

Security Tools in AWS

AWS Config

AWS Config



- Helps with auditing and recording compliance of your AWS resources
- Helps record configurations and changes over time
- Questions that can be solved by AWS Config:
 - Is there unrestricted SSH access to my security groups?
 - Do my buckets have any public access?
 - How has my ALB configuration changed over time?
- You can receive alerts (SNS notifications) for any changes
- AWS Config is a per-region service
- Can be aggregated across regions and accounts
- Possibility of storing the configuration data into S3 (analyzed by Athena)

Config Rules

- Can use AWS managed config rules (over 75)
- Can make custom config rules (must be defined in AWS Lambda)
 - Ex: evaluate if each EBS disk is of type gp2
 - Ex: evaluate if each EC2 instance is t2.micro
- Rules can be evaluated / triggered:
 - For each config change
 - And / or: at regular time intervals
- AWS Config Rules does not prevent actions from happening (no deny)
- Pricing: no free tier; \$0.003 per configuration item recorded per region, \$0.001 per config rule evaluation per region

AWS Config

AWS Config Resource

- View compliance of a resource over time

<input type="radio"/> sg-077b425b1649da83e	EC2 SecurityGroup	 Compliant
<input type="radio"/> sg-0831434f1876c0c74	EC2 SecurityGroup	 Noncompliant
<input type="radio"/> sg-09f10ed254d464f30	EC2 SecurityGroup	 Compliant

- View configuration of a resource over time



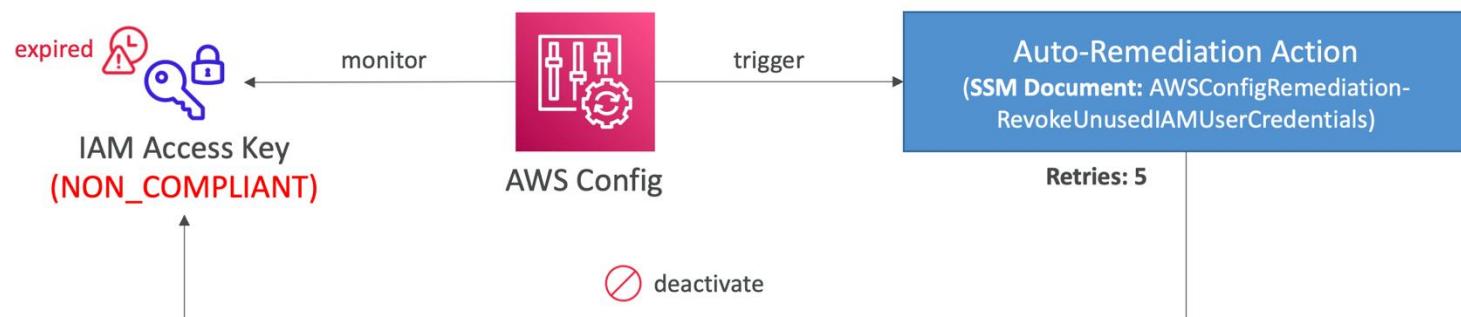
- View CloudTrail API calls of a resource over time



AWS Config

Config Rules – Remediations

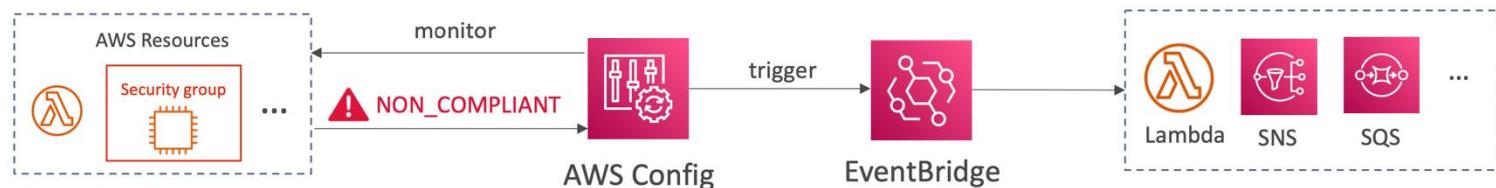
- Automate remediation of non-compliant resources using SSM Automation Documents
- Use AWS-Managed Automation Documents or create custom Automation Documents
 - Tip: you can create custom Automation Documents that invokes Lambda function
- You can set Remediation Retries if the resource is still non-compliant after auto-remediation



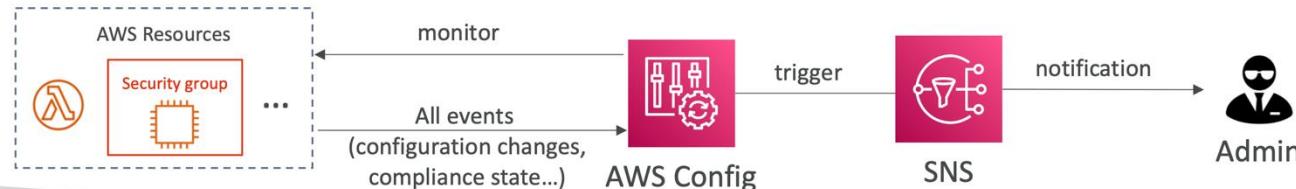
AWS Config

Config Rules – Notifications

- Use EventBridge to trigger notifications when AWS resources are non-compliant



- Ability to send configuration changes and compliance state notifications to SNS (all events – use SNS Filtering or filter at client-side)



AWS Inspector

Amazon Inspector

- Automated Security Assessments
- For EC2 instances
 - Leveraging the AWS System Manager (SSM) agent
 - Analyze against unintended network accessibility
 - Analyze the running OS against known vulnerabilities
- For Container Images push to Amazon ECR
 - Assessment of Container Images as they are pushed
- For Lambda Functions
 - Identifies software vulnerabilities in function code and package dependencies
 - Assessment of functions as they are deployed
- Reporting & integration with AWS Security Hub
- Send findings to Amazon Event Bridge



AWS Inspector

What does Amazon Inspector evaluate?



- Remember: only for EC2 instances, Container Images & Lambda functions
- Continuous scanning of the infrastructure, only when needed
- Package vulnerabilities (EC2, ECR & Lambda) – database of CVE
- Network reachability (EC2)
- A risk score is associated with all vulnerabilities for prioritization

AWS GuardDuty

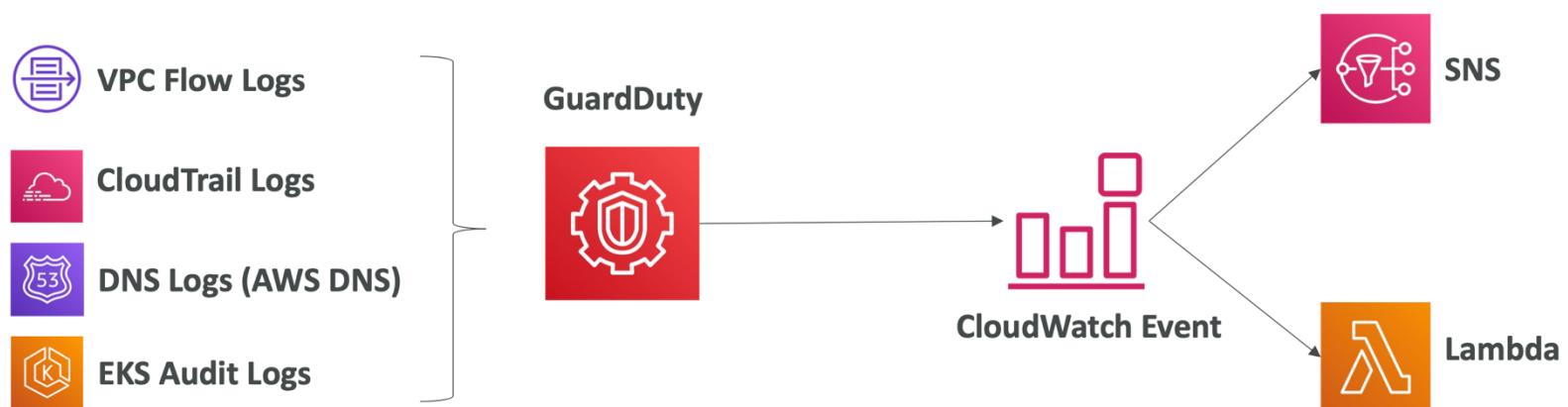
Amazon GuardDuty



- Intelligent Threat discovery to Protect AWS Account
- Uses Machine Learning algorithms, anomaly detection, 3rd party data
- One click to enable (30 days trial), no need to install software
- Input data includes:
 - CloudTrail Events Logs – unusual API calls, unauthorized deployments
 - CloudTrail Management Events – create VPC subnet, create trail, ...
 - CloudTrail S3 Data Events – get object, list objects, delete object, ...
 - VPC Flow Logs – unusual internal traffic, unusual IP address
 - DNS Logs – compromised EC2 instances sending encoded data within DNS queries
 - Kubernetes Audit Logs – suspicious activities and potential EKS cluster compromises
- Can setup CloudWatch Event rules to be notified in case of findings
- CloudWatch Events rules can target AWS Lambda or SNS
- Can protect against CryptoCurrency attacks (has a dedicated “finding” for it)

AWS GuardDuty

Amazon GuardDuty



AWS Trusted Advisor

Trusted Advisor



- No need to install anything – high level AWS account assessment
- Analyze your AWS accounts and provides recommendation:

Cost Optimization



Performance



Security



Fault Tolerance



Service Limits



- Core Checks and recommendations – all customers
- Can enable weekly email notification from the console
- Full Trusted Advisor – Available for **Business & Enterprise** support plans
 - Ability to set CloudWatch alarms when reaching limits
 - Programmatic Access using AWS Support API

AWS Trusted Advisor

Trusted Advisor Checks Examples



- Cost Optimization:
 - low utilization EC2 instances, idle load balancers, under-utilized EBS volumes...
 - Reserved instances & savings plans optimizations,
- Performance:
 - High utilization EC2 instances, CloudFront CDN optimizations
 - EC2 to EBS throughput optimizations, Alias records recommendations
- Security:
 - MFA enabled on Root Account, IAM key rotation, exposed Access Keys
 - S3 Bucket Permissions for public access, security groups with unrestricted ports
- Fault Tolerance:
 - EBS snapshots age, Availability Zone Balance
 - ASG Multi-AZ, RDS Multi-AZ, ELB configuration...
- Service Limits