AWS SECURITY

DETECTION AND RESPONSE

SUMMARY

- Build an automatic or semi-automatic system capable of detecting threats and exploits of security vulnerabilities.
- When a threat is detected, the system will activate automatic response measures or provide notifications to security staff for timely intervention.
- This project helps improve detection and reduce response time to security threats in the AWS cloud environment.

SCOPE OF WORK

- Build serverless web Nodejs (CRUD) on local with simulator (lambda, s3, dynamodb) then deploy on aws
- Added some sensitive data and vulnerabilities
- Set up some services like SNS, SLACK to monitor
- Use services in “Detections And Response” to do 10 scenarios

APPROACH

AWS Service	Description
Amazon GuardDuty	Protect AWS accounts with intelligent threat detection
Amazon Inspector	Automated and continual vulnerability management at scale
AWS Security Hub	Automate AWS security checks and centralize security alerts
Amazon Detective	Analyze and visualize security data to investigate potential security issues
AWS Config	Assess, audit, and evaluate configurations of your resources
Amazon CloudWatch	Observe and monitor resources and applications on AWS, on premises, and on other clouds
AWS CloudTrail	Track user activity and API usage

SOLUTION ARCHITECTURE

Attack Phase:

Users and attackers send requests through Amazon API Gateway.

API Gateway receives the request and passes it to the Lambda Function.

Lambda Function processes requests and interacts with Amazon DynamoDB.

Detect & Investigate Phase:

AWS CloudWatch Logs records logs from Lambda Functions.

VPC Flow Logs record all network traffic flows in the VPC.

DNS Logs records DNS queries.

AWS CloudTrail tracks user and API activity, saving logs to S3.

Amazon GuardDuty analyzes logs to detect threats.

Amazon Macie analytics to protect data and detect sensitive data.

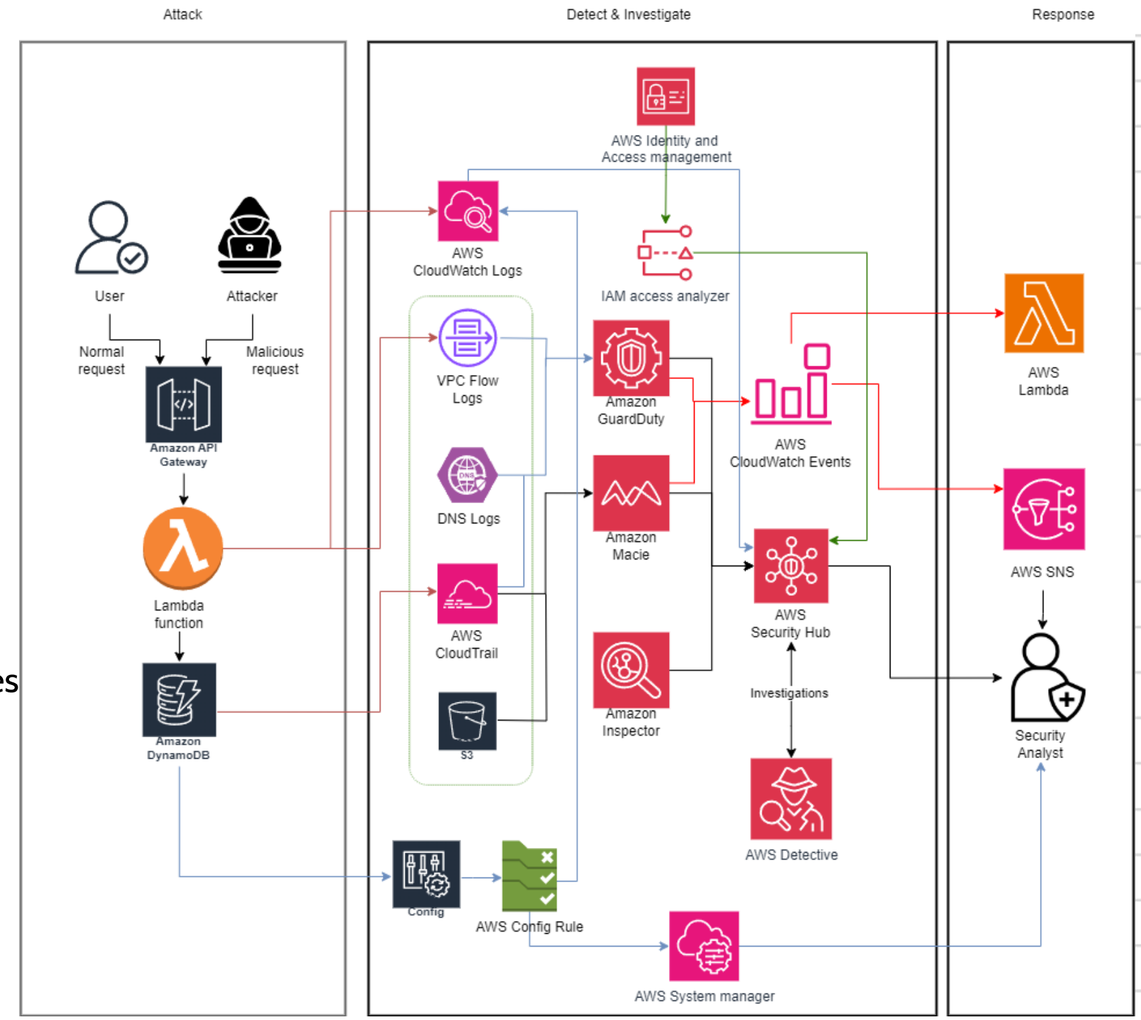
AWS Security Hub centralizes alerts and findings from other services.

Amazon Inspector evaluates applications for security vulnerabilities.

Amazon Detective ingests security data from CloudTrail and VPC Flow Logs, then analyzes and visualizes this data

AWS Config + AWS System Manager:

- AWS Config monitors and records the configuration of AWS resources, allowing assessment against desired configuration.
- AWS System Manager assists in incident response by automating operational tasks across AWS resources.



SOLUTION ARCHITECTURE

Detect & Investigate Phase:

AWS Config + AWS Security Hub:

- Results from AWS Config can be sent to AWS Security Hub, centralizing security alerts and findings.
- It helps in visualizing and managing security data at one place, enhancing the investigation process.

IAM Access Analyzer:

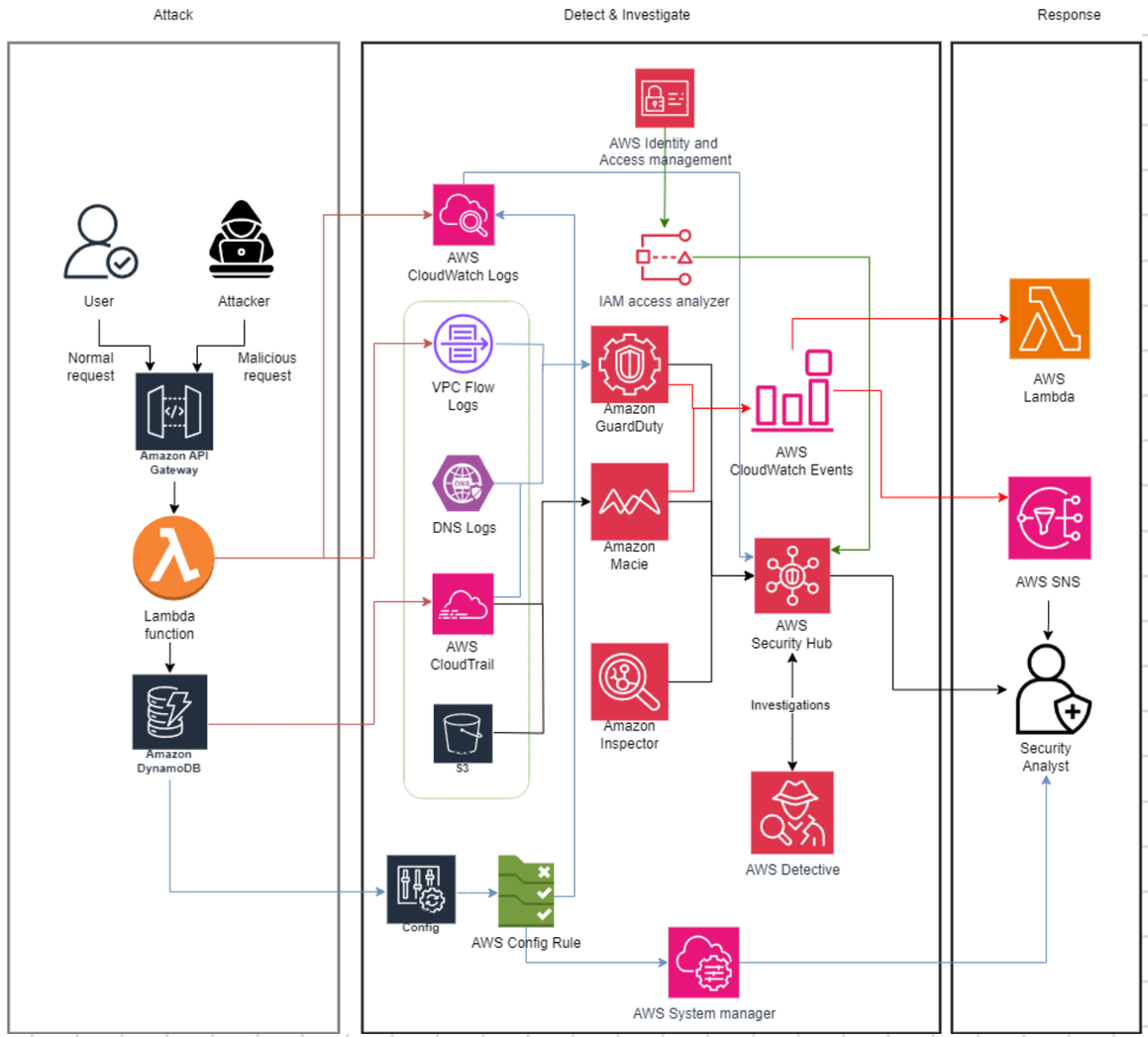
- Integrated into the Detection & Investigation phase under “AWS Identity and Access Management”.
- It analyzes the policies attached to resources and provides detailed findings about resources shared with entities outside the trusted organization.

Response Phase:

AWS CloudWatch Events monitors and reacts to system events.

AWS Lambda is triggered by CloudWatch Events to perform automated tasks.

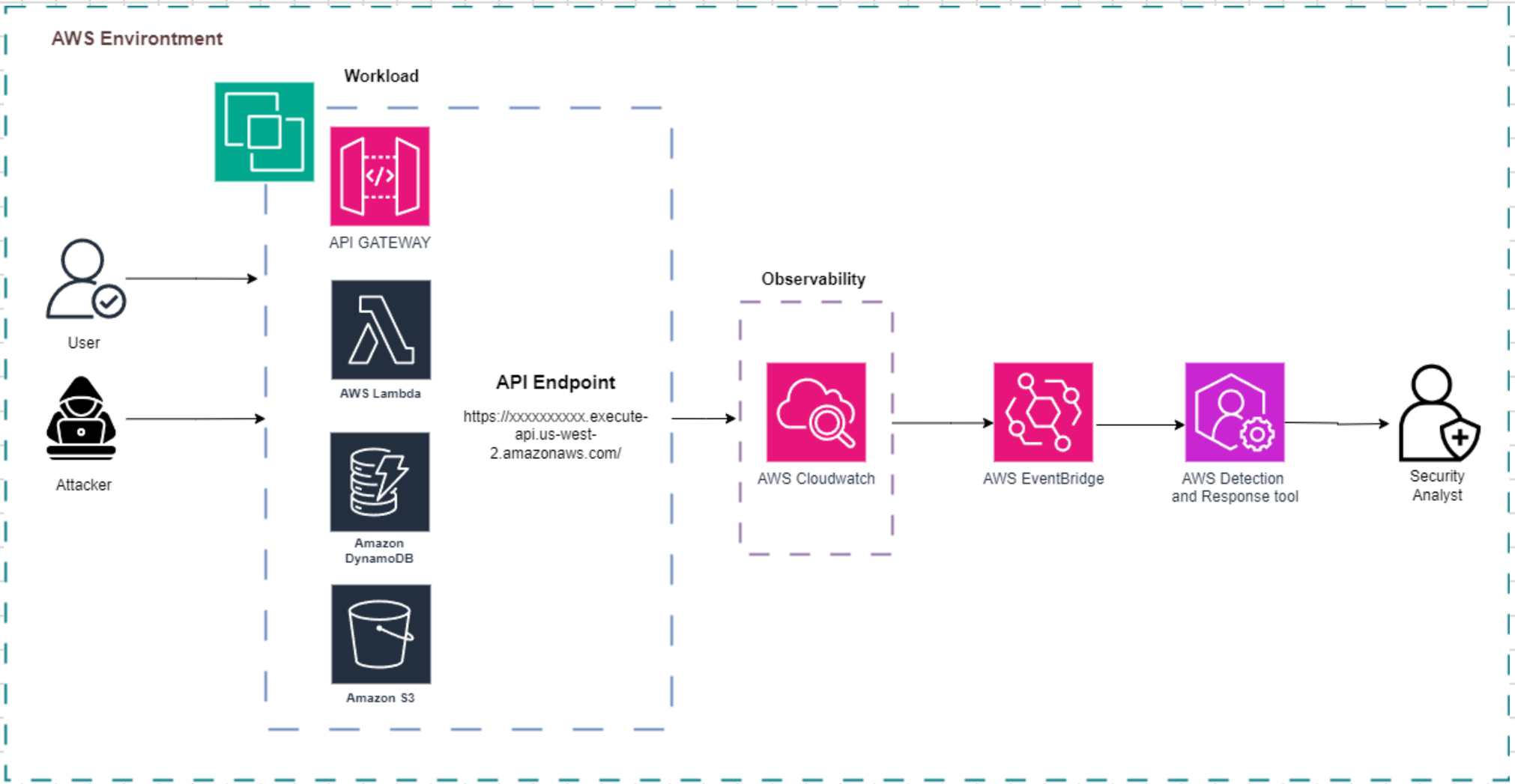
AWS SNS sends notifications to security analysts when alerts occur.



MAIN FEATURE

- Automate threat detection: Use tools like Amazon GuardDuty and AWS Security Hub to automatically detect unusual and potential behavior in AWS accounts.
- Alert and notification management: can provide alert and notification management mechanisms to alert administrators or security teams about important threats and events.
- Analytics and reporting: focused on providing analytics and reporting capabilities to help administrators and security teams better understand threats and behavior on AWS
- Scalability and flexibility: build a scalable and flexible system that can handle large amounts of data and scale as needed.

DEPLOYMENT ARCHITECTURE



ATTACK SCENARIO

1. Use vpc flow logs to check for unusual access
   - Enable VPC Flow Logs on VPC security groups and subnets.
   - Perform monitoring and analysis of traffic flows to detect unusual activities
2. Malware protection uses guarduty
   - Detect malware
3. Inspector to scan lambda vulnerability
   - Scan vulnerability in lambda function use Lambda Standard Scanning & Lambda Code Scanning
4. Use AWS Macie to detect and protect sensitive data:
   - Enable AWS Macie to automatically detect and protect sensitive data in your AWS account and notify admins
5. Use AWS Config to check compliance and detect unwanted changes:
   - Configure AWS Config to automatically check for compliance with security rules and check that resources are configured properly

ATTACK SCENARIO

6. Use AWS Security Hub to detect incidents and respond quickly:
   - Connect your AWS security services to AWS Security Hub to automatically aggregate and analyze security data.
7. Use AWS Detective to analyze and investigate security incidents:
   - Use AWS Detective to automatically analyze and investigate security incidents in your AWS environment.
8. Track user activity and API usage:
   - Use AWS CloudTrail to track and record user activity and API usage in your AWS account.
9. Automatically remediate non-compliant resources:
   - Use AWS Config Rules to define configuration compliance rules and AWS Systems Manager to automatically remediate non-compliant resources.
10. Enhance the security analytics capabilities of AWS Security Hub:
    - AWS Security Hub uses AWS Config to get more information about the configuration of AWS resources. AWS Config rule evaluation results are sent to Security Hub, where they are converted into findings according to the AWS Security Detection Format. This integration increases the depth of information available to Security Hub, allowing for better security assessments.