BATCH : B107 AWS-DevOps

LESSON : **AWS**

DATE : 27.03.2023

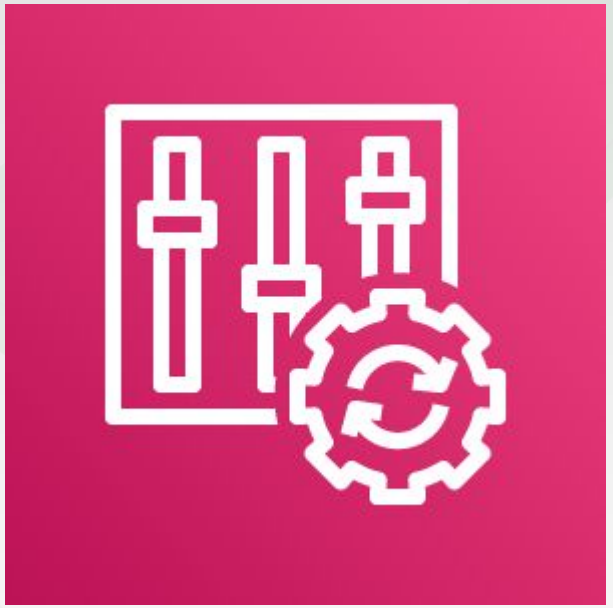
SUBJECT : **Config-CloudTrail etc.**

ZOOM GİRİŞLERİNİZİ LÜTFEN **LMS** SİSTEMİ ÜZERİNDEN YAPINIZ

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 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

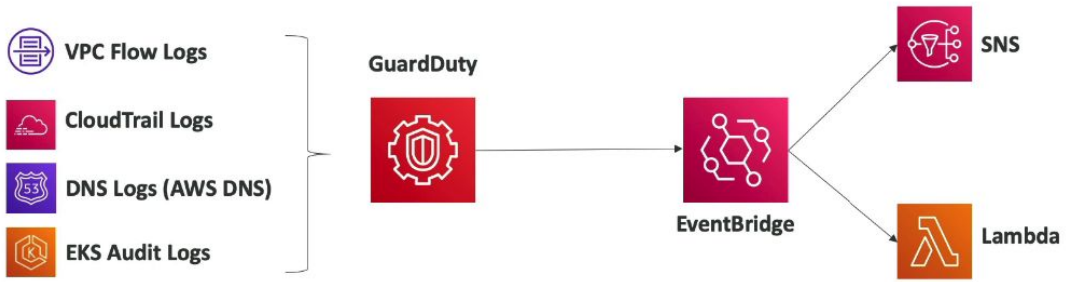
- AWS Trusted Advisor provides recommendations across multiple categories, including cost optimization and security. These recommendations help you follow AWS best practices to optimize your services and resources.
- If you have a Basic or Developer Support plan, you can use the Trusted Advisor console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

AWS Shield

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

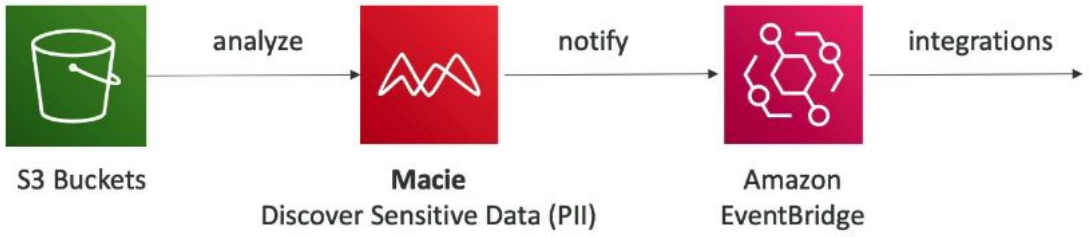
Amazon GuardDuty

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



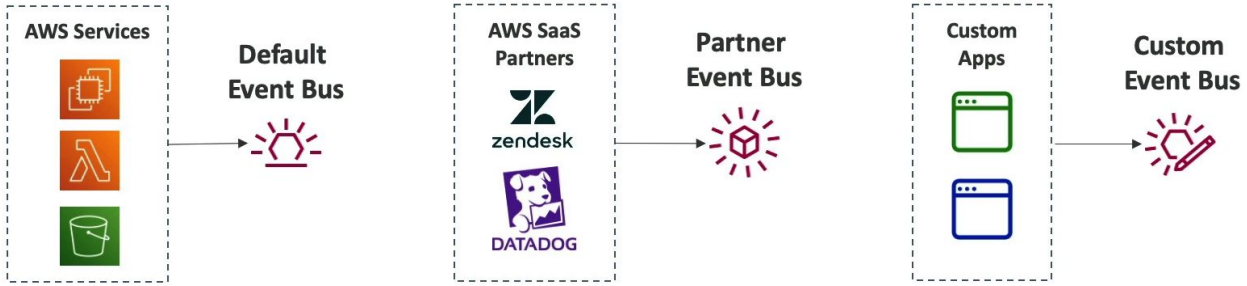
Amazon Macie

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

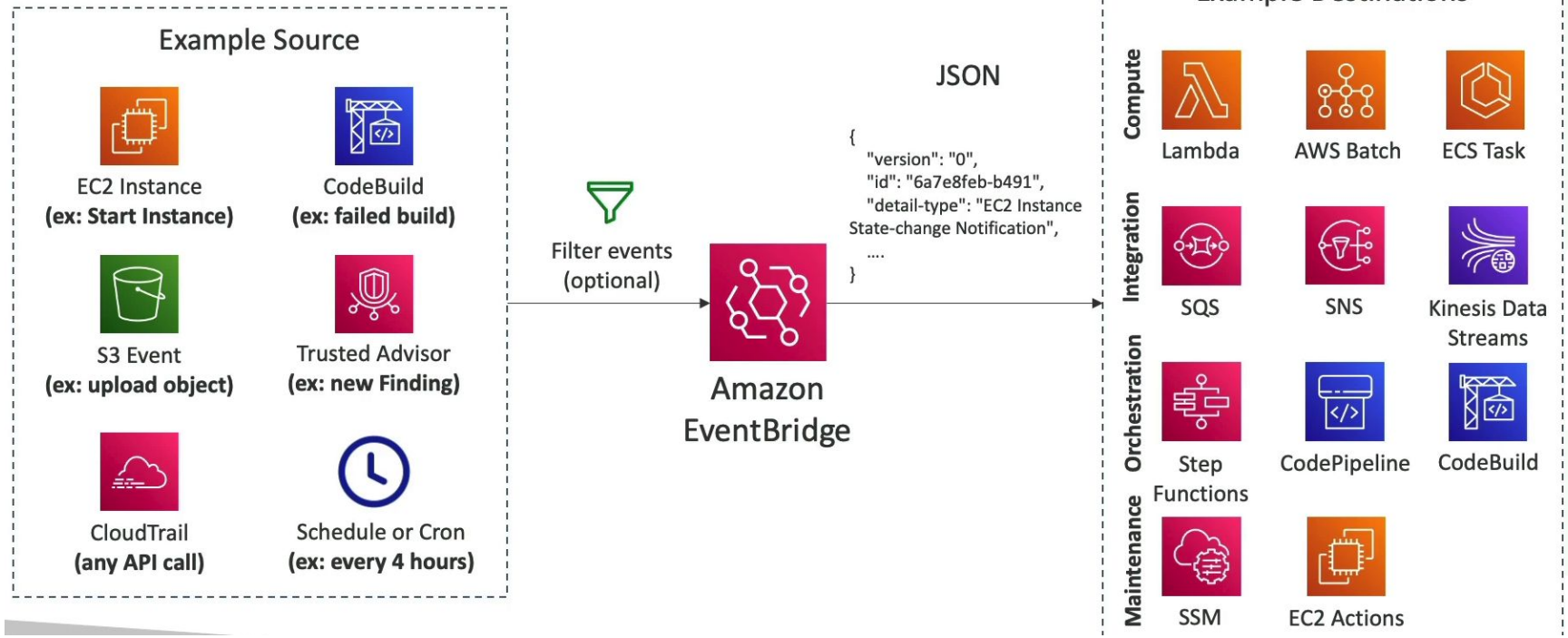


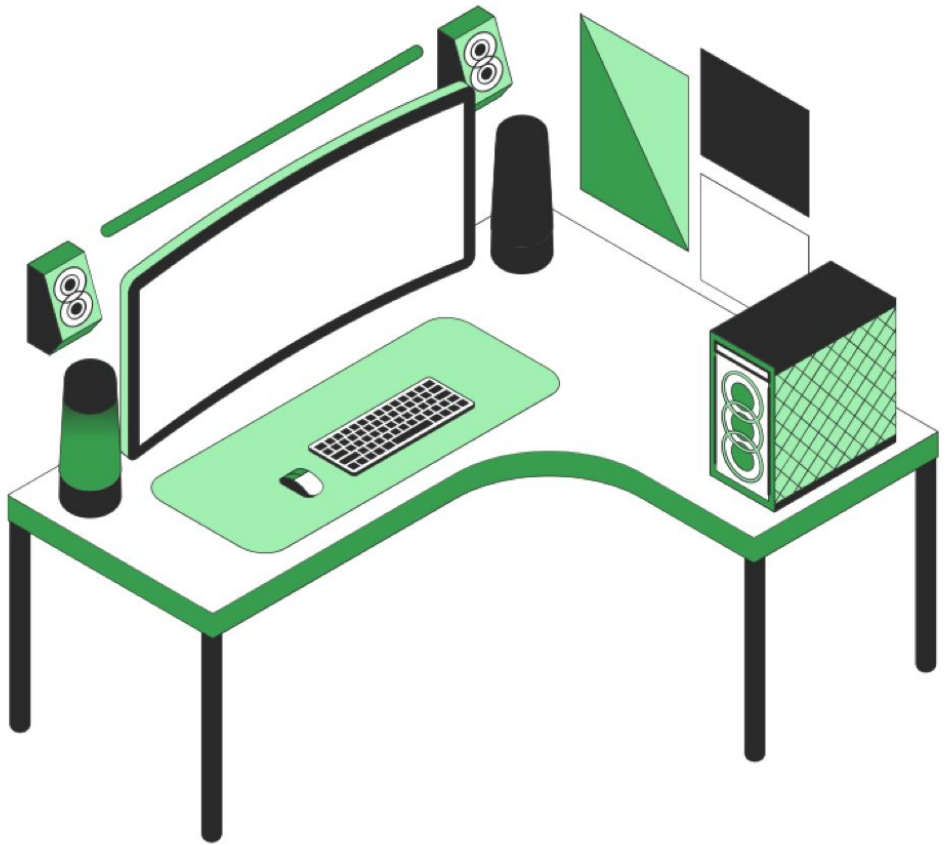
Amazon Macie

EventBridge



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





Do you have any questions?

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