HACKING na WEB DAY 2025

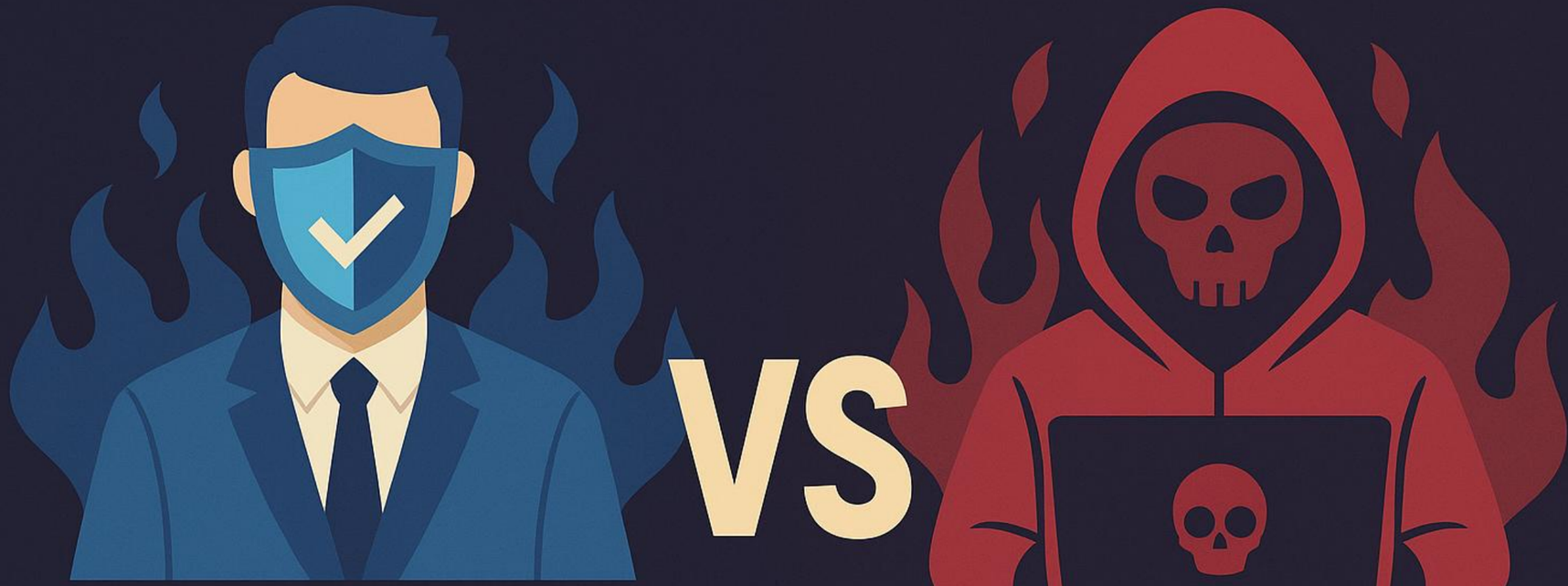
Cloud Moderna ANTI Ataque

Blindagem DevOps Essencial

A proteção que você PRECISA conhecer para sua infraestrutura cloud moderna e pipeline DevOps

Rafael Ferreira

- 10+ anos de XP 👨🏽‍💻
- Senior Platform Engineer
- Algumas Certificações técnicas
- Ciencias da Computação 🎓
- Pós na área de educação
- Host Low0pscast
- Geek, Gamer 🎮
- Filmes 🎬 séries 📺
- Pai de uma golden 🐕


VS
BLUE TEAM
DEFENSE
RED TEAM
ATTACK

Cloud Foundation

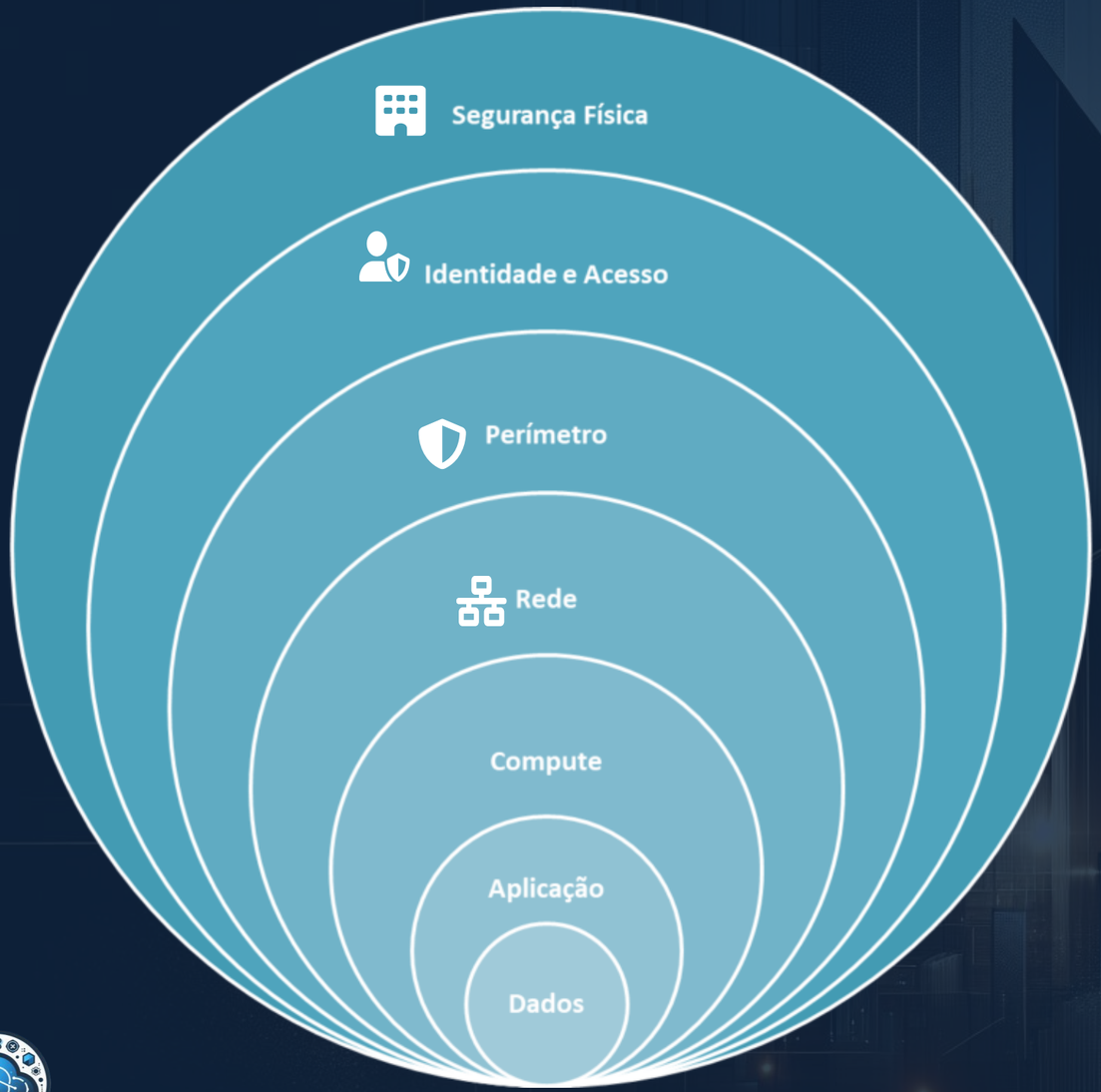
Segurança Base

- Segurança começa na fundação
- Rede estruturada e protegida
- Identidade como perímetro
- Governança
- Monitoramento contínuo

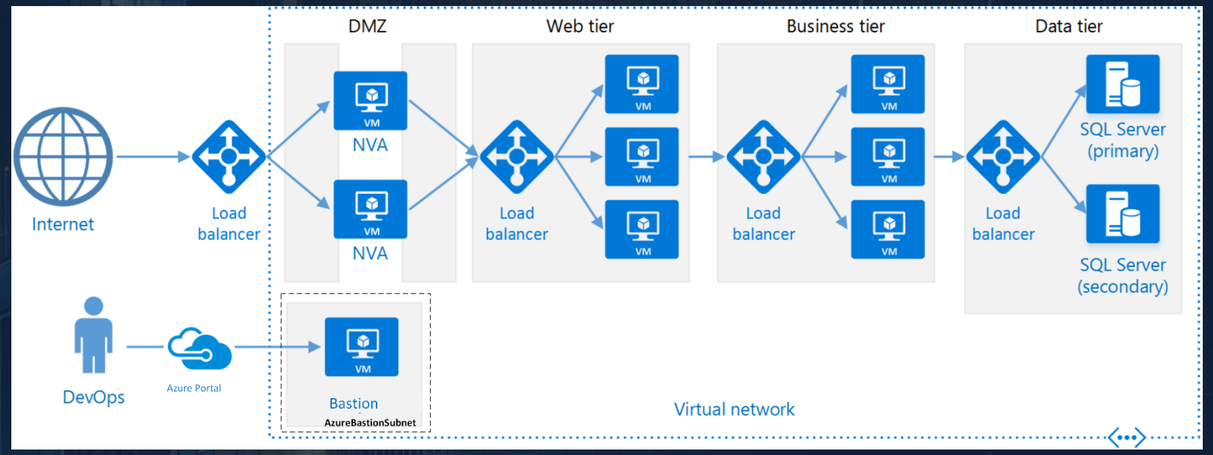
Frameworks Padrão

- Azure Cloud Adoption Framework
- AWS Well-Architected Framework
- Google Cloud Framework
- MCSB - Microsoft Cloud Security Benchmark

Defesa Camadas



Arquitetura em N Camadas



Segurança Física – Provedor

Certificações Padrão

Data centers com certificações rigorosas: ISO 27001 para gestão de segurança, SOC 2 para controles operacionais e PCI-DSS para proteção

Controle Operacional

Acesso físico altamente restrito com múltiplas camadas de autenticação e vigilância 24x7 com monitoramento contínuo e resposta imediata

Identidade e Acesso

Zero
Trust

RBAC
Least Privilege

MFA
Obrigatório

IAM
Centralizado

Microsoft Entra ID

Gerenciando identidades com integração nativa e políticas centralizadas

- Contas de serviço vs. Usuários
- RBAC granular por recursos e subscriptions
- Managed Identities - passwordless

AWS IAM

AWS IAM e Identity Center oferecendo controle de permissões e federação empresarial

- IAM Roles com AssumeRole para acesso temporário Seguro
- Identity Center para SSO federado em organizações
- Cross-account roles com políticas de confiança rigorosas

GCP Identity

Google Cloud IAM com Workload Identity e integração nativa com Google Workspace

- Workload Identity para pods Kubernetes sem secrets
- Organization policies para governança em escala
- Service accounts com rotação automática de chaves

Perimetro - Proteção da Borda

WAF Proteção

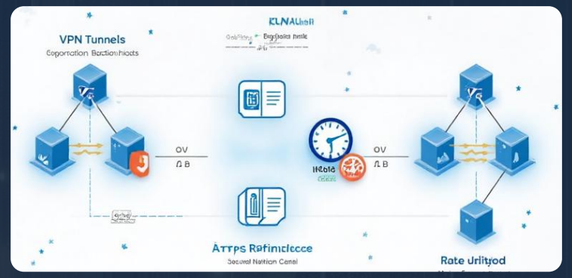
Proteção avançada de borda com Web Application Firewall integrado

- Azure Front Door e WAF integrados
- Filtragem SQLi e XSS automática
- Firewall gerenciando perímetro interno

CDN Shield

Content Delivery Network com proteção DDoS distribuída globalmente

- AWS WAF e Shield Advanced
- Proteção DDoS Layer 3-7 complete
- GCP Armor com CDN integrado



Controle Acesso

Controles de acesso e limitação para exposição mínima controlada

- HTTPS com certificados gerenciados
- Rate Limiting inteligente e adaptativo
- VPN e Bastion para exposição mínima

Rede e Segmentação

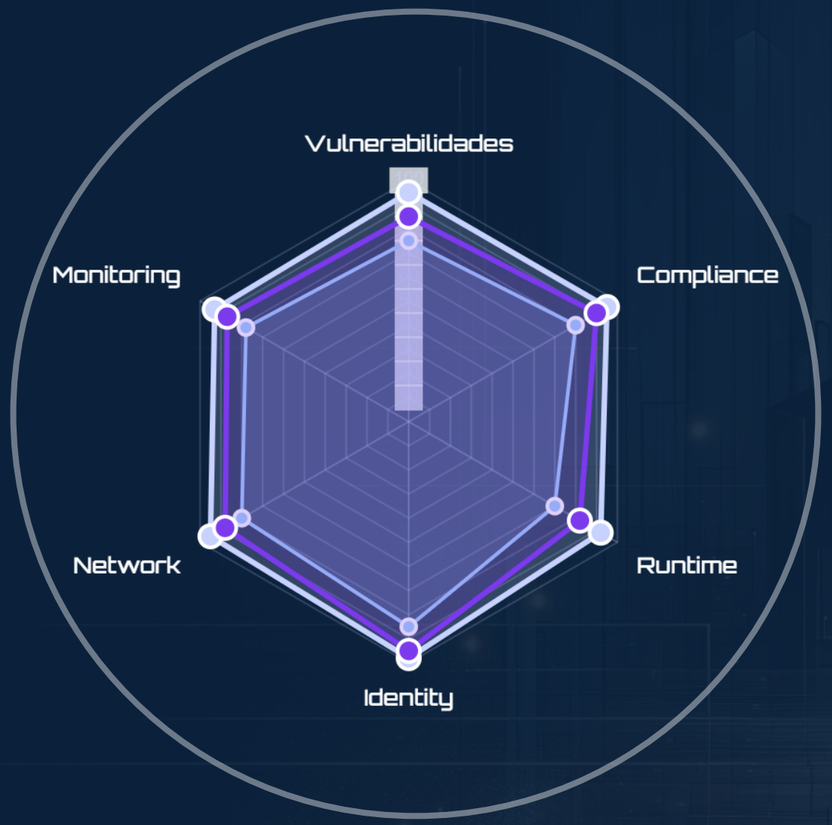
Controles Nativos

Network Security Groups (NSGs) controlando tráfego por sub-rede/VM, Virtual Network Peering com tráfego restrito, Private Link para acesso seguro a serviços PaaS, rotas customizadas (UDR) para inspeção em appliances e Load balancers para distribuição do tráfego.

Proteção Perimetral

Azure Firewall, AWS Network Firewall com proteção anti-DDoS integrada através de Azure DDoS Protection, AWS Shield e GCP Cloud Armor avançado

Compute



Proteção Avançada

Azure Defender, AWS Inspector e GCP OS Config monitoram vulnerabilidades e Azure Policy para governança de VMs e containers

Kubernetes Gerenciado

AKS, EKS e GKE com segurança nativa, RBAC integrado e VNet Integration para isolamento

Serverless Identidade

Managed Identities para Serverless eliminam credenciais expostas e simplificando gestão de permissões

Aplicações

1 Gateway Seguro

APIM, App Services e APIs protegidas atrás do Application Gateway + WAF com SSL/TLS end-to-end

2 Autenticação Moderna

Integração OAuth/OIDC nativa com provedores de identidade e autenticação multi-fator **obrigatória**

3 Gestão Segredos

Azure Key Vault, AWS KMS e GCP Secret Manager para rotação automática e criptografia de credenciais aplicacionais

Dados e Armazenamento

Gestão Chaves

Azure Key Vault, AWS KMS e GCP KMS oferecem gerenciamento centralizado e seguro de chaves criptográficas, certificados , segredos com controles de acesso granulares e rotação automática de chaves.

Criptografia Padrão

Azure Storage Service Encryption, AWS EBS/S3 encryption e GCP CMEK garantem proteção de dados em repouso e trânsito por padrão

Controle e Auditoria

Auditoria completa de acessos com logs detalhados e controle granular de permissões garantindo rastreabilidade total dos dados corporativos

Monitoramento e Resposta

Logs Centralizados

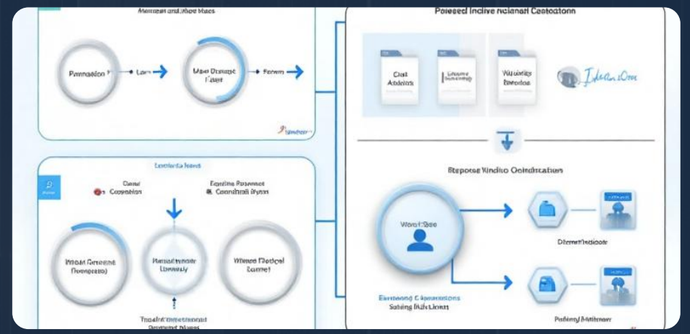
Centralização completa de logs para visibilidade total da infraestrutura

- Azure Monitor com Analytics integrado
- AWS CloudWatch com métricas customizadas
- GCP Cloud Logging com BigQuery

SIEM Inteligente

Inteligência artificial aplicada à segurança para detecção proativa

- Azure Sentinel com ML integrado
- AWS Security Hub centralizado
- GCP Chronicle para análise avançada



Automação Resposta

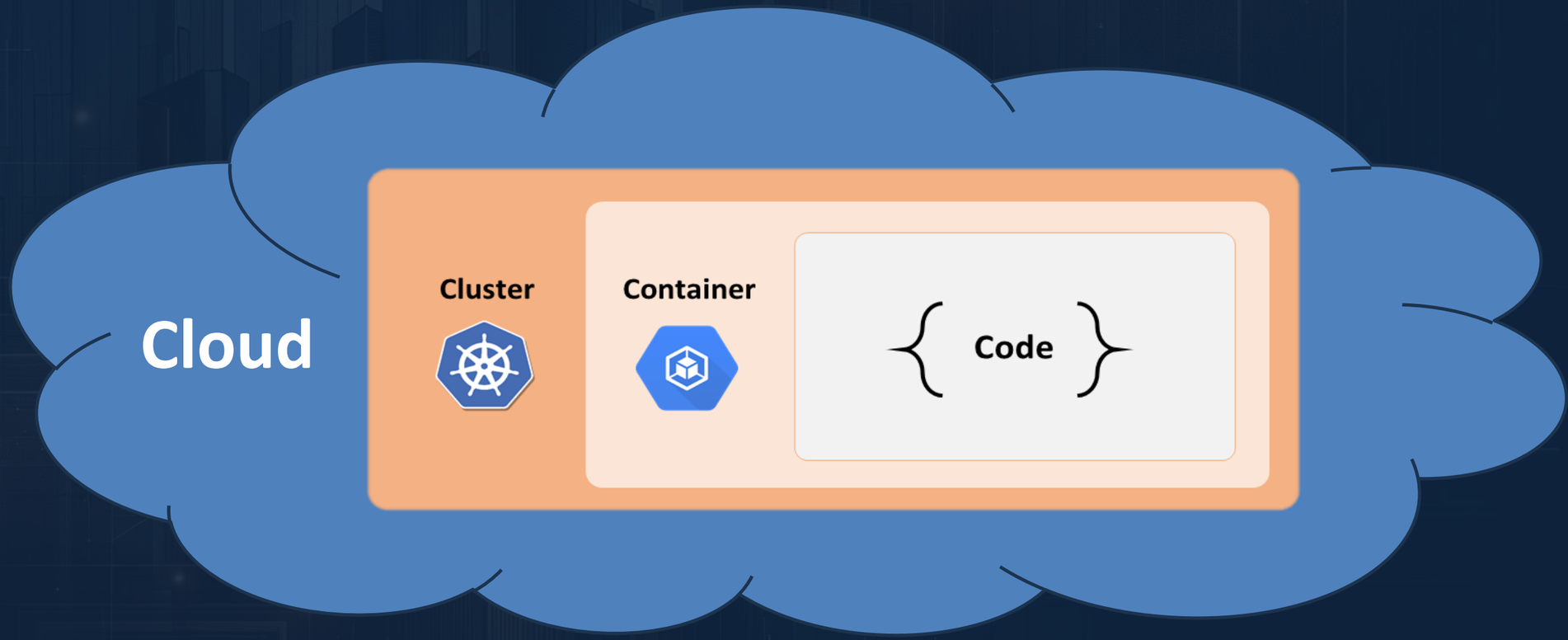
Resposta automatizada para incidentes com tempo de reação mínimo

- Logic Apps para Azure workflows
- AWS Lambda para execução serverless
- GCP Cloud Functions para automação

4 C's Cloud Native Security

Cloud → Cluster → Container → Code

Defesa contínua e integrada em cada camada



Cloud Security Platforms

Microsoft Azure

Azure com Policy, Defender for Cloud e Management Groups para governança centralizada

- Isolamento de Virtual Networks (VNet)
- Identidade Segura - Entra AD (RBAC e Managed Identities)
- Monitoramento contínuo com Azure Monitor
- Detecção e resposta a ameaças com Microsoft Defender for Cloud e Azure Sentinel

Amazon AWS

AWS Config, Organizations e SCP com Security Hub para visibilidade unificada

- Config para auditoria e compliance contínuo
- Organizations com Service Control Policies
- Security Hub para dashboard centralizado

Google Cloud

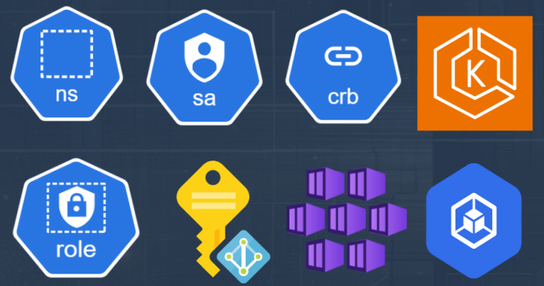
GCP Organization Policies, SCC e IAM para controle granular

- Organization Policies para governança Empresarial
- Security Command Center unificado
- IAM granular com hierarquia recursos

Cluster Kubernetes

Serviços Gerenciados

- Use AKS, EKS, GKE
- RBAC no cluster
- Namespaces separados
- Atualizações automáticas?



Hardening e Compliance

- CIS Benchmark
- Secrets management
- Network Policies
- Private Clusters

Visibilidade Runtime

- Falco para detecção
- Alertas em tempo real
- Audit logs habilitados
- Monitoring avançado

Containers

Proteção Multicamada

Imagens Seguras

Imagens distroless atualizadas com scan contínuo via Trivy/Grype/Snyk, assinatura digital com Cosign e registro privado com controle de acesso granular

Políticas Restritivas

OPA - Open Policy Agent e Gatekeeper/ Kyverno forçam políticas de segurança, execução não-root obrigatória e limites rigorosos de recursos computacionais

Gestão Segredos

Integração nativa com Key Vault e HashiCorp Vault eliminam credenciais hardcoded e implementando rotação automática de senhas

Código Seguro

🔁 Shift Left

- Integre segurança nas fases iniciais do desenvolvimento
- Use SAST (Static Application Security Testing) nas pipelines.
- Ferramentas: SonarQube, semgrep.

🧪 Testes Dinâmicos (DAST)

- Execute testes dinâmicos de segurança em ambientes de stage/pre-prod.
- Automatize o OWASP ZAP no pipeline.
- Inclua fuzzing e testes de API automatizados.
- Identifique libs desatualizadas ou maliciosas - OWASP Dependency-Check, npm audit, pip-audit, Snyk.

🔑 Verificação de Segredos no Código

- Implemente scanners de segredos no repositório e pipeline.
- Ferramentas: Gitleaks, TruffleHog.
- Use pre-commit hooks para bloquear commits com credenciais.

Falando de IaC

DevSecOps Pipeline - CS

Terra Docs

TFlint

sonarqube

Infracost

aqua tfsec

Terratest by Gruntwork.io

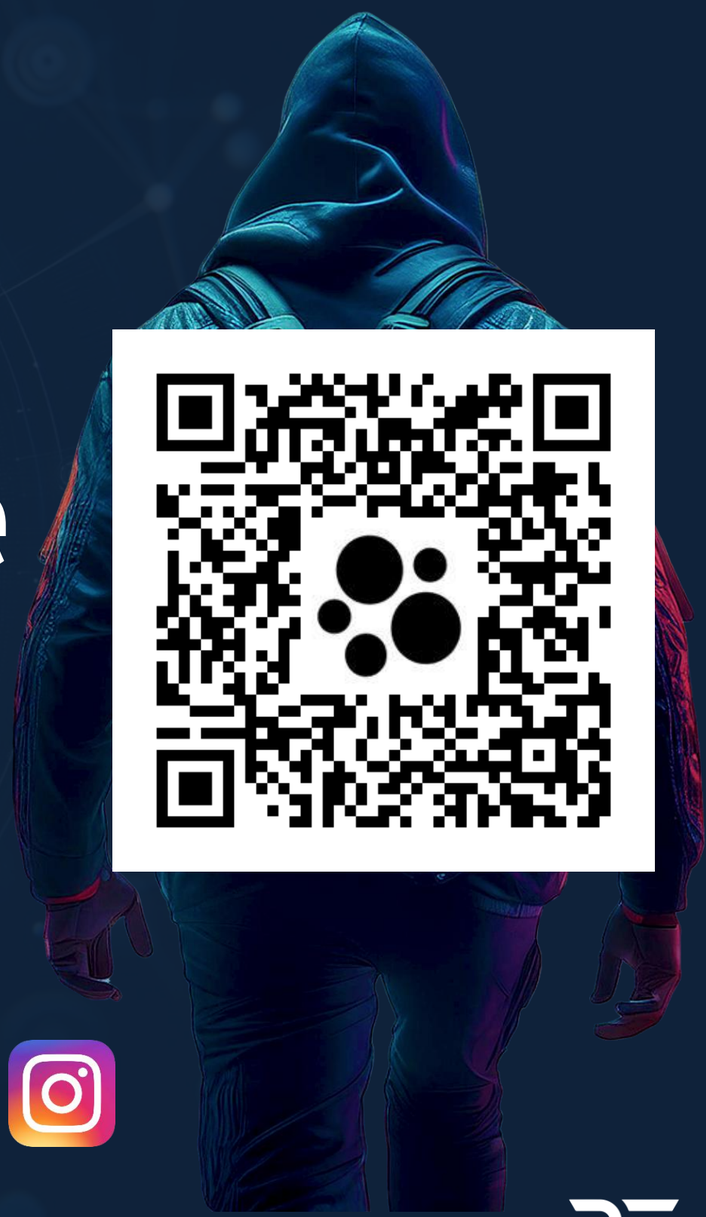
aqua trivy

checkov


SEGURANÇA ACIMA DE TUDO

HACKING 2025 na WEB DAY

Vocês podem me encontrar em



orafaelferreira