Amazon-Web-Services

Exam Questions SCS-C01

AWS Certified Security- Specialty

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
- (Exam Topic 1)
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

NEW QUESTION 2
- (Exam Topic 1)
A company has several workloads running on AWS Employees are required to authenticate using on-premises ADFS and SSO to access the AWS Management Console Developers migrated an existing legacy web application to an Amazon EC2 instance Employees need to access this application from anywhere on the internet but currently, mere is no authentication system but into the application.
How should the Security Engineer implement employee-only access to this system without changing the application?

A. Place the application behind an Application Load Balancer (ALB) Use Amazon Cognito as authentication (or the ALB Define a SAML-based Amazon Cognito user pool and connect it to ADFSimplement AWS SSO in the master account and link it to ADFS as an identity provide' Define the EC2 instance as a managed resource, then apply an IAM policy on the resource
B. Define an Amazon Cognito identity pool then install the connector on the Active Directory server Use the Amazon Cognito SDK on the application instance to authenticate the employees using their
C. Active Directory user names and passwords
D. Create an AWS Lambda custom authorizer as the authenticator for a reverse proxy on Amazon EC2 Ensure the security group on Amazon EC2 only allows access from the Lambda function.

Answer: B

NEW QUESTION 3
- (Exam Topic 1)
A company has several critical applications running on a large fleet of Amazon EC2 instances. As part of a security operations review, the company needs to apply a critical operating system patch to EC2 instances within 24 hours of the patch becoming available from the operating system vendor. The company does not have a patching solution deployed on AWS, but does have AWS Systems Manager configured. The solution must also minimize administrative overhead.
What should a security engineer recommend to meet these requirements?

A. Create an AWS Config rule defining the patch as a required configuration for EC2 instances.
B. Use the AWS Systems Manager Run Command to patch affected instances.
C. Use an AWS Systems Manager Patch Manager predefined baseline to patch affected instances.
D. Use AWS Systems Manager Session Manager to log in to each affected instance and apply the patch.

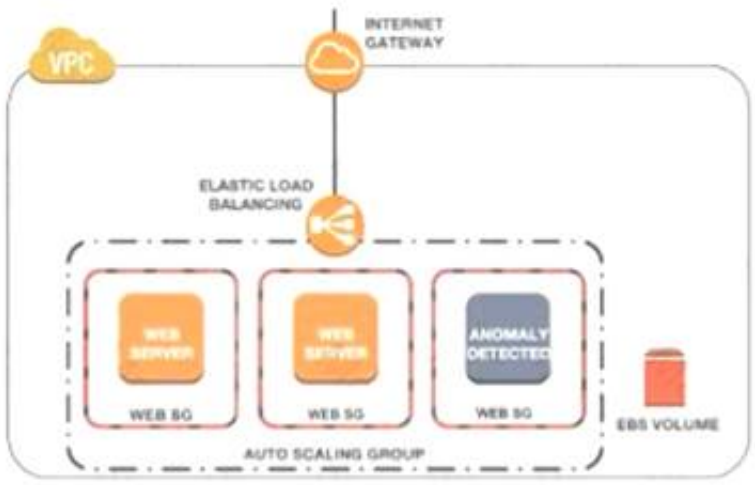
Answer: B

NEW QUESTION 4
- (Exam Topic 1)
A company wants to encrypt data locally while meeting regulatory requirements related to key exhaustion. The encryption key can be no more than 10 days old or encrypt more than 2" 16 objects Any encryption key must be generated on a FIPS-validated hardware security module (HSM). The company is cost-conscious, as plans to upload an average of 100 objects to Amazon S3 each second for sustained operations across 5 data producers
When approach MOST efficiently meets the company's needs?

A. Use the AWS Encryption SDK and set the maximum age to 10 days and the minimum number of messages encrypted to 3" 16. Use AWS Key Management Service (AWS KMS) to generate the master key and data key Use data key caching with the Encryption SDk during the encryption process.
B. Use AWS Key Management Service (AWS KMS) to generate an AWS managed CM
C. Then use Amazon S3 client-side encryption configured to automatically rotate with every object
D. Use AWS CloudHSM to generate the master key and data key
E. Then use Boto 3 and Python to locally encrypt data before uploading the object Rotate the data key every 10 days or after 2" 16 objects have been Uploaded to Amazon 33
F. Use server-side encryption with Amazon S3 managed encryption keys (SSE-S3) and set the master key to automatically rotate.

Answer: A

NEW QUESTION 5
- (Exam Topic 1)
A Security Engineer noticed an anomaly within a company EC2 instance as shown in the image. The Engineer must now investigate what e causing the anomaly.
What are the MOST effective steps to take lo ensure that the instance is not further manipulated while allowing the Engineer to understand what happened?



A. Remove the instance from the Auto Scaling group Place the instance within an isolation security group, detach the EBS volume launch an EC2 instance with a forensic toolkit and attach the E8S volume to investigate
B. Remove the instance from the Auto Scaling group and the Elastic Load Balancer Place the instance within an isolation security group, launch an EC2 instance with a forensic toolkit, and allow the forensic toolkit image to connect to the suspicious Instance to perform the Investigation.
C. Remove the instance from the Auto Scaling group Place the Instance within an isolation security group, launch an EC2 Instance with a forensic toolkit and use the forensic toolkit imago to deploy an ENI as a network span port to inspect all traffic coming from the suspicious instance.
D. Remove the instance from the Auto Scaling group and the Elastic Load Balancer Place the instance within an isolation security group, make a copy of the EBS volume from a new snapshot, launch an EC2 Instance with a forensic toolkit and attach the copy of the EBS volume to investigate.

Answer: B

NEW QUESTION 6
- (Exam Topic 1)
A company has the software development teams that are creating applications that store sensitive data in Amazon S3 Each team's data must always be separate. The company's security team must design a data encryption strategy for both teams that provides the ability to audit key usage. The solution must also minimize operational overhead
what should me security team recommend?

A. Tell the application teams to use two different S3 buckets with separate AWS Key Management Service (AWS KMS) AWS managed CMKs Limit the key process to allow encryption and decryption of the CMKs to their respective teams onl
B. Force the teams to use encryption context to encrypt and decrypt
C. Tell the application teams to use two different S3 buckets with a single AWS Key Management Service (AWS KMS) AWS managed CMK Limit the key policy to allow encryption and decryption of the CMK onl
D. Do not allow the teams to use encryption context to encrypt and decrypt
E. Tell the application teams to use two different S3 buckets with separate AWS Key Management Service (AWS KMS) customer managed CMKs Limit the key policies to allow encryption and decryption of the CMKs to their respective teams only Force the teams to use encryption context to encrypt and decrypt
F. Tell the application teams to use two different S3 buckets with a single AWS Key Management Service (AWS KMS) customer managed CMK Limit the key policy to allow encryption and decryption of the CMK only Do not allow the teams to use encryption context to encrypt and decrypt

Answer: A

NEW QUESTION 7
- (Exam Topic 1)
A company uses a third-party identity provider and SAML-based SSO for its AWS accounts After the third-party identity provider renewed an expired signing certificate users saw the following message when trying to log in:

```
Error: Response Signature Invalid (Service: AWSSecurityTokenService; Status Code: 400; Error Code: InvalidIdentityToken)
```

A security engineer needs to provide a solution that corrects the error and minimizes operational overhead Which solution meets these requirements?

A. Upload the third-party signing certificate's new private key to the AWS identity provider entity defined in AWS identity and Access Management (IAM) by using the AWS Management Console
B. Sign the identity provider's metadata file with the new public key Upload the signature to the AWS identity provider entity defined in AWS Identity and Access Management (IAM) by using the AWS CLI.
C. Download the updated SAML metadata tile from the identity service provider Update the file in the AWS identity provider entity defined in AWS Identity and Access Management (IAM) by using theAWS CLI
D. Configure the AWS identity provider entity defined in AWS Identity and Access Management (IAM) to synchronously fetch the new public key by using the AWS Management Console.

Answer: C

NEW QUESTION 8
- (Exam Topic 1)
An application running on Amazon EC2 instances generates log files in a folder on a Linux file system. The instances block access to the console and file transfer utilities, such as Secure Copy Protocol (SCP) and Secure File Transfer Protocol (SFTP). The Application Support team wants to automatically monitor the application log files so the team can set up notifications in the future.
A Security Engineer must design a solution that meets the following requirements:
• Make the log files available through an AWS managed service.
• Allow for automatic monitoring of the logs.
• Provide an Interlace for analyzing logs.
• Minimize effort.
Which approach meets these requirements^

A. Modify the application to use the AWS SD

B. Write the application logs lo an Amazon S3 bucket
C. install the unified Amazon CloudWatch agent on the instances Configure the agent to collect the application log dies on the EC2 tile system and send them to Amazon CloudWatch Logs
D. Install AWS Systems Manager Agent on the instances Configure an automation document to copy the application log files to AWS DeepLens
E. Install Amazon Kinesis Agent on the instances Stream the application log files to Amazon Kinesis Data Firehose and sot the destination to Amazon Elasticsearch Service

Answer: D

NEW QUESTION 9
- (Exam Topic 1)
A security engineer must develop an encryption tool for a company. The company requires a cryptographic solution that supports the ability to perform cryptographic erasure on all resources protected by the key material in 15 minutes or less
Which AWS Key Management Service (AWS KMS) key solution will allow the security engineer to meet these requirements?

A. Use Imported key material with CMK
B. Use an AWS KMS CMK
C. Use an AWS managed CMK.
D. Use an AWS KMS customer managed CMK

Answer: C

NEW QUESTION 10
- (Exam Topic 1)
A Developer is building a serverless application that uses Amazon API Gateway as the front end. The application will not be publicly accessible. Other legacy applications running on Amazon EC2 will make calls to the application A Security Engineer Has been asked to review the security controls for authentication and authorization of the application
Which combination of actions would provide the MOST secure solution? (Select TWO)

A. Configure an IAM policy that allows the least permissive actions to communicate with the API Gateway Attach the policy to the role used by the legacy EC2 instances
B. Enable AWS WAF for API Gateway Configure rules to explicitly allow connections from the legacy EC2 instances
C. Create a VPC endpoint for API Gateway Attach an IAM resource policy that allows the role of the legacy EC2 instances to call specific APIs
D. Create a usage plan Generate a set of API keys for each application that needs to call the API.
E. Configure cross-origin resource sharing (CORS) in each API Share the CORS information with the applications that call the API.

Answer: AE

NEW QUESTION 10
- (Exam Topic 1)
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 --fi1ters "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: A

NEW QUESTION 12
- (Exam Topic 1)
A global company that deals with International finance is investing heavily in cryptocurrencies and wants to experiment with mining technologies using AWS. The company's security team has enabled Amazon
GuardDuty and is concerned by the number of findings being generated by the accounts. The security team wants to minimize the possibility of GuardDuty finding false negatives for compromised instances that are performing mining
How can the security team continue using GuardDuty while meeting these requirements?

A. In the GuardDuty console, select the CryptoCurrency:EC2/BitcoinTool B'DNS finding and use the suppress findings option
B. Create a custom AWS Lambda function to process newly detected GuardDuty alerts Process the CryptoCurrency EC2/BitcoinTool BIDNS alert and filter outthe high-severity finding types only.
C. When creating a new Amazon EC2 Instance, provide the instance with a specific tag that indicates it is performing mining operations Create a custom AWS Lambda function to process newly detected GuardDuty alerts and filter for the presence of this tag
D. When GuardDuty produces a cryptocurrency finding, process the finding with a custom AWS Lambda function to extract the instance ID from the finding Then use the AWS Systems Manager Run Command to check for a running process performing mining operations

Answer: A

NEW QUESTION 14
- (Exam Topic 1)
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: D

NEW QUESTION 17
- (Exam Topic 1)
Users report intermittent availability of a web application hosted on AWS. Monitoring systems report an excess of abnormal network traffic followed by high CPU utilization on the application web tier. Which of the following techniques will improve the availability of the application? (Select TWO.)

A. Deploy AWS WAF to block all unsecured web applications from accessing the internet.
B. Deploy an Intrusion Detection/Prevention System (IDS/IPS) to monitor or block unusual incoming network traffic.
C. Configure security groups to allow outgoing network traffic only from hosts that are protected with up-to-date antivirus software.
D. Create Amazon CloudFront distribution and configure AWS WAF rules to protect the web applications from malicious traffic.
E. Use the default Amazon VPC for externakfacing systems to allow AWS to actively block malicious network traffic affecting Amazon EC2 instances.

Answer: BD

NEW QUESTION 18
- (Exam Topic 1)
A company has decided to use encryption in its AWS account to secure the objects in Amazon S3 using server-side encryption. Object sizes range from 16.000 B to 5 MB. The requirements are as follows:
• The key material must be generated and stored in a certified Federal Information Processing Standard (FIPS) 140-2 Level 3 machine.
• The key material must be available in multiple Regions. Which option meets these requirements?

A. Use an AWS KMS customer managed key and store the key material in AWS with replication across Regions
B. Use an AWS customer managed key, import the key material into AWS KMS using in-house AWS CloudHS
C. and store the key material securely in Amazon S3.
D. Use an AWS KMS custom key store backed by AWS CloudHSM clusters, and copy backups across Regions
E. Use AWS CloudHSM to generate the key material and backup keys across Regions Use the Java Cryptography Extension (JCE) and Public Key Cryptography Standards #11 (PKCS #11) encryption libraries to encrypt and decrypt the data.

Answer: D

NEW QUESTION 20
- (Exam Topic 1)
A company's web application is hosted on Amazon EC2 instances running behind an Application Load Balancer (ALB) in an Auto Scaling group. An AWS WAF web ACL is associated with the ALB. AWS CloudTrail is enabled, and stores logs in Amazon S3 and Amazon CloudWatch Logs.
The operations team has observed some EC2 instances reboot at random. After rebooting, all access logs on the instances have been deleted. During an investigation, the operations team found that each reboot happened just after a PHP error occurred on the new-user-creation.php file. The operations team needs to view log information to determine if the company is being attacked.
Which set of actions will identify the suspect attacker's IP address for future occurrences?

A. Configure VPC Flow Logs on the subnet where the ALB is located, and stream the data CloudWatch.Search for the new-user-creation.php occurrences in CloudWatch.
B. Configure the CloudWatch agent on the ALB Configure the agent to send application logs to CloudWatch Update the instance role to allow CloudWatch Logs acces
C. Export the logs to CloudWatch Search for the new-user-creation.php occurrences in CloudWatch.
D. Configure the ALB to export access logs to an Amazon Elasticsearch Service cluster, and use the service to search for the new-user-creation.php occurrences.
E. Configure the web ACL to send logs to Amazon Kinesis Data Firehose, which delivers the logs to an S3 bucket Use Amazon Athena to query the logs and find the new-user-creation php occurrences.

Answer: B

NEW QUESTION 21
- (Exam Topic 1)
An application developer is using an AWS Lambda function that must use AWS KMS to perform encrypt and decrypt operations for API keys that are less than 2 KB Which key policy would allow the application to do this while granting least privilege?

A.
```
{
  "Sid": "AllowUseOfTheKey",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::444455556666:role/EncryptionApp"},
  "Action": [
   "kms:*"
  ],
  "Resource": "*"
}
```

B.
```
{
  "Sid": "AllowUseOfTheKey",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::444455556666:role/EncryptionApp"},
  "Action": [
   "kms:Encrypt",
   "kms:Decrypt"
  ],
  "Resource": "*"
}
```

C.
```
{
 "Sid": "AllowUseOfTheKey",
 "Effect": "Allow",
 "Principal": {"AWS": "arn:aws:iam::444455556666:role/EncryptionApp"},
 "Action": [
  "kms:DescribeKey",
  "kms:GenerateDataKey*",
  "kms:Encrypt",
  "kms:ReEncrypt*",
  "kms:Decrypt"
```

D.
```
{
 "Sid": "AllowUseOfTheKey",
 "Effect": "Allow",
 "Principal": {"AWS": "arn:aws:iam::444455556666:role/EncryptionApp"},
 "Action": [
  "kms:DescribeKey",
  "kms:GenerateDataKey*",
  "kms:Encrypt",
  "kms:ReEncrypt*",
  "kms:Disable*",
  "kms:Decrypt"
],
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: B

NEW QUESTION 22
- (Exam Topic 1)
A company is running an application on Amazon EC2 instances in an Auto Scaling group. The application stores logs locally A security engineer noticed that logs were lost after a scale-in event. The security engineer needs to recommend a solution to ensure the durability and availability of log data All logs must be kept for a minimum of 1 year for auditing purposes
What should the security engineer recommend?

A. Within the Auto Scaling lifecycle, add a hook to create and attach an Amazon Elastic Block Store (Amazon EBS) log volume each time an EC2 instance is create
B. When the instance is terminated, the EBS volume can be reattached to another instance for log review.
C. Create an Amazon Elastic File System (Amazon EFS) file system and add a command in the user data section of the Auto Scaling launch template to mount the EFS file system during EC2 instance creation Configure a process on the instance to copy the logs once a day from an instance Amazon Elastic Block Store (Amazon EBS) volume to a directory in the EFS file system.
D. Build the Amazon CloudWatch agent into the AMI used in the Auto Scaling grou
E. Configure the CloudWatch agent to send the logs to Amazon CloudWatch Logs for review.
F. Within the Auto Scaling lifecycle, add a lifecycle hook at the terminating state transition and alert the engineering team by using a lifecycle notification to Amazon Simple Notification Service (Amazon SNS). Configure the hook to remain in the Terminating:Wait state for 1 hour to allow manual review of the security logs prior to instance termination.

Answer: B

NEW QUESTION 25
- (Exam Topic 1)
A company is using AWS Organizations to manage multiple AWS member accounts. All of these accounts have Amazon GuardDuty enabled in all Regions. The company's AW5 Security Operations Center has a centralized security account for logging and monitoring. One of the member accounts has received an excessively high bill A security engineer discovers that a compromised Amazon EC2 instance is being used to mine crypto currency. The Security Operations Center did not receive a GuardDuty finding in the central security account.
but there was a GuardDuty finding in the account containing the compromised EC2 instance. The security engineer needs to ensure an GuardDuty finding are available in the security account.
What should the security engineer do to resolve this issue?

A. Set up an Amazon CloudWatch Event rule to forward ail GuardDuty findings to the security account Use an AWS Lambda function as a target to raise findings
B. Set up an Amazon CloudWatch Events rule to forward all GuardDuty findings to the security account Use an AWS Lambda function as a target to raise findings in AWS Security Hub
C. Check that GuardDuty in the security account is able to assume a role in the compromised account using the GuardDuty fast findings permission Schedule an Amazon CloudWatch Events rule and an AWS Lambda function to periodically check for GuardDuty findings
D. Use the aws GuardDuty get-members AWS CLI command m the security account to see if the account is listed Send an invitation from GuardDuty m the security account to GuardDuty in the compromised account Accept the invitation to forward all future GuardDuty findings

Answer: D

NEW QUESTION 27
- (Exam Topic 1)
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"
                }
            }
        }
    ]
}
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: A

NEW QUESTION 28
- (Exam Topic 1)
A convoys data lake uses Amazon S3 and Amazon Athena. The company's security engineer has been asked to design an encryption solution that meets the company's data protection requirements. The encryption solution must work with Amazon S3 and keys managed by the company. The encryption solution must be protected in a hardware security module that is validated id Federal information Processing Standards (FPS) 140-2 Level 3.
Which solution meets these requirements?

A. Use client-side encryption with an AWS KMS customer-managed key implemented with the AWS Encryption SDK
B. Use AWS CloudHSM to store the keys and perform cryptographic operations Save the encrypted text inAmazon S3
C. Use an AWS KMS customer-managed key that is backed by a custom key store using AWS CloudHSM
D. Use an AWS KMS customer-managed key with the bring your own key (BYOK) feature to import a key stored in AWS CloudHSM

Answer: B

NEW QUESTION 30
- (Exam Topic 1)
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: B

NEW QUESTION 32
- (Exam Topic 1)
A company is operating an open-source software platform that is internet facing. The legacy software platform no longer receives security updates. The software platform operates using Amazon route 53 weighted load balancing to send traffic to two Amazon EC2 instances that connect to an Amazon POS cluster a recent report suggests this software platform is vulnerable to SQL injection attacks. with samples of attacks provided. The company's security engineer must secure this system against SQL injection attacks within 24 hours. The secure, engineer's solution involve the least amount of effort and maintain normal operations during implementation.
What should the security engineer do to meet these requirements?

A. Create an Application Load Balancer with the existing EC2 instances as a target group Create an AWS WAF web ACL containing rules mat protect the application from this attac
B. then apply it to the ALB Test to ensure me vulnerability has been mitigated, then redirect thee Route 53 records to point to the ALB Update security groups on the EC 2 instances to prevent direct access from the internet
C. Create an Amazon CloudFront distribution specifying one EC2 instance as an origin Create an AWS WAF web ACL containing rules that protect the application from this attack, then apply it to me distribution Test to ensure the vulnerability has mitigated, then redirect the Route 53 records to point toCloudFront
D. Obtain me latest source code for the platform and make ire necessary updates Test me updated code to ensure that the vulnerability has been irrigated, then deploy me patched version of the platform to the EC2 instances
E. Update the security group mat is attached to the EC2 instances, removing access from the internet to the TCP port used by the SQL database Create an AWS WAF web ACL containing rules mat protect me application from this attack, men apply it to the EC2 instances Test to ensure me vulnerability has been mitigate
F. then restore the security group to me onginal setting

Answer: A

NEW QUESTION 34
- (Exam Topic 1)
A security engineer has noticed an unusually high amount of traffic coming from a single IP address. This was discovered by analyzing the Application Load Balancer's access logs. How can the security engineer limit the number of requests from a specific IP address without blocking the IP address?

A. Add a rule to the Application Load Balancer to route the traffic originating from the IP address in question and show a static webpage.
B. Implement a rate-based rule with AWS WAF
C. Use AWS Shield to limit the originating traffic hit rate.
D. Implement the GeoLocation feature in Amazon Route 53.

Answer: B

NEW QUESTION 36
- (Exam Topic 1)
After a recent security audit involving Amazon S3, a company has asked assistance reviewing its S3 buckets to determine whether data is properly secured. The first S3 bucket on the list has the following bucket policy.

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Effect":"Allow",
            "Principal":"*",
            "Action":"s3:*",
            "Resource":"arn:aws:s3:::examplebucket/*",
            "Condition":{
                "IpAddress":{
                    "aws:SourceIp":[
                        "10.10.10.0/24"
                    ]
                }
            }
        }
    ]
}
```

Is this bucket policy sufficient to ensure that the data is not publicity accessible?

A. Yes, the bucket policy makes the whole bucket publicly accessible despite now the S3 bucket ACL orobject ACLs are configured.
B. Yes, none of the data in the bucket is publicity accessible, regardless of how the S3 bucket ACL and object ACLs are configured.
C. No, the IAM user policy would need to be examined first to determine whether any data is publicly accessible.
D. No, the S3 bucket ACL and object ACLs need to be examined first to determine whether any data is publicly accessible.

Answer: A

NEW QUESTION 39
- (Exam Topic 1)
Which of the following are valid configurations for using SSL certificates with Amazon CloudFront? (Select THREE)

A. Default AWS Certificate Manager certificate
B. Custom SSL certificate stored in AWS KMS
C. Default CloudFront certificate
D. Custom SSL certificate stored in AWS Certificate Manager
E. Default SSL certificate stored in AWS Secrets Manager
F. Custom SSL certificate stored in AWS IAM

Answer: ACD

NEW QUESTION 44
- (Exam Topic 1)
A company is outsourcing its operational support 1o an external company. The company’s security officer must implement an access solution fen delegating operational support that minimizes overhead.
Which approach should the security officer take to meet these requirements?

A. implement Amazon Cognito identity pools with a role that uses a policy that denies the actions related to Amazon Cognito API management Allow the external company to federate through its identity provider
B. Federate AWS identity and Access Management (IAM) with the external company's identity provider Create an IAM role and attach a policy with the necessary permissions
C. Create an IAM group for me external company Add a policy to the group that denies IAM modifications Securely provide the credentials to the eternal company.
D. Use AWS SSO with the external company's identity provide
E. Create an IAM group to map to the identity provider user group, and attach a policy with the necessary permissions.

Answer: B

NEW QUESTION 47
- (Exam Topic 1)
A company has an application hosted in an Amazon EC2 instance and wants the application to access secure strings stored in AWS Systems Manager Parameter Store When the application tries to access the secure string key value, it fails.
Which factors could be the cause of this failure? (Select TWO.)

A. The EC2 instance role does not have decrypt permissions on the AWS Key Management Sen/ice (AWS KMS) key used to encrypt the secret
B. The EC2 instance role does not have read permissions to read the parameters In Parameter Store
C. Parameter Store does not have permission to use AWS Key Management Service (AWS KMS) to decrypt the parameter
D. The EC2 instance role does not have encrypt permissions on the AWS Key Management Service (AWS KMS) key associated with the secret
E. The EC2 instance does not have any tags associated.

Answer: CE

NEW QUESTION 49
- (Exam Topic 1)
A global company must mitigate and respond to DDoS attacks at Layers 3, 4 and 7 All of the company's AWS applications are serverless with static content hosted on Amazon S3 using Amazon CloudFront and Amazon Route 53
Which solution will meet these requirements?

A. Use AWS WAF with an upgrade to the AWS Business support plan
B. Use AWS Certificate Manager with an Application Load Balancer configured with an origin access identity
C. Use AWS Shield Advanced
D. Use AWS WAF to protect AWS Lambda functions encrypted with AWS KMS and a NACL restricting all Ingress traffic

Answer: C

NEW QUESTION 52
- (Exam Topic 1)
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: BD

NEW QUESTION 54
- (Exam Topic 1)
An AWS account administrator created an IAM group and applied the following managed policy to require that each individual user authenticate using multi-factor authentication:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:*",
            "Resource": "*"
        },
        {
            "Sid": "BlockAnyAccessUnlessSignedInWithMFA",
            "Effect": "Deny",
            "Action": "ec2:*",
            "Resource": "*",
            "Condition": {
                "BoolIfExists": {
                    "aws:MultiFactorAuthPresent": false
                }
            }
        }
    ]
}
```

After implementing the policy, the administrator receives reports that users are unable to perform Amazon EC2 commands using the AWS CLI. What should the administrator do to resolve this problem while still
enforcing multi-factor authentication?

A. Change the value of aws MultiFactorAuthPresent to true.
B. Instruct users to run the aws sts get-session-token CLI command and pass the multi-factor authentication—serial-number and —token-code parameter
C. Use these resulting values to make API/CLI calls
D. Implement federated API/CLI access using SAML 2.0, then configure the identity provider to enforce multi-factor authentication.
E. Create a role and enforce multi-factor authentication in the role trust policy Instruct users to run the sts assume-role CLI command and pass --serial-number and —token-code parameters Store the resulting values in environment variable
F. Add sts:AssumeRole to NotAction in the policy.

Answer: B

NEW QUESTION 59
- (Exam Topic 1)
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 range
C. Associate the security group to the NL
D. Create a second security group for EC2 instances with access on TCP port 443 from the NLB security group.
E. Create an AWS PrivateLink endpoint service in the parent company account attached to the NL
F. Create an AWS security group for the instances to allow access on TCP port 443 from the AWS PrivateLink endpoin
G. Use AWS PrivateLink interface endpoints in the 1,500 subsidiary AWS accounts to connect to the data processing application.
H. Create an AWS security group to allow access on TCP port 443 from the 1,500 subsidiary CIDR block range
I. Associate the security group with EC2 instances.

Answer: D

NEW QUESTION 63
- (Exam Topic 1)
A Security Engineer manages AWS Organizations for a company. The Engineer would like to restrict AWS usage to allow Amazon S3 only in one of the organizational units (OUs). The Engineer adds the following SCP to the OU:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowS3",
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": "*"
        }
    ]
}
```

The next day. API calls to AWS IAM appear in AWS CloudTrail logs In an account under that OU. How should the Security Engineer resolve this issue?

A. Move the account to a new OU and deny IAM:* permissions.
B. Add a Deny policy for all non-S3 services at the account level.
C. Change the policy to:{“Version”: “2012-10-17”,“Statement”: [{“Sid”: “AllowS3”,"Effect": "Allow","Action": "s3:*","Resource": "*/*»}]}
D. Detach the default FullAWSAccess SCP

Answer: C

NEW QUESTION 64
- (Exam Topic 1)
A company is collecting AWS CloudTrail log data from multiple AWS accounts by managing individual trails in each account and forwarding log data to a centralized Amazon S3 bucket residing in a log archive account. After CloudTrail introduced support for AWS Organizations trails, the company decided to further centralize management and automate deployment of the CloudTrail logging capability across all of its AWS accounts.
The company's security engineer created an AWS Organizations trail in the master account, enabled
server-side encryption with AWS KMS managed keys (SSE-KMS) for the log files, and specified the same bucket as the storage location. However, the engineer noticed that logs recorded by the new trail were not delivered to the bucket.
Which factors could cause this issue? (Select TWO.)

A. The CMK key policy does not allow CloudTrail to make encrypt and decrypt API calls against the key.
B. The CMK key policy does not allow CloudTrail to make GenerateDataKey API calls against the key.
C. The IAM role used by the CloudTrail trail does not have permissions to make PutObject API calls against a folder created for the Organizations trail.
D. The S3 bucket policy does not allow CloudTrail to make PutObject API calls against a folder created for the Organizations trail.
E. The CMK key policy does not allow the IAM role used by the CloudTrail trail to use the key for crypto graphicaI operations.

Answer: AD

NEW QUESTION 68
- (Exam Topic 1)
A Security Engineer has several thousand Amazon EC2 instances split across production and development environments. Each instance is tagged with its environment. The Engineer needs to analyze and patch all the development EC2 instances to ensure they are not currently exposed to any common vulnerabilities or exposures (CVEs)
Which combination of steps is the MOST efficient way for the Engineer to meet these requirements? (Select TWO.)

A. Log on to each EC2 instance, check and export the different software versions installed, and verify this against a list of current CVEs.
B. Install the Amazon Inspector agent on all development instances Build a custom rule package, and configure Inspector to perform a scan using this custom rule on all instances tagged as being in the development environment.
C. Install the Amazon Inspector agent on all development instances Configure Inspector to perform a scan using the CVE rule package on all instances tagged as being in the development environment.
D. Install the Amazon EC2 System Manager agent on all development instances Issue the Run command to EC2 System Manager to update all instances
E. Use AWS Trusted Advisor to check that all EC2 instances have been patched to the most recent versionof operating system and installed software.

Answer: CD

NEW QUESTION 71
- (Exam Topic 1)

A developer is creating an AWS Lambda function that requires environment variables to store connection information and logging settings. The developer is required to use an AWS KMS Customer Master Key (CMK> supplied by the information security department in order to adhere to company standards for securing Lambda environment variables.
Which of the following are required for this configuration to work? (Select TWO.)

A. The developer must configure Lambda access to the VPC using the --vpc-config parameter.
B. The Lambda function execution role must have the kms:Decrypt- permission added in the AWS IAM policy.
C. The KMS key policy must allow permissions for the developer to use the KMS key.
D. The AWS IAM policy assigned to the developer must have the kmseGcnerate-DataKcy permission added.
E. The Lambda execution role must have the kms:Encrypt permission added in the AWS IAM policy.

Answer: BC

NEW QUESTION 74
- (Exam Topic 1)
A security engineer is designing a solution that will provide end-to-end encryption between clients and Docker containers running In Amazon Elastic Container Service (Amazon ECS). This solution will also handle volatile traffic patterns
Which solution would have the MOST scalability and LOWEST latency?

A. Configure a Network Load Balancer to terminate the TLS traffic and then re-encrypt the traffic to the containers
B. Configure an Application Load Balancer to terminate the TLS traffic and then re-encrypt the traffic to the containers
C. Configure a Network Load Balancer with a TCP listener to pass through TLS traffic to the containers
D. Configure Amazon Route 53 to use multivalue answer routing to send traffic to the containers

Answer: A

NEW QUESTION 78
- (Exam Topic 1)
An external Auditor finds that a company's user passwords have no minimum length. The company is currently using two identity providers:
• AWS IAM federated with on-premises Active Directory
• Amazon Cognito user pools to accessing an AWS Cloud application developed by the company Which combination o1 actions should the Security Engineer take to solve this issue? (Select TWO.)

A. Update the password length policy In the on-premises Active Directory configuration.
B. Update the password length policy In the IAM configuration.
C. Enforce an IAM policy In Amazon Cognito and AWS IAM with a minimum password length condition.
D. Update the password length policy in the Amazon Cognito configuration.
E. Create an SCP with AWS Organizations that enforces a minimum password length for AWS IAM and Amazon Cognito.

Answer: AD

NEW QUESTION 80
- (Exam Topic 1)
A company uses multiple AWS accounts managed with AWS Organizations Security engineers have created a standard set of security groups for all these accounts. The security policy requires that these security groups be used for all applications and delegates modification authority to the security team only.
A recent security audit found that the security groups are inconsistency implemented across accounts and that unauthorized changes have been made to the security groups. A security engineer needs to recommend a solution to improve consistency and to prevent unauthorized changes in the individual accounts in the future.
Which solution should the security engineer recommend?

A. Use AWS Resource Access Manager to create shared resources for each requited security group and apply an IAM policy that permits read-only access to the security groups only.
B. Create an AWS CloudFormation template that creates the required security groups Execute the template as part of configuring new accounts Enable Amazon Simple Notification Service (Amazon SNS) notifications when changes occur
C. Use AWS Firewall Manager to create a security group policy, enable the policy feature to identify and revert local changes, and enable automatic remediation
D. Use AWS Control Tower to edit the account factory template to enable the snare security groups option Apply an SCP to the OU or individual accounts that prohibits security group modifications from local account users

Answer: B

NEW QUESTION 81
- (Exam Topic 1)
A company's application runs on Amazon EC2 and stores data in an Amazon S3 bucket The company wants additional security controls in place to limit the likelihood of accidental exposure of data to external parties
Which combination of actions will meet this requirement? (Select THREE.)

A. Encrypt the data in Amazon S3 using server-side encryption with Amazon S3 managed encryption keys (SSE-S3)
B. Encrypt the data in Amazon S3 using server-side encryption with AWS KMS managed encryption keys (SSE-KMS)
C. Create a new Amazon S3 VPC endpoint and modify the VPC's routing tables to use the new endpoint
D. Use the Amazon S3 Block Public Access feature.
E. Configure the bucket policy to allow access from the application instances only
F. Use a NACL to filter traffic to Amazon S3

Answer: BCE

NEW QUESTION 84
- (Exam Topic 1)
A company has implemented centralized logging and monitoring of AWS CloudTrail logs from all Regions in

an Amazon S3 bucket. The log Hies are encrypted using AWS KMS. A Security Engineer is attempting to review the log files using a third-party tool hosted on an Amazon EC2 instance The Security Engineer is unable to access the logs in the S3 bucket and receives an access denied error message
What should the Security Engineer do to fix this issue?

A. Check that the role the Security Engineer uses grants permission to decrypt objects using the KMS CMK.
B. Check that the role the Security Engineer uses grants permission to decrypt objects using the KMS CMK and gives access to the S3 bucket and objects
C. Check that the role the EC2 instance profile uses grants permission lo decrypt objects using the KMS CMK and gives access to the S3 bucket and objects
D. Check that the role the EC2 instance profile uses grants permission to decrypt objects using the KMS CMK

Answer: C

NEW QUESTION 85
- (Exam Topic 1)
A company is using AWS Organizations to manage multiple AWS accounts. The company has an application that allows users to assume the AppUser IAM role to download files from an Amazon S3 bucket that is encrypted with an AWS KMS CMK However when users try to access the files in the S3 bucket they get an access denied error.
What should a Security Engineer do to troubleshoot this error? (Select THREE)

A. Ensure the KMS policy allows the AppUser role to have permission to decrypt for the CMK
B. Ensure the S3 bucket policy allows the AppUser role to have permission to get objects for the S3 bucket
C. Ensure the CMK was created before the S3 bucket.
D. Ensure the S3 block public access feature is enabled for the S3 bucket.
E. Ensure that automatic key rotation is disabled for the CMK
F. Ensure the SCPs within Organizations allow access to the S3 bucket.

Answer: ABF

NEW QUESTION 87
- (Exam Topic 1)
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

NEW QUESTION 90
- (Exam Topic 1)
A security engineer is responsible for providing secure access to AWS resources for thousands of developer in a company’s corporate identity provider (idp). The developers access a set of AWS services from the corporate premises using IAM credential. Due to the velum of require for provisioning new IAM users, it is taking a long time to grant access permissions. The security engineer receives reports that developer are sharing their IAM credentials with others to avoid provisioning delays. The causes concern about overall security for the security engineer.
Which actions will meet the program requirements that address security?

A. Create an Amazon CloudWatch alarm for AWS CloudTrail Events Create a metric filter to send a notification when me same set of IAM credentials is used by multiple developer
B. Create a federation between AWS and the existing corporate IdP Leverage IAM roles to provide federated access to AWS resources
C. Create a VPN tunnel between the corporate premises and the VPC Allow permissions to all AWS services only if it originates from corporate premises.
D. Create multiple IAM rotes for each IAM user Ensure that users who use the same IAM credentials cannot assume the same IAM role at the same time.

Answer: B

NEW QUESTION 93
- (Exam Topic 1)
A company hosts its public website on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances are in an EC2 Auto Scaling group across multiple Availability Zones. The website is under a DDoS attack by a specific loT device brand that is visible in the user agent A security engineer needs to mitigate the attack without impacting the availability of the public website.
What should the security engineer do to accomplish this?

A. Configure a web ACL rule for AWS WAF to block requests with a string match condition for the user agent of the loT devic
B. Associate the v/eb ACL with the ALB.
C. Configure an Amazon CloudFront distribution to use the ALB as an origi
D. Configure a web ACL rule for AWS WAF to block requests with a string match condition for the user agent of the loT devic
E. Associate the web ACL with the ALB Change the public DNS entry of the website to point to the CloudFront distribution.
F. Configure an Amazon CloudFront distribution to use a new ALB as an origi
G. Configure a web ACL rule for AWS WAF to block requests with a string match condition for the user agent of the loT devic
H. Change the ALB security group to alow access from CloudFront IP address ranges only Change the public DNS entry of the website to point to the CloudFront distribution.
I. Activate AWS Shield Advanced to enable DDoS protectio
J. Apply an AWS WAF ACL to the AL
K. and configure a listener rule on the ALB to block loT devices based on the user agent.

Answer: D

NEW QUESTION 98
- (Exam Topic 1)
A company's Developers plan to migrate their on-premises applications to Amazon EC2 instances running Amazon Linux AMIs. The applications are accessed by a group of partner companies The Security Engineer needs to implement the following host-based security measures for these instances:
• Block traffic from documented known bad IP addresses
• Detect known software vulnerabilities and CIS Benchmarks compliance. Which solution addresses these requirements?

A. Launch the EC2 instances with an IAM role attache
B. Include a user data script that uses the AWS CLI to retrieve the list of bad IP addresses from AWS Secrets Manager and uploads it as a threat list in Amazon GuardDuty Use Amazon Inspector to scan the instances for known software vulnerabilities and CIS Benchmarks compliance
C. Launch the EC2 instances with an IAM role attached Include a user data script that uses the AWS CLI to create NACLs blocking ingress traffic from the known bad IP addresses in the EC2 instance's subnets Use AWS Systems Manager to scan the instances for known software vulnerabilities, and AWS Trusted Advisor to check instances for CIS Benchmarks compliance
D. Launch the EC2 instances with an IAM role attached Include a user data script that uses the AWS CLI to create and attach security groups that only allow an allow listed source IP address range inboun
E. Use Amazon Inspector to scan the instances for known software vulnerabilities, and AWS Trusted Advisor to check instances for CIS Benchmarks compliance
F. Launch the EC2 instances with an IAM role attached Include a user data script that creates a cron job to periodically retrieve the list of bad IP addresses from Amazon S3, and configures iptabies on the instances blocking the list of bad IP addresses Use Amazon inspector to scan the instances for known software vulnerabilities and CIS Benchmarks compliance.

Answer: D

NEW QUESTION 101
- (Exam Topic 1)
A security engineer needs to configure monitoring and auditing for AWS Lambda.
Which combination of actions using AWS services should the security engineer take to accomplish this goal? (Select TWO.)

A. Use AWS Config to track configuration changes to Lambda functions, runtime environments, tags, handler names, code sizes, memory allocation, timeout settings, and concurrency settings, along with Lambda IAM execution role, subnet, and security group associations.
B. Use AWS CloudTrail to implement governance, compliance, operational, and risk auditing for Lambda.
C. Use Amazon Inspector to automatically monitor for vulnerabilities and perform governance, compliance, operational, and risk auditing for Lambda.
D. Use AWS Resource Access Manager to track configuration changes to Lambda functions, runtime environments, tags, handler names, code sizes, memory allocation, timeout settings, and concurrency settings, along with Lambda IAM execution role, subnet, and security group associations.
E. Use Amazon Macie to discover, classify, and protect sensitive data being executed inside the Lambda function.

Answer: AB

NEW QUESTION 103
- (Exam Topic 1)
A company has a compliance requirement to rotate its encryption keys on an annual basis. A Security Engineer needs a process to rotate the KMS Customer Master Keys (CMKs) that were created using imported key material.
How can the Engineer perform the key rotation process MOST efficiently?

A. Create a new CMK, and redirect the existing Key Alias to the new CMK
B. Select the option to auto-rotate the key
C. Upload new key material into the existing CMK.
D. Create a new CMK, and change the application to point to the new CMK

Answer: A

NEW QUESTION 107
- (Exam Topic 1)
A Security Engineer creates an Amazon S3 bucket policy that denies access to all users. A few days later, the Security Engineer adds an additional statement to the bucket policy to allow read-only access to one other employee Even after updating the policy the employee still receives an access denied message.
What is the likely cause of this access denial?

A. The ACL in the bucket needs to be updated.
B. The IAM policy does not allow the user to access the bucket
C. It takes a few minutes for a bucket policy to take effect
D. The allow permission is being overridden by the deny.

Answer: D

NEW QUESTION 111
- (Exam Topic 1)
A company is developing a new mobile app for social media sharing. The company's development team has decided to use Amazon S3 to store at media files generated by mobile app users The company wants to allow users to control whether their own tiles are public, private, of shared with other users in their social network what should the development team do to implement the type of access control with the LEAST administrative effort?

A. Use individual ACLs on each S3 object.
B. Use IAM groups tor sharing files between application social network users
C. Store each user's files in a separate S3 bucket and apery a bucket policy based on the user's sharing settings
D. Generate presigned UPLs for each file access

Answer: A

NEW QUESTION 114
- (Exam Topic 1)
A large government organization is moving to the cloud and has specific encryption requirements. The first workload to move requires that a customer's data be immediately destroyed when the customer makes that request.
Management has asked the security team to provide a solution that will securely store the data, allow only authorized applications to perform encryption and decryption and allow for immediate destruction of the data
Which solution will meet these requirements?

A. Use AWS Secrets Manager and an AWS SDK to create a unique secret for the customer-specific data
B. Use AWS Key Management Service (AWS KMS) and the AWS Encryption SDK to generate and store a data encryption key for each customer.
C. Use AWS Key Management Service (AWS KMS) with service-managed keys to generate and store customer-specific data encryption keys
D. Use AWS Key Management Service (AWS KMS) and create an AWS CloudHSM custom key store Use CloudHSM to generate and store a new CMK for each customer.

Answer: A

NEW QUESTION 116
- (Exam Topic 1)
A company's security team has defined a set of AWS Config rules that must be enforced globally in all AWS accounts the company owns. What should be done to provide a consolidated compliance overview for the security team?

A. Use AWS Organizations to limit AWS Config rules to the appropriate Regions, and then consolidate the Amazon CloudWatch dashboard into one AWS account.
B. Use AWS Config aggregation to consolidate the views into one AWS account, and provide role access to the security team.
C. Consolidate AWS Config rule results with an AWS Lambda function and push data to Amazon SQ
D. Use Amazon SNS to consolidate and alert when some metrics are triggered.
E. Use Amazon GuardDuty to load data results from the AWS Config rules compliance status, aggregate GuardDuty findings of all AWS accounts into one AWS account, and provide role access to the security team.

Answer: B

NEW QUESTION 120
- (Exam Topic 1)
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 ip tables-based restrictions on the instances.
D. Install the Amazon Inspector agent on the instances.

Answer: A

Explanation:
"To turn off access to instance metadata on an existing instance....." https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/configuring-instance-metadata-service.html You can disable the service for existing (running or stopped) ec2 instances. https://docs.aws.amazon.com/cli/latest/reference/ec2/modify-instance-metadata-options.html

NEW QUESTION 121
- (Exam Topic 1)
A security engineer must use AWS Key Management Service (AWS KMS) to design a key management solution for a set of Amazon Elastic Block Store (Amazon EBS) volumes that contain sensitive data. The solution needs to ensure that the key material automatically expires in 90 days.
Which solution meets these criteria?

A. A customer managed CMK that uses customer provided key material
B. A customer managed CMK that uses AWS provided key material
C. An AWS managed CMK
D. Operating system-native encryption that uses GnuPG

Answer: B

NEW QUESTION 123
- (Exam Topic 1)
A Security Engineer has discovered that, although encryption was enabled on the Amazon S3 bucket example bucket, 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 “${aws:username}” variable.
C. Create a customer-managed CMK for each use
D. Add each user as a key user in their corresponding key policy.
E. Change the applicable IAM policy to grant S3 access to “Resource”: “arn:aws:s3:::examplebucket/${aws:username}/*”

Answer: B

Explanation:
Reference: https://aws.amazon.com/premiumsupport/knowledge-center/iam-s3-user-specific-folder/

NEW QUESTION 125
- (Exam Topic 1)
A company has a website with an Amazon CloudFront HTTPS distribution, an Application Load Balancer (ALB) with multiple web instances for dynamic website content, and an Amazon S3 bucket for static website content. The company's security engineer recently updated the website security requirements:
• HTTPS needs to be enforced for all data in transit with specific ciphers.
• The CloudFront distribution needs to be accessible from the internet only. Which solution will meet these requirements?

A. Set up an S3 bucket policy with the awssecuretransport key Configure the CloudFront origin access identity (OAI) with the S3 bucket Configure CloudFront to use specific cipher
B. Enforce the ALB with an HTTPS listener only and select the appropriate security policy for the ciphers Link the ALB with AWS WAF to allow access from the CloudFront IP ranges.
C. Set up an S3 bucket policy with the aws:securetransport ke
D. Configure the CloudFront origin access identity (OAI) with the S3 bucke
E. Enforce the ALB with an HTTPS listener only and select the appropriate security policy for the ciphers.
F. Modify the CloudFront distribution to use AWS WA
G. Force HTTPS on the S3 bucket with specific ciphers in the bucket polic
H. Configure an HTTPS listener only for the AL
I. Set up a security group to limit access to the ALB from the CloudFront IP ranges
J. Modify the CloudFront distribution to use the ALB as the origi
K. Enforce an HTTPS listener on the AL
L. Create a path-based routing rule on the ALB with proxies that connect lo Amazon S3. Create a bucket policy to allow access from these proxies only.A company Is trying to replace its on-premises bastion hosts used to access on-premises Linux servers with AWS Systems Manager Session Manage
M. A security engineer has installed the Systems Manager Agent on all server
N. The security engineer verifies that the agent is running on all the servers, but Session Manager cannot connect to the
O. The security engineer needs to perform verification steps before Session Manager will work on the servers.Which combination of steps should the security engineer perform? (Select THREE.)
P. Open inbound port 22 to 0 0.0.0/0 on all Linux servers.
Q. Enable the advanced-instances tier in Systems Manager.
R. Create a managed-instance activation for the on-premises servers.
S. Reconfigure the Systems Manager Agent with the activation code and ID.
T. Assign an IAM role to all of the on-premises servers.
. Initiate an inventory collection with Systems Manager on the on-premises servers

Answer: CEF

NEW QUESTION 126
- (Exam Topic 2)
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

NEW QUESTION 127
- (Exam Topic 2)
You are deivising a policy to allow users to have the ability to access objects in a bucket called appbucket. You define the below custom bucket policy

{ "ID": "Policy1502987489630",
"Version": "2012-10-17",
"Statement": [
{
"Sid": "Stmt1502987487640",
"Action": [
"s3:GetObject",
"s3:GetObjectVersion"
],
"Effect": "Allow",
"Resource": "arn:aws:s3:::appbucket",
"Principal": "*"
}
]
}

But when you try to apply the policy you get the error "Action does not apply to any resource(s) in statement." What should be done to rectify the error
Please select:

A. Change the IAM permissions by applying PutBucketPolicy permissions.
B. Verify that the policy has the same name as the bucket nam
C. If no
D. make it the same.
E. Change the Resource section to "arn:aws:s3:::appbucket/*'.
F. Create the bucket "appbucket" and then apply the policy.

Answer: C

Explanation:
When you define access to objects in a bucket you need to ensure that you specify to which objects in the bucket access needs to be given to. In this case, the * can be used to assign the permission to all objects in the bucket
Option A is invalid because the right permissions are already provided as per the question requirement Option B is invalid because it is not necessary that the policy has the same name as the bucket
Option D is invalid because this should be the default flow for applying the policy For more information on bucket policies please visit the below URL:
https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.htmll
The correct answer is: Change the Resource section to "arn:aws:s3:::appbucket/" Submit your Feedback/Queries to our Experts

NEW QUESTION 130
- (Exam Topic 2)
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: C

NEW QUESTION 135
- (Exam Topic 2)
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: AE

Explanation:
https://medium.com/mudita-misra/how-to-audit-your-aws-resources-for-security-compliance-by-using-custom-a

NEW QUESTION 140

- (Exam Topic 2)
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: ACE

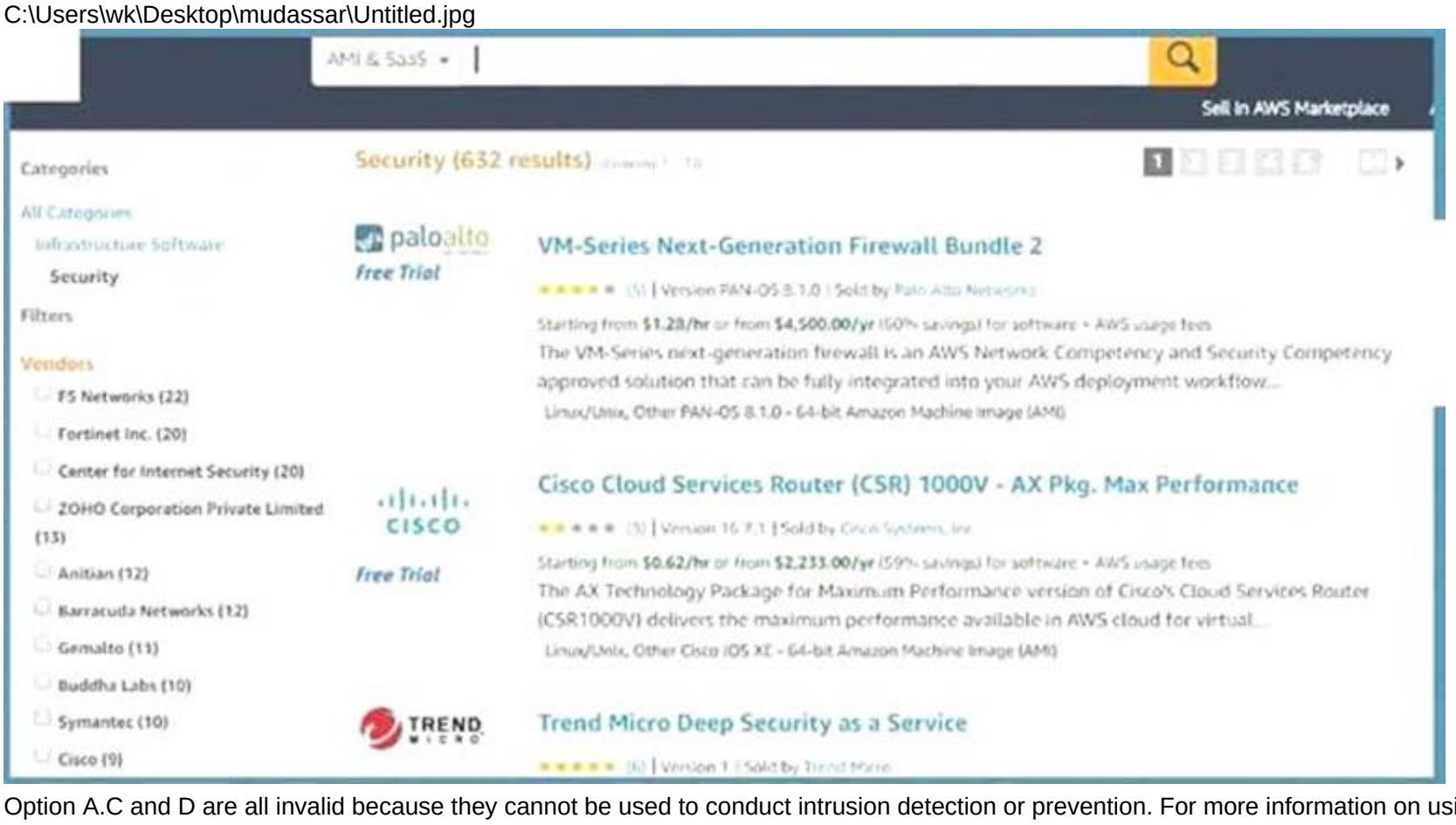
Explanation:
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/best-practices-security.html
If you have created an organization in AWS Organizations, you can create a trail that will log all events for all AWS accounts in that organization. This is sometimes referred to as an organization trail. You can also choose to edit an existing trail in the master account and apply it to an organization, making it an organization trail. Organization trails log events for the master account and all member accounts in the organization. For more information about AWS Organizations, see Organizations Terminology and Concepts. Note Reference: https://docs.aws.amazon.com/awscloudtrail/latest/userguide/creating-trail-organization.html You must be logged in with the master account for the organization in order to create an organization trail. You must also have sufficient permissions for the IAM user or role in the master account in order to successfully create an organization trail. If you do not have sufficient permissions, you will not see the option to apply a trail to an organization.

NEW QUESTION 143
- (Exam Topic 2)
A company wants to have an Intrusion detection system available for their VPC in AWS. They want to have complete control over the system. Which of the following would be ideal to implement?
Please select:

A. Use AWS WAF to catch all intrusions occurring on the systems in the VPC
B. Use a custom solution available in the AWS Marketplace
C. Use VPC Flow logs to detect the issues and flag them accordingly.
D. Use AWS Cloudwatch to monitor all traffic

Answer: B

Explanation:
Sometimes companies want to have custom solutions in place for monitoring Intrusions to their systems. In such a case, you can use the AWS Marketplace for looking at custom solutions.
C:\Users\wk\Desktop\mudassar\Untitled.jpg



Option A.C and D are all invalid because they cannot be used to conduct intrusion detection or prevention. For more information on using custom security solutions please visit the below URL https://d1.awsstatic.com/Marketplace/security/AWSMP_Security_Solution%200verview.pdf
For more information on using custom security solutions please visit the below URL: https://d1 .awsstatic.com/Marketplace/security/AWSMP Security Solution%20Overview.pd1
The correct answer is: Use a custom solution available in the AWS Marketplace Submit your Feedback/Queries to our Experts

NEW QUESTION 145
- (Exam Topic 2)
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:
https://aws.amazon.com/blogs/security/how-to-record-and-govern-your-iam-resource-configurations-using-aws

NEW QUESTION 148
- (Exam Topic 2)
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: BEF

NEW QUESTION 152
- (Exam Topic 2)
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: B

Explanation:
https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_data-sources.html https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_backdoor.html

NEW QUESTION 153
- (Exam Topic 2)
Your company is planning on hosting an internal network in AWS. They want machines in the VPC to authenticate using private certificates. They want to minimize the work and maintenance in working with certificates. What is the ideal way to fulfil this requirement.
Please select:

A. Consider using Windows Server 2016 Certificate Manager
B. Consider using AWS Certificate Manager
C. Consider using AWS Access keys to generate the certificates
D. Consider using AWS Trusted Advisor for managing the certificates

Answer: B

Explanation:
The AWS Documentation mentions the following
ACM is tightly linked with AWS Certificate Manager Private Certificate Authority. You can use ACM PCA to create a private certificate authority (CA) and then use ACM to issue private certificates. These are SSL/TLS X.509 certificates that identify users, computers, applications, services, servers, and other devices internally. Private certificates cannot be publicly trusted
Option A is partially invalid. Windows Server 2016 Certificate Manager can be used but since there is a requirement to "minimize the work and maintenance", AWS Certificate Manager should be used
Option C and D are invalid because these cannot be used for managing certificates. For more information on ACM, please visit the below URL:
https://docs.aws.amazon.com/acm/latest/userguide/acm-overview.html
The correct answer is: Consider using AWS Certificate Manager Submit your Feedback/Queries to our Experts

NEW QUESTION 157
- (Exam Topic 2)
Which of the following is not a best practice for carrying out a security audit? Please select:

A. Conduct an audit on a yearly basis
B. Conduct an audit if application instances have been added to your account
C. Conduct an audit if you ever suspect that an unauthorized person might have accessed your account
D. Whenever there are changes in your organization

Answer: A

Explanation:
A year's time is generally too long a gap for conducting security audits The AWS Documentation mentions the following

You should audit your security configuration in the following situations: On a periodic basis.
If there are changes in your organization, such as people leaving.
If you have stopped using one or more individual AWS services. This is important for removing permissions that users in your account no longer need.
If you've added or removed software in your accounts, such as applications on Amazon EC2 instances, AWS OpsWor stacks, AWS CloudFormation templates, etc.
If you ever suspect that an unauthorized person might have accessed your account.
Option B, C and D are all the right ways and recommended best practices when it comes to conducting audits For more information on Security Audit guideline, please visit the below URL:
https://docs.aws.amazon.com/eeneral/latest/gr/aws-security-audit-euide.html
The correct answer is: Conduct an audit on a yearly basis Submit your Feedback/Queries to our Experts

NEW QUESTION 162
- (Exam Topic 2)
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: A

Explanation:
https://aws.amazon.com/artifact/

NEW QUESTION 163
- (Exam Topic 2)
A company wants to have a secure way of generating, storing and managing cryptographic exclusive access for the keys. Which of the following can be used for this purpose?
Please select:

A. Use KMS and the normal KMS encryption keys
B. Use KMS and use an external key material
C. Use S3 Server Side encryption
D. Use Cloud HSM

Answer: D

Explanation:
The AWS Documentation mentions the following
The AWS CloudHSM service helps you meet corporate, contractual and regulatory compliance requirements for data security by using dedicated Hardware Security Module (HSM) instances within the AWS cloud. AWS and AWS Marketplace partners offer a variety of solutions for protecting sensitive data within the AWS platform, but for some applications and data subject to contractual or regulatory mandates for managing cryptographic keys, additional protection may be necessary. CloudHSM complements existing data protection solutions and allows you to protect your encryption keys within HSMs that are desigr and validated to government standards for secure key management. CloudHSM allows you to securely generate, store and manage cryptographic keys used for data encryption in a way that keys are accessible only by you.
Option A.B and Care invalid because in all of these cases, the management of the key will be with AWS. Here the question specifically mentions that you want to have exclusive access over the keys. This can be achieved with Cloud HSM
For more information on CloudHSM, please visit the following URL: https://aws.amazon.com/cloudhsm/faq:
The correct answer is: Use Cloud HSM Submit your Feedback/Queries to our Experts

NEW QUESTION 164
- (Exam Topic 2)
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 instance
C. Have the ELB decrypt traffic, and route and re-encrypt with the same certificate.
D. Generate an internal self-signed certificate and apply it to the instance
E. Use AWS Certificate Manager to generate a new external certificate for the EL
F. Have the ELB decrypt traffic, and route andre-encrypt with the internal certificate.
G. Upload a new external certificate to the load balance
H. Have the ELB decrypt the traffic and forward it on port 80 to the instances.

Answer: C

NEW QUESTION 166
- (Exam Topic 2)
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? (Select 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: BCE

NEW QUESTION 167
- (Exam Topic 2)
A company is using CloudTrail to log all AWS API activity for all regions in all of its accounts. The CISO has asked that additional steps be taken to protect the integrity of the log files.
What combination of steps will protect the log files from intentional or unintentional alteration? Choose 2 answers from the options given below
Please select:

A. Create an S3 bucket in a dedicated log account and grant the other accounts write only acces
B. Deliver all log files from every account to this S3 bucket.
C. Write a Lambda function that queries the Trusted Advisor Cloud Trail check
D. Run the function every 10 minutes.
E. Enable CloudTrail log file integrity validation
F. Use Systems Manager Configuration Compliance to continually monitor the access policies of S3 buckets containing Cloud Trail logs.
G. Create a Security Group that blocks all traffic except calls from the CloudTrail servic
H. Associate the security group with) all the Cloud Trail destination S3 buckets.

Answer: AC

Explanation:
The AWS Documentation mentions the following
To determine whether a log file was modified, deleted, or unchanged after CloudTrail delivered it you can use CloudTrail log fill integrity validation. This feature is built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing. This makes it computationally infeasible to modify, delete or forge CloudTrail log files without detection.
Option B is invalid because there is no such thing as Trusted Advisor Cloud Trail checks Option D is invalid because Systems Manager cannot be used for this purpose.
Option E is invalid because Security Groups cannot be used to block calls from other services For more information on Cloudtrail log file validation, please visit the below URL:
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-loe-file-validation-intro.htmll For more information on delivering Cloudtrail logs from multiple accounts, please visit the below URL:
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-receive-logs-from-multiple-accounts.htm
The correct answers are: Create an S3 bucket in a dedicated log account and grant the other accounts write only access. Deliver all log files from every account to this S3 bucket, Enable Cloud Trail log file integrity validation
Submit your Feedback/Queries to our Experts

NEW QUESTION 170
- (Exam Topic 2)
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: CE

NEW QUESTION 174
- (Exam Topic 2)
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: CE

Explanation:
The EBS which is AWS resource service is encrypted with CMK and to allow EC2 to decrypt , the IAM user should create a grant (action) and a boolean condition for the AWs resource . This link explains how AWS keys works. https://docs.aws.amazon.com/kms/latest/developerguide/key-policies.html

NEW QUESTION 178
- (Exam Topic 2)
You have a vendor that needs access to an AWS resource. You create an AWS user account. You want to restrict access to the resource using a policy for just that user over a brief period. Which of the following would be an ideal policy to use?
Please select:

A. An AWS Managed Policy
B. An Inline Policy
C. A Bucket Policy
D. A bucket ACL

Answer: B

Explanation:
The AWS Documentation gives an example on such a case
Inline policies are useful if you want to maintain a strict one-to-one relationship between a policy and the principal entity that if s applied to. For example, you want to be sure that the permissions in a policy are not inadvertently assigned to a principal entity other than the one they're intended for. When you use an inline policy, the permissions in the policy cannot be inadvertently attached to the wrong principal entity. In addition, when you use the AWS Management Console to delete that principal entit the policies embedded in the principal entity are deleted as well. That's because they are part of the principal entity.
Option A is invalid because AWS Managed Polices are ok for a group of users, but for individual users, inline policies are better.
Option C and D are invalid because they are specifically meant for access to S3 buckets For more information on policies, please visit the following URL:
https://docs.aws.amazon.com/IAM/latest/UserGuide/access managed-vs-inline
The correct answer is: An Inline Policy Submit your Feedback/Queries to our Experts

NEW QUESTION 179
- (Exam Topic 2)
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 credential
B. Provide the credentials to AnyCompany.Monitor access in IAM access advisor and plan to rotate credentials on a recurring basis.
C. Request an external ID from AnyCompany and add a condition with sts:Externald to the role's trust policy.
D. Require two-factor authentication by adding a condition to the role's trust policy with aws:MultiFactorAuthPresent.
E. Request an IP range from AnyCompany and add a condition with aws:SourceIp to the role's trust policy.

Answer: B

NEW QUESTION 182
- (Exam Topic 2)
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:
https://d1.awsstatic.com/whitepapers/aws_security_incident_response.pdf

NEW QUESTION 187
- (Exam Topic 2)
A company is hosting a website that must be accessible to users for HTTPS traffic. Also port 22 should be open for administrative purposes. The administrator's workstation has a static IP address of 203.0.113.1/32. Which of the following security group configurations are the MOST secure but still functional to support these requirements? Choose 2 answers from the options given below
Please select:

A. Port 443 coming from 0.0.0.0/0
B. Port 443 coming from 10.0.0.0/16
C. Port 22 coming from 0.0.0.0/0
D. Port 22 coming from 203.0.113.1/32

Answer: AD

Explanation:
Since HTTPS traffic is required for all users on the Internet, Port 443 should be open on all IP addresses. For port 22, the traffic should be restricted to an internal subnet.
Option B is invalid, because this only allow traffic from a particular CIDR block and not from the internet Option C is invalid because allowing port 22 from the internet is a security risk
For more information on AWS Security Groups, please visit the following UR https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/usins-network-secunty.htmll
The correct answers are: Port 443 coming from 0.0.0.0/0, Port 22 coming from 203.0.113.1 /32 Submit your Feedback/Queries to our Experts

NEW QUESTION 191
- (Exam Topic 2)
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 Stor
E. 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.
F. 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 rotate
G. Grant permission to the instance role associated with the EC2 instance to access Secrets Manager.

Answer: CE

NEW QUESTION 195
- (Exam Topic 2)
A security team must present a daily briefing to the CISO that includes a report of which of the company's thousands of EC2 instances and on-premises servers are missing the latest security patches. All instances/servers must be brought into compliance within 24 hours so they do not show up on the next day's report.
How can the security team fulfill these requirements?
Please select:

A. Use Amazon QuickSight and Cloud Trail to generate the report of out of compliance instances/servers.Redeploy all out of compliance instances/servers using an AMI with the latest patches.
B. Use Systems Manger Patch Manger to generate the report of out of compliance instances/ server
C. Use Systems Manager Patch Manger to install the missing patches.
D. Use Systems Manger Patch Manger to generate the report of out of compliance instances/ servers.Redeploy all out of1 compliance instances/servers using an AMI with the latest patches.
E. Use Trusted Advisor to generate the report of out of compliance instances/server
F. Use Systems Manger Patch Manger to install the missing patches.

Answer: B

Explanation:
Use the Systems Manger Patch Manger to generate the report and also install the missing patches The AWS Documentation mentions the following
AWS Systems Manager Patch Manager automates the process of patching managed instances with
security-related updates. For Linux-based instances, you can also install patches for non-security updates. You can patch fleets of Amazon EC2 instances or your on-premises servers and virtual machines (VMs) by operating system type. This includes supported versions of Windows, Ubuntu Server, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), and Amazon Linux. You can scan instances to see only a report of missing patches, or you can scan and automatically install all missing patches.
Option A is invalid because Amazon QuickSight and Cloud Trail cannot be used to generate the list of servers that don't meet compliance needs.
Option C is wrong because deploying instances via new AMI'S would impact the applications hosted on these servers
Option D is invalid because Amazon Trusted Advisor cannot be used to generate the list of servers that don't meet compliance needs.
For more information on the AWS Patch Manager, please visit the below URL:
https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-patch.html (
The correct answer is: Use Systems Manger Patch Manger to generate the report of out of compliance instances/ servers. Use Systems Manager Patch Manger to install the missing patches.
Submit your Feedback/Queries to our Experts

NEW QUESTION 200
- (Exam Topic 2)
Your company has mandated that all calls to the AWS KMS service be recorded. How can this be achieved? Please select:

A. Enable logging on the KMS service
B. Enable a trail in Cloudtrail
C. Enable Cloudwatch logs
D. Use Cloudwatch metrics

Answer: B

Explanation:
The AWS Documentation states the following
AWS KMS is integrated with CloudTrail, a service that captures API calls made by or on behalf of AWS KMS in your AWS account and delivers the log files to an Amazon S3 bucket that you specify. CloudTrail captures API calls from the AWS KMS console or from the AWS KMS API. Using the information collected by CloudTrail, you can determine what request was made, the source IP address from which the request was made, who made the request when it was made, and so on.

Option A is invalid because logging is not possible in the KMS service
Option C and D are invalid because Cloudwatch cannot be used to monitor API calls For more information on logging using Cloudtrail please visit the below URL https://docs.aws.amazon.com/kms/latest/developerguide/loeeing-usine-cloudtrail.html The correct answer is: Enable a trail in Cloudtrail
Jubmit your Feedback/Queries to our Experts

NEW QUESTION 205
- (Exam Topic 2)
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. (Select 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: BE

NEW QUESTION 210
- (Exam Topic 2)
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 roo
B. Enable multi-factor authentication of the root user account for each organizational member account.
C. Configure IAM user policies to restrict root account capabilities for each Organizations member account.
D. Create an organizational unit (OU) in Organizations with a service control policy that controls usage of the root use
E. Add all operational accounts to the new OU.
F. Configure AWS CloudTrail to integrate with Amazon CloudWatch Logs and then create a metric filter for RootAccountUsage.

Answer: C

Explanation:
Applying a "Control Policy" in your organization. A policy applied to: 1) root applies to all accounts in the organization 2) OU applies to all accounts in the OU and to any child OUs 3) account applies to one account only Note- this requires that Acquirements: -all features are enabled for the organization in AWS Organizations -Only service control policy (SCP) are supported https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies.html

NEW QUESTION 213
- (Exam Topic 2)
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: ACE

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

NEW QUESTION 218
- (Exam Topic 2)
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

NEW QUESTION 220
- (Exam Topic 2)
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: C

Explanation:
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html

NEW QUESTION 221
- (Exam Topic 2)
Your IT Security team has advised to carry out a penetration test on the resources in their company's AWS Account. This is as part of their capability to analyze the security of the Infrastructure. What should be done first in this regard?
Please select:

A. Turn on Cloud trail and carry out the penetration test
B. Turn on VPC Flow Logs and carry out the penetration test
C. Submit a request to AWS Support
D. Use a custom AWS Marketplace solution for conducting the penetration test

Answer: C

Explanation:
This concept is given in the AWS Documentation
How do I submit a penetration testing request for my AWS resources? Issue
I want to run a penetration test or other simulated event on my AWS architecture. How do I get permission from AWS to do that?
Resolution
Before performing security testing on AWS resources, you must obtain approval from AWS. After you submit your request AWS will reply in about two business days.
AWS might have additional questions about your test which can extend the approval process, so plan accordingly and be sure that your initial request is as detailed as possible.
If your request is approved, you'll receive an authorization number.
Option A.B and D are all invalid because the first step is to get prior authorization from AWS for penetration tests
For more information on penetration testing, please visit the below URL
* https://aws.amazon.com/security/penetration-testing/
* https://aws.amazon.com/premiumsupport/knowledge-center/penetration-testing/ (
The correct answer is: Submit a request to AWS Support Submit your Feedback/Queries to our Experts

NEW QUESTION 223
- (Exam Topic 2)
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: A

Explanation:
By default, Private instance has a private IP address, but no public IP address. These instances can communicate with each other, but can't access the Internet. You can enable Internet access for an instance launched into a nondefault subnet by attaching an Internet gateway to its VPC (if its VPC is not a default VPC) and associating an Elastic IP address with the instance. Alternatively, to allow an instance in your VPC to initiate outbound connections to the Internet but prevent unsolicited inbound connections from the Internet, you can use a network address translation (NAT) instance. NAT maps multiple private IP addresses to a single public IP address. A NAT instance has an Elastic IP address and is connected to the Internet through an Internet gateway.You can connect an instance in a private subnet to the Internet through the NAT instance, which routes traffic from the instance to the Internet gateway, and routes any responses to the instance.

NEW QUESTION 227
- (Exam Topic 2)
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

NEW QUESTION 229
- (Exam Topic 2)
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: BDE

Explanation:
https://d1.awsstatic.com/whitepapers/aws_security_incident_response.pdf

NEW QUESTION 231
- (Exam Topic 2)
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

NEW QUESTION 232
- (Exam Topic 2)
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 functio
B. Then, create a new Amazon CloudWatch metric for Amazon S3 object access to alert when the objects are accessed.
C. Enable Amazon Macie on the S3 buckets that were impacted, then perform data classificatio
D. For identified objects that contain PII, use the research function for auditing AWS CloudTrail logs and S3 bucket logs for GET operations.
E. Enable Amazon GuardDuty and enable the PII rule set on the S3 buckets that were impacted, then perform data classificatio
F. Using the PII findings report from GuardDuty, query the S3 bucket logs by using Athena for GET operations.
G. Enable Amazon Inspector on the S3 buckets that were impacted, then perform data classificatio
H. For identified objects that contain PII, query the S3 bucket logs by using Athena for GET operations.

Answer: B

NEW QUESTION 235
- (Exam Topic 2)
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

NEW QUESTION 236
- (Exam Topic 2)
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: C

NEW QUESTION 239
- (Exam Topic 2)
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: C

Explanation:
https://docs.aws.amazon.com/kms/latest/developerguide/importing-keys-delete-key-material.html

NEW QUESTION 242
- (Exam Topic 2)
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:
https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-restricting-access-to-s3

NEW QUESTION 244
- (Exam Topic 2)
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/

NEW QUESTION 247
- (Exam Topic 2)
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: B

Explanation:
"automatic key rotation has no effect on the data that the CMK protects. It does not rotate the data keys that the CMK generated or re-encrypt any data protected by the CMK, and it will not mitigate the effect of a compromised data key. You might decide to create a new CMK and use it in place of the original CMK. This has the same effect as rotating the key material in an existing CMK, so it's often thought of as manually rotating the key."
https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html

NEW QUESTION 252
- (Exam Topic 2)
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

NEW QUESTION 254
- (Exam Topic 2)
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: AC

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.

NEW QUESTION 257
- (Exam Topic 2)
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 certificat
B. Use that certificate to encrypt data prior to uploading it to DynamoDB.
C. Enable S3 server-side encryption with the customer-provided key
D. Upload the data to Amazon S3, and then use S3Copy to move all data to DynamoDB

E. Create a KMS master ke
F. Generate per-record data keys and use them to encrypt data prior to uploading it to DynamoD
G. Dispose of the cleartext and encrypted data keys after encryption without storing.
H. Use the DynamoDB Java encryption client to encrypt data prior to uploading it to DynamoDB.

Answer: D

Explanation:
Follow the link:
https://docs.aws.amazon.com/dynamodb-encryption-client/latest/devguide/what-is-ddb-encrypt.html

NEW QUESTION 260
- (Exam Topic 2)
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 accoun
B. Verify that a metric filter was created and then mapped to an alar
C. Check the alarm notification action.
D. Check the CloudWatch dashboards to ensure that there is a metric configured with an appropriate dimension for security group changes.
E. Verify that the Analyst's account is mapped to an IAM policy that includes permissions for cloudwatch: GetMetricStatistics and Cloudwatch: ListMetrics.

Answer: B

Explanation:
MetricFilter:
Type: 'AWS::Logs::MetricFilter' Properties:
LogGroupName: '' FilterPattern: >
{ ($.eventName = AuthorizeSecurityGroupIngress) || ($.eventName = AuthorizeSecurityGroupEgress) || ($.eventName = RevokeSecurityGroupIngress) || ($.eventName = RevokeSecurityGroupEgress)
|| ($.eventName = CreateSecurityGroup) || ($.eventName = DeleteSecurityGroup) }
MetricTransformations:
- MetricValue: '1'
MetricNamespace: CloudTrailMetrics MetricName: SecurityGroupEventCount

NEW QUESTION 265
- (Exam Topic 2)
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

NEW QUESTION 267
- (Exam Topic 2)
Your company has a set of resources defined in the AWS Cloud. Their IT audit department has requested to get a list of resources that have been defined across the account. How can this be achieved in the easiest manner?
Please select:

A. Create a powershell script using the AWS CL
B. Query for all resources with the tag of production.
C. Create a bash shell script with the AWS CL
D. Query for all resources in all region
E. Store the results in an S3 bucket.
F. Use Cloud Trail to get the list of all resources
G. Use AWS Config to get the list of all resources

Answer: D

Explanation:
The most feasible option is to use AWS Config. When you turn on AWS Config, you will get a list of resources defined in your AWS Account.
A sample snapshot of the resources dashboard in AWS Config is shown below C:\Users\wk\Desktop\mudassar\Untitled.jpg

Option A is incorrect because this would give the list of production based resources and now all resources Option B is partially correct But this will just add more maintenance overhead.
Option C is incorrect because this can be used to log API activities but not give an account of all resou For more information on AWS Config, please visit the below URL: https://docs.aws.amazon.com/config/latest/developereuide/how-does-confie-work.html
The correct answer is: Use AWS Config to get the list of all resources Submit your Feedback/Queries to our Experts

NEW QUESTION 272
- (Exam Topic 2)
Your IT Security department has mandated that all data on EBS volumes created for underlying EC2 Instances need to be encrypted. Which of the following can help achieve this?
Please select:

A. AWS KMS API
B. AWS Certificate Manager
C. API Gateway with STS
D. IAM Access Key

Answer: A

Explanation:
The AWS Documentation mentions the following on AWS KMS
AWS Key Management Service (AWS KMS) is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data. AWS KMS is integrated with other AWS services including Amazon Elastic Block Store (Amazon EBS), Amazon Simple Storage Service (Amazon S3), Amazon Redshift Amazon Elastic Transcoder, Amazon WorkMail, Amazon Relational Database Service (Amazon RDS), and others to make it simple to encrypt your data with encryption keys that you manage
Option B is incorrect - The AWS Certificate manager can be used to generate SSL certificates that can be used to encrypt traffic transit, but not at rest
Option C is incorrect is again used for issuing tokens when using API gateway for traffic in transit. Option D is used for secure access to EC2 Instances
For more information on AWS KMS, please visit the following URL: https://docs.aws.amazon.com/kms/latest/developereuide/overview.htmll The correct answer is: AWS KMS API
Submit your Feedback/Queries to our Experts

NEW QUESTION 275
- (Exam Topic 2)
Your company has defined privileged users for their AWS Account. These users are administrators for key resources defined in the company. There is now a mandate to enhance the security authentication for these users. How can this be accomplished?
Please select:

A. Enable MFA for these user accounts
B. Enable versioning for these user accounts
C. Enable accidental deletion for these user accounts
D. Disable root access for the users

Answer: A

Explanation:
The AWS Documentation mentions the following as a best practices for IAM users. For extra security, enable multi-factor authentication (MFA) for privileged IAM users (users who are allowed access to sensitive resources or APIs). With MFA, users have a device that generates unique authentication code (a one-time password, or OTP). Users must provide both their normal credentials (like their user name and password) and the OTP. The MFA device can either be a special piece of hardware, or it can be a virtual device (for example, it can run in an app on a smartphone).
Option B,C and D are invalid because no such security options are available in AWS For more information on IAM best practices, please visit the below URL https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html The correct answer is: Enable MFA for these user accounts
Submit your Feedback/Queries to our Experts

NEW QUESTION 278
- (Exam Topic 2)
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: AD

Explanation:
https://aws.amazon.com/blogs/security/how-to-establish-federated-access-to-your-aws-resources-by-using-activ

NEW QUESTION 283
.....

Relate Links

100% Pass Your SCS-C01 Exam with Exambible Prep Materials

https://www.exambible.com/SCS-C01-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/