
AWS
re:Invent

SEC210

Protecting sensitive data with Amazon Macie and Amazon GuardDuty

Himanshu Verma

WW Security Specialist

AWS

AWS re:Invent

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

Key takeaways

- Introduction
- Key capabilities of Amazon Macie and Amazon GuardDuty
- How AWS security services help protect data in Amazon Simple Storage Service (Amazon S3)
- Example use cases
- Next steps



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

Amazon Macie and Amazon GuardDuty: Key capabilities



AWS re:Invent

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

What is Amazon Macie?

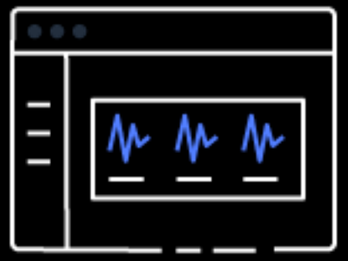


Amazon Macie is a fully managed data security and data privacy service that uses machine learning and pattern matching to discover and protect your sensitive data in AWS

- Discover your sensitive data at scale
- Understand what is accessible (public, shared, unencrypted)

Amazon Macie: Key features

DISCOVER AND PROTECT YOUR SENSITIVE DATA AT SCALE



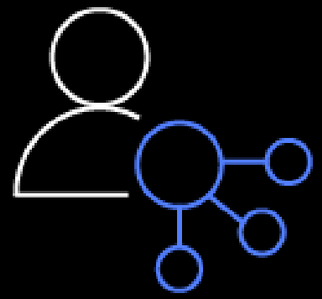
Gain visibility and evaluate

- Bucket inventory
- Bucket policies



Discover sensitive data

- Inspection jobs
- Flexible scope



Centrally manage at scale

- AWS organizations
- Managed and custom data detections



Automate and take actions

- Detailed findings
- Management APIs

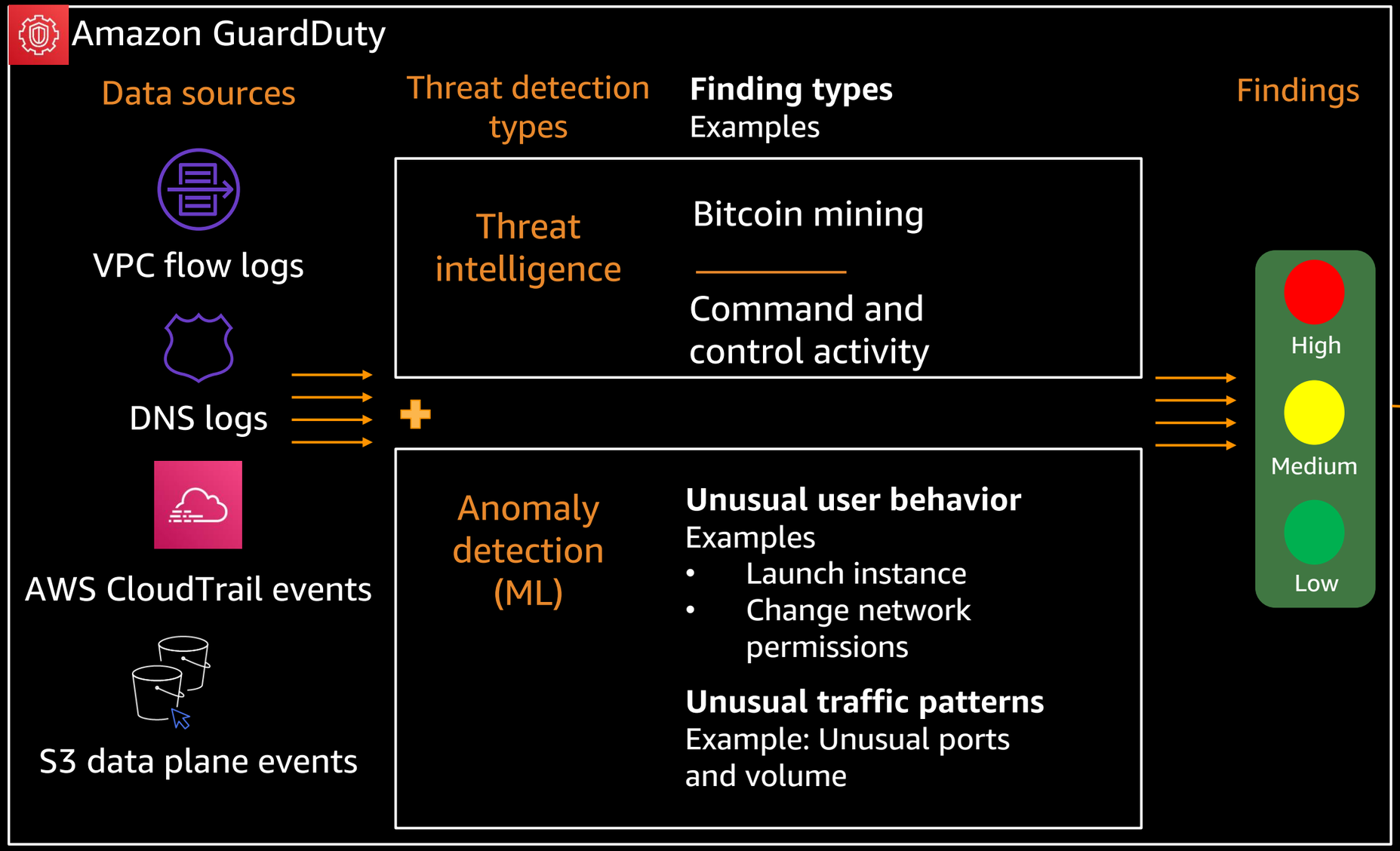
What is Amazon GuardDuty?



Amazon GuardDuty is a threat detection service that uses machine learning, anomaly detection, and integrated threat intelligence to identify and prioritize potential threats

- Identify malicious and highly suspicious activity
- Protect AWS accounts, workloads, and data stored in Amazon S3

Amazon GuardDuty: Key features



How can Amazon Macie and Amazon GuardDuty help protect data in Amazon S3?



AWS re:Invent

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

Scalable and centralized management

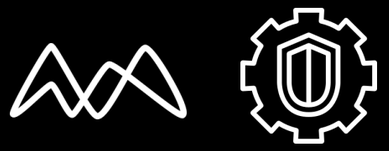
Administrator / member setup



- Designate a delegated administrator



- Add all member accounts

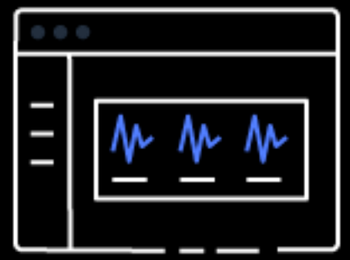


- Auto-enable Amazon Macie on all accounts
- Auto-enable Amazon GuardDuty on all accounts

Evaluate bucket security posture

GAIN VISIBILITY AND EVALUATE

- Gain visibility into S3 bucket inventory
  - Number of buckets
  - Storage size
  - Object count
- Monitor changes to S3 bucket policies
  - Publicly accessible buckets
  - Encrypted vs. unencrypted
  - Shared outside of the account
  - Replicated to external accounts

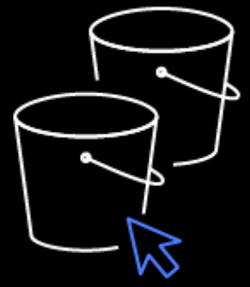


Automatically and continuously updated for all accounts, with alerts for policy findings

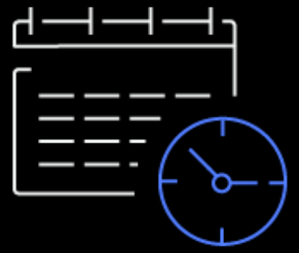
Run inspection jobs on datasets

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 (1-time, daily, weekly, monthly)
- Object criteria (tags, modified time, extension type, size)



- Review classification findings
- Managed data identifiers
  1. *Financial (card, bank account numbers)*
  2. *Personal (names, address, contact)*
  3. *National (passport, ID, driver license)*
  4. *Medical (healthcare, drug agency)*
  5. *Credentials and secrets (AWS secret keys, private keys)*
- Custom data identifiers (*RegEx*)

Detect malicious and anomaly behavior



PROACTIVELY DETECT THREATS TO DATA IN AMAZON S3

Policy

- Bucket made public
- Block public access disabled
- Logging disabled
- Root credentials used

Malicious access

- Data discovery, exfiltration, or modification from:
  - Tor
  - Leaked instance credentials
  - Malicious IPs

Anomalous behavior

- Unusual location
- Unusual bucket
- Unusual volume
- Unusual error volume

Automatically and continuously updated for all buckets in an account

Automate response and remediation

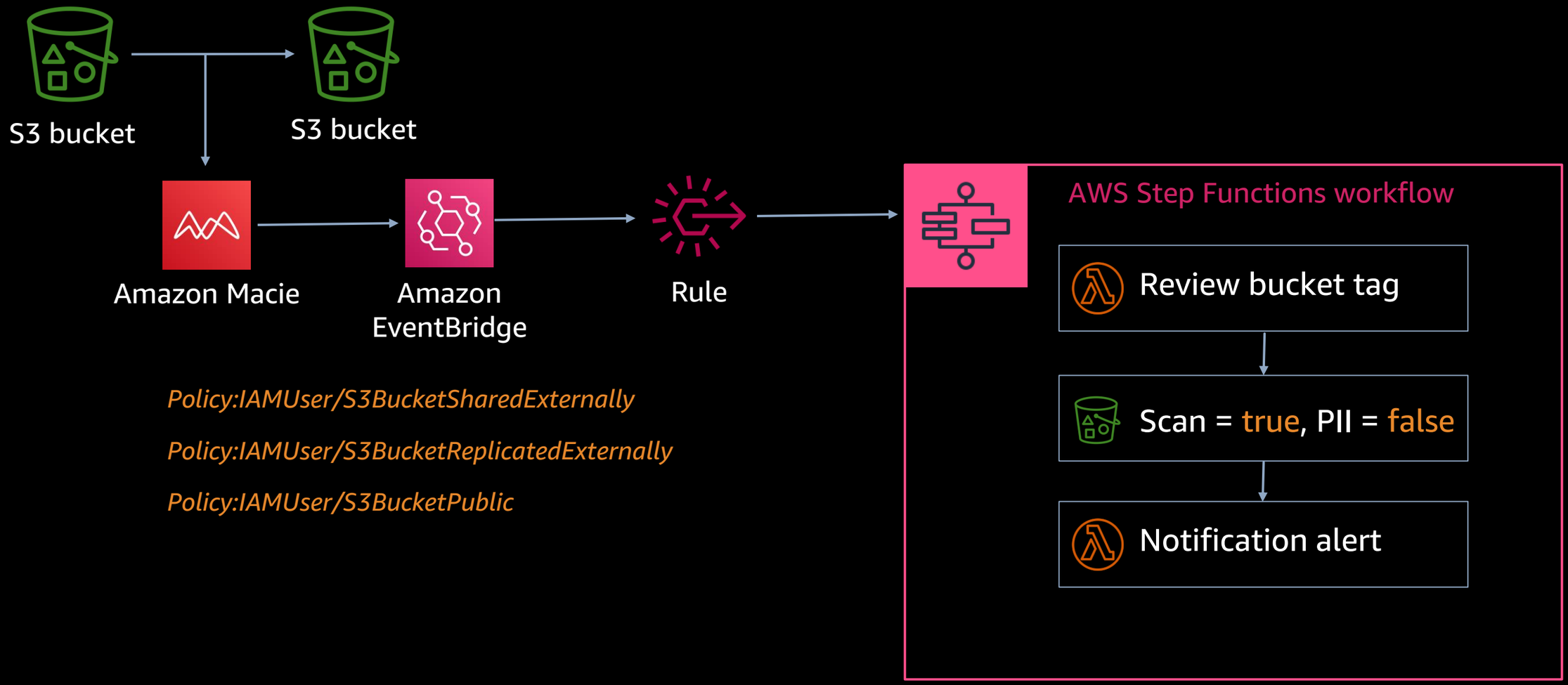


AWS re:Invent

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

Amazon Macie

TRIGGER ALERTS ON BUCKET TAGS AND POLICY FINDINGS



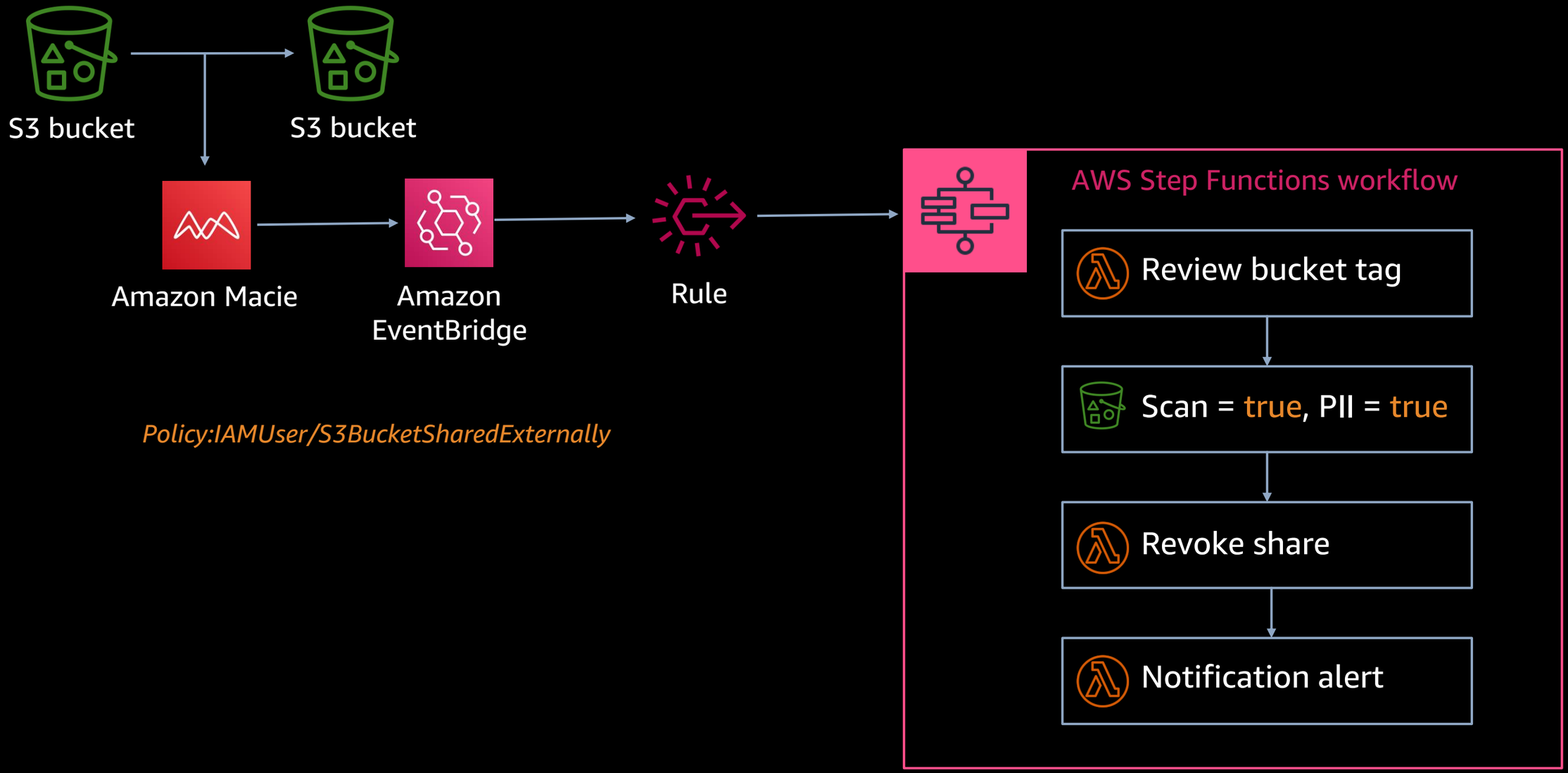
Policy:IAMUser/S3BucketSharedExternally

Policy:IAMUser/S3BucketReplicatedExternally

Policy:IAMUser/S3BucketPublic

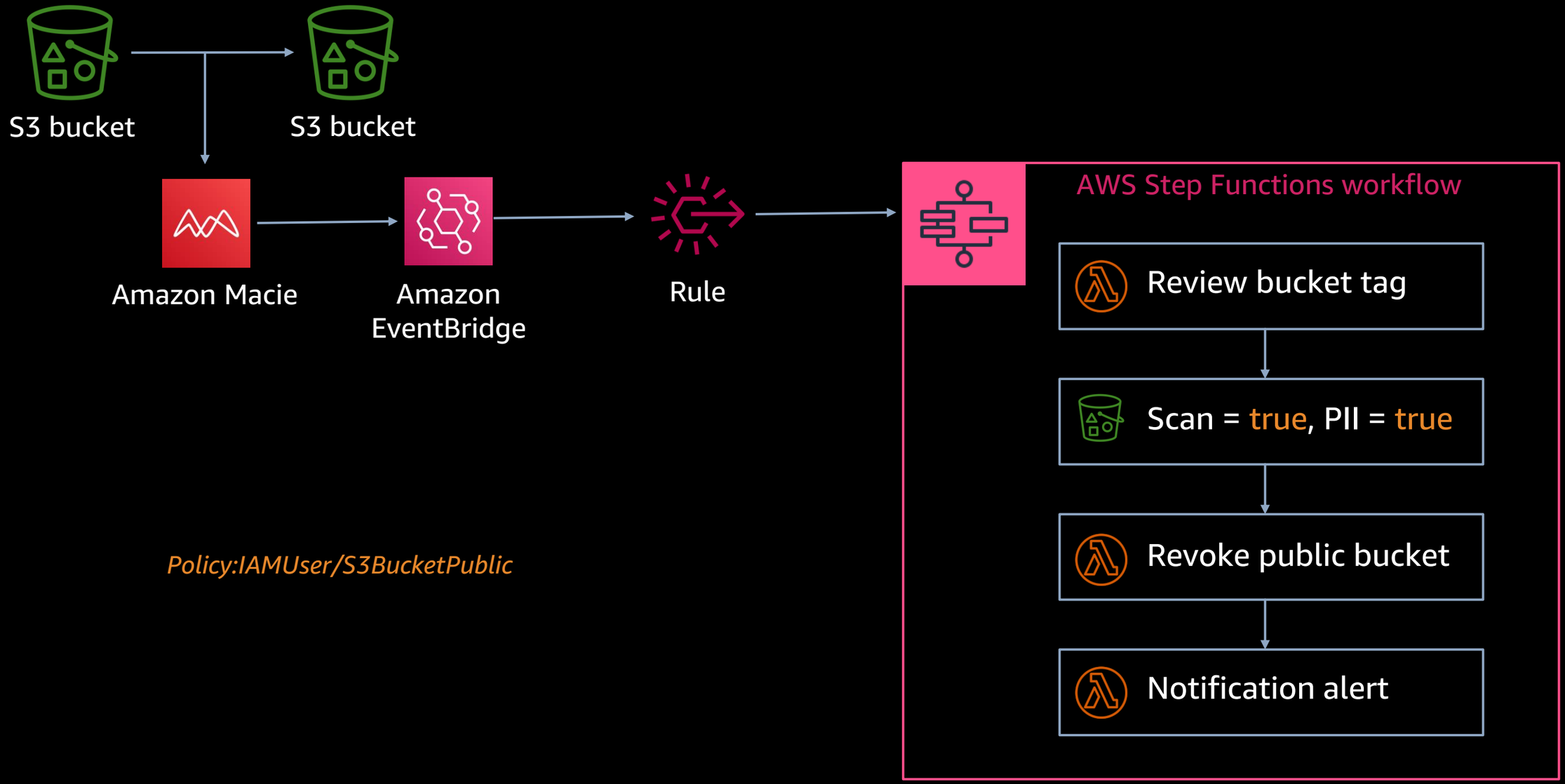
Amazon Macie

REVIEW AND TAKE ACTIONS ON POLICY FINDINGS FOR BUCKETS WITH SENSITIVE DATA



Amazon Macie

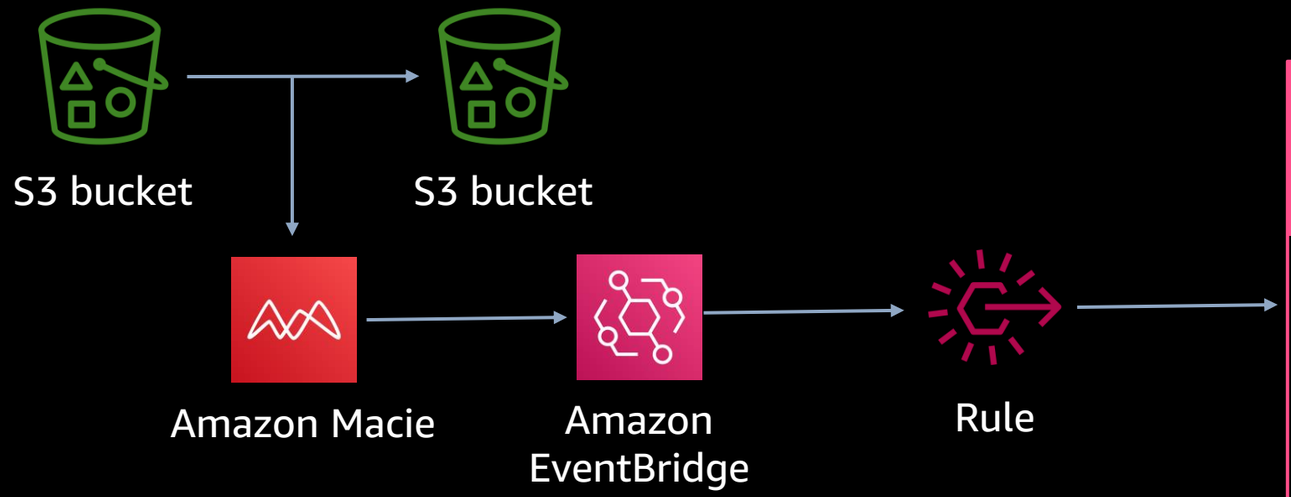
REVIEW AND TAKE ACTIONS ON POLICY FINDINGS FOR BUCKETS WITH SENSITIVE DATA



Policy:IAMUser/S3BucketPublic

Amazon Macie

PROTECT SENSITIVE DATA AND AUTOMATE CONTROLS



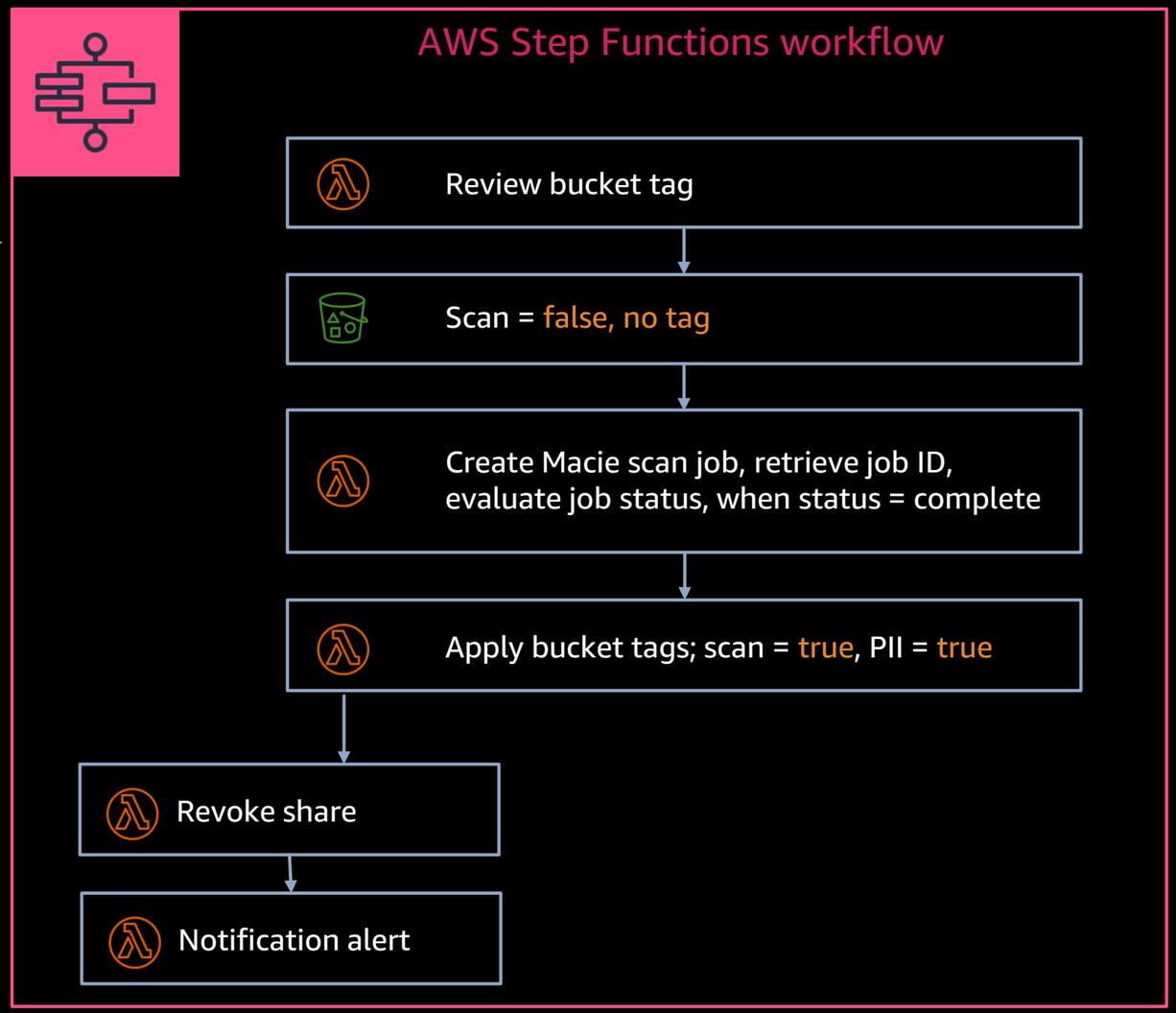
Policy:IAMUser/S3BucketSharedExternally

SensitiveData:S3Object/Personal

SensitiveData:S3Object/Financial

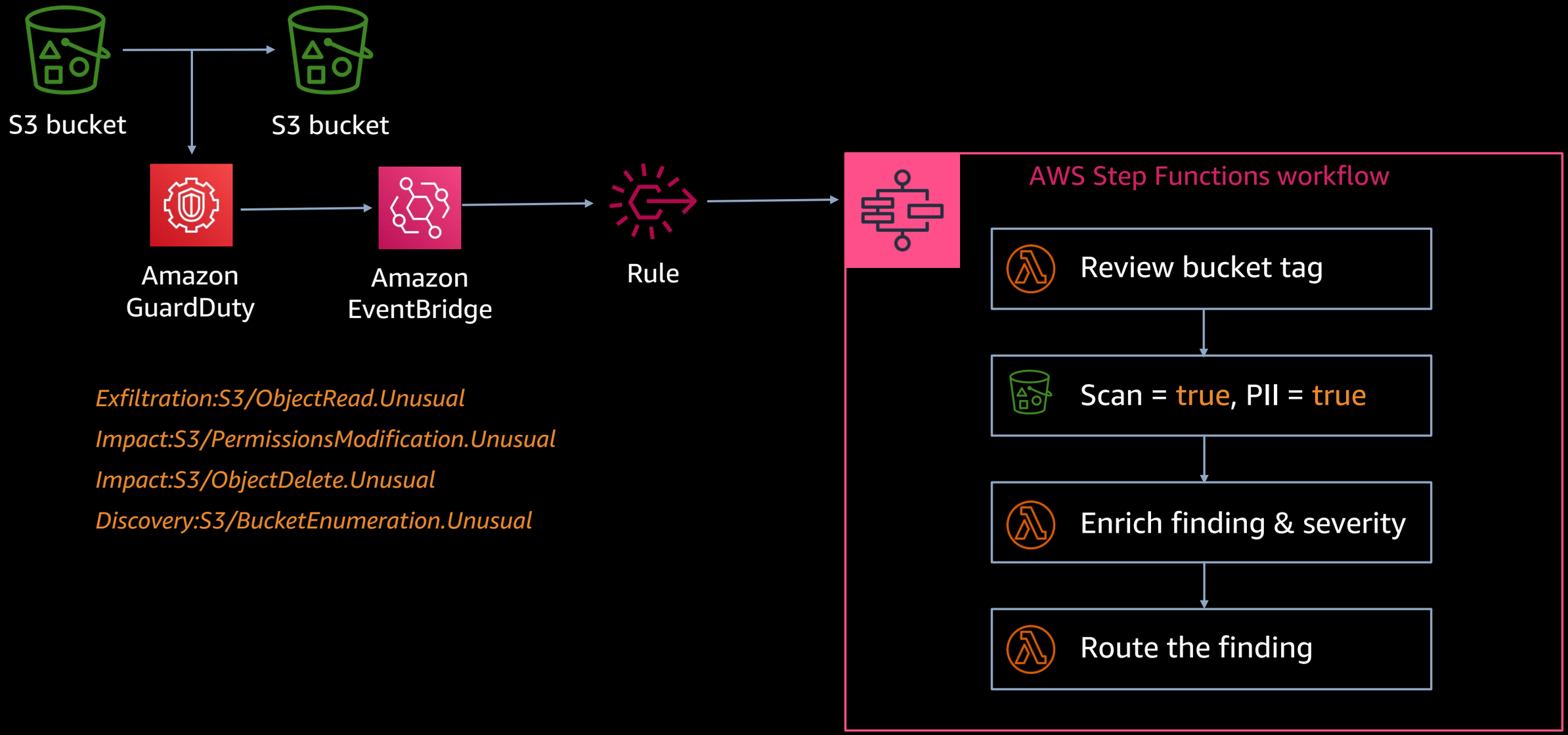
SensitiveData:S3Object/Credentials

SensitiveData:S3Object/CustomIdentifier



Amazon GuardDuty

ENRICH SECURITY TEAM ALERTS FOR POTENTIAL THREATS ON BUCKETS WITH SENSITIVE DATA



Exfiltration:S3/ObjectRead.Unusual

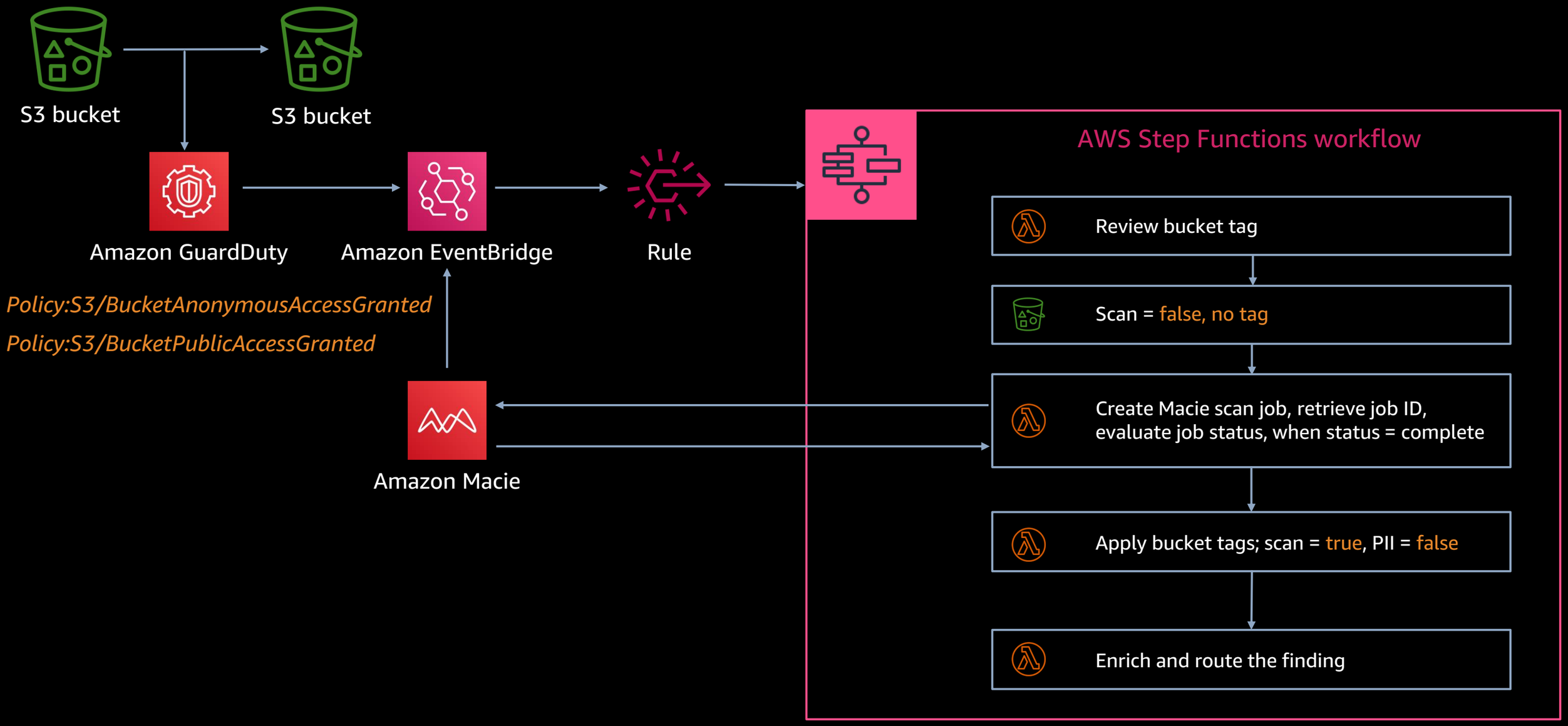
Impact:S3/PermissionsModification.Unusual

Impact:S3/ObjectDelete.Unusual

Discovery:S3/BucketEnumeration.Unusual

Layered security to protect sensitive data

COMBINATION OF SECURITY SERVICES TO IDENTIFY THREATS AND PROTECT DATA



Use cases



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

Continuous inventory evaluation and data governance

Maintain regulatory compliance







Compliance teams are required to monitor where sensitive data resides, protect it properly, and provide evidence that they are enforcing data security and privacy to meet regulatory compliance requirements

Threat detection and monitoring

Automate threat response and remediation







Continuously monitor and profile S3 data access events (data plane operations) and S3 configurations (control plane APIs) to detect suspicious activities:

- Requests coming from an unusual geolocation
- Disabled preventive controls such as S3 block public access
- API call patterns consistent with an attempt to discover misconfigured bucket permissions

Automated response and remediation

Identify, protect, and continuously monitor for risks



- AWS Security Hub collects findings from the security services enabled across your AWS accounts, such as S3 findings from Amazon GuardDuty and policy findings from Amazon Macie
- Security Hub aggregates findings into prebuilt dashboards that show you the current security status of your environment as well as trends so customers can easily identify potential issues and take the necessary next steps
- For example, you can send findings to ticketing, chat, email, or automated remediation systems using integration with Amazon CloudWatch events or Amazon EventBridge

Next steps

- Disable Macie classic (Macie version 1)

  Enable Macie on all accounts

- Enable GuardDuty on all accounts

  Active accounts – enable GuardDuty for S3 protection

- 30-day trial for Amazon GuardDuty and Amazon Macie

  Per account, no cost*

- Take action on the findings

  Filter, suppress, automate response with EventBridge

*Every account that enables Amazon Macie gets at no cost the first 30 days of bucket-level inventory and evaluation for access controls and encryption
Note: This does not include sensitive data discovery, which is charged separately

Thank you!



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.