way to decrypt this data when required?

A.
Request KMS to provide the stored unencrypted data key and then use the retrieved data key to decrypt the data.

B.
Keep the plaintext data key stored in Amazon DynamoDB protected with IAM policies. Query DynamoDB to retrieve the data key to decrypt the data

C.
Use the Encrypt API to store an encrypted version of the data key with another customer managed key. Decrypt the data key and use it to decrypt the data when required.

D.
Store the encrypted data key alongside the encrypted data. Use the Decrypt API to retrieve the data key to decrypt the data when required.

Answer: D

Explanation:

QUESTION NO: 96

A Security Administrator at a university is configuring a fleet of Amazon EC2 instances. The EC2 instances are shared among students, and non-root SSH access is allowed. The Administrator is concerned about students attacking other AWS account resources by using the EC2 instance metadata service.

What can the Administrator do to protect against this potential attack?

A.
Disable the EC2 instance metadata service.

B.
Log all student SSH interactive session activity.

C.
Implement iptables-based restrictions on the instances.

D.
Install the Amazon Inspector agent on the instances.

Answer: C
Explanation:

QUESTION NO: 97

An organization receives an alert that indicates that an EC2 instance behind an ELB Classic Load Balancer has been compromised.

What techniques will limit lateral movement and allow evidence gathering?

A.
Remove the instance from the load balancer and terminate it.

B.
Remove the instance from the load balancer, and shut down access to the instance by tightening the security group.

C.
Reboot the instance and check for any Amazon CloudWatch alarms.

D.
Stop the instance and make a snapshot of the root EBS volume.

Answer: B

Explanation:

QUESTION NO: 98

A Development team has asked for help configuring the IAM roles and policies in a new AWS account. The team using the account expects to have hundreds of master keys and therefore does not want to manage access control for customer master keys (CMKs).

Which of the following will allow the team to manage AWS KMS permissions in IAM without the complexity of editing individual key policies?

A.
The account's CMK key policy must allow the account's IAM roles to perform KMS EnableKey.

B.
Newly created CMKs must have a key policy that allows the root principal to perform all actions.

C.
Newly created CMKs must allow the root principal to perform the kms CreateGrant API operation.

D.
Newly created CMKs must mirror the IAM policy of the KMS key administrator.

Answer: D
Explanation:

QUESTION NO: 99

An Amazon EC2 instance is part of an EC2 Auto Scaling group that is behind an Application Load Balancer (ALB). It is suspected that the EC2 instance has been compromised.

Which steps should be taken to investigate the suspected compromise? (Choose three.)

A.
Detach the elastic network interface from the EC2 instance.

B.
Initiate an Amazon Elastic Block Store volume snapshot of all volumes on the EC2 instance.

C.
Disable any Amazon Route 53 health checks associated with the EC2 instance.

D.
De-register the EC2 instance from the ALB and detach it from the Auto Scaling group.

E.
Attach a security group that has restrictive ingress and egress rules to the EC2 instance.

F.
Add a rule to an AWS WAF to block access to the EC2 instance.

Answer: A,E,F

Explanation:

QUESTION NO: 100

A company has five AWS accounts and wants to use AWS CloudTrail to log API calls. The log files must be stored in an Amazon S3 bucket that resides in a new account specifically built for centralized services with a unique top-level prefix for each trail. The configuration must also enable detection of any modification to the logs.

Which of the following steps will implement these requirements? (Choose three.)

A.
Create a new S3 bucket in a separate AWS account for centralized storage of CloudTrail logs, and enable “Log File Validation” on all trails.

B.
Use an existing S3 bucket in one of the accounts, apply a bucket policy to the new centralized S3 bucket that permits the CloudTrail service to use the "s3: PutObject" action and the "s3 GetBucketACL" action, and specify the appropriate resource ARNs for the CloudTrail trails.

C.
Apply a bucket policy to the new centralized S3 bucket that permits the CloudTrail service to use the "s3 PutObject" action and the "s3 GelBucketACL" action, and specify the appropriate resource ARNs for the CloudTrail trails.

D.
Use unique log file prefixes for trails in each AWS account.

E.
Configure CloudTrail in the centralized account to log all accounts to the new centralized S3 bucket.

F.
Enable encryption of the log files by using AWS Key Management Service

Answer: B,E,F

Explanation:

QUESTION NO: 101

A Security Engineer is implementing a solution to allow users to seamlessly encrypt Amazon S3 objects without having to touch the keys directly. The solution must be highly scalable without requiring continual management. Additionally, the organization must be able to immediately delete the encryption keys.

Which solution meets these requirements?

A.
Use AWS KMS with AWS managed keys and the ScheduleKeyDeletion API with a PendingWindowInDays set to 0 to remove the keys if necessary.

B.
Use KMS with AWS imported key material and then use the DeleteImportedKeyMaterial API to remove the key material if necessary.

C.
Use AWS CloudHSM to store the keys and then use the CloudHSM API or the PKCS11 library to delete the keys if necessary.

D.
Use the Systems Manager Parameter Store to store the keys and then use the service API operations to delete the key if necessary.

Answer: B

Explanation:

QUESTION NO: 102

An application uses Amazon Cognito to manage end users' permissions when directly accessing AWS resources, including Amazon DynamoDB. A new feature request reads as follows:

Provide a mechanism to mark customers as suspended pending investigation or suspended permanently. Customers should still be able to log in when suspended, but should not be able to make changes.

The priorities are to reduce complexity and avoid potential for future security issues.

Which approach will meet these requirements and priorities?

A.
Create a new database field “suspended_status” and modify the application logic to validate that field when processing requests.

B.
Add suspended customers to second Cognito user pool and update the application login flow to check both user pools.

C.
Use Amazon Cognito Sync to push out a “suspension_status” parameter and split the IAM policy into normal users and suspended users.

D.
Move suspended customers to a second Cognito group and define an appropriate IAM access policy for the group.

Answer: A
Explanation:

QUESTION NO: 103

A company stores data on an Amazon EBS volume attached to an Amazon EC2 instance. The data is asynchronously replicated to an Amazon S3 bucket. Both the EBS volume and the S3 bucket are encrypted with the same AWS KMS Customer Master Key (CMK). A former employee scheduled a deletion of that CMK before leaving the company.

The company’s Developer Operations department learns about this only after the CMK has been deleted.

Which steps must be taken to address this situation?

A.
Copy the data directly from the EBS encrypted volume before the volume is detached from the EC2 instance.

B.
Recover the data from the EBS encrypted volume using an earlier version of the KMS backing key.

C.
Make a request to AWS Support to recover the S3 encrypted data.

D.

Make a request to AWS Support to restore the deleted CMK, and use it to recover the data.

Answer: A
Explanation:

QUESTION NO: 104

An AWS Lambda function was misused to alter data, and a Security Engineer must identify who invoked the function and what output was produced. The Engineer cannot find any logs created by the Lambda function in Amazon CloudWatch Logs.

Which of the following explains why the logs are not available?

A.
The execution role for the Lambda function did not grant permissions to write log data to CloudWatch Logs.

B.
The Lambda function was executed by using Amazon API Gateway, so the logs are not stored in CloudWatch Logs.

C.
The execution role for the Lambda function did not grant permissions to write to the Amazon S3 bucket where CloudWatch Logs stores the logs.

D.
The version of the Lambda function that was executed was not current.

Answer: A
Reference: https://docs.aws.amazon.com/lambda/latest/dg/troubleshooting.html

QUESTION NO: 105

A company has Windows Amazon EC2 instances in a VPC that are joined to on-premises Active Directory servers for domain services. The security team has enabled Amazon GuardDuty on the AWS account to alert on issues with the instances.

During a weekly audit of network traffic, the Security Engineer notices that one of the EC2 instances is attempting to communicate with a known command-and-control server but failing.

This alert does not show up in GuardDuty.

Why did GuardDuty fail to alert to this behavior?

A.
GuardDuty did not have the appropriate alerts activated.

B.
GuardDuty does not see these DNS requests.

C.
GuardDuty only monitors active network traffic flow for command-and-control activity.

D.
GuardDuty does not report on command-and-control activity.

Answer: C
Explanation:

QUESTION NO: 106

The AWS Systems Manager Parameter Store is being used to store database passwords used by an AWS Lambda function. Because this is sensitive data, the parameters are stored as type SecureString and protected by an AWS KMS key that allows access through IAM. When the function executes, this parameter cannot be retrieved as the result of an access denied error.

Which of the following actions will resolve the access denied error?

A.
Update the ssm.amazonaws.com principal in the KMS key policy to allow kms: Decrypt.

B.
Update the Lambda configuration to launch the function in a VPC.

C.
Add a policy to the role that the Lambda function uses, allowing kms: Decrypt for the KMS key.

D.
Add lambda.amazonaws.com as a trusted entity on the IAM role that the Lambda function uses.

Answer: A
Reference: https://aws.amazon.com/blogs/compute/sharing-secrets-with-aws-lambda-using-aws-systems-manager-parameter-store/

QUESTION NO: 107

A company's security policy requires that VPC Flow Logs are enabled on all VPCs. A Security Engineer is looking to automate the process of auditing the VPC resources for compliance.

What combination of actions should the Engineer take? (Choose two.)

A.
Create an AWS Lambda function that determines whether Flow Logs are enabled for a given VPC.

B.
Create an AWS Config configuration item for each VPC in the company AWS account.

C.
Create an AWS Config managed rule with a resource type of AWS:: Lambda:: Function.

D.
Create an Amazon CloudWatch Event rule that triggers on events emitted by AWS Config.

E.
Create an AWS Config custom rule, and associate it with an AWS Lambda function that contains the evaluating logic.

Answer: B,D
Explanation:

QUESTION NO: 108

A Security Engineer is looking for a way to control access to data that is being encrypted under a CMK. The Engineer is also looking to use additional authenticated data (AAD) to prevent tampering with ciphertext.

Which action would provide the required functionality?

A.
Pass the key alias to AWS KMS when calling Encrypt and Decrypt API actions.

B.
Use IAM policies to restrict access to Encrypt and Decrypt API actions.

C.

Use kms:EncryptionContext as a condition when defining IAM policies for the CMK.

D.
Use key policies to restrict access to the appropriate IAM groups.

Answer: D
Reference: https://docs.aws.amazon.com/crypto/latest/userguide/crypto-ug.pdf

QUESTION NO: 109

An application makes calls to AWS services using the AWS SDK. The application runs on Amazon EC2 instances with an associated IAM role. When the application attempts to access an object within an Amazon S3 bucket; the Administrator receives the following error message: HTTP 403: Access Denied.

Which combination of steps should the Administrator take to troubleshoot this issue? (Choose three.)

A.
Confirm that the EC2 instance's security group authorizes S3 access.

B.
Verify that the KMS key policy allows decrypt access for the KMS key for this IAM principle.

C.
Check the S3 bucket policy for statements that deny access to objects.

D.
Confirm that the EC2 instance is using the correct key pair.

E.
Confirm that the IAM role associated with the EC2 instance has the proper privileges.

F.
Confirm that the instance and the S3 bucket are in the same Region.

Answer: B,C,E
Explanation:

QUESTION NO: 110

A Security Engineer must implement mutually authenticated TLS connections between containers that communicate inside a VPC.

Which solution would be MOST secure and easy to maintain?

A.
Use AWS Certificate Manager to generate certificates from a public certificate authority and deploy them to all the containers.

B.
Create a self-signed certificate in one container and use AWS Secrets Manager to distribute the certificate to the other containers to establish trust.

C.
Use AWS Certificate Manager Private Certificate Authority (ACM PCA) to create a subordinate certificate authority, then create the private keys in the containers and sign them using the ACM PCA API.

D.
Use AWS Certificate Manager Private Certificate Authority (ACM PCA) to create a subordinate certificate authority, then use AWS Certificate Manager to generate the private certificates and deploy them to all the containers.

Answer: D

Explanation:

QUESTION NO: 111

The Accounting department at Example Corp. has made a decision to hire a third-party firm, AnyCompany, to monitor Example Corp.'s AWS account to help optimize costs.

The Security Engineer for Example Corp. has been tasked with providing AnyCompany with access to the required Example Corp. AWS resources. The Engineer has created an IAM role and granted permission to AnyCompany's AWS account to assume this role.

When customers contact AnyCompany, they provide their role ARN for validation. The Engineer is concerned that one of AnyCompany's other customers might deduce Example Corp.'s role ARN and potentially compromise the company's account.

What steps should the Engineer perform to prevent this outcome?

A.
Create an IAM user and generate a set of long-term credentials. Provide the credentials to AnyCompany. Monitor access in IAM access advisor and plan to rotate credentials on a recurring

basis.

B.
Request an external ID from AnyCompany and add a condition with sts:Externald to the role's trust policy.

C.
Require two-factor authentication by adding a condition to the role's trust policy with aws:MultiFactorAuthPresent.

D.
Request an IP range from AnyCompany and add a condition with aws:SourceIp to the role's trust policy.

Answer: B
Reference: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-user_externalid.html

QUESTION NO: 112

A company maintains sensitive data in an Amazon S3 bucket that must be protected using an AWS KMS CMK. The company requires that keys be rotated automatically every year.

How should the bucket be configured?

A.
Select server-side encryption with Amazon S3-managed keys (SSE-S3) and select an AWS-managed CMK.

B.
Select Amazon S3-AWS KMS managed encryption keys (S3-KMS) and select a customer-managed CMK with key rotation enabled.

C.
Select server-side encryption with Amazon S3-managed keys (SSE-S3) and select a customer-managed CMK that has imported key material.

D.
Select server-side encryption with AWS KMS-managed keys (SSE-KMS) and select an alias to an AWS-managed CMK.

Answer: B
Reference: https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingKMSEncryption.html

QUESTION NO: 113

An Amazon S3 bucket is encrypted using an AWS KMS CMK. An IAM user is unable to download objects from the S3 bucket using the AWS Management Console; however, other users can download objects from the S3 bucket.

Which policies should the Security Engineer review and modify to resolve this issue? (Choose three.)

A.
The CMK policy

B.
The VPC endpoint policy

C.
The S3 bucket policy

D.
The S3 ACL

E.
The IAM policy

Answer: A,C,E
Reference: https://aws.amazon.com/premiumsupport/knowledge-center/decrypt-kms-encrypted-objects-s3/

QUESTION NO: 114

While analyzing a company's security solution, a Security Engineer wants to secure the AWS account root user.

What should the Security Engineer do to provide the highest level of security for the account?

A.
Create a new IAM user that has administrator permissions in the AWS account. Delete the password for the AWS account root user.

B.
Create a new IAM user that has administrator permissions in the AWS account. Modify the

permissions for the existing IAM users.

C.
Replace the access key for the AWS account root user. Delete the password for the AWS account root user.

D.
Create a new IAM user that has administrator permissions in the AWS account. Enable multi-factor authentication for the AWS account root user.

Answer: D

Explanation:

If you continue to use the root user credentials, we recommend that you follow the security best practice to enable multi-factor authentication (MFA) for your account. Because your root user can perform sensitive operations in your account, adding an additional layer of authentication helps you to better secure your account. Multiple types of MFA are available.

Reference: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_root-user.html

QUESTION NO: 115

A Security Engineer is working with a Product team building a web application on AWS. The application uses Amazon S3 to host the static content, Amazon API Gateway to provide RESTful services; and Amazon DynamoDB as the backend data store. The users already exist in a directory that is exposed through a SAML identity provider.

Which combination of the following actions should the Engineer take to enable users to be authenticated into the web application and call APIs? (Choose three.)

A.
Create a custom authorization service using AWS Lambda.

B.
Configure a SAML identity provider in Amazon Cognito to map attributes to the Amazon Cognito user pool attributes.

C.
Configure the SAML identity provider to add the Amazon Cognito user pool as a relying party.

D.
Configure an Amazon Cognito identity pool to integrate with social login providers.

E.

Update DynamoDB to store the user email addresses and passwords.

F.
Update API Gateway to use a COGNITO_USER_POOLS authorizer.

Answer: B,C,F
Explanation:

QUESTION NO: 116

While securing the connection between a company's VPC and its on-premises data center, a Security Engineer sent a ping command from an on-premises host (IP address 203.0.113.12) to an Amazon EC2 instance (IP address 172.31.16.139). The ping command did not return a response. The flow log in the VPC showed the following:

2 123456789010 eni-1235b8ca 203.0.113.12 172.31.16.139 0 0 1 4 336 1432917027 1432917142 ACCEPT OK

2 123456789010 eni-1235b8ca 172.31.16.139 203.0.113.12 0 0 1 4 336 1432917094 1432917142 REJECT OK

What action should be performed to allow the ping to work?

A.
In the security group of the EC2 instance, allow inbound ICMP traffic.

B.
In the security group of the EC2 instance, allow outbound ICMP traffic.

C.
In the VPC's NACL, allow inbound ICMP traffic.

D.
In the VPC's NACL, allow outbound ICMP traffic.

Answer: D
Explanation:

QUESTION NO: 117

A Security Engineer is building a Java application that is running on Amazon EC2. The application communicates with an Amazon RDS instance and authenticates with a user name and password.

Which combination of steps can the Engineer take to protect the credentials and minimize downtime when the credentials are rotated? (Choose two.)

A.
Have a Database Administrator encrypt the credentials and store the ciphertext in Amazon S3. Grant permission to the instance role associated with the EC2 instance to read the object and decrypt the ciphertext.

B.
Configure a scheduled job that updates the credential in AWS Systems Manager Parameter Store and notifies the Engineer that the application needs to be restarted.

C.
Configure automatic rotation of credentials in AWS Secrets Manager.

D.
Store the credential in an encrypted string parameter in AWS Systems Manager Parameter Store. Grant permission to the instance role associated with the EC2 instance to access the parameter and the AWS KMS key that is used to encrypt it.

E.
Configure the Java application to catch a connection failure and make a call to AWS Secrets Manager to retrieve updated credentials when the password is rotated. Grant permission to the instance role associated with the EC2 instance to access Secrets Manager.

Answer: C,E

Explanation:

QUESTION NO: 118

A company has several production AWS accounts and a central security AWS account. The security account is used for centralized monitoring and has IAM privileges to all resources in every corporate account. All of the company's Amazon S3 buckets are tagged with a value denoting the data classification of their contents.

A Security Engineer is deploying a monitoring solution in the security account that will enforce bucket policy compliance. The system must monitor S3 buckets in all production accounts and confirm that any policy change is in accordance with the bucket's data classification. If any change is out of compliance; the Security team must be notified quickly.

Which combination of actions would build the required solution? (Choose three.)

A.
Configure Amazon CloudWatch Events in the production accounts to send all S3 events to the security account event bus.

B.
Enable Amazon GuardDuty in the security account, and join the production accounts as members.

C.
Configure an Amazon CloudWatch Events rule in the security account to detect S3 bucket creation or modification events.

D.
Enable AWS Trusted Advisor and activate email notifications for an email address assigned to the security contact.

E.
Invoke an AWS Lambda function in the security account to analyze S3 bucket settings in response to S3 events, and send non-compliance notifications to the Security team.

F.
Configure event notifications on S3 buckets for PUT; POST, and DELETE events.

Answer: C,E,F
Explanation:

QUESTION NO: 119

A company plans to migrate a sensitive dataset to Amazon S3. A Security Engineer must ensure that the data is encrypted at rest. The encryption solution must enable the company to generate its own keys without needing to manage key storage or the encryption process.

What should the Security Engineer use to accomplish this?

A.
Server-side encryption with Amazon S3-managed keys (SSE-S3)

B.
Server-side encryption with AWS KMS-managed keys (SSE-KMS)

C.
Server-side encryption with customer-provided keys (SSE-C)

D.
Client-side encryption with an AWS KMS-managed CMK

Answer: B

Explanation:

Reference https://aws.amazon.com/s3/faqs/

QUESTION NO: 120

A Security Engineer is defining the logging solution for a newly developed product. Systems Administrators and Developers need to have appropriate access to event log files in AWS CloudTrail to support and troubleshoot the product.

Which combination of controls should be used to protect against tampering with and unauthorized access to log files? (Choose two.)

A.
Ensure that the log file integrity validation mechanism is enabled.

B.
Ensure that all log files are written to at least two separate Amazon S3 buckets in the same account.

C.
Ensure that Systems Administrators and Developers can edit log files, but prevent any other access.

D.
Ensure that Systems Administrators and Developers with job-related need-to-know requirements only are capable of viewing—but not modifying—the log files.

E.
Ensure that all log files are stored on Amazon EC2 instances that allow SSH access from the internal corporate network only.

Answer: A,D

Explanation:

QUESTION NO: 121

A company has a few dozen application servers in private subnets behind an Elastic Load Balancer (ELB) in an AWS Auto Scaling group. The application is accessed from the web over HTTPS. The data must always be encrypted in transit. The Security Engineer is worried about

potential key exposure due to vulnerabilities in the application software.

Which approach will meet these requirements while protecting the external certificate during a breach?

A.
Use a Network Load Balancer (NLB) to pass through traffic on port 443 from the internet to port 443 on the instances.

B.
Purchase an external certificate, and upload it to the AWS Certificate Manager (for use with the ELB) and to the instances. Have the ELB decrypt traffic, and route and re-encrypt with the same certificate.

C.
Generate an internal self-signed certificate and apply it to the instances. Use AWS Certificate Manager to generate a new external certificate for the ELB. Have the ELB decrypt traffic, and route and re-encrypt with the internal certificate.

D.
Upload a new external certificate to the load balancer. Have the ELB decrypt the traffic and forward it on port 80 to the instances.

Answer: C
Explanation:

QUESTION NO: 122

Which of the following are valid event sources that are associated with web access control lists that trigger AWS WAF rules? (Choose two.)

A.
Amazon S3 static web hosting

B.
Amazon CloudFront distribution

C.
Application Load Balancer

D.
Amazon Route 53

E.

VPC Flow Logs

Answer: B,C

Explanation:
Explanation

A web access control list (web ACL) gives you fine-grained control over the web requests that your Amazon API Gateway API, Amazon CloudFront distribution or Application Load Balancer responds to.

Reference: https://docs.aws.amazon.com/waf/latest/developerguide/web-acl.html

QUESTION NO: 123

A company uses identity federation to authenticate users into an identity account (987654321987) where the users assume an IAM role named IdentityRole. The users then assume an IAM role named JobFunctionRole in the target AWS account (123456789123) to perform their job functions.

A user is unable to assume the IAM role in the target account. The policy attached to the role in the identity account is:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/JobFunctionRole"
            ],
            "Effect": "Allow"
        }
    ]
}
```


What should be done to enable the user to assume the appropriate role in the target account?

A.
Update the IAM policy attached to the role in the identity account to be:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [
                "arn:aws:iam::123456789123:role/JobFunctionRole"
            ],
            "Effect": "Allow"
        }
    ]
}
```

B.

Update the trust policy on the role in the target account to be:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::987654321987:role/IdentityRole"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

C.

Update the trust policy on the role in the identity account to be:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": { "AWS": "arn:aws:iam::987654321987:root"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

D.

Update the IAM policy attached to the role in the target account to be:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1502946463000",
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::123456789123:role/JobFunctionRole"
        }
    ]
}
```


Answer: A

Explanation:

QUESTION NO: 124

A Security Engineer is working with the development team to design a supply chain application that stores sensitive inventory data in an Amazon S3 bucket. The application will use an AWS KMS customer master key (CMK) to encrypt the data on Amazon S3. The inventory data on Amazon S3 will be shared of vendors. All vendors will use AWS principals from their own AWS accounts to access the data on Amazon S3. The vendor list may change weekly, and the solution must support cross-account access.

What is the MOST efficient way to manage access control for the KMS CMK7?

A.
Use KMS grants to manage key access. Programmatically create and revoke grants to manage vendor access.

B.
Use an IAM role to manage key access. Programmatically update the IAM role policies to manage vendor access.

C.
Use KMS key policies to manage key access. Programmatically update the KMS key policies to manage vendor access.

D.
Use delegated access across AWS accounts by using IAM roles to manage key access. Programmatically update the IAM trust policy to manage cross-account vendor access.

Answer: A

Explanation:

QUESTION NO: 125

A Security Engineer is setting up an AWS CloudTrail trail for all regions in an AWS account. For added security, the logs are stored using server-side encryption with AWS KMS-managed keys (SSE-KMS) and have log integrity validation enabled.

While testing the solution, the Security Engineer discovers that the digest files are readable, but the log files are not. What is the MOST likely cause?

A.
The log files fail integrity validation and automatically are marked as unavailable.

B.
The KMS key policy does not grant the Security Engineer's IAM user or role permissions to decrypt with it.

C.
The bucket is set up to use server-side encryption with Amazon S3-managed keys (SSE-S3) as the default and does not allow SSE-KMS-encrypted files.

D.
An IAM policy applicable to the Security Engineer’s IAM user or role denies access to the "CloudTrail/" prefix in the Amazon S3 bucket

Answer: B

Explanation:

QUESTION NO: 126

A corporate cloud security policy states that communications between the company's VPC and KMS must travel entirely within the AWS network and not use public service endpoints.

Which combination of the following actions MOST satisfies this requirement? (Choose two.)

A.
Add the aws:sourceVpce condition to the AWS KMS key policy referencing the company's VPC endpoint ID.

B.
Remove the VPC internet gateway from the VPC and add a virtual private gateway to the VPC to prevent direct, public internet connectivity.

C.
Create a VPC endpoint for AWS KMS with private DNS enabled.

D.
Use the KMS Import Key feature to securely transfer the AWS KMS key over a VPN.

E.
Add the following condition to the AWS KMS key policy: "aws:SourceIp": "10.0.0.0/16".

Answer: A,C

Explanation:
Explanation

An IAM policy can deny access to KMS except through your VPC endpoint with the following condition statement:

"Condition": {

"StringNotEquals": {

"aws:sourceVpce": "vpce-0295a3caf8414c94a"

}

}

If you select the Enable Private DNS Name option, the standard AWS KMS DNS hostname

(https://kms.<region>.amazonaws.com) resolves to your VPC endpoint.

QUESTION NO: 127

A company had one of its Amazon EC2 key pairs compromised. A Security Engineer must identify which current Linux EC2 instances were deployed and used the compromised key pair.

How can this task be accomplished?

A.
Obtain the list of instances by directly querying Amazon EC2 using: aws ec2 describe-instances --filters "Name=key-name,Values=KEYNAMEHERE".

B.
Obtain the fingerprint for the key pair from the AWS Management Console, then search for the fingerprint in the Amazon Inspector logs.

C.
Obtain the output from the EC2 instance metadata using: curl http: //169.254.169.254/latest/meta-data/public- keys/0/.

D.
Obtain the fingerprint for the key pair from the AWS Management Console, then search for the fingerprint in Amazon CloudWatch Logs using: aws logs filter-log-events.

Answer: D

Explanation:

QUESTION NO: 128

A Security Engineer for a large company is managing a data processing application used by 1,500 subsidiary companies. The parent and subsidiary companies all use AWS. The application uses TCP port 443 and runs on Amazon EC2 behind a Network Load Balancer (NLB). For compliance reasons, the application should only be accessible to the subsidiaries and should not be available on the public internet. To meet the compliance requirements for restricted access, the Engineer has received the public and private CIDR block ranges for each subsidiary.

What solution should the Engineer use to implement the appropriate access restrictions for the application?

A.
Create a NACL to allow access on TCP port 443 from the 1;500 subsidiary CIDR block ranges. Associate the NACL to both the NLB and EC2 instances

B.
Create an AWS security group to allow access on TCP port 443 from the 1,500 subsidiary CIDR block ranges. Associate the security group to the NLB. Create a second security group for EC2 instances with access on TCP port 443 from the NLB security group.

C.
Create an AWS PrivateLink endpoint service in the parent company account attached to the NLB. Create an AWS security group for the instances to allow access on TCP port 443 from the AWS PrivateLink endpoint. Use AWS PrivateLink interface endpoints in the 1,500 subsidiary AWS accounts to connect to the data processing application.

D.
Create an AWS security group to allow access on TCP port 443 from the 1,500 subsidiary CIDR block ranges. Associate the security group with EC2 instances.

Answer: C

Explanation:

QUESTION NO: 129

To meet regulatory requirements, a Security Engineer needs to implement an IAM policy that restricts the use of AWS services to the us-east-1 Region.

What policy should the Engineer implement?

A.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
          "Effect": "Allow",
          "Action": "*",
          "Resource": "*",
          "Condition": {
              "StringEquals": {
                  "aws:RequestedRegion": "us-east-1"
              }
          }
        }
    ]
}
```


B.

```
{
    "Version": "2012-10-17",
    "Statement": [
          {
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                  "StringEquals":  {
                        "ec2:Region": "us-east-1"
                  }
            }
        }
     ]
}
```

C.

```
{
    "Version": "2012-10-17",
    "Statement": [
          {
            "Effect": "Deny",
            "Action": "*",
            "Resource": "*",
            "Condition":  {
                 "StringNotEquals":  {
                       "aws:RequestedRegion": "us-east-1"
                  }
            }
        }
    ]
}
```

D.

```
{
    "Version": "2012-10-17",
    "Statement": [
          {
            "Effect": "Deny",
            "NotAction": "*",
            "Resource": "*",
            "Condition":  {
                 "StringEquals":  {
                      "aws:RequestedRegion": "us-east-1"
                }
            }
        }
    ]
}
```


Answer: B
Explanation:

QUESTION NO: 130

A company uses user data scripts that contain sensitive information to bootstrap Amazon EC2 instances. A Security Engineer discovers that this sensitive information is viewable by people who should not have access to it.

What is the MOST secure way to protect the sensitive information used to bootstrap the instances?

A.
Store the scripts in the AMI and encrypt the sensitive data using AWS KMS Use the instance role profile to control access to the KMS keys needed to decrypt the data.

B.
Store the sensitive data in AWS Systems Manager Parameter Store using the encrypted string parameter and assign the GetParameters permission to the EC2 instance role.

C.
Externalize the bootstrap scripts in Amazon S3 and encrypt them using AWS KMS. Remove the scripts from the instance and clear the logs after the instance is configured.

D.
Block user access of the EC2 instance's metadata service using IAM policies. Remove all scripts

and clear the logs after execution.

Answer: A

Explanation:

QUESTION NO: 131

A company is building a data lake on Amazon S3. The data consists of millions of small files containing sensitive information. The Security team has the following requirements for the architecture:

• Data must be encrypted in transit.

• Data must be encrypted at rest.

• The bucket must be private, but if the bucket is accidentally made public, the data must remain confidential.

Which combination of steps would meet the requirements? (Choose two.)

A.
Enable AES-256 encryption using server-side encryption with Amazon S3-managed encryption keys (SSE-S3) on the S3 bucket.

B.
Enable default encryption with server-side encryption with AWS KMS-managed keys (SSE-KMS) on the S3 bucket.

C.
Add a bucket policy that includes a deny if a PutObject request does not include aws:SecureTransport.

D.
Add a bucket policy with aws:SourceIp to Allow uploads and downloads from the corporate intranet only.

E.
Add a bucket policy that includes a deny if a PutObject request does not include s3:x-amz-server-side-encryption: "aws:kms".

F.
Enable Amazon Macie to monitor and act on changes to the data lake's S3 bucket.

Answer: B,C

Explanation:

Bucket encryption using KMS will protect both in case disks are stolen as well as if the bucket is public.

This is because the KMS key would need to have privileges granted to it for users outside of AWS.

QUESTION NO: 132

A Security Engineer discovered a vulnerability in an application running on Amazon ECS. The vulnerability allowed attackers to install malicious code. Analysis of the code shows it exfiltrates data on port 5353 in batches at random time intervals.

While the code of the containers is being patched, how can Engineers quickly identify all compromised hosts and stop the egress of data on port 5353?

A.
Enable AWS Shield Advanced and AWS WAF. Configure an AWS WAF custom filter for egress traffic on port 5353

B.
Enable Amazon Inspector on Amazon ECS and configure a custom assessment to evaluate containers that have port 5353 open. Update the NACLs to block port 5353 outbound.

C.
Create an Amazon CloudWatch custom metric on the VPC Flow Logs identifying egress traffic on port 5353. Update the NACLs to block port 5353 outbound.

D.
Use Amazon Athena to query AWS CloudTrail logs in Amazon S3 and look for any traffic on port 5353. Update the security groups to block port 5353 outbound.

Answer: C
Explanation:

QUESTION NO: 133

An Amazon EC2 instance is denied access to a newly created AWS KMS CMK used for decrypt actions. The environment has the following configuration:

The instance is allowed the kms:Decrypt action in its IAM role for all resources

The AWS KMS CMK status is set to enabled

The instance can communicate with the KMS API using a configured VPC endpoint

What is causing the issue?

A.
The kms:GenerateDataKey permission is missing from the EC2 instance's IAM role

B.
The ARN tag on the CMK contains the EC2 instance's ID instead of the instance's ARN

C.
The kms:Encrypt permission is missing from the EC2 IAM role

D.
The KMS CMK key policy that enables IAM user permissions is missing

Answer: D
Explanation:

In a key policy, you use "*" for the resource, which means "this CMK." A key policy applies only to the CMK it is attached to

Reference: https://docs.aws.amazon.com/kms/latest/developerguide/key-policies.html

QUESTION NO: 134

A company has enabled Amazon GuardDuty in all Regions as part of its security monitoring strategy. In one of the VPCs, the company hosts an Amazon EC2 instance working as an FTP server that is contacted by a high number of clients from multiple locations. This is identified by GuardDuty as a brute force attack due to the high number of connections that happen every hour.

The finding has been flagged as a false positive. However, GuardDuty keeps raising the issue. A Security Engineer has been asked to improve the signal-to-noise ratio. The Engineer needs to ensure that changes do not compromise the visibility of potential anomalous behavior.

How can the Security Engineer address the issue?

A.

Disable the FTP rule in GuardDuty in the Region where the FTP server is deployed

B.
Add the FTP server to a trusted IP list and deploy it to GuardDuty to stop receiving the notifications

C.
Use GuardDuty filters with auto archiving enabled to close the findings

D.
Create an AWS Lambda function that closes the finding whenever a new occurrence is reported

Answer: B
Explanation:

Trusted IP lists consist of IP addresses that you have whitelisted for secure communication with your AWS infrastructure and applications. GuardDuty does not generate findings for IP addresses on trusted IP lists. At any given time, you can have only one uploaded trusted IP list per AWS account per region.

Reference: https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_upload_lists.html

QUESTION NO: 135

What are the MOST secure ways to protect the AWS account root user of a recently opened AWS account? (Choose two.)

A.
Use the AWS account root user access keys instead of the AWS Management Console

B.
Enable multi-factor authentication for the AWS IAM users with the AdministratorAccess managed policy attached to them

C.
Enable multi-factor authentication for the AWS account root user

D.
Use AWS KMS to encrypt all AWS account root user and AWS IAM access keys and set automatic rotation to 30 days

E.
Do not create access keys for the AWS account root user; instead, create AWS IAM users

Answer: B,D

Explanation:

QUESTION NO: 136

A company has decided to migrate sensitive documents from on-premises data centers to Amazon S3. Currently, the hard drives are encrypted to meet a compliance requirement regarding data encryption. The CISO wants to improve security by encrypting each file using a different key instead of a single key. Using a different key would limit the security impact of a single exposed key.

Which of the following requires the LEAST amount of configuration when implementing this approach?

A.
Place each file into a different S3 bucket. Set the default encryption of each bucket to use a different AWS KMS customer managed key.

B.
Put all the files in the same S3 bucket. Using S3 events as a trigger, write an AWS Lambda function to encrypt each file as it is added using different AWS KMS data keys.

C.
Use the S3 encryption client to encrypt each file individually using S3-generated data keys

D.
Place all the files in the same S3 bucket. Use server-side encryption with AWS KMS-managed keys (SSE-KMS) to encrypt the data

Answer: D
Reference: https://docs.aws.amazon.com/kms/latest/developerguide/services-s3.html

QUESTION NO: 137

A company has an encrypted Amazon S3 bucket. An Application Developer has an IAM policy that allows access to the S3 bucket, but the Application Developer is unable to access objects within the bucket.

What is a possible cause of the issue?

A.
The S3 ACL for the S3 bucket fails to explicitly grant access to the Application Developer

B.
The AWS KMS key for the S3 bucket fails to list the Application Developer as an administrator

C.
The S3 bucket policy fails to explicitly grant access to the Application Developer

D.
The S3 bucket policy explicitly denies access to the Application Developer

Answer: C
Reference: https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html

QUESTION NO: 138

A Web Administrator for the website example.com has created an Amazon CloudFront distribution for dev.example.com, with a requirement to configure HTTPS using a custom TLS certificate imported to AWS Certificate Manager.

Which combination of steps is required to ensure availability of the certificate in the CloudFront console? (Choose two.)

A.
Call UploadServerCertificate with /cloudfront/dev/ in the path parameter.

B.
Import the certificate with a 4,096-bit RSA public key.

C.
Ensure that the certificate, private key, and certificate chain are PKCS #12-encoded.

D.
Import the certificate in the us-east-1 (N. Virginia) Region.

E.
Ensure that the certificate, private key, and certificate chain are PEM-encoded.

Answer: B,D

Explanation:

QUESTION NO: 139

A Security Engineer has discovered that, although encryption was enabled on the Amazon S3 bucket examplebucket, anyone who has access to the bucket has the ability to retrieve the files. The Engineer wants to limit access to each IAM user can access an assigned folder only.

What should the Security Engineer do to achieve this?

A.
Use envelope encryption with the AWS-managed CMK aws/s3.

B.
Create a customer-managed CMK with a key policy granting “kms:Decrypt” based on the “${aws:username}” variable.

C.
Create a customer-managed CMK for each user. Add each user as a key user in their corresponding key policy.

D.
Change the applicable IAM policy to grant S3 access to “Resource”: “arn:aws:s3:::examplebucket/${aws:username}/*”

Answer: D
Reference: https://aws.amazon.com/premiumsupport/knowledge-center/iam-s3-user-specific-folder/