

# Security testing for Terraform templates



Lead Systems Engineer

Pawel Piwosz



DevOps Institute Ambassador



AWS Community Builders





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?





Let's take a look on some numbers





Average cost  
**\$3.86 million**

Average time to identify and contain

280 days

207 to identify

73 to contain





Percent of breaches caused by  
cloud misconfigurations

19%

# 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
- Unencrypted 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





Unbelievable, but true...

Now things  
will go more  
interesting...



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

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



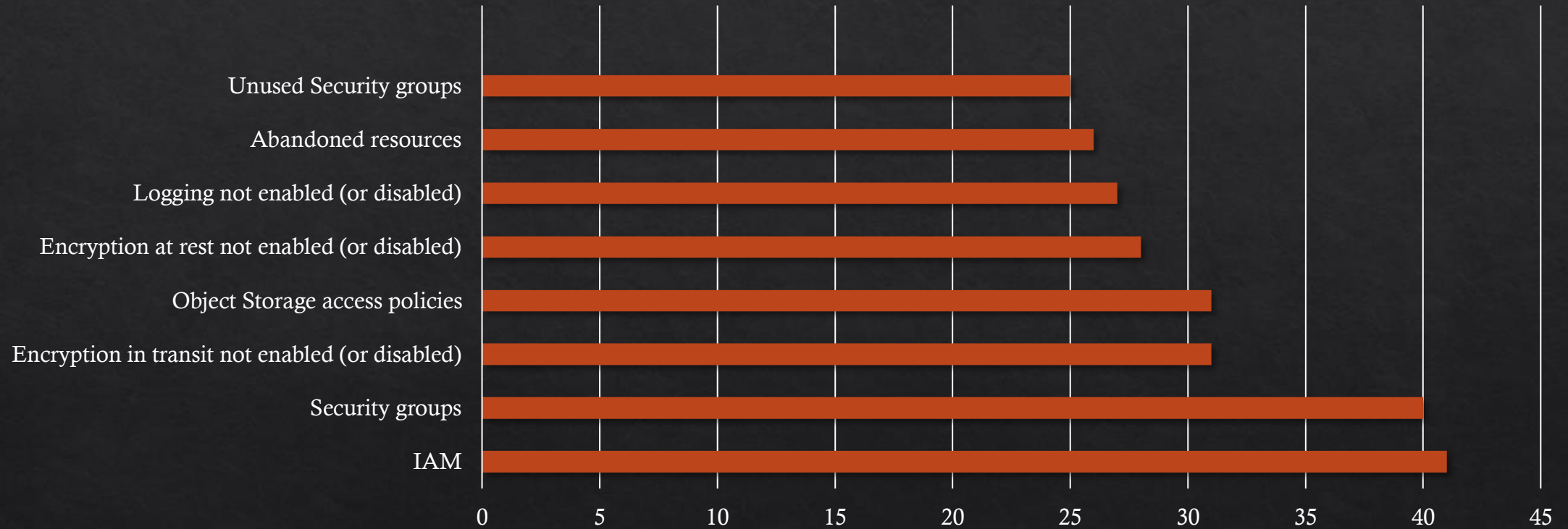
49% of teams had more than ... 50  
misconfigurations per day

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



# Types of misconfigurations

Percent of issues





## How they catch issues?

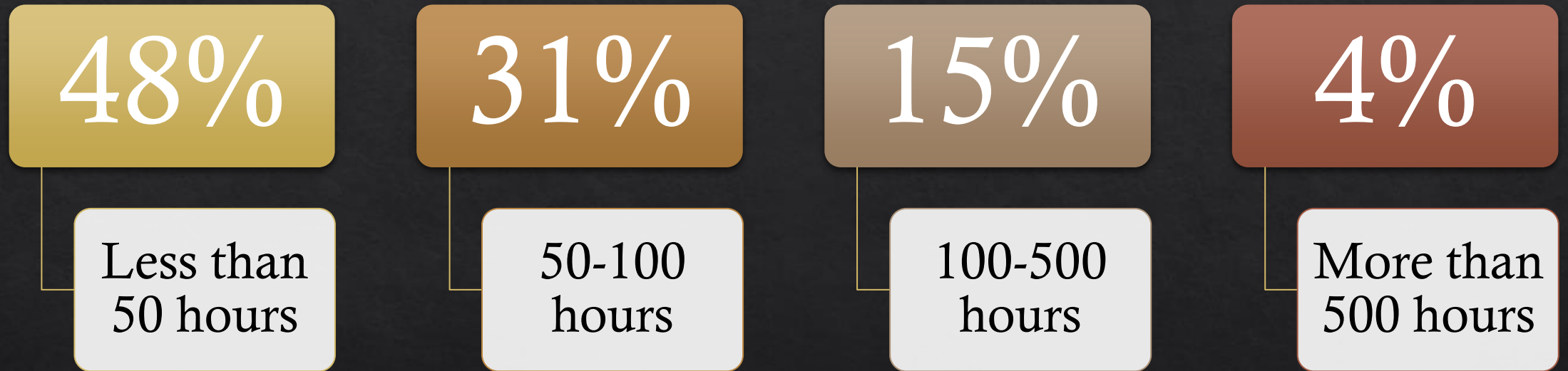
33%

- 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

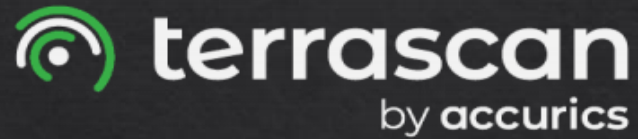
TFSec

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>

A 3D graphic featuring the text "SHOW US YOUR TECH" in white, bold, sans-serif font. The text is arranged in two lines: "SHOW US YOUR" on top and "TECH" in a larger font below. The letters are rendered with a slight shadow and are supported by thin black lines from below. Above the text, several black tech items are arranged: a keyboard, a lens, a speaker, and a power brick. The background is a blue gradient with a subtle grid pattern.

SHOW US YOUR  
TECH



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**







All misconfigurations  
WILL BE explored



$$\begin{aligned}
& I_0(T, \lambda, a, b) = \int_0^T \int_0^{\lambda} \int_0^a \int_0^b \dots \\
& \varphi(\sigma_1, \epsilon) \varphi(\sigma_2, \epsilon) = \varphi(\sqrt{\sigma_1^2 + \sigma_2^2}, \epsilon) \\
& \rho(u) = \frac{\sum_{k=1}^n p_k \log_2 \frac{1}{p_k}}{\sum_{k=1}^n p_k} \quad (a) \sigma_k^2 = \lambda; c_k \epsilon \\
& \eta_1 = \sum_{k=1}^n a_k \epsilon_k \quad \log \varphi(u) = -\frac{\sigma^2 u^2}{2} \quad i^2 = -1; j^2 = -1; i \epsilon^b = -1 \quad \frac{(2u)}{(n+c)} = e^{-2\lambda} \\
& S(u, T) = \frac{2}{\pi} \int_0^{\pi} \frac{\sin \alpha t}{t} dt \quad P(\eta_0 < x) = F(x) \\
& W_k = \binom{n}{k} p^k (1-p)^{n-k} \quad P(\eta < y | \mathcal{F} = x) = \sup_{\tau \leq y} P(\eta < y | \mathcal{F} = x) \\
& S_n = \ln U_n A_n \quad f(t|y) = \frac{2e^{-t}}{\pi} \int_0^{\infty} \frac{e^{-u^2}}{(1-\frac{u^2}{t^2})^2} du \\
& |A_n| = \frac{n!}{2} \left| \int_{-1}^1 f(x) \log_2 \frac{1}{f(x)} dx \right| < \epsilon \quad g^{-1} \cdot g = e \quad \eta_1 = \sqrt{\frac{2n}{\ln 2}} \left( \frac{\eta_0}{\sqrt{2}} + \frac{\eta_0 - \eta_1}{\sqrt{2n}} \right) \quad H_4(x) = \frac{G(x)}{1+G(x)} \\
& \int_{-1}^1 dG_n(x) \geq \frac{1}{2} \sum_{k=0}^n e^{-\frac{2k}{n}} = H(n) \quad \prod_{k=1}^n \bigcup_{i=1}^n H_i; \prod_{n=0}^n X_n \quad \lim_{n \rightarrow \infty} \frac{f(n)}{n} = P_e \quad R = \int_{-\infty}^{\infty} p(x) dx \\
& f_{n+1}(x) = \int_{-1}^1 f_n(u) f_n(t-x) du = \frac{2^{n+1} \epsilon^n e^{-2t}}{n!} \quad \lim_{t \rightarrow \infty} (G(t)) = 0 \quad \lim_{n \rightarrow \infty} \frac{f(n)}{n} = P_e \\
& \log \varphi(t) = i \gamma t - c |t|^\alpha \left[ 1 + i \beta \frac{t}{|t|} \omega(t) \right] \quad \beta(x) = \sum_{k=1}^n \psi^*(k) u^k \quad C_{n+1}(x) \geq \frac{n!}{\prod_{k=1}^n h_k(x)} \left| \frac{\sin \epsilon x}{\epsilon} [\varphi(t) e^{-itx} + \varphi(-t) e^{itx}] \right| \\
& \int_{-\infty}^{\infty} e^{-\frac{u^2}{2}} du = \sqrt{2\pi} \quad |\psi_j(t)| = \left| \int_{-\infty}^{\infty} e^{itx} dF(x) \right| \leq \int_{-\infty}^{\infty} e^{-|ux|} dF(x) = \varphi_x(iu) \quad g^{-1} \psi_j = \{g^{-1} \log |n \epsilon \lambda|\} \quad \mathcal{Q} = F^{-1}(c_p) \quad \varphi_n(x) = \sum_{j=1}^n p_j^x \quad P(C|H) = \\
& \prod_{m=1}^n \prod_{l=1}^m \prod_{r=1}^l \\
& |X \cup Y| = |X| + |Y| - |X \cap Y| \quad \lim_{n \rightarrow \infty} \frac{1}{n} \ln \binom{n}{k} = \frac{1}{2\pi} e^{-\frac{x^2}{2}} \quad P_n(k) = \frac{c^k}{k!} \quad P\left(\limsup_{n \rightarrow \infty} \frac{\ln n}{2n \log \log n} \leq 1\right) = 1 \quad (P_n = 1 - \sqrt{1 - e^{-2n}}) \\
& \mathcal{Q}(X) = \int_1^{\infty} \lambda(x) dP \quad f(x) = -\log_2 \left( \frac{\sum_{k=1}^n p_k \log_2 \frac{1}{p_k}}{\sum_{k=1}^n p_k} - \left( \frac{\sum_{k=1}^n p_k \log_2 \frac{1}{p_k}}{\sum_{k=1}^n p_k} \right)^2 \right) \quad \log \varphi(u) = f\left(\sum_{j=1}^n a_j \psi_j\right) = \sum_{j=1}^n a_j \left(\sum_{k=1}^n b_{kj} \psi_k\right) \frac{(2\epsilon)}{2^{2\epsilon}} \approx \frac{1}{\sqrt{2\epsilon}} \\
& \varphi\left(c \sqrt{\frac{1-x}{n}} - 1\right) = \sqrt{\frac{1-x}{n}} + o\left(\frac{1}{n}\right) \quad \prod_{k=1}^n \left[ \frac{1}{\sqrt{2\epsilon}} \right]^{4n} = e^{-\frac{1}{2}} \quad P_{j,k}^{(m)} = \sum_{l=0}^m p_{j,k}^{(m)} p_{k,l}^{(m-r)} \quad \frac{1}{2\pi} \int_{-\infty}^{\infty} \operatorname{Re} \left\{ \varphi(t) \frac{e^{-ita} - e^{-itb}}{it} \right\} dt \\
& \lim_{N \rightarrow \infty} \int_{-1}^1 f_N(x)^N dx \geq \int_{-1}^1 f(x)^N dx \quad M((\log_2 - 1)^2) = \int_{-1}^1 (x-1)^2 e^{-x} dx \quad \lim_{N \rightarrow \infty} \int_{-1}^1 f_N(x)^N dx = \int_{-1}^1 f(x) \log_2 \frac{1}{f(x)} dx \quad P(\text{am} | \mathcal{F}) \leq \frac{C_p}{\log N} \\
& D^2(J_n) \leq \frac{2}{n} + 2K \left( \frac{1}{n} \sum_{k=1}^n R(k) \right) \quad \det(M) = \det(M) + \det(M^*) = \det(M) \quad h(x) = \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}} \quad \lim_{n \rightarrow \infty} \frac{1}{n} \ln \binom{n}{k} = \frac{1}{2\pi} e^{-\frac{x^2}{2}}
\end{aligned}$$

Security is very complex