



Security testing for Terraform templates



Lead Systems Engineer



DevOps Institute Ambassador



AWS Community Builders

Pawel Piwosz



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

A large pile of US one-dollar coins, showing the reverse side of each coin. The coins are stacked in various layers, creating a textured, dark gray background.

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 million 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...

A photograph of a man in purple shorts jumping off a dark, rocky cliff edge. He is shirtless and has his arms raised in a celebratory or dramatic pose. The ocean below is a vibrant turquoise color with white-capped waves crashing against the rocks. In the background, there are more green hills and mountains under a clear sky.

Now things
will go more
interesting...

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

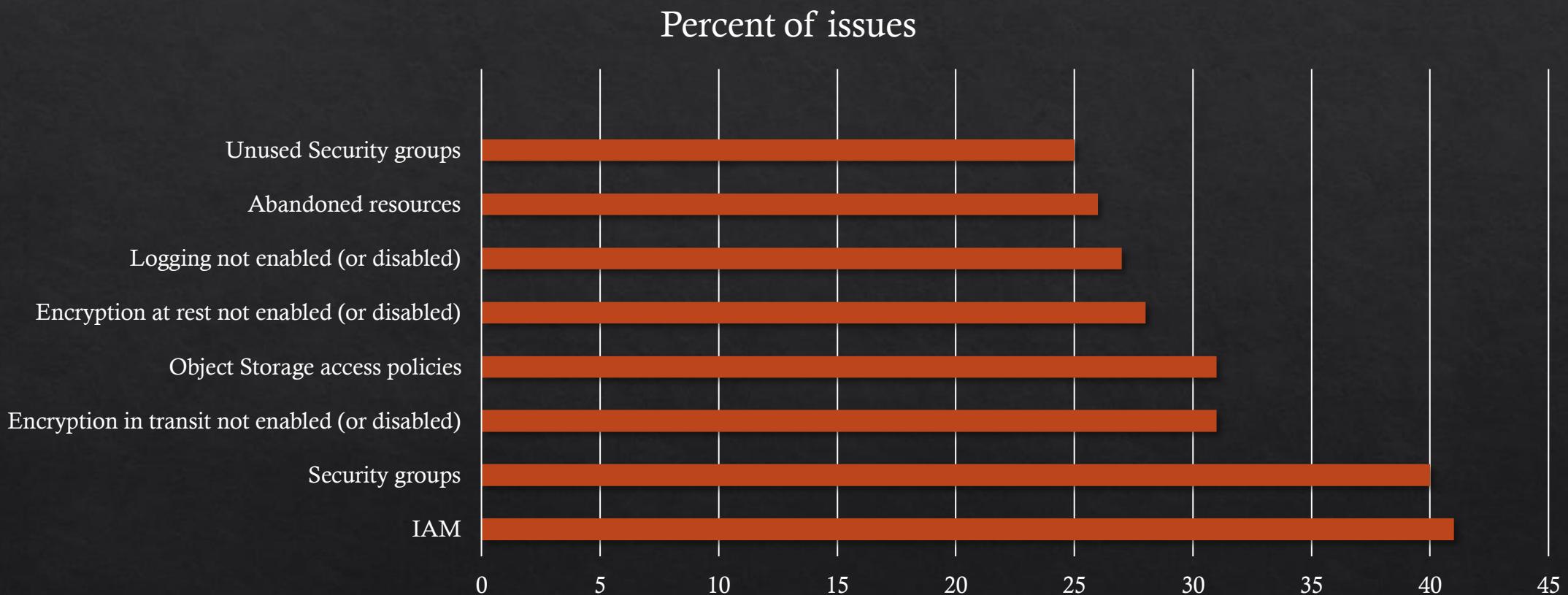
According to Cloud Security Report 2021 by Sonatype (300 responders)

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

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



Types of misconfigurations



How they catch issues?

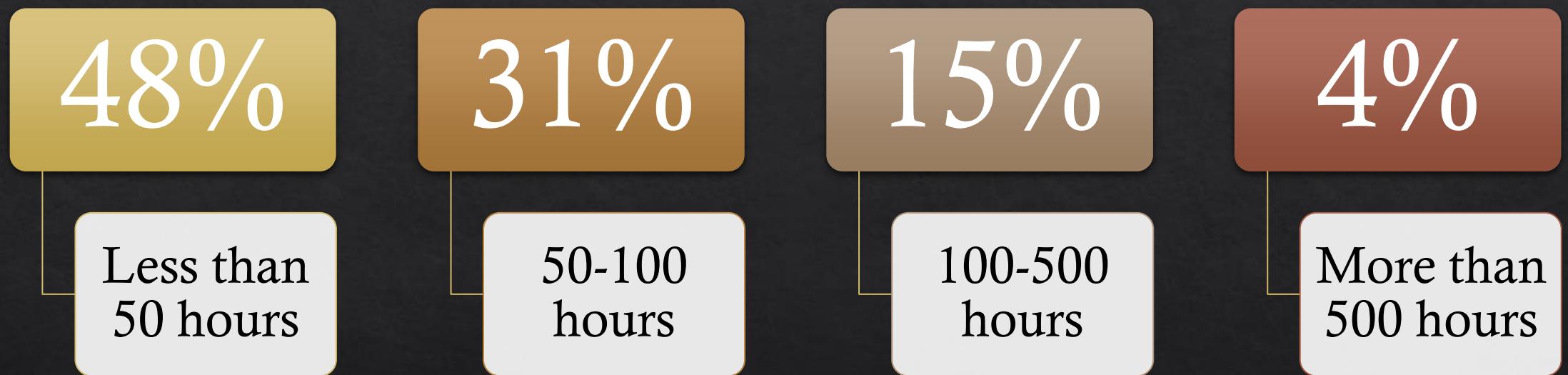
33%

- 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>

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

Security is very complex

$$\begin{aligned}
& \text{IO}(T, z, a, b) = \int_{aT}^{bT} \int_0^{\infty} \left(\int_0^x p_k^*(x) dx - x \int_0^x p_k^*(x) dx + \frac{x}{2} \delta(x) + \int_{aT}^x p_k^*(u) du \right) A(u) = \sum_{k=1}^K b_k p_k^*(bT) \\
& \gamma(E \oplus E) \psi(E \oplus E) = \rho(\sqrt{E} \oplus \sqrt{E}) \\
& \sum_{k=1}^K p_k^* \log \frac{p_k^*}{p_k} \quad c_k p_k^* = 2, c_{16} \\
& \sum_{k=1}^K p_k^* \quad y = \phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x e^{-\frac{t^2}{2}} dt \quad S(x, t) = \frac{2}{\pi} \int_{-\infty}^t \frac{\sin at}{t} dt \quad P(\eta_x < x) = F(x) \\
& \sum_{k=1}^K p_k^* \quad u = \sum_{k=1}^K a_k \frac{1}{k!} \quad \log \psi(u) = -\frac{u^2}{2} \\
& \sum_{k=1}^K p_k^* \quad \lim_{n \rightarrow \infty} \frac{(2n)!}{(2n+1)^{2n}} = e^{-2} \\
& \sum_{k=1}^K p_k^* \quad W_k = \binom{n}{k} p^k (1-p)^{n-k} \quad P(\eta_x \leq y) = \sup_{y' \geq y} P(\eta_{x'} \leq y') = x \\
& S_n = \ln(VTA_n) \\
& |A_n| = \frac{n!}{2^n} \left| \int f(x) \log \frac{f(x)}{f(x)} dx \right| \leq \varepsilon \quad g^{-1} \cdot g = e \\
& \sum_{n=1}^{\infty} e^{-\frac{n^2}{2}} = H(\varepsilon) \quad \prod_{k \in K} \bigcup_{i=1}^{n-1} H_i \quad \prod_{n=0}^{\infty} X_n \quad f_n(t) = \frac{2^n n! e^{-n^2/2}}{(n-1)!} \\
& \int d\delta_n(x) \geq \frac{1}{2} \frac{1}{n-1} \quad H_p(x) = \frac{G_p(x)}{1+G_p(x)} \quad \Delta V = \sum_{n=1}^N \frac{1}{n!} \\
& \lim_{n \rightarrow \infty} \int_{-n}^n f(u) f(t-u) du = \frac{2 \pi i e^{-\pi t/2}}{n!} \quad \lim_{t \rightarrow 0} (g(t)) = 0 \quad \lim_{t \rightarrow \infty} \frac{g(t)}{t} = p_e \quad R = \int_0^\infty p(t) dt \\
& \log \varphi(t) = i g t - c / t^2 \left[1 + o(\frac{1}{t}) \right] \quad B(n) = \sum_{k=1}^n V^*(k, n) \quad C_{i,j} = \sum_{n=1}^{\infty} a_{ij} b_{nj} \\
& \int e^{-\frac{t^2}{2}} dt = F(x) \left(\frac{d}{dx} \right)^{-1} \quad |\psi_j(z)| = \left| \int e^{izx} dF(x) \right| \leq \int e^{-zx} dF(x) = q_j(z) \\
& \prod_{m=1}^{\infty} = \prod_{l=1}^L \prod_{m=l}^{\infty} \\
& |X \cup Y| = |X| + |Y| - |X \cap Y| \quad \lim_{n \rightarrow \infty} \frac{1}{n!} \ln \left(\frac{X}{n!} \right) = \frac{1}{2\pi} e^{-\frac{X^2}{2}} \quad P_n(k) = \frac{c_n}{k!} \quad P(\limsup_{n \rightarrow \infty} \frac{|X_n|}{2 \ln \log n} \leq 1) = 1 \quad (P(A) = 1 - \sqrt{1 - e^{-2P}}) \\
& f: X \rightarrow X \cap W \\
& Q(A) = \int_A \rho(x) dx \quad I'(x) = -\log 2 \left(\frac{\sum_{k=1}^K p_k^* \log \frac{p_k^*}{p_k}}{\sum_{k=1}^K p_k^*} - \left(\frac{\sum_{k=1}^K p_k^* \log \frac{p_k^*}{p_k}}{\sum_{k=1}^K p_k^*} \right)^2 \right) \quad fg(u_i) = f \left(\sum_{j=1}^{m_i} a_{ij} v_j \right) = \sum_{j=1}^{m_i} a_{ij} \left(\sum_{k=1}^{m_j} b_{kj} w_k \right) \frac{z_k}{2^{2k}} \approx \frac{1}{2^{2k}} \\
& q(e^{-\sqrt{\frac{1-q}{nq}} - 1}) = \sqrt{\frac{q(1-q)}{n}} + o(\frac{1}{n}) \quad \prod_{k=1}^r \left[\ln \left(\frac{t}{T_k} \right) \right]^{b_k} = e^{-\frac{t^2}{2}} \quad P_{\tilde{S}_T}^{(m)} = \sum_{k=1}^m \tilde{p}_k^{(m)} P_{T_k} \quad \frac{1}{2\pi} \int_0^\infty \operatorname{Re} \left\{ \varphi(t) \frac{e^{ita} - e^{itb}}{it} \right\} dt \\
& \liminf_{N \rightarrow \infty} \int f_N(x) dx \geq \int f(x) dx \quad \lim_{N \rightarrow \infty} \int_{-1}^1 f_N(x) \log \frac{1}{f(x)} dx = \int_{-1}^1 f(x) \log \frac{1}{f(x)} dx \\
& M(I \tilde{q} - A)^2 = \int (x-1)^2 e^{-x} dx \quad N_{k_1, k_2}^{(2n)} = \binom{2n}{n-k_1, n+k_2} = \binom{2n}{n} \\
& D^2(J_N) \leq \frac{K}{n} + 2K \left(\frac{1}{6} \sum_{k=1}^n Q_k \right) \quad \det(M) \det(M') = \det(M) \quad \ln(XM) = \frac{1}{2\pi} \left[\frac{1}{2} e^{-\frac{X^2}{2}} - e^{-\frac{M^2}{2}} \right] \quad \ln(M) = \frac{1}{2\pi} \left[\frac{1}{2} e^{-\frac{M^2}{2}} - e^{-\frac{Q^2}{2}} \right]
\end{aligned}$$