

ArtiFact, GuardDuty, Inspector, Macie

AWS Artifact (not really a service)



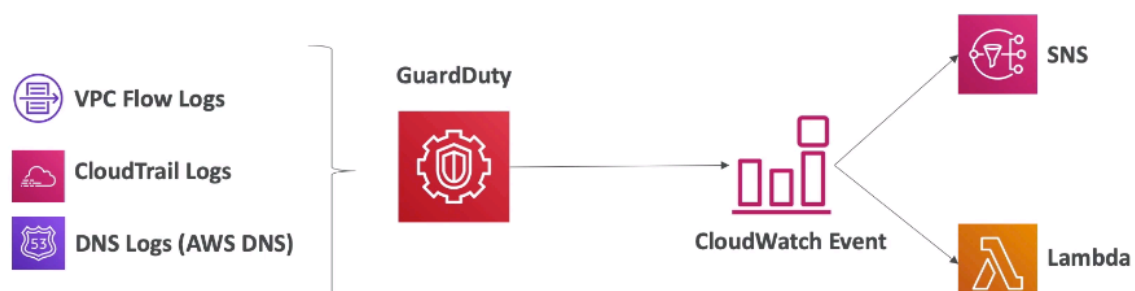
- Portal that provides customers with on-demand access to AWS compliance documentation and AWS agreements
- Artifact Reports - Allows you to download AWS security and compliance documents, like AWS ISO certifications, Payment Card Industry (PCI), and System and Organization Control (SOC) reports
- Artifact Agreements - Allows you to review, accept, and track the status of AWS agreements such as the Business Associate Addendum (BAA)
- Can be used to support internal audit or compliance

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 Logs: unusual API calls, unauthorized deployments
 - VPC Flow Logs: unusual internal traffic, unusual IP address
 - DNS Logs: compromised EC2 instances sending encoded data within DNS queries

Amazon GuardDuty



Amazon Inspector



- Automated Security Assessments for EC2 instances
- Analyze the running OS against known vulnerabilities **ସଂଗୃହ**
- Analyze against unintended network accessibility
- AWS Inspector Agent must be installed on OS in EC2 instances



- After the assessment, you get a report with a list of vulnerabilities

AWS Config



- Helps with auditing and recording compliance of your AWS resources
- Helps record configurations and changes over time
- Possibility of storing the configuration data into S3 (analyzed by Athena)
- 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

Amazon Macie



- Amazon Macie is a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect your sensitive data in AWS.
- Macie helps identify and alert you to sensitive data, such as personally identifiable information (PII)

