Security testing for Terraform templates


epam
Pawel Piwosz
Lead Systems Engineer
AWS
community
builders
AWS Community Builders
AMBASSADOR
DevOps
INSTITUTE
Human of DevOps
DevOps Institute Ambassador

What is Terraform?

It is an Infrastructure as Code tool

What is an Infrastructure as Code then?

Fast

Dynamic

Programmable

Way to deploy

Hidden infrastructure's misconfigurations

Everywhere.

What are we deal with?

Solarwinds (2020)

300k customers

30k used Orion

18k downloaded hacked version

More than 10 government institutions had been affected

As well as Microsoft, Nvidia, Palo alto, Vmware (to list a few)

But it wasn’t a case of bad IaC, right?

IBM and Ponemon Institute Report (2020)

Average time to identify and contain

280 days

207 to identify

73 to contain

Cloud misconfigurations

Imperva (2019)

- Customer records (like API keys, TLS certificates)

Cause?

- Network misconfiguration
- Hardcoded API key
- Not encrypted records

Time to identification

- 10 months(!)

Cloud misconfigurations

CapitalOne (2019)

- More than 100 milion records exposed
- Bank accounts
- Social numbers

Cause?

- IAM policy misconfigurations
- Unecrypted storage

Two causes

Cloud misconfiguration

Configuration drifts

What is a drift?

Unmonitored

Undocumented

Change in the configuration

Done manually

Fact

90% of organizations allow users to make changes without proper process

According to “State of DevSecOps by Accurics (formely) - 2020

Unbelievable, but true…

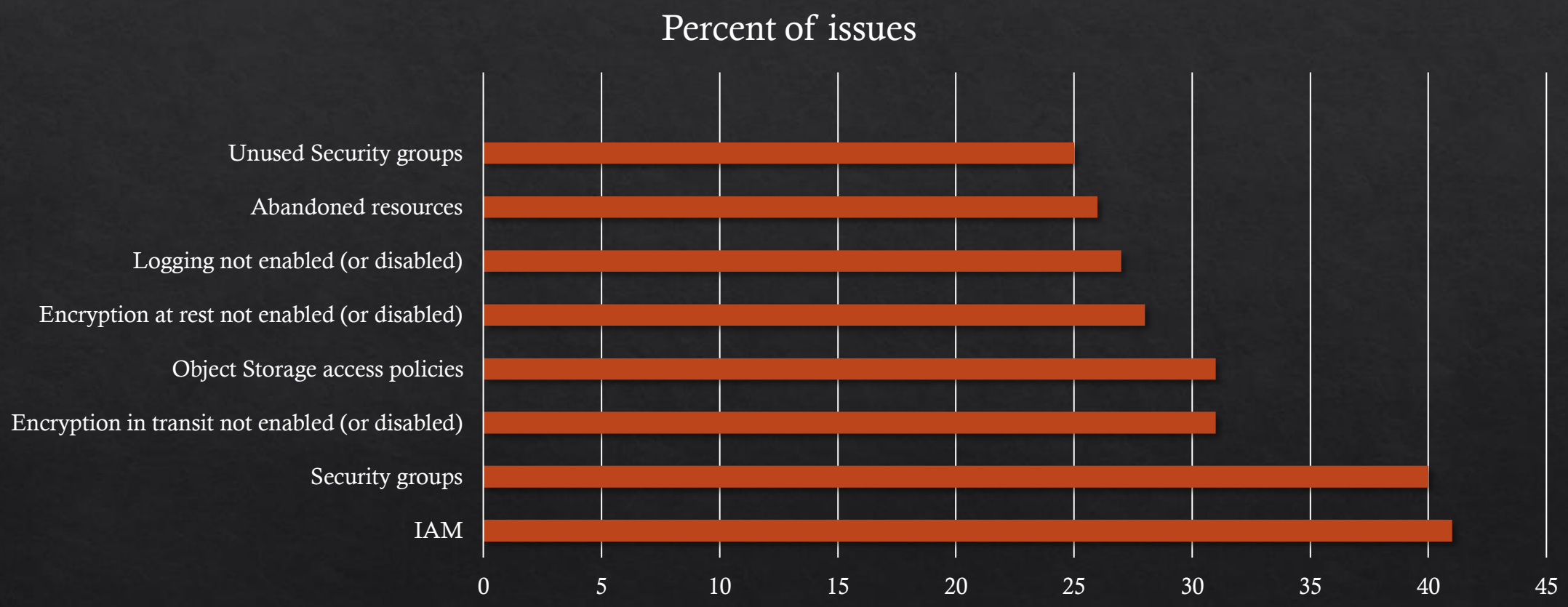
36% of professionals suffered a serious breach because of Cloud misconfiguration

According to Cloud Security Report 2021 by Sonatype (300 responders)

49% of teams had more than … 50 misconfigurations per day

According to Cloud Security Report 2021 by Sonatype (300 responders)

Types of misconfigurations



How they catch issues?

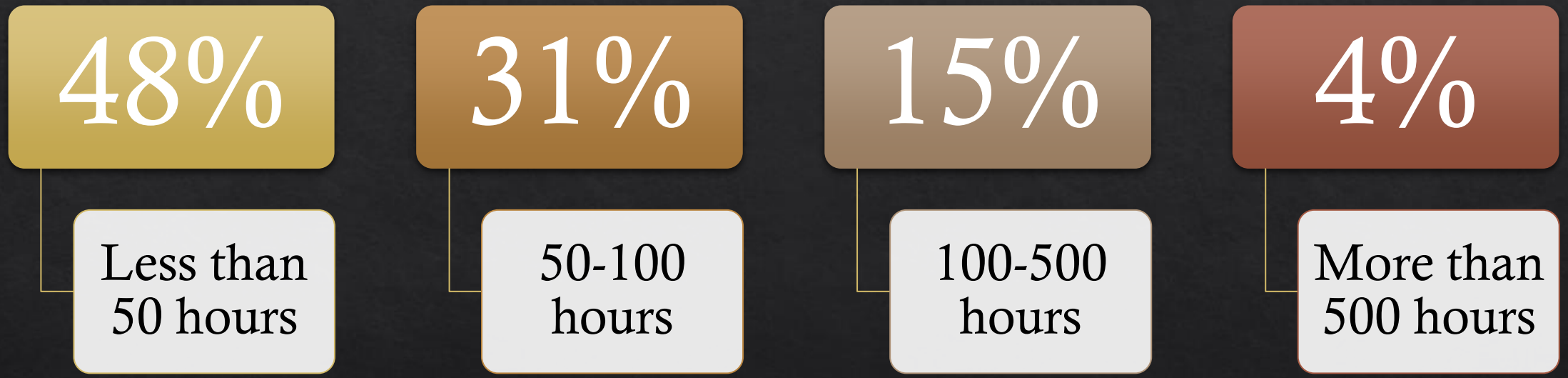
33%

- Manual checks before deployment

27%

- Post-deployment check

Investments (per week)



12 people involved 100% in IaC security per week!!!!!

Shift left

Paradigm not only for software, but for infrastructure as well

Fast feedbacks

SAST also relevant to infrastructure

Everyone is responsible for security!

Implement Open Policy Agent

(or any tools which is using the approach)

OPA is a project under the Cloud Native Computing Foundation

A policy engine that automates and unifies implementation of policies across environments

Use the OPA to enforce, monitor and remediate policies across environments and resources

https://www.openpolicyagent.org/

Control before deployment

If deployed, it is already too late

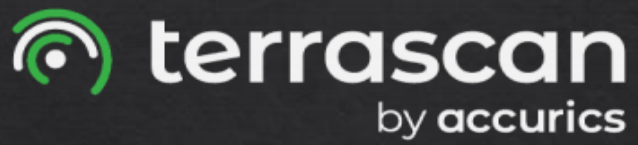
Use dedicated tools to prevent deployments with misconfigured resources

Use CI/CD pipelines

A lot of tools around!

- Checkov
- Terrascan
- TFSec
- CFN-nag
- Snyk
- Accurics (Tenable)

Let’s demo a few of them!



Accurics (Tenable)

https://github.com/accurics/terrascan

Bridgecrew

https://github.com/bridgecrewio/checkov

Aqua

https://github.com/aquasecurity/tfsec

What about drifts?

The challenge

Drifts have to be controlled continuously

“There is always someone with elevated privileges”

Available tools not always cover all possible changes

Management must understand the risk behind “it must be done now!”

Tools

Driftctl (acquired by Snyk)

Kubediff

SaaS tools: Bridgecrew, Accurics

New level

Go boldly beyond “just scans”

Everything as Code

With newest SaaS offerings we are able to create automated control and remediation for infrastructure’s misconfiguration

Security must be implemented on the earliest possible stage and be automated in pipelines

Everything as Code

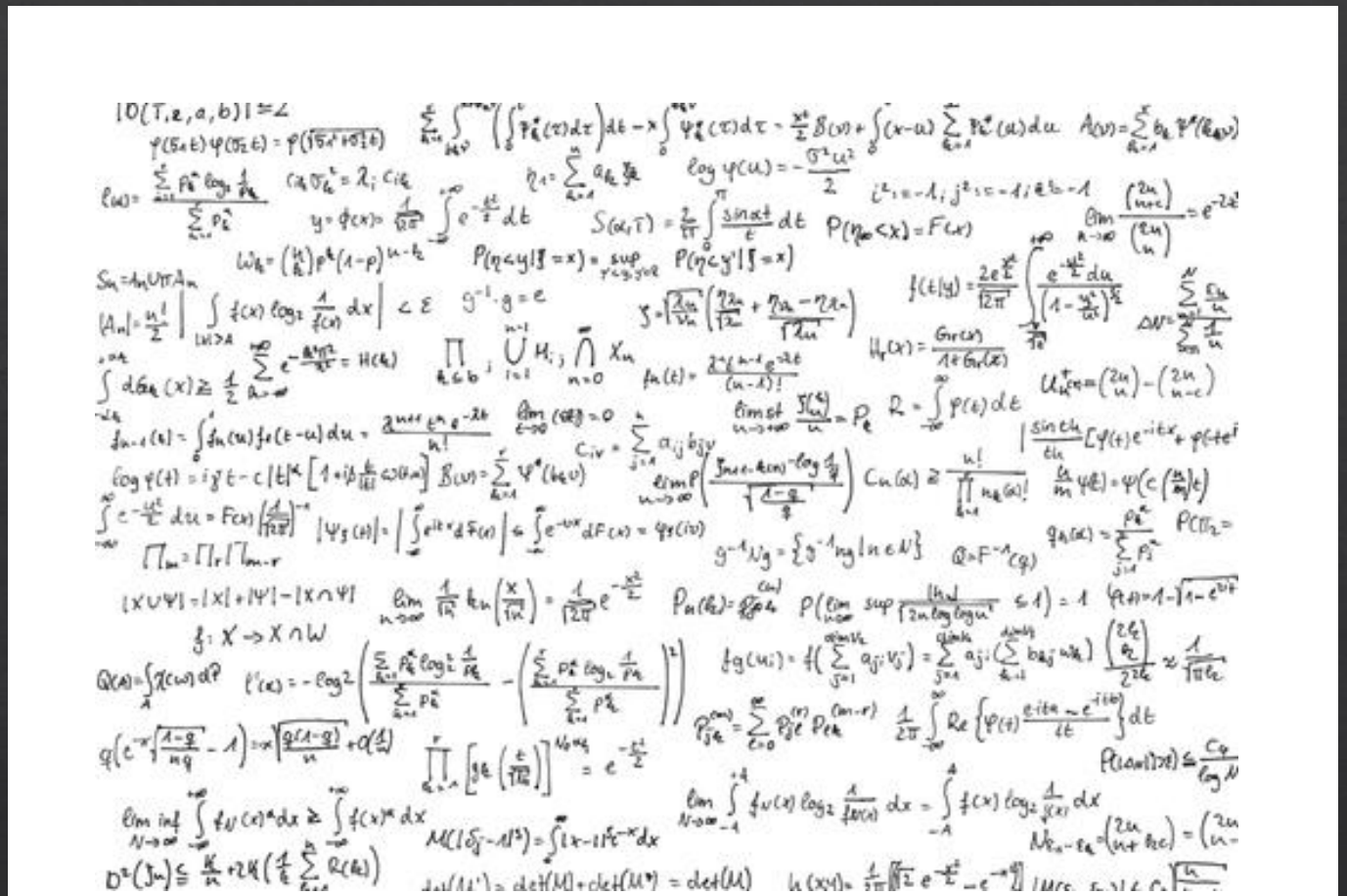
Policy as Code

Security as Code

Drift as Code

Remediation as Code

Do not pretend that you have **security**



Security is very complex