AWS re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

SEC315-R2

Cloud-native data loss-prevention controls with Goldman Sachs

Ilya Epshteyn
Sr. Manager, Identity Solutions
AWS

Birat Niraula
Regional Co-Head of Platform Security Architecture
Goldman Sachs

Agenda

General best practices

Data perimeters

Key scenarios and available controls

Data perimeter controls at Goldman Sachs

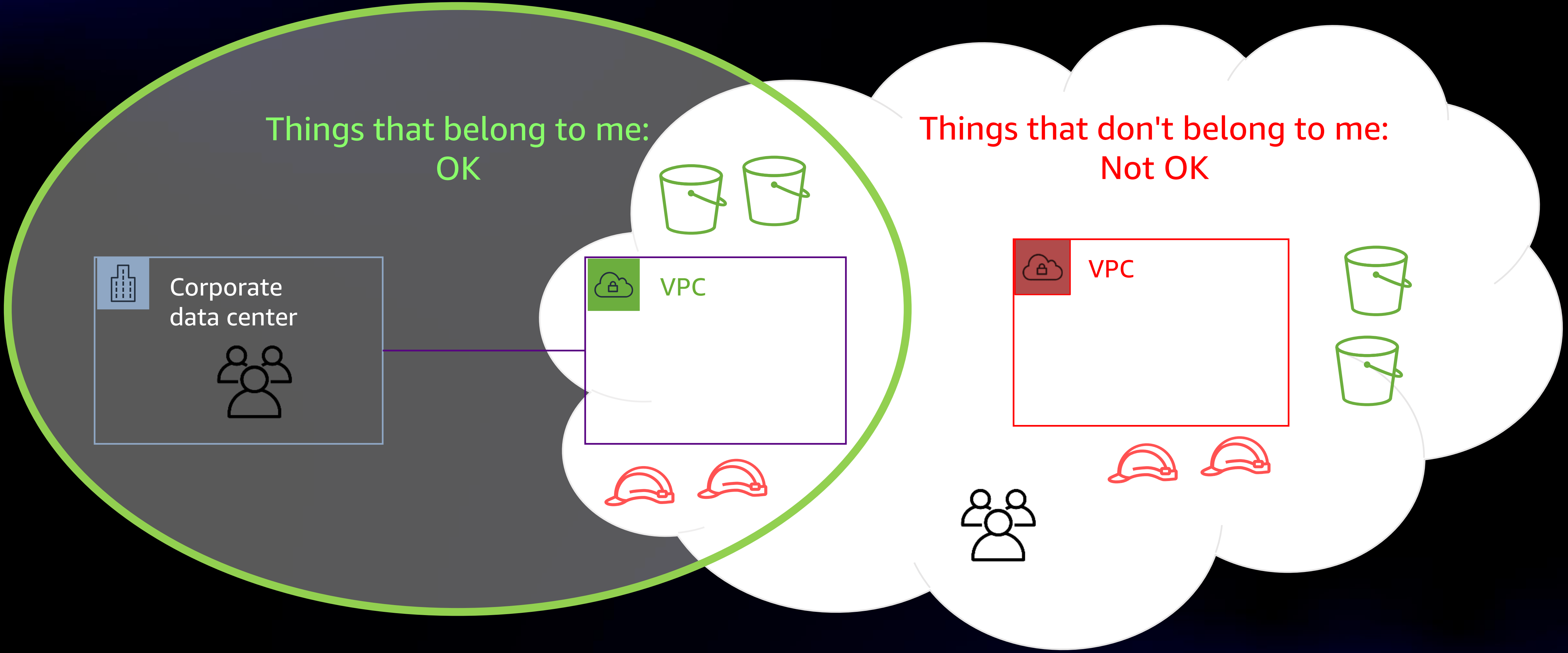
General data protection best practices

- Identify and classify sensitive data
- Encrypt/tokenize/mask sensitive data
- Keep humans away from sensitive data
- Establish data perimeter guardrails
- Implement preventive, detective, and responsive controls

What is a data perimeter?

A set of preventive guardrails that ensure that access to **trusted resources** is restricted to **trusted identities** from **expected network locations**

What is a data perimeter?



Tools for your data perimeter

1

Service control policies

Permission guardrails
for identities

“Prevent users from publishing data to SNS topics that do not belong to my AWS organization”

Tools for your data perimeter

1

Service control policies

Permissions guardrails
for identities

2

VPC endpoint policies

Ensure network access only
from trusted identities

“Prevent users outside my organization from moving my customer data through this VPC endpoint to an Amazon Simple Storage Service (Amazon S3) bucket that I don’t own”

Tools for your data perimeter

1

Service control policies

Permissions guardrails for identities

2

VPC endpoint policies

Ensure network access only from trusted identities

3

Resource-based policies

Ensure access only by your identities and AWS services

“Prevent access to this Amazon Simple Queue Service (Amazon SQS) queue from identities outside my accounts in AWS Organizations, unless they are AWS services”

Tools for your data perimeter

1

Service control policies

Permissions guardrails
for identities

2

VPC endpoint policies

Ensure network access only
from trusted identities

3

Resource-based policies

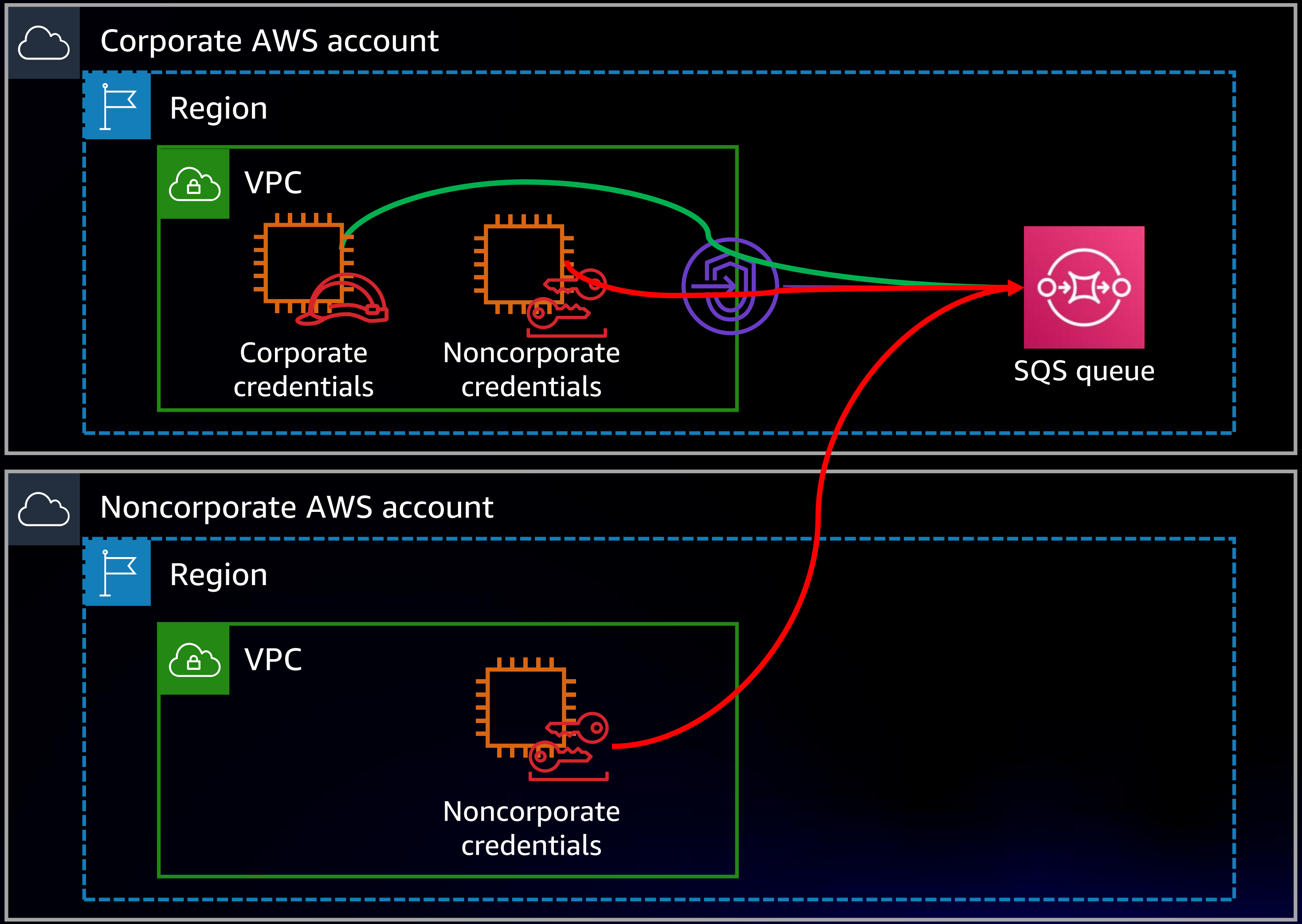
Ensure access only by your
identities and AWS services

...and more to come

Identity: Telling the difference

Configure an identity perimeter in the VPC endpoint policy and resource policy to accept traffic only from principals belonging to your AWS organization

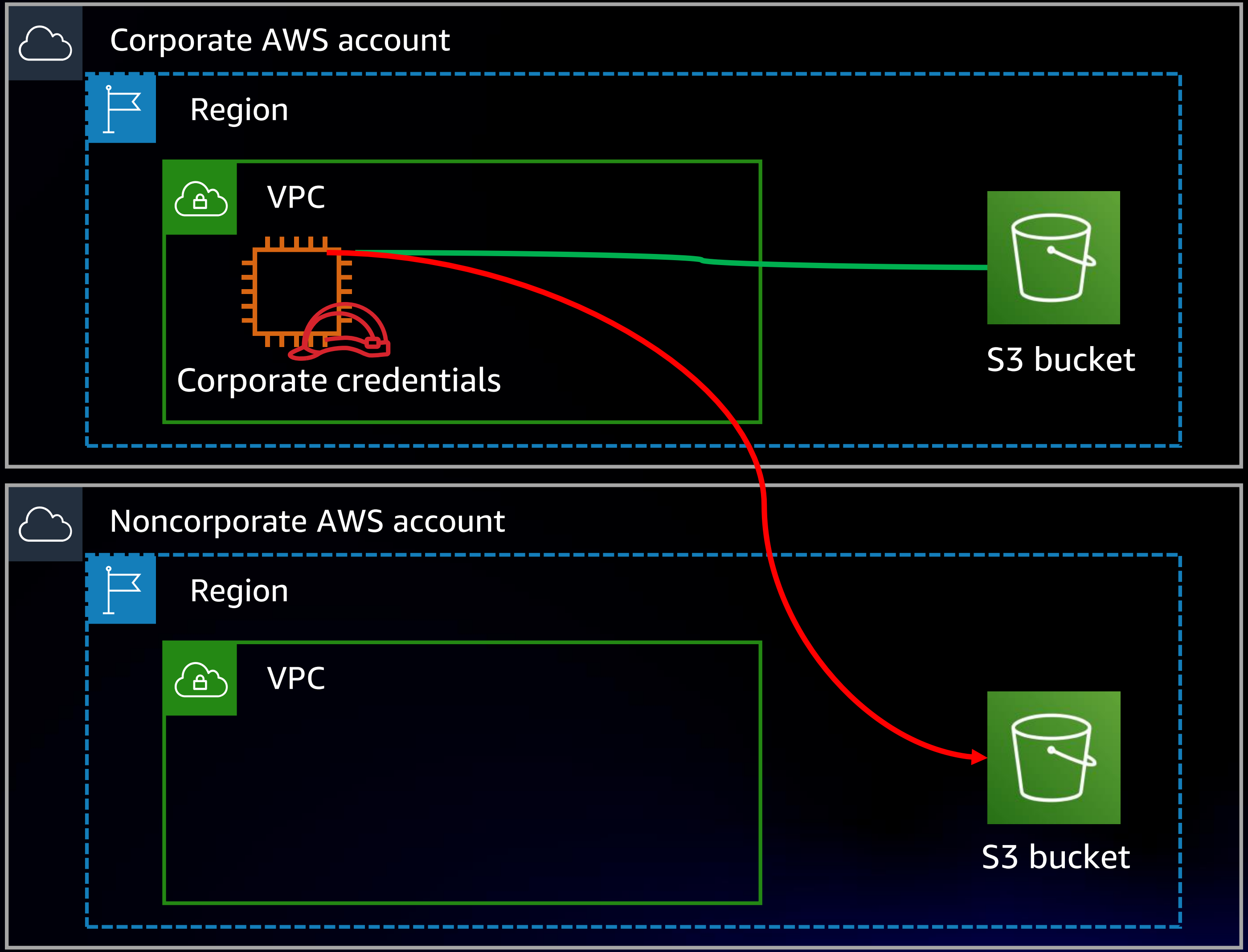
```
{
   "Statement":[
      {
         "Sid":"TrustedPrincipal",
         "Effect":"Deny",
         "Principal":"*",
         "Action":"sqs:SendMessage",
"Resource":"arn:aws:sqs:*:111122223333:queue1",
         "Condition":{
            "StringNotEquals":{
               "aws:PrincipalOrgID":[
                  "o-xxxxxxxxxxx"
               ]
            }
         }
      }
   ]
}
```



Resources: Telling the difference

Configure a resource perimeter for your identities, IAM Policy or SCP, to allow access only to your resources

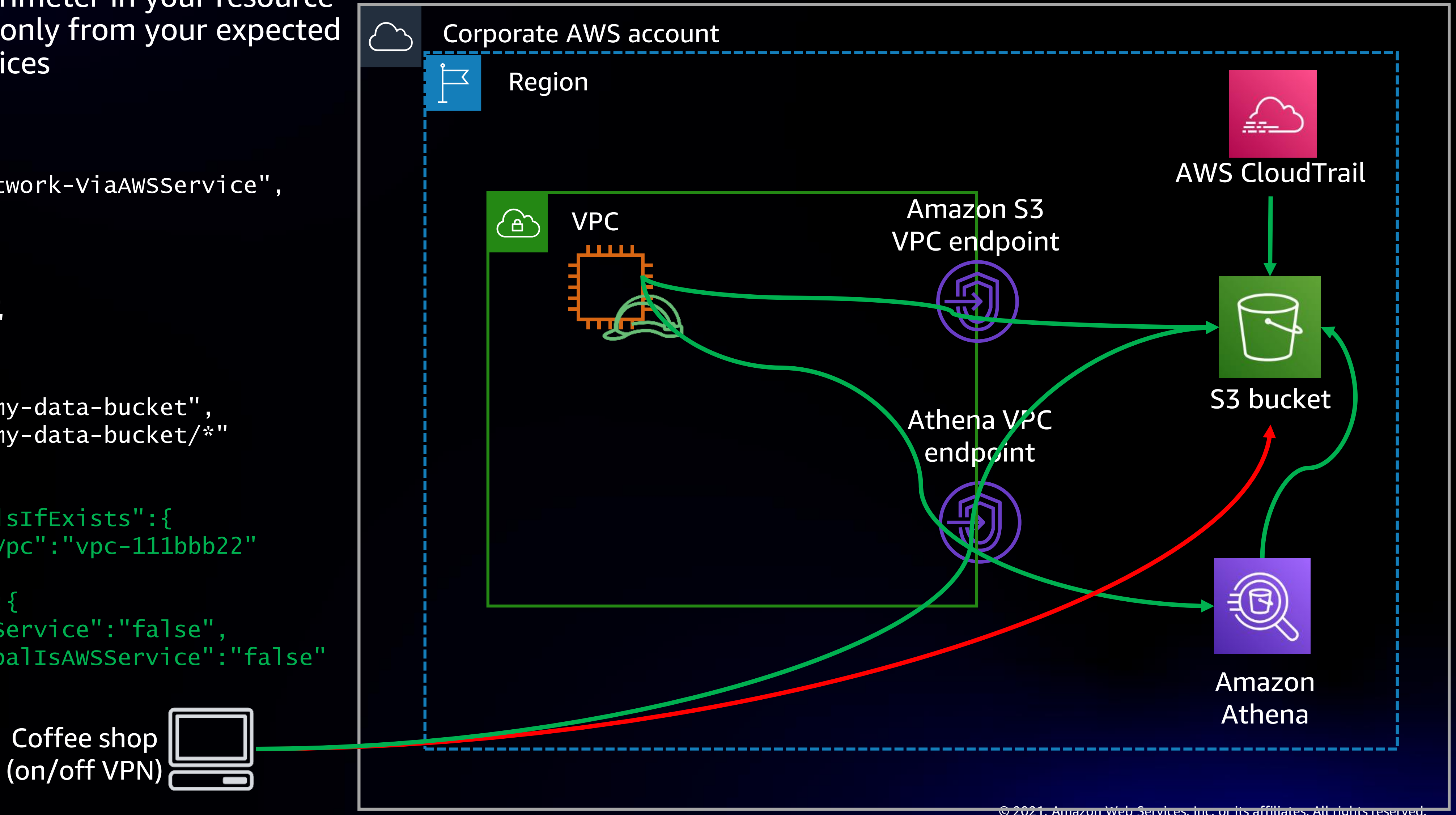
```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"TrustedS3Resources",
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
            "s3:GetObject"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
              “s3:ResourceAccount":"123456789012"
            }
         }
      }
   ]
}
```



Expected network: Telling the difference

Configure a network perimeter in your resource policies to allow access only from your expected networks and AWS services

```
"Statement":[
   {
      "Sid":"trusted-network-ViaAWSService",
      "Effect":"Deny",
      "Principal":"*",
      "Action":[
         "s3:PutObject",
         "s3:GetObject*"
      ],
      "Resource":[
         "arn:aws:s3:::my-data-bucket",
         "arn:aws:s3:::my-data-bucket/*"
      ],
      "Condition":{
         "StringNotEqualsIfExists":{
            "aws:SourceVpc":"vpc-111bbb22"
         },
         "BoolIfExists":{
            "aws:ViaAWSService":"false",
            "aws:PrincipalIsAWSService":"false"
         }
      }
   }
]
```



Data perimeter controls (review)

Perimeter	Applied on	Using	Data perimeter control
Identity	**Resources**	Resource-based policies	Ensure my resources are only accessed by ***my identities*** or AWS service principals on my behalf
	Network	VPC endpoint policy	Ensure only ***my identities*** are allowed from my network
Resource	**Identities**	IAM/SCP policies	Ensure my identities only access ***my resources*** or AWS-owned resources
	Network	VPC endpoint policy	Ensure my network can only access ***my resources*** or AWS-owned resources
Network	**Identities**	IAM/SCP policies	Ensure my identities only access from ***my network*** or AWS service network
	Resources	Resource-based policies	Ensure my resources are only accessed from ***my network*** or from AWS service network

About Goldman Sachs

Goldman Sachs brings people, capital, and ideas together to help our clients and the communities we serve

Innovation is at the heart of Goldman Sachs

As our services grow and evolve, we believe that Public Cloud brings the scaling, flexibility, and innovation we need

Collaborating with AWS has helped us adopt Public Cloud while focusing on operational excellence

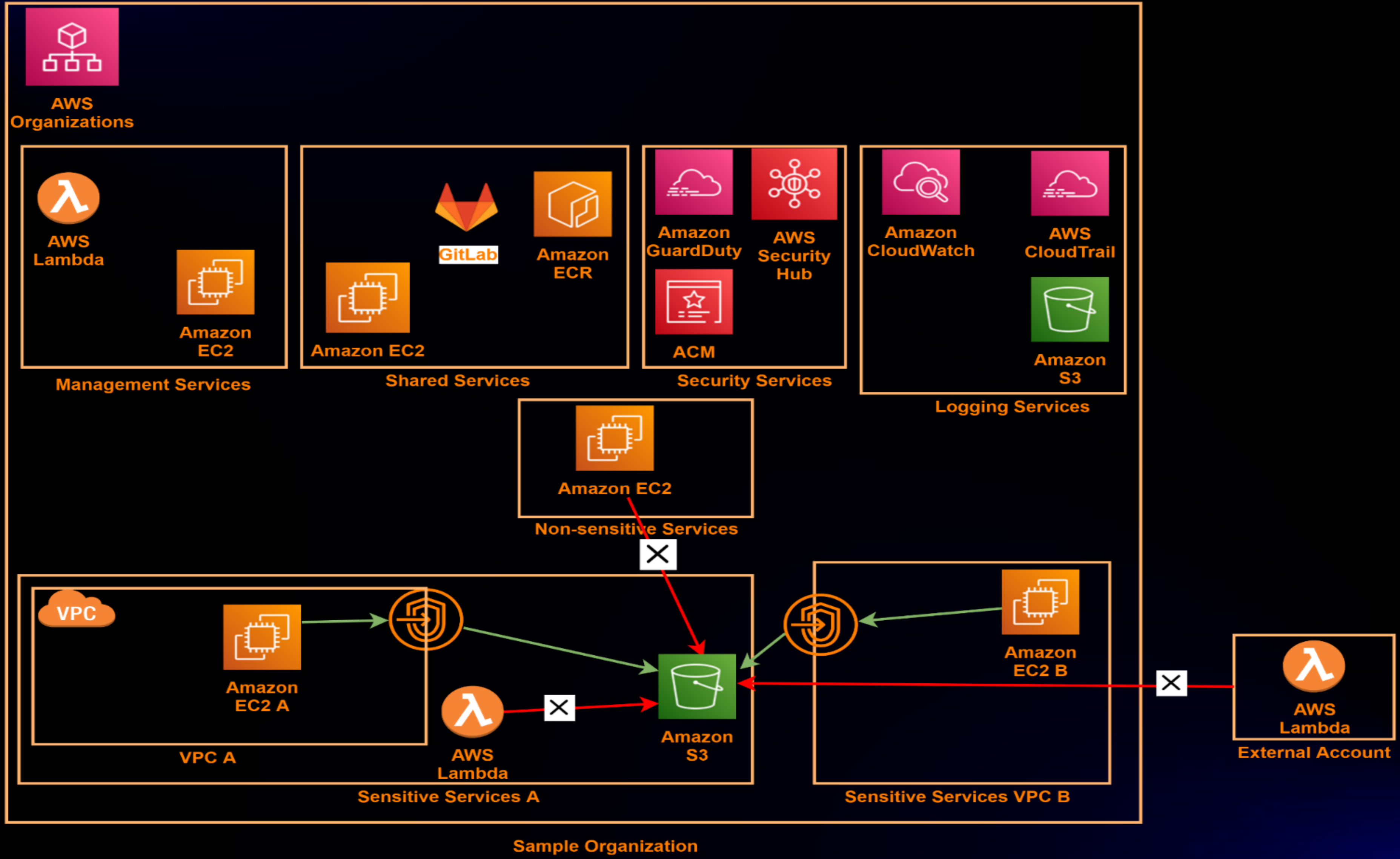
Goldman Sachs

aws

Data perimeter controls at Goldman Sachs

- Cloud security is of paramount importance
    - Security layers and defense in depth
- Security controls
    - Preventive
    - Detective
    - Responsive
- Other security best practices for cloud configuration

Sample application



Preventive controls

- **Architectural review and patterns**
- **CI/CD controls**
- **Workload isolation**
  - Account
  - Network
  - Function (for example data classification)
- **Administrative controls**
  - Authorization/entitlements
  - Organizational and account-level hardening
    - Service control policies
    - Account guardrails

AWS
Organizations

Detective controls

- Continuous-control monitoring
  - Configuration
  - Logs
- Near, real-time detections
  - Signature-based
    - State-based
      e.g. Configuration, encryption of resource, least privilege, etc.
    - Category-based
      e.g. Cross-account/external access, unapproved service, or network path
  - Heuristic analysis
    - Learning-based
      e.g. Malicious IP, anomalous behavior, etc.

AWS CloudTrail

AWS
Config

Amazon
CloudWatch

Responsive controls

- Auto-remediation based on pre-defined detections and playbooks
- Manual playbooks based on incidents or events
- Strategy for enhancement on preventive and detective controls
- Forensics analysis

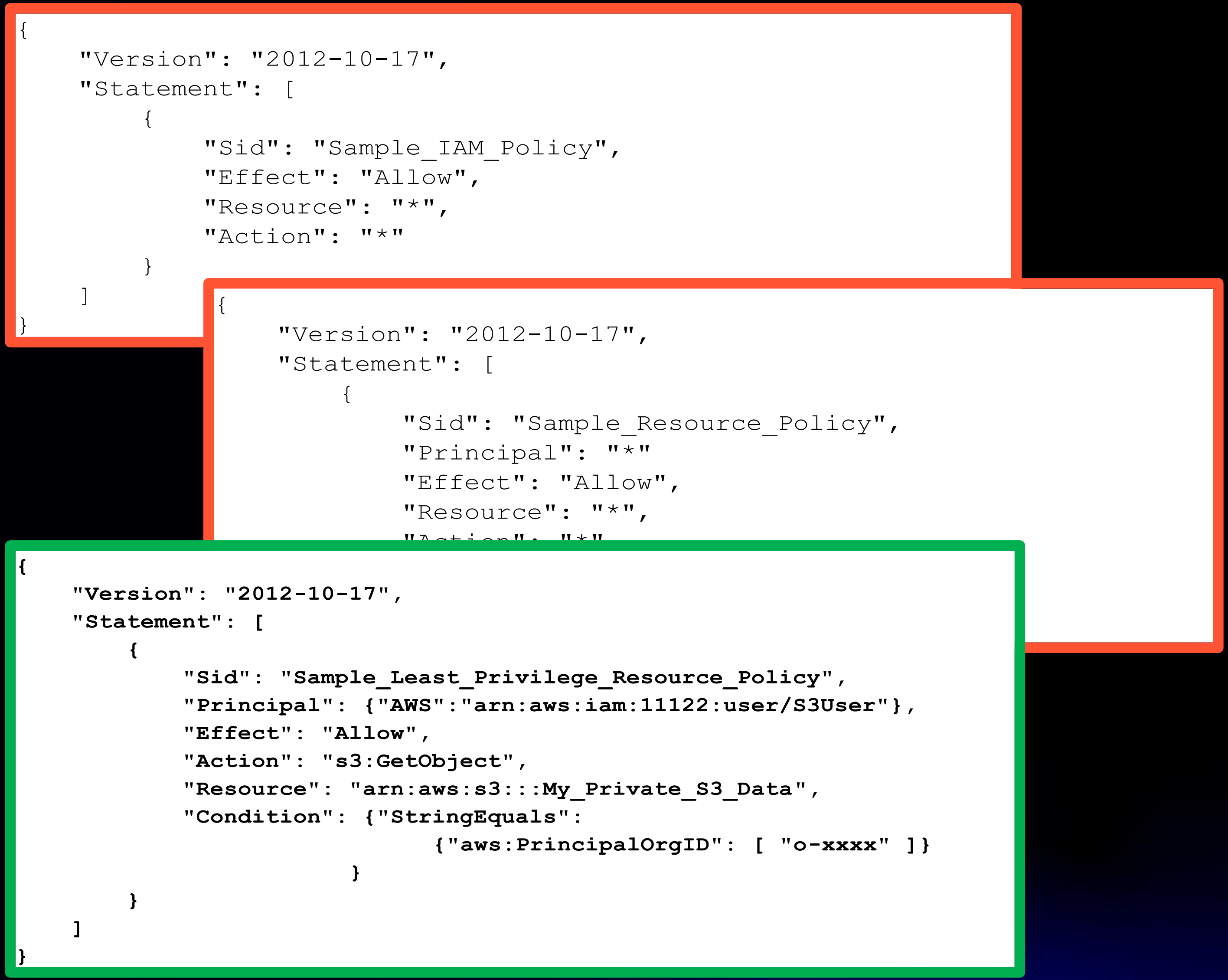
AWS Systems Manager

Automation

Other best practices for cloud configuration

- Least privilege access on policies
  - Principal
  - Action
  - Resource
  - Condition

- Least privilege access policy application
  - IAM role
  - Service control policies
  - Resource-based policies
  - VPC endpoint policies
  - Utilization of policy conditions



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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Sample_Resource_Policy",
            "Principal": "*"
            "Effect": "Allow",
            "Resource": "*",
            "Action": "*"
```

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Sample_Least_Privilege_Resource_Policy",
            "Principal": {"AWS":"arn:aws:iam:11122:user/S3User"},
            "Effect": "Allow",
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::My_Private_S3_Data",
            "Condition": {"StringEquals":
                          {"aws:PrincipalOrgID": [ "o-xxxx" ]}
                      }
        }
    ]
}
```

Relevant sessions

SEC318 Securing your data perimeter with VPC endpoints

SEC319 Building a data perimeter to allow access to authorized users (workshop)

SEC324 A least privilege journey: AWS IAM policies and Access Analyzer

SEC314 The journey to least privilege on AWS

FSI304 Policy as code: How to automate security and compliance (workshop)

Thank you!

Ilya Epshteyn
ilyep@amazon.com

Birat Niraula
birat.niraula@gs.com