
AWS
re:Invent

SEC310

Data protection at scale using Amazon Macie

Neel Sendas

Senior Technical Account Manager, Amazon Web Services

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Agenda

- Drivers for Amazon Macie
- Features of Amazon Macie
- Amazon Macie Use-Case
- Key takeaways



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Related sessions

- SEC211: BBC - Driving security best practices in a decentralized org
- SEC325: Event driven data security using Amazon Macie



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Drivers for Amazon Macie



Productivity trends result in organizations generating growing volumes of data, distributed across multiple shared resources



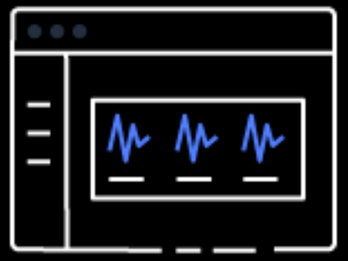
Increased challenge to comply with data privacy regulations with new additional requirements and expanded definitions of sensitive data



Customers have to take on the expense of monitoring and complexity of continuously updating data classifications

Amazon Macie

Discover and protect your sensitive data at scale



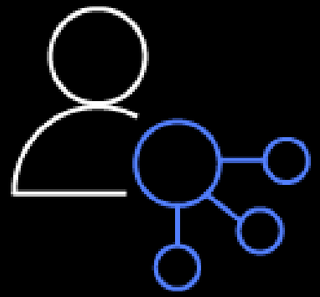
Gain visibility and evaluate

- Bucket inventory
- Bucket policies



Discover sensitive data

- Inspection jobs
- Flexible scope



Centrally manage at scale

- AWS Organizations
- Managed & custom data detections



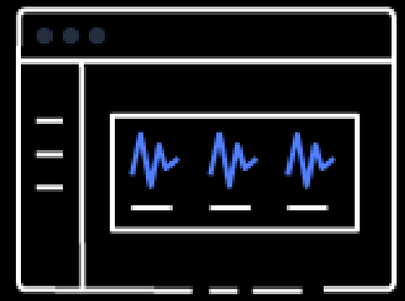
Automate and take actions

- Detailed findings
- Management APIs

Key capabilities – Gain visibility and evaluate

Provides customers visibility into S3 bucket inventory
- Number of buckets
- Storage size
- Object count

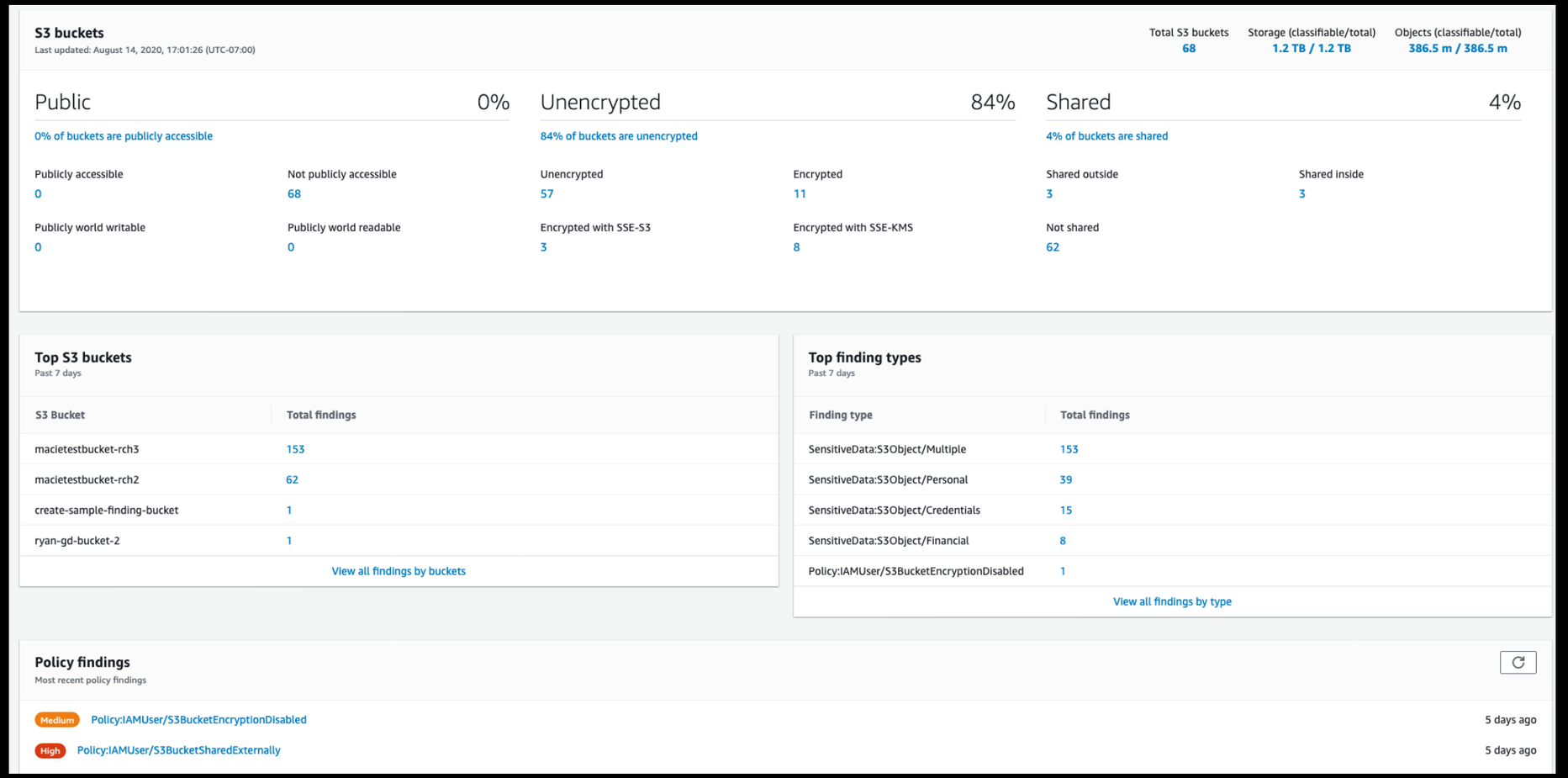
Monitors changes to S3 bucket policies
- Publicly accessible
- Unencrypted
- Shared outside of the account
- Replicated to external accounts



Across multiple accounts and automatically includes new buckets

Key capabilities - Gain visibility and evaluate

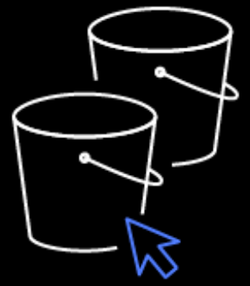
Provides customers visibility into S3 bucket inventory



Filtered by Account
Total bucket count updated in real time, storage and object count updated daily

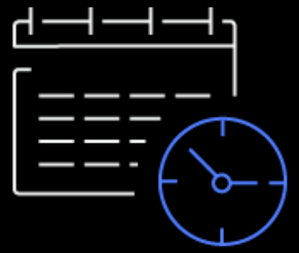
Key capabilities - Discover sensitive data

Ongoing evaluation of your Amazon S3 environment and data



Select target for data discovery

Create and schedule jobs



Define the scope

Scheduled frequency (one-time, daily, weekly, monthly)

Object criteria (Tags, modified time, extension type, size)



Review status (complete, cancelled, idle)

Take actions (Cancel, copy)

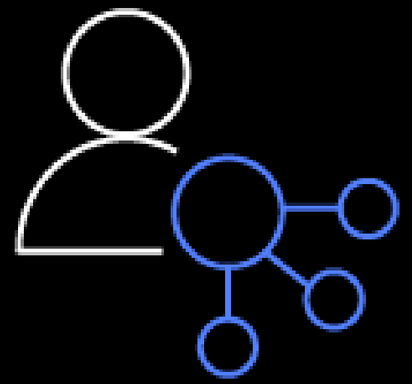
Key capabilities - Centrally manage at scale

Administrator/member setup

- AWS organizations support up to 5,000 member accounts
- Invitation method supports up to 1,000 member accounts

Macie administrator can create jobs on behalf of members

- One-click deployment with no upfront data source integration



Once enabled, Macie generates an ongoing Amazon S3 resource summary across accounts that includes bucket and object counts as well as the bucket-level security and access controls.

Key capabilities – Automate and take actions

Export results to S3 bucket
- Store all sensitive data discovery results in an S3 bucket

Automated actions on alerts
- Simplify with AWS Lambda and Amazon EventBridge

Management APIs
- Integrate with additional services and tools
- Support for AWS CloudFormation



Amazon Macie Use Case



AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Data protection challenges



S3 Buckets provisioned manually and through terraform



All buckets tagged



Encryption required and no public buckets



Limited ability to centrally review this info



Required outside processes to know when a bucket is created



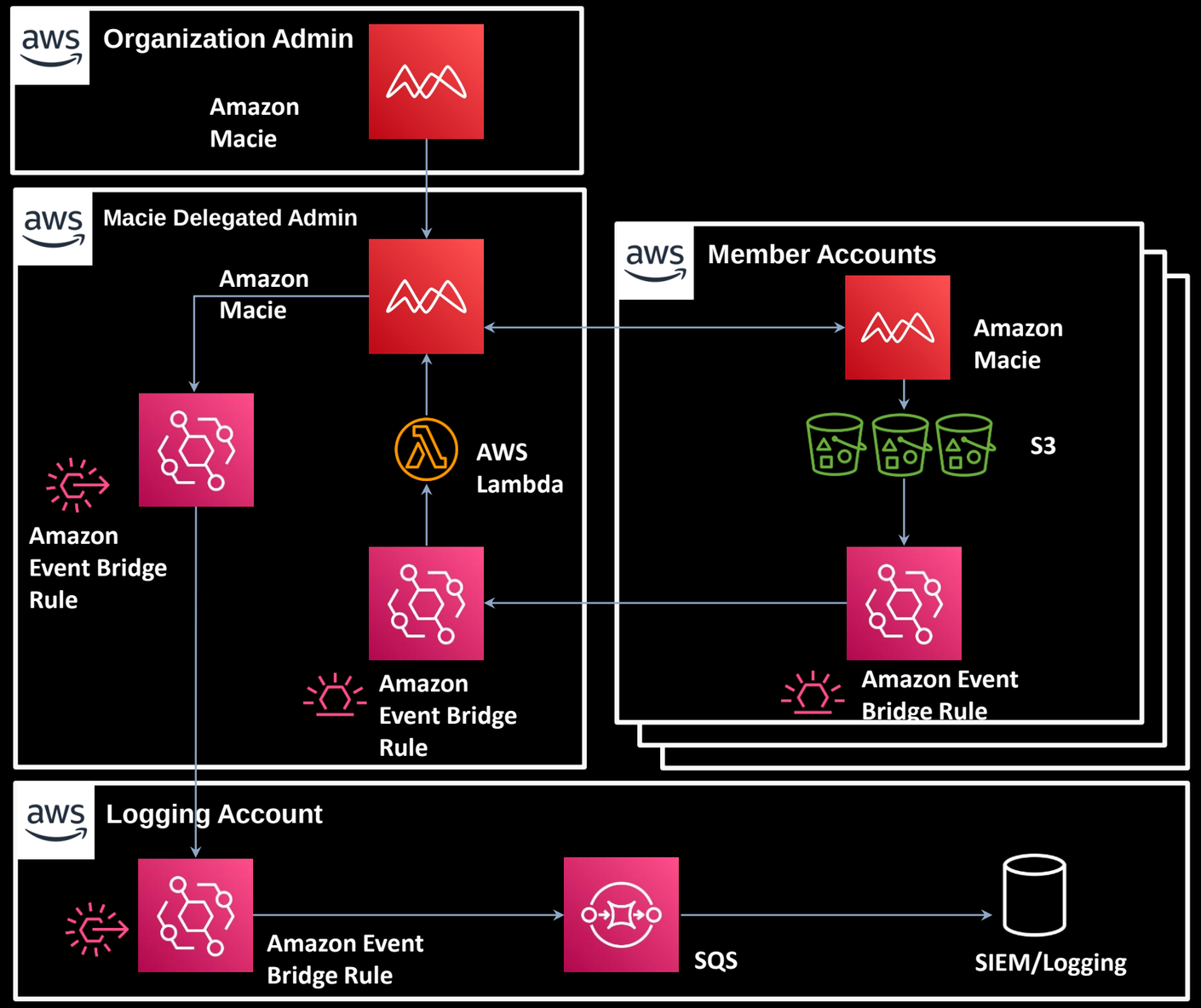
Difficult and decentralized data identification

Macie architecture

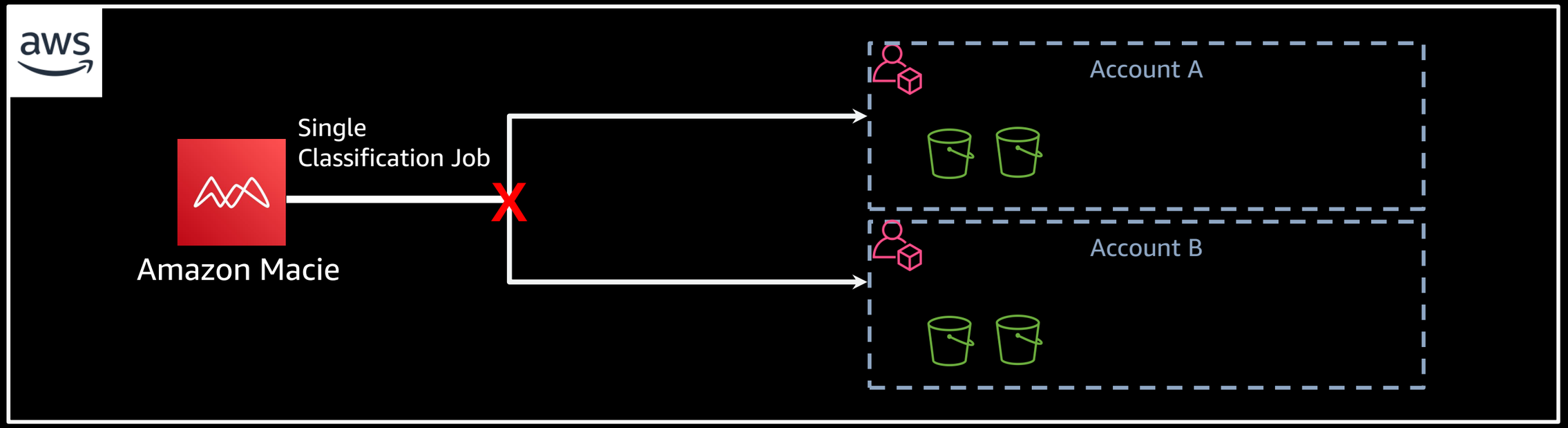
Organizations
a. Start there before implementing Macie

Delegation account
a. Allows for using administrator account for orchestration

Setup
a. Auto enable on new accounts
b. Add existing accounts via script

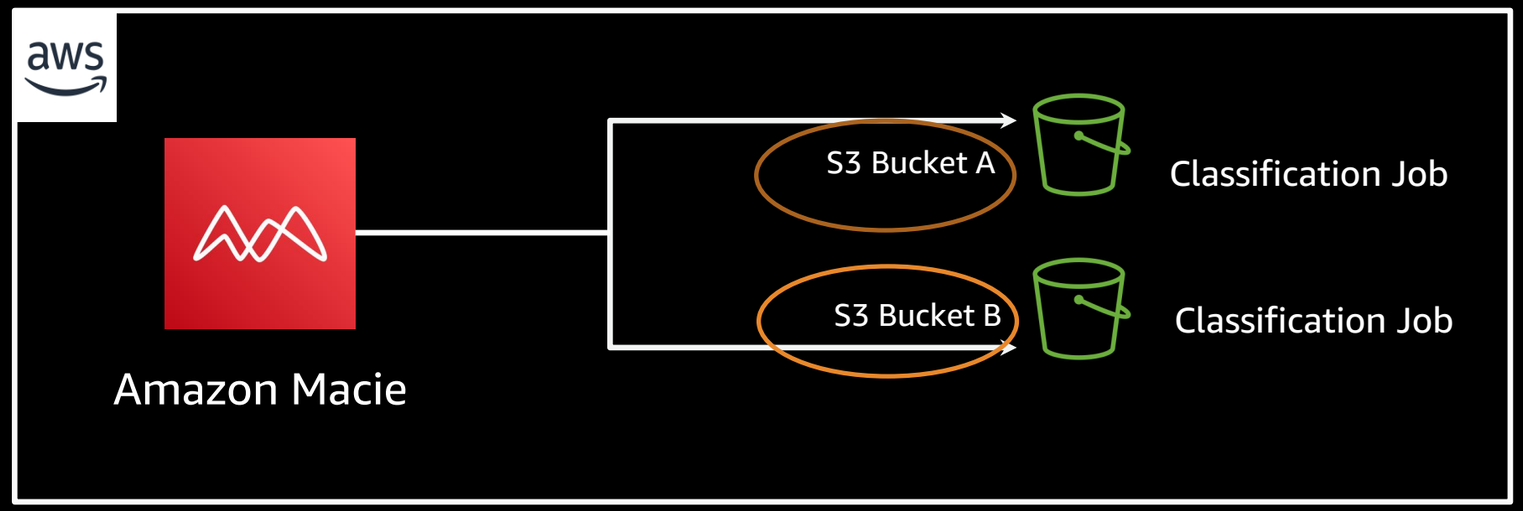


Management considerations



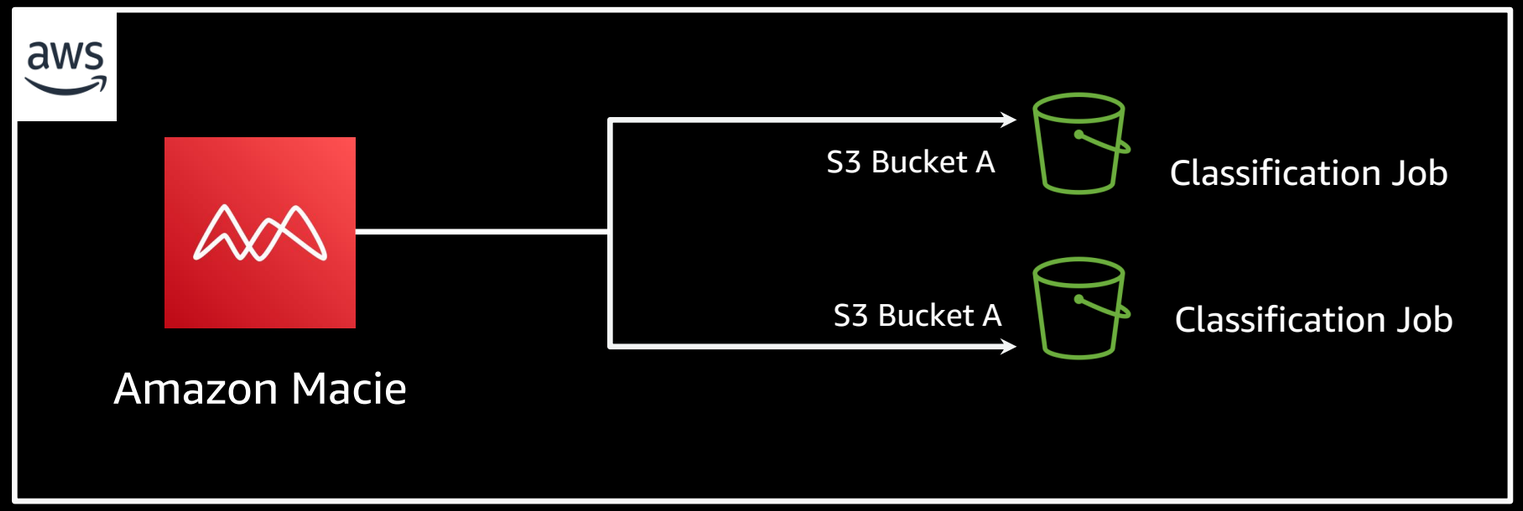
- Use a consistent and descriptive naming standard for jobs
- Tag buckets during scanning to confirm a specific bucket has a job
- If deploying infrastructure through CloudFormation, make change through CloudFormation as well

Cost considerations



DEFAULT:

- One job per S3 bucket
- Ensure you can track when an S3 bucket has a job tied to it



WARNING:

- It is possible to create multiple classification jobs for a single bucket
- but this will incur classification costs n times

Automated remediation

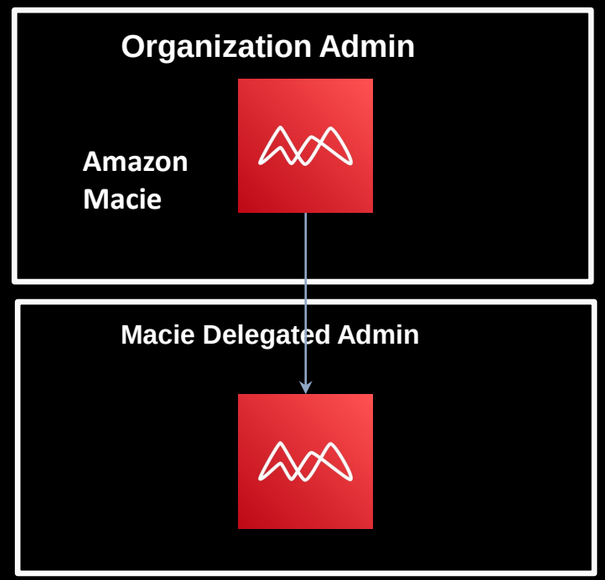


AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Delegate an administrator

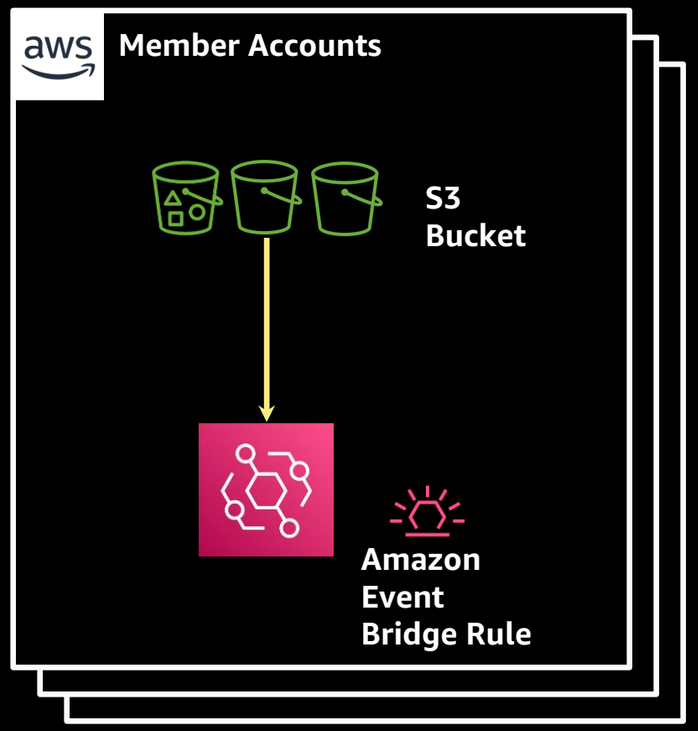
Delegating an admin is a few clicks through the console, or a single CLI call.



aws macie2 enable-organization-admin-account --admin-account-id 123XXXXXX

Track S3 bucket lifecycle via EventBridge rules

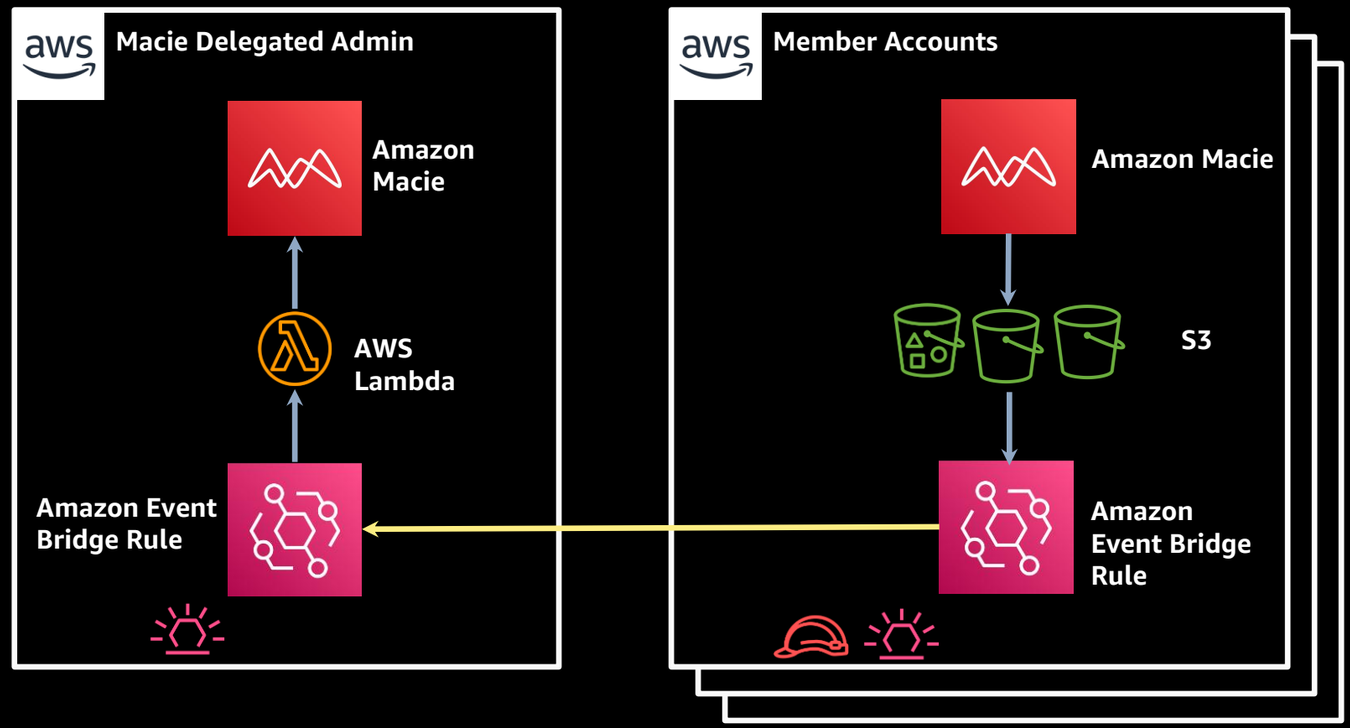
```
{
 "detail-type": [
        "AWS API Call via CloudTrail"
 ],
 "source": ["aws.s3"],
 "detail": {
        "eventSource": [
                "s3.amazonaws.com"
        ],
        "eventName": [
                "CreateBucket",
                "DeleteBucket"
        ]
 }
}
```



Targeting a cross account event bus

A few things are required to set this up

- An event bus and rule in the delegation account
- A role in the member account, targeting the event bus
- An event rule in the member account
- A Lambda for creating jobs

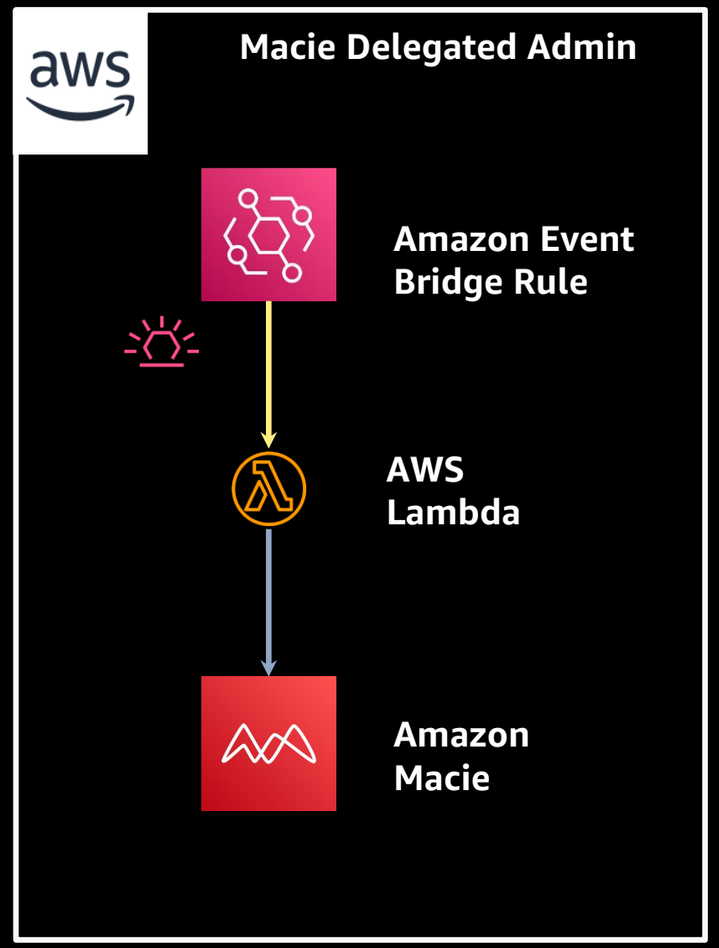


Create/cancel classification jobs from S3 events

- Identical event rule in Macie Delegated Admin account
- Listens for events sent via EventBus
- Triggers Lambda to create or delete classification job

Classification job definitions will determine what to include in jobs
example: VPC flow logs

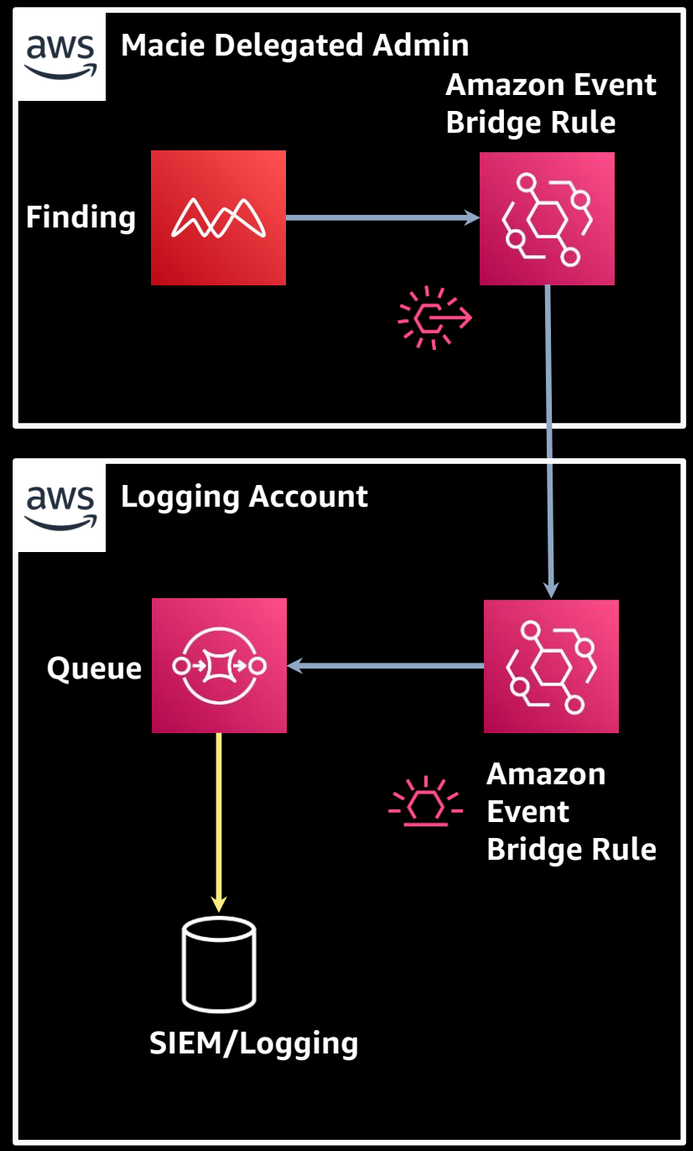
```
{
  "tagScopeTerm": {
    "comparator": "EQ",
    "key": "string",
    "tagValues": [
      {"key": "Ignore", "value": "true"},
    ],
    "target": "S3_OBJECT"
  }
}
```



Take action on job findings

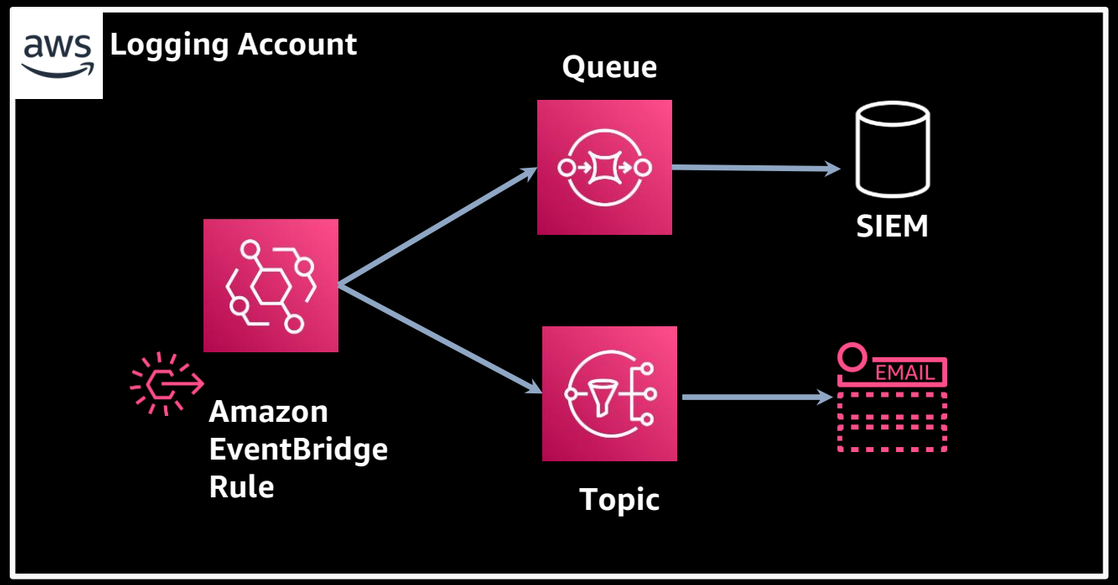
Classification job findings can then trigger an event rule which follows the same pattern

```
{
  "source":[
    "aws.macie"
  ],
  "detail-type":[
    "Macie Finding"
  ]
}
```



Send events to multiple destinations

Fan out architecture allows Macie findings to be consumed by Security Information and Event Management (SIEM) or processed by other services



Key takeaways

- Centralized Macie management and one-click enablement across all accounts
- Review detailed discovery and create actionable plan
- ONLY pay for buckets that you include in a classification job
- Operationalize job finding through routing rules

Thank you!

Neel Sendas
Senior Technical Account
Manager, Amazon Web Services

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Please complete the session survey

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.