Security

AWS being the only commercial cloud that is the most flexible and secure cloud computing environment available today. AWS allows you to automate manual security tasks so you can shift your focus to scaling and innovating your business.

https://aws.amazon.com/security/

>DDOS Overview

DDoS (Distributed Denial of Service) is an attack that attempts to make websites or applications unavailable to your end users.

- Layer 4 DDoS attack
  - Layer 4 is the transport layer (This is also referred to a SYN flood – TCP)
  - TCP 3-way handshake
    - After this is complete the TCP connection is established. The application will then start sending data using layer 8 (application layer) such as HTTP, etc.
- SYN Floods
  - Built in patience of the TCP stack to overwhelm a server by sending larger number of SYN packets, which of course causes the server to soak up resources

When the SYN flood attack is in process, it is trying to eat through the allowed number of TCP connections. This prevents legitimate request from being answered by the server

- Amplification attack
  - This includes NTP, SSDP, DNS, SNMP attacks, etc
  - The attacker can send 3rd party server (NTP) a request using a spoofed IP address
    - NTP stands for network time protocol. Basically the way the internet/computers sync up using atomic clocks so they have the same time.
  - The server will request will then respond to that request with 28-54 times larger payload to the spoofed IP address
    - If the attacker sends a packet with a spoofed IP of 64 bytes, the NTP server would respond with up to 3,456 bytes of traffic
- Layer 7 attack
  - This is when a web server receives a flood of GET or POST request. In most cases from a botnet or large number of compromised computers

>Logging API Calls using CloudTrail

- CloudTrail
  - CloudTrail keeps detailed event logs of every action that occurs against your AWS resources. Each event that CloudTrail logs includes the following parameters:
  - AWS CloudTrail monitors and records account activity across your AWS infrastructure, giving you control over storage, analysis, and remediation actions.
  - Protect your organization from penalties using CloudTrail logs to prove compliance with regulations such as SOC, PCI, and HIPAA.
  - Tracking API Calls, on who and when they made them

- Cloud Trail - Don't forget the things you can track with CloudTrail: username, event time and name, IP address, access key, Region, and error code.
All API calls are denied by default and must be allowed.

*Keep in mind that RDP or SSH traffic aren't logged. Basically, can't log what command someone is entering in using SSH to EC2. Only logging API calls in AWS

CloudTrail Logging

- Time of the API call
- Source IP address of the API caller
- Identity of the API caller
- Metadata around API calls

>Protecting applications using Shield

- AWS Shield
    - AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. AWS Shield provides always-on detection and automatic inline mitigations that minimize application downtime and latency, so there is no need to engage AWS Support to benefit from DDoS protection. There are two tiers of AWS Shield - Standard and Advanced.
        - Shield
            - CloudFront
            - Route 53
            - Elastic Load balancing
            - AWS Global accelerator

AWS Shield protects against SYN/UDP floods, reflection attacks, and other Layer 3 and layer 4 attacks.

- AWS Shield Advanced
    - Enhanced protections for larger and more sophisticated attacks
    - Offers always-on, flow-based monitoring of network traffic and active application monitoring to provide near real-time notifications of DDoS attacks
    - 24/7 access to the DDoS response Team (DRT)
    - Protects your AWS bill against higher fees due to ELB, CloudFront, Route 53 usage spikes during a DDoS attack
    - This cost $3,000 per month

>Filtering Traffic with AWS WAF

WAF = Web Application Firewall

Basically, lets you control access to your content. Using this you can configure conditions such as IP addresses can make this request.

The ALB or CloudFront will either allow this content to be received or give an HTTP 403 status code

WAF Operates at Layer 7

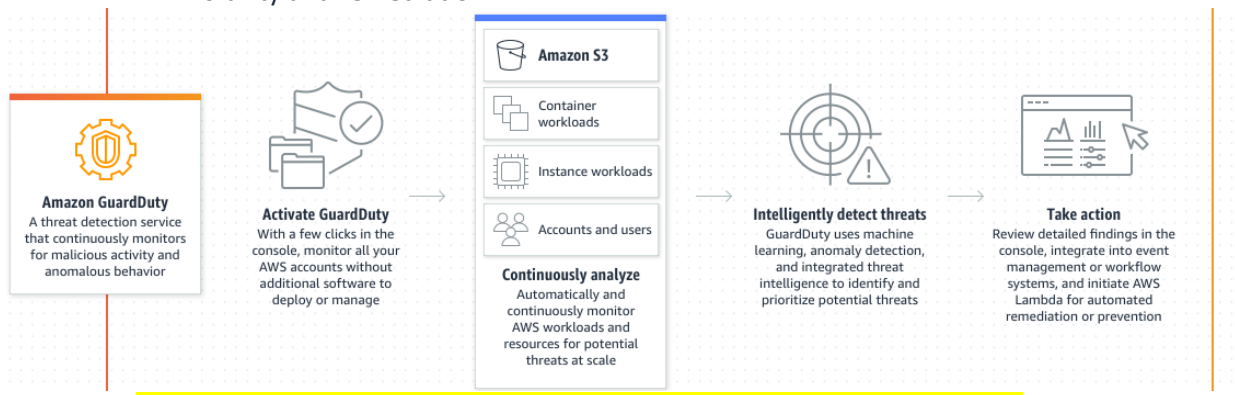
3 Different behaviors for AWS WAF

- Conditions
    - Define conditions by using characteristics of web request

1. IP addresses
2. Country
3. Values
4. Presence of SQL code
5. Presence of a script
6. Strings that appear in request

>Guarding your network with GuardDuty

- GuardDuty
    - Intelligent threat detection system that uncovers unauthorized behavior
    - Amazon GuardDuty is a threat detection service that continuously monitors your AWS accounts and workloads for malicious activity and delivers detailed security findings for visibility and remediation.



    - Uses machine learning, reviews cloudtrail, VPC flow logs, and DNS logs
    - Built-in detection for EC2, S3, and IAM
    - Threat detection with AI
        - 7-14 days to set a baseline
        - Once active – you will see findings on the GuardDuty console and in CloudWatch events
    - Pricing

        - 30 days free

>Monitor S3 buckets with Macie

- Macie automatically finds and classifies sensitive data stored in AWS. It uses machine learning to recognize sensitive data such as personally identifiable information or trade secrets and shows you how that data is being used in AWS. For more information, visit https://aws.amazon.com/macie/
    - Amazon Macie is a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect your sensitive data in AWS.
    - Macie's alerts, or findings, can be searched and filtered in the AWS Management Console and sent to Amazon EventBridge, formerly called Amazon CloudWatch Events, for easy integration with existing workflow or event management systems, or to be used in combination with AWS services, such as AWS Step Functions to take automated remediation actions.

Best way to deliver content from an S3 bucket that only allows users to view content for set period of time will be to create a Pre-signed URLs would allow you to restrict the length of time the content can be viewed.

Classifies sensitive data such as home address, email address, social security number, and debit card, passport, phone number, etc

>Inspector

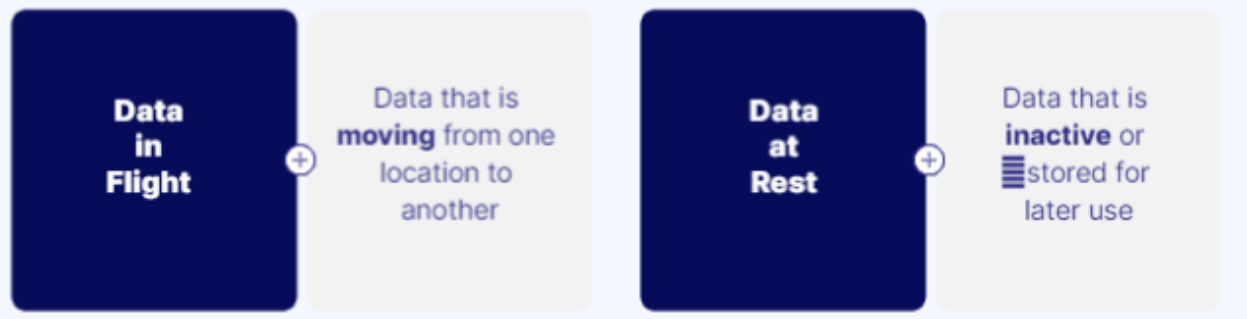
- Inspector
    - Inspector analyzes your EC2 instances for security vulnerabilities and common misconfigurations. For more information, visit https://aws.amazon.com/inspector/
    - Amazon Inspector is an automated vulnerability management service that continually scans AWS workloads for software vulnerabilities and unintended network exposure.
- 2 types of assessments
    - Network Assessments
        - Network config analysis to check for ports reachable from outside the VPC
        - Inspector agent is **not** required
    - Host assessments
        - Vulnerable software (CVE), host hardening (CIS Benchmarks),
        - Inspector agent **is** required

How does this work?

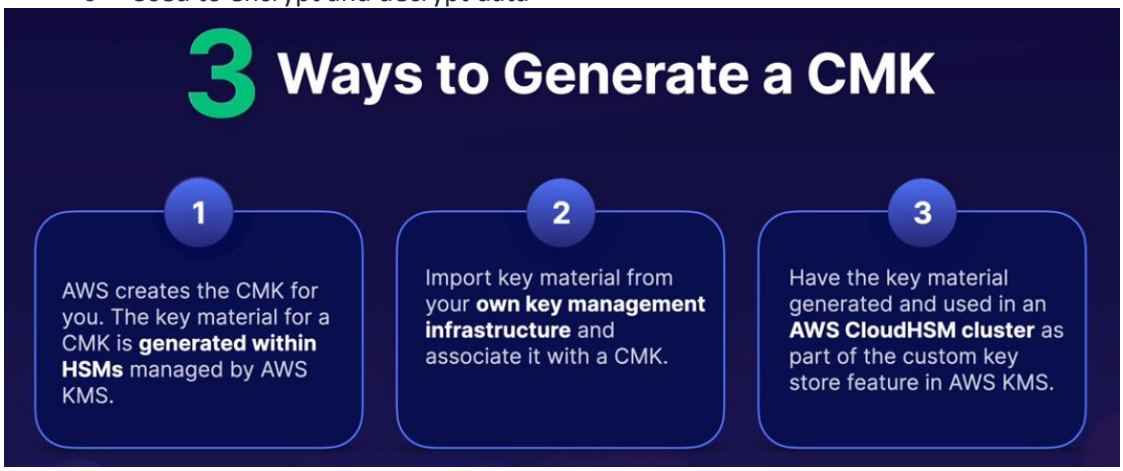
1. Create assessment target
2. Install agents on EC2 Instances
3. Create assessment template
4. Perform assessment run
5. Review findings against rules

>Managing Encryption keys with JMS and CloudHSM

- Understand the difference between data in flight vs data at rest



- Key management service (KMS)
  - AWS Key Management Service (AWS KMS) makes it easy for you to create and manage cryptographic keys and control their use across a wide range of AWS services and in your applications. AWS KMS is a secure and resilient service that uses hardware security modules that have been validated under FIPS 140-2, or are in the process of being validated, to protect your keys. AWS KMS is integrated with AWS CloudTrail to provide you with logs of all key usage to help meet your regulatory and compliance needs.
  - Encryption keys—the data files used to control an object's cryptographic transformation—are mostly managed on AWS by the AWS Key Management Service (KMS).
  - Be aware that AWS Key Management Service (KMS) manages encryption keys. KMS-managed keys are used across a wide range of AWS services, including EBS, RDS, DynamoDB, and S3.
- Customer master key (CMK)
  - Logical representation of a master key. Includes metadata, such as the key ID, creation date, description and key state.
  - Used to encrypt and decrypt data



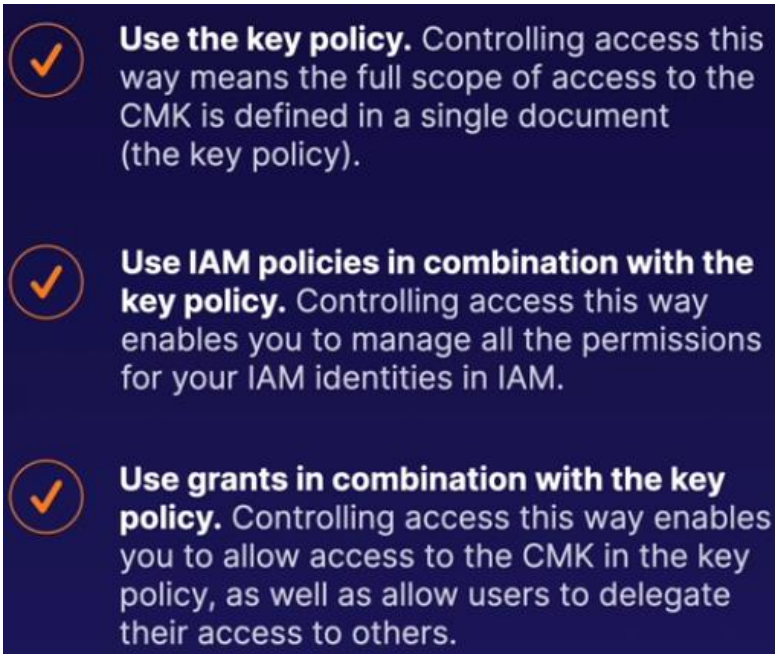
When getting started with KMS you start using the service by requesting the creation of a CMK, and you control the lifecycle of the CMK and who can use or manage it.
You can choose to have AWS KMS automatically rotate CMKs every year, provided that those keys were generated within AWS KMS HSMs. (Not supported for imported keys)

- CloudHSM
  - Hardware security module (HSM) used to generate digital encryption keys

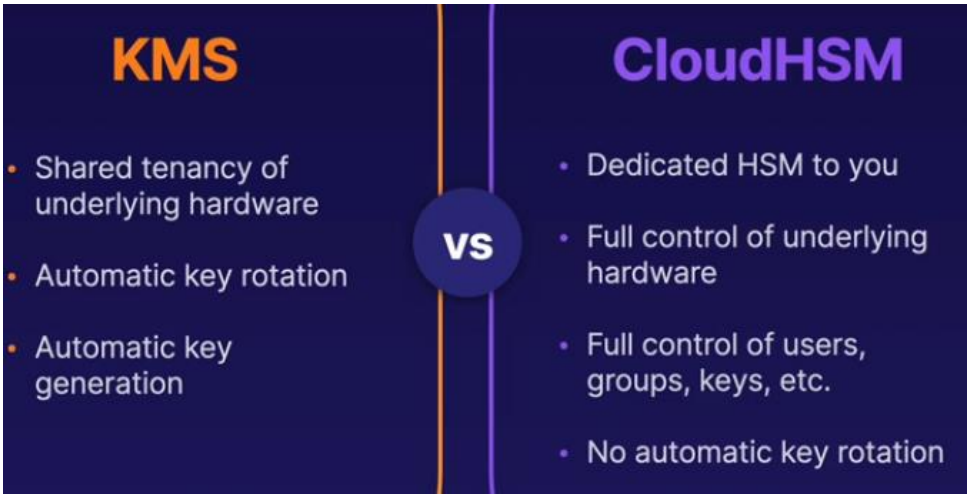
- AWS CloudHSM is a cloud-based hardware security module (HSM) that enables you to easily generate and use your own encryption keys on the AWS Cloud. With CloudHSM, you can manage your own encryption keys using FIPS 140-2 Level 3 validated HSMs.

Policies attached to an IAM identity are called identity-based policies (or IAM policies)… But… polices attached to other kinds of resources are called resource-based policies.

All KMS CMKs have a key policy



KMS vs. CloudHSM



>Secrets Manager

Service that securely stores, encrypts, and rotates your database credentials and other secrets

- Secrets Manager
    - AWS Secrets Manager helps you protect secrets needed to access your applications, services, and IT resources. The service enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle.
    - Your application makes an API call to secrets manager to retrieve the secret programmatically
    - Reduce the risk of credentials being compromised
- What can be stored?
    - RDS Creds
    - Creds for non-RDS databases
    - Any other type of secret, provided you can store it as a key-value pair (SSH keys, API keys)

If you enable rotation, Secrets Manager immediately rotates the secret once to test the configuration. That is why you ensure all your applications that use these creds are updated to retrieve the creds.

ENABLE ROTATION

- That way they are not going to use old creds when trying to connect

>Centralizing WAF Management via AWS Firewall Manager

This is a security management service in a single pane of glass across multiple aws accounts and applications. You can create AWS WAF rules for your ALB, API gateways.

Benefits of firewall manager

1. Benefits of Firewall Manager
    a. Simplify Management of Firewall Rules across your Accounts
        i. One single pane of glass allows you to manage security across multiple AWS services and accounts
    b. Ensure Compliance of Existing and New Applications
        i. Firewall Manager automatically enforces security policies that you create across existing and newly created resources

>Temporarily Sharing S3 Objects Using Presigned URLs or Cookies

So all objects in S3 are private by default. The object owner can optionally share objects with others by creating a preassigned URL.

- Preassigned URL
    - When you create this, you must provide your security creds, specify a bucket name and object key. Only specified duration
    - Access
        - Anyone who receives the presigned URL can then access the object.
        - If you have a video in your bucket and both the bucket and the object are private, you can share the video with others by generating a presigned URL
- Presigned Cookies

- Useful when you want to provide access to multiple restricted files. The cookie will be saved on the user's computer and will be able to view the entire contents of the restricted content.

>Auditing Continuously with AWS Audit Manager

Audit Manager is an automated service that produces reports specific to auditors for PCI compliance, GDPR, and more. Audit manager helps continually audit your AWS usage to make sure you stay compliant with industry standards and regulations.

Transition from manual to automated evidence collection. This allows you to produce automated reports for auditors and reduces the need to compile these reports manually.

>Downloading Compliance Documents from AWS Artifact

AWS Artifact is a single source you can visit to get the compliance-related information that matters to you, such as AWS security and compliance reports or select online agreements

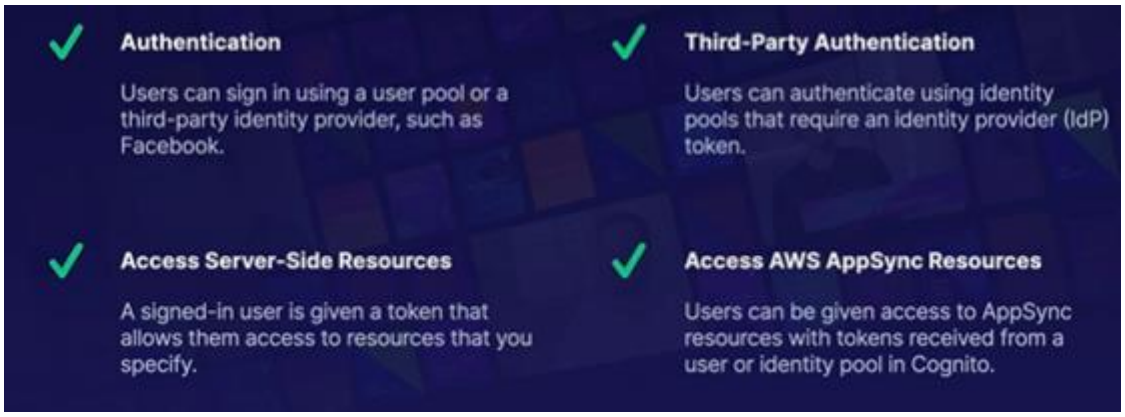
>Authenticating Access with Amazon Cognito

Cognito provides authentication, authorization and user management for your web and mobile apps in a single service without the need for custom code.

- Helps you control access to mobile and web applications
- Amazon Cognito lets you add user sign-up, sign-in, and access control to your web and mobile apps quickly and easily.
- Cognito lets you add user access control to your application. Cognito integrates with many identity providers including Amazon, Google, Microsoft Active Directory, and Facebook. You can also use Cognito to provide your users access to AWS resources without having to give them their own IAM credentials. For more information, visit

https://aws.amazon .com/cognito

Use Cases…

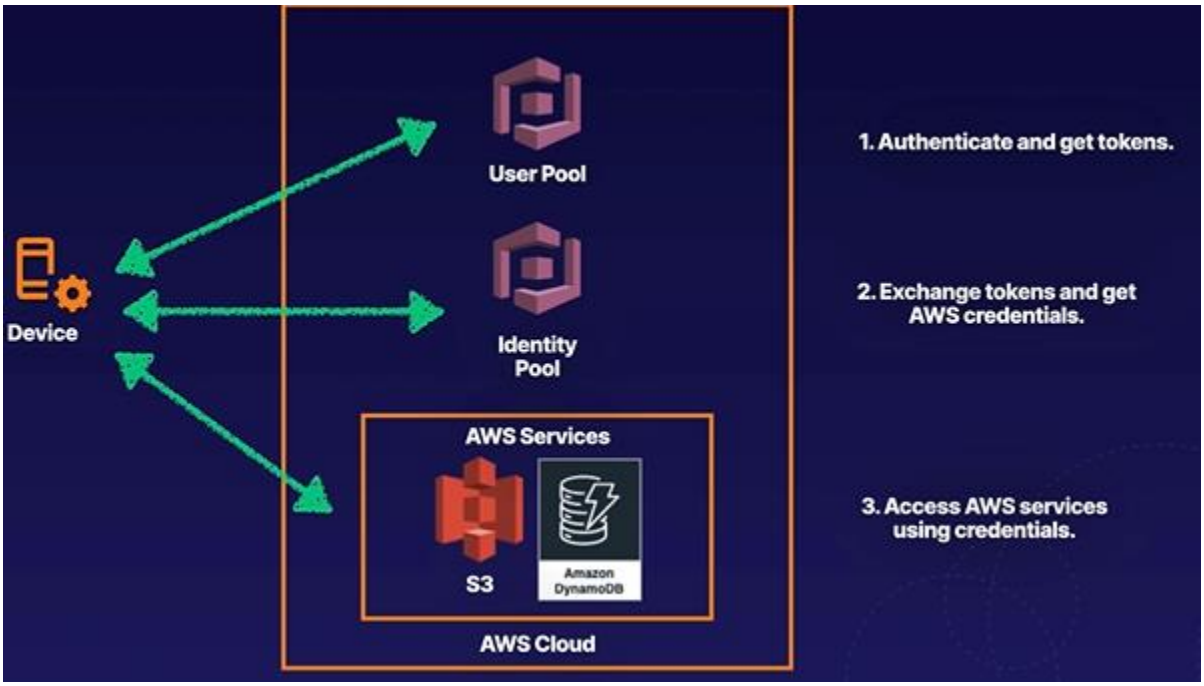


The two main components of Cognito

1. User Pools
    a. Directories of users that provide sign-up and sign-in options for your application users.
2. Identity Pools
    a. Allow you to give your users access to other AWS services.

Example:

You have an application on your phone and you're trying to log in and access the resources to that application is designed to use. You're using your Dropbox app to log in and it is connecting to a user pool in Cognito and you're authenticating and getting tokens. Once the token is received, your device is then going to exchange that token to an identity pool. Which that pool is going to go ahead and give some AWS creds, which you can use those creds to access your AWS services.



>Analyzing Root Cause Using Amazon Detective

Amazon Detective is basically going to be a detractor. They might try and basically confuse you with Inspector or Trusted Advisor.

- Using Detective you can analyze, investigate, and quickly identify the root cause of potential security issues or suspicious activities.
    - It pulls data from all your AWS resources and using machine learning, statistical analysis, and graph theory to build a linked set of data that helps you quickly figure out the root cause.

It utilizes numerous sources such as VPC Flow logs, CloutTrail logs, AEKS audit logs, and Amazon GuardDuty findings.

Of course you have to see if any suspected security instance is actually real or a false positive. Detective generates visualizations that show you what resources, IP, and AWS accounts are connected to your security incident to determine if the finding is an actual malicious activity or not.

>Protecting VPCs with AWS Network Firewall

Any scenario or questions talking about deploying a physical firewall to your VPCs… Think of AWS Network Firewall.

AWS Network Firewall has physical infrastructure in the AWS datacenter that is managed by AWS staff.

This works along with Firewall Manager so you can centrally manage security polices across existing and newly created accounts and VPCs. It also provides an intrusion prevention system (IPS) that gives you active traffic flow inspection.

>Leveraging AWS security hub for collecting security data

- Security Hub is a single place to view all your security alerts from services like Amazon GuardDuty, Amazon Inspector, Amazon Macie, and AWS Firewall Manager… This works across multiple accounts.

Exam Tips

1. DDoS
    a. Know the difference of layer 4 and 7 attacks. Which there are different ways in AWS to prevent this.
2. CloudTrail
    a. Basically, CCTV system to monitor what is going on for your AWS account. Logs all API calls made to your AWS account and stores in S3
3. Shield
    a. Protects against Layer 3 and layer 4 only
    b. Any questions on DDoS mitigation or protection against Layer 3 and 4 attacks. Think of AWS Shield
    c. Talking about application level attacks that is going to be AWS WAF
    d. Advanced shield cost $3k but it will give you a 24/7 DDoS response Team
        i. So, any questions about having a dedicated team to respond to DDoS attack think of AWS Shield Advanced
4. WAF
    a. If you see questions about how to block layer 7 attacks… Think of WAF. But it can block DDoS attacks as well as things like SQL injections, cross-site scripting
    b. Block IP addresses or specific countries
5. GuardDuty
    a. Uses AI to learn what normal behavior looks like
    b. Updates a database of known malicious domains
    c. Monitors cloudtrail logs, VPC flow logs, and DNS logs
    d. Any questions about AI and automation to protect your AWS account and to monitor things like VPC, CloudTrail think of AWS GuardDuty
6. Macie
    a. Remember is it and what does it do?
    b. Macie uses AI to analyze data in S3 and helps identify PII, PHI, and financial data
    c. Great for HIPPA and GDPR compliance as well as preventing identity theft
    d. Macie alerts can be sent to Amazon EventBridge and integrated with your management systems
    e. Automate remediation actions using other AWS services
    f. Any questions about PII and how to prevent from being leaked accidentally in S3 think of Macie
7. Inspector
    a. Used to perform vuln scans on both EC2 instances and VPCs
    b. These can be run once, alt, or run them weekly
8. KMS
    a. Managed service that makes it easy to create and control the encryption keys used to encrypt your data
    b. Start using the service by requesting the creation of a CMK
    c. AWS manages KMS keys

9. Secrets Manager
    a. Securely store your application secrets: database creds, API keys, SSH keys, passwords, etc
    b. Applications use the Secrets Manager API
    c. Rotating creds is super easy
    d. When enabled – Secrets manager will rotate creds right away
    e. Use secrets manager before enabling cred rotation
    f. Need more than 10k parameters, key rotation, or the ability to generate passwords using CloudFormation… Use Secrets Manager
10. Parameter Store
    a. Parameter Store is also integrated with Secrets Manager. You can retrieve Secrets Manager secrets when using other AWS services that already support references to Parameter Store parameters.
    b. If you're trying to cut down cost, choose Parameter Store
11. Advanced IAM Polices
    a. Not explicitly allowed == implicitly denied
    b. Explicit deny > everything else
    c. Only attached policies have effect
    d. AWS joins all applicable policies
    e. Effect, Action, and Resource are the only required parts.
        i. https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-policy-structure.html
12. Certificate Manager
    a. Free service that saves time and money, automatically renew your SSL certs and rotate old certs with new certs supported AWS services
    b. Integrates with ELB, CloudFront, and API Gateway
    c. Know around SSL certs and what services you should use to integrate SSL certs…
        i. Which is Certificate Manager
13. AWS Firewall Manager
    a. If you see any scenario about multiple AWS accounts and resources that need to be secured centrally
        i. Think of this
14. Presigned URLs
    a. If you see any scenario questions where it talks about needing to share private files in your S3 buckets
        i. Think of this
15. Audit Manager
    a. If you see any scenario questions about HIPPA or GDPR compliance that ask about continuous auditing or automating auditing reports.
16. AWS Artifact
    a. This comes up in the exam quite a bit and is often used as a distractor you simply have to know what it is. But anything about audits and compliance reports.
        i. Think AWS Artifact
17. Cognito

   a. User Pool: User directories that provide sign-up and sign-in options for users of your application
   b. Identity pool: Allows your users to access other AWS services
18. Amazon Detective
   a. Detective operates across multiple AWS services and analyzes the root cause of an event.
19. AWS Network Firewall
   a. Any scenarios about filtering your network traffic before it reaches your internet gateway or IPS or any hardware firewall… Think of AWS network firewall.
20. Security Hub
   a. Any scenarios about single place to view all your security alerts across multiple AWS security services and accounts… Think of this