DATE 02/01/2022

Day 25/100 ->

AWS Secrets Manager ->

- Newer service, meant for storing secrets

- Capability to force rotation of secrets every X days

- Automate generation of secrets on rotation (uses Lambda)

- Integration with Amazon RDS (MySQL, PostgreSQL, Aurora).

- Secrets are encrypted using KMS.

- Mostly meant for RDS integration

AWS Artifact -> (not really a service)

- Portal that provides customers with on-demand access to AWS Compliance documentation & AWS agreements.
- Artifact Reports -> Allows you to download AWS security & compliance documents from

third-party auditors, like AWS ISO Certification Payment Card Industry (PCI) and System and Organization Control (SOC) reports

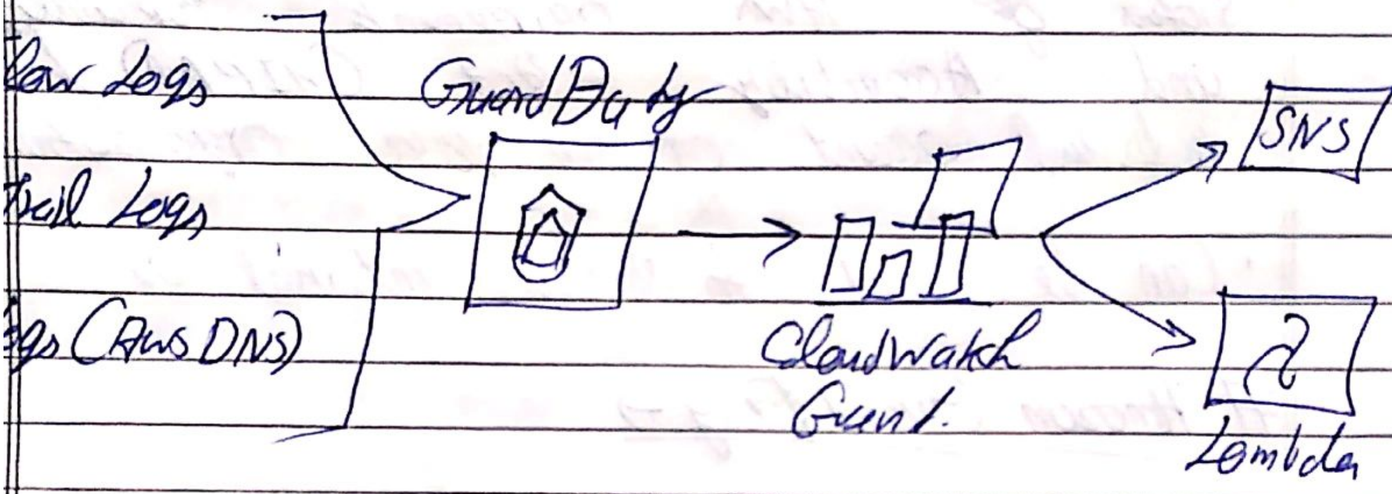
- Artifact Agreements - Allow you to review accept and track the status of AWS agreements portability and Accountility Act. (HIPAA) for an individual account or in your organization

- Can be used to support internal au

Amazon GuardDuty :-

- Intelligent Thread discovery to Protect AWS account.
- Uses Machine learning algorithm, anomaly detection, 3rd party data
- One click to enable (30 day 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

- Can setup CloudWatch Event rules to be notified in case of findings
- CloudWatch Events rules can target AWS Lambda or SNS.



Amazon Inspector

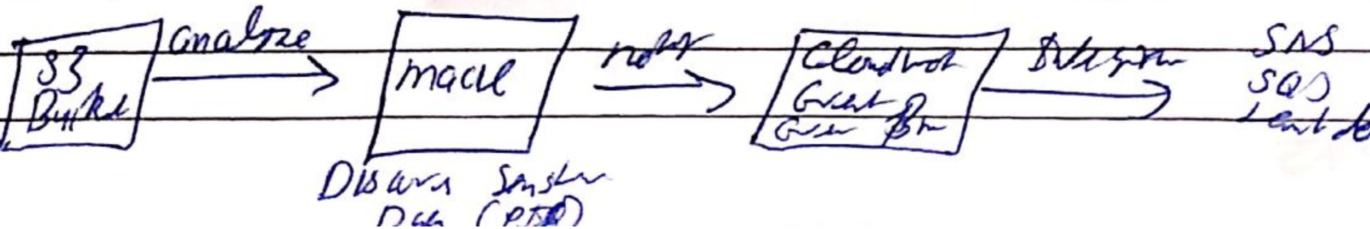
- Automated Security Assessments for EC2 instances
- Analyze the running OS against known vuln.
- Analyze against unintended network accessibility
- AWS Inspector Agent must be installed on OS in EC2 instance
- After the assessment, you get a report with lis of vulnerabilities

AWS Config

- Helps with auditing & recording compliance of your AWS resources
- Helps record Configurations & 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 change over time?
- You can receive alerts (SNS notified) for any changes
- AWS Config is a per-region service
- Can be aggregated accross region & accounts.

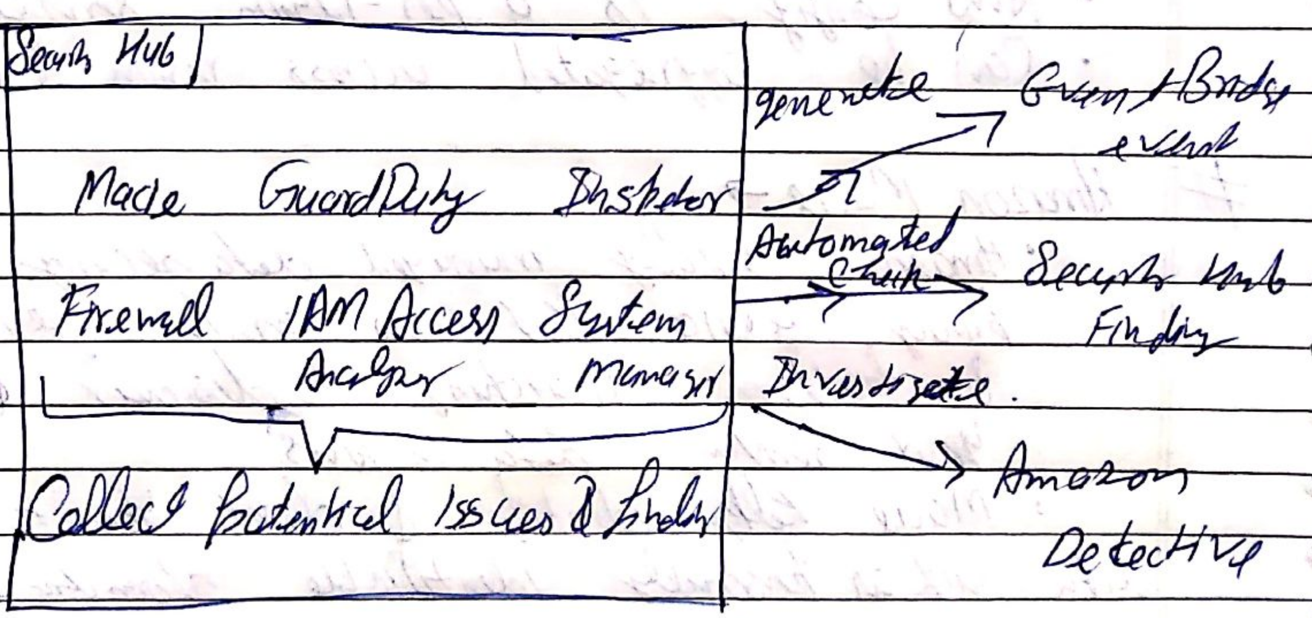
Amazon Macie →

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



AWS Security Hub →

- Central Security tool to manage security across several AWS accounts & automate security checks.
- Integrated dashboards showing current security & complaints status to quickly take action
- Automatically aggreates alert in predefined or personal findin formats from varions AWS service & AWS partner tools
  - GuardDuty
  - Inspector
  - Macie
  - IAM Access Analyzer
  - AWS System Manager
  - AWS Firewall manager
  - AWS partner Network Sol
- Must first enable the ~~AWS~~ AWS Config Service



Amazon Detective

- GuardDuty, Macie & security Hub are used to identify potential security issues or findin
- Sometimes security require deeper analysis to isolate the root cause and take action - it's a complex process
- Amazon Detective analyzes, investigates & quickly identifies the root cause of security issues or suspicious activities (using ML & graphs)
- Automatically collects & processes events from VPC flow Logs, CloudTrail, GuardDuty & create a unified view.
- Produces visualization with details & context to get the root cause.

AWS Abuse