

Infrastructure as Code on Azure:

# Bicep VS Terraform VS Pulumi

**Erwin Staal**

@erwin\_staal



# Erwin Staal

AZURE ARCHITECT 

Tech Lead 



2



@erwin\_staal

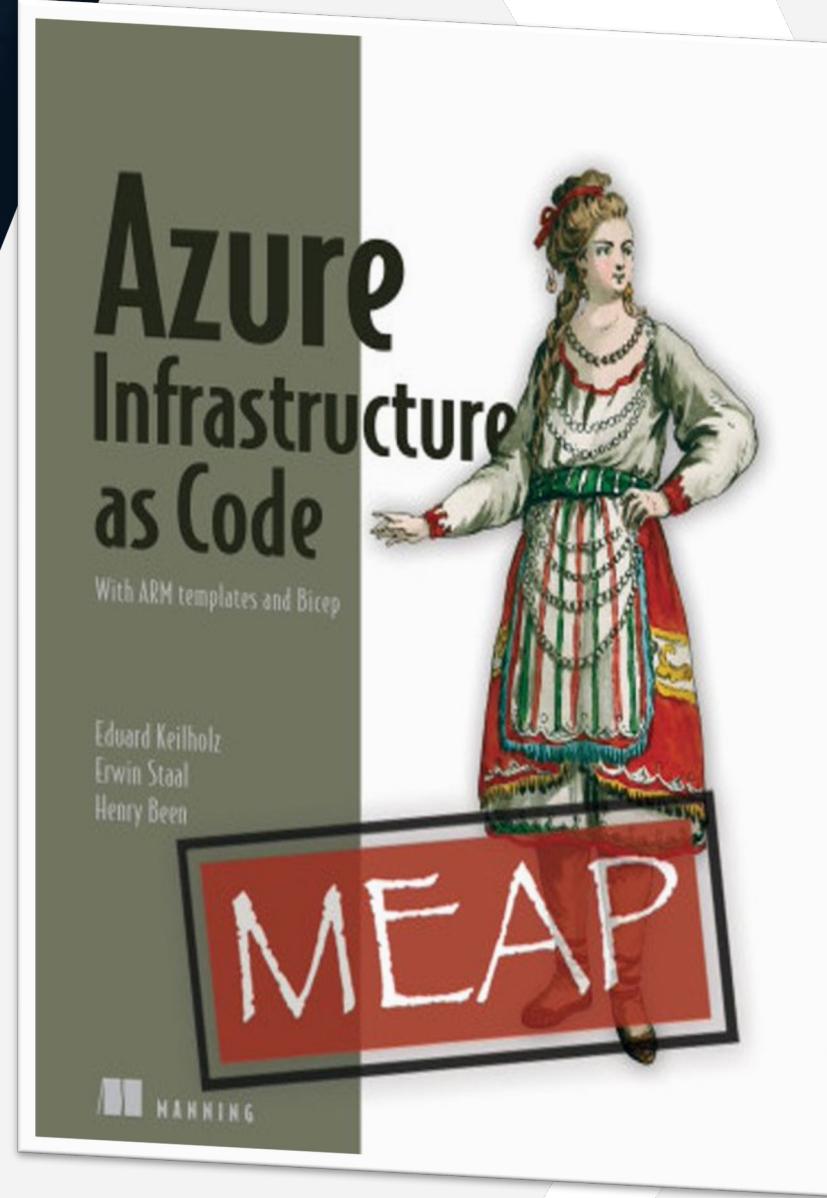
2

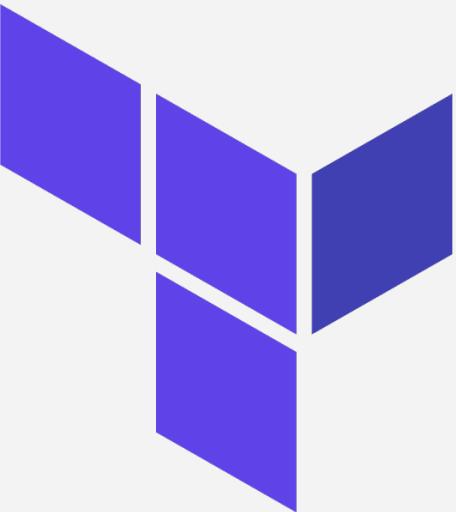
# Erwin Staal

AZURE ARCHITECT



Tech Lead



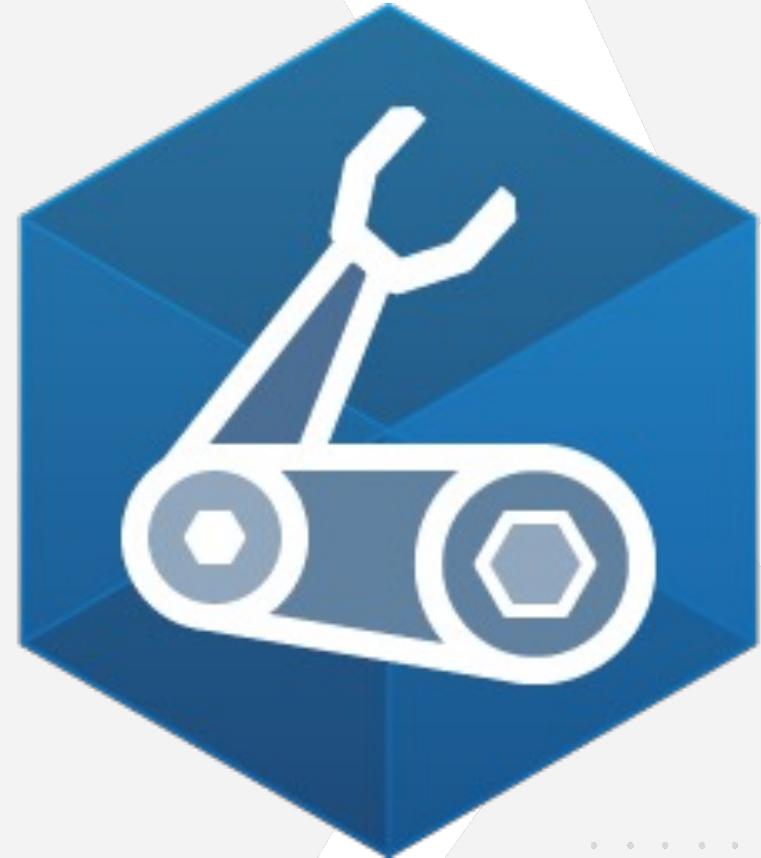


---

# Pulumi



Xspirit

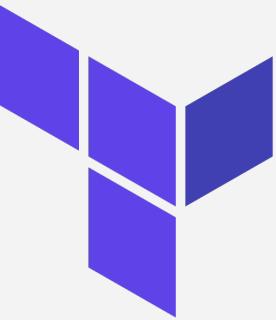


@erwin\_staal



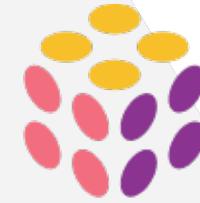
"Bicep is a domain-specific language (DSL) that uses declarative syntax to deploy Azure resources."

- › Created by Microsoft, GA in May 2021
- › Open Source
- › The replacement of ARM Templates
- › Uses a DSL



"Terraform is a tool for building, changing, and versioning infrastructure safely and efficiently. Terraform can manage existing and popular service providers as well as custom in-house solutions."

- › Created by HashiCorp in 2014
- › Open Source
- › Uses a DSL (HCL = HashiCorp Configuration Language)
- › \* Terraform CDK (Cloud Development Kit)



# Pulumi

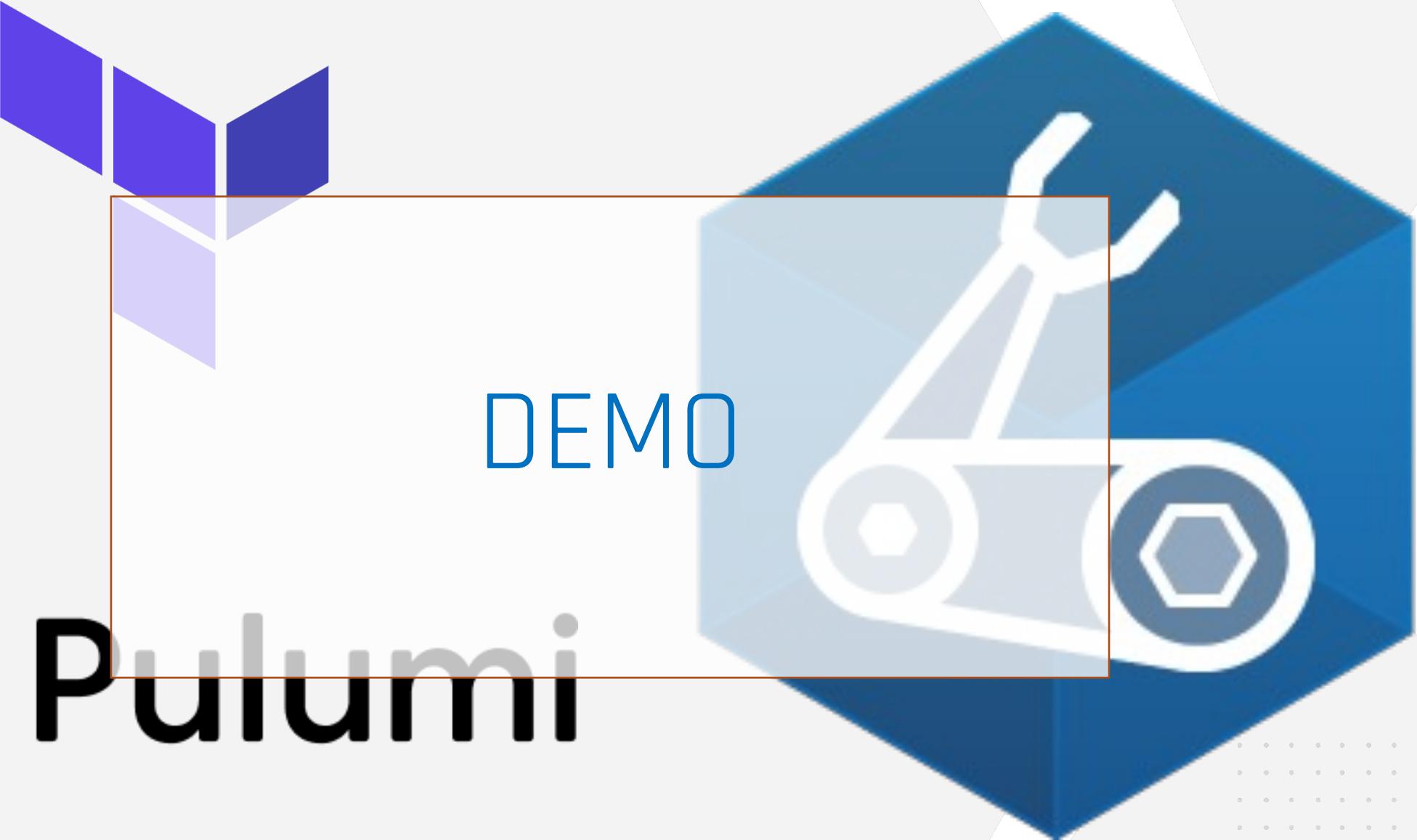
"Pulumi provides the industry's only automation workflow capability that allows software engineering to be applied to solve and manage cloud infrastructure at scale."

- › Created by Pulumi in 2018
- › Open Source
- › Write your IaC in your favorite language: TypeScript, JavaScript, Python, Go, .NET, Java, and YAML



# Pulumi

DEMO



# Deploy with a plan

#Infra Core Transformation Spoke Pipeline • Merged PR 9258  
Enza Zaden SDP 2.0 - Infra Core Transformation

Cancel

Summary Environments Terraform Plan Associated pipelines WhiteSource Bolt Build Report

Triggered by

Repository and version

Enza Zaden SDP 2.0 - Infra Core

main 22e40841

Time started and elapsed

Fri at 15:59

5d 18h 24m

Related

4 work items

4 published

Tests and coverage

Get started

View 15 changes

2 approvals need your review before this run can continue

Review

Stages Jobs

Build 1 job completed 16s 1 artifact

Plan: pndt - ddev 1 job completed 6m 39s 1 artifact

Apply: pndt - ddev 1 job completed 49s 1 artifact

Plan: pndt - dprd 1 job completed 5m 59s 1 artifact

Apply: pndt - dprd Waiting 0/1 checks passed

Plan: pndt - uprd 1 job completed 6m 49s 1 artifact

Apply: pndt - uprd Waiting 0/1 checks passed

# Deploy with a plan

#Infra Core Transformation Spoke Pipeline • Merged PR 9258  
Enza Zaden SDP 2.0 - Infra Core Transformation

Summary Environments **Terraform Plan** Associated pipelines WhiteSource Bolt Build Report

```
# (8 unchanged attributes hidden)

- spark_python_task {
    ~ python_file = "dbfs:/FileStore/entry_points/create_or_refresh_tables.py" -> (known after apply)
        # (1 unchanged attribute hidden)
    }

# (3 unchanged blocks hidden)
}

Plan: 1 to add, 3 to change, 1 to destroy.

Warning: Deprecated Resource

with module.compute.module.app_service_plan.azurerm_app_service_plan.app_service_plan,
on ../azure_modules/app_service_plan/main.tf line 6, in resource "azurerm_app_service_plan" "app_service_plan":
6: resource "azurerm_app_service_plan" "app_service_plan" {

The `azurerm_app_service_plan` resource has been superseded by the
`azurerm_service_plan` resource. Whilst this resource will continue to be
available in the 2.x and 3.x releases it is feature-frozen for
compatibility purposes, will no longer receive any updates and will be
removed in a future major release of the Azure Provider.

(and 3 more similar warnings elsewhere)

Warning: Attribute Deprecated

with module.naming_data_lake.random_string.main,
on ../azure_modules/naming/main.tf line 5, in resource "random_string" "main":
5:   number = var.unique-include-numbers

**NOTE**: This is deprecated, use `numeric` instead.

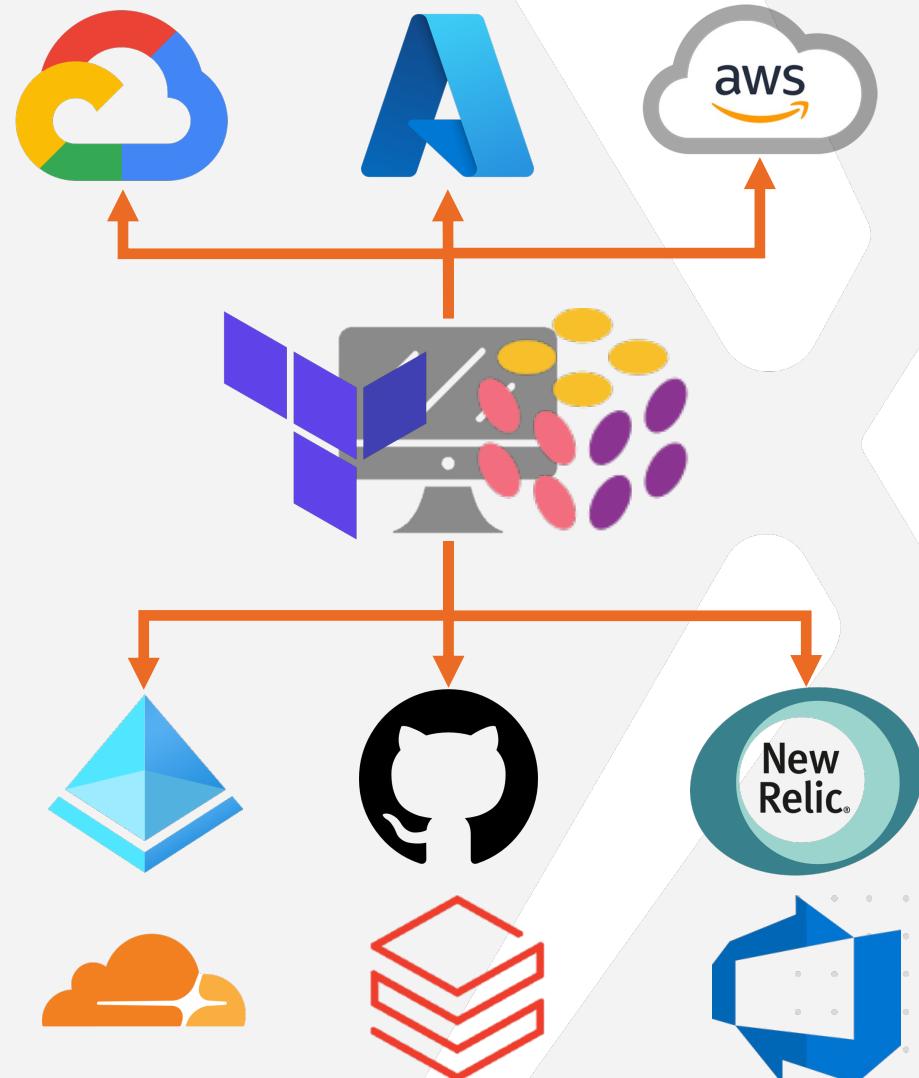
(and 39 more similar warnings elsewhere)
```

Saved the plan to: pnpt-uprd-78485-20230331141109-tf.plan

# Single or Multi Cloud?

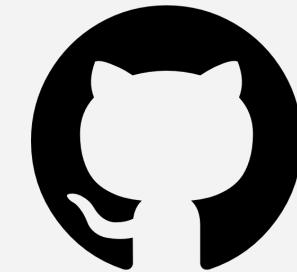


Control Plane vs Data plane



# Terraform and Pulumi Providers

- › Groups resources in logical units per cloud service
- › Official and Community providers
- › Distributed as plugins
- › For Pulumi: Native or Terraform



PagerDuty



# State

- › **Terraform** and **Pulumi** must store state about your managed infrastructure and configuration
- › **Bicep** does not have state
- › **Terraform**: by default, in a local file named "terraform.tfstate"
  - › Can also be stored remotely, which works better in a team environment
- › **Pulumi**: by default, in their SaaS offering
- › State can make things difficult

Terraform state example

```
{  
  "version": 4,  
  "terraform_version": "1.3.0",  
  "serial": 3,  
  "lineage": "9391dd05-a821-ed43-5a1c-8f5f1f59b2e4",  
  "outputs": {},  
  "resources": [  
    {  
      "mode": "managed",  
      "type": "azurerm_resource_group",  
      "name": "rg",  
      "provider": "provider[\"registry.terraform.io/hashicorp/azurerm\"]",  
      "instances": [  
        {  
          "schema_version": 0,  
          "attributes": {  
            "id": "/subscriptions/f0e483fc-9d2f-4a4b-8aee-887a398ff27e/resourceGroups/rg-terraform",  
            "location": "westeurope",  
            "name": "rg-terraform",  
            "tags": null,  
            "timeouts": null  
          },  
          "sensitive_attributes": [],  
          "private": "eyJlMmJmYjczMC1lY2FhLTEzZTYtOGY40C0zNDM2M2JjN2M0YzAiOnsiY3JlYXRlIjo1NDAwMDAwMDAwM  
        }  
      ]  
    },  
    {"check_results": []}  
  ]  
}
```

# State and secrets

- State can contain sensitive data: password, private keys, etc.
- **Terraform** state is stored in plain-text JSON files
- **Pulumi**: state is encrypted with a per stack key
- You need to ensure encryption at rest, IAM, TLS connection, IP whitelisting

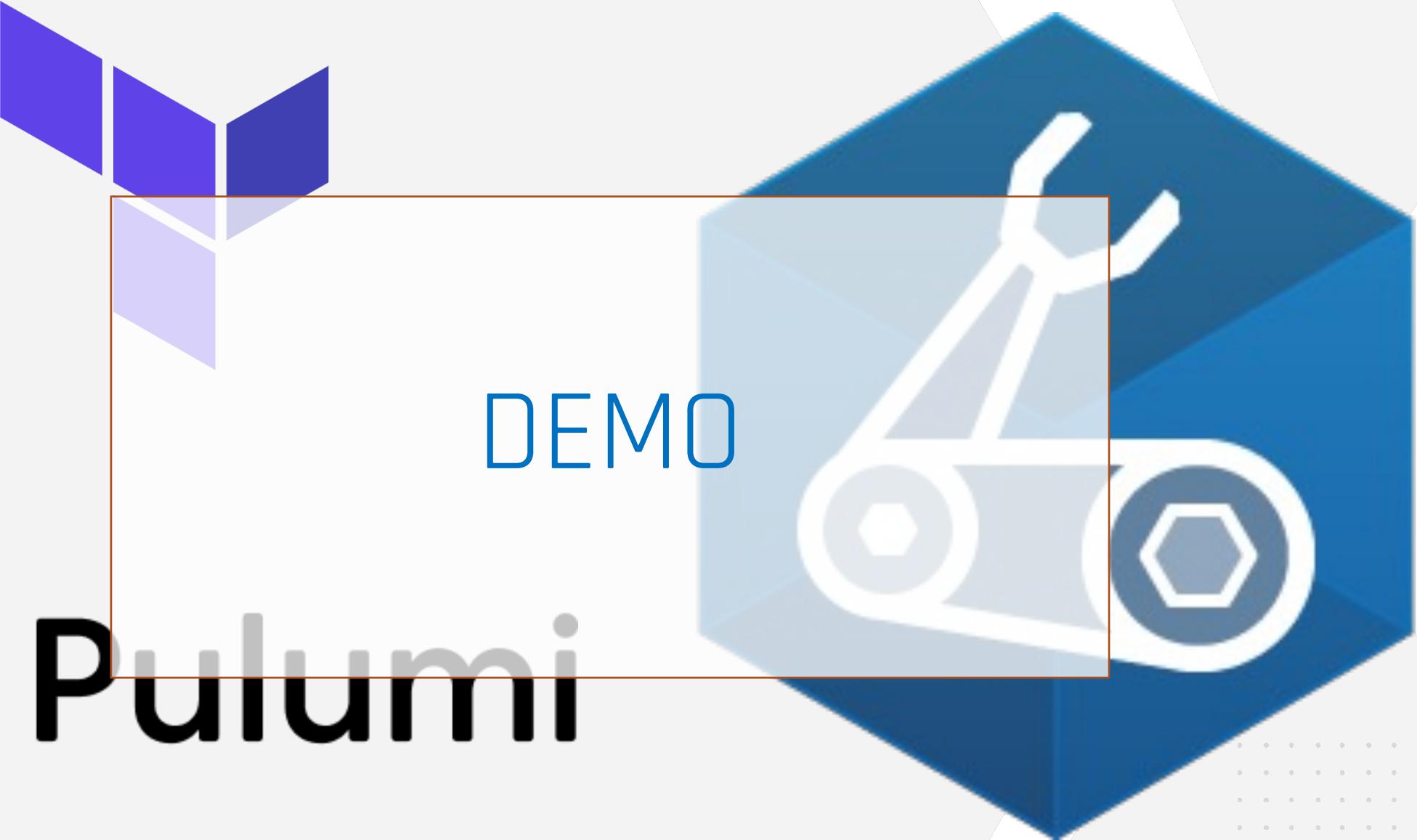
Terraform state example

```
{  
  "mode": "managed",  
  "type": "azurerm_key_vault_secret",  
  "name": "sql_server_admin_password",  
  "provider": "provider[\"registry.terraform.io/hashicorp/azurerm\"]",  
  "instances": [  
    {  
      "schema_version": 0,  
      "attributes": {  
        "content_type": "Managed by Terraform",  
        "expiration_date": "2023-03-12T09:13:17Z",  
        "id": "https://kv-tfsessionadvanced-dev.vault.azure.net/secrets/sql-server-admin-password",  
        "key_vault_id": "/subscriptions/f0e483fc-9d2f-4a4b-8aee-887a39c23456",  
        "name": "sql-admin-password",  
        "resource_id": "/subscriptions/f0e483fc-9d2f-4a4b-8aee-887a39c23456/resourceGroups/rg-tfstate/providers/Microsoft.KeyVault/vaults/kv-tfsessionadvanced-dev/secrets/sql-server-admin-password",  
        "value": "GUIYZ9MSYbv6PX4I33FbNsvVtqVx48aI",  
        "versionless_id": "https://kv-tfsessionadvanced-dev.vault.azure.net/secrets/sql-server-admin-password"  
      }  
    }  
  ]  
}
```



# Pulumi

DEMO

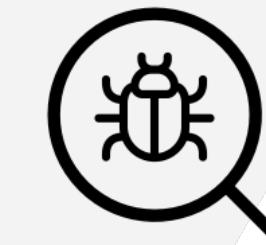
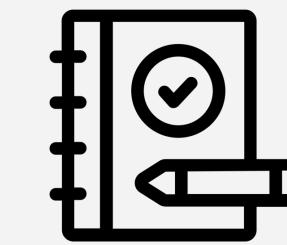
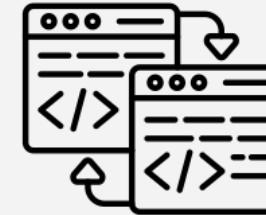
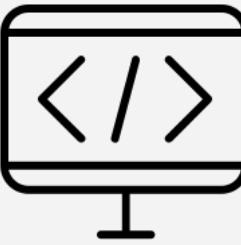


# The power of Pulumi

You can use your favorite programming language: TypeScript, JavaScript, Python, Go, .NET, Java, and YAML

User the power of your favorite IDE

Monitoring / Logging

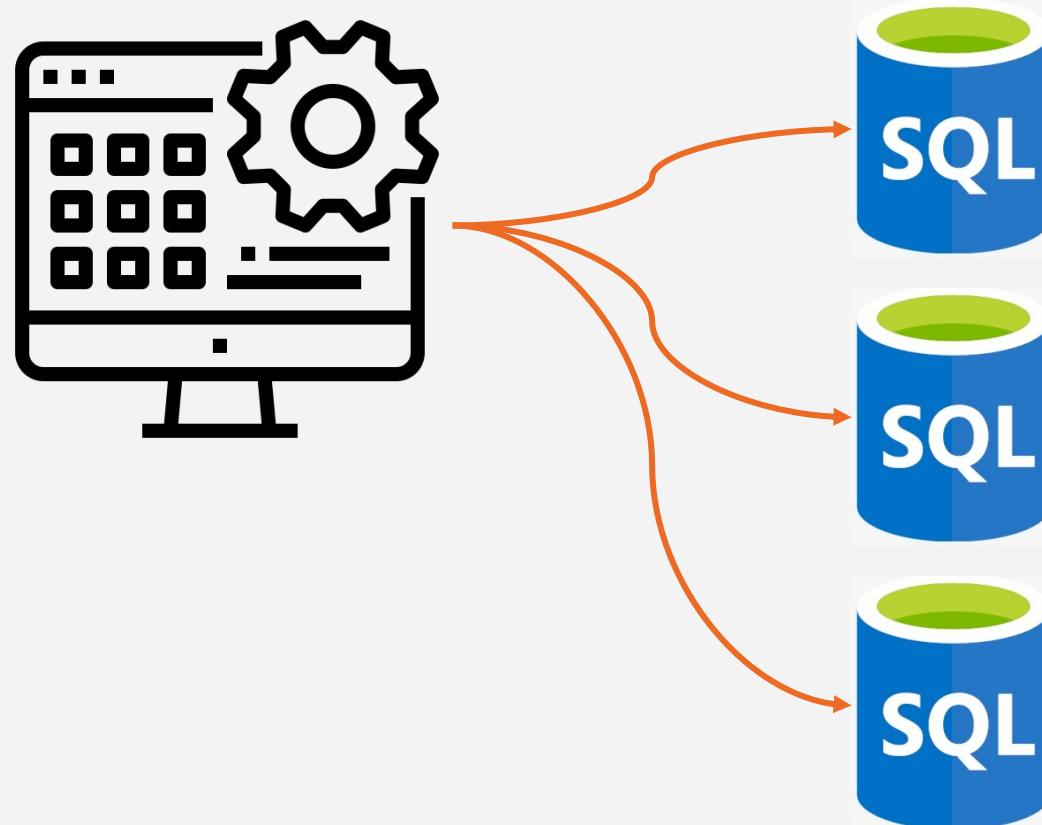


Refactoring

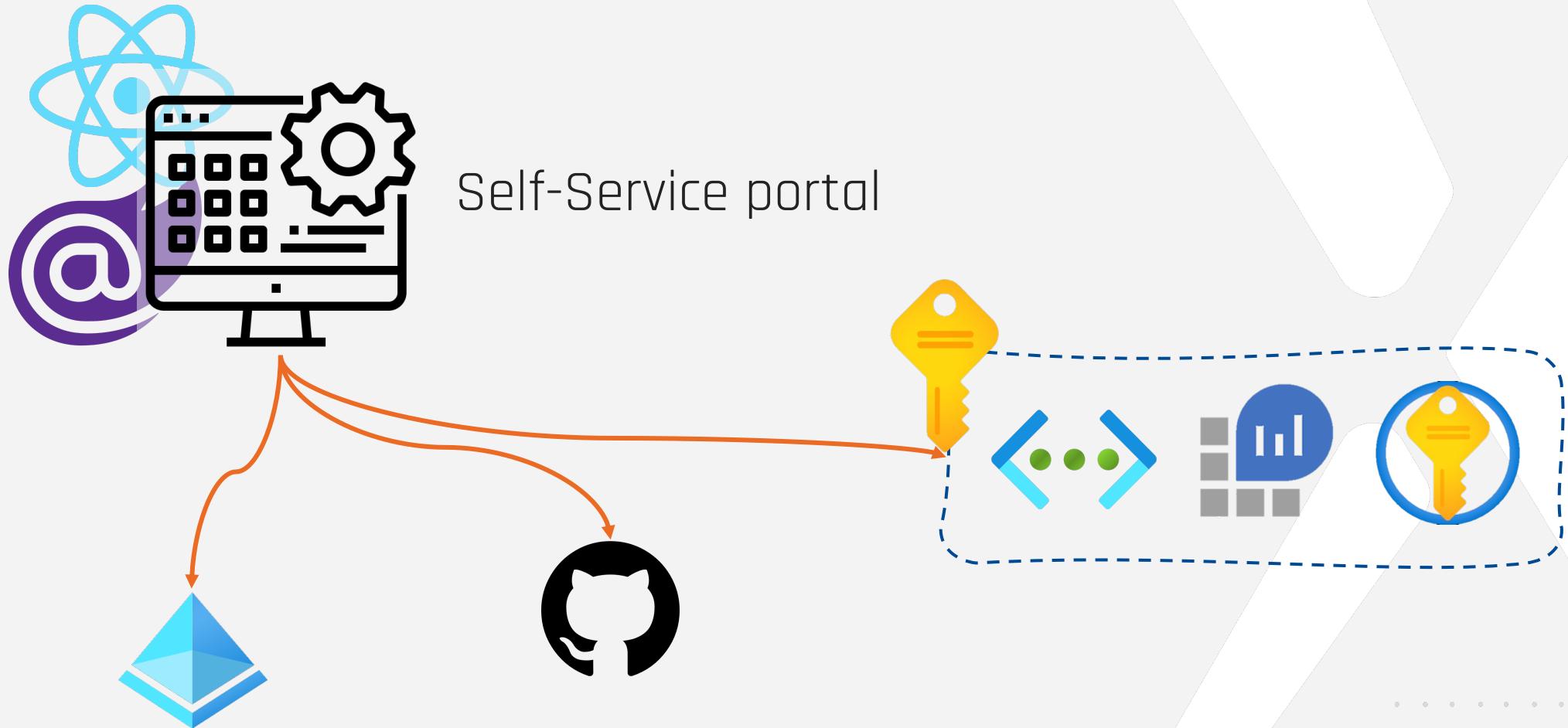
(Unit) testing

Debugging

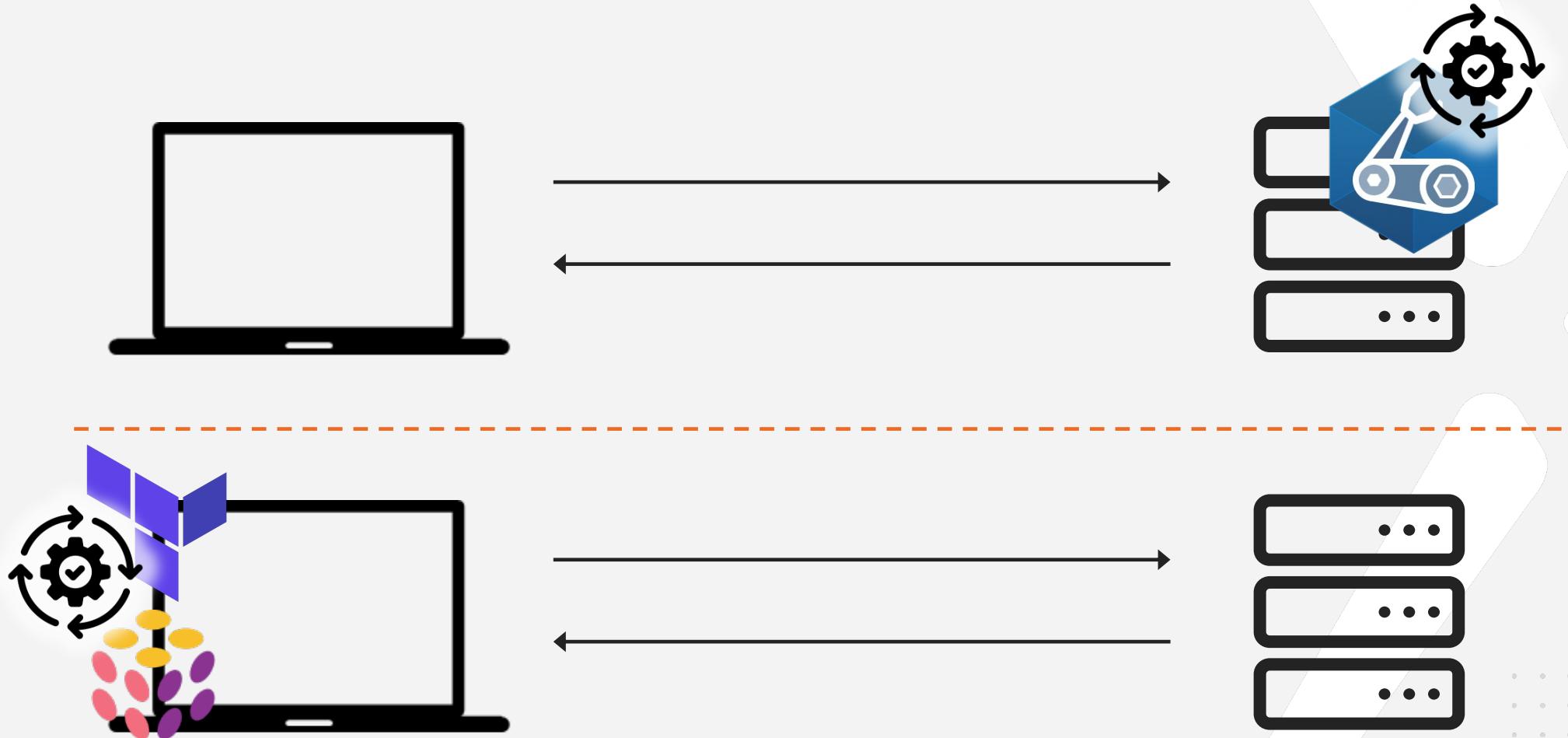
# Have applications create infrastructure



# Self-service tooling by platform teams



# Server vs Client-side execution



# Ecosystem

- › Azure DevOps / GitHub Actions
- › Checkov
- › Linter with a lot of built-in rules (ARM TTK)
- › PSRule



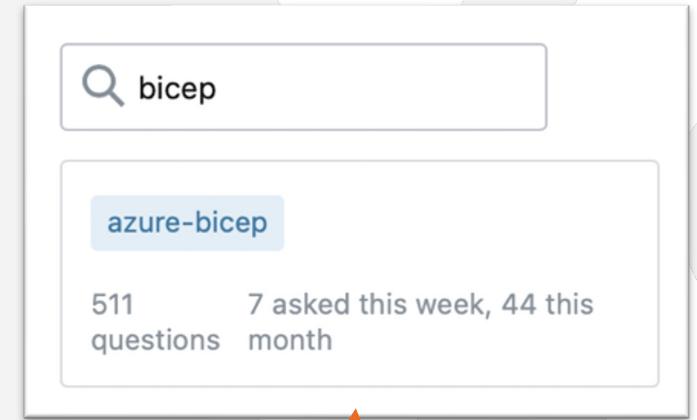
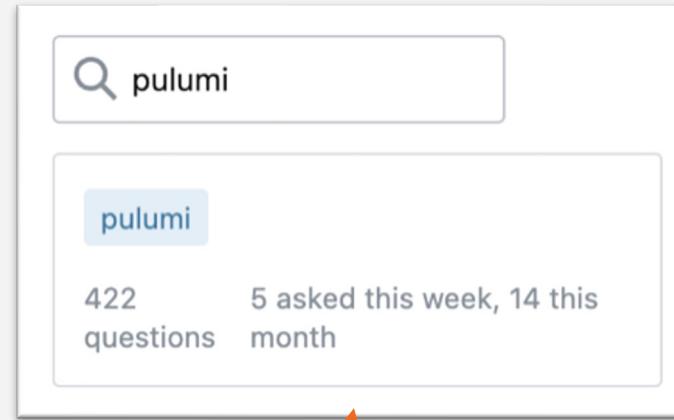
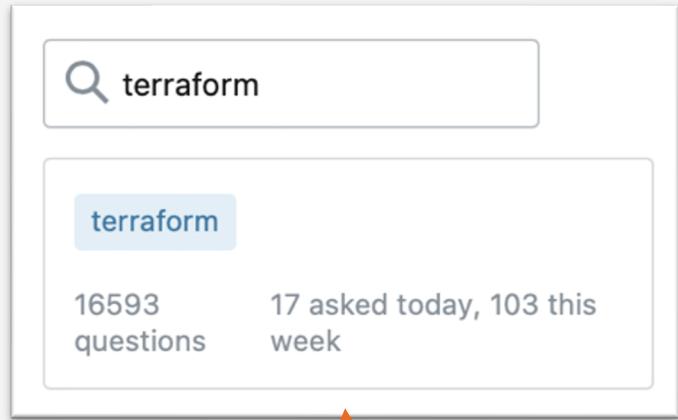
- › Azure DevOps / GitHub Actions
- › Checkov
- › TFSec
- › TFLint
- › Terratest
- › Terradocs
- › Git pre-commit



- › Azure DevOps / GitHub Actions
- › Test frameworks
- › SonarCloud etc.



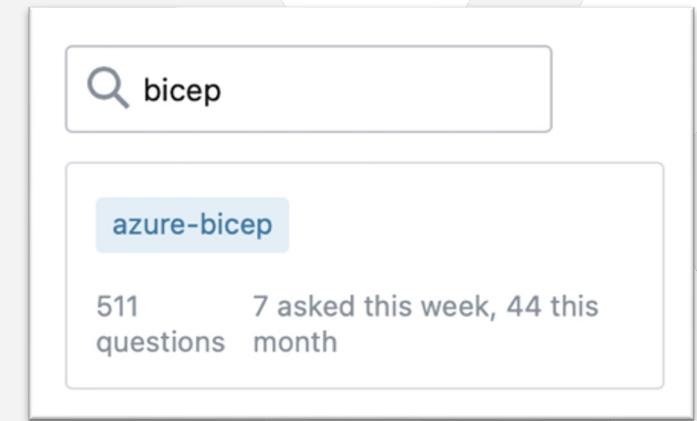
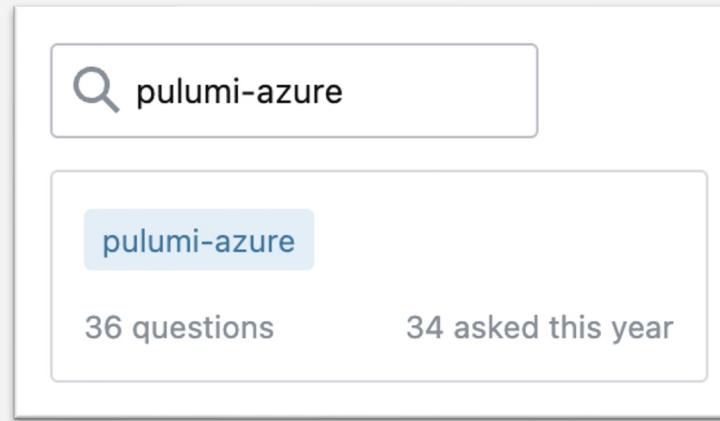
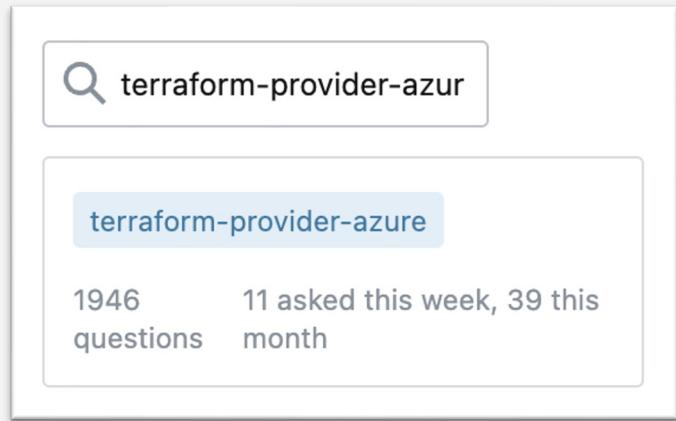
# Community - stackoverflow



This is not all Azure

This is all Azure

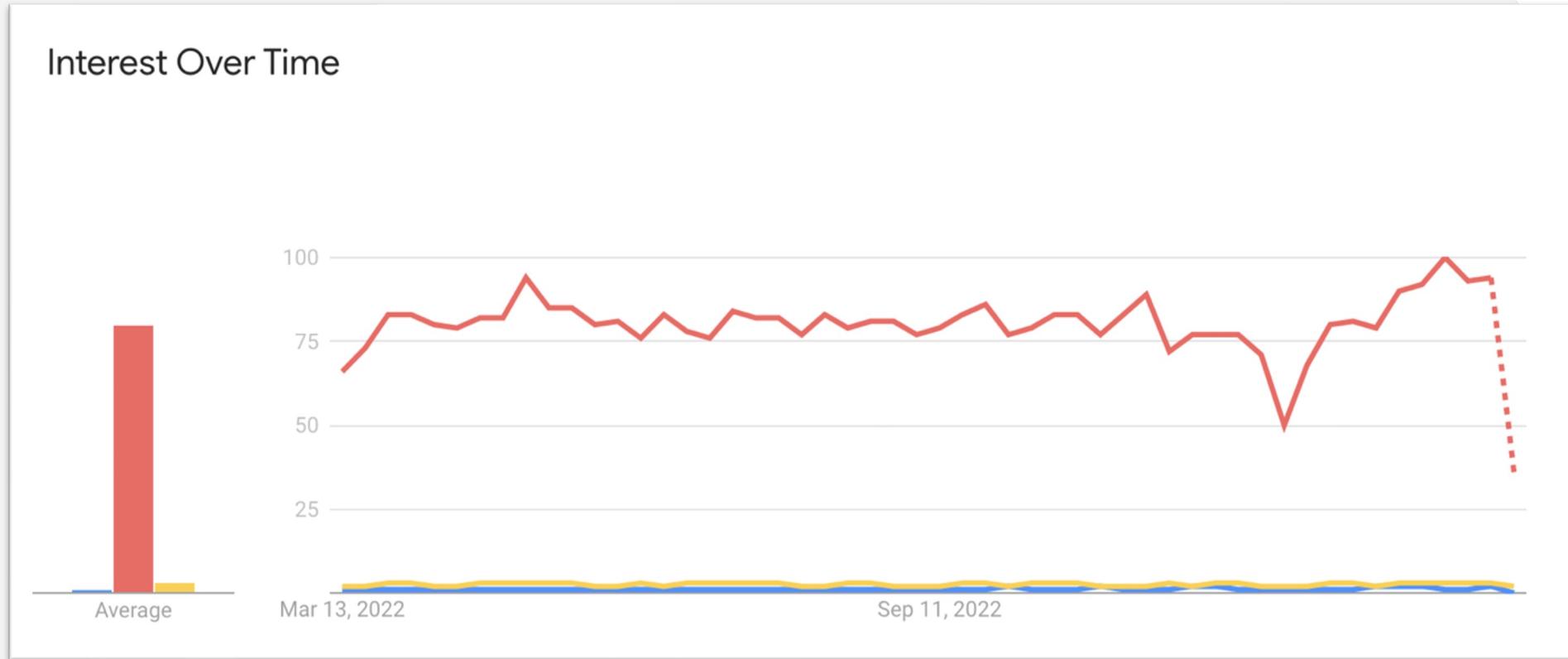
# Community - stackoverflow



# Community - Google Search Trends

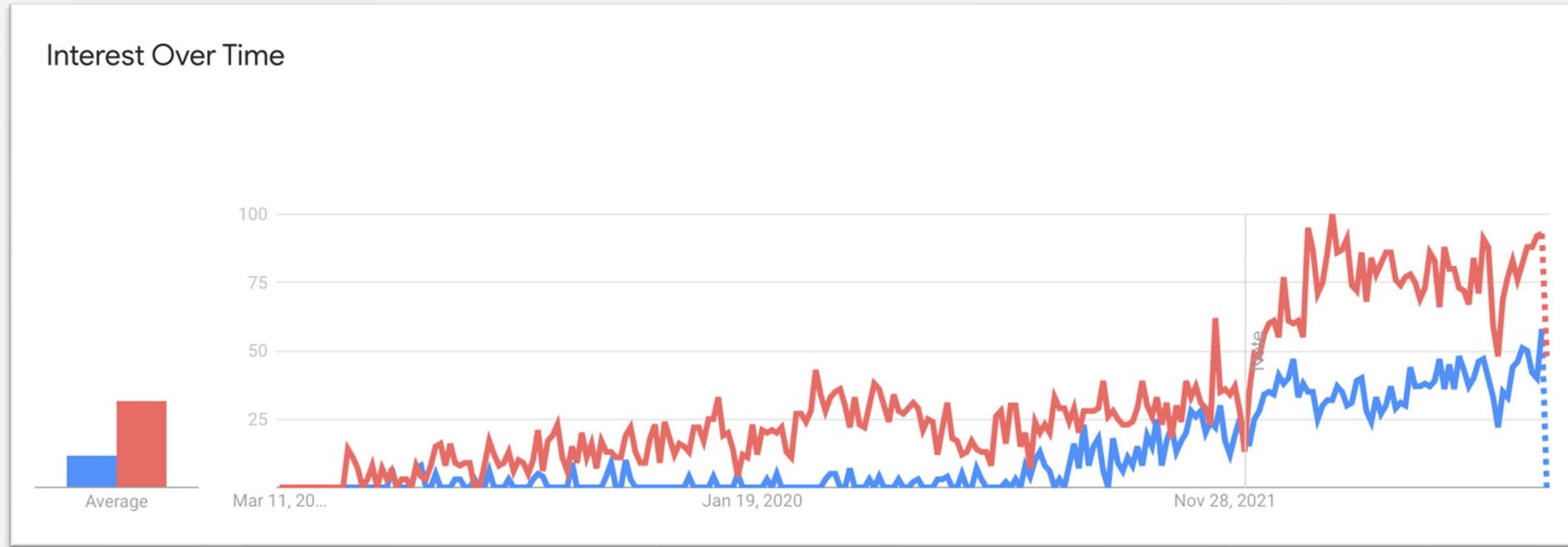
Searched for: terraform, azure bicep and Pulumi, last year

Interest Over Time



# Community - Google Search Trends

Searched for: azure bicep and Pulumi, last 5 years



# So, what is the best tool?



|                         | Simplicity | +++ | ++  | +   |
|-------------------------|------------|-----|-----|-----|
| Power of DSL / Language | +          |     | ++  | +++ |
| Multi Cloud             | -          |     | ++  | +++ |
| Developer Experience    | +++        |     | +   | +++ |
| Deployment              | ++         |     | +++ | +++ |
| Providers               | -          |     | ++  | +++ |
| Community               | ++         |     | +++ | +   |
| Ecosystem               | ++         |     | +++ | +   |
| Build your own workflow | +          |     | +   | +++ |

# Thanks!

**Erwin Staal**

@erwin\_staal



<https://www.erwinstaal.nl>

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

<https://www.github.com/staal-it>

