Answer Sheet

Q1)

You are responsible to deploying a critical application onto AWS. Part of the requirements for this application is to ensure that the controls set for this application met PCI compliance.

Also there is a need to monitor web application logs to identify any malicious activity.

Which of the following services can be used to fulfill this requirement. Choose 2 answers from the options given below

- Amazon AWS Config
- Amazon VPC Flow Logs
- ✅ Amazon Cloudwatch Logs
- ✅ Amazon Cloudtrail

Q2)

A company wishes to enable Single Sign On (SSO) so its employees can login to the management console using their corporate directory identity.

Which steps below are required as part of the process? Select 2 answers from the options given below.

- ✅ Create an IAM role that establishes a trust relationship between IAM and the corporate directory identity provider (IdP)
- Create a Lambda function to assign IAM roles to the temporary security tokens provided to the users.
- Create IAM policies that can be mapped to group memberships in the corporate directory.
- ✅ Create a Direct Connect connection between the corporate network and the AWS region with the company's infrastructure.

Q3)

A company continually generates sensitive records that it stores in an S3 bucket. All objects in the bucket are encrypted using SSE-KMS using one of the company's CMKs.

Company compliance policies require that no more than one month of data be encrypted using the same encryption key.

What solution below will meet the company's requirements?

- Trigger a Lambda function with a monthly CloudWatch event that rotates the key material in the CMK.
- Configure the CMK to rotate the key material every month.
- Trigger a Lambda function with a monthly CloudWatch event that creates a new CMK, updates the S3 bucket to use the new CMK, and deletes the old CMK. (Incorrect)
- ✅ Trigger a Lambda function with a monthly CloudWatch event that creates a new CMK and updates the S3 bucket to use the new CMK.

Q4)

Company policy requires that all insecure server protocols, such as FTP, Telnet, HTTP, etc be disabled on all servers.

The security team would like to regularly check all servers to ensure compliance with this requirement by using a scheduled CloudWatch event to trigger a review of the current infrastructure.

What process will check compliance of the company's EC2 instances?

- Run an Amazon Inspector assessment using the Runtime Behavior Analysis rules package against every EC2 instance.
- Enable a GuardDuty threat detection analysis targeting the port configuration on every EC2 instance. (Incorrect)
- Query the Trusted Advisor API for all best practice security checks and check for "action recommened" status.
- ✅ Trigger an AWS Config Rules evaluation of the restricted-common-ports rule against every EC2 instance.

Q5)

A web application runs in a VPC on EC2 instances behind an ELB Application Load Balancer. The application stores data in an RDS MySQL DB instance.

A Linux bastion host is used to apply schema updates to the database – administrators connect to the host via SSH from a corporate workstation.

The following security groups are applied to the infrastructure-

- ✅ sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from sgLB sgDB :allow port 3306 traffic from sgWeb and sgBastion sgBastion: allow port 22 traffic from the corporate IP address range
- sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from sgLB sgDB :allow port 3306 traffic from sgWeb and sgBastion sgBastion: allow port 22 traffic from the VPC IP address range
- sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from sgLB sgDB :allow port 3306 traffic from sgWeb and sgLB sgBastion: allow port 22 traffic from the VPC IP address range
- sgLB :allow port 80 and 443 traffic from 0.0.0.0/0 sgWeb :allow port 80 and 443 traffic from 0.0.0.0/0 sgDB :allow port 3306 traffic from sgWeb and sgBastion sgBastion: allow port 22 traffic from the corporate IP address range (Incorrect)

Q6)

A company had developed an incident response plan 18 months ago. Regular implementations of the response plan are carried out.

No changes have been made to the response plan have been made since its creation.

Which of the following is a right statement with regards to the plan?

- [x] The response plan does not cater to new services
- [ ] The response plan is not implemented on a regular basis
- [ ] It places too much emphasis on already implemented security controls.
- [ ] The response plan is complete in its entirety (Incorrect)

Q7)

Your application currently uses customer keys which are generated via AWS KMS in the US east region.

You now want to use the same set of keys from the EU-Central region. How can this be accomplished?

- [ ] Use the backing key from the US east region and use it in the EU-Central region
- [ ] Use key rotation and rotate the existing keys to the EU-Central region
- [ ] Export the key from the US east region and import them into the EU-Central region
- [x] This is not possible since keys from KMS are region specific

---

Q8)

You have a requirement to conduct penetration testing on the AWS Cloud for a couple of EC2 Instances.

How could you go about doing this? Choose 2 right answers from the options given below.

- [ ] Work with an AWS partner and no need for prior approval request from AWS
- [x] Use a pre-approved penetration testing tool.
- [x] Get prior approval from AWS for conducting the test
- [ ] Choose the right AMI for the underlying instance type (Incorrect)

Q9)

You currently have an S3 bucket hosted in an AWS Account. It holds information that needs be accessed by a partner account.

Which is the MOST secure way to allow the partner account to access the S3 bucket in your account

- [x] Ensure the partner uses an external id when making the request
- [ ] Ensure an IAM user is created which can be assumed by the partner account.
- [x] Ensure an IAM role is created which can be assumed by the partner account.
- [x] Provide the ARN for the role to the partner account

Q10)

Your company has created a set of keys using the AWS KMS service. They need to ensure that each key is only used for certain services.

For example , they want one key to be used only for the S3 service. How can this be achieved?

- [ ] Define an IAM user , allocate the key and then assign the permissions to the required service
- [x] Use the kms:ViaService condition in the Key policy
- [ ] Create a bucket policy that allows the key to be accessed by only the S3 service.
- [ ] Create an IAM policy that allows the key to be accessed by only the S3 service.

Q11)

You have a set of Customer keys created using the AWS KMS service. These keys have been used for around 6 months.

You are now trying to use the new KMS features for the existing set of key's but are not able to do so. What could be the reason for this.

- [ ] You have not given access via the IAM roles
- [ ] You have not explicitly given access via the IAM policy
- [x] You have not explicitly given access via the key policy
- [ ] You have not explicitly given access via IAM users

Q12)

You are planning on hosting a web application on AWS. You create an EC2 Instance in a public subnet. This instance needs to connect to an EC2 Instance that will host an Oracle database.

Which of the following steps should be followed to ensure a secure setup is in place?

- [x] Create a database security group and ensure the web security group to allowed incoming access
- [x] Place the EC2 Instance with the Oracle database in a separate private subnet
- [ ] Place the EC2 Instance with the Oracle database in the same public subnet as the Web server for faster communication.
- [ ] Ensure the database security group allows incoming traffic from 0.0.0.0/0

Q13)

An EC2 Instance hosts a Java based application that access a DynamoDB table. This EC2 Instance is currently serving

production based users.

Which of the following is a secure way of ensuring that the EC2 Instance access the DynamoDB table

- Use IAM Access Groups with the right permissions to interact with DynamoDB and assign it to the EC2 Instance
- Use IAM Access Keys with the right permissions to interact with DynamoDB and assign it to the EC2 Instance
- Use KMS keys with the right permissions to interact with DynamoDB and assign it to the EC2 Instance
- ✓ Use IAM Roles with permissions to interact with DynamoDB and assign it to the EC2 Instance

---

Q14)

An application running on EC2 instances processes sensitive information stored on Amazon S3. The information is accessed over the Internet.

The security team is concerned that the Internet connectivity to Amazon S3 is a security risk. Which solution will resolve the security concern?

- Access the data through a NAT Gateway.
- Access the data through a VPN connection.
- Access the data through an Internet Gateway.
- ✓ Access the data through a VPC endpoint for Amazon S3

Q15)

Development teams in your organization use S3 buckets to store the log files for various application hosted in development environments in AWS.

The developers want to keep the logs for one month for troubleshooting purposes, and then purge the logs.

What feature will enable this requirement?

- Creating an IAM policy for the S3 bucket.
- ✓ Configuring lifecycle configuration rules on the S3 bucket.
- Adding a bucket policy on the S3 bucket.
- Enabling CORS on the S3 bucket.

Q16)

A company is using a Redshift cluster to store their data warehouse. There is a requirement from the Internal IT Security team to ensure that data gets encrypted for the Redshift database.

How can this be achieved?

- Use SSL/TLS for encrypting the data
- ✓ Use AWS KMS Customer Default master key
- Encrypt the EBS volumes of the underlying EC2 Instances
- Use S3 Encryption

Q17)

A company is deploying a new web application on AWS. Based on their other web applications, they anticipate being the target of frequent DDoS attacks.

Which steps can the company use to protect their application? Select 2 answers from the options given below.

- ✓ Use CloudFront and AWS WAF to prevent malicious traffic from reaching the application
- Use Amazon Inspector on the EC2 instances to examine incoming traffic and discard malicious traffic.
- ✓ Use an ELB Application Load Balancer and Auto Scaling group to scale to absorb application layer traffic.
- Associate the EC2 instances with a security group that blocks traffic from blacklisted IP addresses.

Q18)

A company has resources hosted in their AWS Account. There is a requirement to monitor all API activity for all regions. The audit needs to be applied for future regions as well.

Which of the following can be used to fulfill this requirement.

- Create a Cloudtrail for each region. Use Cloudformation to enable the trail for all future regions.
- ✓ Ensure one Cloudtrail trail is enabled for all regions.
- Ensure Cloudtrail for each region. Then enable for each future region.
- Create a Cloudtrail for each region. Use AWS Config to enable the trail for all future regions.

Q19)

A customer has an instance hosted in the AWS Public Cloud. The VPC and subnet used to host the Instance have been created with the default settings for the Network Access Control Lists. They need to provide an IT Administrator secure access to the underlying instance.

How can this be accomplished.

- Ensure that the security group allows Outbound SSH traffic from the IT Administrator's Workstation

- [x] Ensure that the security group allows Inbound SSH traffic from the IT Administrator's Workstation
- [ ] Ensure the Network Access Control Lists allow Outbound SSH traffic from the IT Administrator's Workstation
- [ ] Ensure the Network Access Control Lists allow Inbound SSH traffic from the IT Administrator's Workstation

---

Q20)

A company is planning to run a number of Admin related scripts using the AWS Lambda service. There is a need to understand if there are any errors encountered when the script run.

How can this be accomplished in the most effective manner.

- [ ] Use the AWS Config service to monitor for errors
- [ ] Use Cloudtrail to monitor for errors
- [x] Use Cloudwatch metrics and logs to watch for errors
- [ ] Use the AWS Inspector service to monitor for errors

Q21)

A company hosts data in S3. There is now a mandate that going forward all data in the S3 bucket needs to encrypt at rest.

How can this be achieved?

- [x] Enable server side encryption on the S3 bucket
- [ ] Use SSL certificates to encrypt the data
- [ ] Use AWS Access keys to encrypt the data
- [ ] Enable MFA on the S3 bucket

Q22)

You are responsible to deploying a critical application onto AWS. Part of the requirements for this application is to ensure that the controls set for this application met PCI compliance. Also there is a need to monitor web application logs to identify any malicious activity.

Which of the following services can be used to fulfil this requirement. Choose 2 answers from the options given below

- [ ] Amazon AWS Config
- [ ] Amazon VPC Flow Logs
- [x] Amazon Cloudwatch Logs
- [x] Amazon Cloudtrail

Q23)

You need to have a cloud security device which would allow to generate encryption keys based on FIPS 140-2 Level 3.

Which of the following can be used for this purpose?

- [x] AWS Cloud HSM
- [ ] AWS managed keys
- [ ] AWS Customer Keys
- [ ] AWS KMS

Q24)

Your company currently has a set of EC2 Instances hosted in a VPC. The IT Security department is suspecting a possible DDos attack on the instances.

What can you do to zero in on the IP addresses which are receiving a flurry of requests.

- [ ] Use AWS Trusted Advisor to get the IP addresses accessing the EC2 Instances
- [ ] Use AWS Config to get the IP addresses accessing the EC2 Instances
- [ ] Use AWS Cloud trail to get the IP addresses accessing the EC2 Instances
- [x] Use VPC Flow logs to get the IP addresses accessing the EC2 Instances

---

Q25)

A company has an existing AWS account and a set of critical resources hosted in that account. The employee who was in-charge of the root account has left the company.

What must be now done to secure the account. Choose 3 answers from the options given below.

- [x] Change the password for the root account
- [x] Confirm MFA to a secure device
- [x] Delete the access keys for the root account
- [ ] Change the password for all IAM users

Q26)

You have a set of application , database and web servers hosted in AWS. The web servers are placed behind an ELB. There are separate security groups for the application, database and web servers. The network security groups have been defined accordingly.

There is an issue with the communication between the application and database servers. In order to troubleshoot the issue between just the application and database server, what is the ideal set of MINIMAL steps you would take

- Check the Outbound security rules for the database security group Check the both the Inbound and Outbound security rules for the application security group
- Check the both the Inbound and Outbound security rules for the database security group Check the Inbound security rules for the application security group
- Check the Outbound security rules for the database security group Check the Inbound security rules for the application security group
- ✓ Check the Inbound security rules for the database security group Check the Outbound security rules for the application security group

---

Q27)

A company is planning on extending their on-premise AWS Infrastructure to the AWS Cloud. They need to have a solution that would give core benefits of traffic encryption and ensure latency is kept to a minimum.

Which of the following would help fulfil this requirement? Choose 2 answers from the options given below

- AWS NAT gateways
- AWS VPC Peering
- ✓ AWS VPN
- ✓ AWS Direct Connect

Q28)

How can you ensure that instance in an VPC does not use AWS DNS for routing DNS requests. You want to use your own managed DNS instance.

How can this be achieved?

- Change the route table for the VPC
- ✓ Create a new DHCP options set and replace the existing one.
- Change the existing DHCP options set
- Change the subnet configuration to allow DNS requests from the new DNS Server

---

Q29)

A windows machine in one VPC needs to join the AD domain in another VPC. VPC Peering has been established. But the domain join is not working.

What is the other step that needs to be followed to ensure that the AD domain join can work as intended?

- ✓ Ensure the security groups for the AD hosted subnet has the right rule for relevant subnets
- Change the VPC peering connection to a Direct Connect connection
- Change the VPC peering connection to a VPN connection
- Ensure that the AD is placed in a public subnet

Q30)

You need to have a requirement o store objects in an S3 bucket with a key that is automatically managed and rotated.

Which of the following can be used for this purpose?

- AWS Customer Keys
- ✓ AWS S3 Server side encryption
- AWS KMS
- AWS Cloud HSM

Q31)

A company stores critical data in an S3 bucket. There is a requirement to ensure that an extra level of security is added to the S3 bucket.

In addition , it should be ensured that objects are available in a secondary region if the primary one goes down.

Which of the following can help fulfill these requirements? Choose 2 answers from the options given below

- Enable the Bucket ACL and add a condition for { "Null": { "aws:MultiFactorAuthAge": true }}
- ✓ For the Bucket policy add a condition for { "Null": { "aws:MultiFactorAuthAge": true }}
- ✓ Enable bucket versioning and also enable CRR
- Enable bucket versioning and enable Master Pays

Q32)

Your company manages thousands of EC2 Instances. There is a mandate to ensure that all servers don't have any critical security flaws.

Which of the following can be done to ensure this? Choose 2 answers from the options given below.

- Use AWS Inspector to patch the servers
- ✓ Use AWS Inspector to ensure that the servers have no critical flaws.

- Use AWS Config to ensure that the servers have no critical flaws.
- ✓ Use AWS SSM to patch the servers

Q33)

You need to inspect the running processes on an EC2 Instance that may have a security issue. How can you achieve this in the easiest way possible.

Also you need to ensure that the process does not interfere with the continuous running of the instance.

- ✓ Use the SSM Run command to send the list of running processes information to an S3 bucket.
- Use AWS Cloudwatch to record the processes running on the server
- Use AWS Cloudtrail to record the processes running on the server to an S3 bucket.
- Use AWS Config to see the changed process information on the server

---

Q34)

You are trying to use the Systems Manager to patch a set of EC2 systems. Some of the systems are not getting covered in the patching process.

Which of the following can be used to troubleshoot the issue? Choose 3 answers from the options given below.

- ✓ Ensure that agent is running on the Instances.
- Check to see if the IAM user has the right permissions for EC2
- ✓ Check to see if the right role has been assigned to the EC2 Instances
- ✓ Check the Instance status by using the Health API.

Q35)

A company has a large set of keys defined in AWS KMS. Their developers frequently use the keys for the applications being developed.

What is one of the ways that can be used to reduce the cost of accessing the keys in the AWS KMS service.

- Create an alias of the key
- ✓ Use Data key caching
- Enable rotation of the keys
- Use the right key policy

Q36)

You are trying to use the AWS Systems Manager run command on a set of Instances. The run command is not working on a set of Instances.

What can you do to diagnose the issue? Choose 2 answers from the options given below

- Ensure the security groups allow outbound communication for the Instance
- Ensure the right AMI is used for the Instance
- ✓ Check the /var/log/amazon/ssm/errors.log file
- ✓ Ensure that the SSM agent is running on the target machine

---

Q37)

You are working for a company and been allocated the task for ensuring that there is a federated authentication mechanism setup between AWS and their On-premise Active Directory.

Which of the following are important steps that need to be covered in this process? Choose 2 answers from the options given below.

- ✓ Configure AWS as the relying party in Active Directory Federation services
- Configure AWS as the relying party in Active Directory
- Ensure the right match is in place for On-premise AD Groups and IAM Groups.
- ✓ Ensure the right match is in place for On-premise AD Groups and IAM Roles.

Q38) Which technique can be used to integrate AWS IAM (Identity and Access Management) with an on-premise LDAP (Lightweight Directory Access Protocol) directory service?

- Use IAM roles to automatically rotate the IAM credentials when LDAP credentials are updated.
- Use AWS Security Token Service from an identity broker to issue short-lived AWS credentials.
- ✓ Use SAML (Security Assertion Markup Language) to enable single sign-on between AWS and LDAP.
- Use an IAM policy that references the LDAP account identifiers and the AWS credentials.

Q39)

You have an EBS volume attached to an EC2 Instance which uses KMS for Encryption. Someone has now gone ahead and deleted the Customer Key which was used for the EBS encryption.

What should be done to ensure the data can be decrypted?

- Request AWS Support to recover the key
- ✓ Copy the data from the EBS volume before detaching it from the Instance
- Create a new Customer Key using KMS and attach it to the existing volume
- Use AWS Config to recover the key

Q40)

You work as an administrator for a company. The company hosts a number of resources using AWS. There is an incident of a suspicious API activity which occurred 11 days ago.

The Security Admin has asked to get the API activity from that point in time. How can this be achieved?

- Search the Cloud Watch metrics to find for the suspicious activity which occurred 11 days ago
- ✓ Search the Cloudtrail event history on the API events which occurred 11 days ago.
- Search the Cloud Watch logs to find for the suspicious activity which occurred 11 days ago
- Use AWS Config to get the API calls which were made 11 days ago.

Q41)

You need to ensure that the cloudtrail logs which are being delivered in your AWS account is encrypted.

How can this be achieved in the easiest way possible?

- Enable S3-KMS for the underlying bucket which receives the log files
- Enable S3-SSE for the underlying bucket which receives the log files
- ✓ Don't do anything since Cloud trail logs are automatically encrypted.
- Enable KMS encryption for the logs which are sent to Cloudwatch

---

Q42)

You have a requirement to serve up private content using the keys available with Cloudfront.

How can this be achieved?

- ✓ Create pre-signed URL's
- Add the keys to the S3 bucket
- Add the keys to the backend distribution.
- Use AWS Access keys

Q43) You are building a system to distribute confidential training videos to employees. Using CloudFront, what method could be used to serve content that is stored in S3, but not publicly accessible from S3 directly?

- Create a S3 bucket policy that lists the CloudFront distribution ID as the Principal and the target bucket as the Amazon Resource Name (ARN).
- Create an Identity and Access Management (IAM) User for CloudFront and grant access to the objects in your S3 bucket to that IAM User.
- Add the CloudFront account security group "amazon-cf/amazon-cf-sg?? to the appropriate S3 bucket policy.
- ✓ Create an Origin Access Identity (OAI) for CloudFront and grant access to the objects in your S3 bucket to that OAI.

Q44)

Your company has a requirement to work with a DynamoDB table. There is a security mandate that all data should be encrypted at rest.

What is the easiest way to accomplish this for DynamoDB.

- Encrypt the table using AWS KMS after it is created
- ✓ Encrypt the table using AWS KMS before it is created
- Use the AWS SDK to encrypt the data before sending it to the DynamoDB table
- Use S3 buckets to encrypt the data before sending it to DynamoDB

Q45)

Your company hosts critical data in an S3 bucket. There is a requirement to ensure that all data is encrypted. There is also metadata about the information stored in the bucket that needs to be encrypted as well.

Which of the below measures would you take to ensure this requirement is fulfilled?

- ✓ Put the metadata in a DynamoDB table and ensure the table is encrypted during creation time.
- Put the metadata as metadata for each object in the S3 bucket and then enable S3 Server KMS encryption.
- Put the metadata as metadata for each object in the S3 bucket and then enable S3 Server side encryption.
- Put the metadata in the S3 bucket itself.

Q46)

One of the EC2 Instances in your company has been compromised. What steps would you take to ensure that you could apply digital forensics on the Instance.

Select 2 answers from the options given below

- ✓ Ensure that the security groups only allow communication to this forensic instance

- ✓ Create a separate forensic instance
- Remove the role applied to the Ec2 Instance
- Terminate the instance

Q47)

One of your company's EC2 Instances have been compromised. The company has strict policies and needs a thorough investigation on to finding the culprit for the security breach.

What would you do in this case. Choose 3 answers from the options given below.

- ✓ Ensure logging and audit is enabled for all services
- ✓ Isolate the machine from the network
- ✓ Take a snapshot of the EBS volume
- Ensure all passwords for all IAM users are changed

Q48)

Your company has a set of EC2 Instances that are placed behind an ELB. Some of the applications hosted on these instances communicate via a legacy protocol. There is a security mandate that all traffic between the client and the EC2 Instances need to be secure.

How would you accomplish this?

- ✓ Use a Classic Load balancer and terminate the SSL connection at the EC2 Instances
- Use an Application Load balancer and terminate the SSL connection at the EC2 Instances
- Use a Classic Load balancer and terminate the SSL connection at the ELB
- Use an Application Load balancer and terminate the SSL connection at the ELB

Q49)

A company has hired a third-party security auditor, and the auditor needs read-only access to all AWS resources and logs of all VPC records and events that have occurred on AWS.

How can the company meet the auditor's requirements without comprising security in the AWS environment? Choose the correct answer from the options below

- The company should contact AWS as part of the shared responsibility model, and AWS will grant required access to the third-party auditor.
- Create a role that has the required permissions for the auditor.
- Create an SNS notification that sends the CloudTrail log files to the auditor's email when CloudTrail delivers the logs to S3, but do not allow the auditor access to the AWS environment.
- ✓ Enable CloudTrail logging and create an IAM user who has read-only permissions to the required AWS resources, including the bucket containing the CloudTrail logs.

Q50)

Your company has a set of EC2 Instances defined in AWS. They need to ensure that all traffic packets are monitored and inspected for any security threats.

How can this be achieved? Choose 2 answers from the options given below

- ✓ Use a third party firewall installed on a central EC2 Instance
- ✓ Use a host based intrusion detection system
- Use Network Access control lists logging
- Use VPC Flow logs
