

Exam Session - Knowledge Check: Security (SAA-C03) 2 of 2

 cloudacademy.com/quiz/exam/3792277/results

#1

What is AWS SSO used for?



AWS SSO helps you implement a federated access control system, providing a portal to your users that allows them to access multiple accounts within your AWS organization without having to supply IAM credentials for each one.



AWS SSO is used to centrally manage and categorize multiple AWS accounts that you own, bringing them together into a single organization, helping to maintain your AWS environment from a security, compliance, and account management perspective.




AWS SSO gives you a comprehensive view of your security alerts and security posture across your AWS accounts.



AWS SSO is used to manage access to AWS services and resources securely, by creating and managing AWS users and groups and by using permissions to allow and deny their access to AWS resources.

Explanation

AWS SSO, which stands for Single Sign-On, is used to help you implement a federated access control system, providing a portal to your users that allows them to access multiple accounts within your AWS organization without having to supply IAM credentials for each one.

 [/course/using-aws-sso-simplify-access-across-aws-organization-1563/using-aws-sso-to-simplify-access-across-your-aws-organization/](#)

#2

What is Amazon Macie?



a fully managed service for searching, visualizing, and analyzing up to petabytes of text and unstructured data



a highly available, secure, and managed workflow orchestration platform




a fully managed machine learning and pattern matching service that helps with data security and data privacy



a managed relational database service for MySQL, PostgreSQL, Oracle, SQL Server, and MariaDB

Explanation

Amazon Macie is a fully managed machine learning and pattern matching service that helps with data security and data privacy.

 [/course/find-phi-sensitive-data-s3-buckets-amazon-macie-2307/how-to-find-phi-and-sensitive-data-in-your-s3-buckets-with-amazon-macie/](#)
#3

The Amazon _____ integration with AWS Security Hub allows you to switch back and forth between them to investigate a security finding.



Inspector



GuardDuty



Macie



Detective

Explanation

The Amazon Detective integration allows you to switch back and forth from Security Hub to Detective and investigate a security finding.

 [/course/automating-centralizing-security-checks-aws-security-hub-2287/aws-security-hub-features/](#)

#4

Amazon Cognito _____ help to provide temporary-access AWS credentials for your users or guests that need access to AWS services.



user pools



attributes




identity pools



assertions

Explanation

The Amazon Cognito identity pools, also known as federated identities, help to provide temporary-access AWS credentials for your users or guests that need access to AWS services.

 [/course/using-amazon-cognito-manage-authentication-authorization-mobile-web-apps-1560/identity-pools/](#)

#5

AWS _____ allows you to protect your VPCs from common network threats by implementing fine-grained firewall rules, enabling you to control which traffic is permitted and which should be blocked.



Network Firewall



Resolver DNS Firewall



Shield



WAF

Explanation

AWS Network Firewalls allow you to protect your VPCs from common network threats by implementing fine-grained firewall rules, enabling you to control which traffic is permitted and which should be blocked.



[/course/using-aws-firewall-manager-centrally-manage-firewall-rules-multiple-accounts-2258/policies/](#)

#6

In AWS Web Application Firewall, _____ are used as the component that is associated with one of the supported resources to determine which web requests are considered safe and which ones are not.



web access control lists



rule routers



whitelisted IPs



IP lists

Explanation

Web access control lists, or web ACLs, are the main building block of the WAF service. And an ACL is used as the component that is associated with one of the supported resources to determine which web requests are considered safe and which ones are not.



[/course/protecting-web-apps-common-exploits-using-aws-waf-1883/an-overview-of-aws-waf/](#)

#7

_____ is an open standard for access delegation, commonly used as a way for Internet users to grant websites or applications access to their information on other websites but without giving them the passwords.



Amazon Cognito



Security Assertion Markup Language 2.0 (SAML 2.0)



OAuth



OpenID Connect

Explanation

“OAuth is an open standard for access delegation, commonly used as a way for Internet users to grant websites or applications access to their information on other websites but without giving them the passwords.” - Wikipedia



[/course/using-aws-identity-federation-simplify-access-scale-1549/using-aws-identity-federation-to-simplify-access-at-scale/](#)

#8

Fill in the blanks: During the identity federation process, one party acts as the _____ provider and the other acts as the _____ provider.



OAuth, SAML



identity, service



access, manager



sign-on, authentication

Explanation

During the federation process, one party would act as an identity provider, known as an IdP, and the other would be the service provider, an SP.

 [/course/using-aws-identity-federation-simplify-access-scale-1549/using-aws-identity-federation-to-simplify-access-at-scale/](#)

#9

AWS Security Hub runs continuous, account-level configuration and security checks based on AWS best practices and industry standards, and provides the result of these checks as a(n)

_____.



readiness score



violation score



security graph



alert table

Explanation

Security Hub runs continuous, account-level configuration and security checks based on AWS best practices and industry standards. It provides the result of these checks as a readiness score, and identifies specific accounts and resources that require attention.

 [/course/automating-centralizing-security-checks-aws-security-hub-2287/aws-security-hub-features/](#)

#10

AWS _____ provide(s) a means of centrally managing and categorizing multiple AWS accounts that you own, bringing them together into a single organization, helping to maintain your AWS environment from a security, compliance, and account management perspective.



organizations



categories



accounts



Central

Explanation

For those unfamiliar with AWS organizations, they provide a means of centrally managing and categorizing multiple AWS accounts that you own, bringing them together into a single organization, helping to maintain your AWS environment from a security, compliance, and account management perspective.



[/course/using-aws-identity-federation-simplify-access-scale-1549/using-aws-identity-federation-to-simplify-access-at-scale/](#)

#11

Which is the typical order for rule priorities in AWS Web Application Firewall, from first to last?



1. denylisted IPs
2. bad signatures
3. allowlisted IPs



1. denylisted IPs
2. allowlisted IPs
3. bad signatures




1. bad signatures
2. denylisted IPs
3. allowlisted IPs



1. allowlisted IPs
2. denylisted IPs
3. bad signatures

Explanation

During both of their configurations, the web ACL or rule group, you'll be asked to verify the rule priorities of the rules that have been added. And this is an important point as rules are executed in the order that they are listed. Typically, these are ordered as shown. Firstly, your allowlisted IPs are allowed; you then have your denylisted IPs, which are blocked, and then any bad signatures, which are also blocked.

 </course/protecting-web-apps-common-exploits-using-aws-waf-1883/understanding-rules-and-rule-groups/>
#12

When you are creating a rule in AWS Web Application Firewall, the _____ rule option asks you to enter the maximum number of requests from a single IP within a five-minute timeframe.

✗

IP

✗

count-based

✓

rate-based

✗

regular

Explanation

When you select a rate-based rule option, and as you can see from the image, you are asked to enter the maximum number of requests from a single IP within a five-minute timeframe. When the count limit is reached, the action of the rule is triggered until the request rate falls back below the rate limit specified.

 </course/protecting-web-apps-common-exploits-using-aws-waf-1883/understanding-rules-and-rule-groups/>
#13

The Amazon Inspector service provides which of the following benefits? (Choose 2 answers)

✓

It assesses the exposure of attack points.

✗

It scales and centralizes security management.

✓

It simplifies compliance.

✗

It automates responses to security attacks.

Explanation

The benefits of Amazon Inspector are simplifying security compliance and enforcing security standards.

 </course/amazon-inspector/what-is-amazon-inspector/>

Covered in this lecture

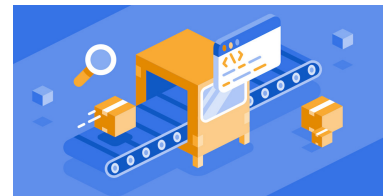
Summary

Course:Amazon Inspector

5m



#14



Which DDoS protection requirements can be satisfied using AWS Shield Standard? (Choose 2 answers)

✗

A web application wants to be protected from DDoS attacks transmitted through Route 53 on the application layer.

✓

A web application hosted on a CloudFront custom origin outside of AWS needs protection on the network layer.

✓

An EC2 web application utilizing Application Load Balancers needs protection from common DDoS attacks on the transport layer.

✗

A web application hosted on Amazon EC2 instances needs to protect its IP addresses from common DDoS attacks over the network and application layers.

Explanation

To answer this question, you should know which network layers AWS Shield Standard can protect and what services it is integrated with.

Scenario 1: A web application wants to be protected from DDoS attacks transmitted through Route 53 on the application layer. AWS Shield is integrated with Route 53, but you need Shield Advanced to protect at the application level.

No, AWS Shield Standard cannot protect resources from traffic over the application layer.

Scenario 2: A web application hosted on a CloudFront custom origin outside of AWS needs protection on the network layer.

Yes, AWS Shield can protect resources from traffic over the transport layer, and because it is integrated with AWS CloudFront, it can protect CloudFront resources, such as custom origins, that are outside of the AWS.

Scenario 3: An EC2 web application utilizing Application Load Balancers needs protection from common DDoS attacks on the transport layer.

Yes, AWS Shield can protect EC2 instances and application load balancers on the transport layer.

A web application hosted on Amazon EC2 instances needs to protect its IP addresses from common DDoS attacks over the network and application layers.

No, AWS Shield would cannot meet these requirements. It does protect EC2 instances, but it does not protect over the application layer.

 </course/protecting-web-apps-aws-waf-shield-firewall-manager/what-is-aws-shield/>

Covered in this lecture

Summary

Course: Protecting Web Apps with AWS WAF, Shield & Firewall Manager

11m



#15



Which of the following lists correctly presents the steps to create an AWS Firewall Manager policy?



1. Choose the policy and region.
2. Describe the policy.
3. Configure policy tags.
4. Define the policy scope.
5. Review and create the policy.



1. Choose the policy and region.
2. Define the policy scope.
3. Describe the policy.
4. Configure policy tags.
5. Review and create the policy.



1. Choose the policy and region.
2. Describe the policy.
3. Define the policy scope.
4. Configure policy tags.
5. Review and create the policy.



1. Configure policy tags.
2. Choose the policy and region.
3. Describe the policy.
4. Define the policy scope.
5. Review and create the policy.

Explanation

The creation of each policy type is generally a five-step process, apart from the Network Firewall Policy, which contains an extra step. So step one, you must choose your policy and region. In this step, you must select which policy you'd like in addition to the region. Step two, describe the policy. So here you need to define the details of the policy, which are dependent on which policy you selected. Step three, define the policy scope. So this step defines which resources and accounts are covered by the policy that you're creating. Step four, configure policy tags. This is an optional step allowing you to associate a resource tag to the policy. Step five, review and create policy.

 [/course/using-aws-firewall-manager-centrally-manage-firewall-rules-multiple-accounts-2258/policies/](#)

#16

Amazon GuardDuty uses data from which of the following AWS services to detect unusual and unexpected behavior? (Choose 3 answers)



AWS CloudTrail event logs



VPC flow logs



DNS logs



CloudWatch Logs

Explanation

Amazon GuardDuty is a regional-based intelligent threat detection service, the first of its kind offered by AWS, which allows users to monitor their AWS account for unusual and unexpected behavior by analyzing AWS CloudTrail event logs, VPC flow logs, and DNS logs. It then uses the data from logs and assesses them against multiple security and threat detection feeds, looking for anomalies and known malicious sources, such as IP addresses and URLs.

</course/understanding-amazon-guardduty/what-is-aws-amazon-guardduty-1/>

Covered in this lecture

What is AWS Amazon GuardDuty?

Course: Understanding Amazon GuardDuty

4m



#17

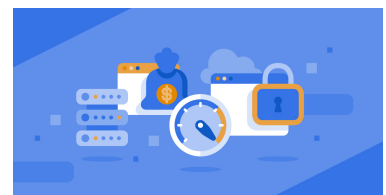
Amazon Cognito is a(n) _____ service.



secrets management



threat detection





authentication and user management



key management

Explanation

At its core, Amazon Cognito is an authentication and user management service.



[/course/using-amazon-cognito-manage-authentication-authorization-mobile-web-apps-1560/cognito-lecture-three/#18](#)

What does Amazon GuardDuty look for?



anomalies and known malicious sources



personally identifiable information (PII)



specific violations of HIPAA



specific violations of GDPR

Explanation

Amazon GuardDuty is a region-based intelligent threat detection service, the first of its kind offered by AWS, which allows users to monitor the AWS account for unusual and unexpected behavior by analyzing CloudTrail event logs, VPC flow logs, and DNS logs. It then uses the data from these logs and assesses them against multiple security and threat detection feeds, looking for anomalies and known malicious sources, such as IP addresses and URLs.



[/course/managing-findings-from-multiple-accounts-using-amazon-guardduty/managing-findings-from-multiple-accounts-using-amazon-guardduty/#19](#)

Which of the following practices is a prerequisite that you must meet before you configure and enable AWS SSO within your accounts?



Manage your users with the default identity user store that comes natively with AWS SSO.



Use a member AWS account of your AWS organization to enable and configure AWS SSO.




Configure AWS Organizations for your accounts using the "All features" option rather than "Consolidated billing features."



Use an external identity pool supported by AWS SSO with SAML 2.

Explanation

There are a number of prerequisites that you must meet before you configure and enable AWS SSO within your accounts. The first of these requires you to configure AWS Organizations for your accounts using the "All features" option rather than just "Consolidated billing features." You must also use the management AWS account of your AWS organization to enable and configure AWS SSO.

 [/course/using-aws-sso-simplify-access-across-aws-organization-1563/using-aws-sso-to-simplify-access-across-your-aws-organization/](#)

#20

Which AWS service can assess the security state of your applications running on EC2 instances?



Amazon GuardDuty



Amazon CloudTrail




Amazon Inspector



Amazon EventBridge

Explanation

Amazon Inspector is an automated security service that can assess your network and the accessibility of your Amazon EC2 instances. Additionally, Amazon Inspector can also assess the security state of your applications running on those instances.

 [/course/aws-incident-response-isolating-your-ec2-instances-2454/isolation-of-your-ec2-instances/](#)

#21

Amazon Cognito _____ allow(s) users to pick up where they left off in your application when switching devices.



Sync



OAuth



user pools



identity pools

Explanation

Amazon Cognito answers another question that many web and mobile applications developers will need help with on some level: the question of how to sync your application's user data across various platforms. This allows the users to pick up where they left off when switching devices. Amazon Cognito Sync can help take care of these data points for you, instead of you having to create your own backend that you would need to maintain and manage yourself.

 [/course/using-amazon-cognito-manage-authentication-authorization-mobile-web-apps-1560/amazon-cognito-sync/](#)

#22

AWS _____ is designed to help protect your infrastructure against distributed denial of service attacks, commonly known as DDoS.



Network Firewall



Resolver DNS Firewall



Shield



WAF

Explanation

Shield Advanced Policy: The AWS Shield service is designed to help protect your infrastructure against distributed denial of service attacks, commonly known as DDoS.



[/course/using-aws-firewall-manager-centrally-manage-firewall-rules-multiple-accounts-2258/policies/](#)

#23

AWS Shield Standard offers DDoS protection against which layer(s) of attacks?



three only



seven only



three, four, and seven



three and four

Explanation

AWS Shield Standard is free to everyone--well, at least anyone who has an AWS account--and it offers DDoS protection against some of the more common layer three, or the network layer, and layer four, or the transport layer, DDoS attacks.



[/course/introduction-to-waf-firewall-manager-shield-1136/what-is-shield/](#)

Covered in this lecture

What is AWS Shield?

Course:Introduction to AWS WAF, Firewall Manager & Shield

4m



#24



What does AWS Security Hub do?



It lets you analyze your deployed EC2 instances to identify potential security issues.



It provides an intelligent threat detection service that allows you to consistently monitor and protect your AWS accounts and workloads for suspicious activity.



It consolidates security findings and alerts across accounts and provider products and displays the results in a single dashboard.



It uses machine learning to help you discover and analyze sensitive data stored in Amazon S3 buckets.

Explanation

AWS Security Hub allows you to start consolidating security findings and alerts across accounts and provider products and display results in a single dashboard.



</course/automating-centralizing-security-checks-aws-security-hub-2287/aws-security-hub-features/>

#25

What is the core function of AWS Firewall Manager?



to rotate, manage, and retrieve secrets



to provision, manage, and deploy SSL/TLS certificates




to provide identity management for your apps



to help you simplify the management of security protection to a range of different resources, between multiple AWS accounts

Explanation

The core function of AWS Firewall Manager is to help you simplify the management of being able to provide security protection to a range of different resources, between multiple AWS accounts.

 [/course/using-aws-firewall-manager-centrally-manage-firewall-rules-multiple-accounts-2258/aws-firewall-manager-and-prerequisites/](#)