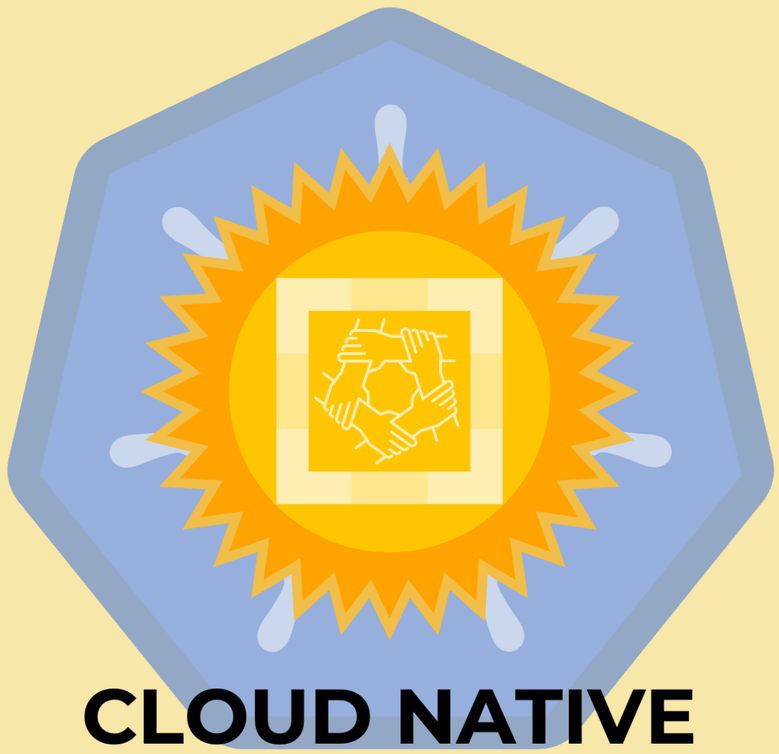


CLOUD NATIVE
COMMUNITY GROUPS
ARARAQUARA - SP

Da Comunidade ao Ambiente Produtivo: Segurança em Kubernetes com Ferramentas Open Source

Código de conduta da comunidade

CLOUD NATIVE
COMMUNITY GROUPS
ARARAQUARA - SP

Lembre-se sempre de respeitar o código de conduta da comunidade

Agenda

- Parte 1
  - Quem somos nós?
  - Nuvem? OpenSource? Segurança?
  - Como a roda gigante não para de girar
  - Q&A

- Parte 2
  - Ferramentas OpenSource de Segurança
  - Trivy
  - KubeSec
  - Falco
  - Q&A

Quem somos nós?

CLOUD NATIVE
COMMUNITY GROUPS
ARARAQUARA - SP

Giovani Martins

5by5

Henrique Polsani

Nubank

Jean Carlos

5by5

Matheus Ulisses

Hapvida NotreDame Intermédica

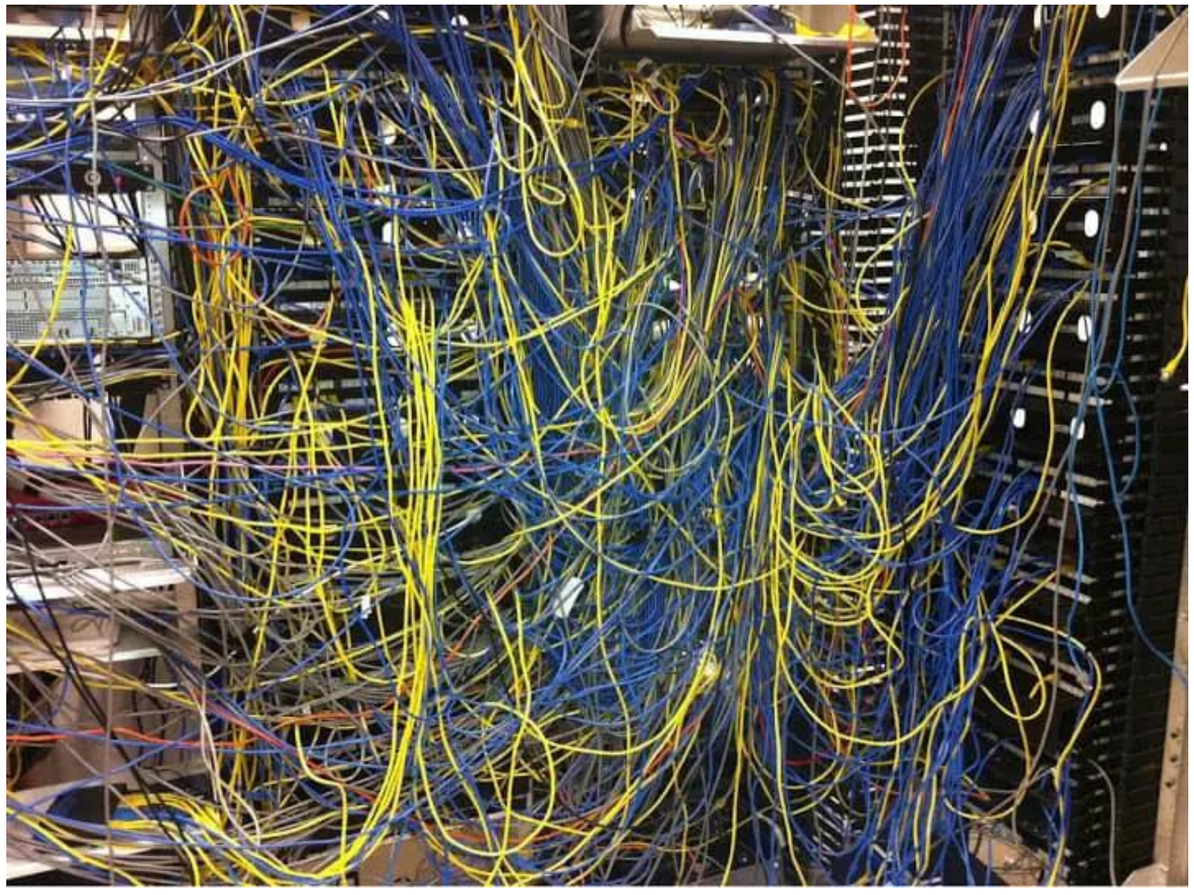
Núvem – Como era feito antigamente?

E em algumas empresas até hoje rs

CLOUD NATIVE
COMMUNITY GROUPS
ARARAQUARA - SP

OnPremise

- Infraestrutura Própria
- Controle Total (Hardware, SO, Redes, etc)
- Provisionamento Manual ou Automatizado
- Escalabilidade Vertical*
- Rede Interna
- Segurança Perimetral
- Responsabilidade Total pela Manutenção
- Investimento Inicial Elevado (CAPEX)
- Custos Operacionais (OPEX)
- Ciclos de Deploy Mais Longos

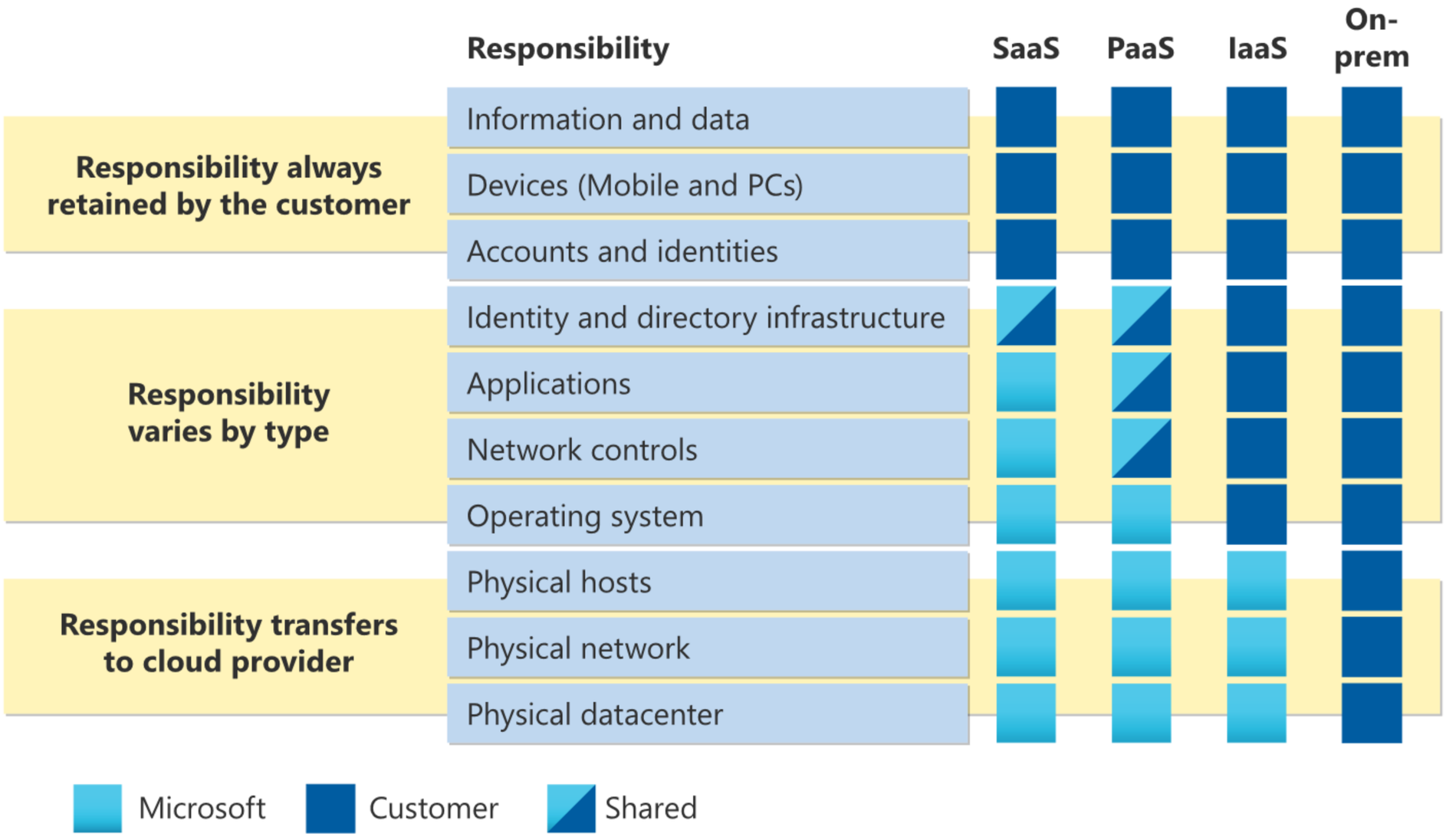


Núvem – A magia dos recursos “infinitos”

Cloud

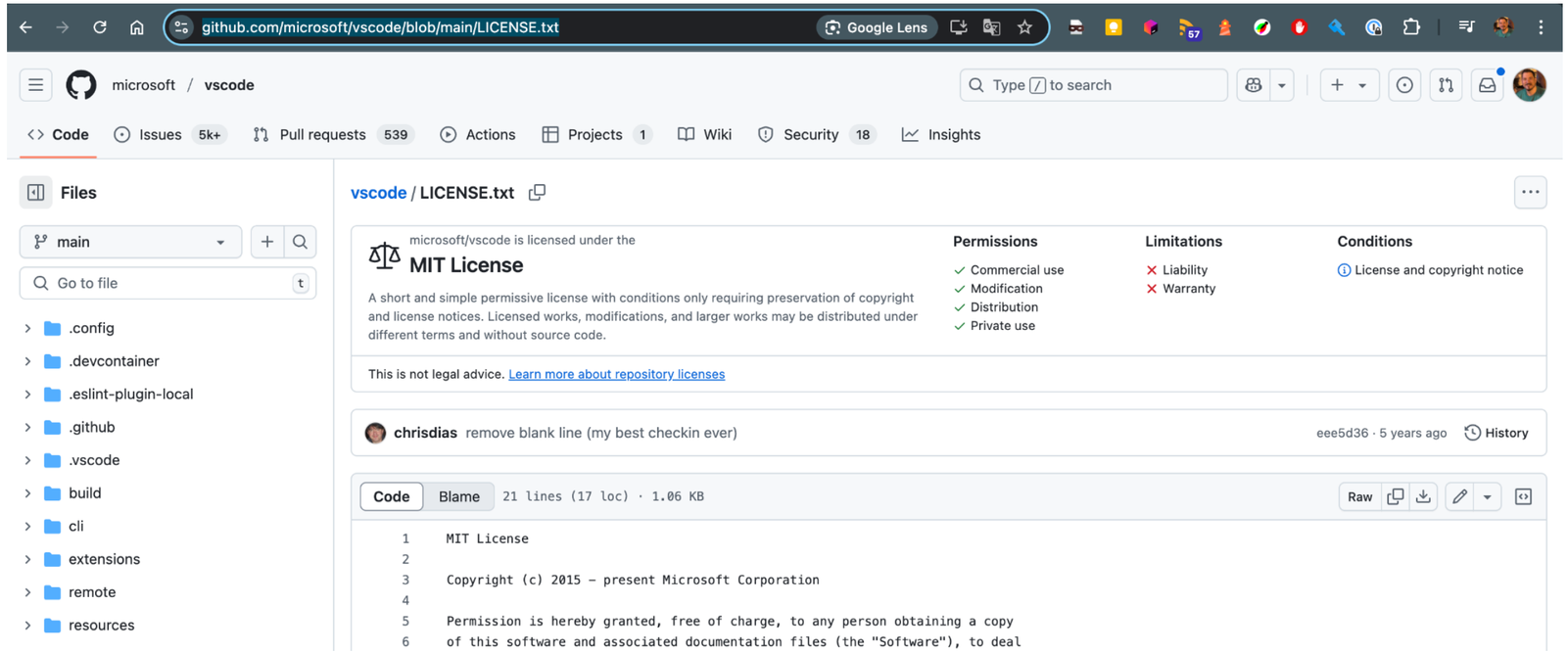
- Infraestrutura como Serviço *
- Menos Controle Direto
- Provisionamento Sob Demanda e Elástico
- Escalabilidade Horizontal (Principalmente)
- Rede Pública e Virtual
- Segurança Compartilhada
- Manutenção Gerenciada (Parcialmente ou Totalmente
- Baixo Investimento Inicial (OPEX)
- Custos Operacionais (OPEX)
- Ciclos de Deploy Mais Rápidos*

Núvem - Tipos de contratações



OpenSource

- O que são projetos Open Source
- Open Source = Grátis?
- Quais as vantagens de se utilizar um projeto Open Source?
- O que preciso prestar atenção ao utilizar um projeto na empresa que trabalho?
  - (https://github.com/microsoft/vscode/blob/main/LICENSE.txt)
- Como contribuir?



Linha do tempo

CLOUD NATIVE
COMMUNITY GROUPS
ARARAQUARA - SP

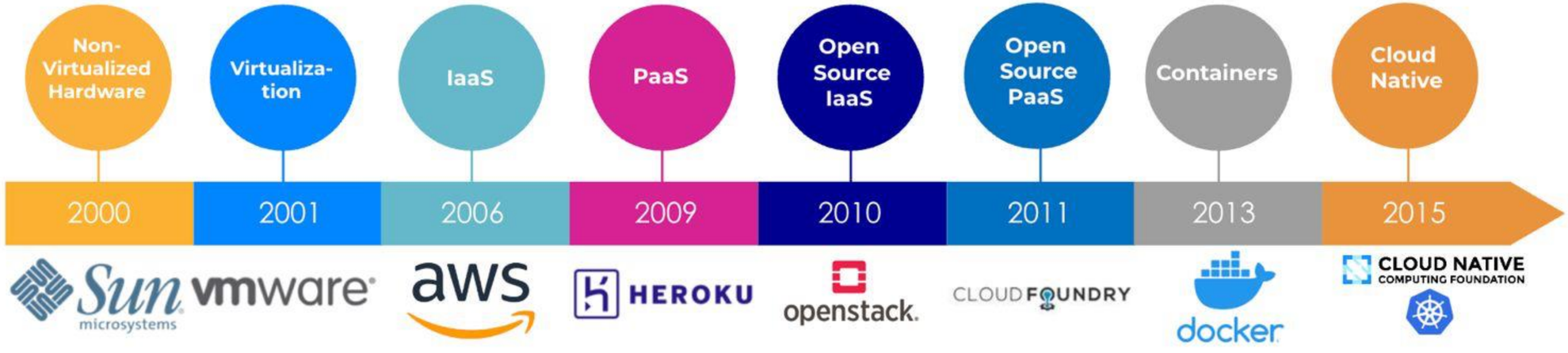
From Virtualization to Cloud Native

CLOUD NATIVE COMPUTING FOUNDATION

THE LINUX FOUNDATION

kubernetes

landscape.cncf.io



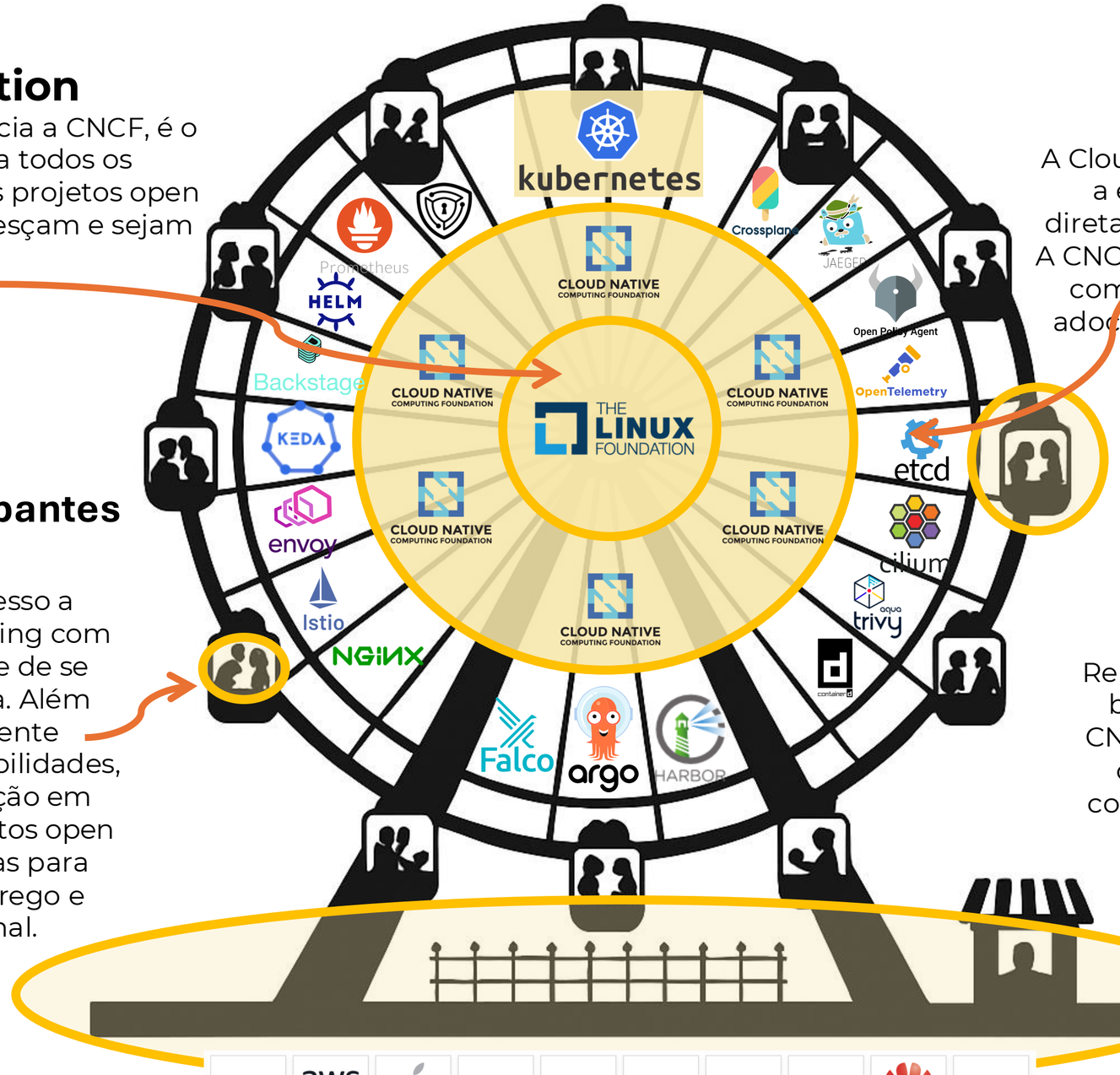
Security Team Sees Kubernetes

Linux Foundation

A Linux Foundation, que gerencia a CNCF, é o centro da roda. Ela conecta todos os participantes e assegura que os projetos open source, como o Kubernetes, cresçam e sejam sustentáveis.

Contribuidores/Participantes de eventos

Os participantes ganham acesso a aprendizado contínuo, networking com outros profissionais e a chance de se envolver em projetos de ponta. Além disso, os CGs são uma excelente plataforma para desenvolver habilidades, como programação, colaboração em equipe, e participação em projetos open source, que podem abrir portas para novas oportunidades de emprego e reconhecimento profissional.



CNCF

A Cloud Native Computing Foundation (CNCF) é a estrutura da roda gigante, que conecta diretamente as empresas e a comunidade local. A CNCF organiza e promove o uso de tecnologias como Kubernetes, ajudando a impulsionar a adoção e inovação na computação em nuvem.

CLOUD NATIVE COMMUNITY GROUPS ARARAQUARA - SP

Community Groups

Representando as comunidades locais que se beneficiam diretamente das iniciativas da CNCF. Eles organizam meetups, workshops e outros eventos para promover a troca de conhecimentos sobre tecnologias de nuvem, como o Kubernetes.

Empresas Patrocinadoras

Elas fornecem o suporte financeiro e estratégico que permite que toda a estrutura funcione.

Community Groups

- O que são Community Groups
- Porque criamos um CG em Araraquara
- Outros CG pelo Brasil e pelo mundo
  - https://community.cncf.io/

CLOUD NATIVE ARARAQUARA, SP
Brazil

CLOUD NATIVE AREQUIPA
Peru

CLOUD NATIVE AYACUCHO
Peru

CLOUD NATIVE BELO HORIZONTE, MG
Brazil

CLOUD NATIVE BRASÍLIA
Brazil

CLOUD NATIVE BUENOS AIRES
Argentina

CLOUD NATIVE COLOMBIA

CLOUD NATIVE COSTA RICA, HEREDIA PROVINCE
Costa Rica

CLOUD NATIVE CUENCA, AZUAY
Ecuador

CLOUD NATIVE CURITIBA, PR
Brazil

CLOUD NATIVE FORTALEZA, CE
Brazil

CLOUD NATIVE GOIÂNIA, GO
Brazil

CLOUD NATIVE GUADALAJARA, JAL.
Mexico

CLOUD NATIVE GUATEMALA GROUPS
Guatemala

CLOUD NATIVE JUIZ DE FORA, MG
Brazil

CLOUD NATIVE LATAM, CDMX

CLOUD NATIVE LIMA
Peru

CLOUD NATIVE MANAGUA, MN
Nicaragua

CLOUD NATIVE PEREIRA, RISARALDA
Colombia

CLOUD NATIVE QUERETARO, QRO.
Mexico

CLOUD NATIVE RIO GRANDE DO NORTE, RN
Brazil

CLOUD NATIVE RIO DE JANEIRO, RJ
Brazil

CLOUD NATIVE SALVADOR, BAHIA, BA
Brazil

CLOUD NATIVE SAN JUAN
Puerto Rico

CLOUD NATIVE SAN SALVADOR, SAN SALVADOR DEPARTMENT
El Salvador

CLOUD NATIVE SANTA CATARINA, SC
Brazil

CLOUD NATIVE SANTIAGO
Chile

CLOUD NATIVE SANTO DOMINGO, DISTRITO NACIONAL
Dominican Republic

CLOUD NATIVE SÃO PAULO CITY
Brazil

CLOUD NATIVE VALE DO PARAÍBA, SP
Brazil

SAST vs. DAST: O que é e qual a diferença?

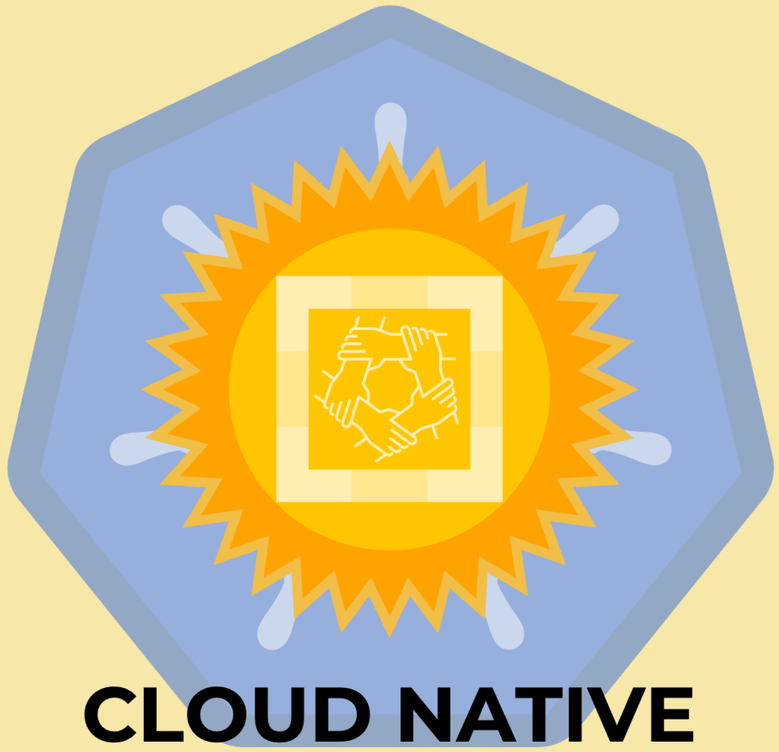
CLOUD NATIVE
COMMUNITY GROUPS
ARARAQUARA - SP

SAST (Static Application Security Testing)

- Analisa o código-fonte sem executá-lo.
- Detecta vulnerabilidades como SQL Injection e XSS.
- Ideal para identificar problemas logo no início do desenvolvimento.

DAST (Dynamic Application Security Testing)

- Testa a aplicação em execução.
- Simula ataques externos para encontrar falhas de segurança.
- Útil para identificar vulnerabilidades que só aparecem em tempo de execução.



CLOUD NATIVE

COMMUNITY GROUPS
ARARAQUARA - SP

Linktree

Q&A

Trivy: Scanner de vulnerabilidades Open Source

- Desenvolvido pela Aqua Security.
- Ferramenta de linha de comando simples e eficiente.
- Realiza análises de segurança em:
  - Imagens de containers
  - Sistemas de arquivos
  - Repositórios Git
  - Scripts de infraestrutura como código (OpenTofu).

Como o Trivy realiza análises de vulnerabilidades ?

- **Imagens Docker**: Verifica pacotes do sistema operacional e dependências da aplicação.
- **Repositórios Git**: Analisa arquivos como package-lock.json para identificar dependências vulneráveis.
- **Sistemas de Arquivos**: Escaneia diretórios locais em busca de vulnerabilidades.
- **IaC**: Detecta configurações inseguras em arquivos como OpenTofu e Kubernetes.

Onde e como utilizar o Trivy

CLOUD NATIVE
COMMUNITY GROUPS
ARARAQUARA - SP

- **Localmente (CLI):** Instalação simples via gerenciadores de pacotes.
- **Via Docker**: Execução sem necessidade de instalação.
- **Operator no Kubernetes**: Monitoramento contínuo de imagens em clusters Kubernetes.
- **Pipelines CI/CD**: Integração com ferramentas como GitHub Actions, GitLab CI, Jenkins.

Exemplo de execução do Trivy

CLOUD NATIVE
COMMUNITY GROUPS
ARARAQUARA - SP

```
/opt/hostedtoolcache/trivy/0.61.1/x64/trivy image --exit-code 2 --format json --scanners secret,vuln,misconfig --list-all-pkgs --ignore-unfixed --output /home/vsts/work/_temp/trivy/t
2025-04-22T21:54:49Z    INFO    [vuln] Vulnerability scanning is enabled
2025-04-22T21:54:49Z    INFO    [misconfig] Misconfiguration scanning is enabled
##[warning]Issues found.
2025-04-22T21:54:49Z    INFO    [secret] Secret scanning is enabled
2025-04-22T21:54:49Z    INFO    [secret] If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2025-04-22T21:54:49Z    INFO    [secret] Please see also https://trivy.dev/v0.61/docs/scanner/secret#recommendation for faster secret detection
2025-04-22T21:54:59Z    INFO    Detected OS     family="debian" version="11.11"
2025-04-22T21:54:59Z    INFO    [debian] Detecting vulnerabilities...   os_version="11" pkg_num=153
2025-04-22T21:54:59Z    INFO    Number of language-specific files       num=1
2025-04-22T21:54:59Z    INFO    [dotnet-core] Detecting vulnerabilities...
2025-04-22T21:54:59Z    INFO    Detected config files   num=0
2025-04-22T21:54:59Z    WARN    Using severities from other vendors for some vulnerabilities. Read https://trivy.dev/v0.61/docs/scanner/vulnerability#severity-selection for details.
Generating reports...
/opt/hostedtoolcache/trivy/0.61.1/x64/trivy convert --format sarif --output /home/vsts/work/_temp/trivy/trivy-results-c928e652-3207-4422-b9f1-aef2598e4fa2.sarif.json /home/vsts/work
```

Exemplo de execução do Trivy

Vulnerabilities 30

Severity ↓	ID	Package	Title
CRITICAL	CVE-2024-0057	NuGet.Packaging	dotnet: X509 Certificates - Validation Bypass across Azure
CRITICAL	CVE-2021-24112	System.Drawing.Common	dotnet: Remote Code Execution Vulnerability
CRITICAL	CVE-2024-0057	NuGet.Packaging	dotnet: X509 Certificates - Validation Bypass across Azure
CRITICAL	CVE-2021-24112	System.Drawing.Common	dotnet: Remote Code Execution Vulnerability
CRITICAL	CVE-2024-0057	NuGet.Packaging	dotnet: X509 Certificates - Validation Bypass across Azure
CRITICAL	CVE-2021-24112	System.Drawing.Common	dotnet: Remote Code Execution Vulnerability
CRITICAL	CVE-2024-21386	Microsoft.AspNetCore.App...	dotnet: Denial of Service in SignalR server
HIGH	CVE-2022-41032	NuGet.Commands	dotnet: Nuget cache poisoning on Linux via world-writable cache directory
HIGH	CVE-2023-29337	NuGet.Commands	dotnet: vulnerability exists in NuGet where a potential race condition can lead to a symlink attack
HIGH	CVE-2023-29337	NuGet.Common	dotnet: vulnerability exists in NuGet where a potential race condition can lead to a symlink attack
HIGH	CVE-2022-41032	NuGet.Protocol	dotnet: Nuget cache poisoning on Linux via world-writable cache directory
HIGH	CVE-2023-29337	NuGet.Protocol	dotnet: vulnerability exists in NuGet where a potential race condition can lead to a symlink attack
HIGH	CVE-2022-41032	NuGet.Commands	dotnet: Nuget cache poisoning on Linux via world-writable cache directory

KUBESEC.IO: Análise de Segurança para Recursos Kubernetes

CLOUD NATIVE
COMMUNITY GROUPS
ARARAQUARA - SP

- Scanner de Segurança Estático
- Foco em Melhores Práticas de Segurança
- Identifica Vulnerabilidades e Riscos de Configuração
- Feedback Precoce
- Não Interfere na Operação do Cluster

Como o Kubesec ajuda no dia a dia

CLOUD NATIVE
COMMUNITY GROUPS
ARARAQUARA - SP

- Segurança Proativa
- Prevenção de Erros de Configuração
- Melhora a Postura de Segurança
- Reduz Riscos e Custos
- Integração Flexível
- Aprendizado e Conscientização

Como usar o Kubesec

- Imagem Docker

```
$ docker run -i kubesec/kubesec:512c5e0 scan /dev/stdin < kubesec-test.yaml
```

- Kubesec-as-a-Service (curl https)

```
$ curl -sSX POST --data-binary @"k8s-deployment.yaml" https://v2.kubesec.io/scan
```

- Binário (Linux/MacOS/Win)
- Kubectl plugin

```
$ kubesec scan k8s-deployment.yaml
```

- Kubernetes Admission Controller

Como usar o Kubesec

- Exemplo de Report


```
[
  {
    "object": "Pod/security-context-demo.default",
    "valid": true,
    "message": "Failed with a score of -30 points",
    "score": -30,
    "scoring": {
      "critical": [
        {
          "selector": "containers[] .securityContext .capabilities .add == SYS_ADMIN",
          "reason": "CAP_SYS_ADMIN is the most privileged capability and should always be
avoided"
        }
      ],
      "advise": [
        {
          "selector": "containers[] .securityContext .runAsNonRoot == true",
          "reason": "Force the running image to run as a non-root user to ensure least
privilege"
        },
        {
          // ...
        }
      ]
    }
  }
]
```

Falco : Detecção de ameaças em tempo real para ambientes Kubernetes, containers e hosts Linux.

- Atua monitorando a atividade do sistema (syscalls) para identificar comportamentos anormais ou não autorizados.
- Permite criar regras customizadas que descrevem comportamentos suspeitos, como:
  - Acesso a arquivos sensíveis;
  - Execução de shells dentro de containers;
  - Modificações suspeitas no sistema.

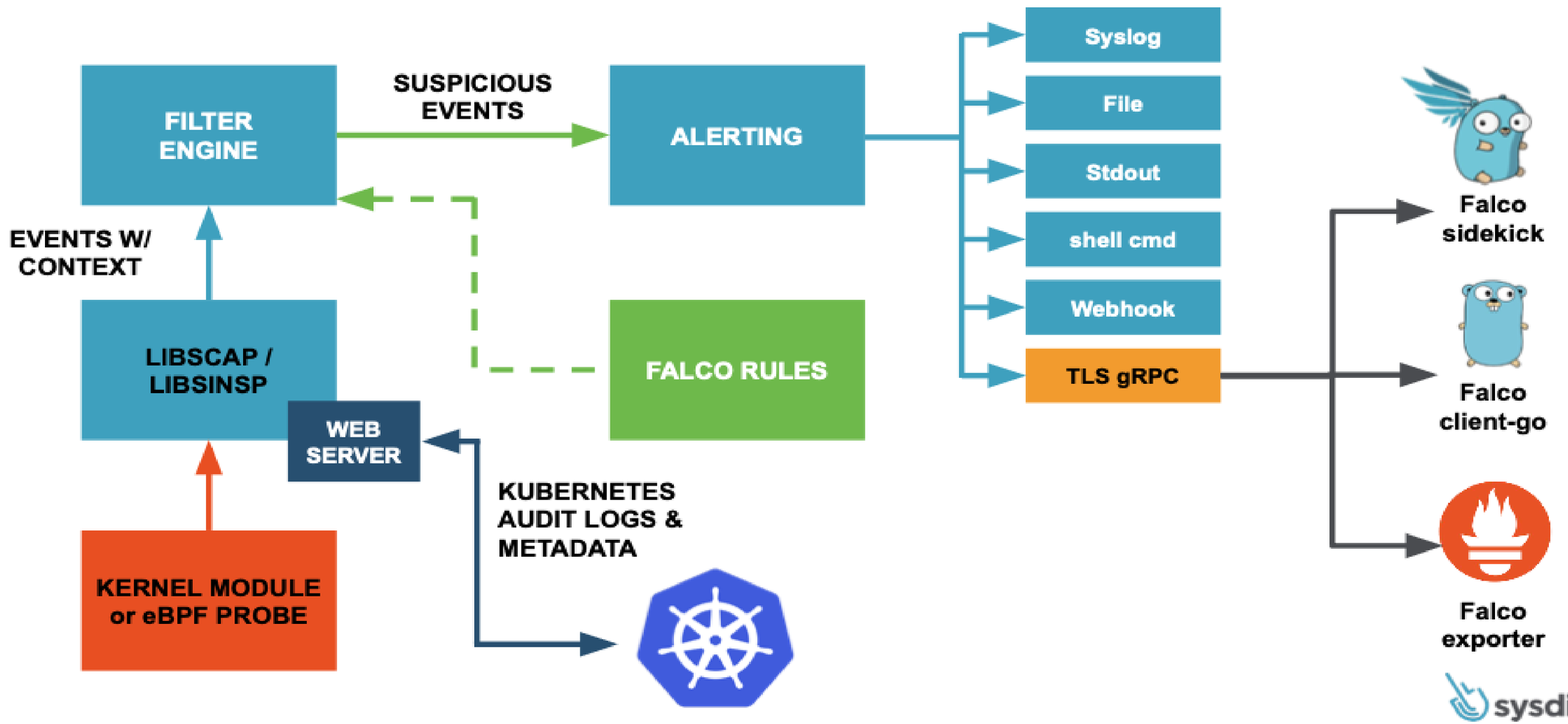
Como o Falco ajuda no dia a dia

CLOUD NATIVE
COMMUNITY GROUPS
ARARAQUARA - SP

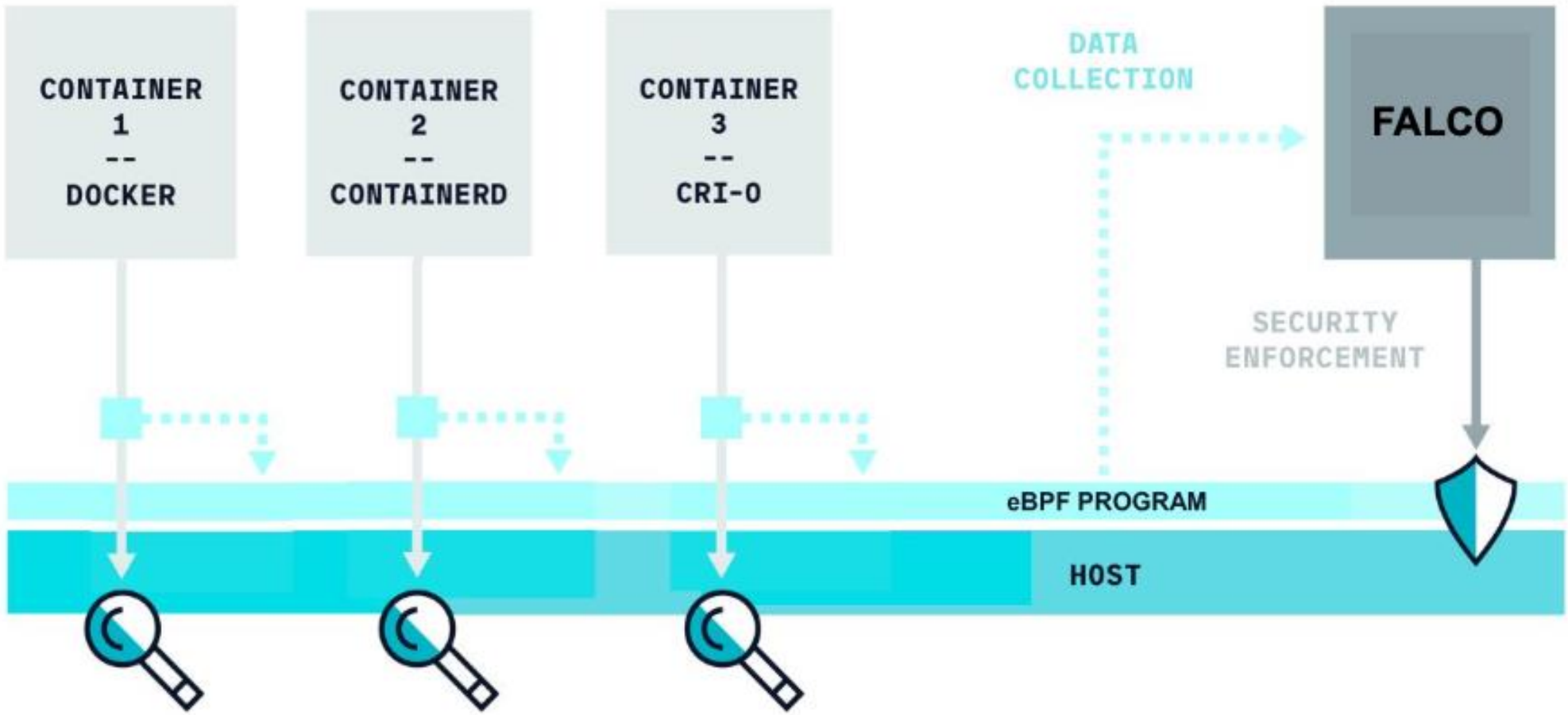
- Ambientes de containers e Kubernetes são altamente dinâmicos e difíceis de proteger com soluções tradicionais de segurança. Muitas vezes, um ataque ou violação só é percebido tarde demais.
- Solução:
  - O Falco oferece visibilidade instantânea sobre eventos críticos, detectando comportamentos anômalos enquanto acontecem.
- Benefícios:
  - Resposta rápida a incidentes;
  - Redução do tempo de detecção de ameaças (MTTD);
  - Integração com SIEMs, alertas e automações (Slack, Webhooks, Prometheus, etc.);
  - Aumento da segurança operacional de ambientes cloud native.

Arquitetura do Falco

Falco architecture



Arquitetura do Falco



Regras do Falco

Falco rule: container activity

```
- rule: Node container runs Node binary
  desc: Detect a process that's not node started in a Node container.
  condition: evt.type=execve and k8s.deployment.name=my-node-app and proc.name!=node
  output: Node container started unexpected process
                (user=%user.name command=%proc.cmdline %container.info)
  priority: INFO
  tags: [container, apps]
```

Something is executing a program

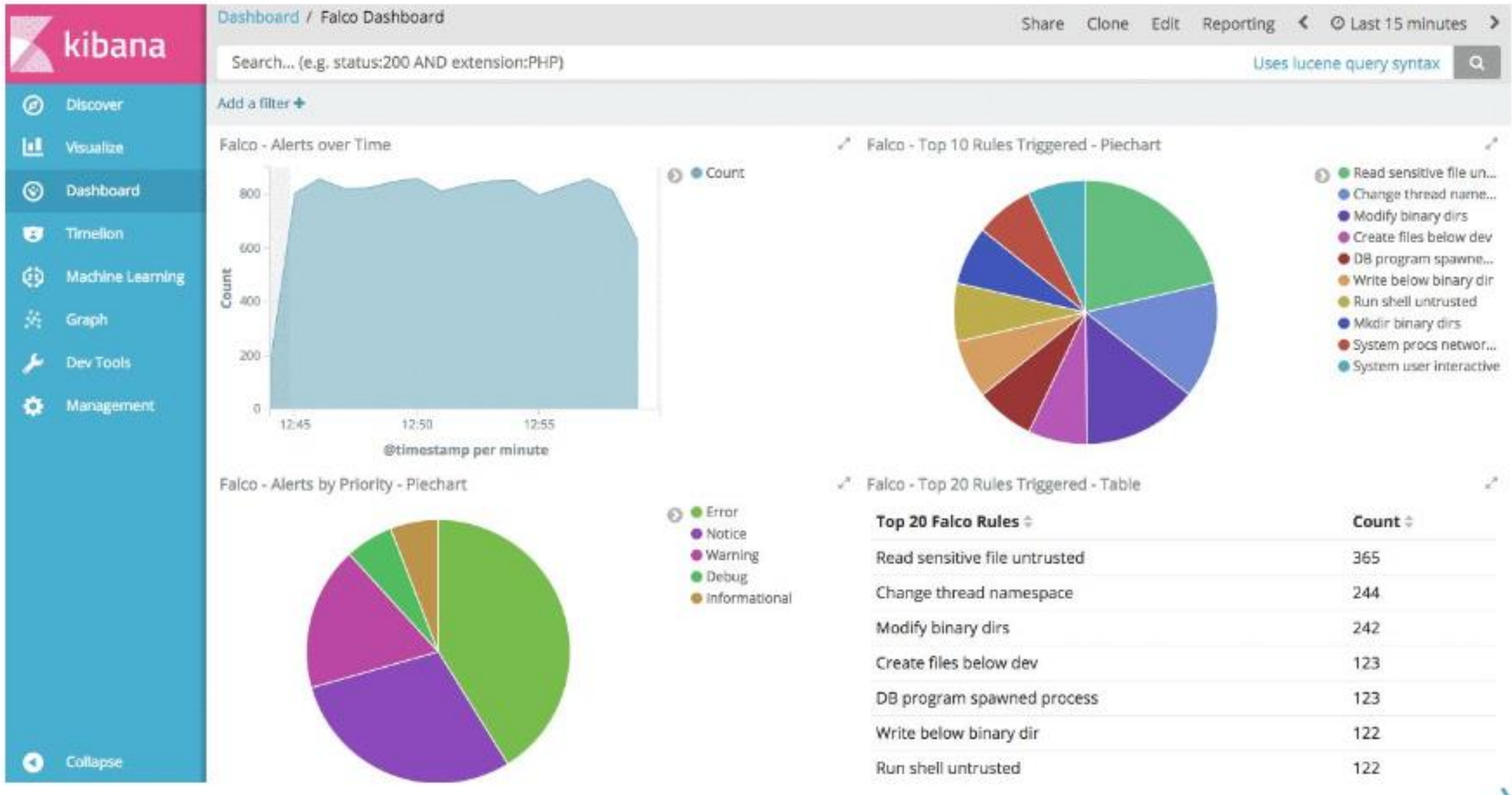
In a container in my Kubernetes deployment for my-node-app

And the process name isn't node

Como acompanhar as analises em tempo real

CLOUD NATIVE
COMMUNITY GROUPS
ARARAQUARA - SP

SIEM



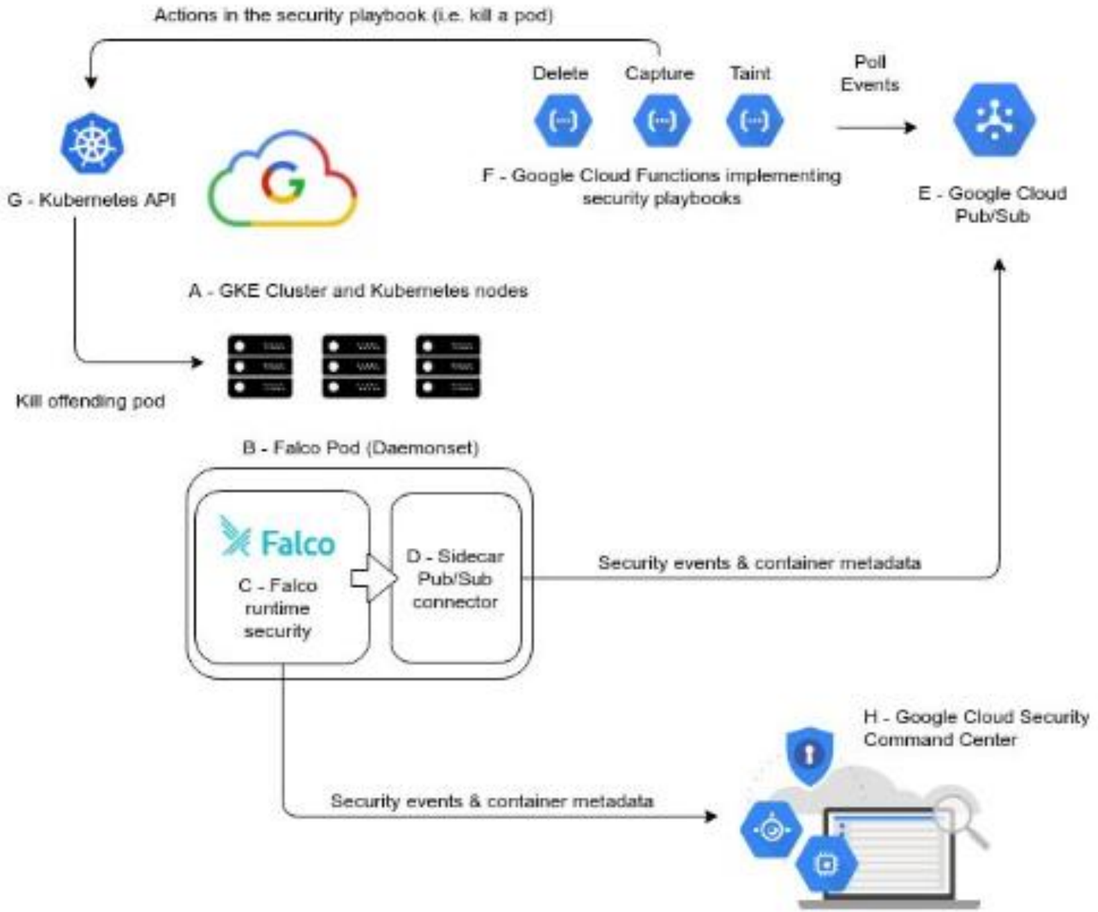
Como responder atividades suspeitas

CLOUD NATIVE
COMMUNITY GROUPS
ARARAQUARA - SP

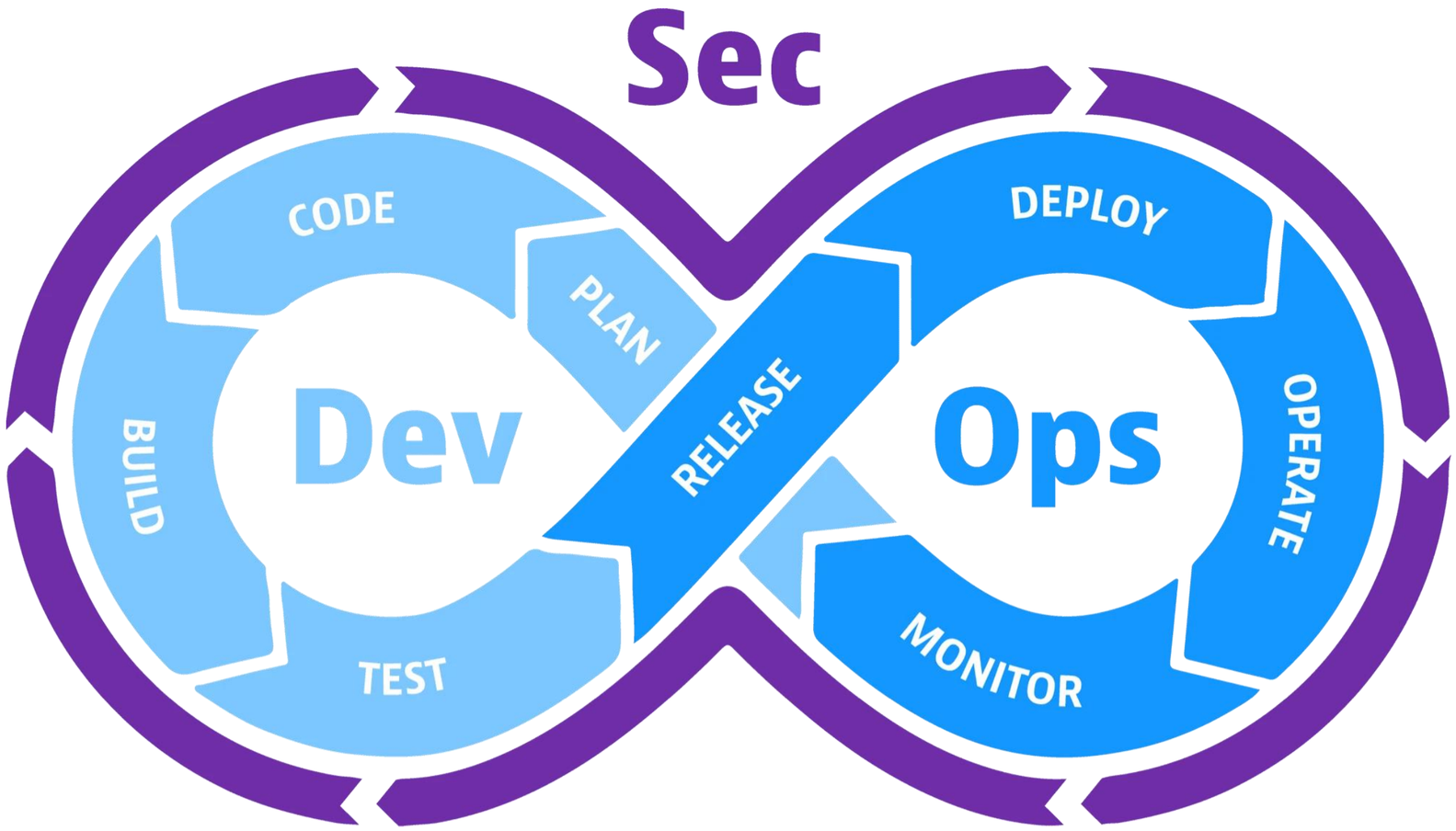
Response Engine

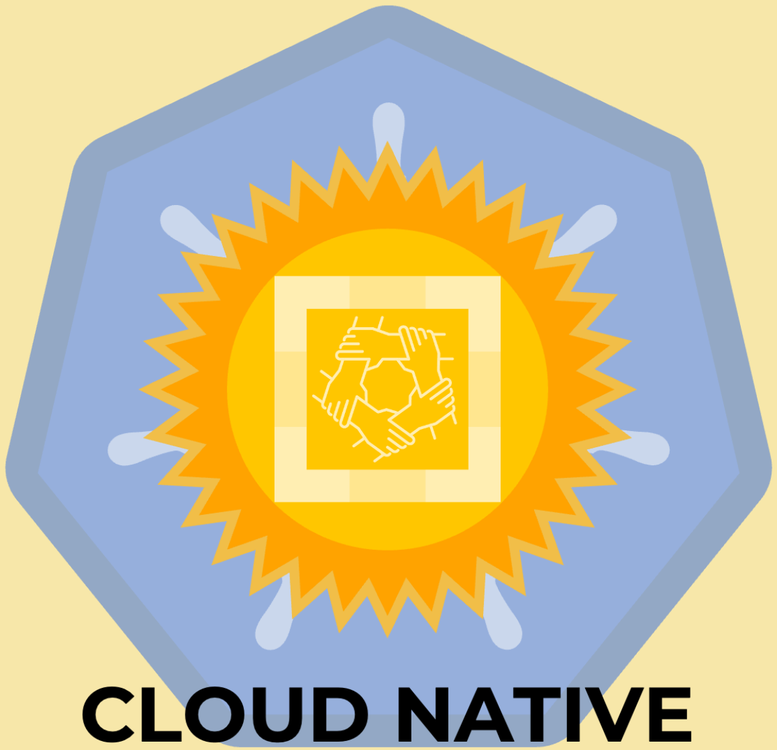
Trigger automated reactions to events
Blocking component of runtime security
Security playbooks executed as FaaS

- Taint a node NoSchedule
- Isolate pod via Network Policy
- Delete offending pod
- Scale down deployment to 0 pods
- Trigger a Sysdig capture
- Send notifications



Fluxo de desenvolvimento





CLOUD NATIVE
COMMUNITY GROUPS
ARARAQUARA - SP

Linktree

Q&A

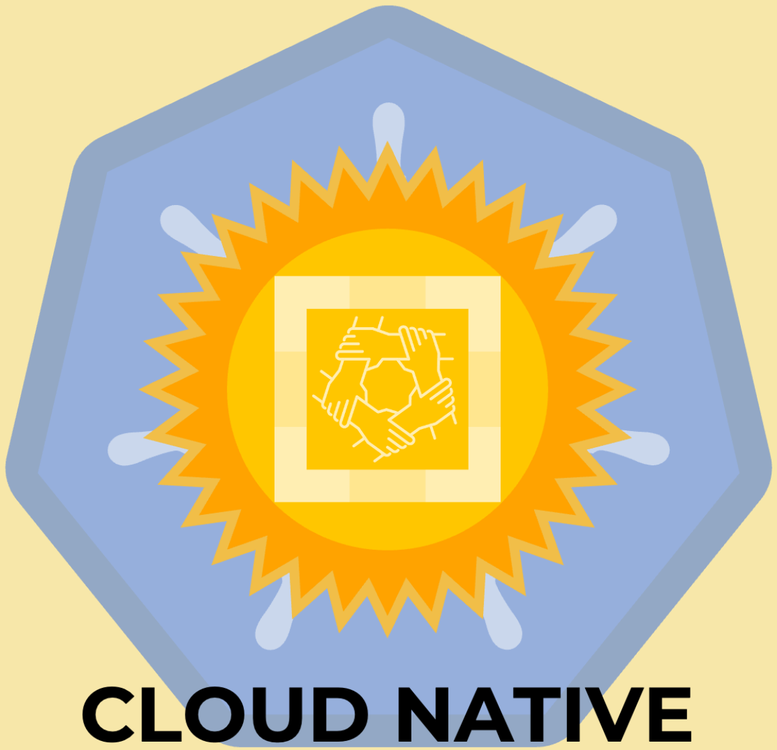
Obrigado!

CLOUD NATIVE

COMMUNITY GROUPS
ARARAQUARA - SP

Linktree

Nos ajude a melhorar cada vez mais



CLOUD NATIVE

COMMUNITY GROUPS
ARARAQUARA - SP