Experiment-8: To study and implement Security as a Service on AWS/Azure

Aim: To understand the security practices available in public cloud platforms and to demonstrate various threat detection, data protection and infrastructure protection services in AWS and Azure.

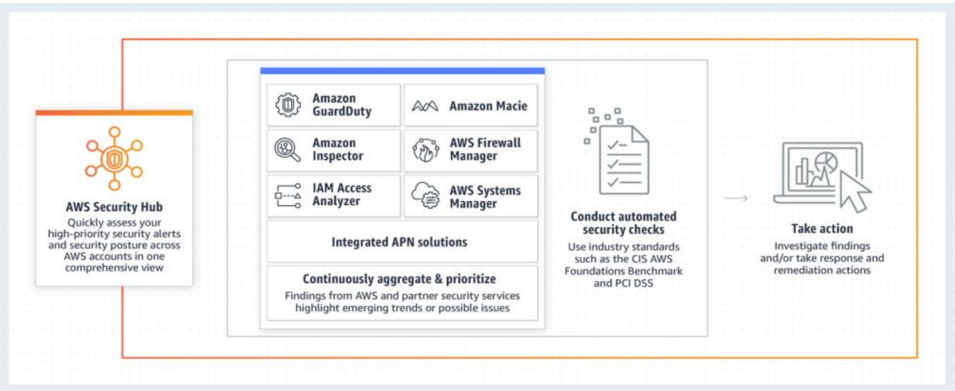
Software required: AWS subscription

Theory:
AWS offers several services for providing security as a service to any type of software that we wish to host. Some are discussed below.

Threat detection

AWS Security Hub

AWS Security Hub is a cloud security posture management service that performs security best practice checks, aggregates alerts, and enables automated remediation.


AWS Security Hub
Quickly assess your high-priority security alerts and security posture across AWS accounts in one comprehensive view
Amazon GuardDuty
Amazon Macie
Amazon Inspector
AWS Firewall Manager
IAM Access Analyzer
AWS Systems Manager
Integrated APN solutions
Continuously aggregate & prioritize
Findings from AWS and partner security services highlight emerging trends or possible issues
Conduct automated security checks
Use industry standards such as the CIS AWS Foundations Benchmark and PCI DSS
Take action
Investigate findings and/or take response and remediation actions

AWS Security Hub is a cloud security posture management service that performs automated, continuous security best practice checks against AWS resources. Security Hub aggregates security alerts (i.e. findings) from various AWS services and partner products in a standardized format so that we can more easily take action on them. To maintain a complete view of our security posture in AWS, we need to integrate multiple tools and services including threat detections from Amazon GuardDuty, vulnerabilities from Amazon Inspector,

sensitive data classifications from Amazon Macie, resource configuration issues from AWS Config, and AWS Partner Network Products. Security Hub simplifies how you understand and improve your security posture with automated security best practice checks powered by AWS Config rules and automated integrations with dozens of AWS services and partner products.

Infrastructure protection

AWS Shield

AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. AWS Shield provides always-on detection and automatic inline mitigations that minimize application downtime and latency, so there is no need to engage AWS Support to benefit from DDoS protection. There are two tiers of AWS Shield - Standard and Advanced.

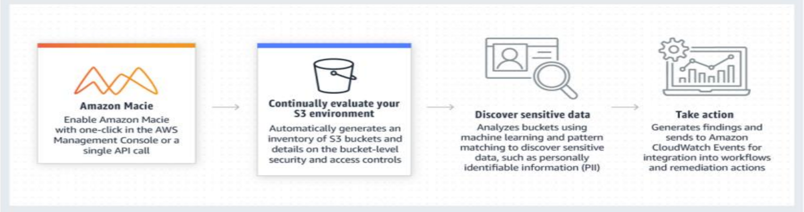
Benefits:

- **Easy to use**: Like most AWS services, AWS Shield is an easy-to-use service designed to allow you to protect your applications quickly and easily. AWS Shield can be used for existing applications or new applications using the AWS Management Console. No routing changes are required for enabling these protections.
- **Cost-efficient**: AWS Shield Standard is automatically enabled for all AWS customers at no additional cost. With AWS Shield Advanced, customers get AWS WAF and AWS Firewall Manager at no additional cost.

Data protection

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 our sensitive data in AWS.



Amazon Macie
Enable Amazon Macie with one-click in the AWS Management Console or a single API call

Continually evaluate your S3 environment
Automatically generates an inventory of S3 buckets and details on the bucket-level security and access controls

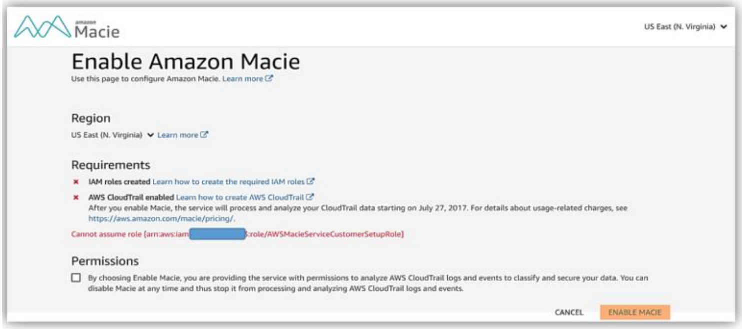
Discover sensitive data
Analyzes buckets using machine learning and pattern matching to discover sensitive data, such as personally identifiable information (PII)

Take action
Generates findings and sends to Amazon CloudWatch Events for integration into workflows and remediation actions

As organizations manage growing volumes of data, identifying and protecting their sensitive data at scale can become increasingly complex, expensive, and time-consuming. Amazon Macie automates the discovery of sensitive data at scale and lowers the cost of protecting data. Macie automatically provides an inventory of Amazon S3 buckets including a list of unencrypted buckets, publicly accessible buckets, and buckets shared with AWS accounts outside those which have been defined in AWS Organizations. Then, Macie applies machine learning and pattern matching techniques to the buckets we select to identify and alerts us to sensitive data, such as personally identifiable information (PII).

Step 1: Enabling Amazon Macie

To enable the Macie service, you must have the appropriate **IAM** roles created for the service, and additionally you will need to have **AWS Cloud Trail** enabled in your account.



Enable Amazon Macie
Use this page to configure Amazon Macie. Learn more

Region
US East (N. Virginia) Learn more

Requirements
✗ IAM roles created Learn how to create the required IAM roles
✗ AWS CloudTrail enabled Learn how to create AWS CloudTrail
After you enable Macie, the service will process and analyze your CloudTrail data starting on July 27, 2017. For details about usage-related charges, see https://aws.amazon.com/macie/pricing/.
Cannot assume role [arn:aws:iam[redacted]:role/AWSMacieServiceCustomerSetupRole]

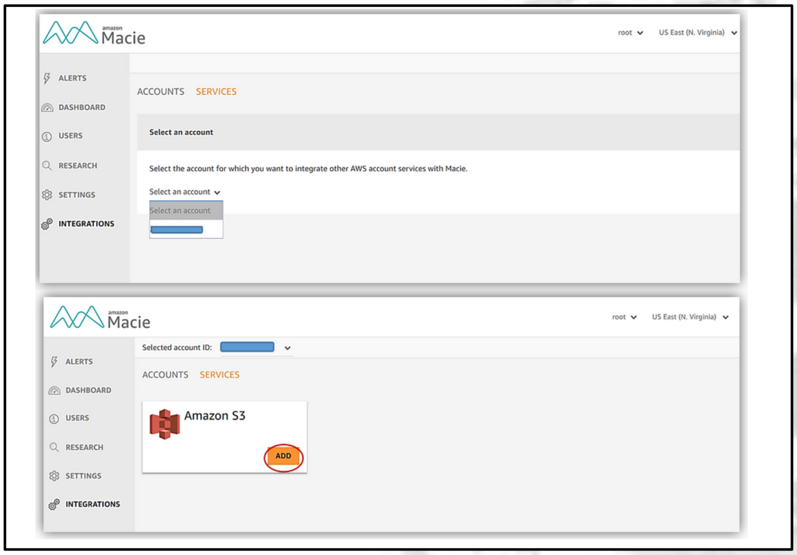
Permissions
□ By choosing Enable Macie, you are providing the service with permissions to analyze AWS CloudTrail logs and events to classify and secure your data. You can disable Macie at any time and thus stop it from processing and analyzing AWS CloudTrail logs and events.

Create these roles and turn on the AWS Cloud Trail service in your account. To make things easier for you to setup Macie, you can take advantage of a sample template for Cloud Formation provided in the Macie User Guide that will set up required IAM roles and policies for you, you then would only need to setup a trail as noted in the Cloud Trail documentation.

If you have multiple AWS accounts, you should note that the account you use to enable the Macie service will be noted as the master account, you can integrate other accounts with the Macie service but they will have the member account designation. Users from member accounts will need to use an IAM role to federate access to the master account in order to access the Macie console.

Now that your IAM roles are created and CloudTrail is enabled, you can click the **Enable Macie** button to start Macie's data monitoring and protection.

Step 2: Integrate with S3



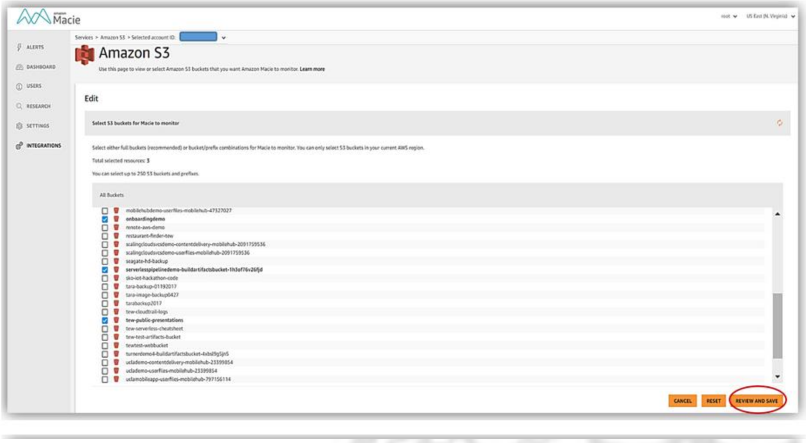
Select the account for which you want to integrate other AWS account services with Macie.

In order to integrate with S3, go to the **Integrations** tab of the Macie console. Once on the **Integrations** tab, you will see two options: **Accounts** and **Services. The Account** option is used to integrate member accounts with Macie and to set your data retention policy. If you want to integrate specific S3 buckets with Macie, you can click the **Services** option and go to the **Services** tab.

When you integrate Macie with the S3 service, a trail and a S3 bucket will be created to store logs about S3 data events. To get started, use the **Select an account** drop down to choose an account. Once your account is selected, the services available for integration are presented. You can select the **Amazon S3** service by clicking the **Add** button.

Step 3: Choose buckets that you want Macie to analyze

You can select the buckets that I want Macie to analyze, selecting the **Review and Save** button takes me to a screen which confirms that you desire object level logging by clicking **Save** button.



Services > Amazon S3 > Selected account ID: [redacted]

Amazon S3

Use this page to view or select Amazon S3 buckets that you want Amazon Macie to monitor. **Learn more**

Edit

Select S3 buckets for Macie to monitor

Select either full buckets (recommended) or bucket/prefix combinations for Macie to monitor. You can only select S3 buckets in your current AWS region.

Total selected resources: **3**

You can select up to 250 S3 buckets and prefixes.

All Buckets

- □ mobilehubdemo-userfiles-mobilehub-47527027
- ☑ **onboardingdemo**
- □ remote-aws-demo
- □ restaurant-finder-tew
- □ scalingcloudsvcsdemo-contentdelivery-mobilehub-2091759536
- □ scalingcloudsvcsdemo-userfiles-mobilehub-2091759536
- □ seagate-hd-backup
- ☑ **serverlesspipelinedemo-buildartifactsbucket-1h3of76v26fjd**
- □ sko-iot-hackathon-code
- □ tara-backup-01192017
- □ tara-image-backup0427
- □ tarabackup2017
- □ tew-cloudtrail-logs
- ☑ **tew-public-presentations**
- □ tew-serverless-cheatsheet
- □ tew-test-artifacts-bucket
- □ tewtest-webbucket
- □ turnerdemo4-buildartifactsbucket-4xbsl9g5jn5
- □ uclademo-contentdelivery-mobilehub-23399854
- □ uclademo-userfiles-mobilehub-23399854
- □ uclamobileapp-userfiles-mobilehub-797156114

Conclusion:-

Sign and Remark:

R1 (3 Marks)	R2 (2 Marks)	R3 (5 Marks)	R4 (5 Mark)	Total (15 Marks)	Signature