



BATCH :
LESSON :
DATE :
SUBJECT :

149

AWS

14.09.2023

Config-CloudTrail etc.

ZOOM GİRİŞLERİNİZİ LÜTFEN LMS SİSTEMİ ÜZERİNDEN YAPINIZ



/ techproeducation

TECHPROEDUCATION



techproeducation.com



+1 (917) 768-7466



Config-CloudTrail-Trusted Advisor ..

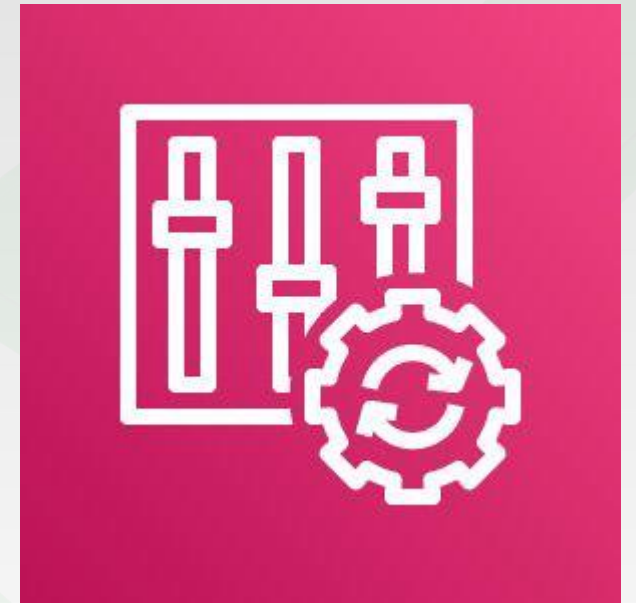


AWS Config

- AWS Config continually assesses, audits, and evaluates the configurations and relationships of your resources on AWS, on premises, and on other clouds.
- It records the configuration of resources in your account.
- It checks if the configurations comply with the rules.
- It can store the results in S3.
- It can send alerts

AWS Config can answer questions like:

- is there unrestricted SSH access on Security Groups?
- are S3 buckets publicly accessible?





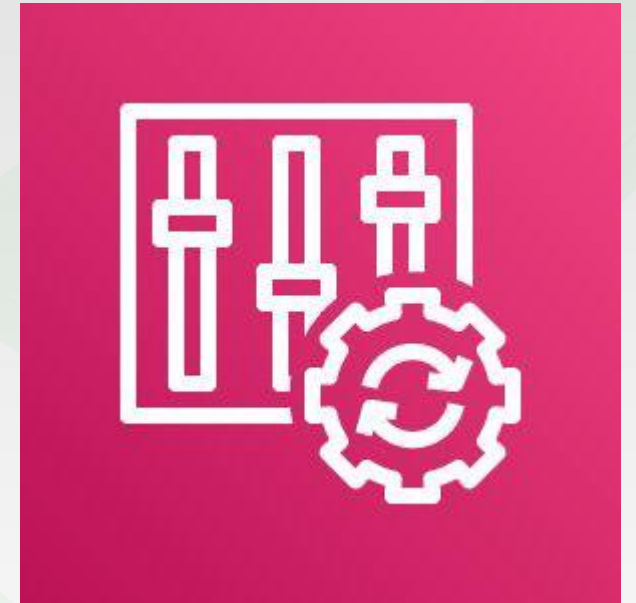
AWS Config

Key Features:

- Inventory
- Change Tracking
- Compliance Checks
- Notifications

Why Use AWS Config?

- Audit
- Security
- Optimization
- Troubleshooting





AWS CloudTrail

- AWS CloudTrail provides visibility into user activity by recording actions taken on your account. CloudTrail records important information about each action, including who made the request, the services used, the actions performed, parameters for the actions, and the response elements returned by the AWS service.
- It is enabled by default.
- It can store the results in S3 or CloudWatch logs.
- It can send alerts.

AWS Config can answer questions like:

- who changed SSH access on Security Groups?
- who changed S3 buckets publicly accessible?





Config-CloudTrail-CloudWatch

- Think of a Load Balancer
 - CloudWatch deals with
 - incoming connection metrics
 - visualising error codes
 - AWS Config deals with
 - tracking Security Group rules for LB
 - tracking config changes for LB
 - ensure a TLS/SSL certificate is assigned to LB (compliance)
 - CloudTrail deals with
 - tracking who made any changes to LB with API calls



Solution Architect Cases

1

You have made a configuration change and would like to evaluate the impact of it on the performance of your application. Which AWS service should you use? CloudWatch, CloudTrail

CloudWatch

2

Someone has terminated an EC2 instance in your AWS account last week, which was hosting a critical database that contains sensitive data.

Which AWS service helps you find who did that and when? CloudWatch, Config, CloudTrail.

CloudTrail

3

You are running a website on a fleet of EC2 instances with OS that has a known vulnerability on port 84. You want to continuously monitor your EC2 instances if they have port 84 exposed.

How should you do this? Setup CloudWatch Metrics, Setup CloudTrail Trails, Setup Config Rules

Setup Config Rules



AWS Trusted Advisor

- AWS Trusted Advisor provide recommendations across multiple categories, including cost optimization and security. These recommendations help you follow AWS best practices to optimize your services and resources.
- If you have a Basic or Developer Support plan, you can use the Trusted Advisor console to access all checks in the Service Limits category and six checks in the Security category.





AWS Shield

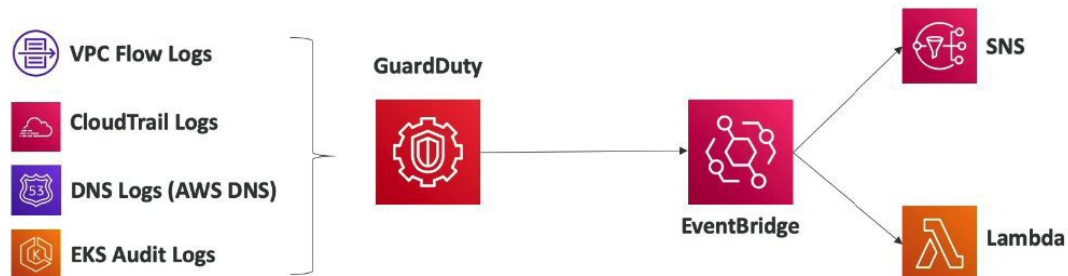
- AWS Shield protects from DDoS attacks.
 - Shield Standard: Free for AWS customers
 - Shield Advanced





Amazon GuardDuty

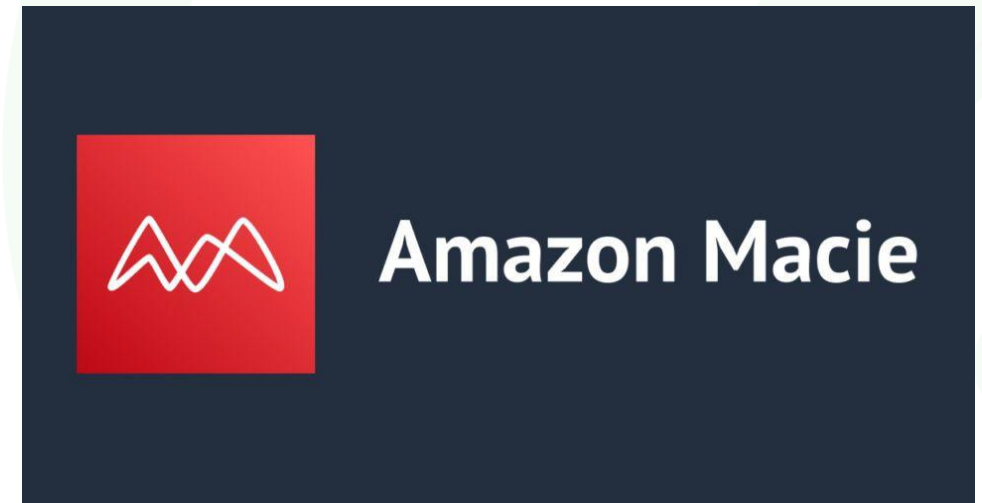
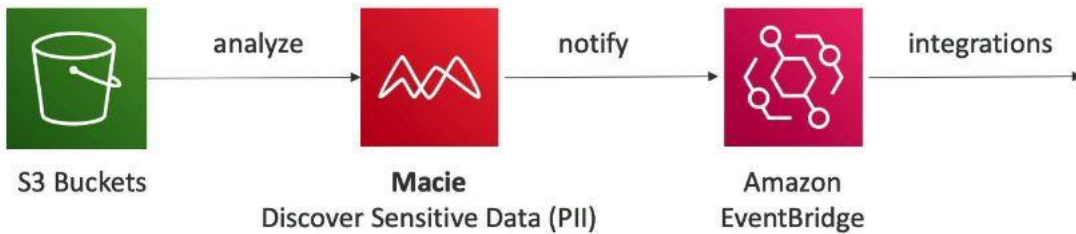
- Intelligent threat discovery.
- Uses machine learning
- Can protect against CryptoCurrency attacks
- Input data:
 - CloudTrail Logs
 - VPC Flow Logs
 - DNS Logs
 - Kubernetes Audit Logs





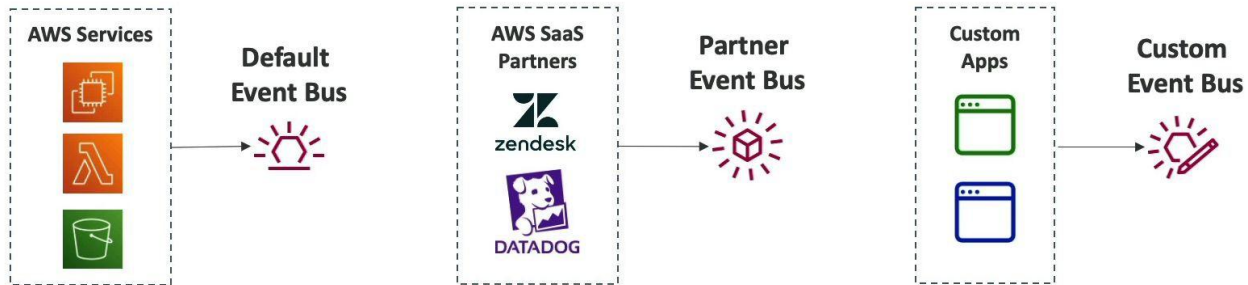
Amazon Macie

- Fully managed data security and data privacy service.
- Uses machine learning and pattern matching.
- Discovers and protects sensitive data.

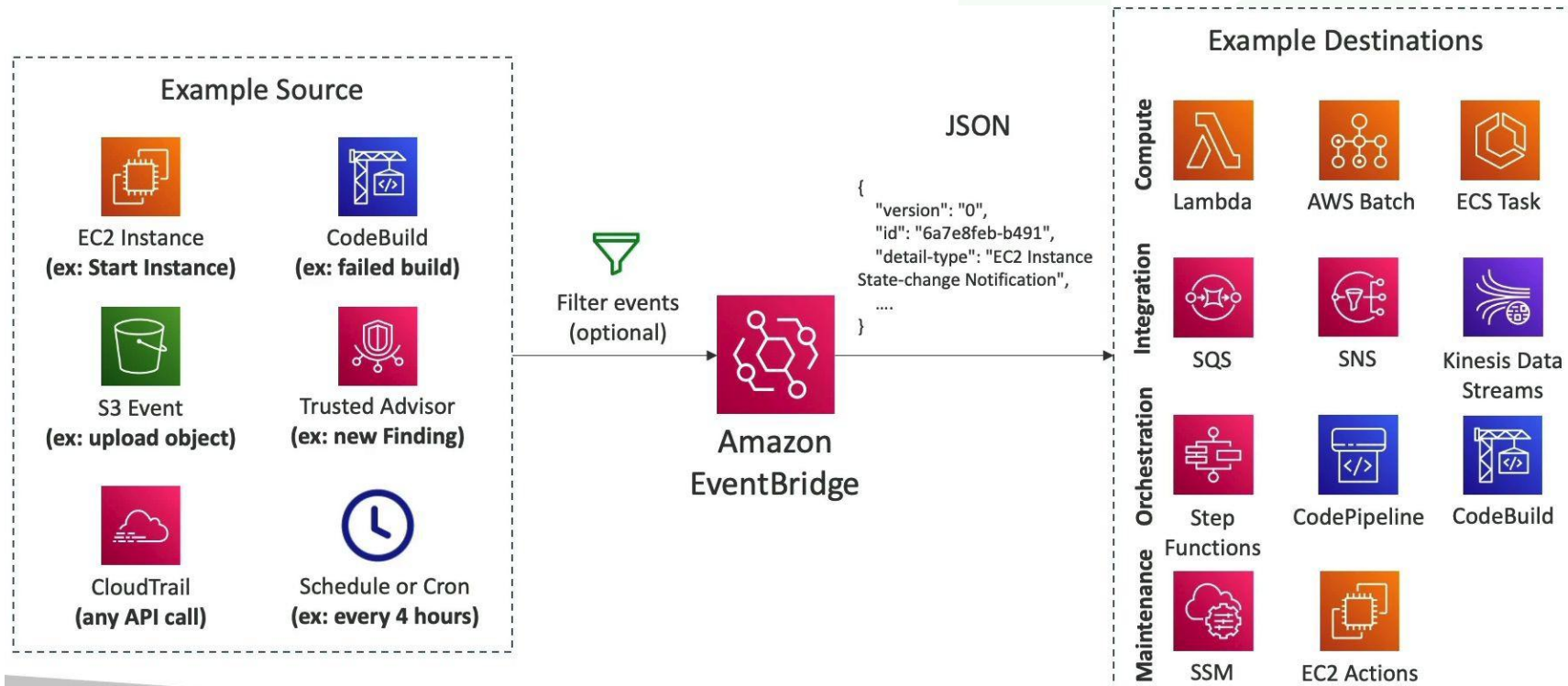




EventBridge



- Schedule cron jobs
- event pattern: React to a service doing something
 - example: IAM root user sign in —> send SNS email notification





AWS WAF

- AWS WAF is a web application firewall service .
- helps protect web applications from various attacks by filtering and monitoring HTTP/HTTPS traffic between a web application and the Internet.
- It gives you control over which traffic to allow or block to your applications by defining customizable web security rules.



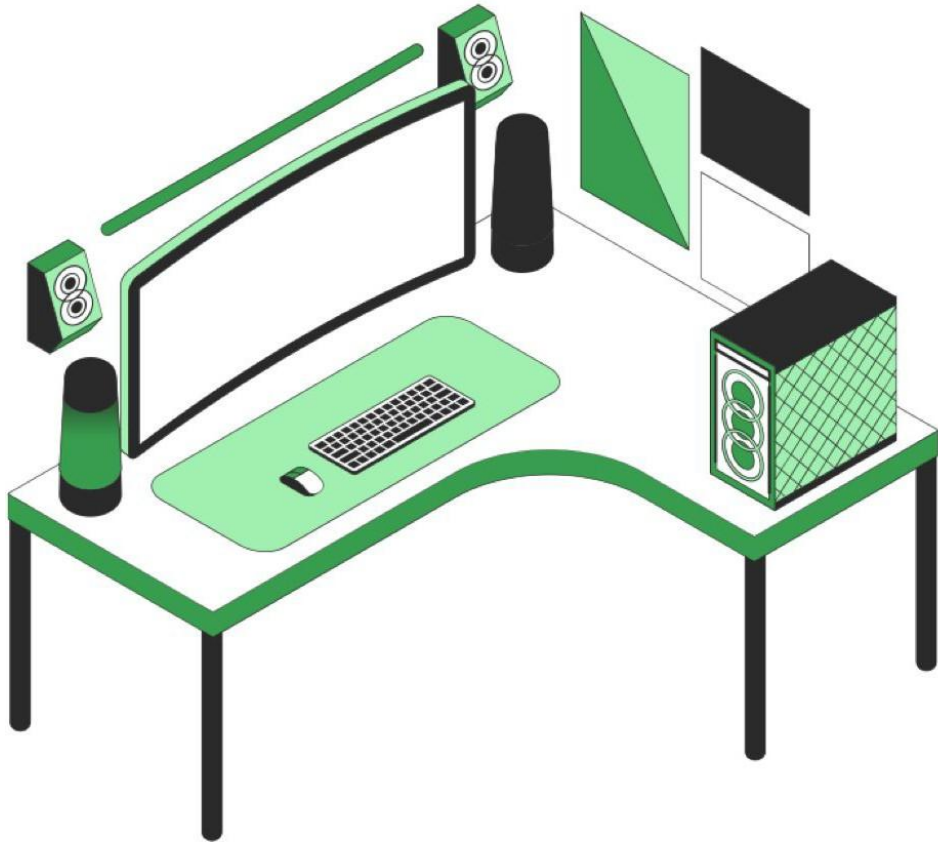
**AWS Web Application
Firewall**



AWS Cost Explorer

- AWS Cost Explorer is a tool that enables you to visualize, understand, and manage your AWS costs and usage over time.
- It's part of the AWS Cost Management suite.
- Offers graphs and tables to help you analyze your AWS spending.
- You can filter by services, accounts, tags, and more to break down your expenses.
- You can access Cost Explorer data programmatically via API for further analysis.





Do you
have any
questions?

Send it to us! We hope you learned something new.