

# Common security pitfalls in AWS for highly regulated industries

# % whoami Daniel Rankov

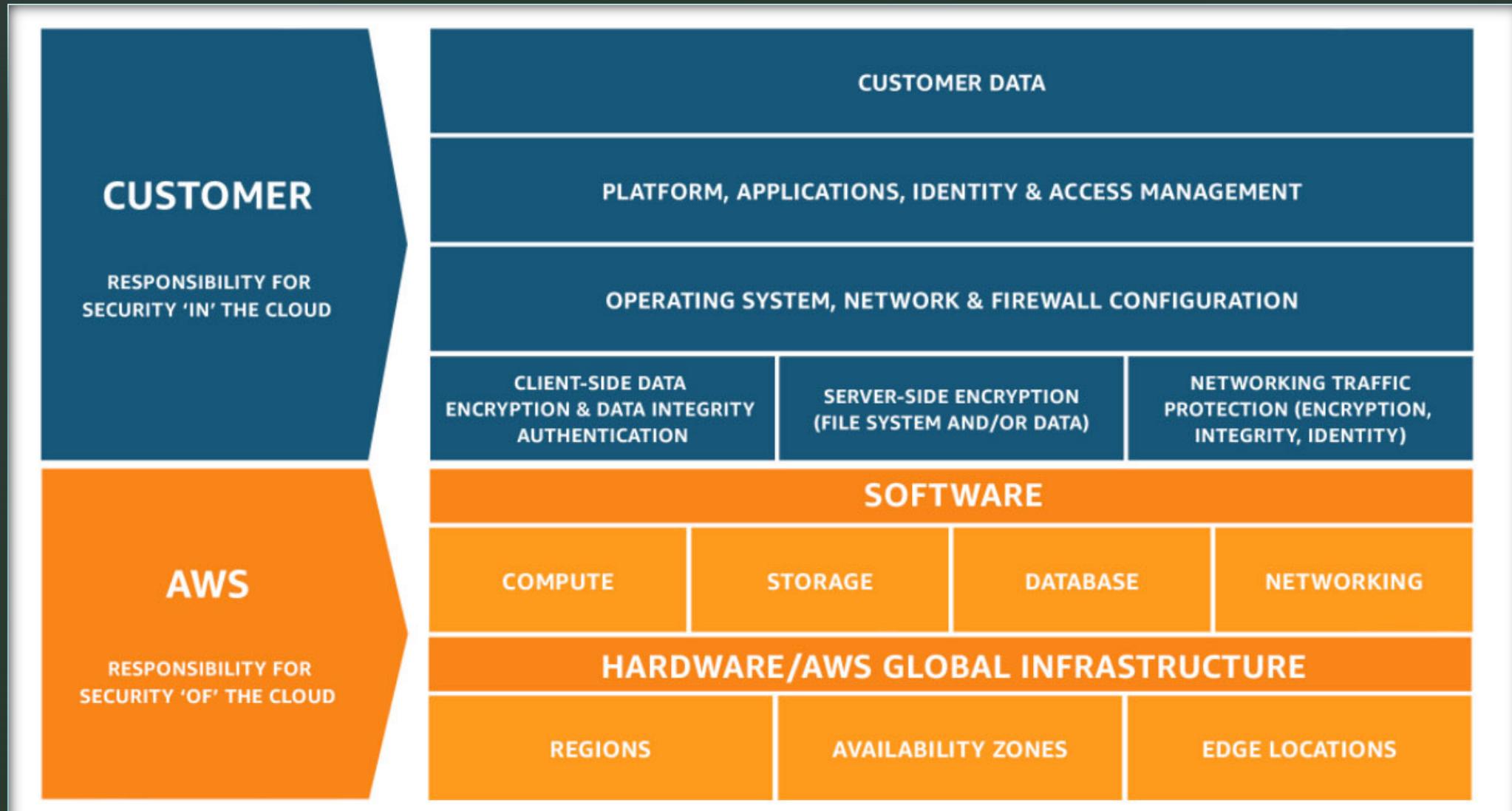
- Cloud & DevOps Consultant
- Multiple certifications on AWS, including Solution Architect and DevOps professional levels
- Leading Cloud & DevOps teams in multicloud environments
- Corporate AWS and DevOps training
- AWS Bulgaria User Group Co-Organizer
- AWS Community Hero

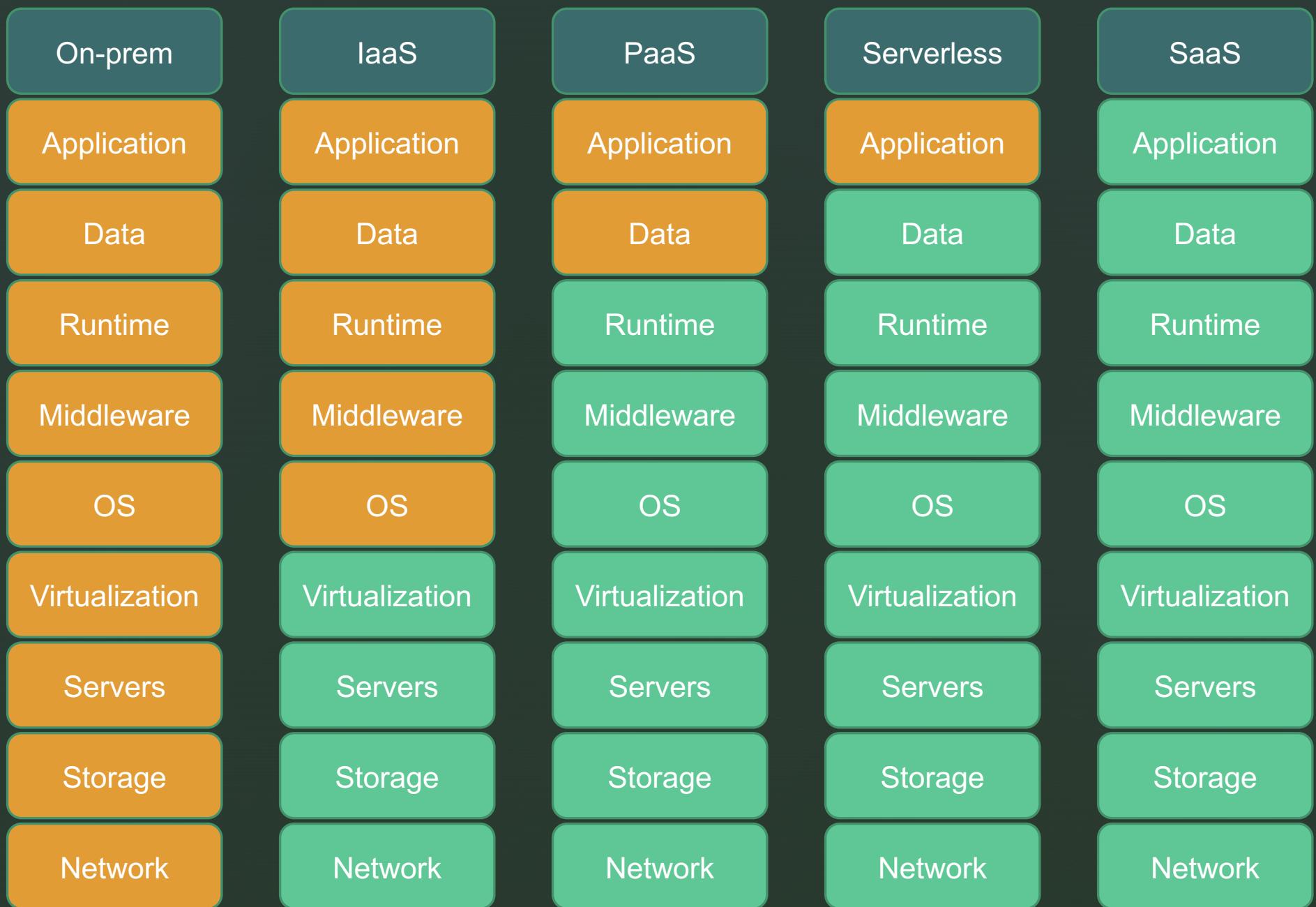


# Regulated industries

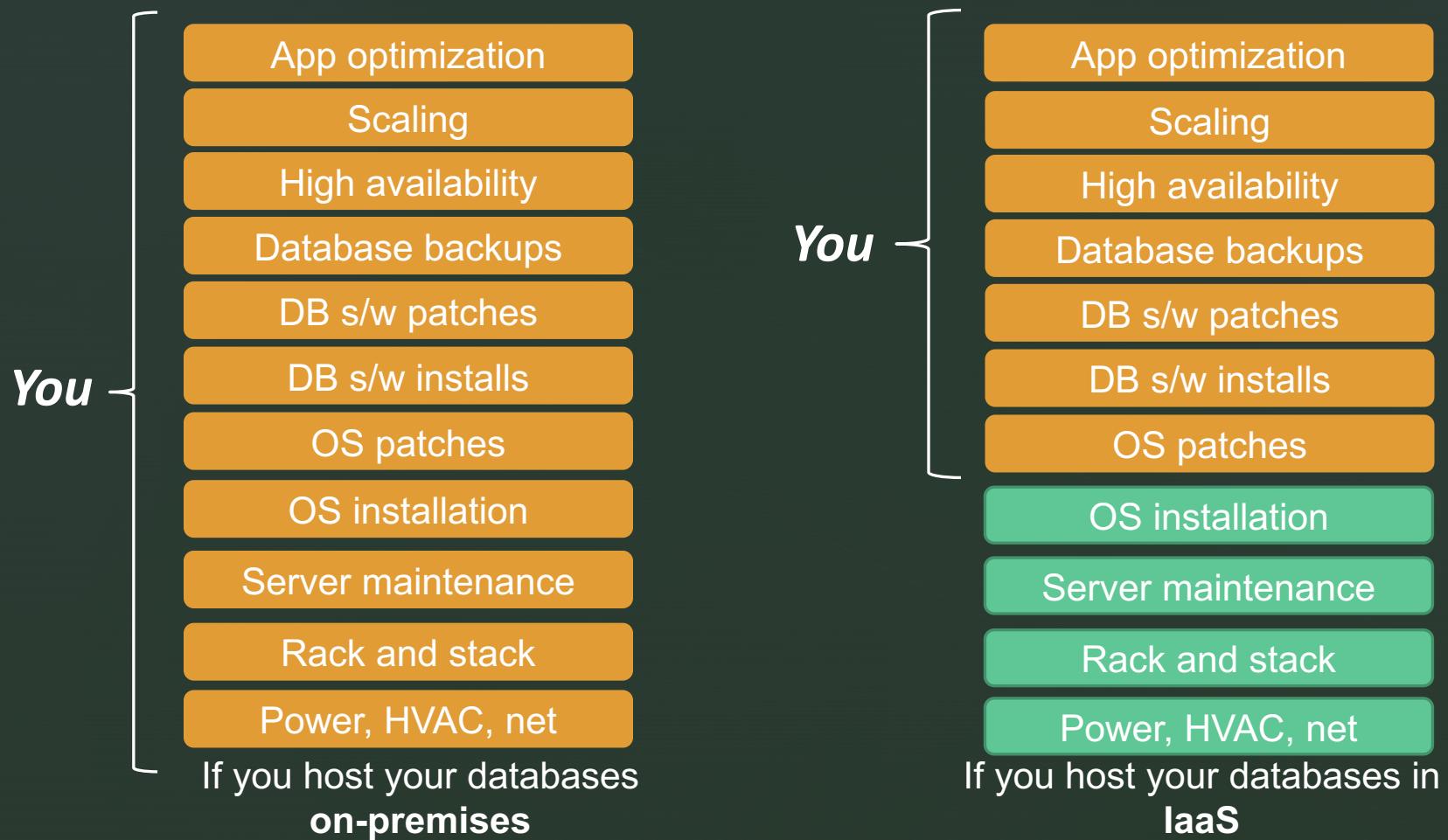
- Healthcare
- Banking
- Insurance
- Telecommunications
- Energy
- Agriculture
- Defence

# AWS Shared Responsibility Model





# Managed service – Relational database



# Managed service – Relational database

*You* →

App optimization

Scaling

High availability

Database backups

DB s/w patches

DB s/w installs

OS patches

OS installation

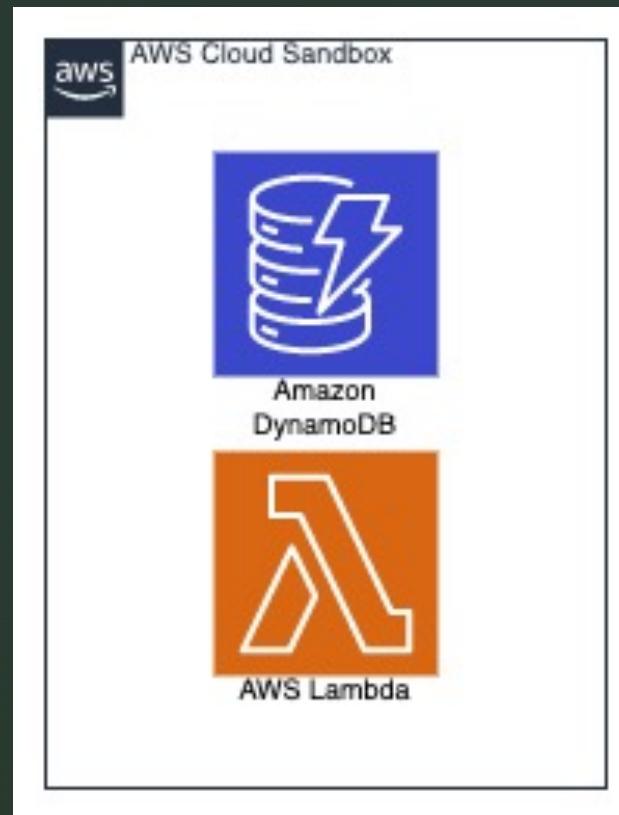
Server maintenance

Rack and stack

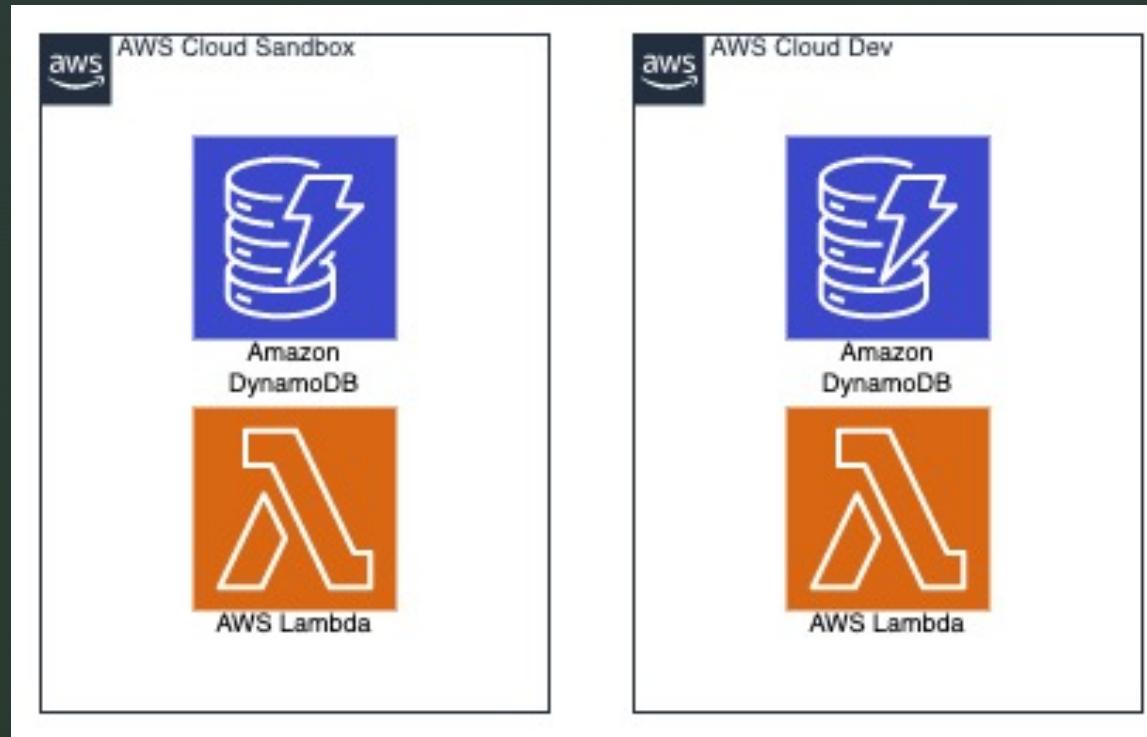
Power, HVAC, net

If you host your databases in  
a **managed database service**

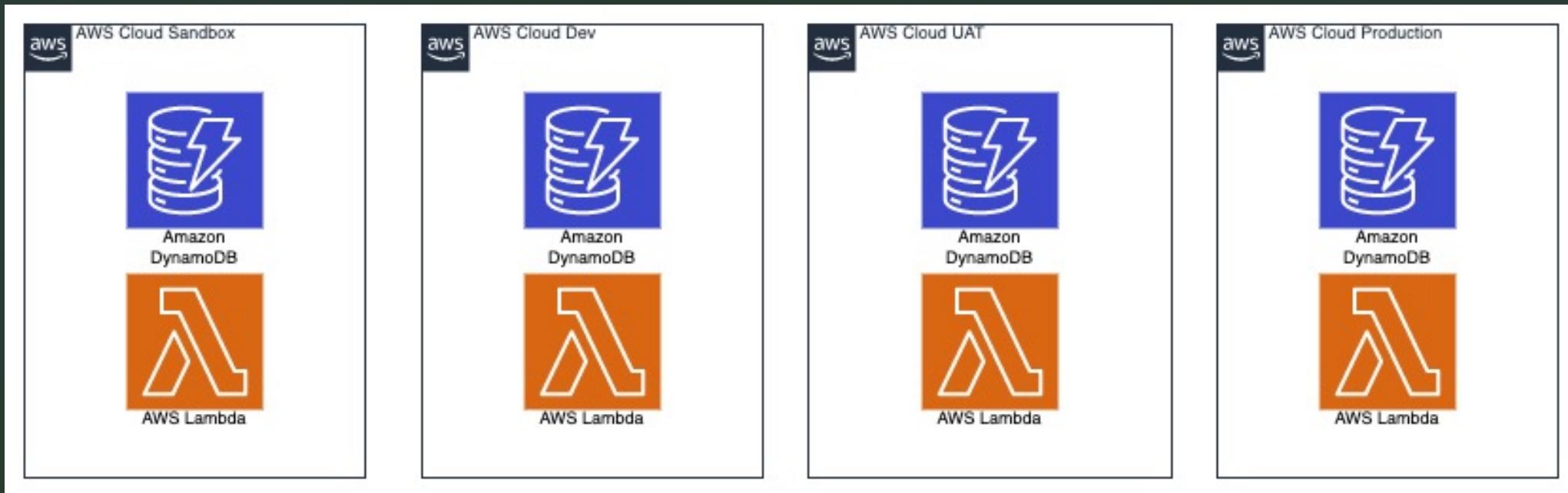
# AWS account structure



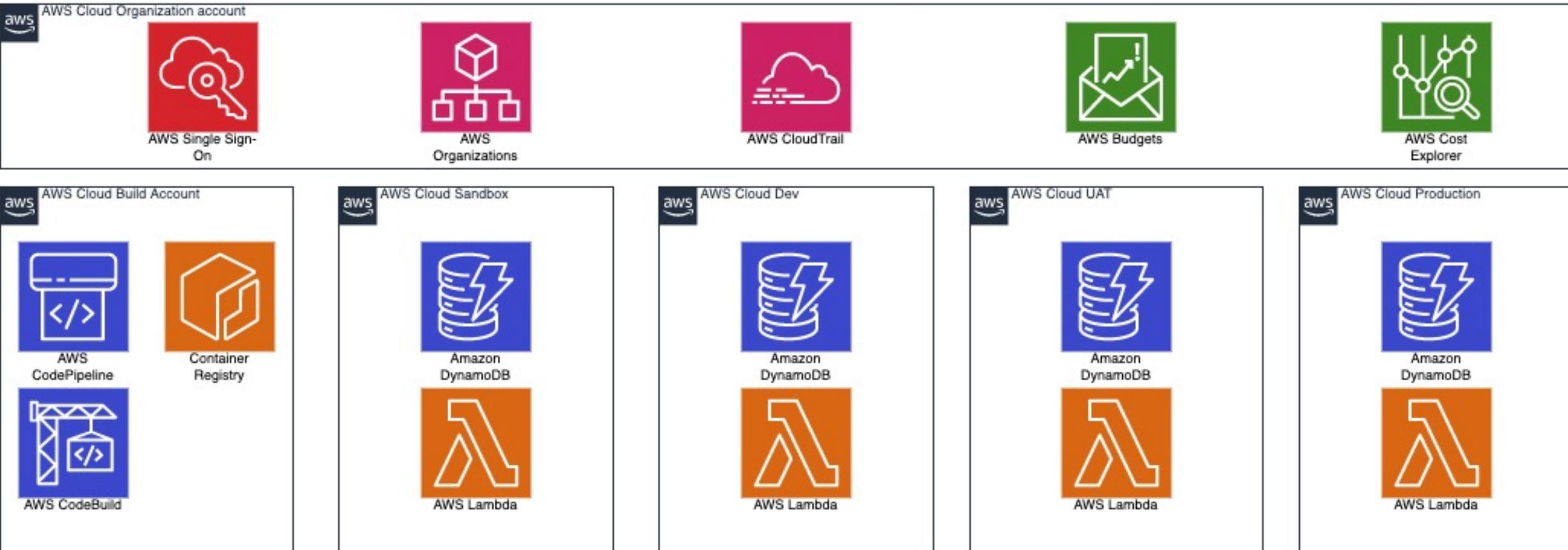
# AWS account structure

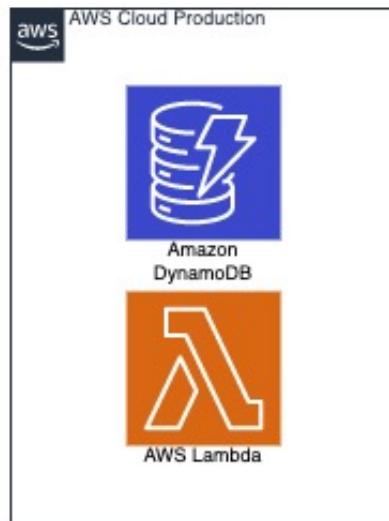
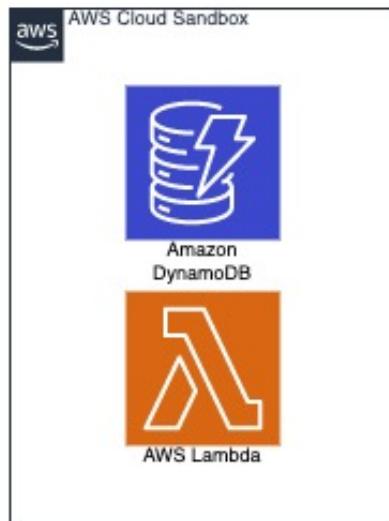
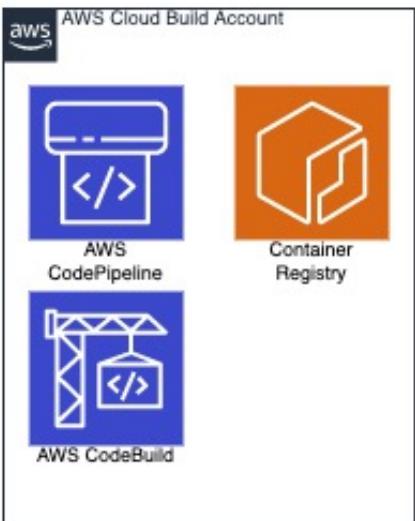
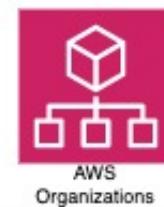


# AWS account structure



# AWS account structure

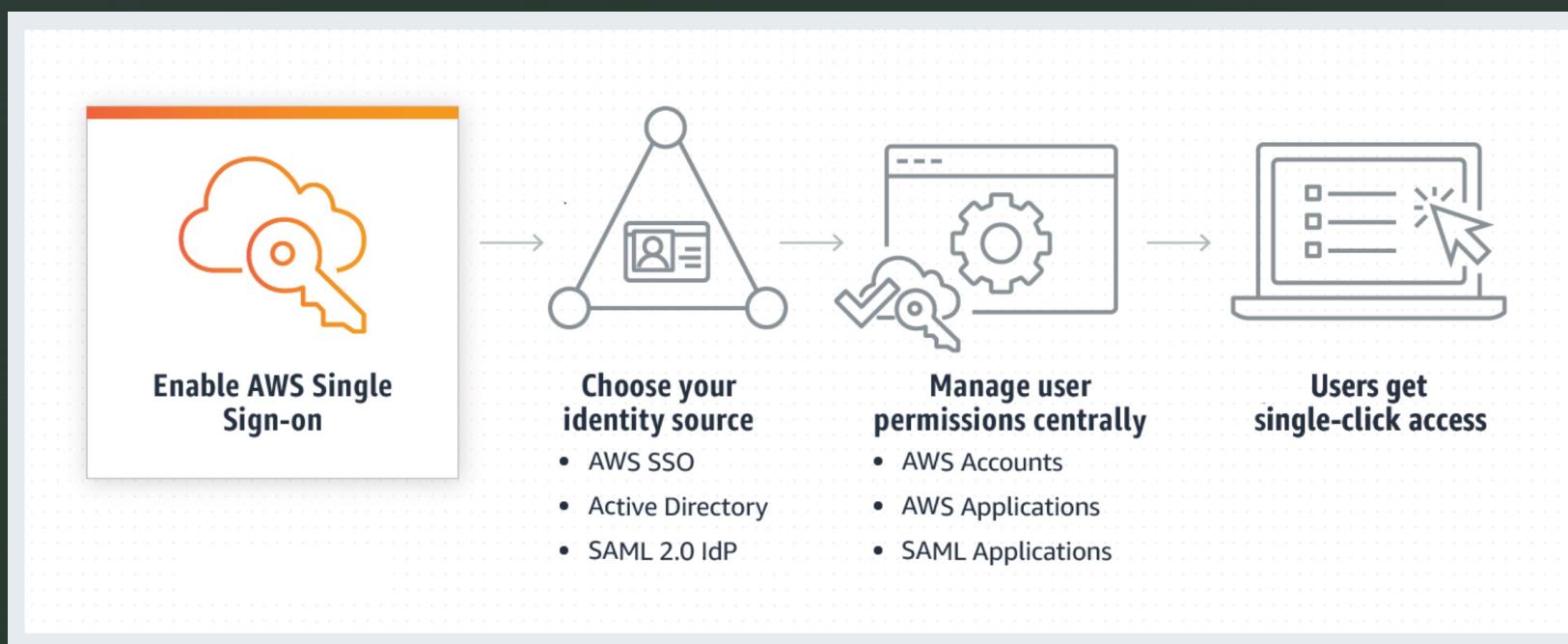




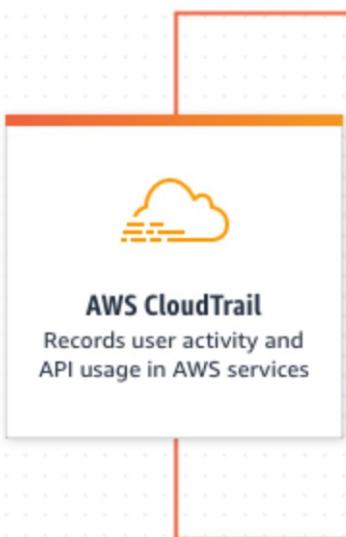
# AWS service control policies (SCPs)

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "AllowsAllActions",  
      "Effect": "Allow",  
      "Action": "*",  
      "Resource": "*"  
    },  
    {  
      "Sid": "DenyDynamoDB",  
      "Effect": "Deny",  
      "Action": "dynamodb:*",  
      "Resource": "*"  
    }  
  ]  
}
```

# AWS Single Sign-On



# AWS CloudTrail



**Store**  
Deliver events to Amazon S3 and Amazon CloudWatch Logs



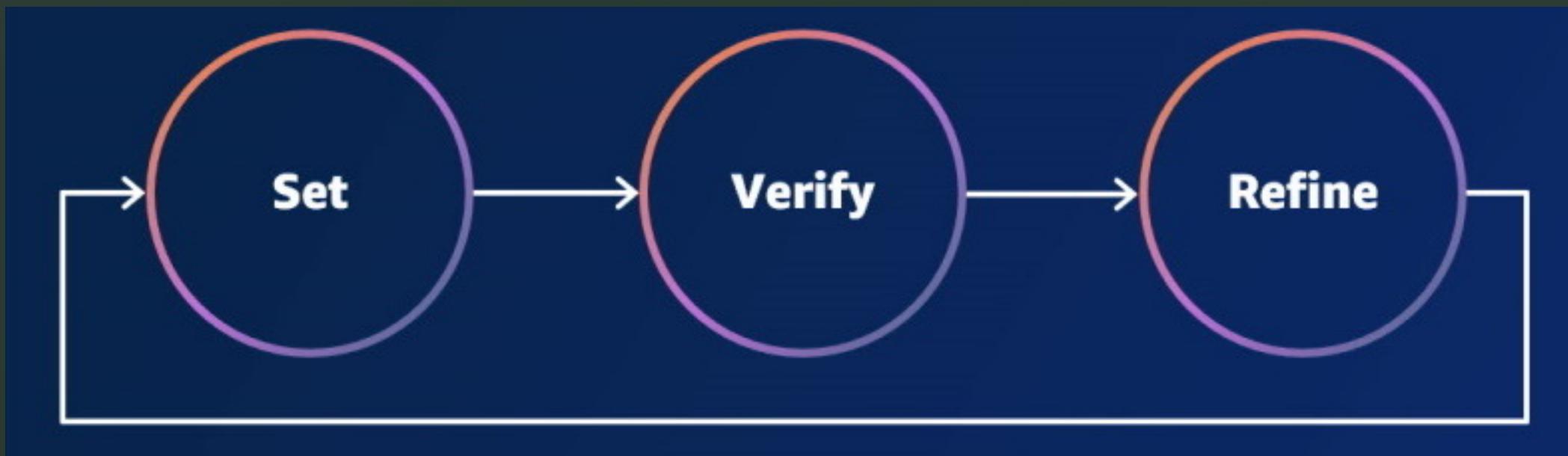
**Monitor**  
Detect unusual API activity with CloudTrail Insights or Amazon EventBridge



**Analyze**  
View recent events in the AWS CloudTrail console, or analyze log files with Amazon Athena



# IAM Access Analyzer



# AWS SecurityHub

## AWS Foundational Security Best Practices v1.0.0

### Overview

Last updated 2 hours ago

Security score



100 of 620 checks failed



Enabled

**139**

Failed

**20**

Unknown

**0**

No data

**0**

Passed

**119**

Disabled

**14**

### Enabled controls (139)

statuses and check counts updated 2 hours ago

[Disable](#)

[Download](#)

Filter enabled controls

Compliance  
Status

Severity

ID

Title

Failed  
checks



Failed

Critical

EC2.19

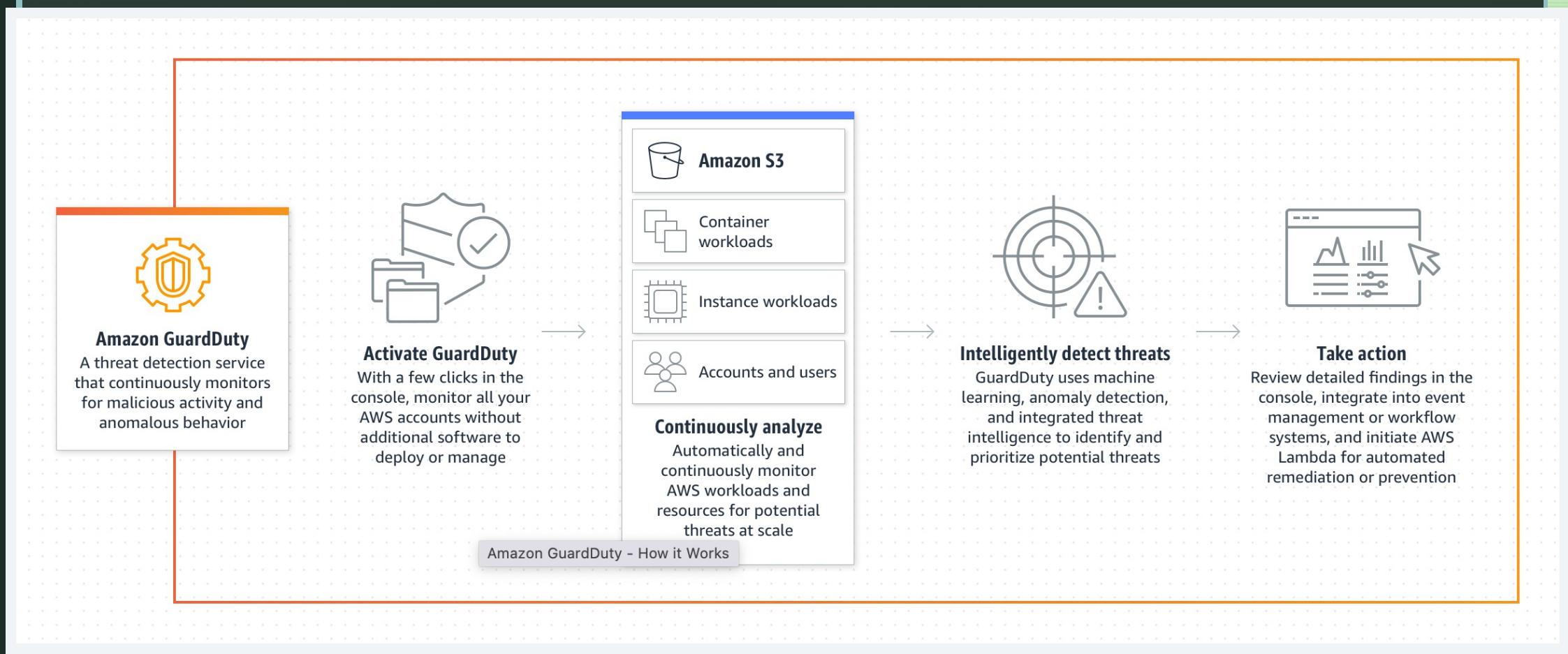
Security groups should not allow unrestricted access to ports with high risk

1 of 20

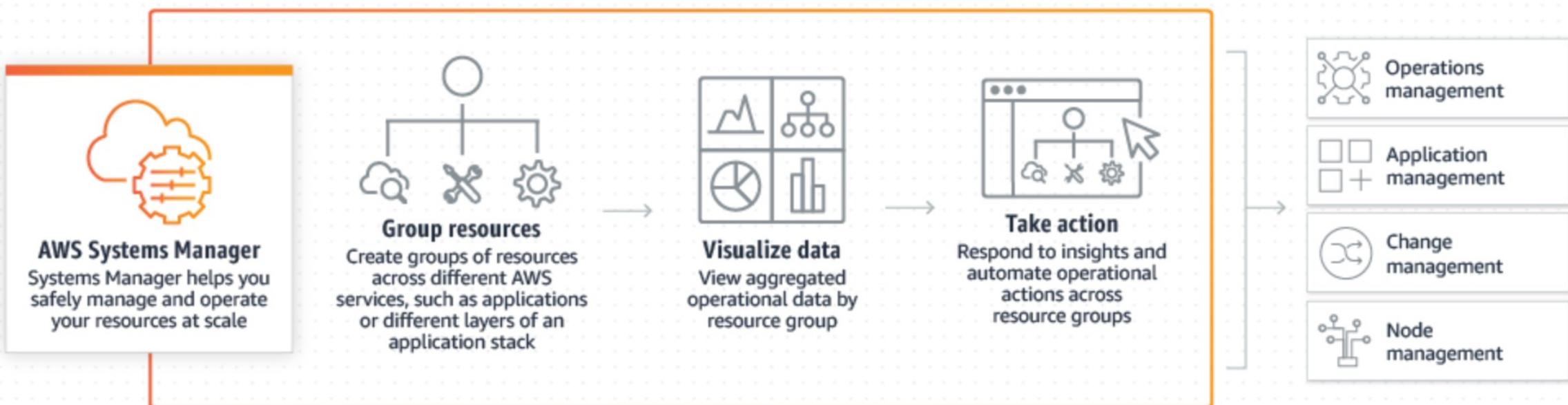
# AWS Config Conformance Packs

- [Operational Best Practices for FedRAMP\(Moderate\)](#)
- [Operational Best Practices for FFIEC](#)
- [Operational Best Practices for HIPAA Security](#)
- [Operational Best Practices for K-ISMS](#)
- [Operational Best Practices for Load Balancing](#)
- [Operational Best Practices for Logging](#)
- [Operational Best Practices for Management and Governance Services](#)
- [Operational Best Practices for MAS Notice 655](#)
- [Operational Best Practices for MAS TRMG](#)
- [Operational Best Practices for Monitoring](#)
- [Operational Best Practices for NBC TRMG](#)
- [Operational Best Practices for NERC CIP](#)
- [Operational Best Practices for NCSC Cloud Security Principles](#)
- [Operational Best Practices for NCSC Cyber Assesment Framework](#)
- [Operational Best Practices for Networking and Content Delivery Services](#)
- [Operational Best Practices for NIST 800-53 rev 4](#)
- [Operational Best Practices for NIST 800-53 rev 5](#)

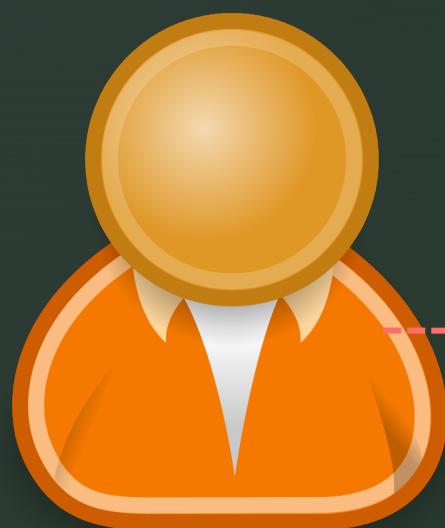
# Amazon GuardDuty



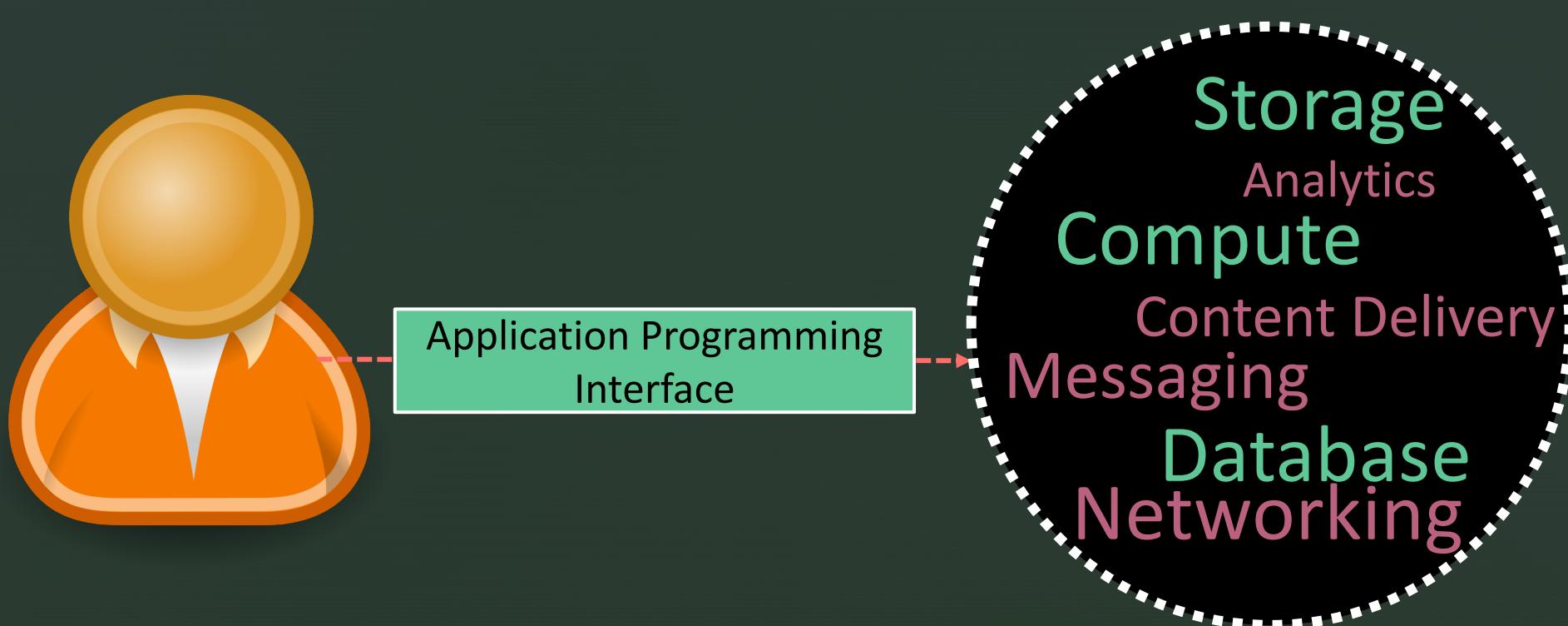
# AWS Systems Manager



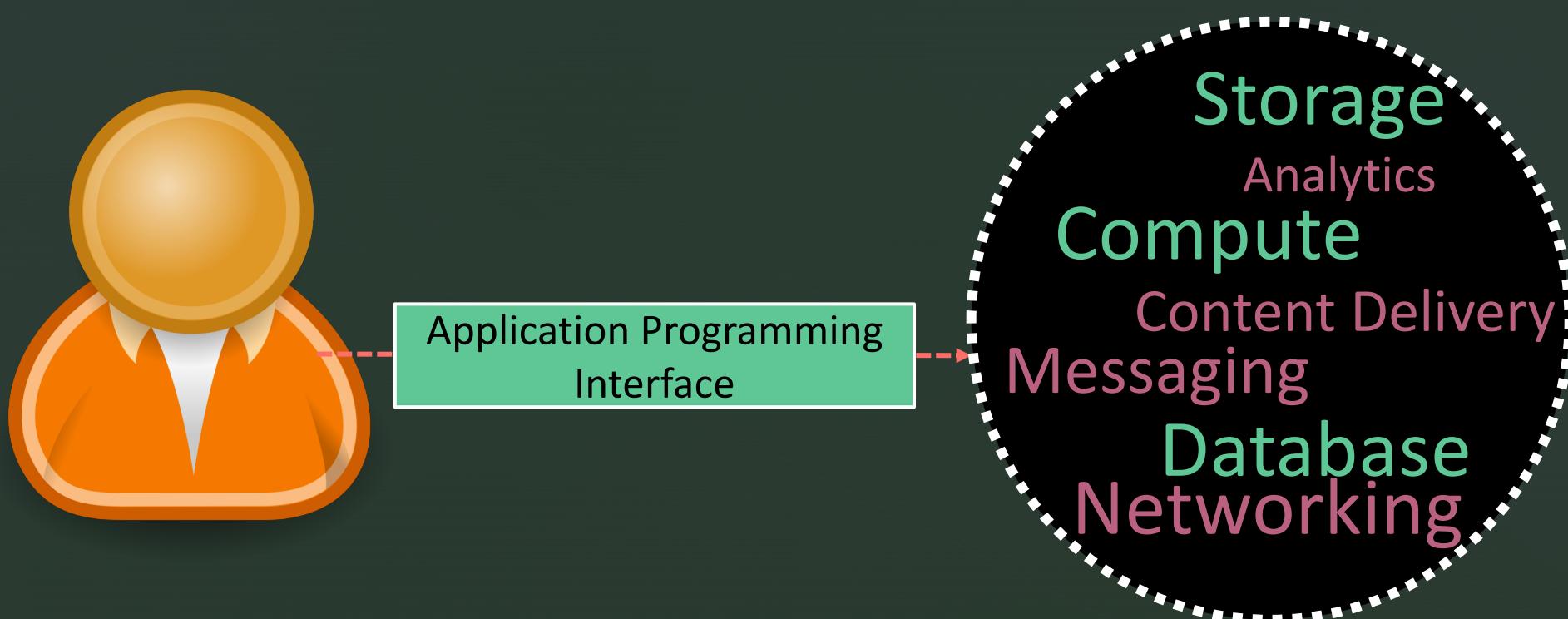
# Create Infrastructure - manual



# Create Infrastructure - API

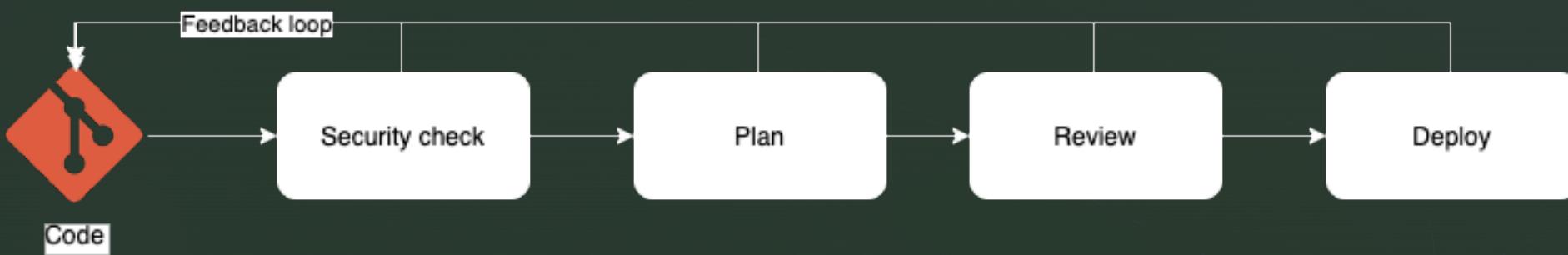


# Create Infrastructure – Infrastructure as Code (IaC)



# Infrastructure as code (IaC) benefits

- Secure
- Auditable and Traceable
- Repeatable and Consistent
- Documented
- Part of the CI/CD Process
- Cost-Efficient



# Shift security left - Checkov

## Policy-as-code for everyone

Checkov scans cloud infrastructure configurations to find misconfigurations before they're deployed.

Checkov uses a common command line interface to manage and analyze infrastructure as code (IaC) scan results across platforms such as Terraform, CloudFormation, Kubernetes, Helm, ARM Templates and Serverless framework.

Get started →

```
PASSED for resource: aws_s3_bucket.operations
File: /aws/s3.tf:32-44
Guide: https://docs.bridgecrew.io/docs/s3\_2-across-all-accounts-for-everyone

Check: CKV_AWS_21: "Ensure all data stored in the S3 bucket is encrypted"
PASSED for resource: aws_s3_bucket.operations
File: /aws/s3.tf:32-44
Guide: https://docs.bridgecrew.io/docs/s3\_16-end-to-end-encryption

Check: CKV_AWS_93: "Ensure S3 bucket policy does not allow public access. (Prevent lockouts needing root account fixes)"
PASSED for resource: aws_s3_bucket.operations
File: /aws/s3.tf:32-44
Guide: https://docs.bridgecrew.io/docs/bc\_aws\_s3\_bucket

Check: CKV_AWS_130: "Ensure VPC subnets do not assign private IP ranges to public IP ranges"
FAILED for resource: aws_subnet.eks_subnet1
File: /aws/eks.tf:42-51

42 |   resource aws_subnet "eks_subnet1" {
43 |     vpc_id           = aws_vpc.vpc.id
44 |     cidr_block       = "10.10.0.0/16"
45 |     availability_zone = var.availability_zones[0]
46 |     map_public_ip_on_launch = true
47 |     tags = {
48 |       Name = "eks-subnet1"
```

# Security control matrix

| HIPAA Regulatory Citation<br>(45 C.F.R. § xxx.xxx) | Name   | HIPAA Regulation Text   | HIPAA Rule Category | AWS Commentary   |
|--|--|---|---------------------|--|
| §164.308(a)(5)(ii)(A)                              | Security Awareness and Training — Security Reminders                         | Periodic security updates.  | Security Rule       | The customer is responsible for implementing security reminders as a part of the customer's security awareness training procedures. As one illustrative example, the customer may, during a quarterly meeting, remind workforce members with access to ePHI to lock their workstations when away.  |
| §164.308(a)(5)(ii)(B)                              | Security Awareness, Training, and Tools — Protection from Malicious Software | Procedures for guarding against, detecting, and reporting malicious software. | Security Rule       | The customer is responsible for training its workforce members on procedures for guarding against malicious software. There are AWS partners that can help guard against, detecting, and reporting malicious software: <a href="https://aws.amazon.com/security/partner-solutions/#infrastructure">https://aws.amazon.com/security/partner-solutions/#infrastructure</a>   |
| §164.308(a)(5)(ii)(C)                              | Security Awareness, Training, and Tools — Log-in Monitoring                  | Procedures for monitoring log-in attempts and reporting discrepancies.        | Security Rule       | The customer is responsible for training appropriate workforce members on how to monitor log-in attempts and identify discrepancies. As one illustrative example, the customer should train appropriate workforce members on how to use AWS CloudTrail to identify suspicious attempts to access AWS.  |
| §164.308(a)(5)(ii)(D)                              | Security Awareness, Training, and Tools — Password Management                | Procedures for creating, changing, and safeguarding passwords.                | Security Rule       | The customer, at its discretion, may choose to provide AWS user accounts and privileges to workforce members within the customer's AWS infrastructure. The customer is responsible for configuring the password policies to be enforced, and is responsible for all aspects of developing and managing mechanisms and procedures for creating, changing, and safeguarding passwords within its operating systems and applications.<br>For more information, refer to:<br><a href="http://docs.aws.amazon.com/IAM/latest/UserGuide/getting-started_create-admin-group.html">http://docs.aws.amazon.com/IAM/latest/UserGuide/getting-started_create-admin-group.html</a><br><a href="http://docs.aws.amazon.com/IAM/latest/UserGuide/access.html">http://docs.aws.amazon.com/IAM/latest/UserGuide/access.html</a><br><a href="http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords_account-policy.htm">http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords_account-policy.htm</a> |

# Data residency and sovereignty



● Regions   ● Coming Soon

# Reference architectures



## Security, identity, and compliance

Learn how to meet your security and compliance goals using AWS infrastructure and services.

### Identity and access management

Manage access to AWS services and resources.

### Detection

Learn how to detect suspicious activity in your AWS account.

### Infrastructure protection

Monitor and control your network infrastructure.

### Data protection

Operate the security services that protect your data.

### Compliance

Implement compliance controls with AWS.

### Incident response

Learn how to automate incident response and recovery.



## Analytics and big data

Build secure, reliable, cost-effective data-processing architectures.

### Data lakes

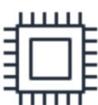
Best practices for setting up and managing data lakes.

### Data analytics

Analyze your data at scale on AWS.

### Data management

Store and manage your data in the cloud.



## Compute and HPC

Learn how to develop, deploy, run, and scale your applications.

### Core compute

Deploying secure, reliable compute capacity.

### High performance computing

Best practices for high performance computing.

### EC2 Spot and Fleet

Guidance for running EC2 Spot instances and Spot Fleet.



## Containers

Learn the most secure, reliable, and scalable way to

### DevOps practices

Leverage containers to enable DevOps workflows.

### Observability

Enable visibility and anomaly detection.

### Container security

Best practices for securing your containers.

# AWS Compliance program

|   |  |   |   |  |
|---|--|---|---|--|
|  <b>CSA</b><br>Cloud Security Alliance™                            |  <b>CyberGRX</b><br>Third Party Cyber Risk Management Exchange Member |  <b>ISO 9001</b><br>International Organization for Standardization |  <b>ISO 27001</b><br>International Organization for Standardization                           |  <b>ISO 27017</b><br>International Organization for Standardization |
| Cloud Security Alliance Controls  | Third Party Risk Management  | Global Quality Standard   | Security Management Controls  | Cloud Specific Controls  |
|  <b>ISO 2701</b><br>International Organization for Standardization |  <b>ISO 27018</b><br>International Organization for Standardization   |  <b>PCI DSS Level 1</b><br>PARTICIPATING ORGANIZATION™             |  <b>SOC 1</b><br>Audit Controls Report  |  <b>SOC 2</b><br>Security, Availability, & Confidentiality Report   |
| <b>ISO 27701</b><br>Privacy Information Management  | <b>ISO 27018</b><br>Personal Data Protection   | <b>PCI DSS Level 1</b><br>Payment Card Standards  | <b>SOC 1</b><br>Audit Controls Report   | <b>SOC 2</b><br>Security, Availability, & Confidentiality Report   |
|  <b>CJIS</b><br>Criminal Justice Information Services            |  <b>DoD SRG</b><br>Department of Defense Data Processing            |  <b>FedRAMP</b><br>Government Data Standards                     |  <b>FERPA</b><br>Educational Privacy Act   |  <b>FIPS</b><br>Government Security Standards                       |
|  <b>FISMA</b><br>Federal Information Security Management Act     |  <b>GxP</b><br>Quality Guidelines and Regulations                   |  <b>HIPAA</b><br>Protected Health Information                    |  <b>HITRUST CSF Certified</b><br>Health Information Trust Alliance Common Security Framework |  <b>ITAR</b><br>International Arms Regulations                      |

## Customers in Regulated Industries

For security and compliance, customers choose AWS. To see more examples of customer success stories, visit our [Testimonials webpage](#).



*"AWS allowed us to store information in a cost effective manner while alleviating the burden of supporting the necessary infrastructure since AWS takes care of that. It really is a win-win for us and our customers."*



Healthcare



Financial Services



Education



Government

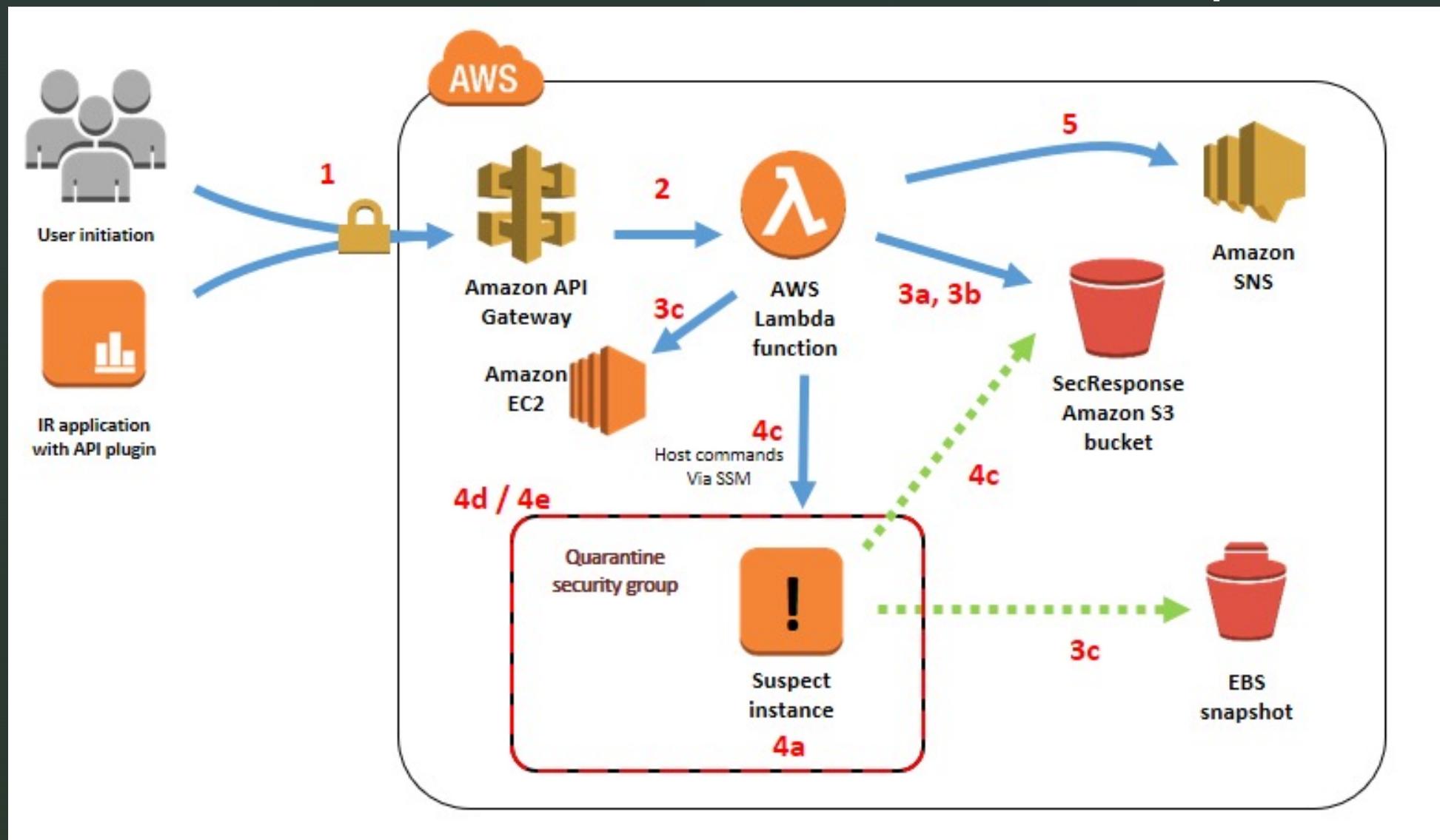


Energy

# People

- Break the wall
- Work together
- We all want the same thing

# Automated incident response



# Recap

- Know AWS Shared Responsibility Model
- Use multi-account strategy
- Use managed services
- Enable Security Hub
- Use Infrastructure as Code (IaC)
- Work together

# AWS re:Inforce

- <https://reinforce.awsevents.com>

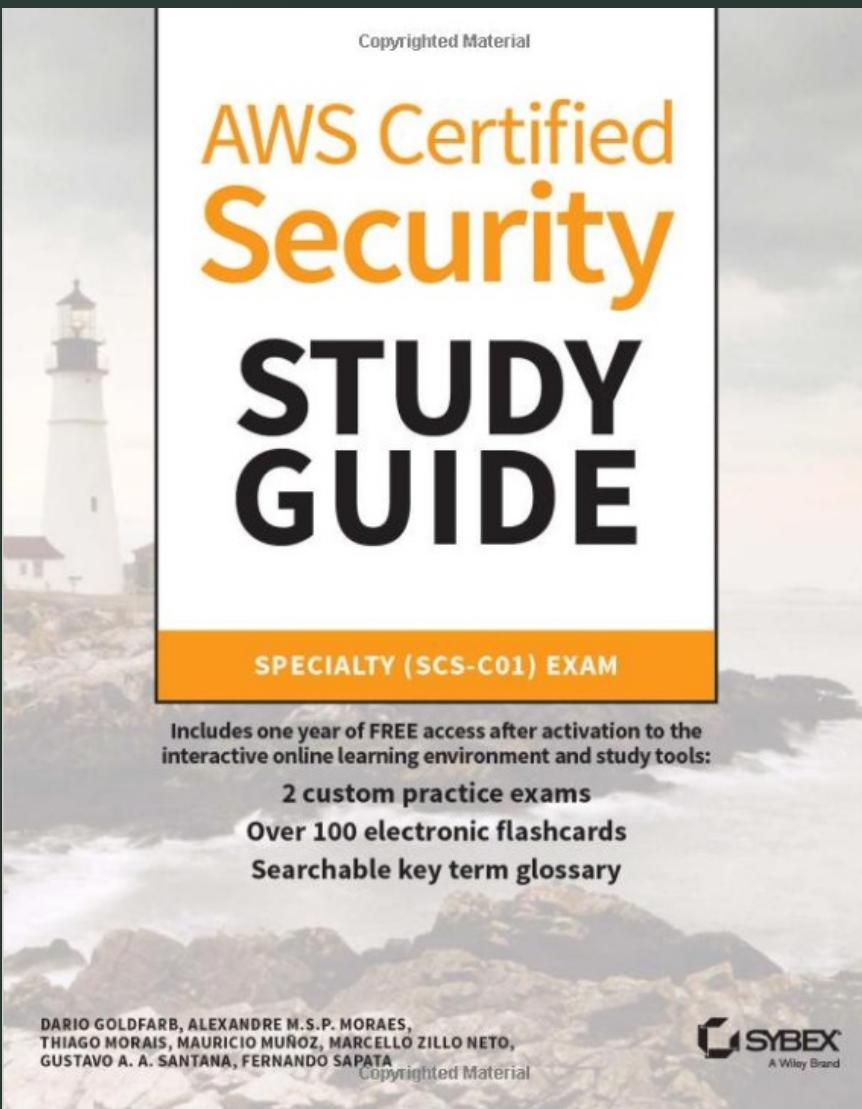


RE:INFORCE 2022

Because security is  
the **top priority**

Join us in summer 2022 for two days to reinforce your AWS security posture. Discover how AWS is innovating in the world of cloud security, and then hone your technical skills in expert-led interactive sessions. You'll hear the latest from industry-leading speakers in security, compliance, identity, and privacy and meet fellow security professionals at our fun events. Stay tuned for more updates and information about attending re:Inforce 2022.

# Resources



# Resources

- Infrastructure as Code
  - <https://www.terraform.io/>
  - <https://aws.amazon.com/cdk/>
  - <https://aws.amazon.com/cloudformation/>
- AWS Security resources
  - <https://aws.amazon.com/security/>
  - <https://aws.amazon.com/compliance/>
  - <https://aws.amazon.com/blogs/security/>
  - <https://aws.amazon.com/podcasts/aws-podcast/>
  - <https://aws.amazon.com/certification/certified-security-specialty/>

# Resources

- AWS Security
  - <https://aws.amazon.com/blogs/security/how-to-automate-incident-response-in-aws-cloud-for-ec2-instances/>
  - <https://aws.amazon.com/blogs/security/use-iam-access-analyzer-to-generate-iam-policies-based-on-access-activity-found-in-your-organization-trail/>
  - <https://reinforce.awsevents.com>
- AWS Bulgaria User Group
  - <https://www.meetup.com/AWS-Bulgaria/>

Thank you

<https://www.linkedin.com/in/danielrankov/>

<https://twitter.com/DanielRankov>