1. (Domain 3: Infrastructure Security, Hard) A company runs a web application on Amazon EC2 instances behind an Application Load Balancer (ALB). They want to protect against common web exploits like SQL injection and cross-site scripting. They also require detailed logs for auditing and compliance. Which combination of AWS services and configurations should they implement?

a) AWS WAF with managed rules, AWS Shield Standard, ALB access logs enabled. b) Amazon Inspector, AWS Config, CloudTrail logs enabled. c) AWS WAF with custom rules, AWS Shield Advanced, CloudWatch Logs for WAF. d) AWS Firewall Manager, AWS Network Firewall, S3 bucket for storing web server logs.

2. (Domain 2: Security Logging and Monitoring, Medium) A security analyst is investigating a potential security incident. They need to analyze VPC Flow Logs for a specific time period across multiple accounts in their organization. What is the MOST efficient way to aggregate and query these logs centrally?

a) Configure VPC Flow Logs to publish to individual CloudWatch Logs groups in each account, then manually consolidate the logs. b) Configure VPC Flow Logs to publish to Amazon S3 in each account, then use AWS Glue to aggregate and analyze the logs. c) Configure a central S3 bucket, use AWS Organizations to automatically publish VPC Flow Logs from all accounts to this bucket, and use Amazon Athena to query the logs. d) Configure VPC Flow Logs to publish to a central CloudWatch Logs group using a cross-account subscription filter, and use CloudWatch Logs Insights to query the logs.

3. (Domain 4: Identity and Access Management, Hard) A company has a strict requirement that all AWS API calls made by applications running on EC2 instances must be authenticated using temporary credentials with the least privilege. The solution needs to be scalable and minimize operational overhead. Which approach BEST meets these requirements?

a) Create IAM users with access keys for each application and store the credentials in AWS Secrets Manager. b) Use instance profiles associated with IAM roles and configure applications to use the AWS SDK to retrieve temporary credentials. c) Implement a custom credential provider that uses AWS STS to assume a role with the required permissions. d) Configure applications to sign API requests using SigV4 with hardcoded access keys.

4. (Domain 5: Data Protection, Medium) A company stores sensitive data in an Amazon S3 bucket. They need to ensure that the data is encrypted at rest and in transit, and that access to the data is tightly controlled. Which combination of configurations will satisfy these requirements?

a) Enable default encryption on the S3 bucket with an AWS KMS key, and use a bucket policy to enforce HTTPS-only access. b) Use client-side encryption with a customer-managed key, and configure a restrictive bucket policy that only allows specific IAM users and roles. c) Enable server-side encryption with S3-managed keys (SSE-S3), and use a bucket policy to allow access only from within the VPC. d) Enable server-side encryption with customer-provided keys (SSE-C), and use an S3 access control list (ACL) to grant access to authorized users.

5. (Domain 1: Threat Detection and Incident Response, Hard) A security team has noticed an increase in suspicious activity originating from a specific subnet within their VPC. They want to quarantine the affected instances automatically while preserving forensic data for analysis. What is the most effective automated approach to achieve this?

a) Use Amazon GuardDuty findings to trigger an AWS Lambda function that modifies security groups to deny all traffic and creates EBS snapshots of the instances. b) Configure Amazon Inspector to trigger an AWS Systems Manager Automation document that isolates the instances by placing them in a quarantine VPC and takes EBS snapshots. c) Use AWS Security Hub findings to invoke an AWS Step Functions workflow that terminates the instances and sends notifications to the security team. d) Create a CloudWatch Events rule that triggers an Amazon SNS topic, which then notifies the security team to manually quarantine the instances.

6. (Domain 6: Management and Security Governance, Medium) A company is adopting a multi-account AWS strategy. They want to ensure that all accounts adhere to a baseline set of security configurations, such as enforcing encryption for all EBS volumes and preventing public access to S3 buckets. Which service can help them establish and maintain these configurations at scale?

a) AWS Organizations b) AWS Config c) AWS Service Catalog d) AWS Control Tower

7. (Domain 3: Infrastructure Security, Hard) A company uses AWS Direct Connect for a dedicated connection to their on-premises data center. They want to encrypt all traffic traversing this connection to meet compliance requirements. What is the recommended approach to achieve this?

a) Configure IPsec VPN tunnels over the Direct Connect connection. b) Enable MACsec on the Direct Connect connection using AWS Site-to-Site VPN. c) Enable encryption in transit for the applications running on EC2 instances. d) Use AWS PrivateLink to establish a private connection to the on-premises network.

8. (Domain 2: Security Logging and Monitoring, Medium) You are designing a security monitoring solution for a web application that is expected to generate a high volume of logs. You need to retain these logs for at least one year for compliance purposes and also require the ability to perform real-time analysis of the log data. Which combination of AWS services is MOST cost-effective and meets these requirements?

a) CloudWatch Logs with a one-year retention policy, and CloudWatch Logs Insights for real-time analysis. b) CloudTrail logs stored in an S3 bucket with a lifecycle policy to transition to Amazon S3 Glacier after 30 days, and Amazon Athena for analysis. c) CloudWatch Logs with a one-month retention policy, streamed to Amazon Kinesis Data Firehose, which delivers to Amazon S3 with a lifecycle policy to transition to Amazon S3 Glacier after one month, and Amazon OpenSearch Service for real-time analysis. d) VPC Flow Logs published to Amazon Kinesis Data Streams, which are then processed by an AWS Lambda function and stored in Amazon DynamoDB for real-time analysis.

9. (Domain 4: Identity and Access Management, Hard) A development team needs access to an Amazon RDS database from their on-premises development environment. The solution should follow the principle of least privilege, avoid storing long-term credentials, and work with existing Active Directory for user management. What is the recommended approach?

a) Create IAM users with access keys for each developer and configure the RDS database to allow connections from the on-premises network. b) Establish a VPN connection between the on-premises network and the VPC, and use IAM roles with temporary credentials to access the RDS database. c) Use AWS Directory Service to create a managed Microsoft AD in the VPC, establish a trust relationship with the on-premises Active Directory, and configure the RDS database to use IAM DB

authentication. d) Configure the RDS database to use password authentication and store the credentials in AWS Secrets Manager.

10. (Domain 5: Data Protection, Medium) A company is migrating a large database to Amazon Aurora. They want to encrypt the data at rest using a customer-managed KMS key and ensure that the key is rotated automatically every year. What steps should they take to achieve this?

a) Create a customer-managed KMS key with automatic key rotation enabled, and specify this key when creating the Aurora DB cluster. b) Use an AWS-managed KMS key for the Aurora DB cluster and create a CloudWatch Events rule to trigger a Lambda function that rotates the key annually. c) Enable default encryption for the Aurora DB cluster and use a key policy to control access to the key. d) Create a customer-managed KMS key without automatic rotation and manually rotate the key every year.

11. (Domain 1: Threat Detection and Incident Response, Hard) A security team is responding to a potential data breach. They need to quickly identify all EC2 instances that have communicated with a known malicious IP address over the past 24 hours. Which combination of services and actions can provide this information MOST efficiently?

a) Use VPC Flow Logs stored in S3 and analyze them using Amazon Athena with a SQL query that filters for the malicious IP address. b) Use AWS Config to identify all EC2 instances and then manually check the security group rules for each instance. c) Use Amazon GuardDuty findings to identify affected instances and then inspect the CloudTrail logs for API calls made by those instances. d) Use Amazon Inspector to scan all EC2 instances and generate a report that includes network connections.

12. (Domain 6: Management and Security Governance, Medium) A company wants to enforce a policy that requires all new EC2 instances to be launched only from approved AMIs. Which combination of AWS services can help them achieve this?

a) AWS Organizations and Service Control Policies (SCPs). b) AWS Config and AWS Lambda. c) AWS Service Catalog and IAM. d) AWS Systems Manager and AWS CloudFormation.

13. (Domain 3: Infrastructure Security, Hard) A company is designing a highly available and secure architecture for a web application using EC2 instances and an Application Load Balancer (ALB). They need to ensure that the instances can only be accessed through the ALB and that SSH access is restricted to a specific bastion host. Which configuration provides the BEST security posture?

a) Place the EC2 instances and the ALB in the same public subnet, configure the security group for the instances to allow traffic only from the ALB's security group, and configure a separate security group for the bastion host to allow SSH access from a specific IP range. b) Place the EC2 instances in a private subnet and the ALB in a public subnet, configure the security group for the instances to allow traffic only from the ALB's security group, and configure a separate security group for the bastion host to allow SSH access from a specific IP range. c) Place the EC2 instances and the ALB in the same private subnet, configure the security group for the instances to allow traffic only from the ALB's security group, and use AWS Systems Manager Session Manager for SSH access. d) Place the EC2 instances in a public subnet and the ALB in a private subnet, configure the security group for the instances to allow traffic only from the ALB's security group, and configure a NAT gateway for internet access.

14. (Domain 2: Security Logging and Monitoring, Medium) You need to monitor changes to security group rules in your VPC. You want to be notified immediately when a security group rule is added or removed that allows inbound traffic on port 22 (SSH). Which combination of AWS services can help you achieve this?

a) CloudTrail logs, CloudWatch Events, and Amazon SNS. b) VPC Flow Logs, Amazon Athena, and Amazon QuickSight. c) AWS Config, AWS Lambda, and Amazon SES. d) Amazon GuardDuty and AWS Security Hub.

15. (Domain 4: Identity and Access Management, Hard) A company is implementing a new policy that requires all IAM users to enable MFA for their accounts. They also want to enforce a password policy that requires passwords to be at least 14 characters long and rotated every 90 days. How can they implement these policies for all existing and new IAM users?

a) Use AWS Organizations to create a Service Control Policy (SCP) that denies access to any IAM user who does not have MFA enabled, and create an IAM password policy that applies to all users. b) Manually enable MFA for each IAM user and update the password policy for each user individually. c) Use AWS Config to

identify users without MFA and send them a notification to enable it, and use CloudFormation to create a template that sets the password policy for new users. d) Use the AWS CLI to script the enabling of MFA for all users and the modification of the password policy.

16. (Domain 5: Data Protection, Hard) A company is using AWS KMS to manage encryption keys for their applications. They have a requirement to use only FIPS 140-2 validated HSMs for key storage and cryptographic operations. How can they ensure that their KMS keys meet this requirement?

a) Use AWS-managed keys in KMS. b) Use customer-managed keys with imported key material. c) Use customer-managed keys in a custom key store backed by an AWS CloudHSM cluster. d) Use customer-managed keys with automatic key rotation enabled.

17. (Domain 1: Threat Detection and Incident Response, Medium) You are setting up Amazon GuardDuty in your AWS environment. You want to receive notifications about high-severity findings immediately and also want to store all findings for long-term analysis. Which is the best combination of actions to take?

a) Configure CloudWatch Events to trigger an SNS topic for high-severity findings and enable S3 export for all findings. b) Configure GuardDuty to send findings to Security Hub and create a CloudWatch alarm for high-severity findings in Security Hub. c) Use the GuardDuty API to poll for new findings and send email notifications using Amazon SES. d) Enable GuardDuty findings to be sent to CloudWatch Logs and use CloudWatch Logs Insights to query for high-severity findings.

18. (Domain 6: Management and Security Governance, Hard) A company wants to grant permissions to an auditor to review security configurations across multiple AWS accounts within their organization. The auditor should have read-only access to relevant services like AWS Config, AWS Security Hub, and Amazon GuardDuty, but should not be able to make any changes. What is the MOST secure and scalable way to achieve this?

a) Create an IAM user in each account with the required permissions and provide the auditor with the credentials for each user. b) Create a cross-account IAM role in each account with the required permissions and have the auditor assume this role from a central account. c) Use AWS Organizations to create a Service Control Policy (SCP) that grants the required permissions to all accounts and have the auditor use

a single IAM user in the management account. d) Use AWS Control Tower to create a custom blueprint that grants the required permissions to the auditor's IAM user in a dedicated audit account.

19. (Domain 3: Infrastructure Security, Medium) Your company is deploying a new application on Amazon ECS using the Fargate launch type. You need to ensure that the containers have restricted network access and can only communicate with specific AWS services and a designated database. Which is the best combination of techniques to implement network security for these containers?

a) Use security groups, network ACLs, and a NAT gateway. b) Use task definitions with specific port mappings and a service discovery mechanism. c) Use security groups, task definitions with awsvpc network mode, and VPC endpoints. d) Use a service mesh like AWS App Mesh and implement strict traffic routing rules.

20. (Domain 4: Identity and Access Management, Hard) A company has a hybrid cloud environment with applications running both on-premises and in AWS. They want to implement a Single Sign-On (SSO) solution that allows users to access AWS resources using their existing on-premises Active Directory credentials. The solution should also support Multi-Factor Authentication (MFA). Which combination of AWS services can achieve this MOST effectively?

a) AWS Directory Service for Microsoft Active Directory, AWS IAM Identity Center (successor to AWS Single Sign-On), and a third-party MFA provider. b) AWS IAM, AWS Secrets Manager, and Amazon Cognito. c) AWS Directory Service for Microsoft Active Directory, AWS Site-to-Site VPN, and AWS IAM. d) AWS IAM Identity Center (successor to AWS Single Sign-On), Amazon Cognito, and AWS MFA.

21. (Domain 5: Data Protection, Hard) A company needs to encrypt data stored in Amazon S3 using server-side encryption with customer-provided keys (SSE-C). The keys must be securely stored and managed on-premises. The solution must minimize changes to the existing application code that uploads objects to S3. What is the most effective way to achieve this?

a) Store the encryption keys in AWS Secrets Manager and retrieve them before each S3 upload operation. b) Use AWS Key Management Service (KMS) with

imported key material to generate data keys and use them for SSE-C. c) Develop a custom key management service that runs on-premises and provides keys to the application via an API. d) Modify the application to use an HTTPS proxy that intercepts S3 upload requests, adds the necessary encryption headers with keys from an on-premises key store, and forwards the requests to S3.

22. (Domain 1: Threat Detection and Incident Response, Medium) Your security team has detected an unusual pattern of API calls originating from an EC2 instance. They suspect that the instance might be compromised. You need to isolate the instance for further investigation without losing its current state. What steps should you take?

a) Terminate the instance, create an AMI from it, and launch a new instance from the AMI in a restricted VPC. b) Modify the instance's security group to deny all inbound and outbound traffic, create an EBS snapshot, and then terminate the instance. c) Detach the instance from its Auto Scaling group, change its security group to allow only specific forensic tools, and take an EBS snapshot. d) Stop the instance, create an AMI from it, and detach the EBS volumes for analysis.

23. (Domain 4: Identity and Access Management, Hard) A company wants to grant temporary access to their AWS resources to a third-party auditor. The auditor should only have read-only access to specific services for a limited time and should authenticate using their own corporate credentials (SAML 2.0 based). What is the most secure way to achieve this?

a) Create an IAM user for the auditor and provide them with long-term access keys. b) Configure an IAM role with the required permissions and have the auditor assume the role using AWS STS after authenticating with their corporate IdP. c) Use AWS IAM Identity Center (successor to AWS Single Sign-On) to create a permission set and assign it to the auditor, who will authenticate through their IdP. d) Grant the auditor's corporate identity provider access to your AWS account using cross-account IAM roles.

24. (Domain 2: Security Logging and Monitoring, Medium) You are responsible for monitoring security events across multiple AWS accounts in your organization. You want to aggregate security findings from AWS Security Hub, Amazon GuardDuty, and Amazon Inspector into a single view and be able to perform automated remediation actions. What is the recommended approach?

a) Configure each service to send findings to a central Amazon S3 bucket and use Amazon Athena to query the findings. b) Enable AWS Security Hub in each account, designate a Security Hub administrator account, enable cross-region aggregation, and use the Security Hub API to trigger remediation actions. c) Use AWS CloudFormation StackSets to deploy a custom solution that collects findings from each service and stores them in Amazon DynamoDB. d) Configure each service to send findings to a central CloudWatch Logs group and use CloudWatch Logs Insights for analysis and CloudWatch Events to trigger remediation.

25. (Domain 6: Management and Security Governance, Hard) A company is implementing a multi-account AWS strategy using AWS Organizations. They want to ensure that all new accounts created within the organization automatically have AWS Config and AWS CloudTrail enabled, configured to send data to a central logging account. How can they achieve this with the least operational overhead?

a) Use AWS CloudFormation StackSets to deploy the necessary resources in each new account after it is created. b) Use AWS Organizations service control policies (SCPs) to enforce the creation of AWS Config and CloudTrail resources. c) Use AWS Control Tower to create a custom blueprint that includes the configuration of AWS Config and CloudTrail. d) Use AWS Organizations to apply an organizational unit (OU)-level policy that automatically enables AWS Config and CloudTrail for all accounts within the OU.

26. (Domain 3: Infrastructure Security, Medium) You are designing a web application that requires users to upload files. You want to ensure that the files are scanned for malware before they are stored in an Amazon S3 bucket. What is the most efficient way to implement this?

a) Directly upload files to an S3 bucket and use Amazon Inspector to scan the objects. b) Use an EC2 instance to receive the file uploads, scan them with an anti-malware solution, and then upload them to S3. c) Directly upload files to an S3 bucket and use S3 Event Notifications to trigger an AWS Lambda function that scans the objects using an integrated third-party anti-malware solution. d) Use API Gateway to receive file uploads, trigger a Lambda function for scanning, and then store the files in S3.

27. (Domain 5: Data Protection, Medium) A company stores highly sensitive data in an Amazon RDS for PostgreSQL database. They require encryption at rest with a

customer-managed key, and the ability to audit all access to the encryption key. Which combination of AWS services and features should they use?

a) Amazon RDS encryption with an AWS-managed key, and AWS CloudTrail for auditing. b) Amazon RDS encryption with a customer-managed key in AWS KMS, and AWS CloudTrail for auditing key usage. c) Transparent Data Encryption (TDE) in PostgreSQL with a key stored in AWS Secrets Manager, and Amazon RDS Enhanced Monitoring. d) Amazon RDS encryption with a customer-provided key, and Amazon CloudWatch Logs for auditing.

28. (Domain 1: Threat Detection and Incident Response, Hard) Your company has a web application that uses Amazon Cognito for user authentication. You notice a sudden increase in failed login attempts for multiple user accounts, indicating a potential brute-force attack. How can you automatically mitigate this attack in real time?

a) Enable Amazon GuardDuty to detect the attack and automatically block the source IP addresses using AWS WAF. b) Use Amazon Cognito advanced security features to enable adaptive authentication, which will automatically challenge suspicious sign-in attempts with MFA or block them. c) Configure Amazon CloudWatch alarms to monitor failed login attempts and trigger an AWS Lambda function that updates the user pool configuration to block further attempts. d) Use AWS Shield Advanced to mitigate the attack at the network level and prevent it from reaching the application.

29. (Domain 4: Identity and Access Management, Medium) You need to grant an application running on an EC2 instance access to an Amazon DynamoDB table. The application should only have read access to specific items in the table. What is the most secure way to grant these permissions?

a) Create an IAM user with access keys and store the credentials in the application's configuration file. b) Create an IAM role with a policy that grants read access to the DynamoDB table and allows fine-grained access control using condition keys, then assign the role to the EC2 instance profile. c) Use Amazon Cognito to authenticate the application and grant it temporary access to the DynamoDB table. d) Configure the DynamoDB table to allow public read access and use the AWS SDK in the application to retrieve the data.

30. (Domain 2: Security Logging and Monitoring, Hard) A company is using AWS CloudTrail to log API activity in their AWS account. They need to retain these logs for seven years for compliance purposes. They also want to be able to quickly search for specific events, such as the creation of an IAM user or changes to a security group, within the last 90 days. What is the most cost-effective solution that meets these requirements?

a) Store all CloudTrail logs in an Amazon S3 bucket with a lifecycle policy to transition the logs to Amazon S3 Glacier after 90 days and use Amazon Athena to query the logs. b) Store all CloudTrail logs in an Amazon S3 bucket with a lifecycle policy to transition the logs to Amazon S3 Glacier Deep Archive after 90 days, create a CloudTrail Lake and use it to query events within the last 90 days. c) Store all CloudTrail logs in Amazon CloudWatch Logs with a retention period of seven years and use CloudWatch Logs Insights to query the logs. d) Store the last 90 days of CloudTrail logs in Amazon OpenSearch Service and the rest in an Amazon S3 bucket with a lifecycle policy to transition them to Amazon S3 Glacier after 90 days.

31. (Domain 6: Management and Security Governance, Medium) A company wants to prevent users from launching EC2 instances in specific AWS regions. Which is the best approach to enforce this restriction?

a) Create an IAM policy that denies the `ec2:RunInstances` action for the specified regions and attach it to all users and roles. b) Use AWS Organizations to create a Service Control Policy (SCP) that denies the `ec2:RunInstances` action for the specified regions. c) Configure AWS Config rules to detect non-compliant instances and automatically terminate them. d) Use AWS Systems Manager Automation to regularly scan for instances in the restricted regions and terminate them.

32. (Domain 3: Infrastructure Security, Hard) You are designing a solution to securely connect your on-premises network to your VPC. You need a highly available, low-latency connection that supports BGP for dynamic routing. You also require the ability to encrypt traffic in transit. Which solution BEST meets these requirements?

a) AWS Site-to-Site VPN with two VPN connections using different virtual private gateways. b) AWS Direct Connect with two connections to different locations, and IPsec VPN tunnels configured over the Direct Connect connections. c) AWS Client

VPN Endpoint for secure access from individual users. d) AWS PrivateLink to establish a private connection to the on-premises network.

33. (Domain 5: Data Protection, Medium) A company is using Amazon S3 to store sensitive data. They want to implement client-side encryption using customer-managed keys stored in AWS KMS. They need to ensure that the data keys used for encryption are unique for each object and are never stored in plaintext. What is the correct approach?

a) Generate a data key using KMS, encrypt the data with the data key, store the encrypted data key alongside the encrypted data in S3, and discard the plaintext data key. b) Generate a data key using KMS, encrypt the data with the data key, store the plaintext data key in AWS Secrets Manager, and then upload the encrypted data to S3. c) Use an AWS-managed key in KMS to encrypt the data and store the encrypted data in S3. d) Generate a unique data key on the client-side, encrypt the data with the data key, encrypt the data key with a KMS key, store both the encrypted data and the encrypted data key in S3.

34. (Domain 1: Threat Detection and Incident Response, Medium) You are using Amazon Detective to investigate a potential security incident. You have identified a suspicious EC2 instance. What are two key pieces of information that Detective can provide to help you understand the instance's activity and its potential role in the incident? (Choose two)

a) The instance's security group rules. b) A timeline of API calls made by and to the instance. c) The instance's operating system and installed software. d) A visual representation of the instance's network traffic patterns. e) The instance's CPU and memory utilization metrics.

35. (Domain 4: Identity and Access Management, Hard) A company needs to provide their developers with access to the AWS Management Console. The developers should only be able to view resources related to their specific projects and should not be able to access other projects or billing information. The solution should also minimize the number of IAM users and policies that need to be managed. Which approach is most aligned with these requirements?

a) Create a separate IAM user for each developer and assign them permissions based on their project. b) Use IAM roles with project-specific tags and configure the developers to assume these roles when they need access to the console. c) Use

AWS IAM Identity Center (successor to AWS Single Sign-On) to create permission sets based on projects and assign them to developer groups. d) Create a single IAM user with read-only access to all resources and use resource tags to filter the resources visible to each developer.

36. (Domain 2: Security Logging and Monitoring, Medium) You need to monitor your AWS environment for any changes to IAM policies. You want to receive a notification whenever a policy is created, updated, or deleted. Which combination of AWS services can help you achieve this?

a) AWS Config, Amazon SNS, and Amazon SQS. b) AWS CloudTrail, Amazon CloudWatch Events, and Amazon SNS. c) Amazon Inspector, AWS Security Hub, and Amazon SES. d) VPC Flow Logs, Amazon Athena, and Amazon QuickSight.

37. (Domain 6: Management and Security Governance, Hard) A company has a strict requirement that all EBS volumes must be encrypted. They want to prevent the creation of any unencrypted EBS volumes in their AWS environment. What is the most effective way to enforce this policy?

a) Use AWS Config to detect unencrypted EBS volumes and automatically encrypt them using an AWS Lambda function. b) Use AWS Organizations to create a Service Control Policy (SCP) that denies the `ec2:CreateVolume` action unless the `Encrypted` parameter is set to `true`. c) Enable default EBS encryption for the AWS account and use IAM policies to restrict users from disabling it. d) Use AWS Systems Manager Automation to regularly scan for unencrypted EBS volumes and terminate the associated EC2 instances.

38. (Domain 3: Infrastructure Security, Medium) You are designing a security solution for a three-tier web application running on EC2 instances behind an Application Load Balancer (ALB). The application requires that only the web servers can access the database servers, and the web servers can only be accessed through the ALB. How should you configure the security groups to achieve this?

a) Allow inbound traffic to the web server security group from the ALB security group on the application port, and allow inbound traffic to the database server security group from the web server security group on the database port. b) Allow inbound traffic to the web server security group from the internet on the application port, and allow inbound traffic to the database server security group from the web server security group on the database port. c) Allow inbound traffic to the web

server security group from the ALB security group on all ports, and allow inbound traffic to the database server security group from the internet on the database port. d) Allow inbound traffic to the web server security group from the internet on the application port, and allow inbound traffic to the database server security group from the ALB security group on the database port.

39. (Domain 5: Data Protection, Hard) A company is using AWS KMS to manage encryption keys for their applications. They need to comply with a regulatory requirement that mandates the use of hardware security modules (HSMs) under their exclusive control for storing and managing cryptographic keys. Which KMS key type should they use to meet this requirement?

a) AWS managed keys. b) Customer managed keys with imported key material. c) Customer managed keys in a custom key store backed by an AWS CloudHSM cluster. d) Customer managed keys with automatic key rotation.

40. (Domain 4: Identity and Access Management, Medium) What is the primary security benefit of using IAM roles instead of IAM users for applications running on EC2 instances?

a) Roles provide multi-factor authentication. b) Roles can be used to access resources across multiple AWS accounts. c) Roles use temporary security credentials that are automatically rotated. d) Roles can be used to manage access to on-premises resources.

Answers and Explanations:

1. Answer: c) * **Explanation:** AWS WAF with custom rules allows for granular control over traffic filtering based on specific patterns or threats. AWS Shield Advanced provides enhanced DDoS protection. CloudWatch Logs for WAF provides detailed logs of requests inspected and actions taken by WAF.

2. Answer: c) * **Explanation:** Using a central S3 bucket with AWS Organizations ensures that VPC Flow Logs from all accounts are automatically collected in one place. Amazon Athena allows for efficient querying of the logs using SQL.

3. Answer: b) * **Explanation:** Instance profiles associated with IAM roles allow EC2 instances to securely obtain temporary credentials without the need to manage long-term access keys. This approach is scalable and follows the principle of least privilege.

4. Answer: a) * **Explanation:** Enabling default encryption with an AWS KMS key ensures that data is encrypted at rest. Using a bucket policy to enforce HTTPS-only access ensures that data is encrypted in transit.

5. Answer: a) * **Explanation:** GuardDuty can detect suspicious activity and trigger automated responses using Lambda functions. Modifying security groups to deny traffic effectively isolates the instances, and creating EBS snapshots preserves the instance state for forensic analysis.

6. Answer: d) * **Explanation:** AWS Control Tower provides a way to set up and govern a secure, multi-account AWS environment. It uses AWS Organizations and other services to establish guardrails and enforce security configurations.

7. Answer: a) * **Explanation:** Configuring IPsec VPN tunnels over the Direct Connect connection provides encryption for all traffic traversing the dedicated connection.

8. Answer: c) * **Explanation:** This combination offers a cost-effective solution for storing logs with a long retention period while enabling real-time analysis. Kinesis Data Firehose can efficiently stream logs to S3, and transitioning to Glacier after one month reduces storage costs. OpenSearch Service provides real-time search and analytics capabilities.

9. Answer: c) * **Explanation:** Using AWS Directory Service with a trust relationship to on-premises Active Directory allows developers to use their existing credentials. IAM DB authentication eliminates the need to manage database passwords and provides granular access control.

10. Answer: a) * **Explanation:** Creating a customer-managed KMS key with automatic rotation enabled ensures that the encryption key is rotated automatically every year, meeting the requirement.

11. Answer: a) * **Explanation:** VPC Flow Logs record network traffic to and from instances. Analyzing these logs with Amazon Athena allows you to quickly identify instances that have communicated with a specific IP address using SQL queries.

12. Answer: c) * **Explanation:** AWS Service Catalog allows you to create and manage catalogs of approved IT services, including AMIs. IAM can be used to control who can launch instances from specific AMIs in the catalog.

13. Answer: b) * **Explanation:** Placing the EC2 instances in a private subnet and the ALB in a public subnet is a best practice for security. Configuring the security group for the instances to allow traffic only from the ALB's security group ensures that the instances can only be accessed through the ALB. The bastion host in a separate security group with restricted SSH access provides a secure way to manage the instances.

14. Answer: a) * **Explanation:** CloudTrail logs API calls, including changes to security group rules. CloudWatch Events can be used to create rules that trigger based on specific events in CloudTrail logs, such as changes to security group rules that allow inbound traffic on port 22. Amazon SNS can then be used to send notifications when the rule is triggered.

15. Answer: a) * **Explanation:** AWS Organizations and Service Control Policies (SCPs) can be used to enforce policies across multiple accounts. An SCP can deny access to any IAM user who does not have MFA enabled. The IAM password policy can be set globally and applies to all users.

16. Answer: c) * **Explanation:** Using customer-managed keys in a custom key store backed by an AWS CloudHSM cluster ensures that the keys are stored and used in FIPS 140-2 validated HSMs. CloudHSM provides single-tenant HSMs that meet this requirement.

17. Answer: a) * **Explanation:** Configuring CloudWatch Events to trigger an SNS topic for high-severity findings provides immediate notifications. Enabling S3 export for all findings ensures that they are stored for long-term analysis and auditing.

18. Answer: b) * **Explanation:** Creating a cross-account IAM role in each account with the required permissions allows the auditor to assume the role from a central account, providing a secure and scalable way to grant access without managing multiple users and credentials.

19. Answer: c) * **Explanation:** Security groups act as firewalls for tasks in awsvpc network mode. Task definitions with awsvpc mode allow you to assign an ENI to

each task, enabling granular network control. VPC endpoints provide private connectivity to specific AWS services without traversing the internet.

20. Answer: a) * **Explanation:** AWS Directory Service for Microsoft Active Directory allows you to create a managed AD in AWS that can establish a trust relationship with your on-premises AD. AWS IAM Identity Center (successor to AWS Single Sign-On) provides SSO capabilities, allowing users to sign in with their AD credentials. Integration with a third-party MFA provider adds an extra layer of security.

21. Answer: d) * **Explanation:** Using an HTTPS proxy allows you to intercept the S3 upload requests and add the necessary SSE-C headers (including the encryption key) before they reach S3. This approach minimizes changes to the application code as it doesn't need to handle the encryption process directly. The proxy handles retrieving the keys from the on-premises key store and adding them to the request.

22. Answer: c) * **Explanation:** Detaching the instance from its Auto Scaling group prevents it from being terminated automatically. Changing its security group to allow only specific forensic tools isolates the instance while still allowing for investigation. Taking an EBS snapshot preserves the instance's data for analysis.

23. Answer: b) * **Explanation:** Configuring an IAM role with the required permissions and having the auditor assume the role using AWS STS after authenticating with their corporate IdP is the most secure way to grant temporary access. This approach leverages SAML 2.0 federation and avoids creating long-term credentials.

24. Answer: b) * **Explanation:** Enabling AWS Security Hub in each account, designating a Security Hub administrator account, and enabling cross-region aggregation provides a centralized view of security findings. Security Hub also allows for automated remediation actions through integration with other services like AWS Systems Manager and AWS Lambda.

25. Answer: c) * **Explanation:** AWS Control Tower provides the easiest way to set up and govern a secure, multi-account AWS environment. You can create a custom blueprint that includes the configuration of AWS Config and AWS CloudTrail to be automatically applied to new accounts.

26. Answer: c) * **Explanation:** Using S3 Event Notifications to trigger an AWS Lambda function that scans uploaded objects for malware is the most efficient approach. This allows for asynchronous scanning without impacting the upload process and leverages the scalability of Lambda.

27. Answer: b) * **Explanation:** Using a customer-managed key in AWS KMS provides control over the encryption key and allows for auditing of all key usage through AWS CloudTrail. This combination meets the requirements for encryption at rest and auditability.

28. Answer: b) * **Explanation:** Amazon Cognito advanced security features include adaptive authentication, which can automatically assess the risk of a sign-in attempt based on factors like IP address, device, and location. It can then challenge suspicious attempts with MFA or block them, mitigating brute-force attacks in real time.

29. Answer: b) * **Explanation:** Creating an IAM role with a policy that grants read access to the DynamoDB table and is assigned to the EC2 instance profile is the most secure approach. The policy can use condition keys to further restrict access to specific items, following the principle of least privilege.

30. Answer: b) * **Explanation:** CloudTrail Lake allows to run SQL-based queries on your events. Data can be stored in CloudTrail Lake for up to seven years. With this option you can store data for seven years and quickly query events from last 90 days. Transitioning logs to Amazon S3 Glacier Deep Archive after 90 days further reduces storage costs.

31. Answer: b) * **Explanation:** Service Control Policies (SCPs) in AWS Organizations allow you to manage permissions at the organization or organizational unit (OU) level. An SCP that denies the `ec2:RunInstances` action for the specified regions effectively prevents users from launching instances in those regions.

32. Answer: b) * **Explanation:** AWS Direct Connect provides a dedicated, low-latency connection. Using two connections to different locations ensures high availability. Configuring IPsec VPN tunnels over the Direct Connect connections provides encryption for traffic in transit. BGP support enables dynamic routing.

33. Answer: a) * **Explanation:** Generating a data key using KMS, encrypting the data with it, storing the encrypted data key (wrapped by KMS) alongside the encrypted data, and discarding the plaintext data key is the standard pattern for client-side encryption. This ensures that the data key is unique for each object and never stored in plaintext.

34. Answer: b) and d) * **Explanation:** Amazon Detective provides a timeline of API calls made by and to the instance, helping to understand its activity. It also provides a visual representation of the instance's network traffic patterns, highlighting potential communication with suspicious entities.

35. Answer: c) * **Explanation:** Using AWS IAM Identity Center (successor to AWS Single Sign-On) is the most scalable and efficient approach. Permission sets can be created based on projects and assigned to developer groups. Developers authenticate once and gain access to the resources defined in their assigned permission sets. This minimizes the number of IAM users and policies that need to be managed.

36. Answer: b) * **Explanation:** AWS CloudTrail logs API calls, including changes to IAM policies. Amazon CloudWatch Events can be used to create rules that trigger based on specific events in CloudTrail logs, such as policy modifications. Amazon SNS can then be used to send notifications when the rule is triggered.

37. Answer: b) * **Explanation:** An SCP that denies the `ec2:CreateVolume` action unless the `Encrypted` parameter is set to `true` effectively prevents the creation of unencrypted EBS volumes at the organization level. This is the most effective way to enforce the policy.

38. Answer: a) * **Explanation:** The web server security group should allow inbound traffic only from the ALB security group on the application port (e.g., 80 or 443). The database server security group should allow inbound traffic only from the web server security group on the database port (e.g., 3306 for MySQL). This configuration ensures that only the web servers can access the database servers and that the web servers can only be accessed through the ALB.

39. Answer: c) * **Explanation:** Using customer-managed keys in a custom key store backed by an AWS CloudHSM cluster allows you to use HSMs under your exclusive control for storing and managing cryptographic keys, meeting the regulatory requirement.

40. Answer: c) * **Explanation:** IAM roles use temporary security credentials that are automatically rotated by AWS. This eliminates the need to manage long-term access keys and improves security by reducing the risk of compromised credentials.