commercetools
Next generation commerce

Shifting Left - Securing Infrastructure as Code

2022

Akshita Rastogi
Head Of Products - Infrastructure & Tooling

Agenda

01 Introduction

02 Security Now Vs Then

03 How Has IaC Changed the Game?

04 Self-Realization of the Water Level

05 What Does It Take To Build a Trust ~~Wall~~ Gateway

06 Q & A

Are you dealing with 1000s of Security Alerts?

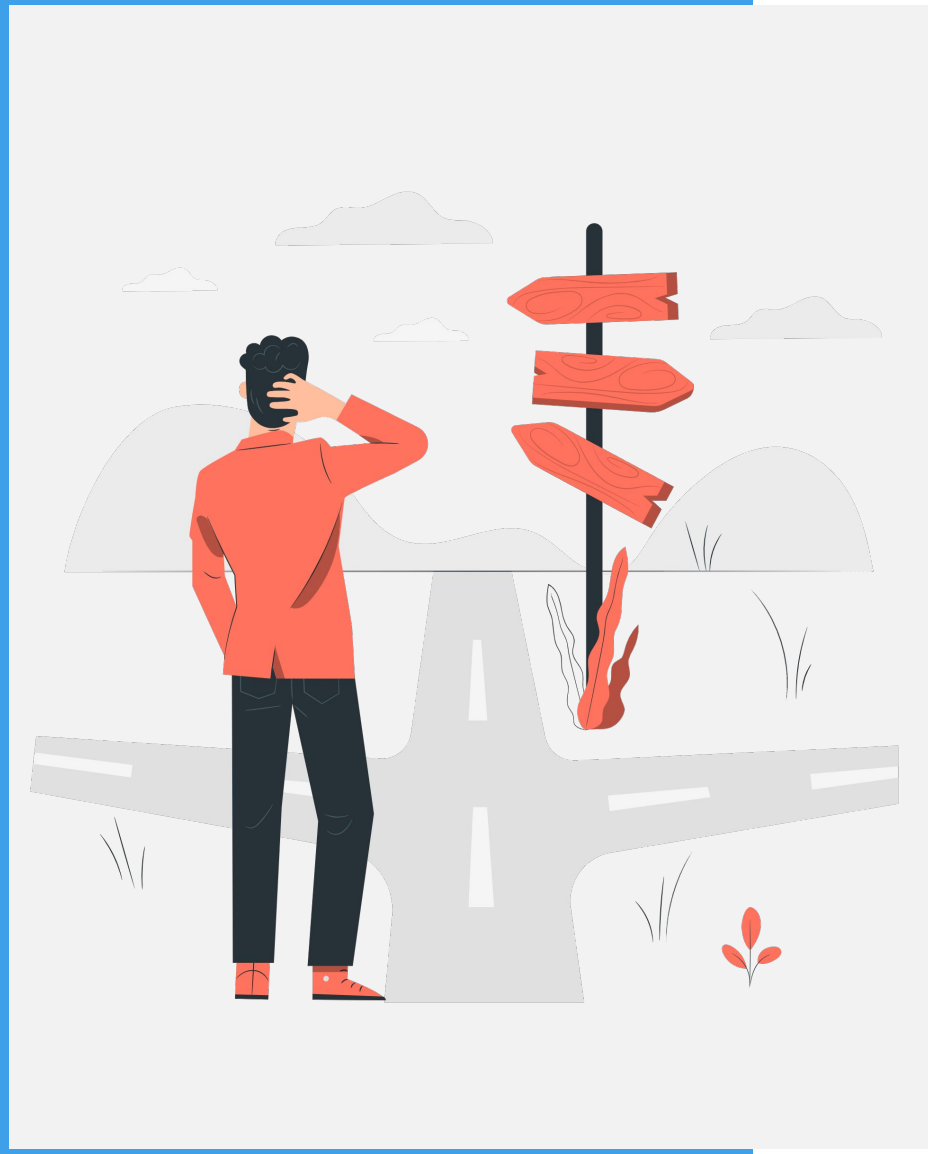
Does your manager keep pushing the delivery dates due to security concerns?

Are you tired of last-minute high-priority vulnerability fixes?

I have been at the receiving end of these problem statements and found myself tirelessly nodding yes every time they showed up

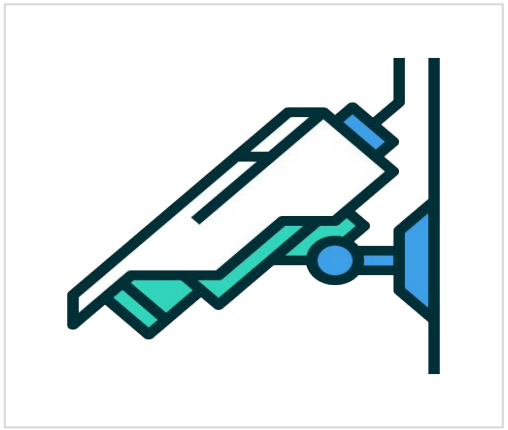
When presented with the opportunity to build a product line that could address them, a roller coaster ride-like experience began, full of ups and downs and a great sense of achievement at the end of it

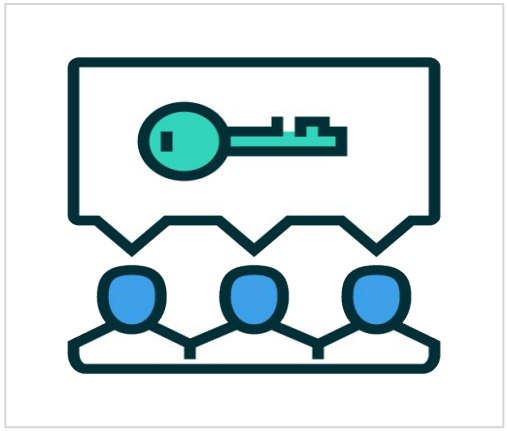
Hi! :) I'm Akshita, Head Of Product - Infrastructure & Tooling @commercetools



Security Then Vs Now

Left? Right?





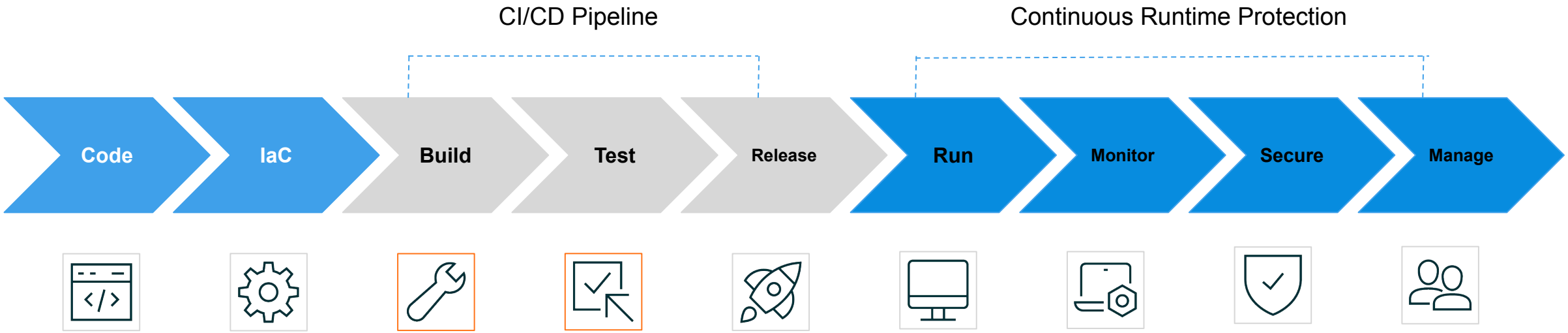
A while back, we used to have surveillance cameras to secure the infra. Then we had RFIDs, biometric, different modes of authentication and layers of authorisation.

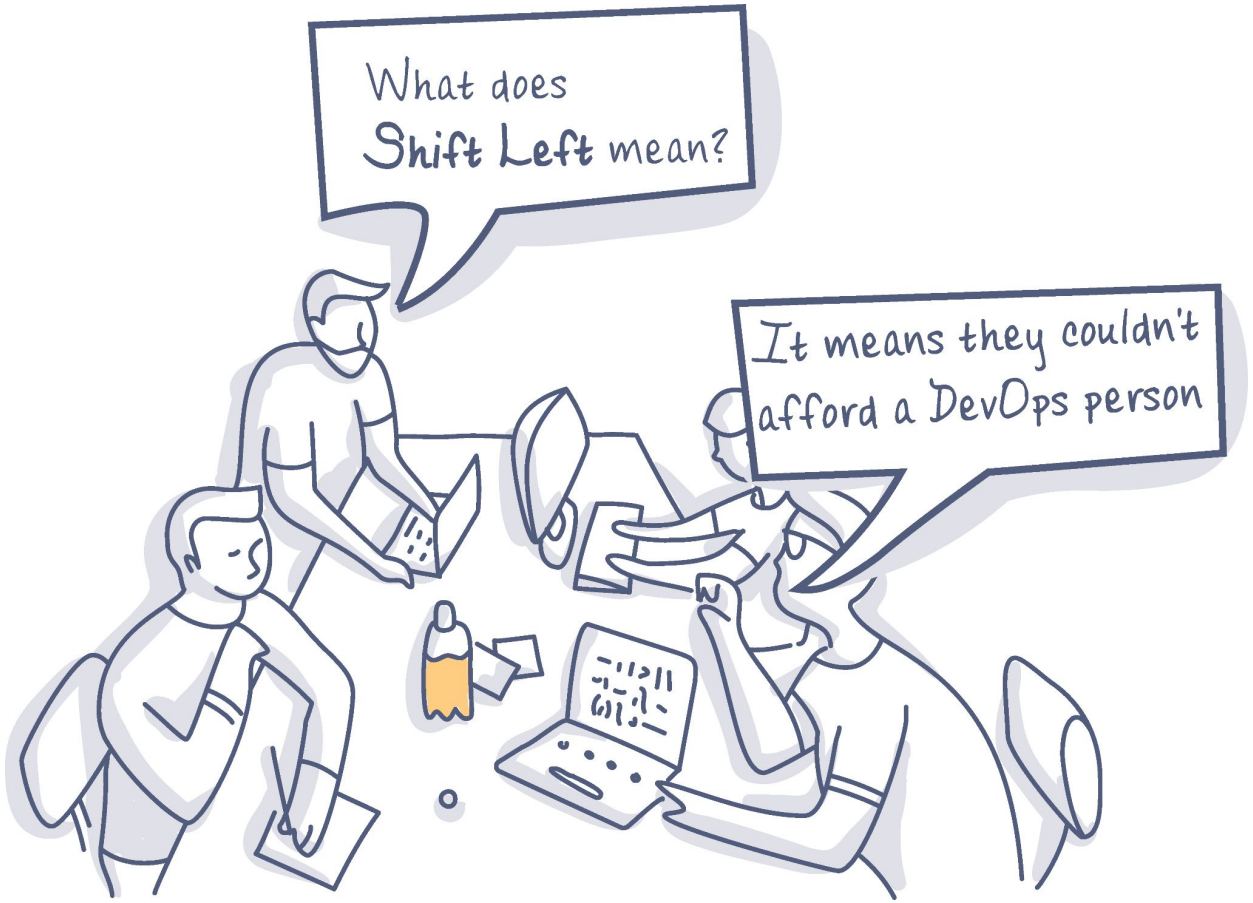
But as the security domain evolved so did the means to breach security, we did change with time and codified our infrastructure.
This meant IaC but security as code as well.

Now we aim to maintain and deploy our infrastructure as IaC and ensure it’s security as code.

We see issues getting translated through the levels of the software development cycle.

Imagine fixing something that could have been caught in layer 1 but got multiplied and enlarged through 9 layers of its life cycle.





A common myth regarding Shift Left is that Securing IaC is an alternative to a DevOps Engineer.

DevOps is a practice. Engineers that are engineering the IaC are not Security Experts.

Shifting Left has nothing to do with DevOps practices.

Even if you have a big DevOps enablement team with world-class highly skilled SREs, the risk of not securing your IaC increases exponentially .

Why Take a Step Back In The Security Cycle?

To reduce the Mean Time To Detect vulnerabilities

- Quickly identifying issues
- Early in the build life cycle
- To catch them in runtime

To facilitate the process if vulnerability prioritisation

- With 1000s of CSPM alerts, its helps to understand the impact.
- Helps in prioritising which one should get your attention first.

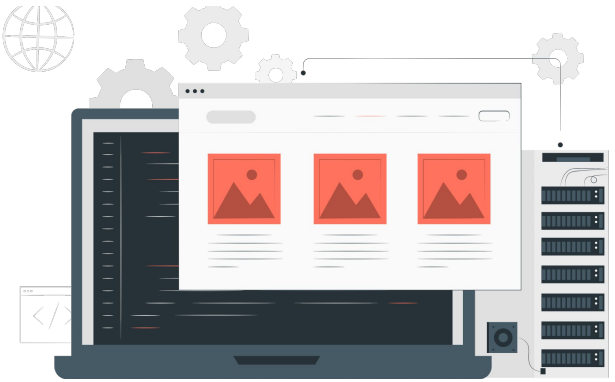
To enable the developers

- By helping them identify issues early in the SDLC process
- Earlier the better?

To integrate the security tools in order to automate vulnerability assessment

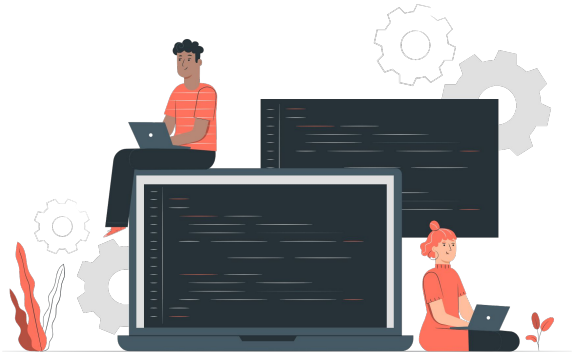
- This helps in preventing the vulnerabilities from being deployed to any environments.
- Automated assessment of IaC code.
- Reduced chances of human error and misconfigurations.

How Has IaC Changed the Game?

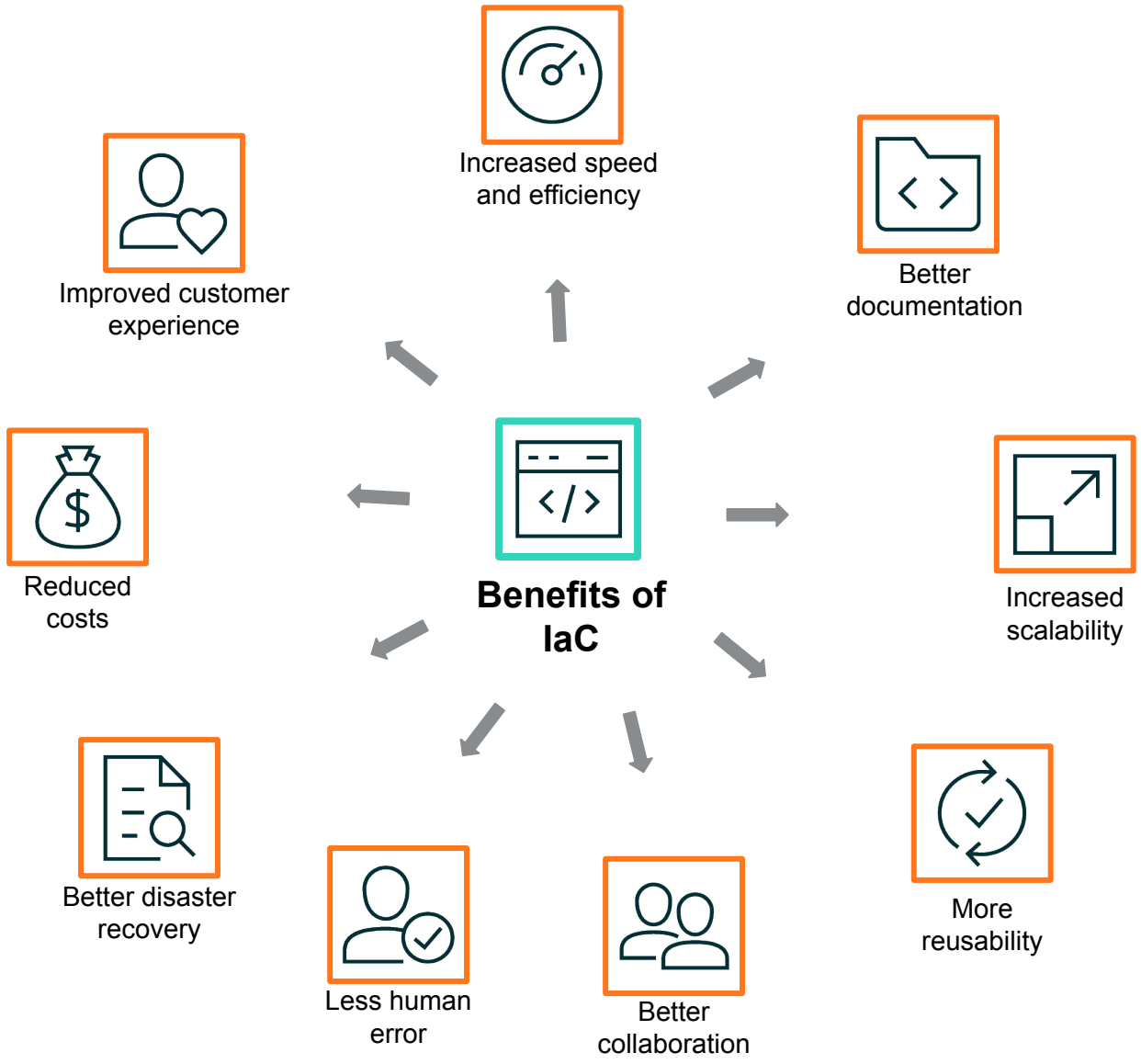


Applications need infrastructure in order to run. Infrastructure could be anything from servers to databases to networks, anything an application requires to function.

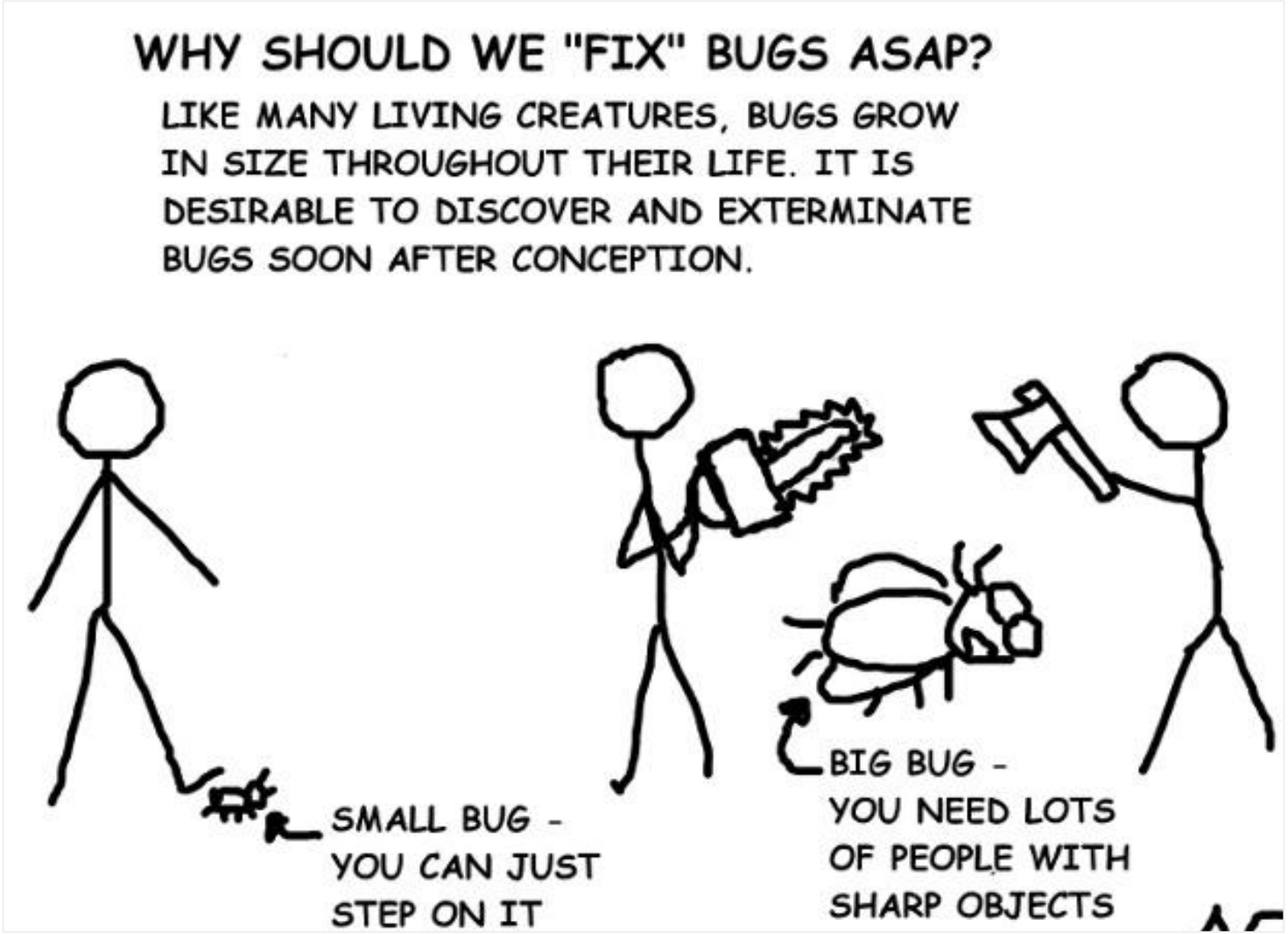
Previously, organizations would have infrastructure provisioned manually by engineers, thereby making the entire process cumbersome, complex, and prone to human errors. Even on cloud, it was done manually.

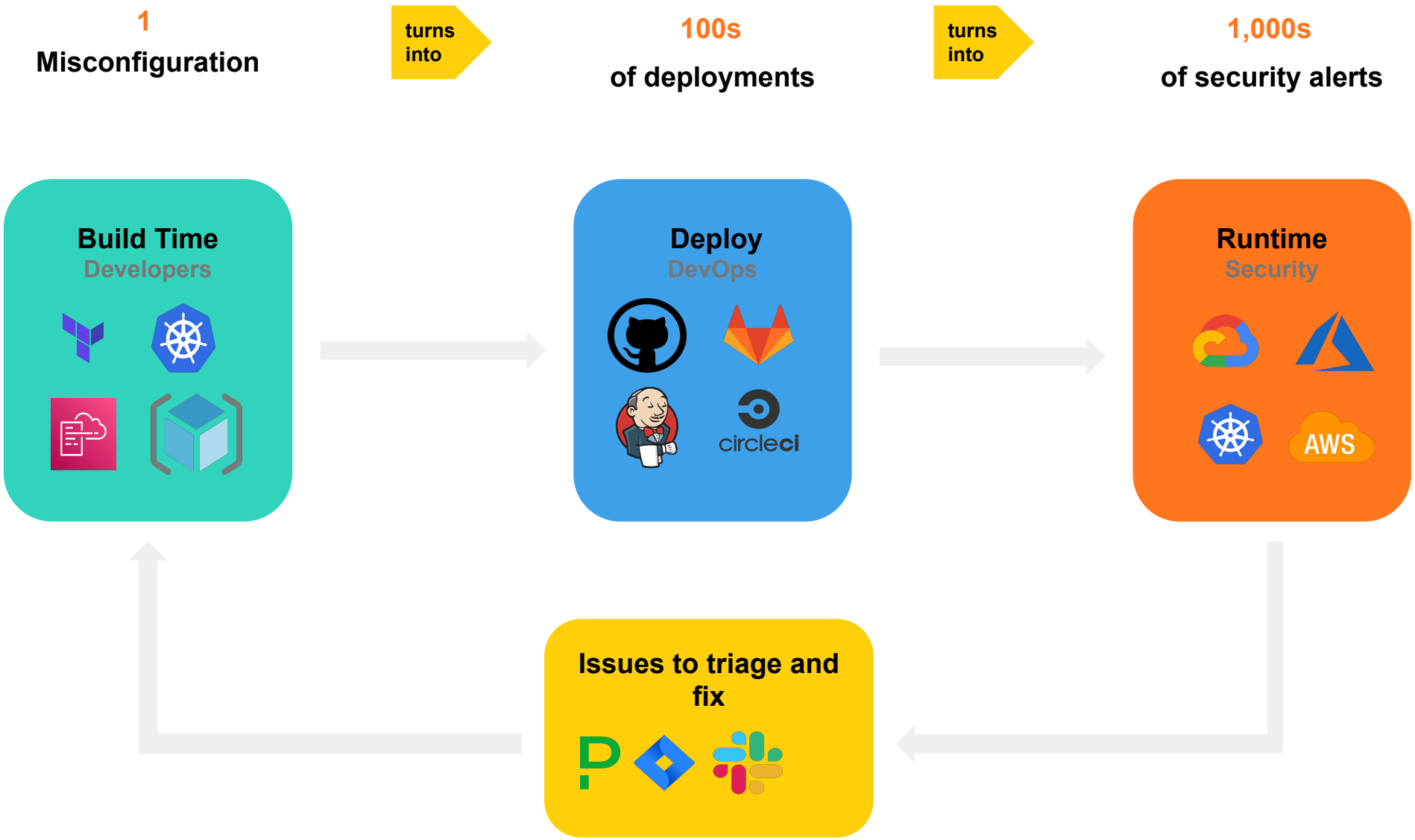


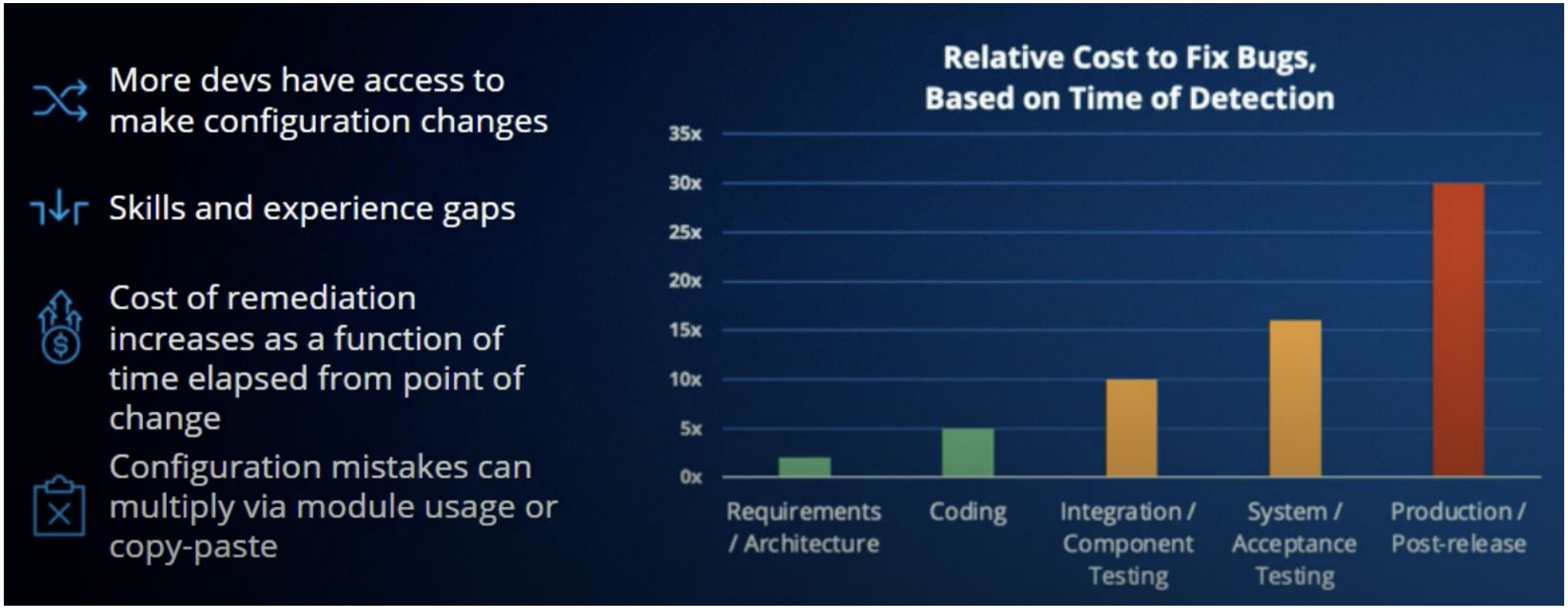
IaC is all about automating the provisioning of infrastructure through writing code and interacting with the APIs. This makes the infrastructure more scalable and automates the deployment & configuration.


Increased speed and efficiency
Better documentation
Increased scalability
More reusability
Better collaboration
Less human error
Better disaster recovery
Reduced costs
Improved customer experience
Benefits of IaC

Risks or Disadvantages of Using IaC?


WHY SHOULD WE "FIX" BUGS ASAP?
LIKE MANY LIVING CREATURES, BUGS GROW IN SIZE THROUGHOUT THEIR LIFE. IT IS DESIRABLE TO DISCOVER AND EXTERMINATE BUGS SOON AFTER CONCEPTION.
SMALL BUG - YOU CAN JUST STEP ON IT
BIG BUG - YOU NEED LOTS OF PEOPLE WITH SHARP OBJECTS

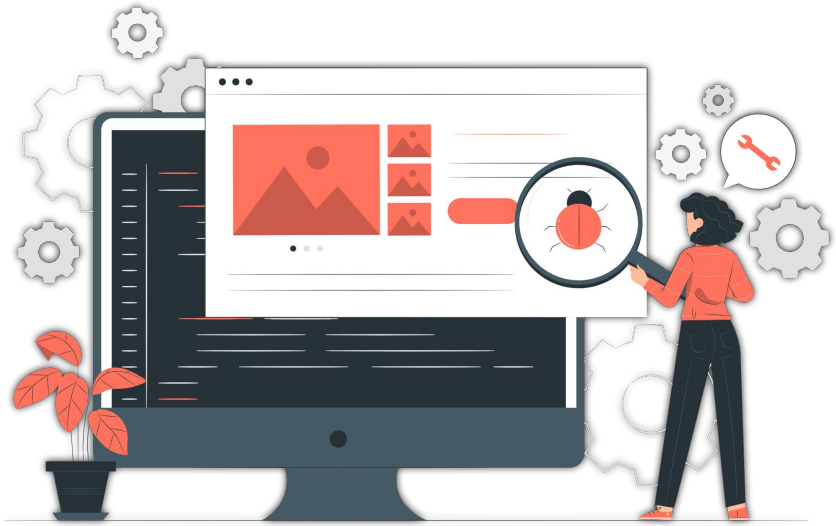

1
Misconfiguration
turns into
100s
of deployments
turns into
1,000s
of security alerts
Build Time
Developers
Deploy
DevOps
circleci
Runtime
Security
AWS
Issues to triage and fix

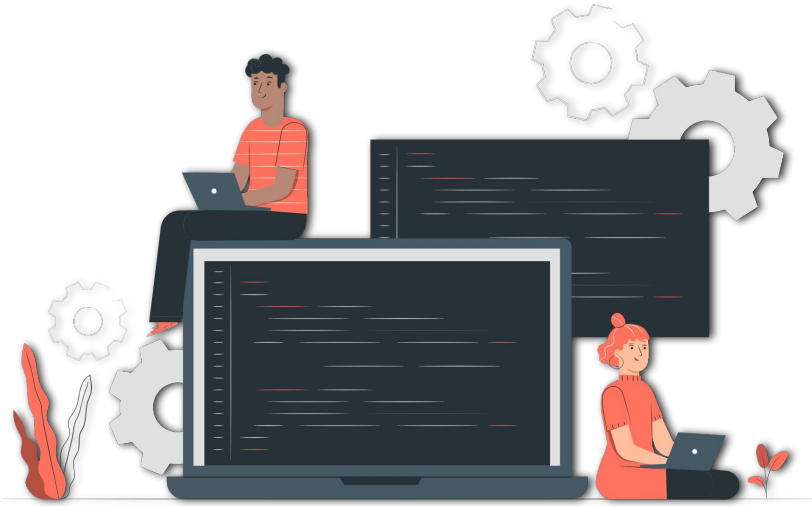

More devs have access to make configuration changes
Skills and experience gaps
Cost of remediation increases as a function of time elapsed from point of change
Configuration mistakes can multiply via module usage or copy-paste
Relative Cost to Fix Bugs, Based on Time of Detection
35x
30x
25x
20x
15x
10x
5x
0x
Requirements / Architecture
Coding
Integration / Component Testing
System / Acceptance Testing
Production / Post-release

source: NIST

Self-Realisation of the Water Level

What Could Possibly Go Wrong When Deploying Infrastructure using IaC?





While deploying infrastructure using IaC, any organization's main issue is reviewing the code.

Unfortunately for the industry, IaC is not secure by default. Reviewing someone else’s code is anyways a big task. Sometimes boring and time consuming.

GameSettings.cs × {} User Settings

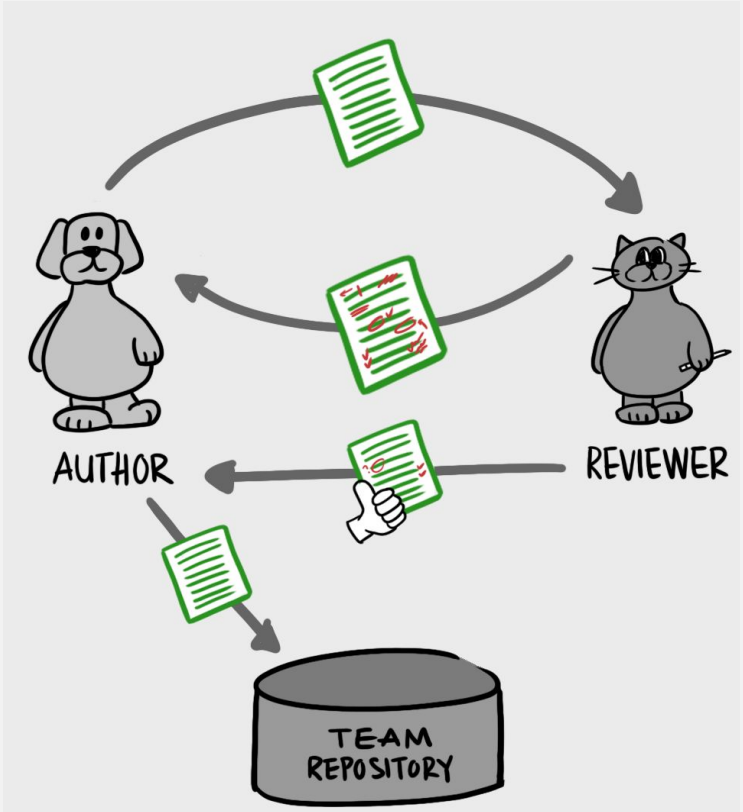
```
6   public class GameSettings : MonoBehaviour {
7       public static string gameMode = "none";
8       public static int numLives = 2545;
9       public static int scores = 4568;
10      public static int kills = 123456;
11      public static int allMoney = 123456;
12
13      //Comment 1
14      public static void ApplicationFocus(bool hasFocus){
15          if (hasFocus == false){
16              PlayerPrefsFile.Save ();
17          } else if (hasFocus){
18              PlayerPrefsFile.Save ();
19          }
20          if (hasFocus == false) {
21              PlayerPrefsFile.SetInt (GameSettings.gameMode + "_numOfLives", GameSettings.numLives);
22          } else if (hasFocus){
23              PlayerPrefsFile.DeleteKey(GameSettings.gameMode + "_numOfLives");
24          }
25      }
26
27      //Comment 2
28      public static void ResultGame(int kills, int scores, int money){
29          StoreWeapons.money += money;
30          GameSettings.allMoney += money;
31          GameSettings.kills += kills;
32          GameSettings.scores += scores;
33          StatisticsGame.UpdateData (GameSettings.scores, StoreWeapons.money, GameSettings.kills);
34      }
35
```

Zom.sln Строка 37, столбец 26 Размер интервала табуляции: 4 UTF-8 with BOM

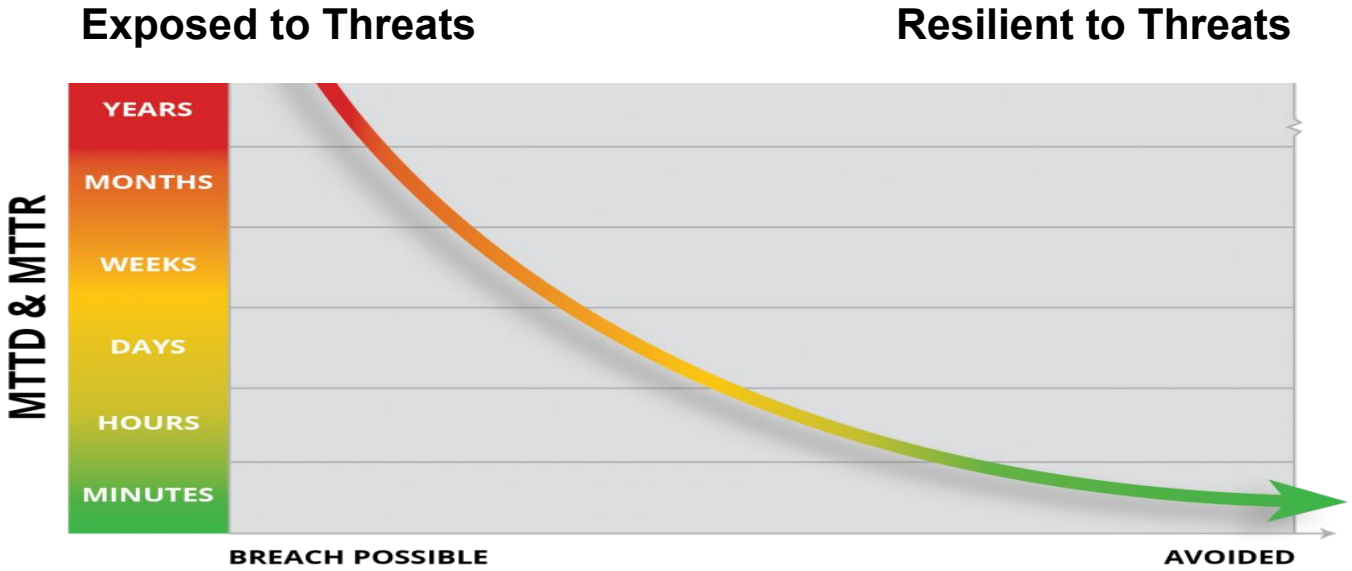
When it is about IaC, you have to review the unknown. What is the unknown here?

If you see the Application code, you can see the mistake because it is written in front of you. But when you see/review the IaC code, you have to see what is not written.

```
28  # configure s3 bucket for tf state
29  resource "aws_s3_bucket" "this" {
30    bucket = "tf-dev-state-bucket"
31
32    lifecycle {
33      prevent_destroy = true
34    }
35
36    versioning {
37      enabled = true
38    }
39
40    server_side_encryption_configuration {
41      rule {
42        apply_server_side_encryption_by_default {
43          sse_algorithm = "AES256"
44        }
45      }
46    }
47
48    tags = {
49      Environment = "Dev"
50      Terraform   = "true"
51    }
52  }
```

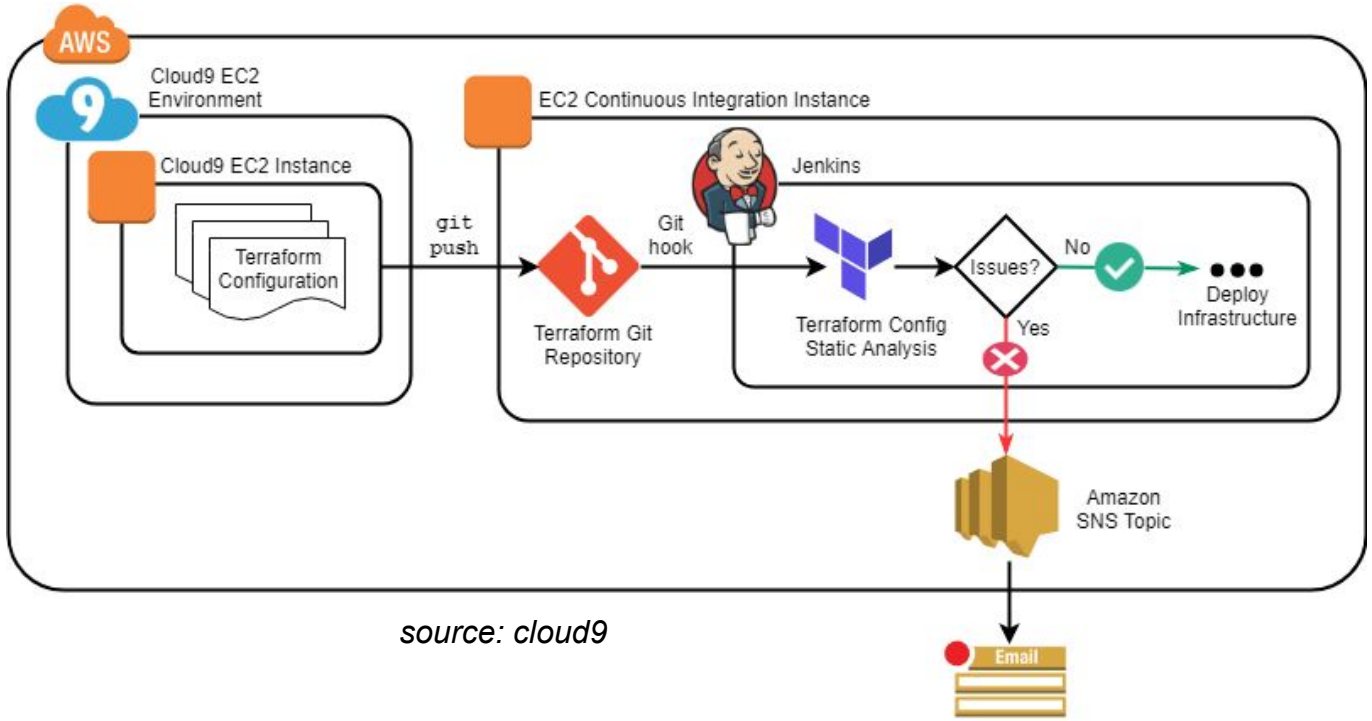


How To Make Sure Your Code is *Automatically* Reviewed *Before* getting Deployed?

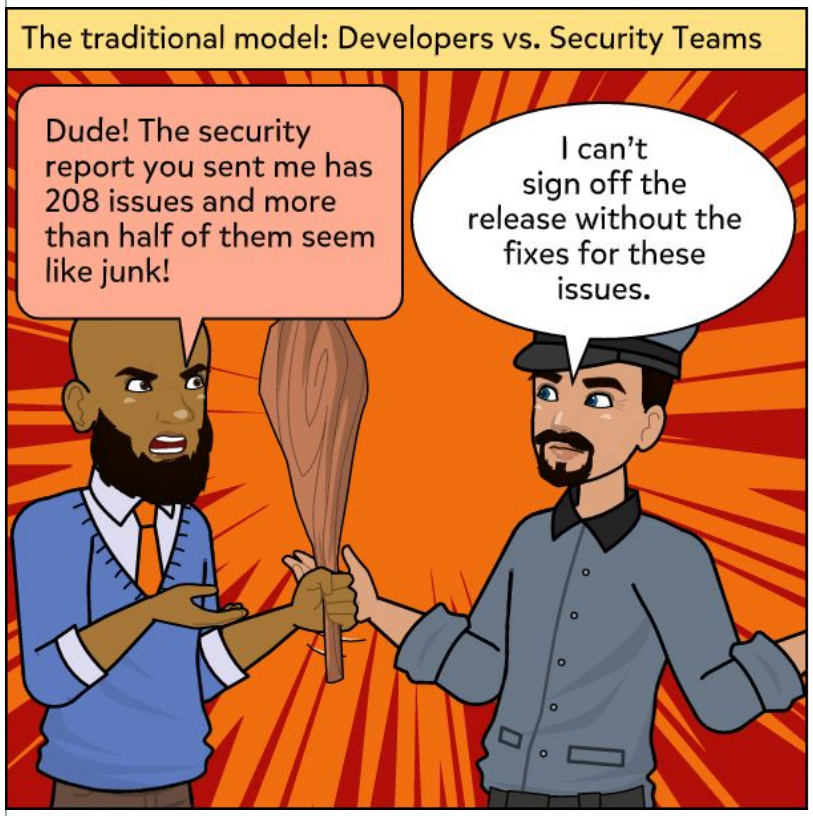


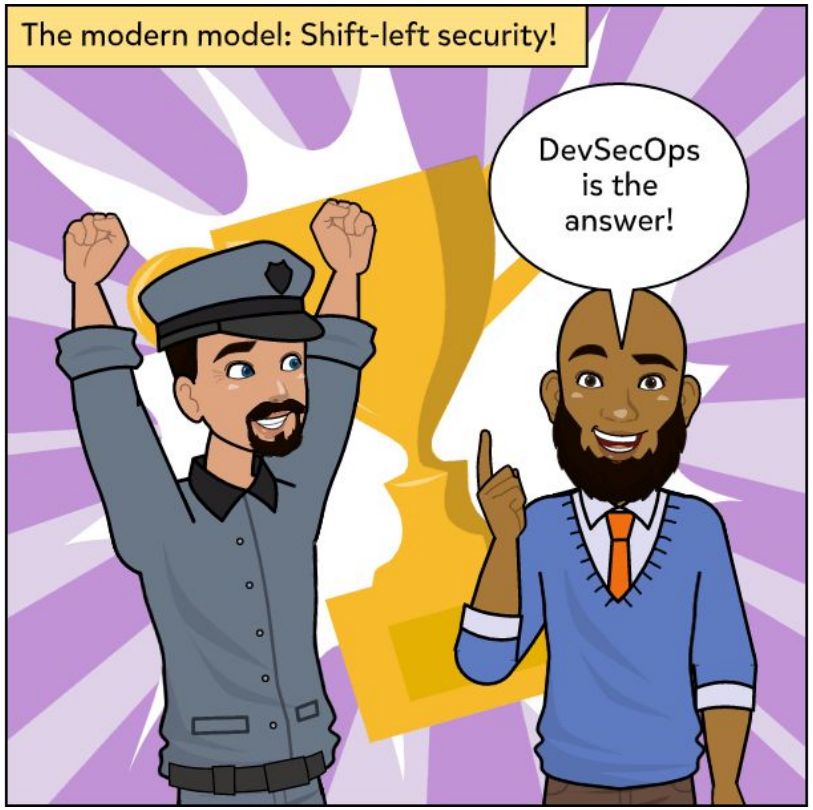
- Manual code review of IaC Templates (Tf, CFT, ARM, etc) is very ***dull, time consuming*** and ***hard*** task.
- Reviewers ***lack context*** about the code change.
- It is very evident that MTTR ***increases exponentially*** as a function of MTTD.

- Coders assume your CI/CD to ***already enforce*** quality standards.
- Have you ever seen a developer willingly use security tool? ***They WON'T***
- IaC authors or Developers ***expect rapid feedback*** in the tools that they already use like PRs, Slack, Email, etc.



source: cloud9





How Do You Accomplish Your Goal To *Shift Left* for *Securing IaC*?

“. . . I *Don’t* Think We Need A Security Tool to Secure My IaC Templates”

Changes that we make to our IaC templates have a direct impact on Cloud Security and Compliance.

Mis-configurations in the cloud [mostly deployed through IaC] are the main source of data breaches.

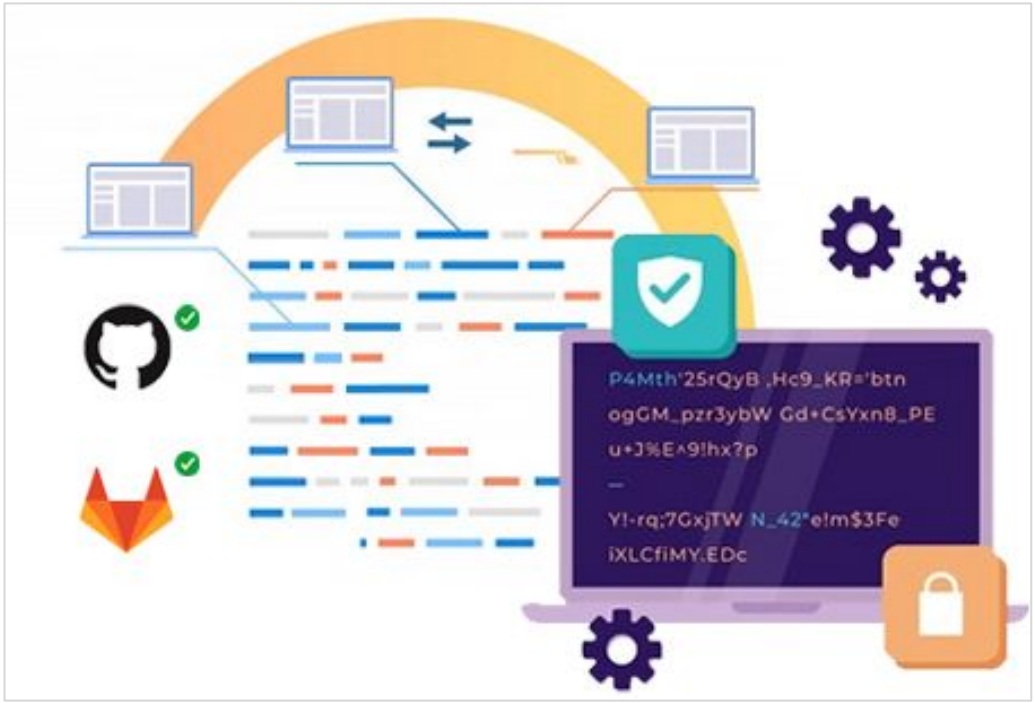
It is critical to have a CSPM Solution integrated, but what about the time taken to detect and the cost involved in fixing these vulnerabilities post they being detected in Production workloads?

We generally are contended with the Cloud Security Posture Management findings, but in a typical production environment, there are 1000s of findings. The number could be remarkably reduced by introducing IaC Security Tool early in the life cycle.

“. . . I ~~Don’t~~ Think We Need A Security Tool to Secure My IaC Templates”

“I Already Have A Security Tool Integrated In My CI/CD Pipeline”

How Do You Measure The Success Of It?



Source: c3m.io

- If the **coverage** provided by your Security Tool is significantly low, then even the best of the tools will not be efficient enough to solve the pitfalls of adopting IaC for infrastructure deployments.

- If you have teams in your organizations already practicing and using the IaC Security tool, **build on the existing initiative** and **vocalize** the usage and benefits of adopting the IaC Security journey.

- Scaling coverage for better results through automation would be something that would interest you if you already have a solution in place and are **looking at improving the efficacy** of the solution.

- Timely measure the coverage, compliance scores and time taken to mitigate the vulnerabilities. We should **aim at lowering the gap between MTTR and MTTD**. Improve code quality.

What Does It Take To Build a Trust ~~Wall~~ Gateway

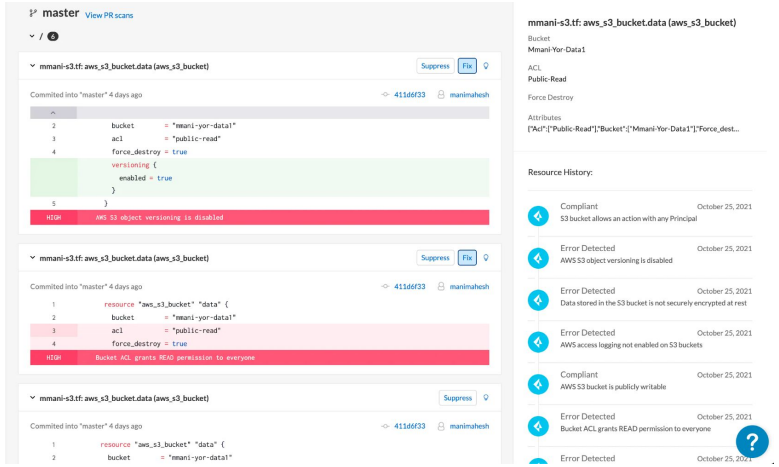
What Does Your Security Tool Need To *Succeed* ?

Seamless integration with CI/CD Platforms

Ability to identify resource drift and alert for the same. [*source: snyk.io*]

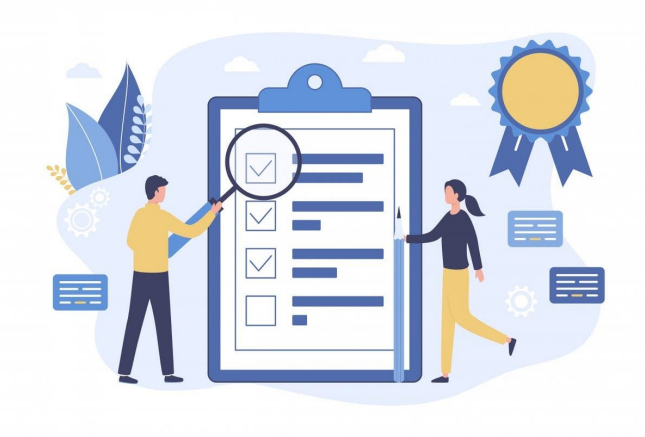
Executive and Detailed Summary Report generation must be supported

Better coverage with security policies



Guided recommendations to fix misconfigurations in the code for developers [*source: bridgecrew*]

Easy to configure new policies



Ability to view and track compliance posture

RISK

Ability to provide Risk Score associated with each of the vulnerabilities

We Create People Driven Innovations

We Are Open Source And Innovative By Design

🚀 We make rapid progress by being early adopters of React, Scala, and GraphQL

📋 We share & contribute to the open source community: https://github.com/sangria-graphql

⚙️ We <3 Automation and Machine Learning

https://commercetools.com/careers

Questions?
:)

LinkedIn

Thank you!