Security Services Overview

Chandra Lingam, Cloud Wave LLC

Introduction

The security products page (https://aws.amazon.com/products/security/) has a good overview of key services and capabilities.

I have added additional information on active attack visibility and response (i.e., is the service simply reporting suspicious activities or actively defending attacks). It is important to know this distinction as you evaluate questions in the exam.

Identity and Access Management

Services in this category help you enforce principles of least access privileges required to complete a job.

They cover a broad spectrum of identity and access management, such as single account identity management, multi-account single sign-on, corporate identity federation, share resources, and so forth.

These services ensure the caller has appropriate credentials and is authorized to perform the action.

These services block attackers who attempt to access resources with invalid credentials or attempt to perform actions that they are not authorized to perform.

CloudTrail will capture API interactions with these services.

Service	Use Case
AWS Identity and Access Management (IAM)	Securely manage access to services and resources
IAM Access Analyzer	Identify resources (such as S3 bucket, IAM Roles, KMS Keys, Lambda functions, SQS Queue) that are shared with external accounts outside of your organization
AWS Single Sign-On (SSO)	Cloud Single-sign-on Service
Amazon Cognito	Identity management for your apps
AWS Directory Service	Managed Active Directory
AWS Resource Access Manager (RAM)	Share AWS resources securely between accounts
AWS Organizations	Central governance and management across AWS accounts

Detection

The services in this list can detect deviations from normal usage and behavior. These services have a dashboard to give you visibility into findings and severity. Most services also publish the findings as CloudWatch Events.

For automated remediation, you need to define CloudWatch Rules to watch for specific events from these services and configure a target to initiate the workflow.

Service	Use Case	Active Attack Visibility and Response
AWS Security Hub	Unified Security and Compliance Center	The dashboard aggregates security alerts from GuardDuty, Macie, Inspector, IAM

	Automate Security checks and view compliance status	Access analyzer, Firewall Manager, and AWS partner solutions Use CloudWatch Events and Lambda for automated remediation
Amazon GuardDuty	Managed threat detection service Continuous monitoring of suspicious activities	Detailed visibility into findings Use CloudWatch Events and Lambda for automated remediation
Amazon Inspector	Analyze application, instance security	Inspector is a scheduled service However, you can trigger an inspector assessment from CloudWatch Events in response to a resource change. For example, monitor for security group or NACL changes using CloudWatch Events and trigger an inspector assessment for new exposures
AWS Config	Record configurations of your AWS resources and detect configuration drift	Scheduled (example check for key age) and Continuous monitoring of resources (example, configuration change). Visibility into configuration and compliance change timelines Automated remediation for compliance violation or trigger a workflow
AWS CloudTrail	Track user activity and API usage	Visibility into API activities Use CloudWatch Events for automation workflow
AWS IoT Device Defender	Security management for IoT devices	Detect configuration changes and deviations from defined behaviors Use CloudWatch Events for automation workflow

Infrastructure protection

These services actively block attacks and protect your application and resources

Except for Shield Standard, all other services provide full visibility into attacks and malicious requests

Service	Use Case	Active Attack Visibility and Response
AWS Shield – Standard	DDoS Protection against layer 3 and 4 attacks	No visibility to customers. AWS handles attacks behind the scenes
AWS Shield – Advanced	Advanced DDoS mitigation techniques, customizable	Dashboard with full visibility into attacks in progress

	protection, choose resources to be protected	CloudWatch metrics and Alarms 24x7 access to DDoS Response Team
AWS Web Application Firewall (WAF)	Filter, Block malicious web traffic (layer 7 attacks)	Dashboard with full visibility into how many requests matched the rule criteria CloudWatch metrics and alarms
AWS Firewall Manager	Centrally configure and manage firewall rules across accounts and applications	You can define mandatory firewall rules, and this service automatically applies the rules to existing and new resources. For example, what WAF rules to apply for the Application load balancer, API Gateway, CloudFront distributions. Enabling AWS Shield Advanced protection for specific resources Attaching specific security groups for EC2 and ENI resources

Data Protection

The services in this section provide the capability to protect data at rest and data in transit.

The API activities are reported in CloudTrail, and when you enable trail capture, the trail publishes events to the CloudWatch Event bus. So, you can configure rules to watch for specific events and trigger a workflow.

Service	Use Case	Active Attack Visibility and Response
Amazon Macie	Discover and protect your sensitive data in S3	Dashboard with detailed visibility into findings CloudWatch Event integration for automated remediation
AWS Key Management Service	Key storage and management	API calls to KMS are captured in CloudTrail Use CloudWatch Events for automation workflow
AWS CloudHSM	Single-tenant, Hardware-based key storage for regulatory compliance	API calls are captured in CloudTrail Use CloudWatch Events for automation workflow
AWS Certificate Manager	Provision, manage and deploy public and private	API calls are captured in CloudTrail

	SSL/TLS certificates (for HTTPS)	Use CloudWatch Events for automation workflow
AWS Secrets Manager	Rotate, manage, and retrieve secrets	API calls are captured in CloudTrail Use CloudWatch Events for automation workflow

Incident Response

These services provide tools to help investigate security incidents and recover from disasters.

Service	Use Case
Amazon Detective	Detective is an interactive tool to investigate security issues. Analyze and find the root cause of security issues
CloudEndure Disaster Recovery	Fast, automated disaster recovery Continuously replicates your machine, including OS, system state, databases, applications and files to a different region and account that you configure In case of a disaster, you can instruct this service to provision the required infrastructure automatically

Compliance

Service	Use Case
AWS Artifact	Access AWS compliance reports such as Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, ISO reports and so forth Review, manage and accept your agreements with AWS