Answer Sheet

Q1)

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

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

- Use AWS Config to see what actions were taken by the user.
- Use the Amazon CloudWatch Logs console to filter CloudTrail data by user.
- ✓ Use the AWS CloudTrail console to search for user activity.
- Use Amazon Athena to query CloudTrail logs stored in Amazon S3.

Q2)

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

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

- Update the policy, keeping the vault lock in place.
- Copy the vault data to Amazon S3, delete the vault, and create a new vault with the data.
- ✓ Call the abort-vault-lock operation, fix the typo, and call the initiate-vault-lock again.
- Update the policy and call initiate-vault-lock again to apply the new policy.

Q3)

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

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

- AWS IAM access keys
- ✓ AWS IAM roles
- AWS IAM users
- AWS IAM groups

Q4)

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

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

- ✓ The secret key used by the Auditor is missing or incorrect.
- The Amazon EC2 role used by the Auditor must be set to the destination account role.
- ✓ The Auditor has not been granted sts:AssumeRole for the role in the destination account.
- The Auditor is using the incorrect password.
- The external ID used by the Auditor is missing or incorrect.
- ✓ The role ARN used by the Auditor is missing or incorrect.

Q5)

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

Which of the following solutions will meet these requirements?

- ✓ Route all traffic throughout a TCP listener on a Classic Load Balancer, and terminate the TLS connection on the EC2 instances.

Explanation:-
"If you use HTTPS or SSL for your front-end connections, you must deploy an X.509 certificate (SSL server certificate) on your load balancer. The load balancer decrypts requests from clients before sending them to the back-end instances (known as SSL termination). For more information, see SSL/TLS Certificates for Classic Load Balancers.

If you don't want the load balancer to handle the SSL termination (known as SSL offloading), you can use TCP for both the front-end and back-end connections, and deploy certificates on the registered instances handling requests."

SSL Server Certificates, section in the end of the page.

https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-listener-config.html

- Offload SSL termination onto an SSL listener on a Classic Load Balancer, and use a TCP connection between the load balancer and the EC2 instances.
- Create an HTTPS listener using an Application Load Balancer, and route all of the communication through that load balancer.
- Offload SSL termination onto an SSL listener using an Application Load Balancer, and re-spawn and SSL connection between the load balancer

and the EC2 instances.

Q6)

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

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

- Require all inbound and outbound network traffic to route through an AWS Direct Connect connection.
- Require all inbound network traffic to route through a bastion host in the private subnet.
- ✅ Configure AWS WAF to provide DDoS attack protection for the ALB.
- ✅ Move the web servers to private subnets without public IP addresses.
- Configure the application's EC2 instances to use NAT gateways for all inbound traffic.

Q7)

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?

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

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

- Configure IAM user policies to restrict root account capabilities for each Organizations member account.
- Disable the use of the root user account at the organizational root. Enable multi-factor authentication of the root user account for each organizational member account.

Explanation:-

The answer is not correct because organization root includes every user/group account in every account

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

Explanation:-

The option is incorrect as it will not modify user's access or permission

Q8)

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

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

- email-imap.us-east-1.amazonaws.com over port 993
- ✅ email-smtp.us-east-1.amazonaws.com over port 587
- email-pop3.us-east-1.amazonaws.com over port 995
- email.us-east-1.amazonaws.com over port 8080

Q9) A threat assessment has identified a risk whereby an internal employee could exfiltrate sensitive data from production host running inside AWS (Account 1). The threat was documented as follows:
Server X has outbound internet access configured via a proxy server. Legitimate access to S3 is required so that the application can upload encrypted files to an S3 bucket. Server X is currently using an IAM instance role. The proxy server is not able to inspect any of the server communication due to TLS encryption.
Which of the following options will mitigate the threat? (Choose two.)

- Remove the IAM instance role from the application server and save API access keys in a trusted and encrypted application config file.
- Modify the S3 bucket policy for the legitimate bucket to allow access only from the public IP addresses associated with the application server.
- Block outbound access to public S3 endpoints on the proxy server.
- ✅ Configure Network ACLs on Server X to deny access to S3 endpoints.
- ✅ Bypass the proxy and use an S3 VPC endpoint with a policy that whitelists only certain S3 buckets within Account 1.

Q10) A company will store sensitive documents in three Amazon S3 buckets based on a data classification scheme of "Sensitive," "Confidential," and "Restricted." The security solution must meet all of the following requirements:
• Each object must be encrypted using a unique key.
• Items that are stored in the "Restricted" bucket require two-factor authentication for decryption.
• AWS KMS must automatically rotate encryption keys annually.

Which of the following meets these requirements?

- Create a CMK with unique imported key material for each data classification type, and rotate them annually. For the "Restricted" key material, define the MFA policy in the key policy. Use S3 SSE-KMS to encrypt the objects.
- Create a CMK for each data classification type, and within the CMK policy, enable rotation of it annually, and define the MFA policy. S3 can then create DEK grants to uniquely encrypt each object within the S3 bucket.
- Create a CMK grant for each data classification type with EnableKeyRotation and MultiFactorAuthPresent set to true. S3 can then use the grants to encrypt each object with a unique CMK.
- ✅ Create a Customer Master Key (CMK) for each data classification type, and enable the rotation of it annually. For the "Restricted" CMK, define the MFA policy within the key policy. Use S3 SSE-KMS to encrypt the objects.

Q11)

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

The credentials must be stored so that the EC2 instances and the Lambda functions can access them. No other access is allowed.

The access logs must record when the credentials were accessed and by whom.

What should the Security Engineer do to meet these requirements?

- ✅ Store the database credentials in AWS Secrets Manager. Create an IAM role with access to Secrets Manager by using the EC2 and Lambda service principals in the role's trust policy. Add the role to an EC2 instance profile. Attach the instance profile to the EC2 instances. Set up Lambda to use the new role for execution.
- None of these
- Store the database credentials in AWS KMS. Create an IAM role with access to KMS by using the EC2 and Lambda service principals in the role's trust policy. Add the role to an EC2 instance profile. Attach the instance profile to the EC2 instances and the Lambda function.
- Store the database credentials in AWS Key Management Service (AWS KMS). Create an IAM role with access to AWS KMS by using the EC2 and Lambda service principals in the role's trust policy. Add the role to an EC2 instance profile. Attach the instance profile to the EC2 instances. Set up Lambda to use the new role for execution.

Q12)

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

What can be done to implement the above policy?

- Import new key material to the existing CMK and manually rotate the CMK.
- Use AWS Command Line interface to create an AWS Lambda function to rotate the existing CMK annually.
- Enable automatic key rotation annually for the CMK.
- ✅ Create a new CMK, import new key material to it, and point the key alias to the new CMK.

Q13)

A water utility company uses a number of Amazon EC2 instances to manage updates to a fleet of 2,000 Internet of Things (IoT) field devices that monitor water quality. These devices each have unique access credentials.

An operational safety policy requires that access to specific credentials is independently auditable.

What is the MOST cost-effective way to manage the storage of credentials?

- Use AWS Secrets Manager to store the credentials.
- Store the credentials in a JSON file on Amazon S3 with server-side encryption.
- Use AWS Key Management System to store a master key, which is used to encrypt the credentials. The encrypted credentials are stored in an Amazon RDS instance.
- ✅ Use AWS Systems Manager to store the credentials as Secure Strings Parameters. Secure by using an AWS KMS key.

Q14)

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

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

- Check that the trust relationship grants the service "cwlogs.amazonaws.com" permission to write objects to the Amazon S3 staging bucket.
- ✅ Check whether any application log entries were rejected because of invalid time stamps by reviewing /var/cwlogs/rejects.log.
- ✅ Verify that the permissions used by the agent allow creation of log groups/streams and to put log events.
- Use an EC2 run command to confirm that the "awslogs" service is running on all instances.
- Verify that the time zone on the application servers is in UTC.

Q15)

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?

- Use Amazon EC2 Systems Manager to deploy images, and review AWS CloudTrail logs for changes.
- Copy AWS CloudFormation templates to S3, and audit for changes from the template.
- Run the GenerateCredentialReport via the AWS CLI, and copy the output to Amazon S3 daily for auditing purposes.
- ✓ Use AWS Config to review the IAM policy assigned to users before and after the incident.

Q16)

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

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

- Launch an EC2-based firewall product from the AWS Marketplace, and implement the required rules in that product.
- Use a NAT gateway to control ingress and egress according to the requirements.
- Configure AWS WAF rules to implement the required rules.
- ✓ Use the operating system built-in, host-based firewall to implement the required rules.

Q17) 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:

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

- "Condition": { "Bool": { "kms:GrantIsForAWSResource": true } }
- ✓ "Condition": { "Bool": { "kms:ViaService": "ec2.us-west-2.amazonaws.com" } }
- kms:CreateGrant
- ✓ kms:GenerateDataKey
- kms:Decrypt

Q18) A Security Administrator has a website hosted in Amazon S3. The Administrator has been given the following requirements:
• Users may access the website by using an Amazon CloudFront distribution.
• Users may not access the website directly by using an Amazon S3 URL.
Which configurations will support these requirements? (Choose two.)

- Configure the S3 bucket policy so that it is accessible only through VPC endpoints, and place the CloudFront distribution into the specified VPC.
- Implement security groups so that the S3 bucket can be accessed only by using the intended CloudFront distribution.
- ✓ Modify the S3 bucket permissions so that only the origin access identity can access the bucket contents.
- ✓ Associate an origin access identity with the CloudFront distribution.
- Implement a "Principal": "cloudfront.amazonaws.com" condition in the S3 bucket policy.

Q19) A Security Engineer has created an Amazon CloudWatch event that invokes an AWS Lambda function daily. The Lambda function runs an Amazon Athena query that checks AWS CloudTrail logs in Amazon S3 to detect whether any IAM user accounts or credentials have been created in the past 30 days. The results of the Athena query are created in the same S3 bucket. The Engineer runs a test execution of the Lambda function via the AWS Console, and the function runs successfully. After several minutes, the Engineer finds that his Athena query has failed with the error message: "Insufficient Permissions". The IAM permissions of the Security Engineer and the Lambda function are shown below:
Security Engineer -
What is causing the error?

- The Lambda function does not have permissions to access the CloudTrail S3 bucket.
- The Athena service does not support invocation through Lambda.
- ✓ The Security Engineer does not have permissions to start the Athena query execution.
- The Lambda function does not have permissions to start the Athena query execution.

Q20)

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

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

- Configure the CloudWatch Logs agent on each EC2 instance within the VPC. Perform inspection from the log data within CloudWatch Logs.
- Configure Elastic Load Balancing (ELB) access logs. Perform inspection from the log data within the ELB access log files.
- Enable VPC Flow Logs for all subnets in the VPC. Perform inspection from the Flow Log data within Amazon CloudWatch Logs.
- ✓ Configure the host-based agent on each EC2 instance within the VPC. Perform inspection within the host-based agent.
- ✓ Configure a proxy solution on Amazon EC2 and route all outbound VPC traffic through it. Perform inspection within proxy software on the EC2 instance.

Q21)

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

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

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

- Call KMS.Encrypt() in the client, passing in the data file contents, and call KMS.Decrypt() server-side.
- Upload an SSL certificate to IAM, and configure Amazon CloudFront with the passphrase for the private key.
- Create a new VPC with an Amazon VPC VPN endpoint, and update the web service's DNS record.

Q22) 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?

- Change the CMK alias every 90 days, and update key-calling applications with the new key alias.
- Change the CMK permissions to ensure that individuals who can provision keys are not the same individuals who can use the keys.
- Generate a new Customer Master Key (CMK), re-encrypt all existing data with the new CMK, and use it for all future encryption operations.
- ✅ 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.

Q23)

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

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

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

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

"s3: *", "sts:*"
],
"Effect": "Deny",
"Resource": "*"
}
]
}
```

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

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

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

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

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

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

"NotAction": [
"dynamodb:*", "rds:*", "ec2:*",
"s3:*", "sts:*"
],
"Effect": "Deny",
"Resource": "*"
}
]
}

Q24)

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

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

What is the MOST likely cause of the authentication errors?

- The Secrets Manager IAM policy does not allow access to the RDS database.
- Enabling rotation in Secrets Manager causes the secret to rotate immediately and the applications are using the earlier credential.
- ✅ Migrating the credential to RDS requires that all access come through requests to the Secrets Manager.
- The Secrets Manager IAM policy does not allow access for the applications.

Q25)

A Security Engineer launches two Amazon EC2 instances in the same Amazon VPC but in separate Availability Zones. Each instance has a public IP address and is able to connect to external hosts on the internet.

The two instances are able to communicate with each other by using their private IP addresses, but they are not able to communicate with each other when using their public IP addresses.

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

- Add the public IP addresses to the ingress rules of the instance security groups.
- Add the instance IDs to the ingress rules of the instance security groups.
- Add 0.0.0.0/0 to the egress rules of the instance security groups.
- ✅ Associate the instances to the same security groups.

Q26)

The Security Engineer is managing a web application that processes highly sensitive personal information. The application runs on Amazon EC2.

The application has strict compliance requirements, which instruct that all incoming traffic to the application is protected from common web exploits and that all outgoing traffic from the EC2 instances is restricted to specific whitelisted URLs.

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

- ✅ Use AWS WAF to scan inbound traffic for web exploits. Use a third-party AWS Marketplace solution to restrict egress traffic to specific whitelisted URLs.
- Use AWS WAF to scan inbound traffic for web exploits. Use VPC Flow Logs and AWS Lambda to restrict egress traffic to specific whitelisted URLs.
- Use AWS Shield to scan inbound traffic for web exploits. Use a third-party AWS Marketplace solution to restrict egress traffic to specific whitelisted URLs.
- Use AWS Shield to scan inbound traffic for web exploits. Use VPC Flow Logs and AWS Lambda to restrict egress traffic to specific whitelisted URLs.

Q27) A company recently experienced a DDoS attack that prevented its web server from serving content. The website is static and hosts only HTML, CSS, and PDF files that users download. Based on the architecture shown in the image, what is the BEST way to protect the site against future attacks while minimizing the ongoing operational overhead?

- Move all the files to an Amazon S3 bucket. Create a CloudFront distribution in front of the bucket and terminate the web server.
- Launch an Application Load Balancer in front of the EC2 instance. Create an Amazon CloudFront distribution in front of the Application Load Balancer.
- Launch a second Amazon EC2 instance in a new subnet. Launch an Application Load Balancer in front of both instances.
- ✅ Move all the files to an Amazon S3 bucket. Have the web server serve the files from the S3 bucket.

Q28)

The Information Technology department has stopped using Classic Load Balancers and switched to Application Load Balancers to save costs.

After the switch, some users on older devices are no longer able to connect to the website.

What is causing this situation?

- The cipher suites on the Application Load Balancers are blocking connections.
- ✅ The intermediate certificate is installed within the Application Load Balancer.
- The Perfect Forward Secrecy settings are not configured correctly.
- Application Load Balancers do not support older web browsers.

Q29)

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

What is the SIMPLEST way to meet these requirements?

- None of these
- Enable AWS CloudTrail by creating a new trail and applying the trail to all regions. Specify a single Amazon S3 bucket as the storage location.
- ✅ Enable AWS CloudTrail by creating individual trails for each region, and specify a single Amazon S3 bucket to receive log files for later analysis.
- Enable AWS Trusted Advisor security checks in the AWS Console, and report all security incidents for all regions.

Q30)

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?

- Enable Amazon S3 event notifications to trigger an AWS Lambda function that sends an email alarm when there are new CloudTrail API entries.
- Configure Amazon Athena to read from the CloudTrail S3 bucket and query the logs to examine account activities.
- Configure Amazon Macie to classify and discover sensitive data in the Amazon S3 bucket that contains the CloudTrail audit logs.
- ✅ Implement a "write-only" CloudTrail event filter to detect any modifications to the AWS account resources.

Q31)

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?

- Enable Amazon Inspector on the S3 buckets that were impacted, then perform data classification. For identified objects that contain PII, query the S3 bucket logs by using Athena for GET operations.
- Enable Amazon GuardDuty and enable the PII rule set on the S3 buckets that were impacted, then perform data classification. Using the PII findings report from GuardDuty, query the S3 bucket logs by using Athena for GET operations.
- ✅ Enable Amazon Macie on the S3 buckets that were impacted, then perform data classification. For identified objects that contain PII, use the research function for auditing AWS CloudTrail logs and S3 bucket logs for GET operations.
- Using Amazon Athena, query the impacted S3 buckets by using the PII query identifier function. Then, create a new Amazon CloudWatch metric for Amazon S3 object access to alert when the objects are accessed.

Q32)

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

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

- Using Amazon CloudTrail, create a new CloudTrail event that detects the deactivation of CloudTrail logs, and a separate CloudTrail event that detects the creation of root API keys. Then use a Lambda function to enable CloudTrail and deactivate the root API keys.
- ✅ Using Amazon CloudWatch, create a CloudWatch event that detects AWS CloudTrail deactivation and a separate Amazon Trusted Advisor check to automatically detect the creation of root API keys. Then use a Lambda function to enable AWS CloudTrail and deactivate the root API keys.
- Using Amazon Inspector, review all of the API calls and configure the inspector agent to leverage SNS topics to notify security of the change to AWS CloudTrail, and revoke the new API keys for the root user.
- Using AWS Config, create a config rule that detects when AWS CloudTrail is disabled, as well as any calls to the root user create-api-key. Then use a Lambda function to re-enable CloudTrail logs and deactivate the root API keys.

Q33)

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

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

- Configure the target region's AWS service to communicate with the source region's AWS KMS so that it can decrypt the resource in the target region.
- ✅ Use AWS services that replicate data across regions, and re-wrap the data encryption key created in the source region by using the CMK in the target region so that the target region's CMK can decrypt the database encryption key.
- Configure AWS KMS to automatically synchronize the CMK between regions so that it can be used to decrypt the resource in the target region.
- Copy the application's AWS KMS CMK from the source region to the target region so that it can be used to decrypt the resource after it is copied to the target region.

Q34)

An organization policy states that all encryption keys must be automatically rotated every three years.

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

✅ AWS managed Customer Master Key (CMK)

Explanation:-AWS managed CMKs. You cannot manage key rotation for AWS managed CMKs. AWS KMS automatically rotates AWS managed CMKs every three years (1095 days). refer - https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html

- Customer managed CMK with AWS generated key material
- Customer managed CMK with imported key material
- AWS managed data key

Q35)

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.)

- Revoke all network ingress and egress except for to/from a forensics.
- Log in to each instance with administrative credentials to restart the instance.
- ✅ Capture a memory dump.
- ✅ Create EBS Snapshots of each of the volumes attached to the compromised instances.
- ✅ Use AWS Artifact to capture an exact image of the state of each instance.
- Run Auto Recovery for Amazon EC2.

Q36) A Security Administrator is configuring an Amazon S3 bucket and must meet the following security requirements:
• Encryption in transit
• Encryption at rest
• Logging of all object retrievals in AWS CloudTrail
Which of the following meet these security requirements? (Choose three.)

- ✅ Enable Amazon CloudWatch Logs for the AWS account.
- ✅ Set up default encryption for the S3 bucket.
- Enable a security group for the S3 bucket that allows port 443, but not port 80.
- ✅ Specify "aws:SecureTransport": "true" within a condition in the S3 bucket policy.
- Enable API logging of data events for all S3 objects.
- Enable S3 object versioning for the S3 bucket.

Q37) What is the function of the following AWS Key Management Service (KMS) key policy attached to a customer master key (CMK)?

- The key policy allows WorkMail or SES to encrypt or decrypt on behalf of the user for any CMK in the account.
- 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.
- The ExampleUser principal can transparently encrypt and decrypt email exchanges specifically between ExampleUser and AWS.
- ✅ The Amazon WorkMail and Amazon SES services have delegated KMS encrypt and delegated KMS encrypt and decrypt permissions to the ExampleUser principal in the 111122223333 account.

Q38) 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.
What does the statement allow?

- ✅ Only principals from account 111122223333 that have an IAM policy applied that grants access to this key to use the key.
- All principals from account 111122223333 to use the key but only on Amazon S3.
- Only the root user from account 111122223333 to use the key.
- All principals from all AWS accounts to use the key.

Q39)

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

What is the MOST efficient way to meet these requirements?

- Install the Amazon CloudWatch Logs Agent on the EC2 instances, and configure it to send the application logs to CloudWatch Logs.
- Create a simple cron job on the EC2 instances that synchronizes the application logs to an Amazon S3 bucket by using rsync.
- Enable AWS CloudTrail logging for the AWS account, create a new Amazon S3 bucket, and then configure Amazon CloudWatch Logs to receive the application logs from CloudTrail.
- ✅ Write an AWS Lambda function that logs into the EC2 instance to pull the application logs from the EC2 instance and persists them into an Amazon S3 bucket.

Q40)

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?

- Post the question on the AWS Discussion Forums.
- ✅ Use AWS Artifact to access AWS compliance reports.
- Read the AWS Customer Agreement.
- Run AWS Config and evaluate the configuration outputs.

Q41)

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

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

- ✅ The CMK specified in the application is not enabled.
- ✅ The CMK specified in the application is using the CMK KeyID instead of CMK Amazon Resource Name.
- The CMK specified in the application is currently is use.
- The CMK specified in the application does not exist.
- The CMK specified in the application is using an alias.

Q42)

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

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

- ✅ Add a statement to the IAM policy used by the application to allow cloudwatch:putMetricData.
- Modify the IAM role used by the application by adding the CloudWatchFullAccess managed policy.
- Add a statement to the IAM policy used by the application to allow logs:putLogEvents and logs:createLogStream
- Add a trust relationship to the IAM role used by the application for cloudwatch.amazonaws.com.

Q43)

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?

- Update the key pair in any AMI used to launch the EC2 instances, then restart the EC2 instances.
- ✅ Use the EC2 RunCommand to modify the authorized_keys file on any EC2 instance that is using the key.
- Use the modify-instance-attribute API to change the key on any EC2 instance that is using the key.
- Delete the key-pair key from the EC2 console, then create a new key pair.

Q44)

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

How can the Application team's requirements be met?

- Create an AWS Config rule for each network ACL and security group configuration, send the logs to Amazon S3, and use Amazon Athena to query the logs.
- Install an Amazon Inspector agent on each EC2 instance, send the logs to Amazon S3, and use Amazon EMR to query the logs.
- ✅ Turn on VPC Flow Logs, send the logs to Amazon S3, and use Amazon Athena to query the logs.

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

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

Q45)

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

Which design will meet the requirements with MINIMUM effort?

- Create a file watcher that copies data to Amazon Kinesis when the application writes to the log file. Have Kinesis trigger a Lambda function to update Amazon CloudWatch metrics with the log data. Set up CloudWatch alerts based on the metrics.
- Create a scheduled process to copy the application log files to AWS CloudTrail. Use S3 events to trigger Lambda functions that update CloudWatch metrics with the log data. Set up CloudWatch alerts based on the metrics.
- Install and configure the Amazon CloudWatch Logs agent on the application's EC2 instance. Create a CloudWatch metric filter to monitor the application logs. Set up CloudWatch alerts based on the metrics.
- ✅ Create a scheduled process to copy the component's logs into Amazon S3. Use S3 events to trigger a Lambda function that updates Amazon CloudWatch metrics with the log data. Set up CloudWatch alerts based on the metrics.

Q46)

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

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

- Amazon Cloud Directory
- AssumeRoleWithWebIdentity API
- ✅ Amazon Cognito
- Active Directory (AD) Connector

Q47)

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

Which of the following options should the Security Engineer use?

- Create an Amazon CloudWatch alarm to detect aged access keys and use an AWS Lambda function to disable the keys older than 90 days.
- Write a script that uses the GenerateCredentialReport, GetCredentialReport, and UpdateAccessKey APIs.
- Define an IAM policy that denies access if the key age is more than three months and apply to all users.
- ✅ In the AWS Console, choose the IAM service and select "Users". Review the "Access Key Age" column.

Q48)

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

How can the InfoSec team ensure compliance with this mandate?

- ✅ Deploy AWS Config rules and check all running instances for compliance.
- Patch all running instances by using AWS Systems Manager.
- Terminate all Amazon EC2 instances and relaunch them with approved AMIs.
- Define a metric filter in Amazon CloudWatch Logs to verify compliance.

Q49)

A pharmaceutical company has digitized versions of historical prescriptions stored on premises. The company would like to move these prescriptions to AWS and perform analytics on the data in them.

Any operation with this data requires that the data be encrypted in transit and at rest.

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

- Digitized files -> Amazon Kinesis Data Streams -> Kinesis Client Library consumer -> Amazon S3 -> Athena
- Digitized files -> Amazon Kinesis Data Firehose -> Amazon S3 -> Amazon Athena
- ✅ Digitized files -> Amazon Kinesis Data Analytics
- Digitized files -> Amazon Kinesis Data Firehose -> Amazon Elasticsearch

---

Q50) The Security Engineer created a new AWS Key Management Service (AWS KMS) key with the following key policy: What are the effects of the key policy? (Choose two.)

- The policy allows the KMS service-linked role in account 111122223333 to have full access to the KMS key.
- The policy allows the root user in account 111122223333 to have full access to the KMS key.
- ✅ The policy allows all IAM users in account 111122223333 to have full access to the KMS key.
- ✅ The policy allows access for the AWS account 111122223333 to manage key access though IAM policies.
- The policy allows all IAM roles in account 111122223333 to have full access to the KMS key.

Q51)

A company uses AWS Organization to manage 50 AWS accounts. The finance staff members log in as AWS IAM users in the FinanceDept AWS account.

The staff members need to read the consolidated billing information in the MasterPayer AWS account.

They should not be able to view any other resources in the MasterPayer AWS account. IAM access to billing has been enabled in the MasterPayer account.

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

- ✅ Create an AWS IAM role in the MasterPayer account with the ViewBilling permission, then grant the finance users in the FinanceDept account the permission to assume that role.
- Create an AWS IAM role in the FinanceDept account with the ViewBilling permission, then grant the finance users in the MasterPayer account the permission to assume that role.
- Create an IAM group for the finance users in the MasterPayer account, then attach the AWS managed ReadOnlyAccess IAM policy to the group.
- Create an IAM group for the finance users in the FinanceDept account, then attach the AWS managed ReadOnlyAccess IAM policy to the group.

Q52)

A Solutions Architect is designing a web application that uses Amazon CloudFront, an Elastic Load Balancing Application Load Balancer, and an Auto Scaling group of Amazon EC2 instances.

The load balancer and EC2 instances are in the US West (Oregon) region.

It has been decided that encryption in transit is necessary by using a customer-branded domain name from the client to CloudFront and from CloudFront to the load balancer.

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

- Two in the US West (Virginia) region and none in the US West (Oregon) region.
- One in the US West (Oregon) region and none in the US East (Virginia) region.
- Two in the US West (Oregon) region and none in the US East (Virginia) region.
- ✅ One in the US West (Oregon) region and one in the US East (Virginia) region.

Q53) A Security Engineer has been asked to troubleshoot inbound connectivity to a web server. This single web server is not receiving inbound connections from the internet, whereas all other web servers are functioning properly.
The architecture includes network ACLs, security groups, and a virtual security appliance. In addition, the Development team has implemented Application Load Balancers (ALBs) to distribute the load across all web servers. It is a requirement that traffic between the web servers and the internet flow through the virtual security appliance.
The Security Engineer has verified the following:
1. The rule set in the Security Groups is correct
2. The rule set in the network ACLs is correct
3. The rule set in the virtual appliance is correct
Which of the following are other valid items to troubleshoot in this scenario? (Choose two.)

- ✅ Verify the registered targets in the ALB.
- ⚪ Verify that the 0.0.0.0/0 route in the route table for the web server subnet points to the virtual security appliance.
- ✅ Verify which Security Group is applied to the particular web server's elastic network interface (ENI).
- ⚪ Verify that the 0.0.0.0/0 route in the route table for the web server subnet points to a NAT gateway.
- ⚪ Verify that the 0.0.0.0/0 route in the public subnet points to a NAT gateway.

Q54) Which approach will generate automated security alerts should too many unauthorized AWS API requests be identified?

- ⚪ Use the Amazon Personal Health Dashboard to monitor the account's use of AWS services, and raise an alert if service error rates increase.
- ✅ Run an Amazon Athena SQL query against CloudTrail log files. Use Amazon QuickSight to create an operational dashboard.
- ⚪ Configure AWS CloudTrail to stream event data to Amazon Kinesis. Configure an AWS Lambda function on the stream to alarm when the threshold has been exceeded.
- ⚪ Create an Amazon CloudWatch metric filter that looks for API call error codes and then implement an alarm based on that metric's rate.

Q55)

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

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

- ✅ Open the global CloudTrail configuration in the master account, and verify that the storage location is set to the correct S3 bucket.
- ✅ Confirm in the CloudTrail Console that each trail is active and healthy.
- ⚪ Create a new CloudTrail configuration in the account, and configure it to log to the account's S3 bucket.
- ✅ Verify that the S3 bucket policy allows access for CloudTrail from the production AWS account IDs.
- ⚪ Verify that the log file prefix is set to the name of the S3 bucket where the logs should go.
- ⚪ Confirm in the CloudTrail Console that the S3 bucket name is set correctly.

Q56)

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

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

- ⚪ Create a CloudWatch Logs metric to isolate a value that changes at least once during the period before logging stops.
- ⚪ Configure an Amazon Kinesis producer to first put the logs into Amazon Kinesis Streams.
- ✅ Verify that the OS Log rotation rules are compatible with the configuration requirements for agent streaming.
- ⚪ Ensure that file permissions for monitored files that allow the CloudWatch Logs agent to read the file have not been modified.
- ✅ Use AWS CloudFormation to dynamically create and maintain the configuration file for the CloudWatch Logs agent.

Q57)

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

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

- ⚪ Add a route to all route tables that black holes traffic to the Amazon DNS IP.
- ⚪ Add a rule to all network access control lists that deny access to the Amazon DNS IP.
- ⚪ Deny access to the Amazon DNS IP within all security groups.
- ✅ Disable DNS resolution within the VPC configuration.

Q58)

An employee accidentally exposed an AWS access key and secret access key during a public presentation.

The company Security Engineer immediately disabled the key.

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

- ⚪ Analyze the resource inventory in AWS Config for IAM user activity.
- ⚪ Download and analyze the IAM Use report from AWS Trusted Advisor.
- ⚪ Analyze Amazon CloudWatch Logs for activity.
- ✅ Analyze AWS CloudTrail for activity.
- ✅ Download and analyze a credential report from IAM.

Q59) Which of the following minimizes the potential attack surface for applications?

- Design network security in a single layer within the perimeter network (also known as DMZ, demilitarized zone, and screened subnet) to facilitate quicker responses to threats.
- Use AWS Direct Connect for secure trusted connections between EC2 instances within private subnets.
- Use security groups to provide stateful firewalls for Amazon EC2 instances at the hypervisor level.
- ✓ Use network ACLs to provide stateful firewalls at the VPC level to prevent access to any specific AWS resource.