Answer Sheet

Q1) A financial institution has the following security requirements:
• Cloud-based users must be contained in a separate authentication domain.
• Cloud-based users cannot access on-premises systems.
As part of standing up a cloud environment, the financial institution is creating a number of Amazon managed databases and Amazon EC2 instances. An Active Directory service exists on-premises that has all the administrator accounts, and these must be able to access the databases and instances.
How would the organization manage its resources in the MOST secure manner? (Choose two.)

- Establish a two-way trust between the new and existing Active Directory services.
- Establish a one-way trust relationship from the new Active Directory to the existing Active Directory service.
- ✓ Establish a one-way trust relationship from the existing Active Directory to the new Active Directory service.
- ✓ Configure an additional on-premises Active Directory service to manage the cloud resources.
- Configure an AWS Managed Microsoft AD to manage the cloud resources.

Q2)

An organization wants to be alerted when an unauthorized Amazon EC2 instance in its VPC performs a network port scan against other instances in the VPC.

When the Security team performs its own internal tests in a separate account by using pre-approved third-party scanners from the AWS Marketplace, the Security team also then receives multiple Amazon GuardDuty events from Amazon CloudWatch alerting on its test activities.

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

- Grant the Security team's EC2 instances a role with permissions to call Amazon GuardDuty API operations.
- ✓ Install the Amazon Inspector agent on the EC2 instances that the Security team uses.
- Add the Elastic IP addresses of the Security team's EC2 instances to a trusted IP list in Amazon GuardDuty.
- Use a filter in AWS CloudTrail to exclude the IP addresses of the Security team's EC2 instances.

Q3)

An organization is moving non-business-critical applications to AWS while maintaining a mission-critical application in an on-premises data center.

An on-premises application must share limited confidential information with the applications in AWS.

The internet performance is unpredictable.

Which configuration will ensure continued connectivity between sites MOST securely?

- VPN Gateway over AWS Direct Connect
- AWS Snowball Edge
- ✓ VPN and a cached storage gateway
- AWS Direct Connect

Q4)

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.)

- Attach the AmazonSQSFullAccess managed policy to the role used by the instances.
- ✓ Verify that the access key attached to the role used by the instances is active.
- Verify that the SQS resource policy does not explicitly deny access to the role used by the instances.
- Configure and assign an MFA device to the role used by the instances.
- ✓ Verify that the role attached to the instances contains policies that allow access to the queue.

Q5)

A company has a forensic logging use case whereby several hundred applications running on Docker on EC2 need to send logs to a central location.

The Security Engineer must create a logging solution that is able to perform real-time analytics on the log files, grants the ability to replay events, and persists data.

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

- Amazon SQS
- ✓ Amazon Kinesis
- Amazon Elasticsearch
- ✓ Amazon CloudWatch
- Amazon Athena

Q6) Which of the following is the most efficient way to automate the encryption of AWS CloudTrail logs using a Customer Master Key (CMK) in AWS KMS?

- Use encrypted API endpoints so that all AWS API calls generate encrypted CloudTrail log entries using the TLS certificate from the encrypted API call.
- ✓ Configure CloudTrail to use server-side encryption using KMS-managed keys to encrypt and decrypt CloudTrail logs.
- Use the KMS direct encrypt function on the log data every time a CloudTrail log is generated.
- Use the default Amazon S3 server-side encryption with S3-managed keys to encrypt and decrypt the CloudTrail logs.

Q7)

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?

- ✓ In CloudWatch, verify that the alarm threshold "consecutive periods" value is equal to, or greater than 1.
- In SNS, ensure that the subscription used by these alerts has not been deleted.
- In Amazon SNS, determine whether the "Account spend limit" has been reached for this alert.
- In CloudTrail, verify that the trail logging bucket has a log prefix configured.

Q8) 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?

- Construct an AWS WAF rule to replace existing HTTP headers with the required security headers by using regular expressions.
- Migrate the legacy application to an Amazon S3 static website and front it with an Amazon CloudFront distribution.
- ✓ Implement an AWS Lambda@Edge origin response function that inserts the required headers.
- Configure an Amazon Route 53 routing policy to send all web traffic that does not include the required headers to a black hole.

Q9)

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

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

- Verify that the network access control lists and security groups of the EC2 instances have the access to send logs over SNMP.
- Connect to the EC2 instances that are not sending logs. Use the command prompt to verify that the right permission have been set for the Amazon SNS topic.
- Verify that the EC2 instances have a route to the public AWS API endpoints.
- ✓ Log in to the AWS account and select CloudWatch Logs. Check for any monitored EC2 instances that are in the "Alerting" state and restart them using the EC2 console.
- ✓ Connect to the EC2 instances that are not sending the appropriate logs and verify that the CloudWatch Logs agent is running.

Q10)

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

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

- Use AWS Config rules to detect 0.0.0.0/0 and invoke an AWS Lambda function to update the security group with the organization's firewall IP.
- Use a host-based firewall to prevent access from all but the organization's firewall IP.
- Delete the internet gateway associated with the VPC.
- ✓ Use network access control lists to block source IP addresses matching 0.0.0.0/0.

Q11)

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?

- Create IAM roles for CloudFront, and change the S3 bucket/object permission so that only the IAM role has access.
- ✓ Set up a CloudFront origin access identity (OAI), and change the S3 bucket/object permission so that only the OAI has access.
- Change the S3 bucket/object permission so that only the bucket owner has access.
- Redirect S3 bucket access to the corresponding CloudFront distribution.

Q12)

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).

- [x] Configure AWS as a trusted relying party for the Active Directory
- [ ] Create a SAML provider with Amazon Cloud Directory.
- [x] Create a SAML provider with IAM.
- [ ] Create IAM groups with permissions corresponding to each Active Directory group.
- [x] Create IAM roles with permissions corresponding to each Active Directory group.
- [ ] Configure IAM as a trusted relying party for Amazon Cloud Directory.

Q13)

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?

- [ ] Verify that the Analyst's account is mapped to an IAM policy that includes permissions for cloudwatch: GetMetricStatistics and Cloudwatch: ListMetrics.
- [x] Check the CloudWatch dashboards to ensure that there is a metric configured with an appropriate dimension for security group changes.
- [ ] Ensure that CloudTrail and S3 bucket access logging is enabled for the Analyst's AWS account. B. Verify that a metric filter was created and then mapped to an alarm. Check the alarm notification action.

Q14)

Example.com hosts its internal document repository on Amazon EC2 instances. The application runs on EC2 instances and previously stored the documents on encrypted Amazon EBS volumes. To optimize the application for scale, example.com has moved the files to Amazon S3.

The security team has mandated that all the files are securely deleted from the EBS volume, and it must certify that the data is unreadable before releasing the underlying disks.

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

- [x] Delete the data by using the operating system delete commands. Run Quick Format on the drive and then release the EBS volumes back to AWS.
- [ ] Delete the encryption key used to encrypt the EBS volume. Then, release the EBS volumes back to AWS.
- [ ] Release the volumes back to AWS. AWS immediately wipes the disk after it is deprovisioned.
- [ ] Change the volume encryption on the EBS volume to use a different encryption mechanism. Then, release the EBS volumes back to AWS.

Q15) A Systems Administrator has written the following Amazon S3 bucket policy designed to allow access to an S3 bucket for only an authorized AWS IAM user from the IP address range 10.10.10.0/24:
When trying to download an object from the S3 bucket from 10.10.10.40, the IAM user receives an access denied message.
What does the Administrator need to change to grant access to the user?

- [ ] Change the "Action" from ["s3:*"] to ["s3:GetObject", "s3:ListBucket"]
- [ ] Change the "Version" from "2012-10-17" to the last revised date of the policy
- [ ] Change the "Principal" from "*" to {AWS:"arn:aws:iam: : account-number: user/username"}
- [x] Change the "Resource" from "arn: aws:s3:::Bucket" to "arn:aws:s3:::Bucket/*".

Q16) The Security Engineer has discovered that a new application that deals with highly sensitive data is storing Amazon S3 objects with the following key pattern, which itself contains highly sensitive data.
Pattern:
"randomID_datestamp_PII.csv"
Example:
"1234567_12302017_000-00-0000 csv"
The bucket where these objects are being stored is using server-side encryption (SSE).
Which solution is the most secure and cost-effective option to protect the sensitive data?

- [ ] Store all sensitive objects in Binary Large Objects (BLOBS) in an encrypted Amazon RDS instance.
- [ ] Use a random and unique S3 object key, and create an S3 metadata index in Amazon DynamoDB using client-side encrypted attributes.
- [x] Add an S3 bucket policy that denies the action s3:GetObject
- [ ] Remove the sensitive data from the object name, and store the sensitive data using S3 user-defined metadata.

Q17)

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

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

- [x] Verify that the S3 bucket defined in CloudTrail exists.
- [ ] Remove any lifecycle policies on the S3 bucket that are archiving objects to Amazon Glacier.
- [ ] Verify that the IAM role used by CloudTrail has access to write to Amazon CloudWatch Logs.
- [ ] Verify that the S3 bucket policy allow CloudTrail to write objects.
- [x] Verify that the log file prefix defined in CloudTrail exists in the S3 bucket.

Q18)

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'?

- Create a KMS master key. Generate per-record data keys and use them to encrypt data prior to uploading it to DynamoDS. Dispose of the cleartext and encrypted data keys after encryption without storing.
- ✅ Enable S3 server-side encryption with the customer-provided keys. Upload the data to Amazon S3, and then use S3Copy to move all data to DynamoDB
- Use AWS Certificate Manager to request a certificate. Use that certificate to encrypt data prior to uploading it to DynamoDB.
- Use the DynamoDB Java encryption client to encrypt data prior to uploading it to DynamoDB.

Q19)

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

Q20)

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.

Q21)

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

What is the most efficient way to meet these requirements?

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

Explanation:-
This is correct the answer because, it IDS host-based has the ability to identify, from there we will push logs to cloudwatch then metric creation then alarm.

Many AWS customers install host-based IDS software, such as the open-source product OSSEC, that includes file integrity checking and rootkit detection software. Use these products to analyze important system files and folders and calculate checksum that reflects their trusted state, and then regularly check to see whether these files have been modified and alert the system administrator.

Refer: https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf

- Install antivirus software and ensure that signatures are up-to-date. Configure Amazon CloudWatch alarms to send alerts for security events.
- Export system log files to Amazon S3. Parse the log files using an AWS Lambda function that will send alerts of any unauthorized system login attempts through Amazon SNS.
- Use Amazon CloudWatch Logs to detect file system changes. If a change is detected, automatically terminate and recreate the instance from the most recent AMI. Use Amazon SNS to send notification of the event.

Q22)

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

How can this be accomplished? (Choose two.)

- ✅ Create a VPN connection from the data center to each of the three VPCs. Use an on-premises scanning engine to scan the instances in each VPC. Complete the penetration test request form for all three VPCs.
- Create a VPN connection from the data center to each of the three VPCs. Use an on-premises scanning engine to scan the instances in each VPC. Do not complete the penetration test request form.
- ✅ Create a VPN connection from the data center to VPC A. Use an on-premises scanning engine to scan the instances in all three VPCs. Complete the penetration test request form for all three VPCs.
- Deploy a pre-authorized scanning engine from the Marketplace into each VPC, and scan instances in each VPC from the scanning engine in that VPC. Do not complete the penetration test request form.
- Deploy a pre-authorized scanning engine from the AWS Marketplace into VPC B, and use it to scan instances in all three VPCs. Do not complete the penetration test request form.

Q23)

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.)

- Use AWS Key Management Services to encrypt all the traffic between the chant end application servers.
- ✓ Use Amazon Inspector to periodically scan the backend instances.
- ✓ Use Elastic Load Balancing to offload Secure Sockets Layer encryption.
- Review the application security groups to ensure that only the necessary ports are open.
- Use AWS Certificate Manager to encrypt all traffic between the client and application servers.

Q24)

For compliance reasons, an organization limits the use of resources to three specific AWS regions.

It wants to be alerted when any resources are launched in unapproved regions.

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

- Analyze Amazon CloudWatch Logs for activities in unapproved regions.
- Monitor Amazon S3 Event Notifications for objects stored in buckets in unapproved regions.
- Develop an alerting mechanism based on processing AWS Cloud Trail logs.
- ✓ Use AWS Trusted Advisor to alert on all resources being created.

Q25)

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

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

- Route all traffic to the workload through AWS WAF. Add each employee's home IP address into an AWS WAF rule, and block all other traffic.
- Use a VPN appliance from the AWS Marketplace for users to connect to, and restrict workload access to traffic from that appliance.
- ✓ Create a virtual gateway for VPN connectivity for each employee, and restrict access to the workload from within the VPC.
- Add each employee's home IP address to the security group for the application so that only those users can access the workload.

Q26)

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

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

- ✓ Place the security appliance in the public subnet with the internet gateway
- Disable the Network Source/Destination check on the security appliance's elastic network interface
- Disable network ACLs.
- Configure the security appliance's elastic network interlace for promiscuous mode.

Q27) 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?

- Amazon DynamoDB with server-side encryption
- ✓ AWS CloudHSM
- Amazon S3 with default encryption
- AWS Systems Manager Parameter Store

Q28) An AWS account includes two S3 buckets: bucket1 and bucket2. The bucket2 does not have a policy defined, but bucket1 has the following bucket policy:
In addition, the same account has an IAM User named "alice", with the following IAM policy.
Which buckets can user "alice" access?

- Both bucket1 and bucket2
- Bucket2 only
- ✓ Bucket1 only
- Neither bucket1 not bucket2

Q29)

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?

- ✓ Have each application use an IAM policy in a user context to have specific access permissions on the KMS CMK.
- Have each application use a grant on the KMS CMK to add or remove specific access controls on the KMS CMK.

- Have each application assume an IAM role that provides permissions to use the AWS Certificate Manager CMK.
- Change the key policy permissions associated with the KMS CMK for each application when it must access the data in Amazon S3.

Q30)

A distributed web application is installed across several EC2 instances in public subnets residing in two Availability Zones.

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

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

- ✅ Use network ACLs.
- Install intrusion prevention software (IPS) on each instance.
- Update security groups to deny traffic from the originating source IP addresses.
- Use custom route tables to prevent malicious traffic from routing to the instances.

Q31)

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.)

- Configure Amazon Cognito to add relying party trust between Active Directory and AWS.
- Configure Active Directory to add relying party trust between Active Directory and AWS.
- ✅ Configure Amazon Cloud Directory to support a SAML provider.
- Create IAM groups with permissions corresponding to each Active Directory group.
- ✅ Create IAM roles with permissions corresponding to each Active Directory group.

Q32)

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

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

- AWS Firewall Manager
- ✅ VPC Flow Logs
- AWS Key Management Service (AWS KMS)
- Amazon Athena
- ✅ AWS CloudTrail
- ✅ Security groups

Q33)

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

Q34) 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

Q35) TPT Limited is developing a system for distribution of the confidential training videos to employees. The content created is stored in Amazon S3. How to use CloudFront to serve content but not publicly accessible from Amazon 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.
- None of these

Q36)

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

Q37)

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.

Q38)

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

Q39)

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

Q40)

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

Q41)

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.

Q42)

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

Q43)

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?

- An outbound rule must be added to the network ACL to allow the response to be sent to the client on the HTTP port.
- 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.
- ✅ The outbound rules on the security group do not allow the response to be sent to the client on the HTTP port.
- The outbound rules on the security group do not allow the response to be sent to the client on the ephemeral port range.

Q44) A company has two AWS accounts, each containing one VPC. The first VPC has a VPN connection with its corporate network. The second VPC, without a VPN, hosts an Amazon Aurora database cluster in private subnets. Developers manage the Aurora database from a bastion host in a public subnet as shown in the image.
A security review has flagged this architecture as vulnerable, and a Security Engineer has been asked to make this design more secure. The company has a short deadline and a second VPN connection to the Aurora account is not possible.
How can a Security Engineer securely set up the bastion host?

- Create an AWS Direct Connect connection between the corporate network and the Aurora account, and adjust the Aurora security group for this connection.
- Move the bastion host to the VPC with VPN connectivity. Create a cross-account trust relationship between the bastion VPC and Aurora VPC, and update the Aurora security group for the relationship.
- ✅ Create a SSH port forwarding tunnel on the Developer's workstation to the bastion host to ensure that only authorized SSH clients can access the bastion host.
- Move the bastion host to the VPC and VPN connectivity. Create a VPC peering relationship between the bastion host VPC and Aurora VPC.

Q45) An organization operates a web application that serves users globally. The application runs on Amazon EC2 instances behind an Application Load Balancer.
There is an Amazon CloudFront distribution in front of the load balancer, and the organization uses AWS WAF. The application is currently experiencing a volumetric, attack whereby the attacker is exploiting a bug in a popular mobile game.
The application is being flooded with HTTP requests from all over the world with the User-Agent set to the following string: Mozilla/5.0 (compatible; ExampleCorp; ExampleGame/1.22; Mobile/1.0)
What mitigation can be applied to block attacks resulting from this bug while continuing to service legitimate requests?

- Create an IP-based blacklist in AWS WAF to block the IP addresses that are originating from requests that contain ExampleGame/1.22 in the User-Agent header.
- ✅ Create a rate-based rule in AWS WAF to limit the total number of requests that the web application services.
- Create a geographic restriction on the CloudFront distribution to prevent access to the application from most geographic regions
- Create a rule in AWS WAF rules with conditions that block requests based on the presence of ExampleGame/1.22 in the User-Agent header

---

Q46)

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?

- Move the workload to a Dedicated Host, as this provides additional network security controls and monitoring.
- Use IPv6 addressing exclusively on the EC2 hosts, as this prevents the hosts from being accessed from the internet.
- ✅ Within the Amazon VPC configuration, mark the VPC as private and disable Elastic IP addresses.
- Use AWS Config to detect whether an Internet Gateway is added and use an AWS Lambda function to provide auto-remediation.

Q47)

A Developer who is following AWS best practices for secure code development requires an application to encrypt sensitive data to be stored at rest, locally in the application, using AWS KMS.

What is the simplest and most secure way to decrypt this data when required?

- ✅ Store the encrypted data key alongside the encrypted data. Use the Decrypt API to retrieve the data key to decrypt the data when required.
- Use the Encrypt API to store an encrypted version of the data key with another customer managed key. Decrypt the data key and use it to decrypt the data when required.
- Keep the plaintext data key stored in Amazon DynamoDB protected with IAM policies. Query DynamoDB to retrieve the data key to decrypt the data
- Request KMS to provide the stored unencrypted data key and then use the retrieved data key to decrypt the data.

Q48)

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?

- ✅ Implement ip tables-based restrictions on the instances.
- Log all student SSH interactive session activity.
- Disable the EC2 instance metadata service.
- Install the Amazon Inspector agent on the instances.

Q49)

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?

- Reboot the instance and check for any Amazon CloudWatch alarms.
- Remove the instance from the load balancer, and shut down access to the instance by tightening the security group.
- Remove the instance from the load balancer and terminate it.
- ✅ Stop the instance and make a snapshot of the root EBS volume.

Explanation:-While the instance is stopped, you can treat its root volume like any other volume, and modify it (for example, repair file system problems or update software). refer - https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/Stop_Start.html Rebooting the instance won't prevent lateral movement when the attacker/malware has persistence.

Q50)

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

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

- Newly created CMKs must allow the root principal to perform the kms CreateGrant API operation.
- Newly created CMKs must have a key policy that allows the root principal to perform all actions.
- The account's CMK key policy must allow the account's IAM roles to perform KMS EnableKey.
- ✅ Newly created CMKs must mirror the IAM policy of the KMS key administrator.

Q51)

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 has been compromised.

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

- ✅ Attach a security group that has restrictive ingress and egress rules to the EC2 instance.
- De-register the EC2 instance from the ALB and detach it from the Auto Scaling group.
- Disable any Amazon Route 53 health checks associated with the EC2 instance.
- Initiate an Amazon Elastic Block Store volume snapshots of all volumes on the EC2 instance.
- ✅ Detach the elastic network interface from the EC2 instance.
- ✅ Add a rule to an AWS WAF to block access to the EC2 instance.

Q52)

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 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 there requirements? (Choose three.)

- ✅ Configure CloudTrail in the centralized account to log all accounts to the new centralized S3 bucket.
- 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.
- Use unique log file prefixes for trials in each AWS account.
- ✅ 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.
- Create a new S3 bucket in a separate AWS account for centralized storage of CloudTrail logs, and enable "Log File Validation" on all trails.
- ✅ Enable encryption of the log files by using AWS Key Management Service

---

Q53)

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?

- Use the Systems Manager Parameter Store to store the keys and then use the service API operations to delete the key if necessary.
- Use AWS CloudHSM to store the keys and then use the CloudHSM API or the PKCS11 library to delete the keys if necessary.
- ✅ Use KMS with AWS imported key material and then use the DeleteImportedKeyMaterial API to remove the key material if necessary.

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

Q54) An application uses Amazon Cognito to manage end users' permissions when directly accessing AWS resources, including Amazon DynamoDB. A new feature request reads as follows:
Provide a mechanism to mark customers as suspended pending investigation or suspended permanently. Customers should still be able to log in when suspended, but should not be able to make changes.
The priorities are to reduce complexity and avoid potential for future security issues.
Which approach will meet these requirements and priorities?

- Move suspended customers to a second Cognito group and define an appropriate IAM access policy for the group.
- Use Amazon Cognito Sync to push out a "suspension_status" parameter and split the IAM policy into normal users and suspended users.
- Add suspended customers to second Cognito user pool and update the application login flow to check both user pools.
- ✓ Create a new database field "suspended_status" and modify the application logic to validate that field when processing requests.

Q55) A company stores data on an Amazon EBS volume attached to an Amazon EC2 instance. The data is asynchronously replicated to an Amazon S3 bucket. Both the EBS volume and the S3 bucket are encrypted with the same AWS KMS Customer Master Key (CMK). A former employee scheduled a deletion of that CMK before leaving the company.
The company's Developer Operations department learns about this only after the CMK has been deleted.
Which steps must be taken to address this situation?

- Make a request to AWS Support to recover the S3 encrypted data.
- Recover the data from the EBS encrypted volume using an earlier version of the KMS backing key.
- ✓ Copy the data directly from the EBS encrypted volume before the volume is detached from the EC2 instance.
- Make a request to AWS Support to restore the deleted CMK, and use it to recover the data.

Q56)

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?

- The execution role for the Lambda function did not grant permissions to write to the Amazon S3 bucket where CloudWatch Logs stores the logs.
- The Lambda function was executed by using Amazon API Gateway, so logs are not stored in CloudWatch Logs.
- ✓ The execution role for the Lambda function did not grant permissions to write log data to CloudWatch Logs.
- The version of the Lambda function that was executed was not current.

Q57)

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?

- ✓ GuardDuty only monitors active network traffic flow for command-and-control activity.
- GuardDuty does not see these DNS requests.
- GuardDuty did not have the appropriate alerts activated.
- GuardDuty does not report on command-and-control activity.

Q58)

The AWS Systems Manager Parameter Store is being used to sore database passwords used by an AWS Lambda function. Because this is sensitive data, the parameters are stored as type SecureString and protected by an AWS KMS key that allows access through IAM.

When the function executes, this parameter cannot be retrieved as the result of an access denied error.

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

- Add Lambda.amazonaws.com as a trusted entity on the IAM role that the Lambda function uses.
- Add a policy to the role that the Lambda function uses, allowing kms: Decrypt for the KMS key.
- Update the Lambda configuration to launch the function in a VPC.
- ✓ Update the ssm.amazonaws.com principal in the KMS key policy to allow kms: Decrypt.

Q59)

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.)

- Create an AWS Config custom rule, and associate it with an AWS Lambda function that contains the evaluating logic.
- ✓ Create an Amazon CloudWatch Event rule that triggers on events emitted by AWS Config.
- Create an AWS Config managed rule with a resource type of AWS:: Lambda:: Function.
- ✓ Create an AWS Config configuration item for each VPC in the company AWS account.

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

Q60) The Security Engineer is given the following requirements for an application that is running on Amazon EC2 and managed by using AWS CloudFormation templates with EC2 Auto Scaling groups:
-Have the EC2 instances bootstrapped to connect to a backend database.
-Ensure that the database credentials are handled securely.
-Ensure that retrievals of database credentials are logged.
Which of the following is the MOST efficient way to meet these requirements?

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

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

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

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