O Lado Ofensivo da Nuvem

táticas de ataque em on-prem, híbrido e multi-cloud

*E se o **próximo ataque** viesse da sua **própria pipeline**?*

CodeIsland CLOUD 2025

PATROCINADORES:

DRAGONBD NE0B1TS SOLUÇÕES EM TECNOLOGIA KuberLink CLOUD SOLUTIONS API4COM dati

Leandro Venâncio

https://linktr.ee/leandro.venancio

Who am I?

Prof. Leandro **Venâncio**

Pai da **Laura** e está chegando mais N.

Arquiteto em Segurança de Aplicação e Nuvem

Profissional com mais de 25 anos de experiência no mercado da tecnologia. Amplo conhecimento em segurança da informação, privacidade de dados, desenvolvimento seguro e computação em nuvem.

Possui MBA em Gestão da segurança da informação, cursando pós-graduação em Ethical Hacking e Cyber Security, pós-graduação em Lei Geral de Proteção de Dados.

Especialista em Gestão de Tecnologia da informação, Desenvolvimento Orientado a Objetos em Java e em Gestão da Informação e Inteligência nos Negócios (Business Intelligence).

Encorajo e incentivo aos participantes a continuarmos esse papo através das minhas redes sociais.

Avisos Legais

Meu empregador **não tem qualquer responsabilidade** sobre o que iremos tratar durante essa apresentação.

Este material foi elaborado exclusivamente para o **Code Island Cloud 2025**, e qualquer informação nele contida não deve ser reproduzida, divulgada ou publicada sem a devida atribuição, menção aos **direitos autorais** e propósito para o qual foi desenvolvido.

Este documento é destinado aos que desejam **aprofundar seus conhecimentos** em segurança da informação.

Fonte: https://img.freepik.com/premium-vector/red-disclaimer-sign-badge-icon-vector-illustration_100456-9686.jpg

Público-alvo

Objetivos

- **Compreender** vetores on-prem → híbrido → multi-cloud.
- **Encontrar** padrões de falhas recorrentes, em
  - identidade;
  - configuração;
  - CI/CD;
  - supply chain (sbom).
- **Playbook** defensivo prático com ações de alto impacto.

Panorama: por que o problema cresce?

- **Adoção** híbrida e multi-cloud = mais pontos.
- **Automação** e **N**on-**h**uman **I**dentities (**NHIs**) (service accounts, bots) proliferam credenciais.
- **Pipelines** e **registries**.

Superfície de ataque

- **Diagrama**:

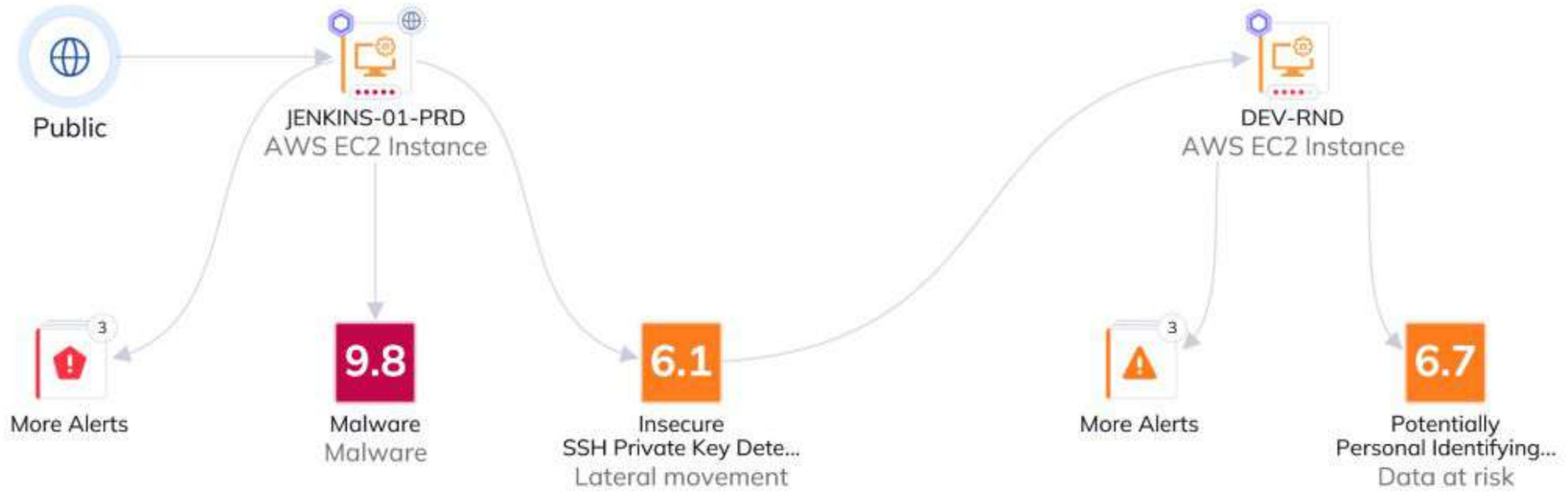
  AD/IdP, Endpoints on-prem, Jump Host, CI/CD, Artifact Registry, Conta Cloud, Cluster Kubernetes.

- **Jóia da coroa**:

  tokens/credenciais, pipelines, rede, dependências

Superfície de ataque

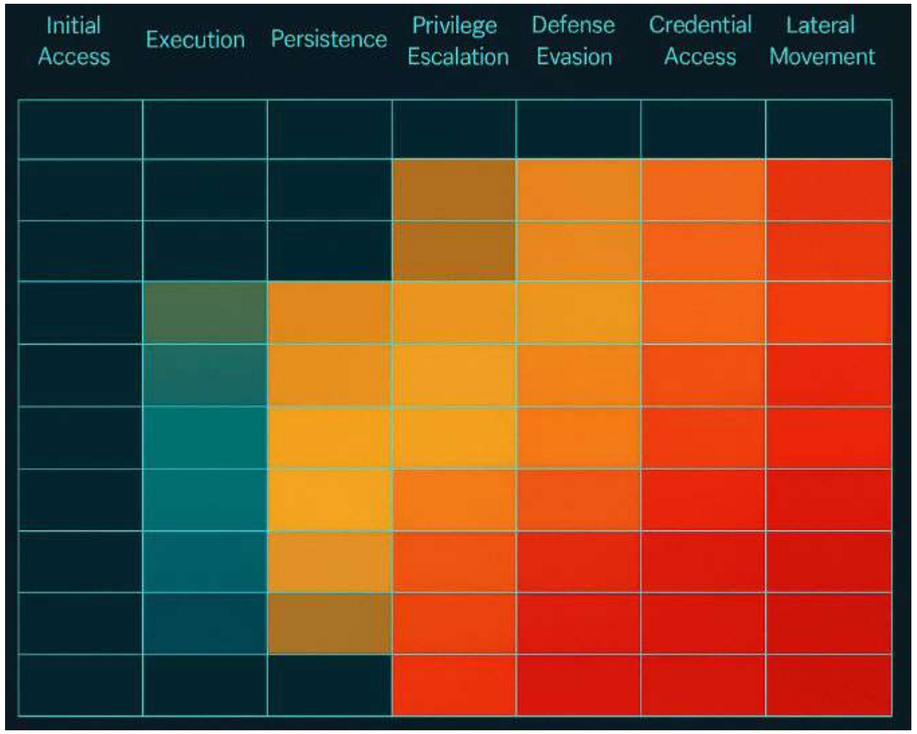
diagrama



Como usar MITRE ATT&CK

for Cloud

- **Catálogo** de comportamentos (recon, persistência, evasão)
- **Usar** para threat modelling, e;
- **Mapear** gaps de detecção.



DRAGONBD

NE0B1TS
SOLUÇÕES EM TECNOLOGIA

KuberLink
CLOUD SOLUTIONS

API4COM

dati

Vetor

identidade & tokens

- **Problemas**: privilégios excessivos; service principals com segredos; tokens long-lived.
- **Indicadores**: uso de credenciais fora de horários, tokens rotacionados raramente.
- **Mitigações**: short-lived creds; MFA; inventário de NHIs.

Vetor

Configuração & Rede

- **Problemas**: buckets públicos, ACLs permissivas, peering mal segmentado.
- **Indicadores**: tráfego cross-account inesperado, downloads massivos de buckets.
- **Mitigações**: IaC review gates, políticas de deny public, network segmentation.

DRAGONBD

NE0B1TS
SOLUÇÕES EM TECNOLOGIA

KuberLink
CLOUD SOLUTIONS

API4COM

dati

Vetor

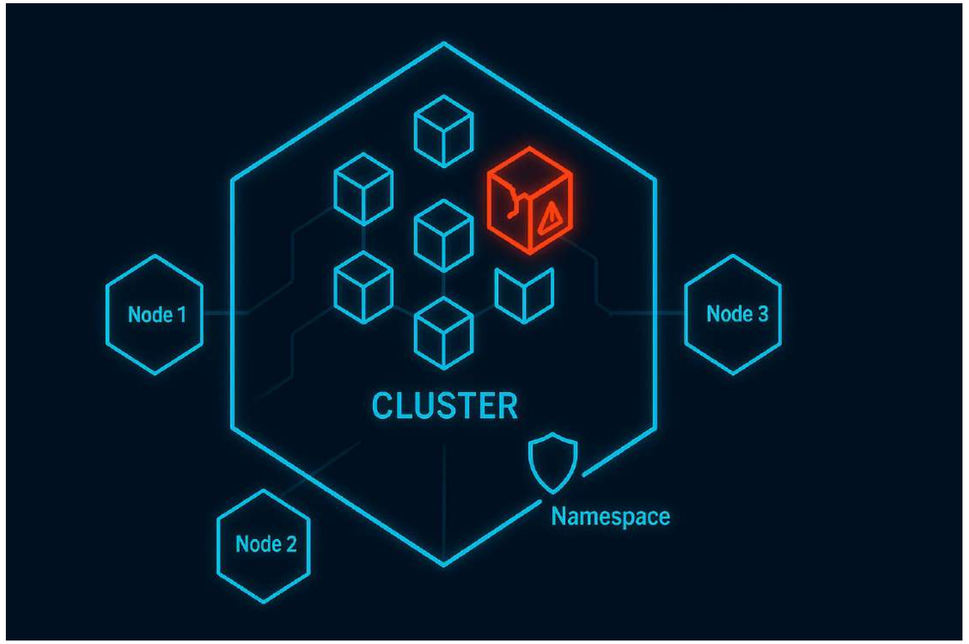
CI/CD & Supply Chain

- **Problemas**: secretos em claro; imagens não assinadas; dependências vulneráveis.
- **Indicadores**: artefatos deployados por contas inativas, mudanças em pipeline sem PR.
- **Mitigações**: signing, SBOM, scanning automatizado, segredos em vaults.

Vetor

Runtime, Containers & Kubernetes

- **Problemas**: RBAC permissivo; pods privilegiados; imagens não verificadas.
- **Indicadores**: criação de pods com capabilities elevadas; execs remotos incomuns.
- **Mitigações**: admission controllers, image attestation, runtime EDR.



DRAGONBD

NE0B1TS
SOLUÇÕES EM TECNOLOGIA

KuberLink
CLOUD SOLUTIONS

API4COM

dati

Attack path

walkthrough

Case:

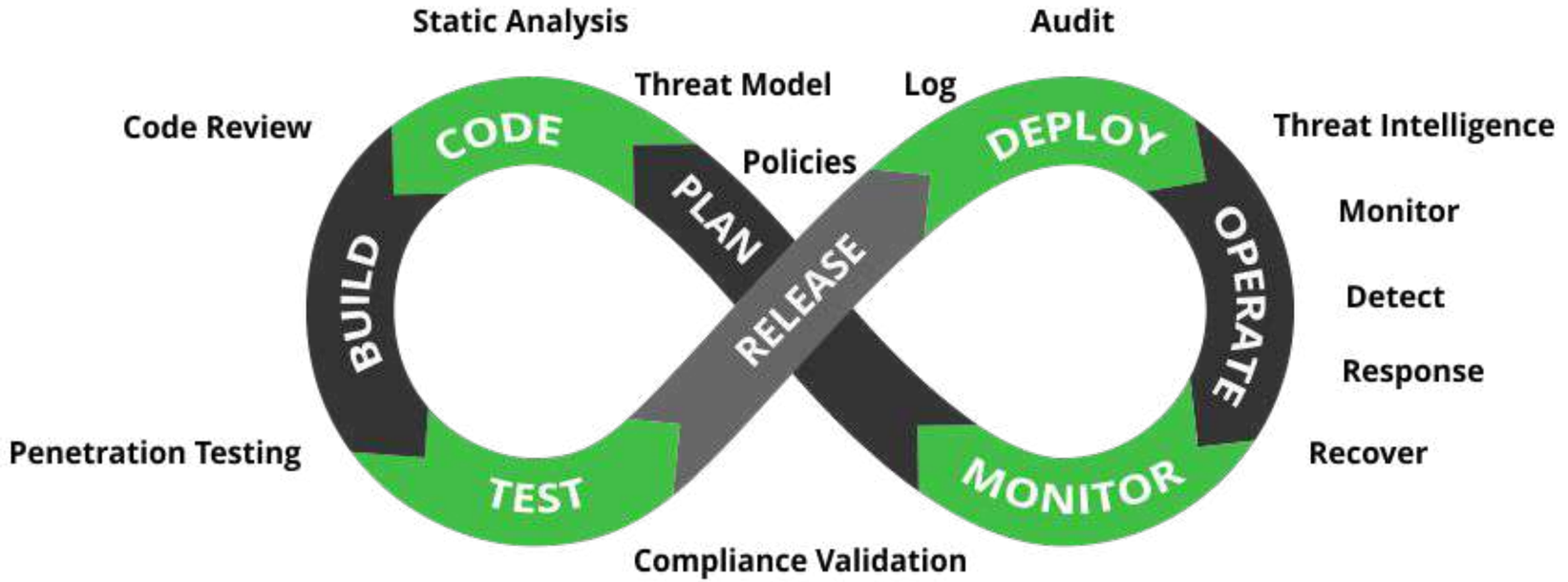
1. Um **colaborador** faz download de artefato em laptop pessoal;
2. O **malware** exfiltra o token do CI local;
3. O **token** é usado para **disparar job** com credenciais do pipeline;
4. O **job** injeta imagem maliciosa no registry;
5. A **imagem** é promovida e roda em produção.

Onde teríamos barrado esse ataque?

IdP, controle de pipeline, gates de IaC, verificação de imagens, cada um é um ponto de quebra.

Attack path

walkthrough



DRAGONBD

NE0B1TS
SOLUÇÕES EM TECNOLOGIA

KuberLink
CLOUD SOLUTIONS

API4COM

dati

Playbook defensivo

6 ações

- **Inventário** e **classificação** de identidades (humanas e NHIs);
- **Rotacionar** credenciais de curta duração + MFA no IdP;
- **Bloqueio** "no-public" por padrão para buckets e registries;
- **Segredos** centralizados em Vault; remover credenciais das pipelines;
- **Signing** & **SBOM** nos artefatos de CI/CD;
- **Telemetria focal**: logs de identidade, auditoria de API, EDR para containers/VMs.

Métricas & KPIs sugeridos

- Tempo médio de rotação de credenciais (dias)
- % de pipelines com scanning & signing
- % de workloads com menor privilégio (least privilege)
- Nº de alertas acionáveis por semana (identidade e runtime)

DRAGONBD

NE0B1TS
SOLUÇÕES EM TECNOLOGIA

KuberLink
CLOUD SOLUTIONS

API4COM

dati

Exercício

- **Objetivo**: validar cadeia IdP → CI → Deploy em 1 dia;
- **Escopo**: 1 app, 1 pipeline, 1 conta cloud não-prod;
- **Critério de sucesso**: detecção e rollback automático

Recursos

Complementares

- **MITRE ATT&CK** for Cloud;
- **C**loud **S**ecurity **A**lliance – **CSA** (Top Threats);
- **Whitepapers** sobre **Supply-Chain Security** (SBOM, signing);
- Ferramentas de attack-path / exposure management.

Ataques recentes

Brasil registra 315 bilhões de tentativas de ataques cibernéticos somente em 2025, aponta Fortinet

No primeiro semestre deste ano, América Latina foi alvo de 374 bilhões de tentativas de ataques cibernéticos, dos quais 84% foram no Brasil

Dados integram o relatório Cenário Global de Ameaças, elaborado pela empresa sobre o comportamento cibernético na região (krisanapong detraphiphat/Getty Images)

Após ataques de hackers, BC anuncia limites para transferências via PIX e regras mais rígidas para autorização de novas instituições

Instituições de pagamento não autorizadas terão limites de R$ 15 mil para TED e PIX. Para Banco Central, crime organizado tem relação com recentes ataques ao sistema.

Por Alexandro Martello, g1 — Brasília
05/09/2025 10h56 · Atualizado há 2 semanas

DRAGONBD

NE0B1TS
SOLUÇÕES EM TECNOLOGIA

KuberLink
CLOUD SOLUTIONS

API4COM

dati

Reflexão

A cibersegurança é uma questão importante, e que deve ser **levada a sério** por todas as organizações.

Tendo como premissa a **mitigação dos incidentes**, para **proteção do** seu **patrimônio** físico, digital e ajudando a manter a sociedade segura.

Fonte: https://images.pexels.com/photos/5380646/pexels-photo-5380646.jpeg?auto=compress&cs=tinysrgb&w=1260&h=750&dpr=1

DRAGONBD

NE0B1TS
SOLUÇÕES EM TECNOLOGIA

KuberLink
CLOUD SOLUTIONS

API4COM

dati

Obrigado!

Code Island CLOUD 2025

Redes sociais

PATROCINADORES:

DRAGONBD NE0B1TS SOLUÇÕES EM TECNOLOGIA KuberLink CLOUD SOLUTIONS API4COM dati

Leandro Venâncio

https://linktr.ee/leandro.venancio