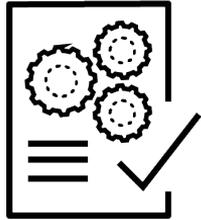


Scaling Security in a Cloud Native World

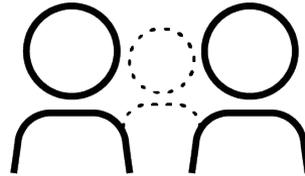
JUNE 2022
DAVID MACLEAN

Implementing DevSecOps

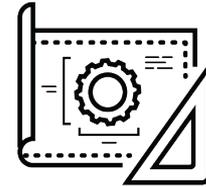
Large Financial Services Organisation - United Kingdom



Improve “Release Fitness”
Build the artifact once

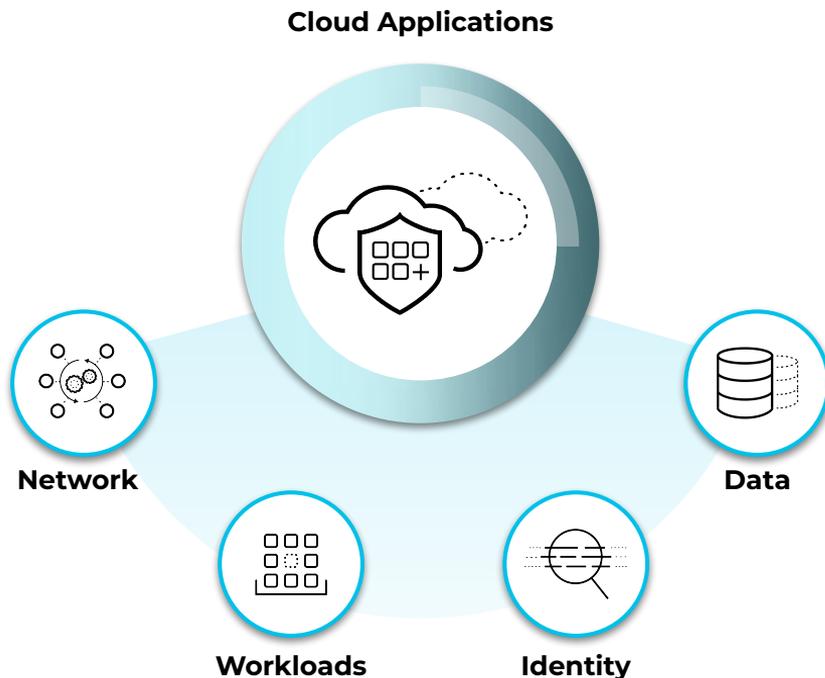


Improve Developer Experience
Deploy with speed and confidence



Align Security to the App Lifecycle
Security as Policies and Code

Cloud Applications are at the heart of Digital Transformation



The Cloud Application Environment

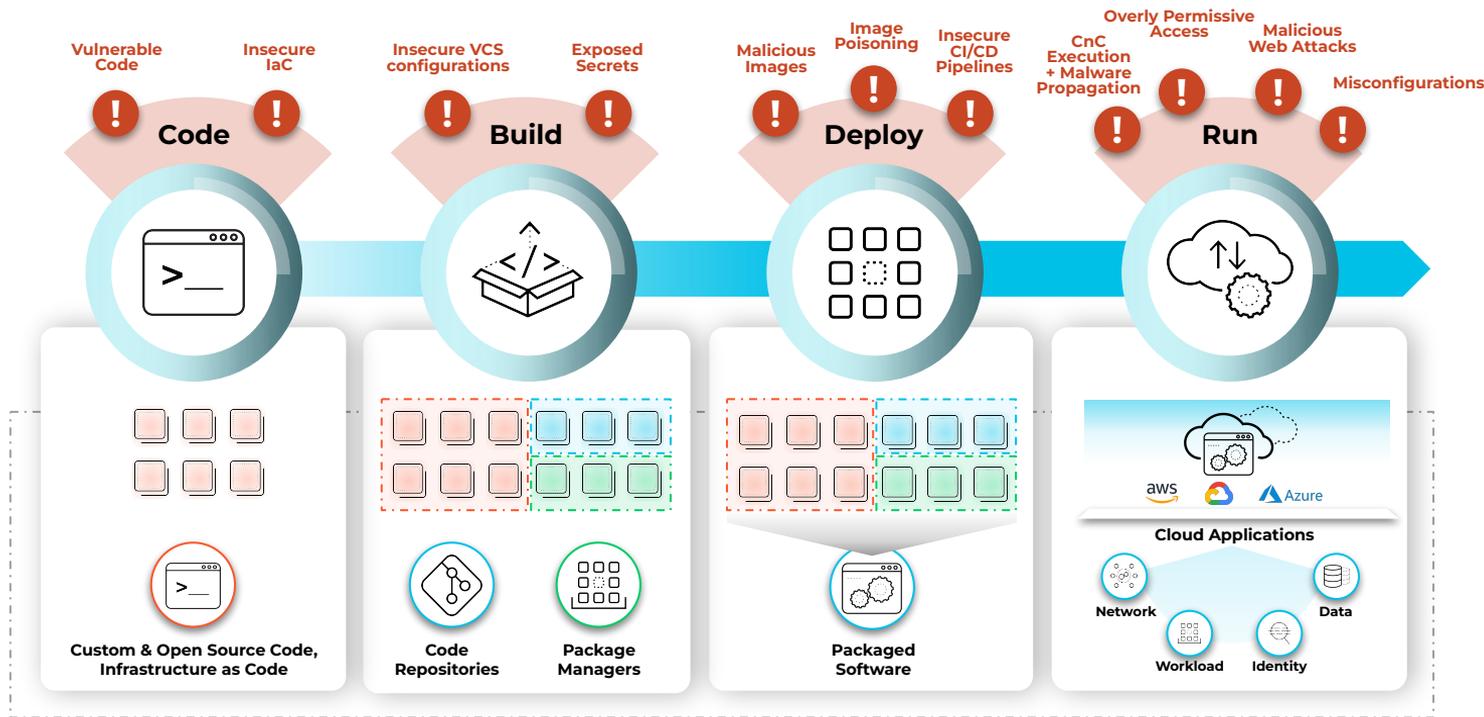
- Elastic Networks
- Dynamic Workloads - Host, Container, Serverless
- Complex Identities
- Growing Data Stores

Benefits

- Scale up or down fast
- Self-service, operational efficiency
- Better resource utilization

Cloud Native Application Risks and Threats

At Every Stage Of Cloud Applications



100 : 10 : 1



CHALLENGE

Runtime Security on its own does not Scale

100/10/1



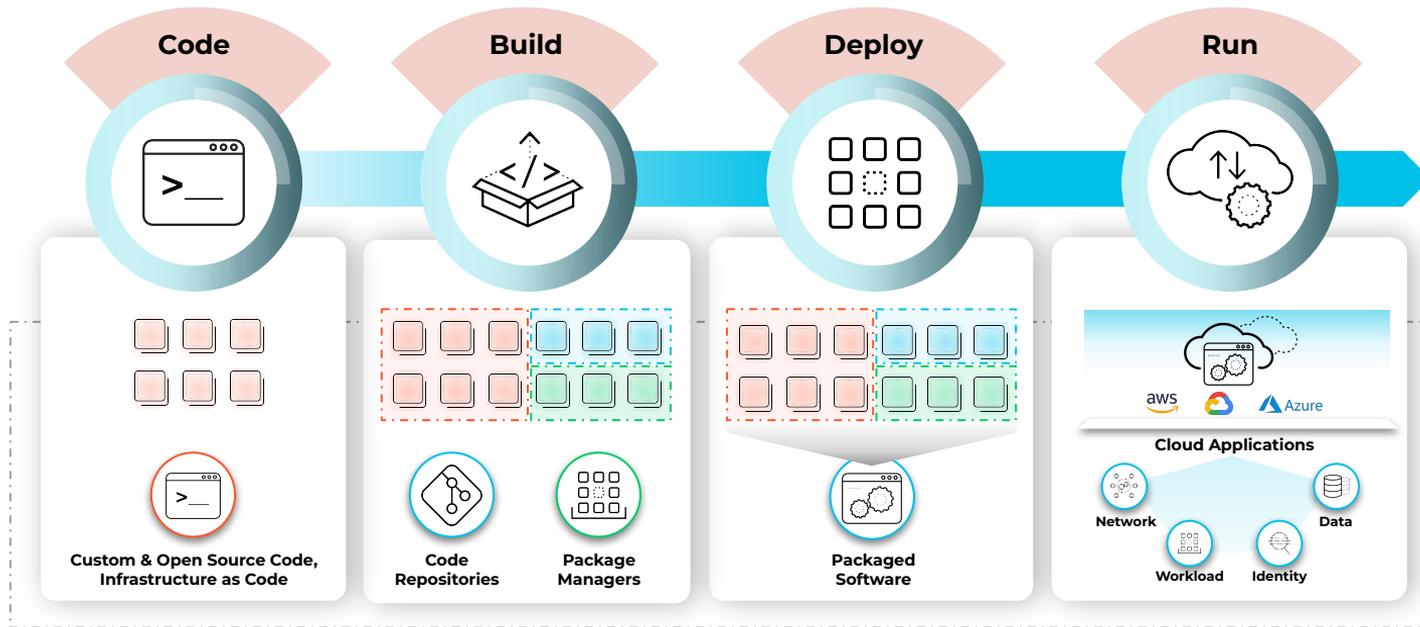
100 x
Developers



10 x DevOps +
QE Engineers



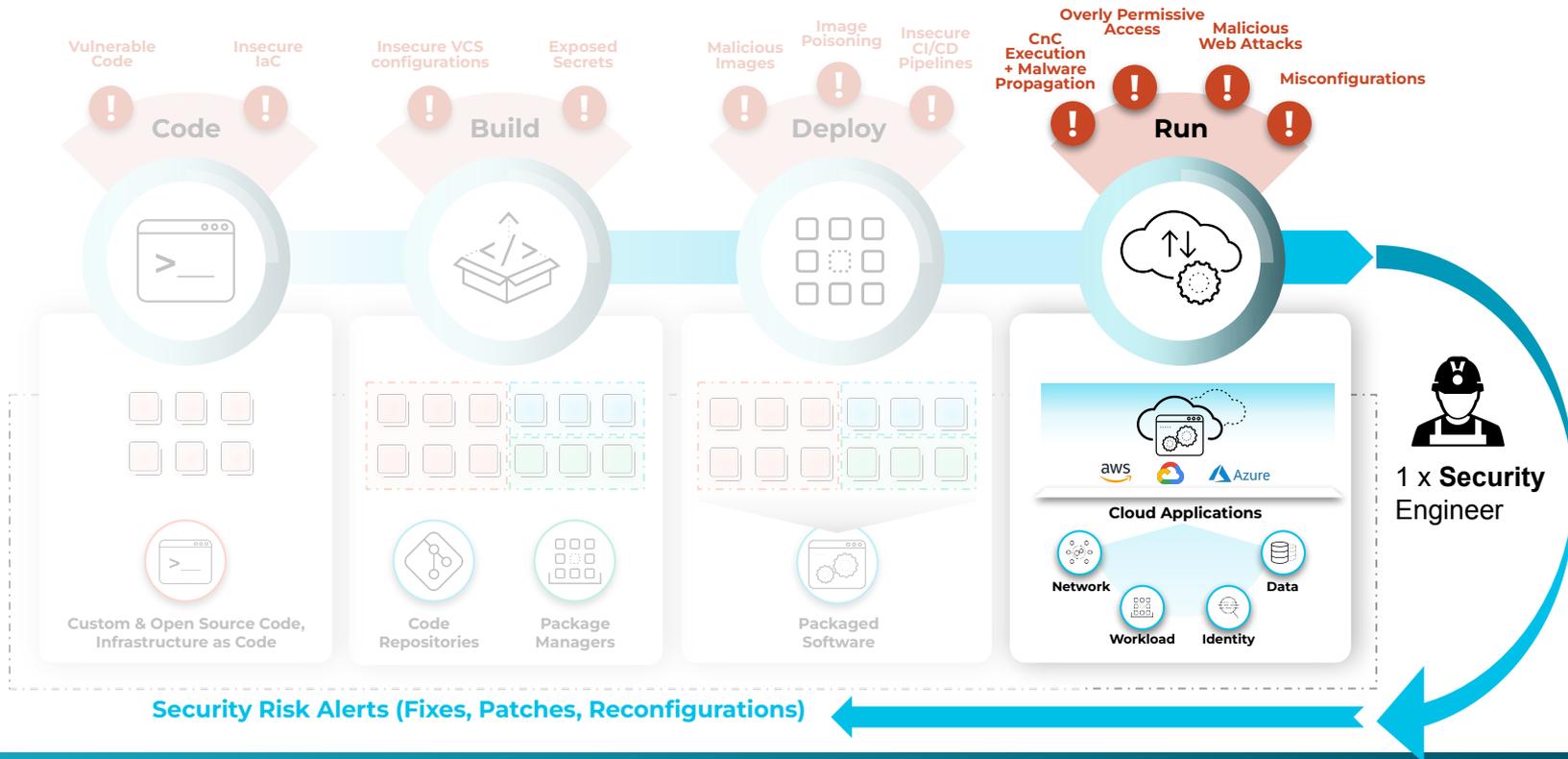
1 x Security
Engineer



Generation 1.0 Cloud Security

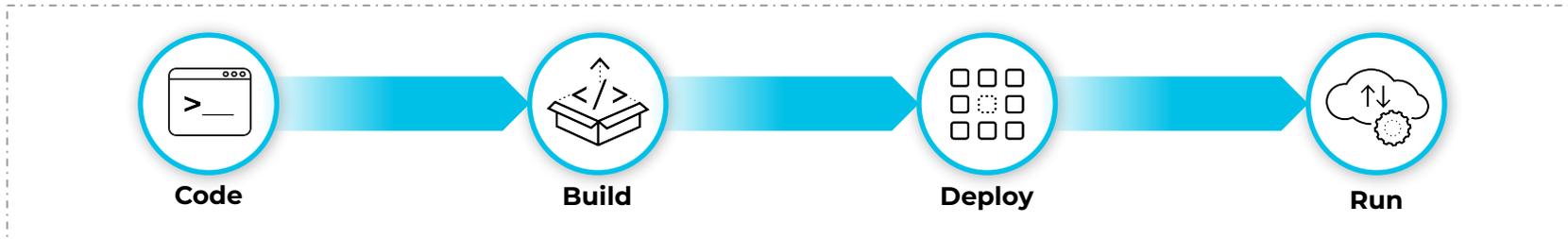
Only in the Runtime Environment

ALL Visibility and Enforcement is here



Prevention-First “Shift Left” Approach

Prevent Misconfigurations in Code and Vulnerabilities in Dependencies



PREVENTION FIRST

Prevent IaC misconfigs & Open Source vulnerabilities

Prevent Code Repo Vulnerabilities

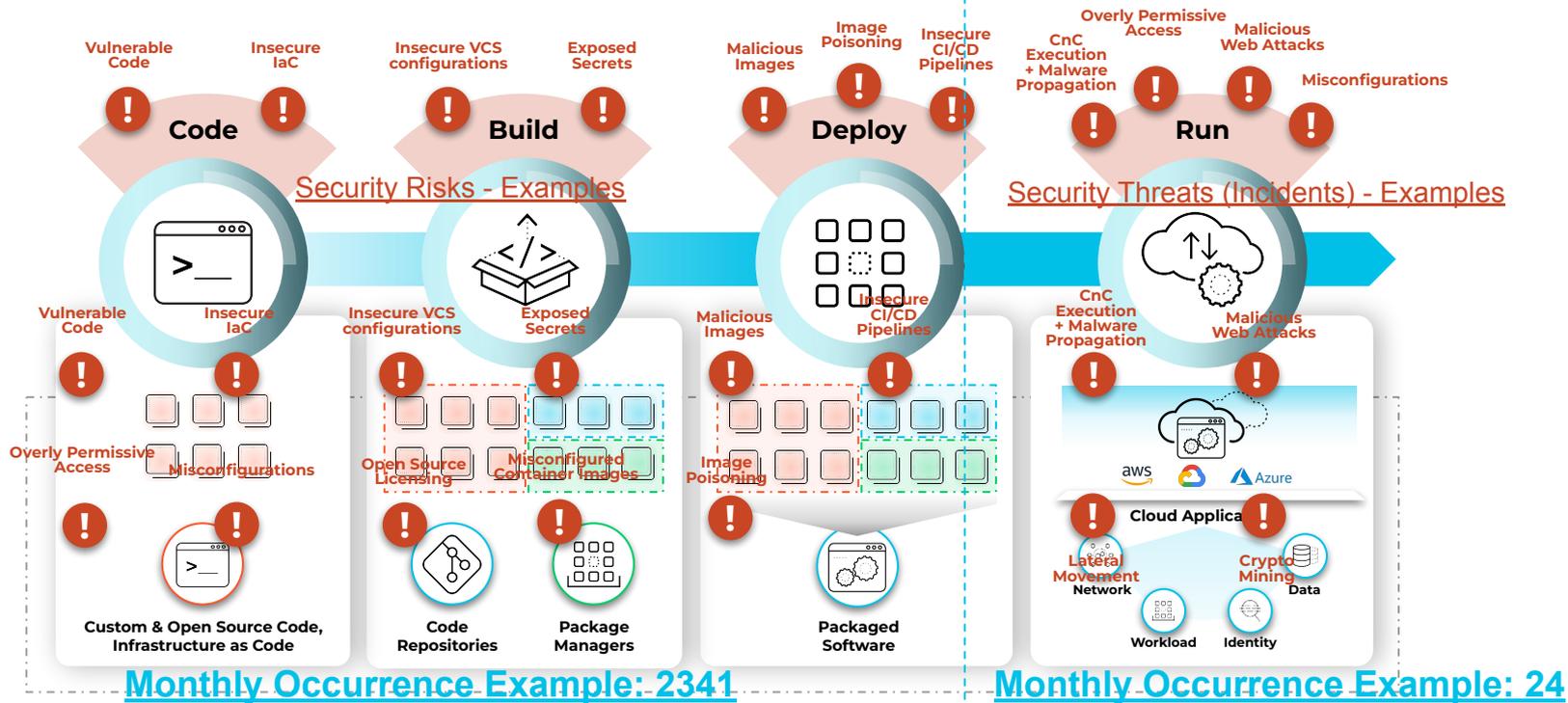
Prevent Vulnerable Images

Prevent Application Exploitations

Focus on Preventing Threats Across the Cloud App Lifecycle

Cloud Native Application Risks Vs Threats

99% Can "Shift Left"



Can Security Threats “Shift Left”?

Some of the 1% Threats can be reviewed within the Code, Build and Deploy Phases

The screenshot displays the Palo Alto Networks Cloud Platform interface, divided into several sections:

- Monitor / Runtime:** Shows incident explorer, container models, host observations, app-embedded observations, and image analysis sandbox.
- Image analysis sandbox:** Displays details for 'sandbox/test:1', including image ID, OS distribution (Ubuntu 14.04.6 LTS), and analysis summary (Time: Aug 10, 2021 10:11:05, Duration: 1s, Verdict: Suspicious findings).
- Suspicious findings (10):** Lists findings such as Crypto miner, Dropper, Kernel Module, Modified Binary, and Fileless Execution.
- Container behaviour:** Shows a table of network connections with IP addresses, ports, and countries. A map on the right visualizes outbound connections to various countries, with a legend listing countries like Antigua and Barbuda, Barbados, and Saint Lucia.

IP Address	Port	Country	Connection Type
5.43.64.0			Connection
23.236.0.0			Connection
Port	80	Barbados	
5.182.185.0			Connection
2.17.107.0			Connection
41.78.48.0			Connection
2.20.45.0			Connection
3.5.44.0			Connection

Outbound connections to various countries:

- Antigua and Barbuda (1)
- Barbados (1)
- Dominica (1)
- Dominican Republic (1)
- Saint Lucia (1)
- Puerto Rico (1)
- Trinidad and Tobago (1)
- Guyana (1)
- Venezuela (1)
- Suriname (1)

Cloud Security 1.0

Protection Focused on Runtime

Remediation only at runtime is costly

Visibility Without Prevention

Visibility alone is not Security

Lazy scans lead to Blind Spots

In cloud, attackers can find and exploit vulnerabilities in as little as 30 minutes

Incomplete Security Across Architectures

Enterprises adopt cloud in different ways, and need flexibility securing their journeys

Lack of Scale

Point solutions simply do not scale

The Future of Securing Cloud Applications

Leverage a comprehensive **CNAPP (Cloud Native Application Protection Platform)**

Cloud Security 1.0 Approach

Protection Focused on Runtime

Visibility Without Prevention

Lazy scans lead to Blind Spots

Incomplete Security Across Architectures

Lack of Scalability

CNAPP - Cloud Native Application Protection Platform

Comprehensive Security from Code to Cloud

Prevention-First Approach

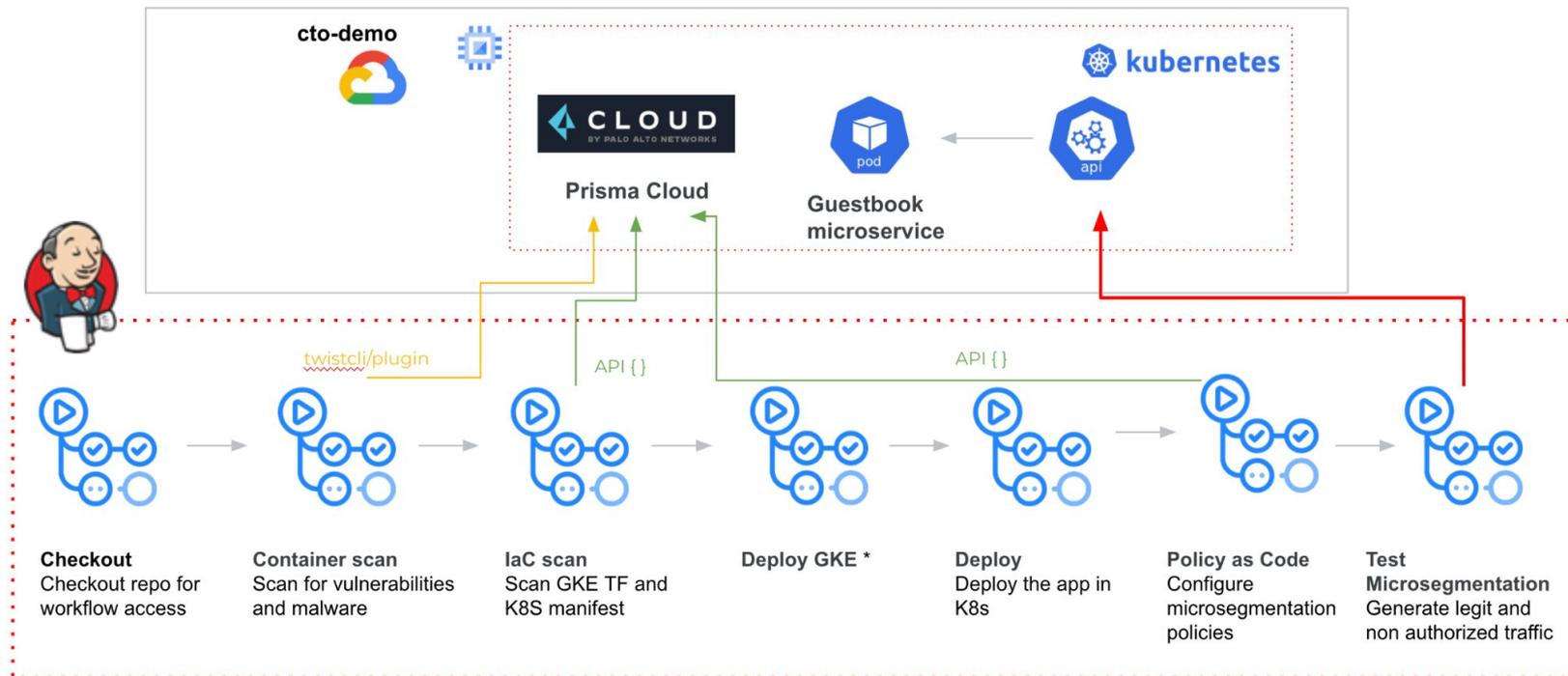
Continuous, Real Time Visibility

Security Choice For Every Cloud Journey

Cloud Scale Security

Adding to CNAPP after “Shifting Left”...

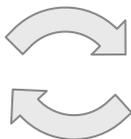
Policies-As-Code



Adding to CNAPP after “Shifting Left”...

Drift Detection and Response

```
dmaclean@M-1 ~ % aws s3api  
put-object-acl --bucket  
tf-test-bucket --key examplekey  
--acl public-read
```



```
resource "aws_s3_bucket" "source" {  
  provider = aws.central  
  bucket   = "tf-test-bucket"  
  acl      = "private"
```

The screenshot shows the Prisma Cloud interface for a project named 'achiar99/prisma'. A drift detection alert is visible for the resource 's3.tf:aws_s3_bucket.sample_bucket_achia_prisma (aws_s3_bucket)'. The alert message states: 'Drift detected on AWS resource `arn:aws:s3::sample-bucket-achia-prisma`'. Below the alert, the Terraform configuration for the bucket is shown, highlighting the differences between the current state and the expected state. The current state shows the bucket is not encrypted and has a private ACL, while the expected state shows it should be encrypted and have a public-read ACL. The resource history on the right side of the console shows several events, including 'Drift Detected' on May 10, 2022, and 'Compliant' status for various checks.

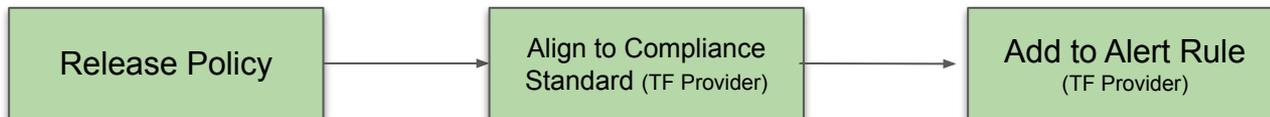
Adding to CNAPP after “Shifting Left”...

Automate Policy Testing and Implementation

Policy Testing Pipeline



Publishing Pipeline



GitOps delivered Security Policy Authoring

THANK YOU