cloudrail

Continuous Security for IaC in GitOps

DevSecOps Days Pittsburgh, June 16, 2021

Speaker: Yoni Leitersdorf, CEO and Founder
@yonadavl y@indeni.com

About Me

Yoni Leitersdorf

CEO & founder of Indeni Cloudrail

Coding since age 6

Served at the world-renowned IDF 8200 unit for the Israeli Intelligence Corps

Security my passion

Agenda

Cloud misconfiguration is the #1 risk to cloud environments in 2021. The average breach costs $4.4M.

But **you** already know that...

Sources: Trend Micro (2020), Ponemon Institute (2020)

Why is this happening?

- Developers running fast but security teams stopping the release.
  - Result: developers don’t like security.
- Security issues found too late in the process and not fixed.
  - Result: security doesn’t like developers, cloud environment isn’t secure.

Fundamentally, there aren’t enough security people to support developers

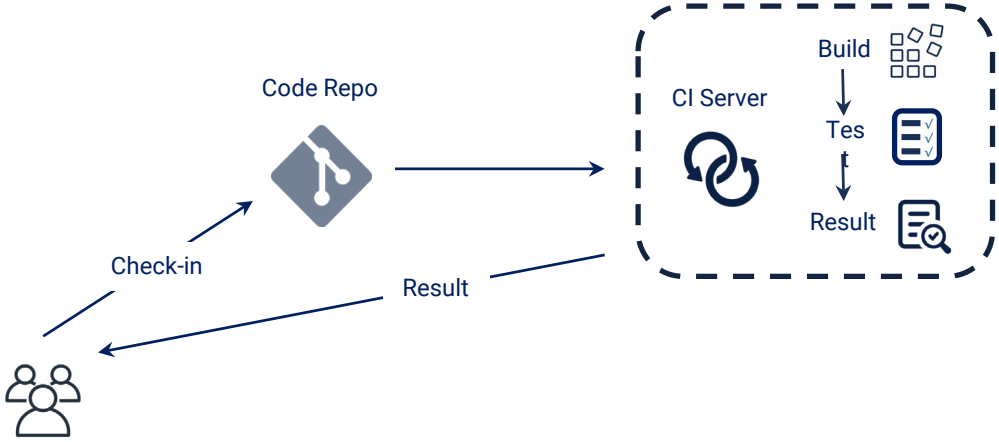
It doesn’t have to be this way.

We can make developers AND security happy, while keeping the pace of development (making business happy).

CI/CD Concepts

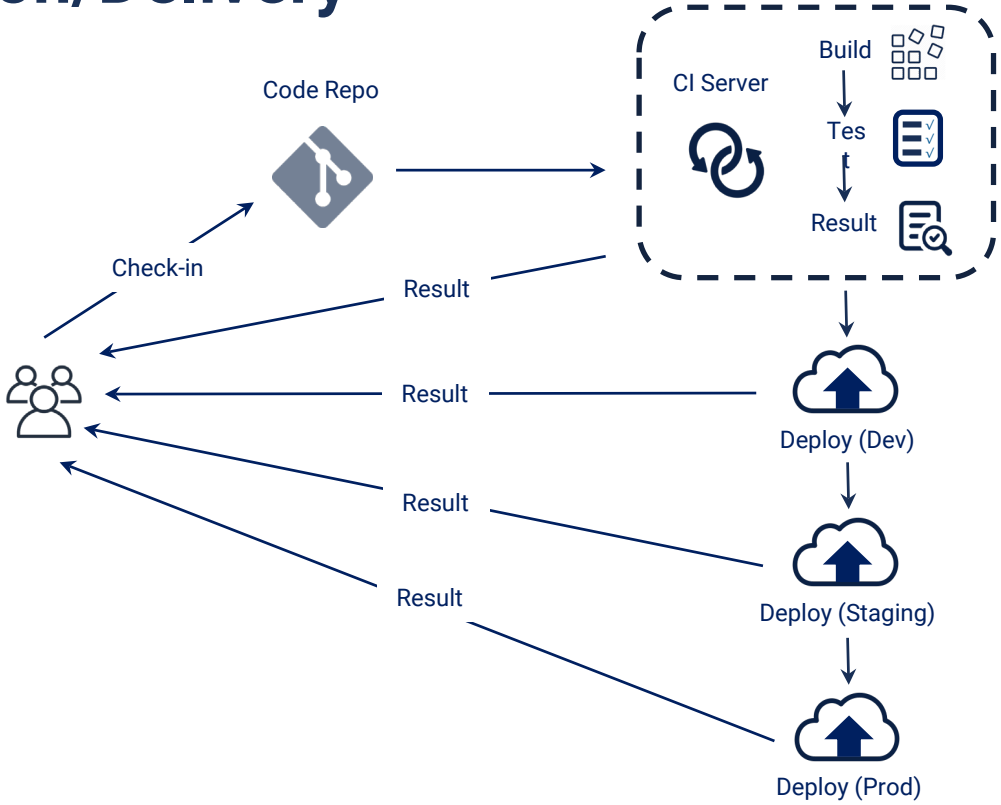
Continuous Integration

- Write and merge code often
- Commit to a shared code repository such as Git
- Automatically build and test code on every commit
- Fast feedback loops



Continuous Integration/Delivery

- Create release artifacts for CD
- Deploy code artifacts to resources
- Validate apps and services are functioning
- Monitor to verify state and recover if failing



GitOps Concepts

GitOps is managing operations by Git

3 Practices that make up a mature GitOps practice:

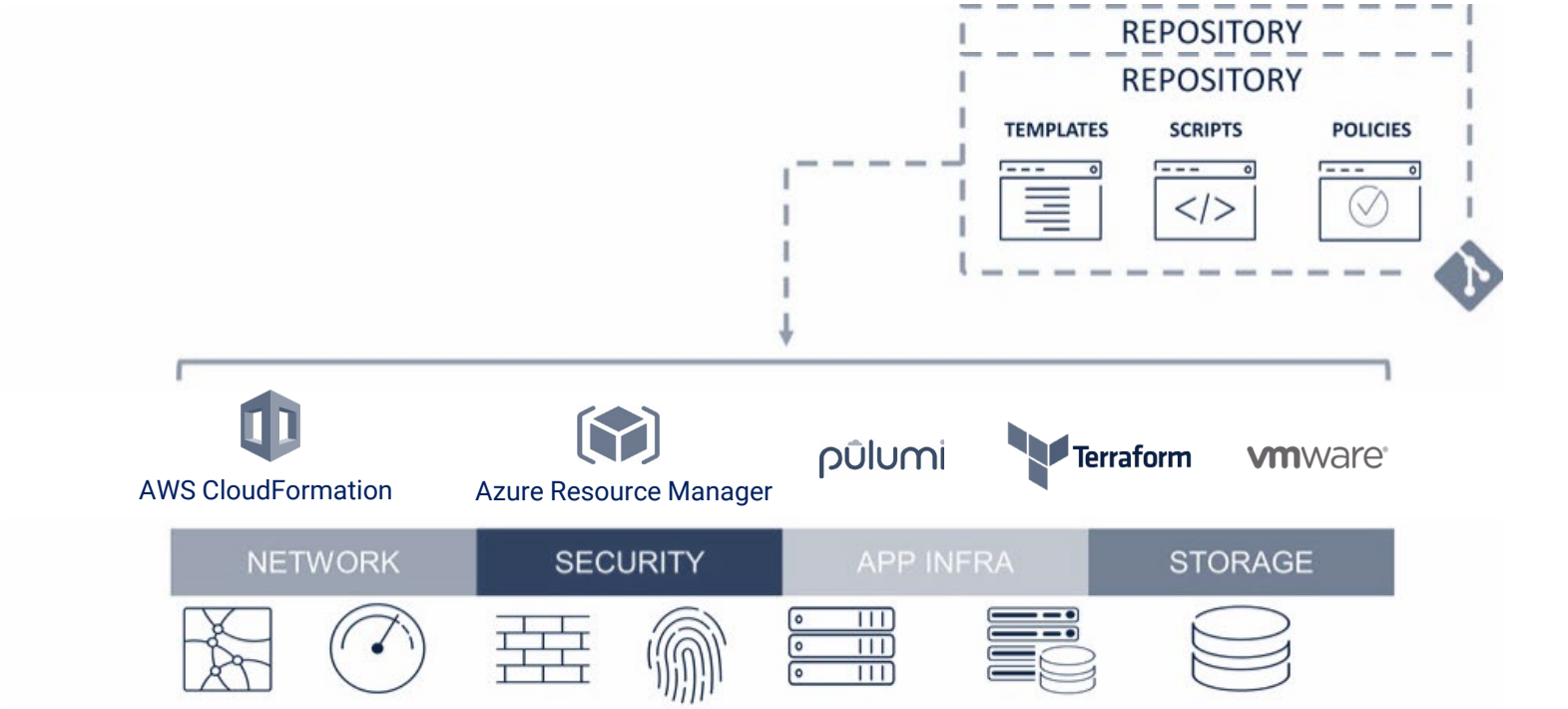
GitOps =

Infrastructure-as-Code (IaC)

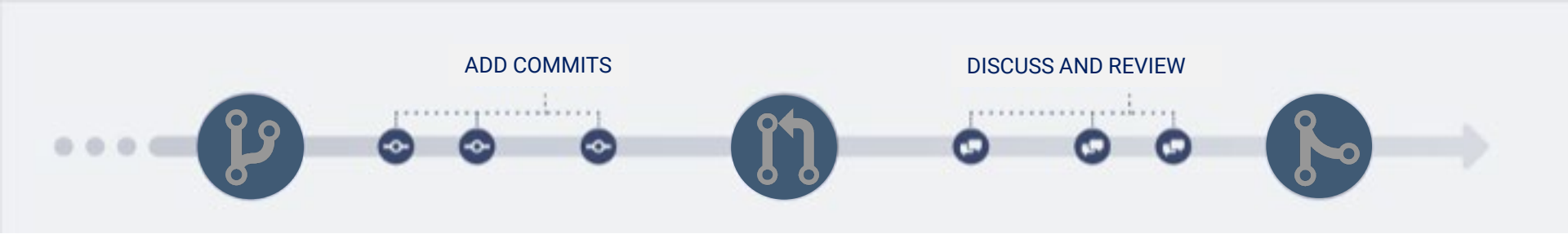
+ PRs/MRs

+ CI/CD

Git repository as the single source of truth for the definition of your Infrastructure



Pull/Merge Requests as the Agents of Change



Create a Branch

Create a branch in your project where you can safely experiment and make changes

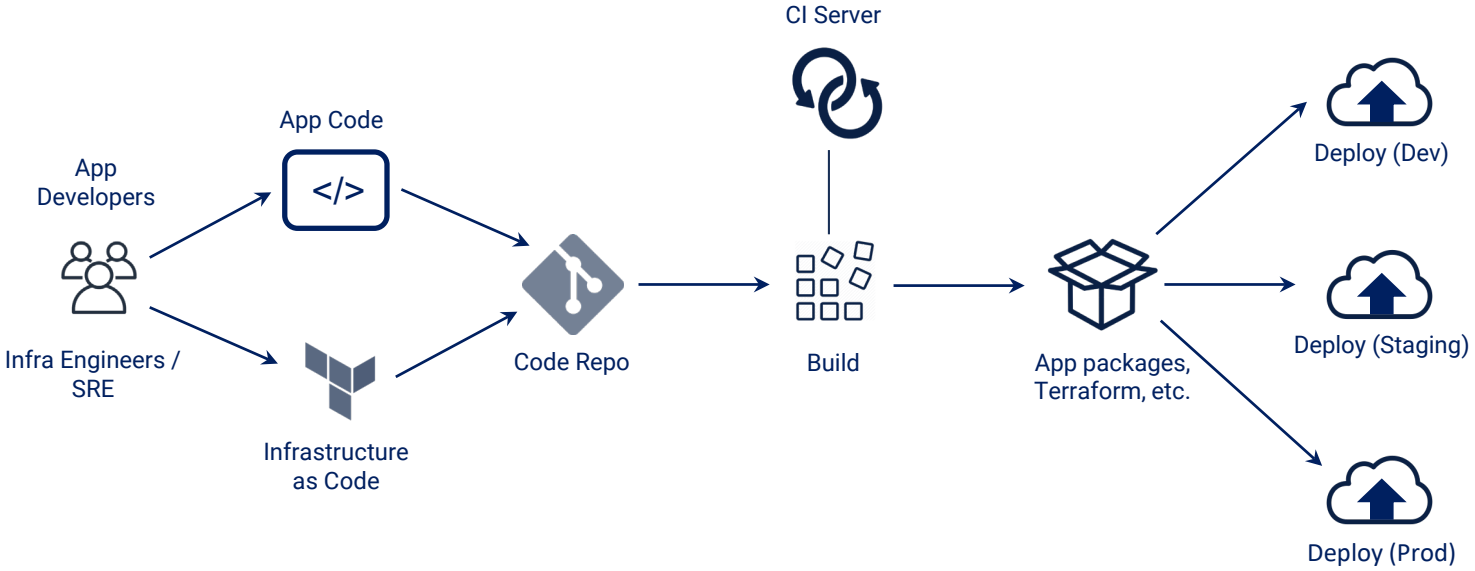
Open a Merge Request

Use a merge request to get feedback on your changes

Merge and Deploy

Merge your changes into your main branch and deploy your infrastructure

Adding IaC to the CI/CD Pipeline

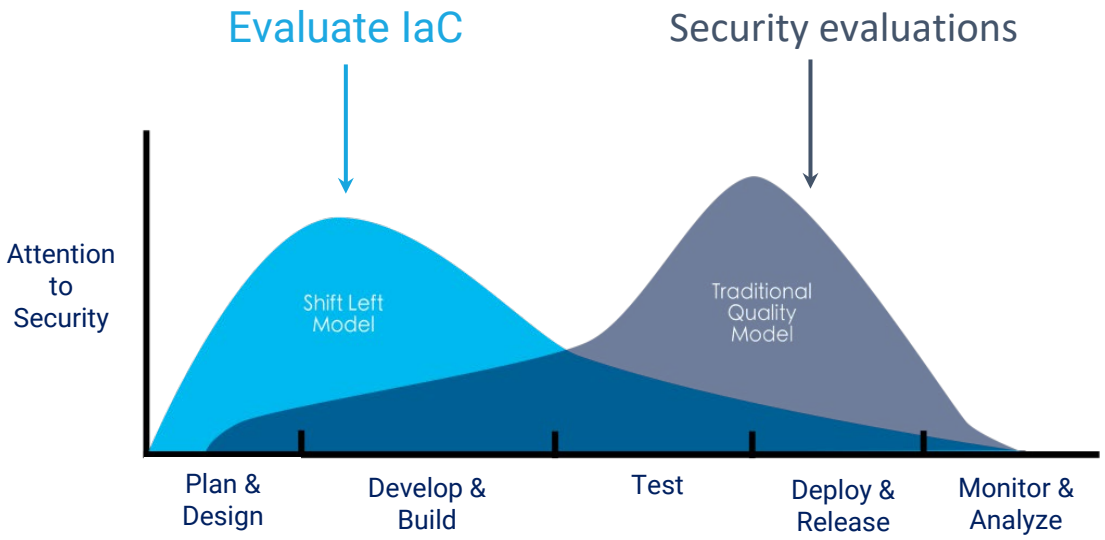


DEMO: IaC + Git @ Cloudrail

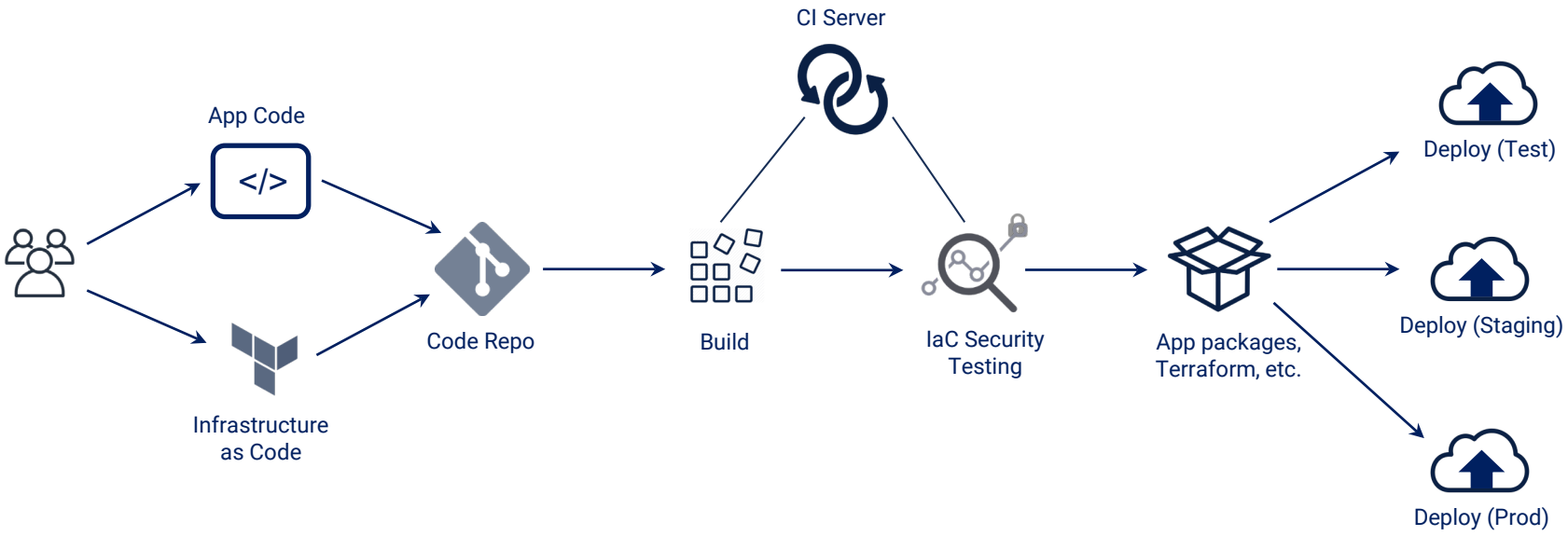
With Infrastructure-as-Code, we can apply the same software disciplines and quality gates that are used to manage application code to the Cloud infrastructure.

Even security.

Legacy Approach to Security uncover issues too late in the process



IaC Security Testing in the CI/CD Pipeline



Static vs. Dynamic Analysis for IaC

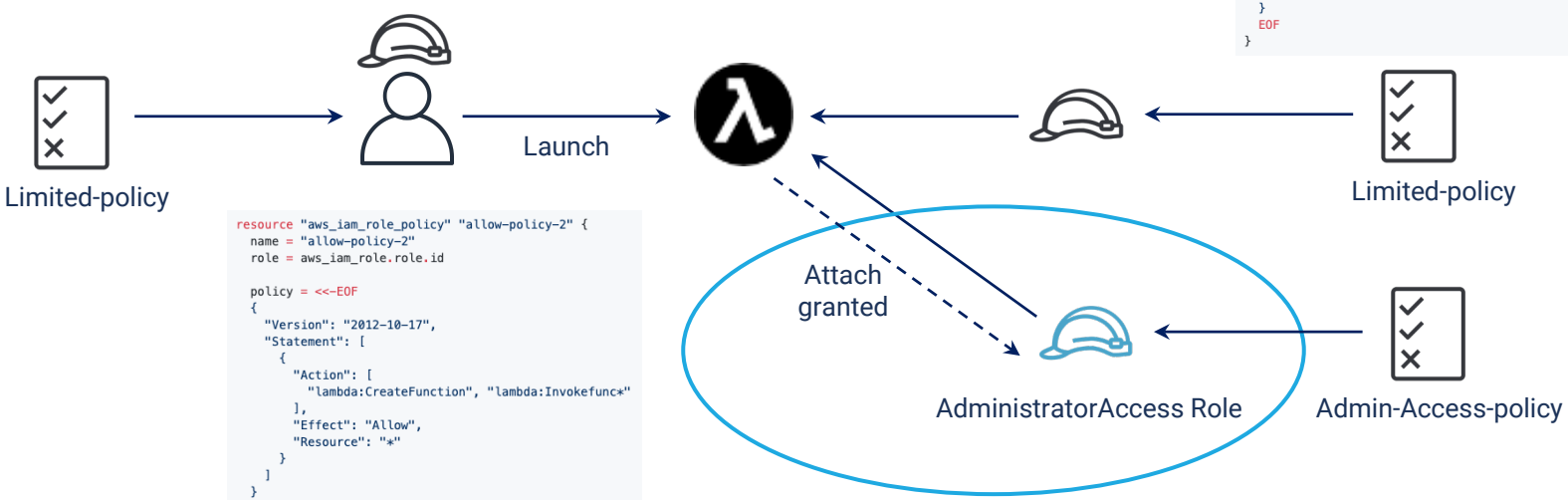
	Static Analysis	**Dynamic Analysis**
How does it work	Scan source IaC (e.g. Terraform, AWS CloudFormation, etc.).	Scan both the source IaC files together with the live Cloud environments
Pros	Simple to use and can be done faster as compared to Dynamic Analysis.	Much more comprehensive approach with higher degree of accuracy and catch sophisticated issues hidden from Static Analysis (e.g. drift, privilege escalation, etc.)
Cons	Can be noisy and unable to perform comprehensive security analysis.	The scans takes longer to run and with more resources.

Comparison:

How cloud misconfigurations are identified by static analysis, vs dynamic

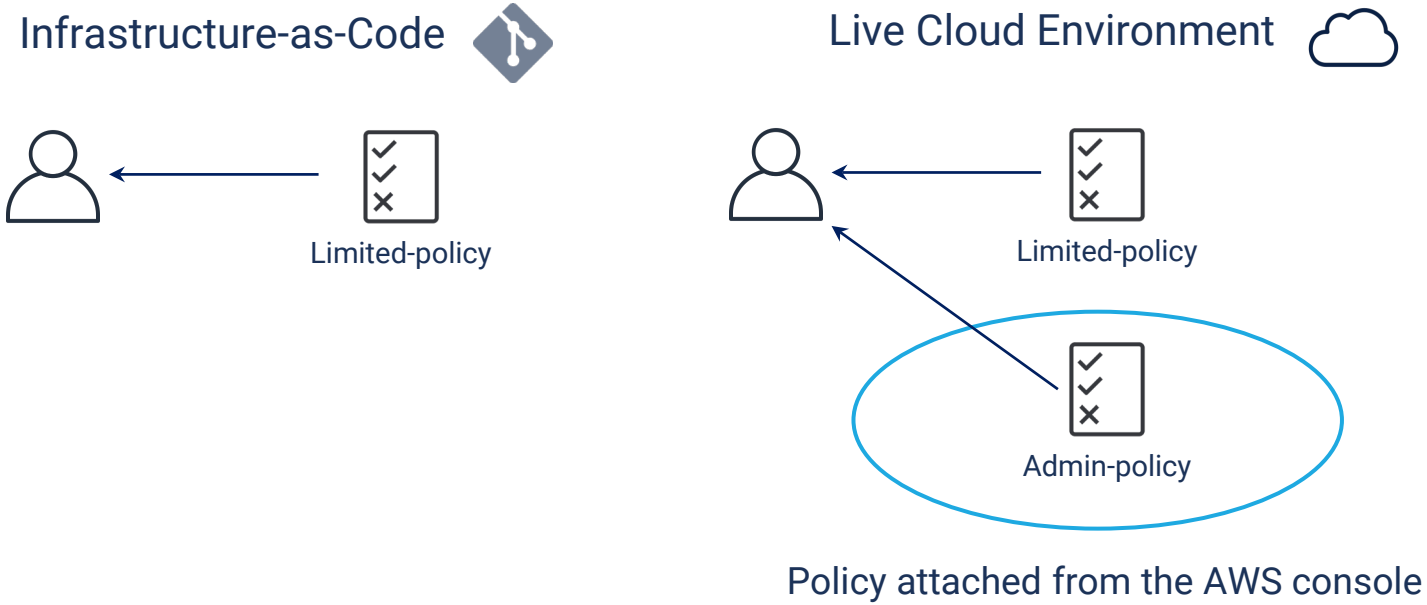
Avoid Privilege Escalation

```
resource "aws_iam_role_policy" "allow-policy-1" {
  name = "allow-policy-1"
  role = aws_iam_role.role.id

  policy = <<-EOF
  {
    "Version": "2012-10-17",
    "Statement": [
      {
        "Action": [
          "iam:PassRole"
        ],
        "Effect": "Allow",
        "Resource": "*"
      }
    ]
  }
  EOF
}
```

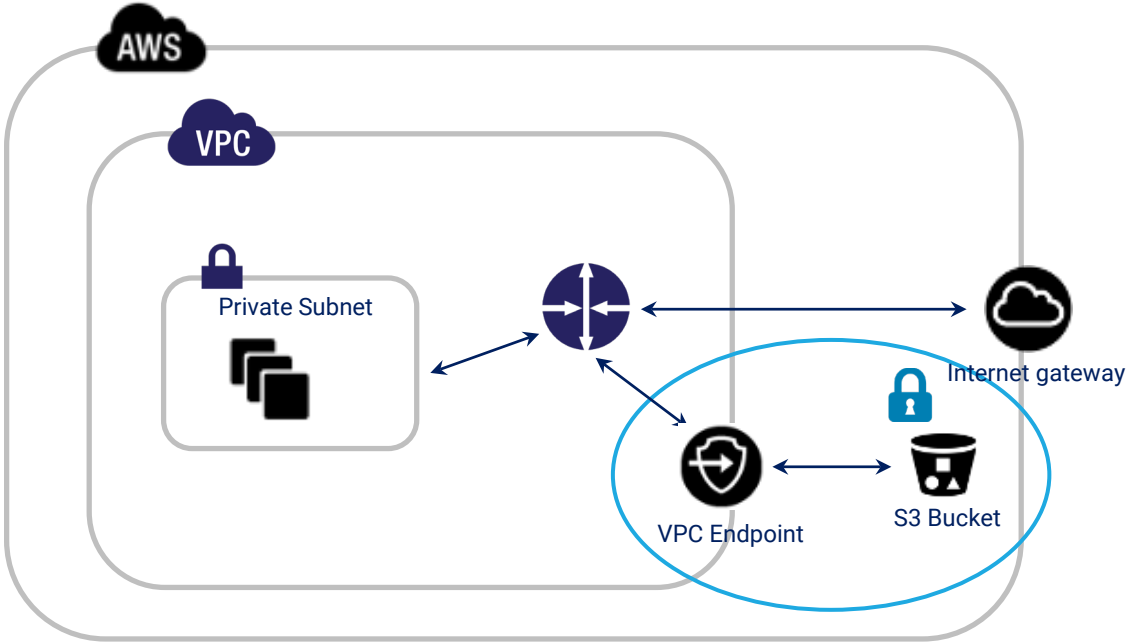



```
resource "aws_iam_role_policy" "allow-policy-2" {
  name = "allow-policy-2"
  role = aws_iam_role.role.id

  policy = <<-EOF
  {
    "Version": "2012-10-17",
    "Statement": [
      {
        "Action": [
          "lambda:CreateFunction", "lambda:Invokefunc*"
        ],
        "Effect": "Allow",
        "Resource": "*"
      }
    ]
  }
  EOF
}
```

IAM Drift Resulting in Over Privileged User

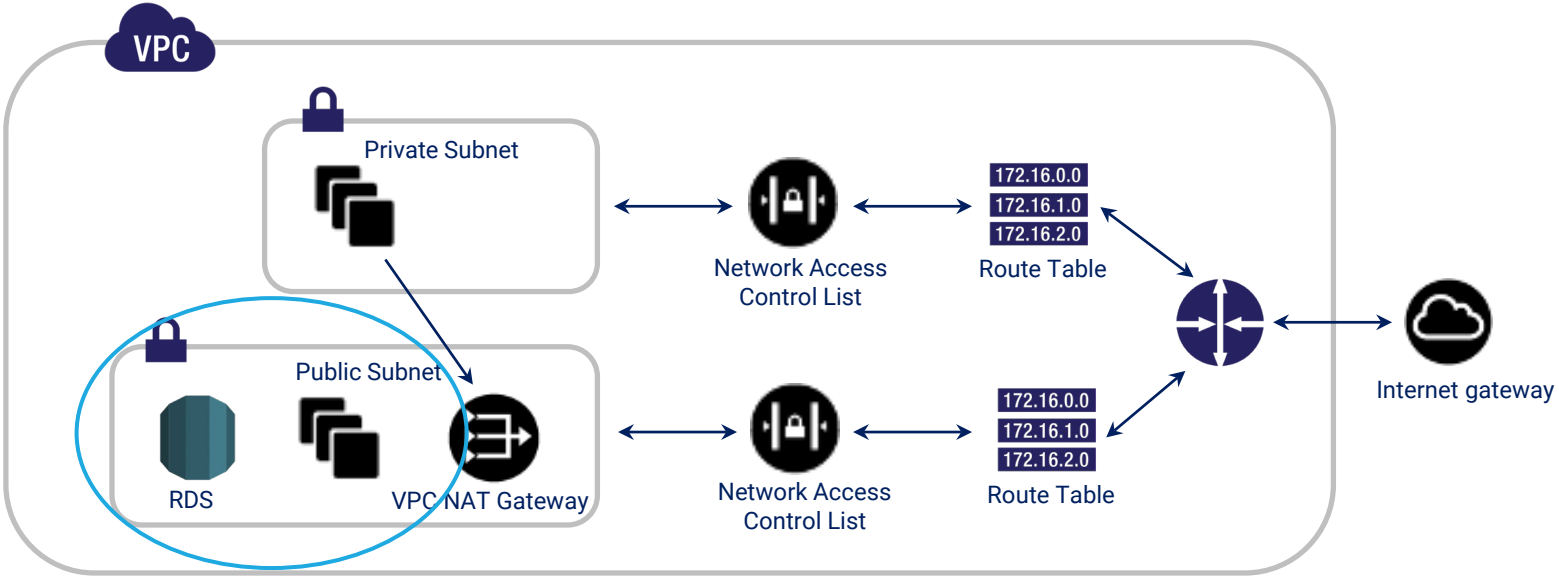


Protecting S3 Buckets



S3 not public by their ACLs
S3 not public by their policy
Follow least privilege concepts
Encrypt data at rest & in transit
Use VPC Endpoints

Inadvertently Deploying RDS Database in a Public Subnet



DEMO: IaC security tools in action

checkov by bridgecrew

cloudrail

TFSEC

https://github.com/iacsecurity/tool-compare

Developer Perspective

Speed
Full automation
Familiar tools

Security Team Perspective

Guardrails for developers
Visibility into the SDLC
Improved Cloud security posture

Development & Security teams working in harmony!

Roadmap for your GitOps Journey

IaC

Shift from manual configuration to configuration by code

IaC in CI/CD

Integrate IaC into the CI/CD Pipeline

Static Analysis

Scan IaC files without live cloud environment

Dynamic Analysis

Scan IaC files together with the live cloud environment

Policy Enforcement

Stop the pipeline if security or compliance issue is detected

Key Takeaways

Provision Cloud Infrastructure using IaC

Automate Cloud deployment with the CI/CD Pipeline

Automate security review - start with Static Analysis

Advance to Dynamic Analysis for continuous security

cloudrail

Thank you.