AWS SECURITY SERVICES

14 March 2024 13:41

1. DDoS Attack Overview:
    - DDoS stands for Distributed Denial of Service, aimed at making a website or application unavailable to users.
    - It can be achieved through mechanisms like large packet floods, reflection, and amplification techniques using botnets.
2. Layer 4 DDoS Attack (SYN Flood):
    - Operates at the transport layer (TCP) and exploits the three-way handshake process.
    - Overwhelms servers with a large number of SYN packets, ignoring SYN-ACK responses, exhausting server resources.
3. Amplification Attacks:
    - Utilize third-party servers (e.g., NTP, DNS) to amplify attack traffic.
    - Attackers send requests with spoofed IP addresses, and servers respond with larger payloads, creating traffic amplification.
4. Layer 7 DDoS Attack:
    - Occurs at the application layer (HTTP) and involves flooding servers with GET or POST requests.
    - Typically carried out using botnets or compromised computers.
5. Exam Tips:
    - Understand the nature of DDoS attacks and their goal of rendering services unavailable.
    - Differentiate between Layer 4 (SYN Flood) and Layer 7 (HTTP flood) attacks.
    - Know about amplification attacks and how they leverage third-party servers.
    - Recognize the need for different mitigation strategies for Layer 4 and Layer 7 attacks, which will be covered in subsequent lectures.

1. CloudTrail Overview:
    - CloudTrail records AWS management console actions and API calls, providing visibility into user and resource activity.
    - It captures details such as the user or account that made the API call, the time of the call, the source IP address, request parameters, and response elements.
2. How CloudTrail Works:
    - CloudTrail monitors API calls made to the AWS cloud, including actions like provisioning resources (e.g., EC2 instances, S3 buckets) and managing services (e.g., DynamoDB tables).
    - It logs this activity in S3 buckets, allowing for incident investigation, intrusion detection, and compliance auditing.
3. Exam Tips:
    - Understand that CloudTrail acts as a monitoring and logging tool for API calls and AWS management console actions.
    - Differentiate CloudTrail from other AWS services like CloudWatch, Amazon Inspector, and Trusted Advisor.
    - Remember that CloudTrail logs are stored in S3 and can be used for incident investigation, intrusion detection, and compliance auditing.
    - Be prepared for scenario-based questions in the exam that may involve distinguishing CloudTrail from other AWS services or understanding its use cases.

1. AWS Shield Overview:
    - AWS Shield provides free DDoS protection for all AWS customers on Elastic Load Balancers, Amazon CloudFront, and Route 53.
    - It defends against common DDoS attack types, including SYN or UDP floods, reflection attacks, and other Layer 3 and Layer 4 attacks.
2. AWS Shield Advanced:
    - AWS Shield Advanced offers enhanced protection against larger and more sophisticated attacks.
    - It provides always-on flow-based monitoring of network traffic and real-time notifications of DDoS attacks.
    - Subscribers have access to the DDoS Response Team (DRT) for 24/7 assistance in managing and mitigating application layer DDoS attacks.
    - Shield Advanced also protects against higher fees resulting from usage spikes during DDoS attacks.
3. Costs:
    - AWS Shield is free for all AWS customers.
    - AWS Shield Advanced costs $3,000 USD per month.
4. Enabling Shield Advanced:
    - To subscribe to Shield Advanced, navigate to the AWS Management Console, select Shield under WAF and Shield, and click "Subscribe to Shield Advanced."
    - Tick the required boxes and hit "Subscribe" to enable Shield Advanced.
5. Exam Tips:
    - Understand the difference between AWS Shield and AWS Shield Advanced.
    - Remember that Shield protects against Layer 3 and Layer 4 attacks, while AWS WAF (Web Application Firewall) is used for application-level attacks.
    - Shield Advanced provides additional features and access to a dedicated DDoS Response Team.
    - Be prepared for scenario-based questions related to DDoS protection and mitigation in the exam.

   Knowing the features and differences between AWS Shield and AWS Shield Advanced is crucial for protecting applications against DDoS attacks in AWS environments. If you have any questions, feel free to ask, otherwise, you can proceed to the next lecture. Thank you!>

1. AWS WAF Overview:
    - AWS WAF stands for Web Application Firewall, and it allows you to monitor HTTP and HTTPS requests forwarded to Amazon CloudFront or an Application Load Balancer.
    - It enables you to control access to your content by configuring conditions such as IP addresses allowed to make requests, required query string parameters, and more.
    - AWS WAF operates at Layer 7 of the OSI model, making it suitable for protecting against layer 7 attacks such as SQL injection and cross-site scripting.
2. Behaviors:
    - AWS WAF allows three main behaviors: allow all requests except the ones specified, block all requests except the ones specified, or count the requests that match specified properties without taking action.
3. Conditions:
    - Conditions can be defined based on various characteristics of web requests, including IP addresses, country of origin, request headers, presence of SQL code or scripts, and specific string patterns or regex patterns.
4. Exam Tips:
    - Remember that AWS WAF operates at Layer 7, making it suitable for protecting

against layer 7 attacks.
- In exam scenarios involving layer 7 attacks or the need to filter web traffic based on specific criteria, consider using AWS WAF.
- AWS WAF can block layer 7 DDoS attacks, SQL injections, cross-site scripting, and can also be used to block access from specific countries or IP addresses.

Understanding the capabilities of AWS WAF and its use cases is important for securing web applications in AWS environments. If you have any questions, feel free to ask, otherwise, you can proceed to the next lecture. Thank you!

1. GuardDuty Overview:
   - GuardDuty is a threat detection service that employs machine learning to detect malicious activity in AWS accounts.
   - It monitors various sources of data, including CloudTrail logs, VPC Flow Logs, and DNS logs, to identify suspicious behavior such as unusual API calls, unauthorized deployments, compromised instances, and reconnaissance activities.
   - GuardDuty alerts appear in the GuardDuty console and can also be delivered via CloudWatch Events.
2. Features:
   - GuardDuty receives feeds from third-party sources like Proofpoint and CrowdStrike, enhancing its threat detection capabilities with known malicious domains and IP addresses.
   - It allows centralized threat detection across multiple AWS accounts and provides automated responses through CloudWatch Events and Lambda functions.
   - GuardDuty leverages machine learning and anomaly detection to establish a baseline of normal behavior in the AWS environment, which typically takes 7 to 14 days to set up.
3. Pricing:
   - GuardDuty offers a 30-day free trial, after which charges are based on the quantity of CloudTrail events and the volume of DNS and VPC Flow Logs data.
4. Exam Tips:
   - Understand that GuardDuty utilizes AI and machine learning to detect abnormal or malicious behavior in AWS accounts, alerting users through the GuardDuty console and CloudWatch Events.
   - GuardDuty integrates with various AWS services, including CloudTrail, VPC Flow Logs, and DNS logs, to provide comprehensive threat detection.
   - CloudWatch Events can be used to trigger automated responses, such as Lambda functions, to address detected threats proactively.
   - In exam scenarios involving the use of AI and automation for threat detection and monitoring in AWS environments, consider AWS GuardDuty as the appropriate service.

Remembering the capabilities and features of AWS GuardDuty is essential for effectively detecting and responding to security threats in AWS accounts. If you have any questions, feel free to ask, otherwise, you can proceed to the next lecture. Thank you!

1. Firewall Manager Overview:
   - Firewall Manager is a security management service provided by AWS.
   - It offers a single pane of glass for managing firewall rules across multiple AWS accounts and applications within AWS organizations.
2. Features:
   - With Firewall Manager, you can create and manage AWS WAF rules for application load balancers, API gateways, CloudFront distributions, and more.
   - It enables the mitigation of DDoS attacks using AWS Shield Advanced for various resources such as application load balancers, Elastic IP addresses, CloudFront distributions, etc.
3. Benefits:

- Centralized management: Firewall Manager simplifies the management of firewall rules across multiple AWS accounts.
- Compliance enforcement: It automatically enforces security policies across existing and newly created resources, ensuring compliance with organizational security standards.

4. Exam Tips:
   - Understand that Firewall Manager provides a centralized solution for managing firewall rules across multiple AWS accounts and applications.
   - In exam scenarios involving the need to secure resources centrally across AWS organizations, consider AWS Firewall Manager as the appropriate service.
   - Firewall Manager integrates with AWS WAF and AWS Shield Advanced to provide comprehensive security management capabilities.

   Remembering the capabilities and benefits of AWS Firewall Manager is essential for effectively managing security across multiple AWS accounts and applications. If you have any questions, feel free to ask, otherwise, you can proceed to the next lecture. Thank you!

1. What is Macie?
   - Macie is a service that uses machine learning and pattern matching to automatically analyze data stored in S3 buckets.
   - It identifies sensitive data such as PII, PHI, and financial information, helping organizations ensure compliance with regulations like HIPAA and GDPR.
2. Personally Identifiable Information (PII):
   - PII includes personal data used to establish an individual's identity, such as name, address, social security number, passport number, etc.
   - Macie helps identify and classify PII stored in S3 buckets, helping organizations prevent data breaches and identity theft.
3. Automated Analysis of Data:
   - Macie uses AI to recognize sensitive data within S3 objects and alerts users about unencrypted or public buckets.
   - It can also detect buckets shared with AWS accounts outside the defined AWS organizations.
4. Macie Alerts and Integration:
   - Macie alerts can be filtered and searched in the AWS console.
   - Alerts are sent to Amazon EventBridge and can be integrated with security incident and event management systems.
   - Integration with AWS Security Hub allows for broader analysis of an organization's security posture.
   - Remediation actions can be automated using AWS services like Step Functions.
5. Exam Tips:
   - Understand that Macie is an automated solution for discovering and classifying sensitive data in S3 buckets.
   - It helps organizations comply with regulations like HIPAA and GDPR and prevent data leaks and identity theft.
   - Macie alerts can be integrated with various AWS services for automated response and remediation actions.
   - In exam scenarios involving the protection of sensitive data in S3, consider Macie as a solution for automated data analysis and alerting.

   Remembering the capabilities and benefits of AWS Macie is crucial for effectively monitoring and protecting sensitive data stored in S3 buckets. If you have any questions, feel free to ask, otherwise, you can proceed to the next lecture. Thank you!

From <https://chat.openai.com/c/d6fe90a1-a00b-4374-9bfc-54c5891880f3>

1. What is Amazon Inspector?
    - Amazon Inspector is an automated security assessment service that helps identify vulnerabilities or deviations from best practices in applications deployed on AWS.
    - It inspects EC2 instances and network configurations for security issues and compliance violations.
2. Assessment Findings and Types:
    - After performing an assessment, Inspector generates detailed security findings prioritized by severity level.
    - There are two types of assessments:
        - Network assessments: Analyze network configurations to identify open ports and vulnerabilities accessible from outside the VPC. No agent installation is required for network assessments.
        - Host assessments: Evaluate the security of EC2 instances by checking for vulnerable software and adherence to security best practices. An agent is installed on the EC2 instances for host assessments.
3. How it Works:
    - To use Inspector, you create an assessment target and install agents on EC2 instances (if performing host assessments).
    - Assessment templates are created to specify the rules and parameters for the assessment.
    - Assessment runs are performed based on the templates, and findings are reviewed in the Inspector dashboard or via API.
    - Inspector provides detailed reports on assessment findings, including severity levels and recommendations for remediation.
4. Exam Tips:
    - Understand that Inspector is used for vulnerability scans on EC2 instances and network configurations.
    - Host assessments require the installation of an agent on EC2 instances, while network assessments do not.
    - Inspector generates detailed findings reports prioritized by severity level.
    - If exam scenarios involve identifying vulnerabilities or compliance violations in AWS resources, consider AWS Inspector as a solution.

Remembering the capabilities and usage of AWS Inspector is essential for ensuring the security and compliance of applications deployed on AWS. If you have any questions, feel free to ask, otherwise, you can proceed to the next lecture. Thank you!

From <https://chat.openai.com/c/d6fe90a1-a00b-4374-9bfc-54c5891880f3>

AWS Key Management Service (KMS):

- KMS is a managed service that simplifies the creation and management of encryption keys used to encrypt data.
- It integrates with various AWS services such as EBS, S3, and RDS to enable easy encryption of data.
- With KMS, you have centralized control over the lifecycle and permissions of your encryption keys.
- Customer Master Keys (CMKs) are logical representations of master keys that include metadata and key material.
- You can generate CMKs in three ways: AWS creates the CMK for you, import key material from your own infrastructure, or use AWS CloudHSM for custom key store.
- Key policies are used to control access to CMKs, and there are three ways to manage permissions: key policy, IAM policies, and grants.
- Automatic key rotation is supported for CMKs generated within AWS KMS HSMs but not for imported keys or keys in AWS CloudHSM clusters.

AWS CloudHSM:

- AWS CloudHSM is a cloud-based hardware security module that allows you to generate and use your own encryption keys on the AWS Cloud.
- It provides dedicated HSMs for customers, offering full control over the underlying hardware.
- Unlike KMS, CloudHSM does not support automatic key rotation, but it offers complete control over users, groups, and keys.

Exam Tips:

- Understand the purpose of KMS and how it simplifies the management of encryption keys.
- Know the three ways to generate CMKs in KMS: AWS-generated, import key material, or using AWS CloudHSM.
- Be familiar with key policies and the three methods of controlling permissions in KMS.
- Differentiate between KMS and CloudHSM in terms of shared tenancy, key rotation, and control over hardware.
- Remember the scenarios where KMS or CloudHSM might be preferred based on the level of control and automation required.

By mastering the concepts of KMS and CloudHSM, you'll be well-prepared to manage encryption keys effectively on AWS. If you have any questions, feel free to ask, otherwise, you can proceed to the next lecture. Thank you!

From <https://chat.openai.com/c/d6fe90a1-a00b-4374-9bfc-54c5891880f3>

AWS Secrets Manager:

- Secrets Manager securely stores, encrypts, and rotates sensitive information such as database credentials, API keys, SSH keys, and passwords.
- It offers encryption in-transit and at-rest using AWS Key Management Service (KMS), ensuring that secrets are always encrypted.
- Secrets Manager automatically rotates credentials, enhancing security by regularly updating secrets.
- Fine-grained access controls can be applied using IAM policies to restrict access to stored secrets.
- It provides an API that applications can use to programmatically retrieve secrets, reducing the risk of credentials being compromised compared to hardcoding them in applications.

Storing Secrets:

- Secrets Manager can store various types of secrets, including RDS credentials, credentials for non-RDS databases, and any other type of secret provided as a key-value pair.
- When enabling rotation for secrets, Secrets Manager immediately rotates the secrets once to test the configuration. It's crucial to ensure that all applications using the credentials are updated to retrieve them from Secrets Manager before enabling rotation.

Exam Tips:

- Understand the purpose of Secrets Manager in securely storing application secrets and automatically rotating credentials.
- Know the types of secrets that can be stored in Secrets Manager, including database credentials, API keys, SSH keys, and passwords.
- Be aware of the process and considerations when enabling rotation for secrets, especially regarding updating applications to retrieve credentials from Secrets Manager before rotation.
- Secrets Manager is an essential service for maintaining the security of sensitive information in AWS environments.

By mastering the concepts of Secrets Manager, you'll be well-prepared to securely manage and rotate secrets for your applications on AWS. If you have any questions, feel free to ask, otherwise, you can proceed to the next lecture. Thank you!

Parameter Store:

- Parameter Store is a capability of AWS Systems Manager that provides secure, hierarchical storage for configuration data management and secrets management.
- It allows storing various types of data, including passwords, database strings, Amazon Machine Image IDs, and license codes, as parameter values.
- Parameter Store supports storing values as plain text or encrypted data.
- Unlike Secrets Manager, Parameter Store is free to use.

Limitations:

- There are limitations to consider when using Parameter Store:
  - A maximum limit of 10,000 parameters that can be stored.
  - Parameter Store does not support key rotation.

Exam Tips:

- When faced with scenario-based questions in the exam where you need to choose between Parameter Store and Secrets Manager:
  - If cost optimization is a priority and the number of parameters needed is within the limit of 10,000, Parameter Store is the preferable choice.
  - If key rotation, the need for more than 10,000 parameters, or features like generating passwords using CloudFormation are required, Secrets Manager should be used.

Understanding the differences between Parameter Store and Secrets Manager, along with their respective use cases and limitations, is crucial for making informed decisions in AWS environments and for exam preparation.
That concludes the lecture on Parameter Store. If you have any questions, feel free to ask, or you can proceed to the next lecture. Thank you!

Privacy and Access:

- All objects in S3 are private by default, and only the object owner has permission to access them.
- Presigned URLs provide time-limited access to S3 objects by granting temporary permissions to download them.
- Anyone who receives the presigned URL can access the object during the specified duration.

Presigned URLs vs. Presigned Cookies:

- Presigned URLs are suitable for sharing individual files, whereas presigned cookies are useful for providing access to multiple restricted files.
- Presigned cookies are stored on the user's computer, allowing them to browse the entire contents of the restricted content.

Generating a Presigned URL:

- Presigned URLs can be generated using the AWS CLI or programmatically.
- The URL includes the bucket name, object key, expiration date and time, and optionally, the HTTP method.

Exam Tips:

- When faced with scenario-based questions where you need to share private files in S3, consider using presigned URLs.
- Presigned URLs are easy to generate and provide temporary access to S3 objects.
- You can set the expiration date for the presigned URL, typically in seconds.

Understanding how to use presigned URLs effectively is essential for managing access to S3 objects securely. If you have any questions, feel free to ask, or you can proceed to the next lecture. Thank you!

From <https://chat.openai.com/c/d6fe90a1-a00b-4374-9bfc-54c5891880f3>

Amazon Resource Names (ARNs):

- ARNs uniquely identify AWS resources and follow a specific syntax:

arn:partition:service:region:account_id:resource.

- The partition identifies the AWS partition (e.g., AWS or AWS China).
- Services represent the AWS service (e.g., IAM, S3, DynamoDB).
- Regions specify the AWS region (e.g., us-east-1, eu-central-1).
- Account ID is the 12-digit AWS account number.
- Resources represent the specific resource within the service.

IAM Policies:

- IAM policies are JSON documents that define permissions.
- Policies consist of statements, each of which matches an AWS API request.
- Statements include the SID (Statement ID), effect (allow or deny), actions, resources, and conditions.
- Policies can be attached to IAM identities (identity policies) or AWS resources (resource policies).

Permission Boundaries:

- Permission boundaries delegate administration to other users and prevent privilege escalations.
- They control the maximum permissions that an IAM policy can grant.
- Use cases include restricting developer access to specific services and allowing application owners to create roles for their resources.

Exam Tips:

- Practice reading and understanding IAM policies, as you may encounter scenario-based questions on the exam.
- Remember the implicit deny principle: if an action is not explicitly allowed, it's implicitly denied.
- Explicit deny always takes precedence over explicit allow.
- Policies must be attached to IAM identities or resources to take effect.
- You can have multiple policies attached to a single resource, with AWS evaluating all applicable policies.

Understanding these advanced IAM concepts is crucial for designing secure and granular access control in AWS environments.

From <https://chat.openai.com/c/d6fe90a1-a00b-4374-9bfc-54c5891880f3>

AWS Certificate Manager (ACM):

- ACM allows you to create, manage, and deploy public and private SSL/TLS certificates for use with AWS services.
- It integrates seamlessly with other AWS services such as Elastic Load Balancing, CloudFront distributions, and API Gateway.
- ACM simplifies SSL certificate management and deployment in your AWS environment.

Benefits of AWS Certificate Manager:

- Cost: ACM provides SSL certificates for free, eliminating the need to purchase certificates from third-party providers.
- Automation: ACM automates the renewal and deployment of SSL certificates, reducing manual effort.
- Easy Setup: ACM makes it easy to create SSL certificates with just a few clicks in the AWS Management Console.

Exam Tips:

- Understand what ACM is and its primary purpose: managing SSL certificates for AWS services.
- Be familiar with the supported AWS services for integrating SSL certificates, such as Elastic Load Balancer, CloudFront, and API Gateway.
- Remember the benefits of ACM, including cost savings, automation of certificate renewal, and ease of setup.
- Expect scenario-based questions related to SSL certificate management and integration with AWS services on the exam.

Overall, AWS Certificate Manager is a valuable tool for securing your AWS resources with SSL/TLS certificates while minimizing costs and manual effort

From <https://chat.openai.com/c/d6fe90a1-a00b-4374-9bfc-54c5891880f3>

AWS Audit Manager:

- AWS Audit Manager is a service that enables continuous auditing of your AWS usage to ensure compliance with industry standards and regulations.
- It automates the process of producing reports specific to auditors for various compliance frameworks such as PCI, GDPR, HIPAA, etc.
- Audit Manager facilitates the transition from manual to automated evidence collection, reducing the need for manual report compilation and revisiting audits periodically.

Use Cases:

- Continuous Auditing: Audit Manager continuously evaluates your AWS environment against industry standards and regulations, providing automated reports to assess compliance.
- Automated Report Generation: It automates the generation of reports for auditors, helping validate compliance with internal policies and external regulations.
- Internal Risk Assessments: Audit Manager allows you to create or customize pre-built frameworks for assessing internal risk and compliance, launching assessments to collect evidence and validate policy adherence.

Exam Tips:

- Understand the purpose of AWS Audit Manager: continuous auditing and compliance monitoring for AWS environments.
- Be familiar with the use cases of Audit Manager, particularly its role in automating report generation, facilitating internal risk assessments, and ensuring compliance with industry standards and regulations.
- Expect scenario-based questions related to continuous auditing, compliance, and adherence to industry standards such as PCI, GDPR, HIPAA, etc., on the exam.

Overall, AWS Audit Manager is a valuable tool for organizations seeking to maintain compliance with industry standards and regulations by automating the auditing process and generating reports for auditors

From <https://chat.openai.com/c/d6fe90a1-a00b-4374-9bfc-54c5891880f3>

AWS Artifact:

- AWS Artifact is a centralized source where users can access compliance-related information, including AWS security and compliance reports, as well as select online agreements.
- It provides various compliance reports such as AWS SOC reports, PCI reports, GDPR reports, ISO reports, HIPAA reports, and more.

Demonstration:

- In the AWS Management Console, users can navigate to AWS Artifact by searching for it.
- Within AWS Artifact, users can search for specific compliance reports by typing keywords such as PCI.
- Users can then select and download the desired compliance report.

Exam Tips:

- Understand the purpose of AWS Artifact: a centralized source for accessing compliance-related information and reports.
- Know the available compliance documents, including SOC reports, PCI reports, GDPR reports, ISO reports, HIPAA reports, and more.
- Recognize that AWS Artifact may appear in exam questions related to audits and the

need to download compliance reports. If compliance reports are not mentioned in the scenario, Artifact is likely a distractor.
Overall, AWS Artifact provides users with easy access to compliance-related documents and reports, simplifying the process of obtaining and sharing compliance information.

From <https://chat.openai.com/c/d6fe90a1-a00b-4374-9bfc-54c5891880f3>

Amazon Cognito:

- Amazon Cognito is a service that provides authentication, authorization, and user management for web and mobile applications without requiring custom code.
- Users can sign in directly with a username and password or via third-party identity providers such as Facebook, Amazon, Google, or Apple.
- Key features include sign-up and sign-in options, access for guest users, identity brokering, synchronization of user data across devices, and integration with AWS services.

User Pools and Identity Pools:

- User pools are directories of users that provide sign-up and sign-in options.
- Identity pools allow users to access other AWS services.
- User pools and identity pools can be used separately or together.

How it Works:

- The device sends a login request to the login provider, which validates the user's credentials.
- Once authenticated, the device sends a GetId request to Amazon Cognito to obtain an identity ID.
- Cognito exchanges the identity ID for temporary AWS credentials using AssumeRoleWithWebIdentity, allowing access to AWS services.

Exam Tips:

- Understand the purpose of user pools and identity pools in Cognito.
- Know the sequence of events: device authentication with user pool, token exchange with identity pool, and obtaining AWS credentials.
- User pools provide sign-up and sign-in options, while identity pools allow access to other AWS services.
- Familiarize yourself with Cognito's use cases and features, as they may appear in exam questions.

Overall, Amazon Cognito simplifies the authentication and authorization process for web and mobile applications, integrating with various identity providers and AWS services

From <https://chat.openai.com/c/d6fe90a1-a00b-4374-9bfc-54c5891880f3>

Amazon Detective:

- Amazon Detective enables users to analyze, investigate, and identify the root cause of potential security issues or suspicious activities in their AWS environment.
- It leverages machine learning, statistical analysis, and graph theory to build a linked set of data from AWS resources, aiding in the rapid identification of security issues.

Data Sources:

- Detective pulls data from various sources within the AWS account, including VPC Flow Logs, CloudTrail logs, EKS audit logs, and Amazon GuardDuty findings.

Use Cases:

- Triage Security Findings: Detective helps users quickly assess suspected security incidents by generating visualizations that show the connections between resources, IP addresses, and AWS accounts to determine if findings are genuine threats or false positives.
- Threat Hunting: Users can proactively search for potential security threats by utilizing Detective's detailed visualizations on specific resources, such as IP addresses, AWS accounts, VPCs, and EC2 instances.

Exam Tips:

- Understand that Detective analyzes the root cause of security events and helps in determining if an event is a genuine security threat or a false positive.
- Look for the term "root cause" in scenario-based questions to identify Detective as a potential solution.
- Differentiate Detective from Amazon Inspector, which focuses on automated vulnerability management for EC2 and container workloads.

Overall, Amazon Detective provides a powerful tool for security analysis and investigation, leveraging advanced techniques to identify and address potential security issues in AWS environments.

From <https://chat.openai.com/c/d6fe90a1-a00b-4374-9bfc-54c5891880f3>

AWS Network Firewall:

- AWS Network Firewall is a managed service that simplifies the deployment of physical firewall protection across VPCs.
- It includes firewall rules engines for complete control over network traffic, allowing actions like blocking outbound Server Message Block (SMB) requests to prevent malicious activity spread.

Benefits:

- Managed Infrastructure: AWS handles the management of physical firewall infrastructure, reducing management overhead for users.
- Integration with AWS Firewall Manager: Allows centralized management of security policies across accounts and VPCs.
- Intrusion Prevention System (IPS): Provides active traffic flow inspection, filtering internet traffic using methods like access control lists, stateful inspection, protocol detection, and intrusion prevention.

Use Cases:

- Filtering Internet Traffic: Network Firewall enables filtering of internet traffic using various methods, including access control lists and intrusion prevention, to prevent data loss and block known malware communications.
- Filtering Outbound Traffic: Provides outbound traffic filtering based on URL/domain name, IP address, and content to prevent data loss and block malicious communications.
- Inspecting VPC-to-VPC Traffic: Automatically inspects traffic moving between VPCs, as well as across multiple accounts, enhancing security and preventing unauthorized access.

Exam Tips:

- If a scenario question involves filtering network traffic before it reaches the internet gateway or requires intrusion prevention systems or hardware firewall requirements, consider AWS Network Firewall as a solution.

Overall, AWS Network Firewall offers robust protection for VPCs by simplifying the deployment and management of physical firewall protection and providing advanced features for traffic filtering and intrusion prevention.

AWS Security Hub:

- AWS Security Hub is a centralized platform for viewing security alerts from various AWS security services like Amazon GuardDuty, Amazon Inspector, Amazon Macie, and AWS Firewall Manager.
- It provides a single pane of glass for monitoring security alerts across multiple AWS accounts, enabling effective security management and threat detection.

Use Cases:

- Cloud Security Posture Management (CSPM): Security Hub offers automated checks compliant with common security frameworks like the Center for Information Security

(CIS) and PCI DSS. This enables users to ensure compliance and identify security issues proactively.

- Correlating Security Findings: By aggregating security findings from different services into one place, Security Hub allows security staff to correlate findings and gain new insights, facilitating better threat identification and response.

Exam Tips:

- If a scenario question involves the need for a single platform to view security alerts from various AWS security services across multiple accounts, consider AWS Security Hub as the solution.
- Remember that Security Hub helps with CSPM by offering automated compliance checks and facilitates the correlation of security findings for improved threat detection.

Overall, AWS Security Hub serves as a vital tool for managing and monitoring security alerts across AWS environments, enhancing security posture, and enabling efficient threat detection and response.

From <https://chat.openai.com/c/d6fe90a1-a00b-4374-9bfc-54c5891880f3>

DDoS Protection:

- DDoS attacks aim to make websites or applications unavailable.
- Common attacks include Layer 4 (SYN floods) and Layer 7 (GET/POST request floods).

CloudTrail:

- CloudTrail provides logging of API calls made to AWS services for incident investigation and compliance purposes.

Shield:

- AWS Shield protects against DDoS attacks, particularly Layer 3 and Layer 4 attacks.

WAF (Web Application Firewall):

- WAF operates at Layer 7 and can block various attacks like SQL injections and cross-site scripting.

Firewall Manager:

- AWS Firewall Manager centrally manages security policies across multiple AWS accounts and resources.

GuardDuty:

- GuardDuty uses AI to identify abnormal or malicious behavior in AWS environments.

Macie:

- Macie uses AI to analyze data in S3 and helps identify sensitive information for compliance and security purposes.

Inspector:

- Inspector performs vulnerability scans on EC2 instances and VPCs.

KMS (Key Management Service) and CloudHSM:

- KMS provides managed encryption key services, while CloudHSM offers dedicated hardware for key management.

Secrets Manager:

- Secrets Manager securely stores application secrets and supports credential rotation.

Parameter Store:

- Parameter Store is used for storing configuration data and secrets.

Presigned URLs:

- Presigned URLs are used for granting temporary access to private S3 objects.

IAM Policies:

- IAM policies control access to AWS resources, and you must understand their precedence rules and types.

Certificate Manager:

- ACM provides SSL certificates for use with AWS services, with automated renewal and integration.

Audit Manager:

- Audit Manager provides continuous auditing for compliance purposes.

Artifact:

- AWS Artifact provides compliance reports for audits.

Cognito:

- Cognito offers authentication and user management services for web and mobile apps.

Detective:

- Detective analyzes security data across AWS services to identify root causes of security issues.

Network Firewall:

- AWS Network Firewall provides managed protection against Layer 3 and Layer 4 attacks.

Security Hub:

- Security Hub is a centralized platform for viewing security alerts from various AWS security services across multiple accounts.

From <https://chat.openai.com/c/d6fe90a1-a00b-4374-9bfc-54c5891880f3>