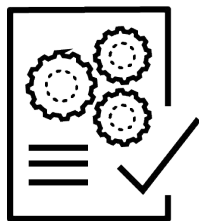


Scaling Security in a Cloud Native World

JUNE 2022
DAVID MACLEAN

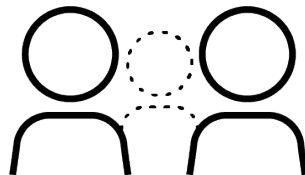
Implementing DevSecOps

Large Financial Services Organisation - United Kingdom

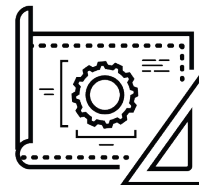


Improve “Release Fitness”

Build the artifact once

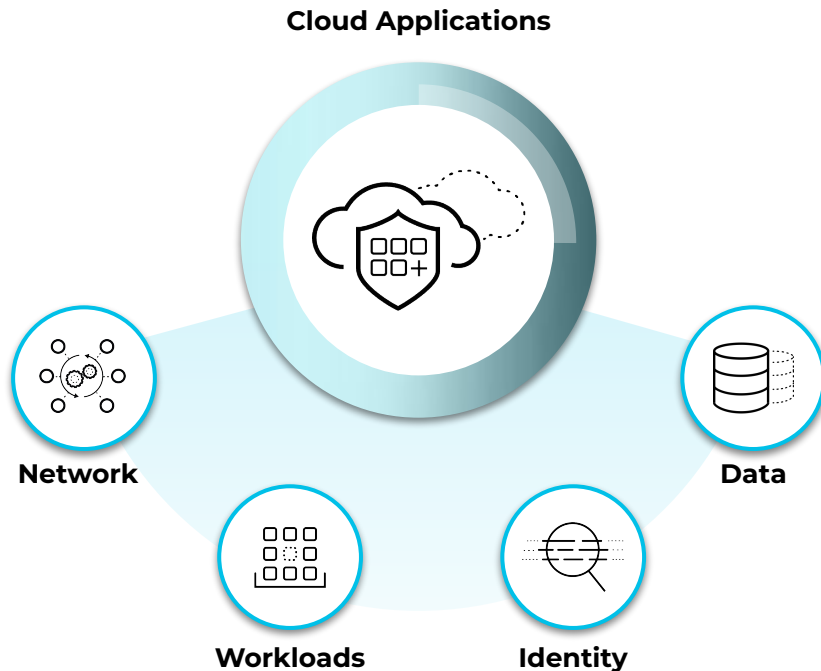


Improve Developer Experience
Deploy with speed and confidence



Align Security to the App Lifecycle
Security as Policies and Code

Cloud Applications are at the heart of Digital Transformation



The Cloud Application Environment

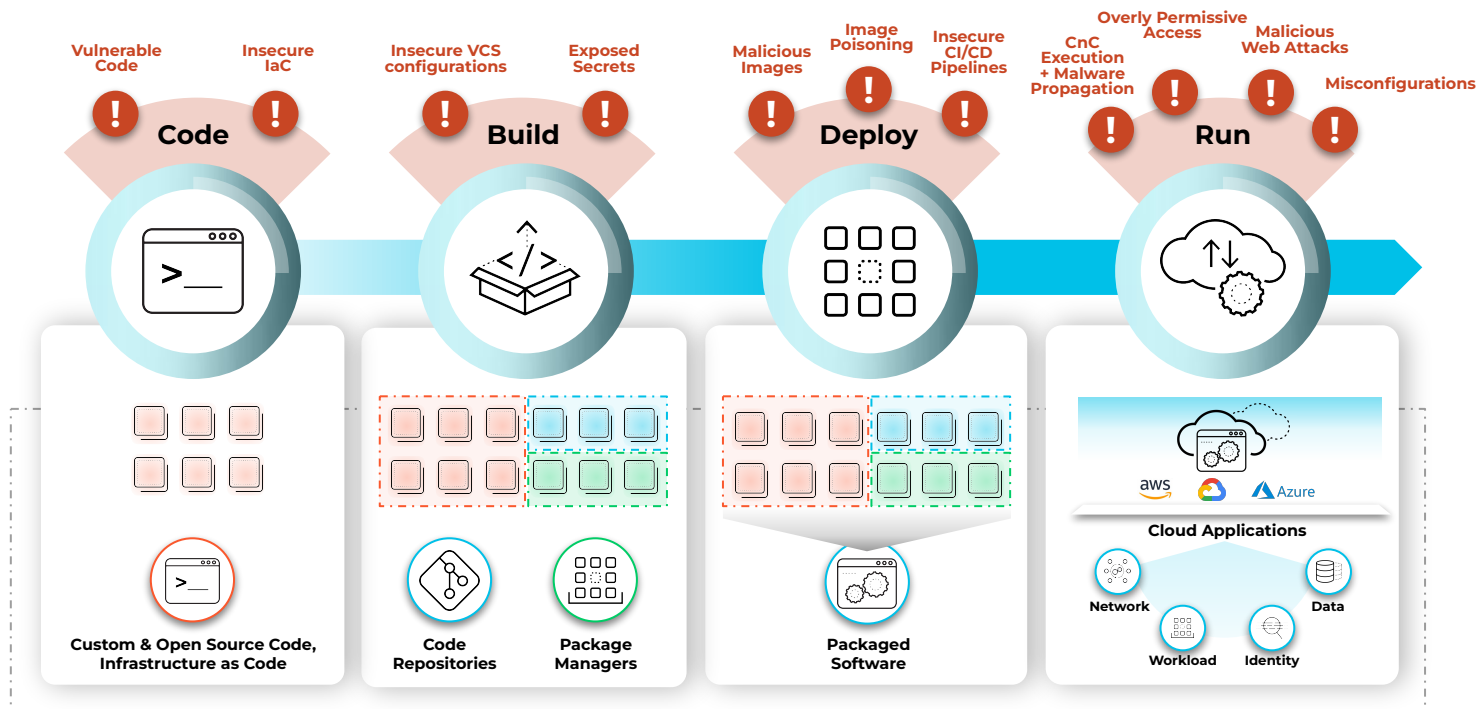
- Elastic Networks
- Dynamic Workloads - Host, Container, Serverless
- Complex Identities
- Growing Data Stores

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



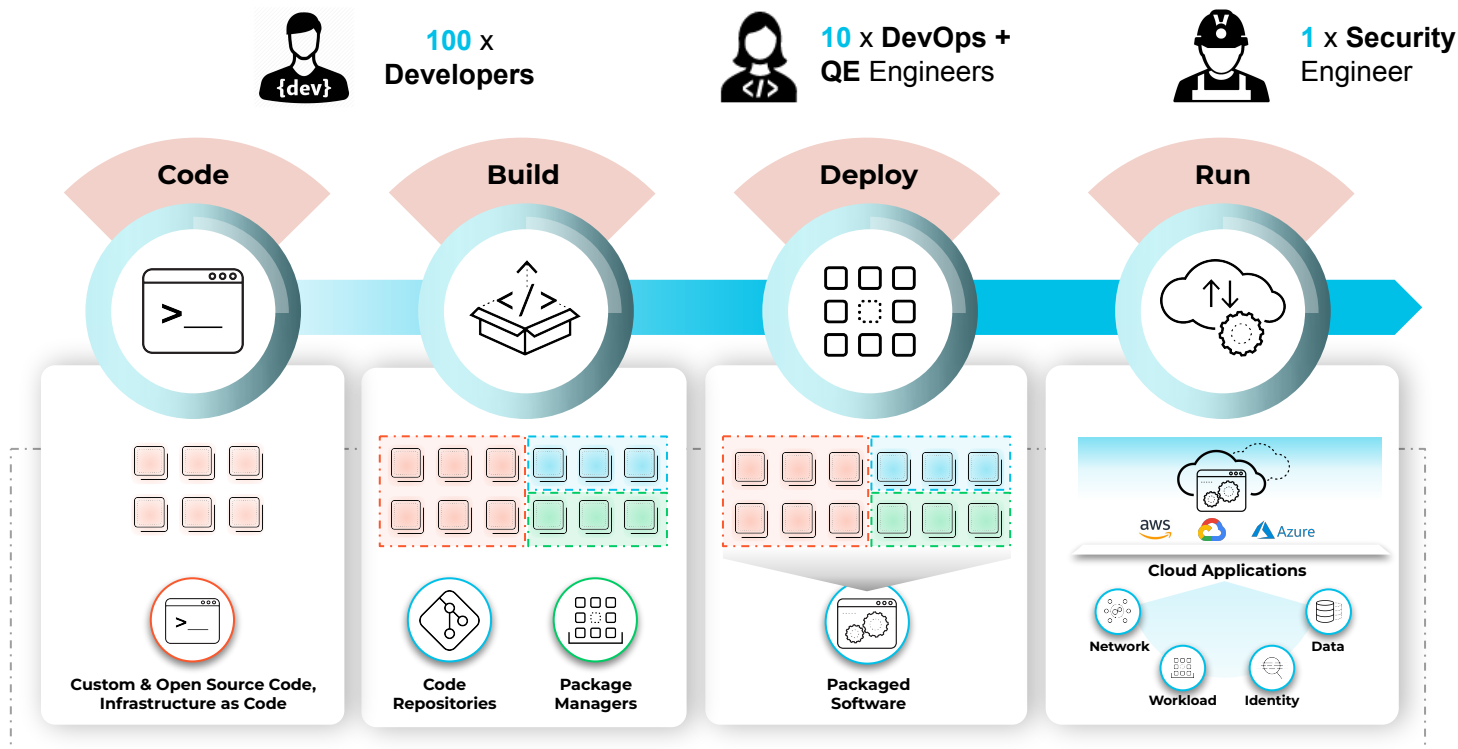
100 : 10 : 1



CHALLENGE

Runtime Security on its own does not Scale

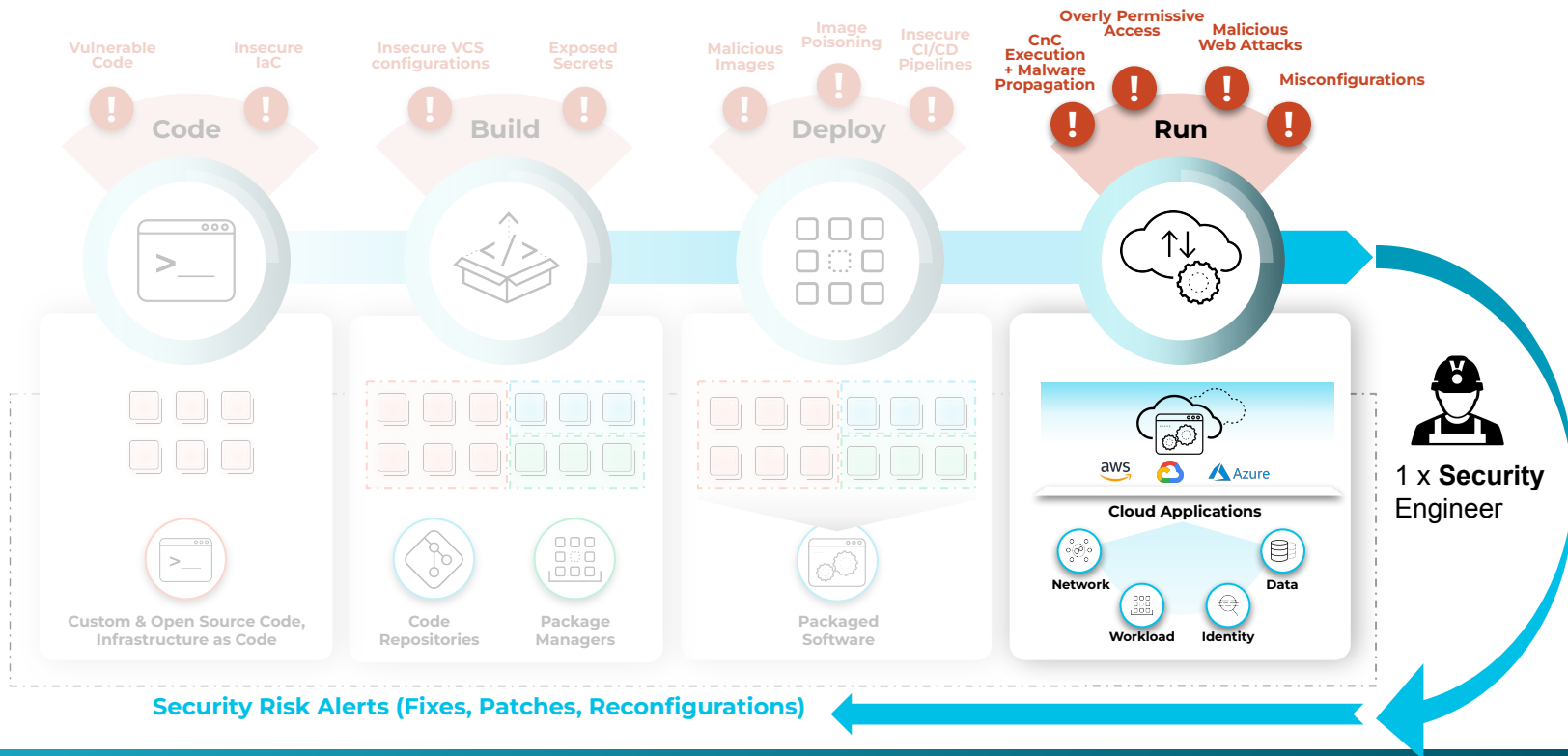
100/10/1



Generation 1.0 Cloud Security

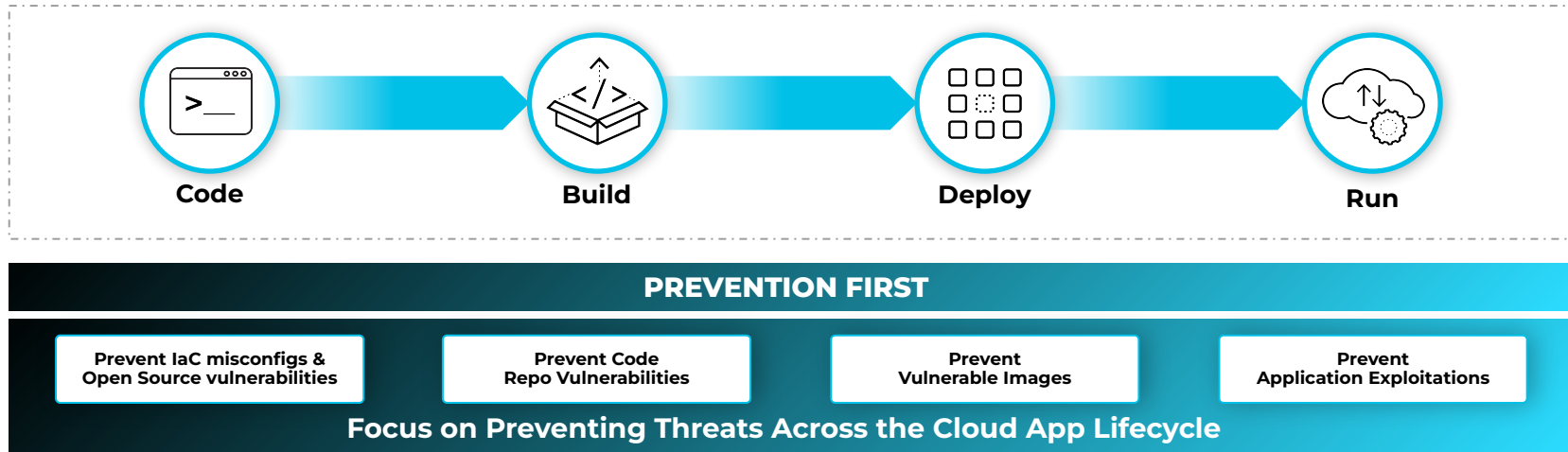
Only in the Runtime Environment

ALL Visibility and Enforcement is here



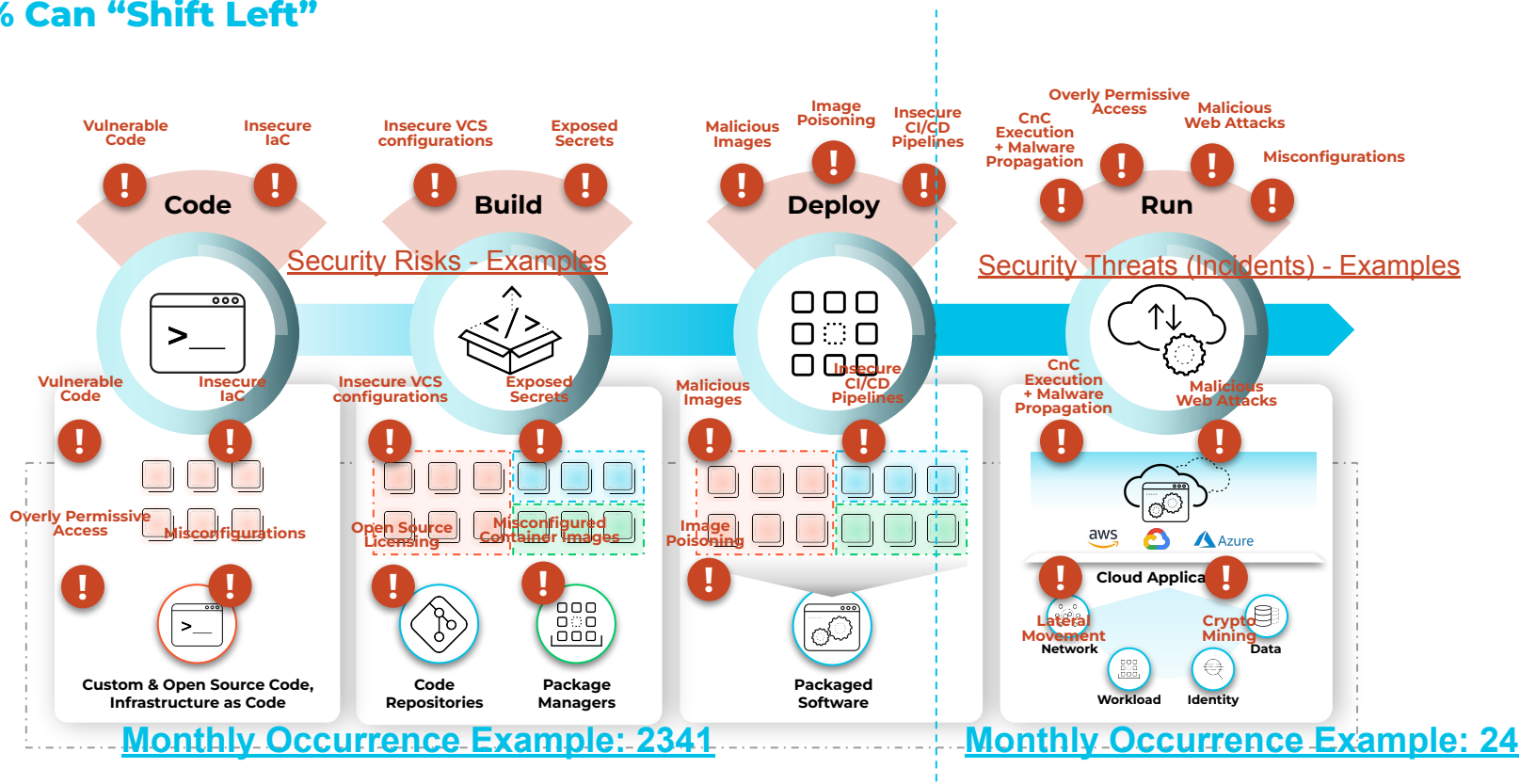
Prevention-First “Shift Left” Approach

Prevent Misconfigurations in Code and Vulnerabilities in Dependencies



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 Native Environment (CNE) interface, which is divided into several sections for monitoring and analyzing container security.

Left Sidebar: Contains navigation options: Radars, Defend, Monitor, ATT&CK, Events, Runtime (selected), Vulnerabilities, Compliance, WAAS, and Manage.

Top Bar: Shows the current view as 'Monitor / Runtime' and includes tabs for Incident explorer, Container models, Host observations, App-Embedded observations, and Image analysis sandbox (selected).

Image analysis sandbox: Displays details for a specific image, 'sandbox/test:1'. It includes fields for Image ID, OS distribution (Ubuntu 14.04.6 LTS), and an entrypoint (/bin/entrypoint.sh). The analysis summary shows a verdict of 'Highest severity' and 'Suspicious findings'.

Suspicious findings (10): A list of detected threats, including Crypto miner, Dropper, Kernel Module, Modified Binary, and Fileless Execution. An 'Expand (5 more)' link is available.

Container behaviour: A section showing network activity. It includes a filter bar with 'Filter by keywords and attributes' and a 'View by: Type Time' dropdown. The main table lists network connections with columns for IP address, port, and country. The 'Outbound c' section shows a map of the world with numbered locations, indicating the source of the connections.

Table Data:

IP Address	Port	Country	Connection
5.43.64.0			Connection
23.236.0.0			Connection
Port	80		
Country	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 c: A map showing the distribution of connections across various countries, including Antigua and Barbuda, Barbados, Dominica, Dominican Republic, Saint Lucia, Puerto Rico, Trinidad and Tobago, Guyana, Venezuela, and Suriname.

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

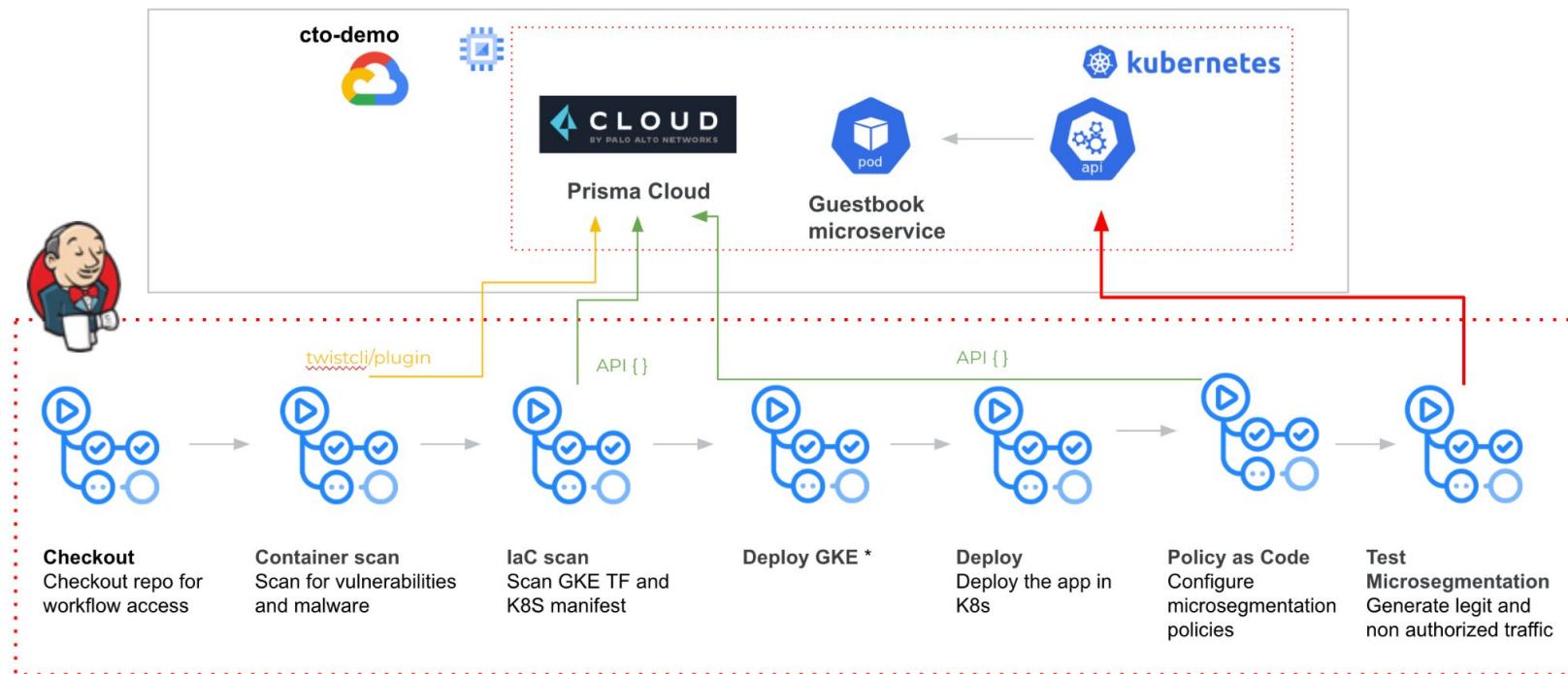
Continuous, Real Time Visibility

Security Choice For Every Cloud Journey

Cloud Scale Security

Adding to CNAPP after “Shifting Left”...

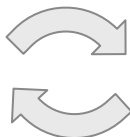
Policies-As-Code



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 Palo Alto Prisma Cloud console interface. On the left, a sidebar contains navigation icons. The main area displays a drift detection alert 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, a comparison table shows the configuration differences between the current state and the desired state.

Current State	Desired State
<pre>resource "aws_s3_bucket" "sample_bucket_achia_prisma" { # bucket is not encrypted bucket = "sample-bucket-achia-prisma" - acl = "private" versioning { enabled = false } enabled = true git_repo = "terraform_samples" s3r_trace = "cd87bc48-5f9e-4187-a84e-9bb8e7ed9f8f" }</pre>	<pre>resource "aws_s3_bucket" "sample_bucket_achia_prisma" { # bucket is not encrypted bucket = "sample-bucket-achia-prisma" + versioning { enabled = true } git_repo = "terraform_samples" s3r_trace = "cd87bc48-5f9e-4187-a84e-9bb8e7ed9f8f" + grant { uri = "http://acs.amazonaws.com/groups/s3/LogDelivery" type = "Group" permissions = ["FULL_CONTROL"] } + grant { uri = "http://acs.amazonaws.com/groups/global/AllUsers" type = "Group" permissions = ["READ", "READ_ACP"] } + grant { uri = "http://acs.amazonaws.com/groups/global/AuthenticatedUsers" type = "Group" permissions = ["READ", "READ_ACP"] } }</pre>

On the right side of the console, a panel for the resource `s3.tf:aws_s3_bucket.sample_bucket.achia_prisma (aws_s3_bucket)` shows its configuration, including ACL (Private), Versioning (Enabled: True), and Force Destroy. Below this, a "Resource History" section lists several events, including "Drift Detected" on May 10, 2022, and "Error Detected" on May 8, 2022.

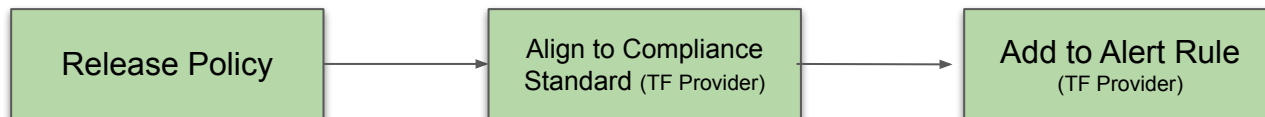
Adding to CNAPP after “Shifting Left”...

Automate Policy Testing and Implementation

Policy Testing Pipeline



Publishing Pipeline



GitOps delivered Security Policy Authoring

THANK YOU