

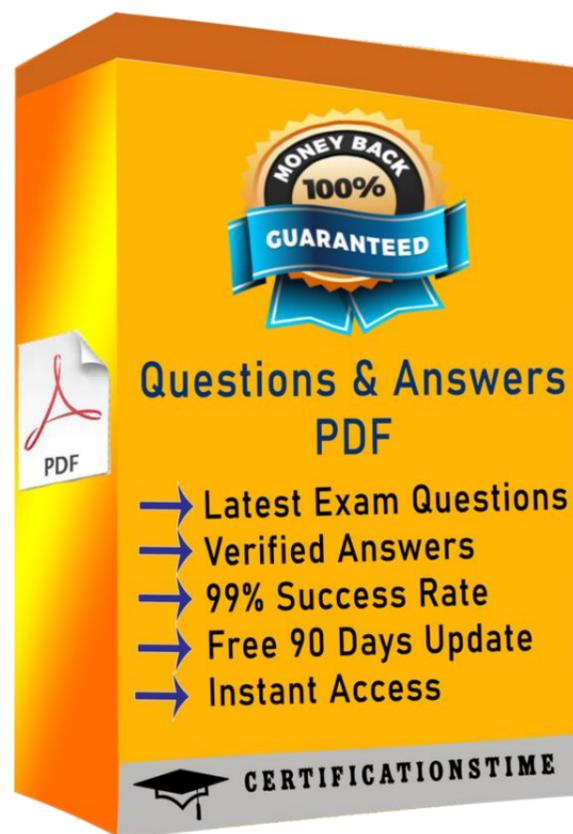


Amazon

AWS-Certified-Security-Specialty

AWS Certified Security Specialty

<https://certificationtime.com/>





QUESTION 1

A global company that deals with International finance is investing heavily in cryptocurrencies and

wants to experiment with mining technologies using AWS. The company's security team has enabled

Amazon GuardDuty and is concerned by the number of findings being generated by the accounts.

The security team wants to minimize the possibility of GuardDuty finding false negatives for

compromised instances that are performing mining

How can the security team continue using GuardDuty while meeting these requirements?

A. In the GuardDuty console, select the CryptoCurrency:EC2/BitcoinTool B'DNS finding and use the suppress findings option

B. Create a custom AWS Lambda function to process newly detected GuardDuty alerts Process the CryptoCurrency EC2/BitcoinTool BIDNS alert and filter out the high-severity finding types only.

C. When creating a new Amazon EC2 Instance, provide the instance with a specific tag that indicates

it is performing mining operations Create a custom AWS Lambda function to process newly detected GuardDuty alerts and filter for the presence of this tag

D. When GuardDuty produces a cryptocurrency finding, process the finding with a custom AWS

Get Certified In First Attempt

visit - <https://certificationstime.com/>



Lambda function to extract the instance ID from the finding Then use the AWS Systems Manager

Run Command to check for a running process performing mining operations

Correct Answer: A

QUESTION 2

After multiple compromises of its Amazon EC2 instances, a company's Security Officer is mandating that memory dumps of compromised instances be captured for further analysis. A Security Engineer just received an EC2 abuse notification report from AWS stating that an EC2 instance running the

most recent Windows Server 2019 Base AMI is compromised.

How should the Security Engineer collect a memory dump of the EC2 instance for forensic analysis?

- A. Give consent to the AWS Security team to dump the memory core on the compromised instance and provide it to AWS Support for analysis.
- B. Review memory dump data that the AWS Systems Manager Agent sent to Amazon CloudWatch Logs.
- C. Download and run the EC2Rescue for Windows Server utility from AWS.
- D. Reboot the EC2 Windows Server, enter safe mode, and select memory dump.

Correct Answer: A

QUESTION 3

A Developer signed in to a new account within an AWS Organizations organizations unit (OU) containing multiple accounts. Access to the Amazon S3 service is restricted with the following SCP:

Get Certified In First Attempt

visit - <https://certificationstime.com/>



How can the Security Engineer provide the Developer with Amazon S3 access without affecting other naccounts?

- A. Move the SCP to the root OU of Organizations to remove the restriction to access Amazon S3.
- B. Add an IAM policy for the Developer, which grants S3 access.
- C. Create a new OU without applying the SCP restricting S3 access. Move the Developer account to this new OU.
- D. Add an allow list for the Developer account for the S3 service.

Correct Answer: B

QUESTION 4

A Security Administrator is restricting the capabilities of company root user accounts. The company uses AWS Organizations and has enabled it for all feature sets, including consolidated billing. The top-level account is used for billing and administrative purposes, not for operational AWS resource purposes.

How can the Administrator restrict usage of member root user accounts across the organization?

- A. Disable the use of the root user account at the organizational root. Enable multi-factor authentication of the root user account for each organizational member account.
- B. Configure IAM user policies to restrict root account capabilities for each Organizations member account.
- C. Create an organizational unit (OU) in Organizations with a service control policy that controls usage of the root user. Add all operational accounts to the new OU.

Get Certified In First Attempt

visit - <https://certificationstime.com/>



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

Correct Answer: C

Explanation/Reference:

Applying a "Control Policy" in your organization. A policy applied to: 1) root applies to all accounts in

the organization 2) OU applies to all accounts in the OU and to any child OUs 3) account applies to one account only Note- this requires that Acquirements: -all features are enabled for the organization

in AWS Organizations -Only service control policy (SCP) are supported

https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies.html

QUESTION 5

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?

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

Get Certified In First Attempt

visit - <https://certificationtime.com/>



Visit and Download Full Version Certificationtime Exam Dumps

<https://certificationtime.com/updated/aws-certified-security-specialty-exam-dumps-pdf/>

Correct Answer: A

Explanation/Reference:

Explanation: <https://stackoverflow.com/questions/45449053/cloudwatch-alert-on-any-instancecreation>

For the Full Access Visit:

<https://certificationtime.com/updated/aws-certified-security-specialty-exam-dumps-pdf/>

Get Certified In First Attempt

visit - <https://certificationtime.com/>