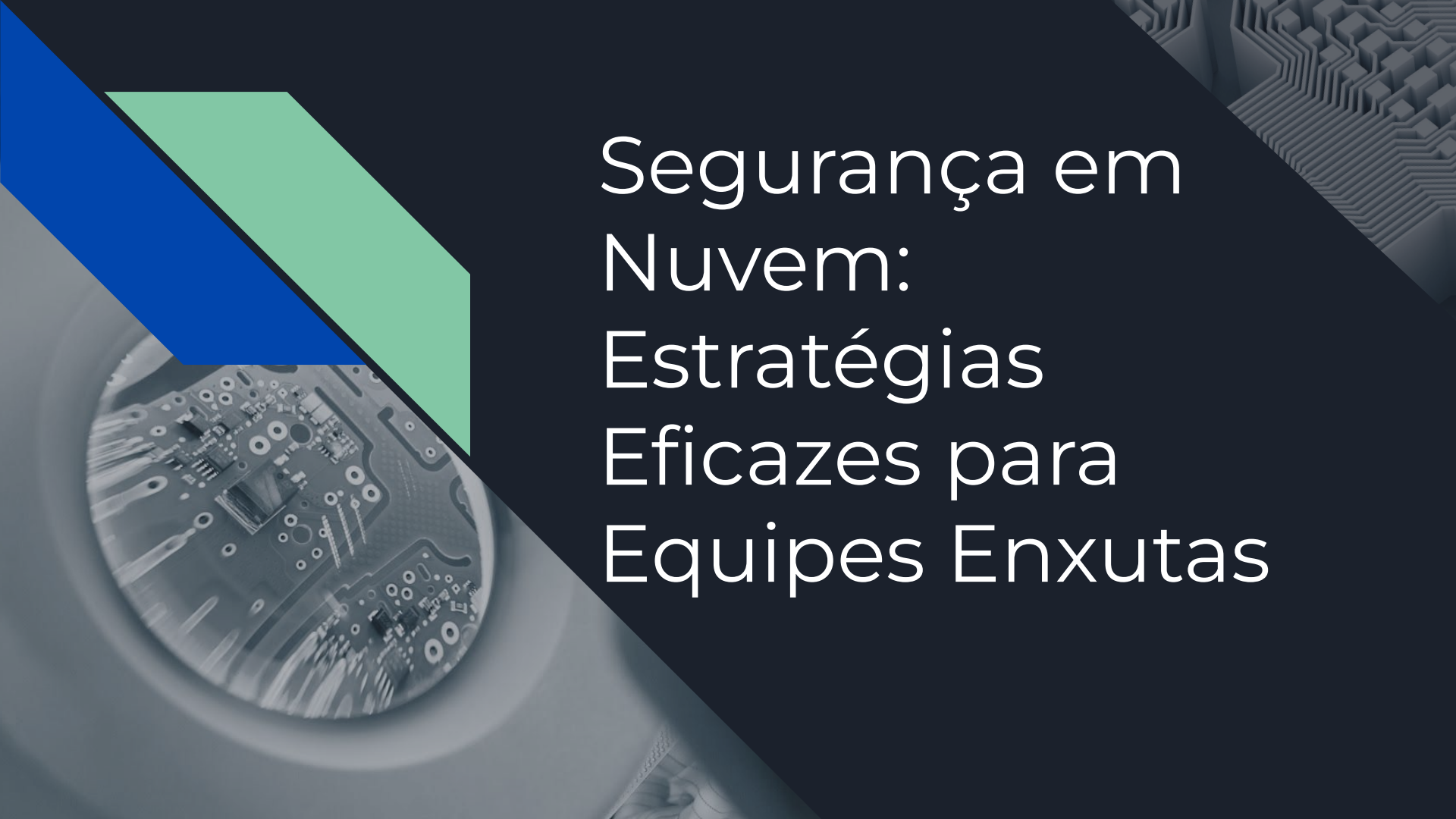


Segurança em Nuvem: Estratégias Eficazes para Equipes Enxutas

Índice

O cenário atual

US CHANNEL NEWS July 16, 2024

New Snowflake Data Breach Exposes Millions of Customers

Snowflake data breach exposes 2M Advance Auto Parts customers. Sensitive info compromised due to lack of MFA. New security measures and MFA adoption urged.

ALLISON FRANCIS

Research Threat intelligence Microsoft Defender Attacker techniques, tools, and infrastructure

20 min read

Storm-0501: Ransomware attacks ending to hybrid cloud environments

Threat Intelligence

Fortinet confirms data breach, extortion demand

Fortinet confirmed that a threat actor stole data from a third-party cloud-based shared file drive, which affected a small number of customers, but many questions remain.

By **Arielle Waldman,** News Writer

Published: **13 Sep 2024**

Microsoft finally explains breach: An engineer's account was hacked

Other failures along the way included a signing key improperly appearing in a crash dump.

DAN GOODIN – SEP 6, 2023 6:11 PM | 69

Alguns números

1. **45% das violações são baseadas na nuvem**.
2. **72% das organizações optam por serviços baseados na nuvem** ao adquirir novas tecnologias, o que significa que a maioria das empresas já experimentou uma violação;
3. **Quase 23% dos incidentes** de segurança em nuvem são resultados de má configuração da nuvem, e **27% das empresas** já enfrentaram violações de segurança em sua infraestrutura de nuvem pública.
4. As configurações incorretas de recursos na nuvem são uma das principais preocupações para organizações que utilizam nuvens públicas. Erros podem ocorrer durante os processos de configuração e implantação.
5. 82% das configurações incorretas na nuvem têm origem em erros humanos e não em falhas de software
6. Mais de 79% das organizações utilizam mais de um provedor de nuvem, e a crescente complexidade dos ambientes multi-cloud leva a um aumento nas configurações incorretas na nuvem.
7. Segundo o Gartner, os gastos globais com serviços de nuvem pública devem crescer 20,4% em 2024, atingindo US$ 678,8 bilhões, impulsionados por pressões inflacionárias e condições macroeconômicas. Todos os segmentos devem crescer, com destaque para IaaS, que liderará o aumento.

Fonte: *Relatório SentinelOne: 50+ Cloud Security Statistics in 2024*

Enquete

- Quantos já trabalham com segurança em nuvem?

- Quantas pessoas trabalham em sua equipe de segurança em nuvem?

Os 3 pilares de segurança em nuvem

01 **Configurações** - *“80% das invasões decorrem de falhas de configuração.”*

O pilar - **Configurações**

“80% das invasões decorrem de falhas de configuração”

Dark Cloud: Inside The Pentagon's Leaked Internet Surveillance Archive

UpGuard Team
Published Nov 17, 2017

Twitch source code, creator earnings exposed in 125GB leak

Twitch blames a "server configuration change" for the massive data leak.

AX SHARMA – OCT 6, 2021 4:31 PM | 134

O pilar - **Configurações**

“80% das invasões decorrem de falhas de configuração”

Ferramentas

OpenSource	Pago	AWS	Azure	GCP
prowler	Prisma Cloud	SCP	Defender 4 cloud	SCC
Cloud Custodian	Wiz	Security HUB	Azure Policy	Asset Inventory
Open Policy Agent	Orca	Config		Org Policy

Os 3 pilares de segurança em nuvem

01 **Configurações** - *“80% das invasões decorrem de falhas de configuração.”*

02 **Identidade** - *“Na nuvem, a identidade é o novo perímetro.”*

O pilar - **Identidade**

“Na nuvem, a identidade é o novo perímetro.”

Uber Confirms Data Breach after Third-Party Vendor Gets Hacked

Uber recently suffered another data breach that the company confirmed is unrelated to a major data breach it suffered in September.

Sumeet Wadhwani Asst. Editor, Spiceworks Ziff Davis

December 14, 2022

O pilar - **Configurações**

“80% das invasões decorrem de falhas de configuração”

Ferramentas

OpenSource

- prowler
- Cloud Custodian
- Open Policy Agent

Pago

- Prisma Cloud
- Cyberark CEM

AWS

- Access Analyzer
- Identity Center

Azure

- Defender 4 cloud
- Azure Policy

GCP

- Asset Inventory
- IAM
- Workforce id federation

Os 3 pilares de segurança em nuvem

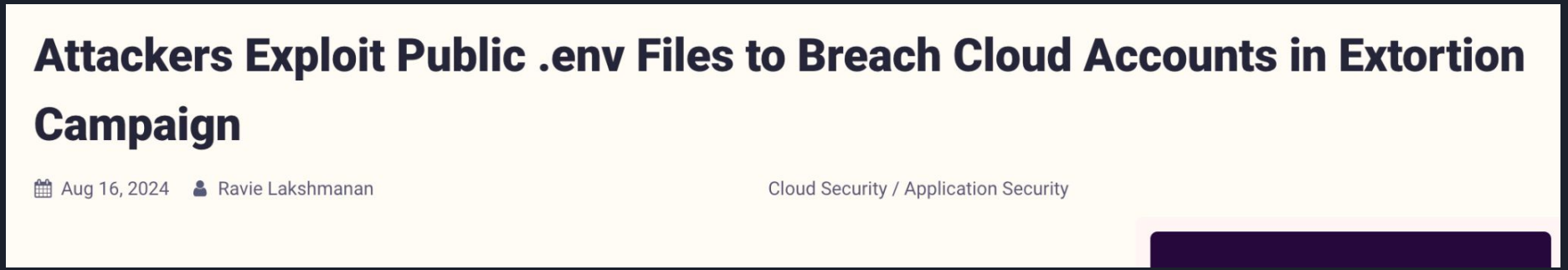
01 **Configurações** - *“80% das invasões decorrem de falhas de configuração.”*

02 **Identidade** - *“Na nuvem, a identidade é o novo perímetro.”*

03 **Aplicações** - *“Aplicações mal protegidas são a porta de entrada para grande parte dos ataques modernos.”*

O pilar - **Identidade**

“Na nuvem, a identidade é o novo perímetro.”



Attackers Exploit Public .env Files to Breach Cloud Accounts in Extortion Campaign

Aug 16, 2024 Ravie Lakshmanan

Cloud Security / Application Security

O pilar - **Aplicações**

“Aplicações mal protegidas são a porta de entrada para grande parte dos ataques modernos.”

Ferramentas

OpenSource	Pago	AWS	Azure	GCP
aqua trivy	Prisma Cloud	WAF	Application Gateway	Cloud Armor
Falco	Cloudflare WAF	Inspector	Defender 4 containers	APIGee API Security
Open Policy Agent	SALT API Security	Shield Advanced	Defender 4 APIs	Container analysis

Elaborando uma estratégia eficaz

Para escalar a segurança, precisamos aplicar 3 princípios!

1. **Automatizar e prevenir**

A estratégia - **Automatizar e prevenir**

Parafraseando o perdido em marte: ***“Precisamos automatizar até fazer bico”.***

Nativo

AWS SCP

AWS Config + Conformance Pack

Azure Policy

GCP Org Policy

Infra as Code

Terraform

Crossplane

Elaborando uma estratégia eficaz

Para escalar a segurança, precisamos aplicar 3 princípios!

1. **Automatizar e prevenir**
2. **Descentralizar**

A estratégia - **Descentralizar**

*“**Segurança é** um esporte **coletivo**: para escalar, **todos precisam jogar**, e no mesmo time”*

- **Criar e promover fóruns de discussão;**
- **Estabelecer metas em comum;**
- **Defina modelos de colaboração entre equipes;**
- **Entregue as ferramentas de segurança nas mãos das equipes;**

Elaborando uma estratégia eficaz

Para escalar a segurança, precisamos aplicar 3 princípios!

1. **Automatizar e prevenir**
2. **Descentralizar**
3. **Educar**

A estratégia - **Educar**

*“O **conhecimento** é o **guardrail** mais **poderoso**: equipes bem preparadas constroem ambientes mais seguros.”*

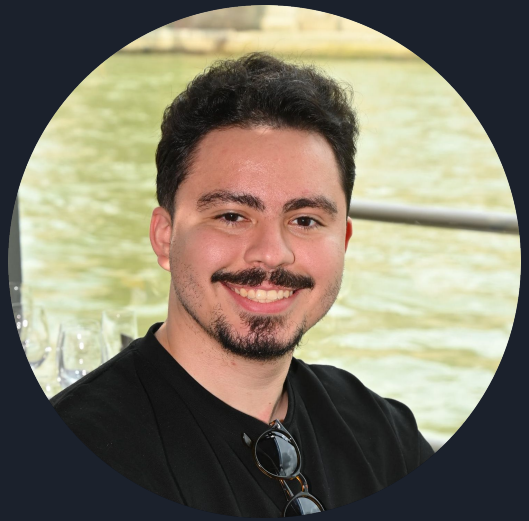
- **Base de conhecimento atualizada;**
- **Workshops, palestras e MeetUps;**
- **Conteúdo gravado;**
- **Treinamentos com fornecedores e fabricantes;**

Por onde começar?

1. Entenda os objetivos estratégicos da sua empresa e de suas lideranças, o quanto estão dispostos a investir e o risco que podem tolerar.
2. Escolha um pilar para começar (Configurações, Identidades ou Aplicações);
3. Desenvolva guardrails (para parar de enxugar gelo), automações para corrigir falhas e templates de IaC para as equipes criarem recursos com segurança desde o início.
4. Engaje, eduque e envolva as equipes de tech que criam recursos em nuvem, para que elas sintam ser responsáveis pela segurança também.

Dúvidas?

Meus contatos



Jonatas Winston

Cloud Security | Cyber Security | Grupo Boticário

Linktr.ee: linktr.ee/wnst

LinkedIn: linkedin.com/in/jonataswinston

Instagram: @jonatas_winson

GitHub: winstonsec / blrvio