IAM Best Practices

- User Accounts
- Password Policies
- Credential Rotation
- Enable MFA
- Use Lease Privilege Guidelines
- Use IAM Roles
- Implement Policy Conditions
- Enable CloudTrail

IAM Best Practices

CHAPTER 8

User Accounts

EPISODE 8.01

DEMO

- Creating user accounts

Password Policies

EPISODE 8.02

Default Password Policy

- Min 8 characters
- Max 128 characters
- At least 3 of these 4 character types:
  - Uppercase
  - Lowercase
  - Numbers
  - Special characters
- Can’t be the same as the account name or email

Password Best Practices

- Change password periodically
- Use a unique password for AWS
- Avoid easily guessed passwords

DEMO

- Setting IAM User Password Policies
- https://docs.amazonaws.cn/en_us/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html

Credential Rotation

EPISODE 8.03

DEMO

- Password Rotation Policies

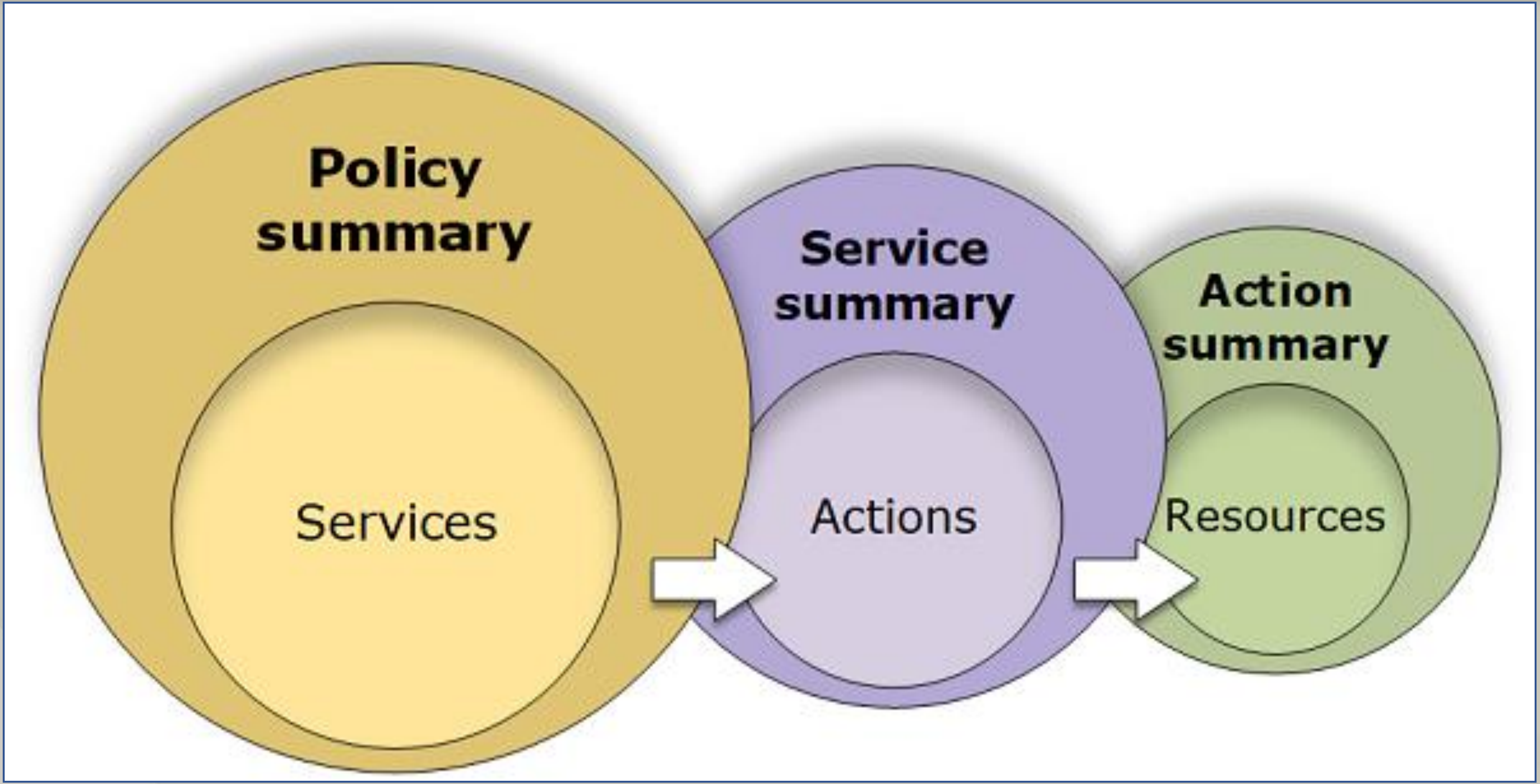
Least Privilege Guidelines

EPISODE 8.04

Least Privilege

- Grant only the access needed
  - Granting more access creates vulnerabilities
    - Opens the door to mistakes
  - Opens the door for attackers

Review Permissions



DEMO

- Viewing Policy Summaries

IAM Roles

EPISODE 8.05

DEMO

- Creating Roles
- Configuring Roles

Policy Conditions

EPISODE 8.06

DEMO

- Creating an IAM policy
- Defining policy conditions
- Additional Best Practices
  - https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html

Enable CloudTrail

EPISODE 8.07

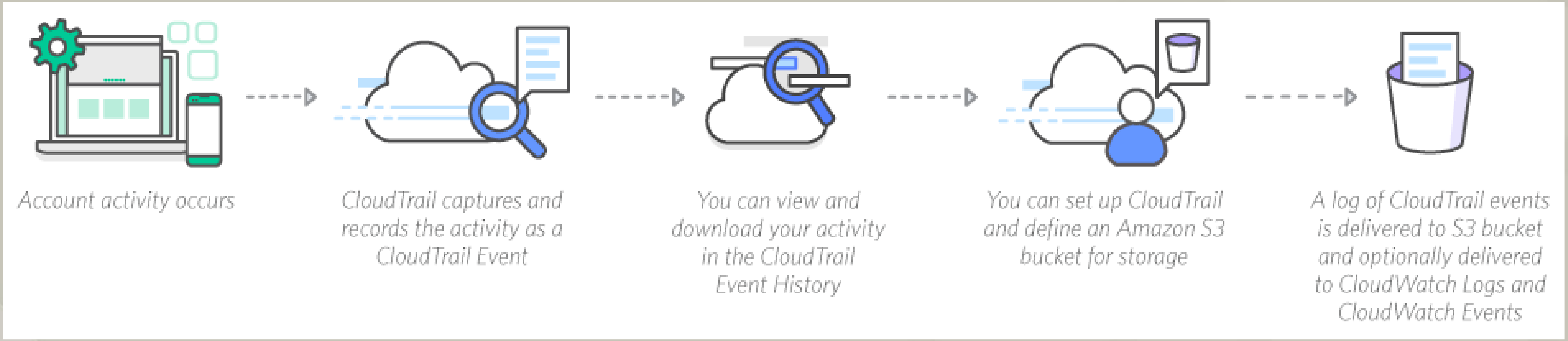
CloudTrail

- Logging services
  - Governance
  - Compliance
  - Auditing

CloudTrail

- Event histories
  - Management Console
  - AWS SDK
  - Command line
  - Additional AWS services

CloudTrail



Account activity occurs

CloudTrail captures and records the activity as a CloudTrail Event

You can view and download your activity in the CloudTrail Event History

You can set up CloudTrail and define an Amazon S3 bucket for storage

A log of CloudTrail events is delivered to S3 bucket and optionally delivered to CloudWatch Logs and CloudWatch Events

DEMO

- Enabling CloudTrail

- EPISODE 8.02
- Password Policies

Default Password Policy

- Min 8 characters
- Max 128 characters
- At least 3 of these 4 character types:
  - Uppercase
  - Lowercase
  - Numbers
  - Special characters
- Can’t be the same as the account name or email

Password Best Practices

- Change password periodically
- Use a unique password for AWS
- Avoid easily guessed passwords

- EPISODE 8.03
- Credential Rotation

Credential Rotation

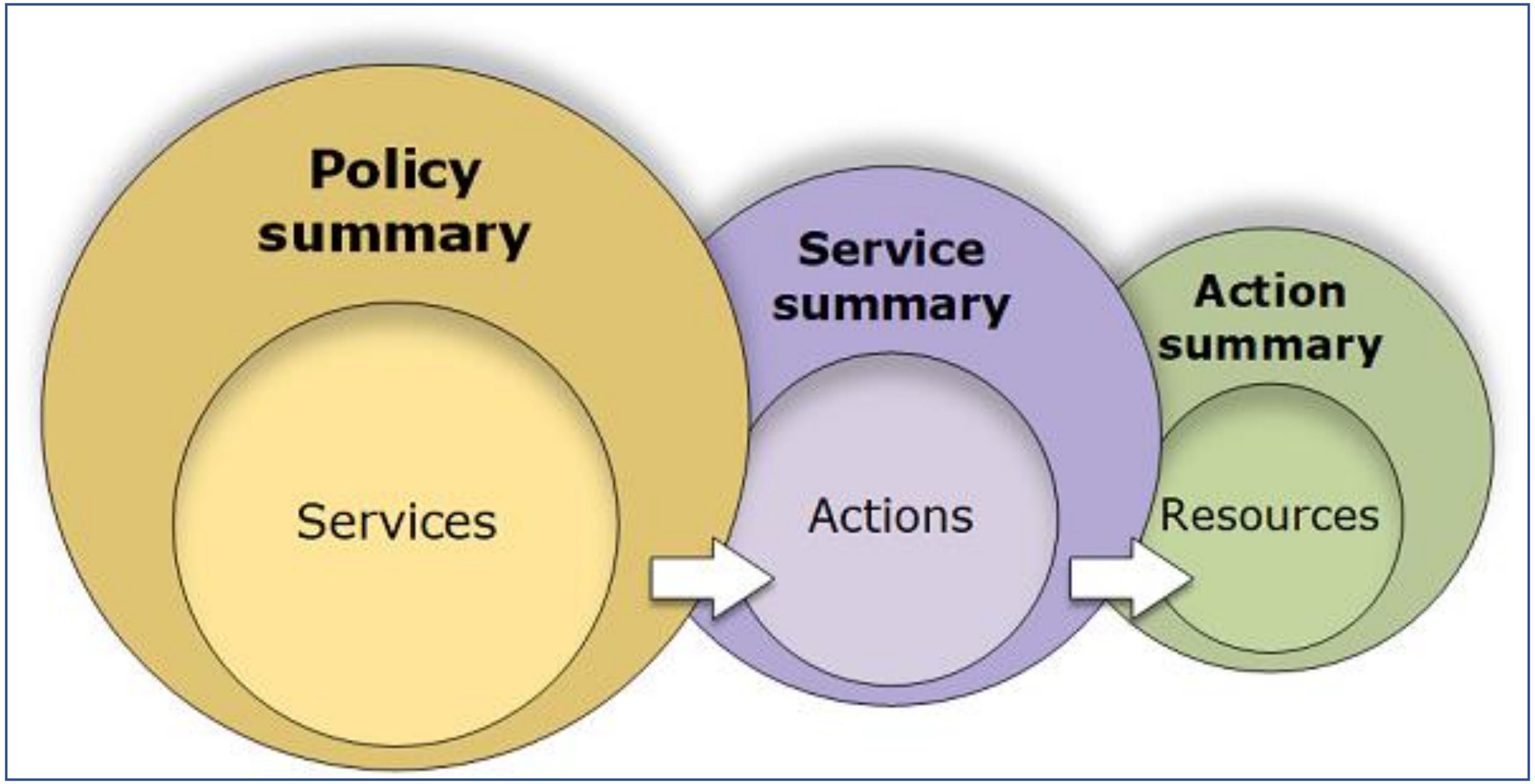
- Reduces vulnerabilities
  - Limits the time for an attack
  - Reminds users of security focus
  - Helps reduce reuse of passwords across systems

- EPISODE 8.05
- Use Least Privilege Guidelines

Least Privilege Principle

- Grant only the access needed
  - Granting more access creates vulnerabilities
    - Opens the door to mistakes
  - Opens the door for attackers

Review Permissions



- EPISODE 8.04
- Enable CloudTrail

CloudTrail

- Logging services

  - Governance

  - Compliance

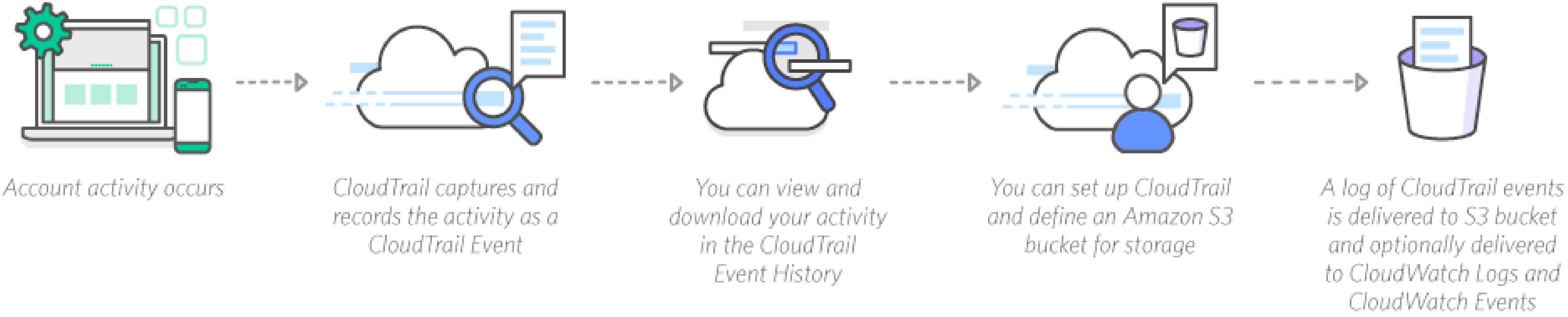
  - Auditing

CloudTrail

- Event histories

  - Management Console
  - AWS SDK
  - Command line
  - Additional AWS services

CloudTrail



Account activity occurs

CloudTrail captures and records the activity as a CloudTrail Event

You can view and download your activity in the CloudTrail Event History

You can set up CloudTrail and define an Amazon S3 bucket for storage

A log of CloudTrail events is delivered to S3 bucket and optionally delivered to CloudWatch Logs and CloudWatch Events