CLOUDETEER | DECODED

From Code to Cloud

Building Resilient Infrastructure with IaC and Automated Deployments

Roman Schwarz & Melody Sofia Eroshevich

&

Roman Schwarz
Senior Site Reliability Engineer

Melody Sofia Eroshevich
Site Reliability Engineer & Community Lead

Incidents

Missing Policy caused Production Risk

A missing policy integration allowed an **insecure configuration** (open security group) into **production**. The issue bypassed review and **required a rollback**.

Provider Update caused Massive Change

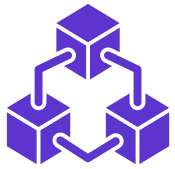
A **missing lock file** and **loose provider constraints** (v1.*) triggered a provider upgrade, making a small code change produce a huge, **unexpected** Terraform plan.

Manual Hotfix caused Silent Drift

Manual remediation in the cloud console introduced drift. Because Terraform state was unaware, a later terraform apply **reverted the fix**, causing a **repeat outage**.

Resilience in IaC

CLOUDETEER | DECODED



Consistency

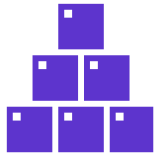
Dev, QA, and production should run identical code paths and modules — no snowflakes.

Auditability

Every plan, approval, and policy must be stored, visible, and reviewable at any time.

Reversibility

Always keep a safe rollback path to restore a known good state if needed.



Small Blast Radius

Split deployments into smaller units so one failure or lock doesn't block the whole platform.

Incident 1

CLOUDETEER | DECODED

Missing Policy caused Production Risk

A missing policy integration allowed an **insecure configuration** (open security group) into **production**. The issue bypassed review and **required a rollback**.

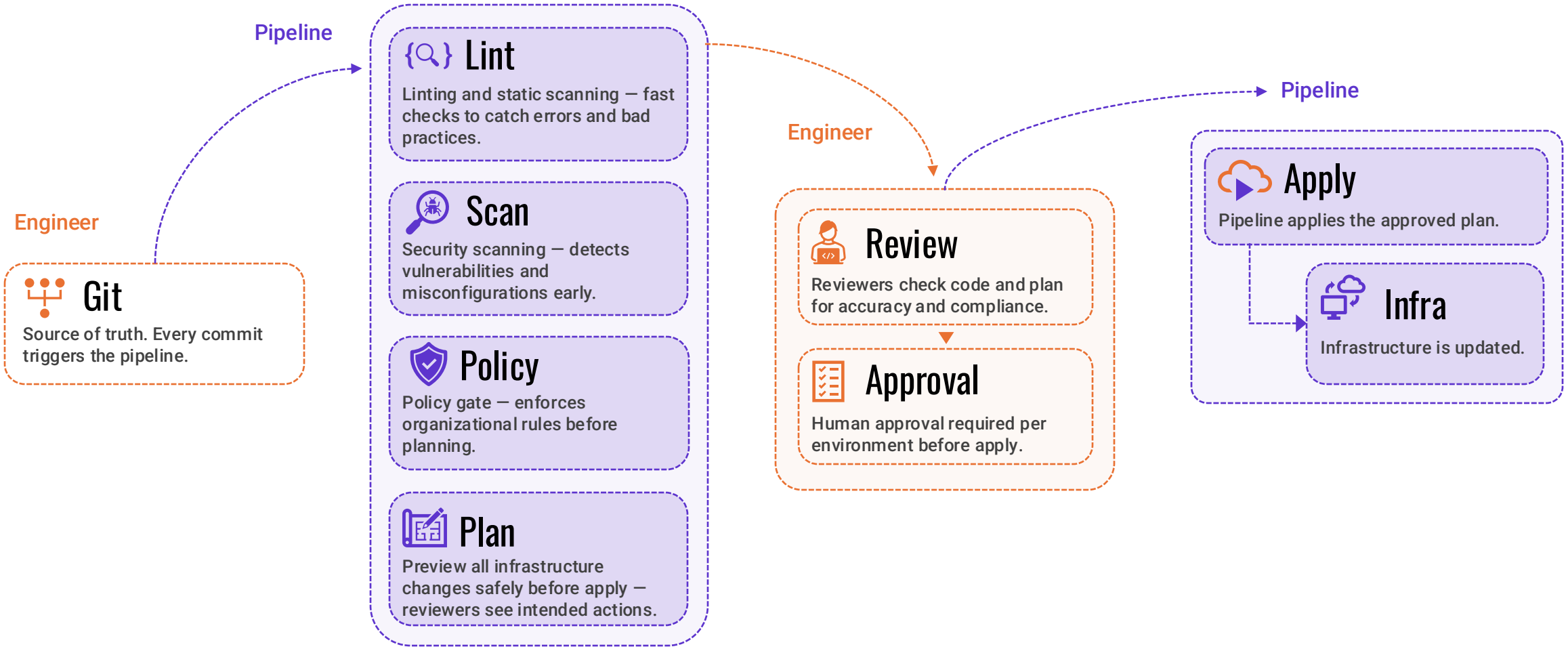
Provider Update caused Massive Change

A **missing lock file** and **loose provider constraints** (~> 1.0) triggered a provider upgrade, making a small code change produce a huge, **unexpected** Terraform plan.

Manual Hotfix caused Silent Drift

Manual remediation in the cloud console introduced drift. Because Terraform state was unaware, a later terraform apply **reverted the fix**, causing a **repeat outage**.

Delivery Architecture



Policy & Security Gates

CLOUDETEER | DECODED

TFLint

Static Rules

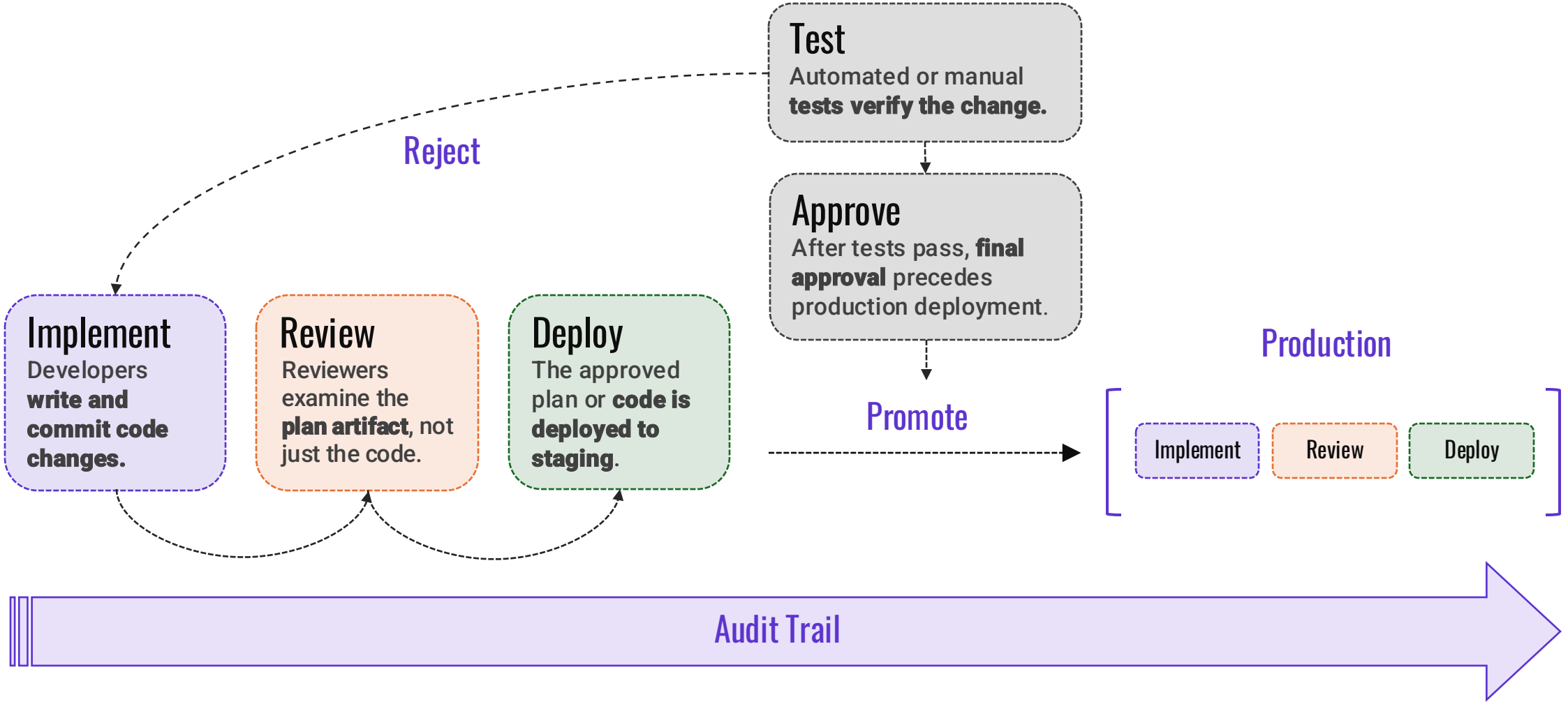
Trivy

Security Scanning

Conftest

Organization Policies

Approvals & Promotions



Incident 2

CLOUDETEER | DECODED

Missing Policy caused Production Risk

A missing policy integration allowed an **insecure configuration** (open security group) into **production**. The issue bypassed review and **required a rollback**.

Provider Update caused Massive Change

A **missing lock file** and **loose provider constraints** (~> 1.0) triggered a provider upgrade, making a small code change produce a huge, **unexpected** Terraform plan.

Manual Hotfix caused Silent Drift

Manual remediation in the cloud console introduced drift. Because Terraform state was unaware, a later terraform apply **reverted the fix**, causing a **repeat outage**.

Import & Prevent Destroy

CLOUDETEER | DECODED

import.tf

```hcl
resource "leaseweb_dedicated_server" "vm01" {
  reference                     = "vm01"
  reverse_lookup                = "vm01.example.com"
  public_network_interface_opened = true
  public_ip_null_routed         = false
}

import {
  to = leaseweb_dedicated_server.vm01
  id = "11111111-2222-3333-4444-555555555555"
}
```

prevent_destroy.tf

```hcl
resource "leaseweb_dedicated_server_installation" "ubuntu" {
  dedicated_server_id = leaseweb_dedicated_server.vm01.id
  operating_system_id = "UBUNTU_24_04_64BIT"

  lifecycle {
    prevent_destroy = true
  }
}
```

Versioning

CLOUDETEER | DECODED

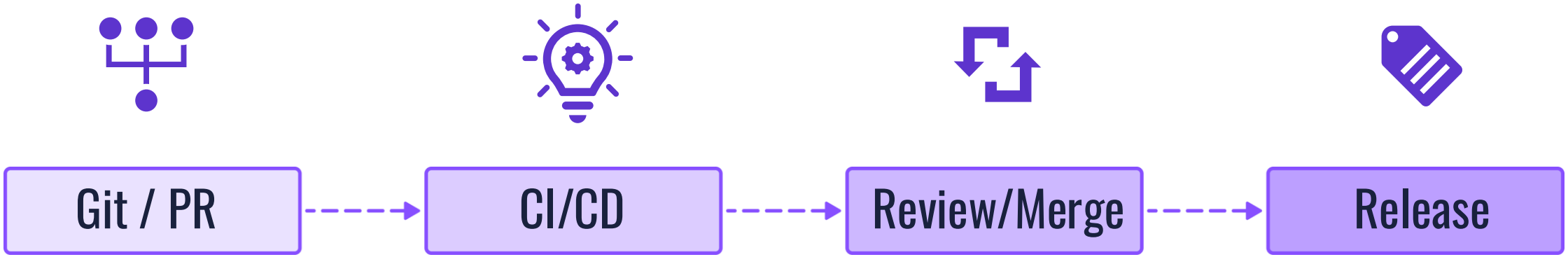
main.tf

```hcl
terraform {
  required_version = ">= 1.13"

  required_providers {
    leaseweb = {
      version = "~> 1.28.0"
      source  = "leaseweb/leaseweb"
    }
  }
}

module "vm" {
  source  = "cloudeteer/vm/leaseweb"
  version = "1.33.8"
}
```

.terraform.lock.hcl

```hcl
provider "registry.terraform.io/leaseweb/leaseweb" {
  version     = "1.28.1"
  constraints = "~> 1.28.0"
  hashes = [
    "h1:q5wYZwqSV+4nWTpJYdAwJ/L/CJIKs0rrffJj1bkc9fE="
  ]
}
```

Module Testing Workflow



- Review & Publish
- Semantic Versioning
- Predictable Releases

- terraform test
- Static Analysis
- Security Scan
- Documentation Validation

- Confirm correct version constraints
- Avoid breaking changes

- Final step: Release
- Automatic Semantic Versioning

Incident 3

CLOUDETEER | DECODED

Missing Policy caused Production Risk

A missing policy integration allowed an **insecure configuration** (open security group) into **production**. The issue bypassed review and **required a rollback**.

Provider Update caused Massive Change

A Terraform **missing lock file** and **loose provider constraints** triggered a provider upgrade, making a small code change produce a huge, **unexpected** Terraform plan.

Manual Hotfix caused Silent Drift

Manual remediation in the cloud console introduced drift. Because Terraform state was unaware, a later terraform apply **reverted the fix**, causing a **repeat outage**.

Scheduled Drift Detection

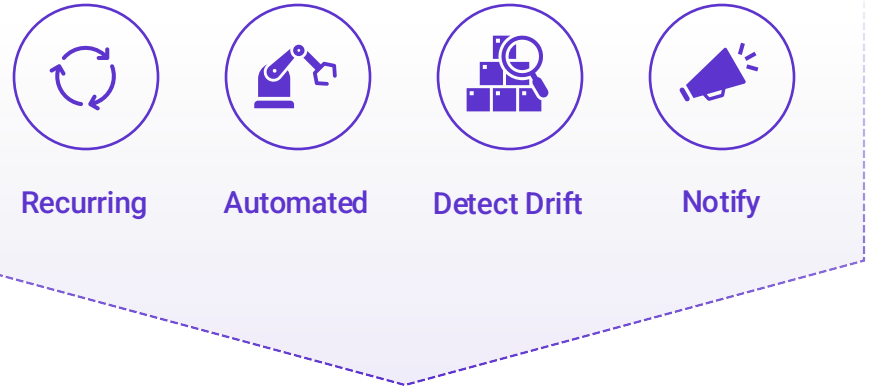
CLOUDETEER | DECODED

Terraform State

terraform.tfstate

```
{
  "version": 4,
  "terraform_version": "1.13.3",
  "resources": [
    {
      "mode": "managed",
      "type": "leaseweb_dedicated_server",
      "name": "vm01",
      "instances": [
        {
          "attributes": {
            "reference": "vm01",
            "reverse_lookup": "vm01.example.com",
            "public_network_interface_opened": true,
            "public_ip_null_routed": false
          }
        }
      ]
    }
  ]
}
```

Scheduled Pipeline



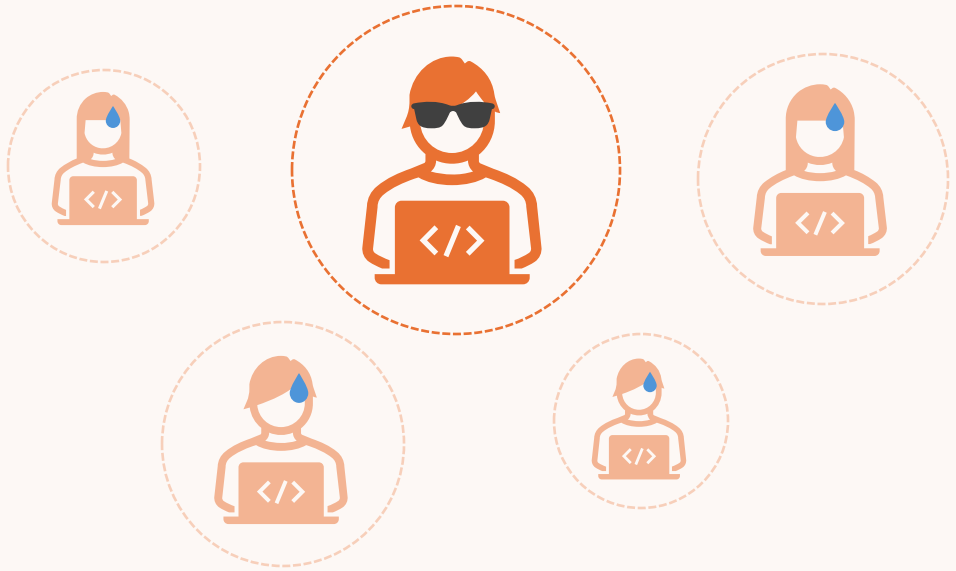
$ terraform plan -refresh-only || notify.sh

Infrastructure

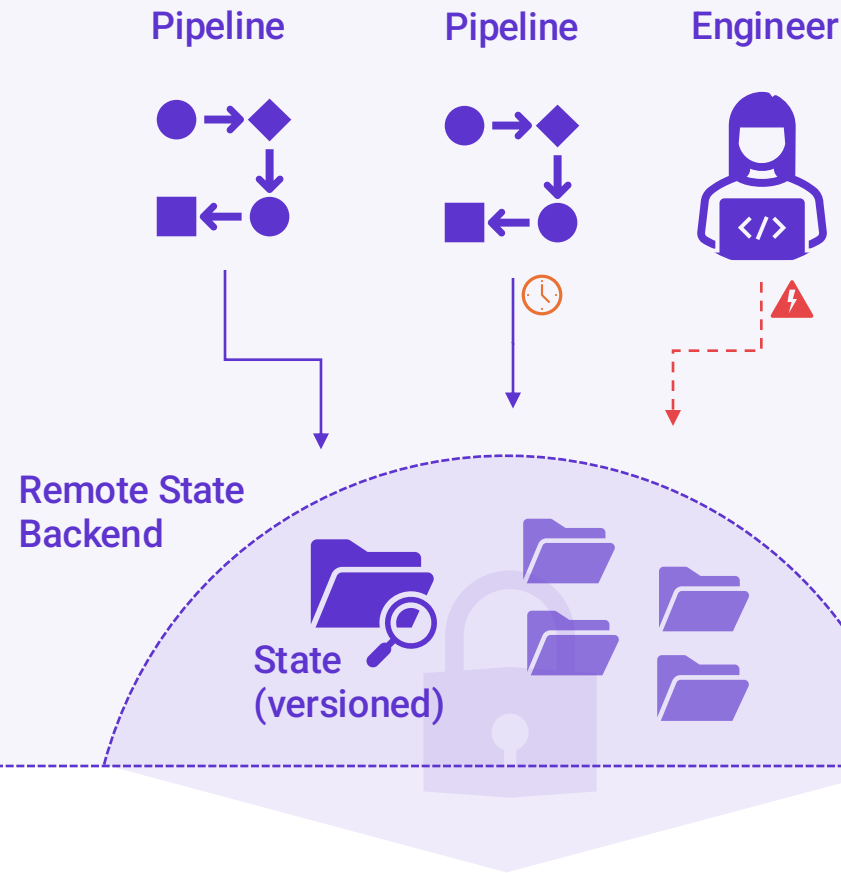
State & Locking

✗ Single State on Developer Machine

- No collaborative development
- No central pipeline



✓ Shared State with Locking Mechanism



Field Notes

CLOUDETEER | DECODED

Missing Policy caused Production Risk

A missing policy integration allowed an **insecure configuration** (open security group) into **production**. The issue bypassed review and **required a rollback**.

Provider Update caused Massive Change

A **missing lock file** and **loose provider constraints** (~> 1.0) triggered a provider upgrade, making a small code change produce a huge, **unexpected** Terraform plan.

Manual Hotfix caused Silent Drift

Manual remediation in the cloud console introduced drift. Because Terraform state was unaware, a later terraform apply **reverted the fix**, causing a **repeat outage**.

Field Notes

CLOUDETEER | DECODED

Policy is the First Line of Defence

Automate security and compliance — policies remember what humans forget.

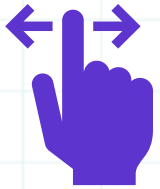
Version Control is Risk Control

Lock your provider versions — consistency is the foundation of resilience.

Detect, Don't Assume

Continuously detect drift — awareness prevents costly recovery.

Key Takeaways



Design for **control**, **not** for **speed**

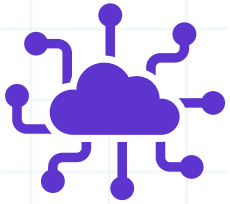
☑

Version and **verify** everything.

☑

Detect early, recover fast.

☑



Build systems that **remember**.

☑

References

Resource	Description / Purpose	Link
CLOUDETER DECODED Blog	Engineering blog by Cloudeteer with deep dives into cloud technologies and infrastructure automation.	https://engineering.cloudeteer.de/
CLOUDETEER Terraform Modules	Official Cloudeteer Terraform modules for reusable infrastructure components.	https://registry.terraform.io/namespaces/cloudeteer
Leaseweb Terraform Provider	Terraform provider for managing LeaseWeb infrastructure.	https://registry.terraform.io/providers/LeaseWeb/leaseweb/
Terraform Docs & Guides	Official HashiCorp Terraform documentation and learning resources.	https://developer.hashicorp.com/terraform
Trivy	Security scanner for containers, IaC, and dependencies.	https://trivy.dev/
TFLint	Linter for Terraform code to detect errors and enforce best practices.	https://github.com/terraform-linters/tflint
Conftest	Tool for testing configuration files using Open Policy Agent (OPA).	https://www.conftest.dev/
Checkov	Static analysis tool for scanning IaC for security and compliance misconfigurations.	https://www.checkov.io/

EOF

CLOUDETEER | DECODED

Thank you for listening.
Your attention and engagement means a lot.

LinkedIn
https://www.linkedin.com/showcase/cloudeteer-decoded/

Email
engineering@cloudeteer.de