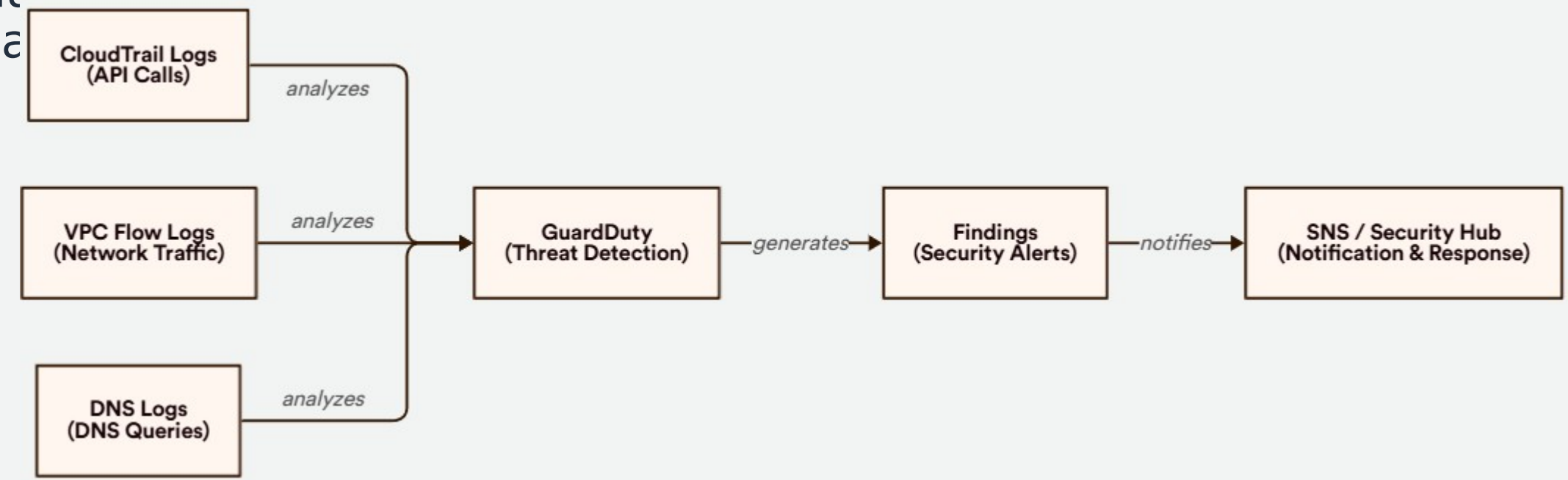
Amazon GuardDuty – Detecção de Ameaças Inteligente

Marlon Brehmer Anesi • Arquiteto de Soluções

O que é o GuardDuty?

- Serviço de detecção de ameaças que analisa comportamento e atividades maliciosas em contas AWS
- Baseado em machine learning, inteligência de ameaças e padrões de ataque
- Não exige instalação de agentes — funciona por leitura de logs na

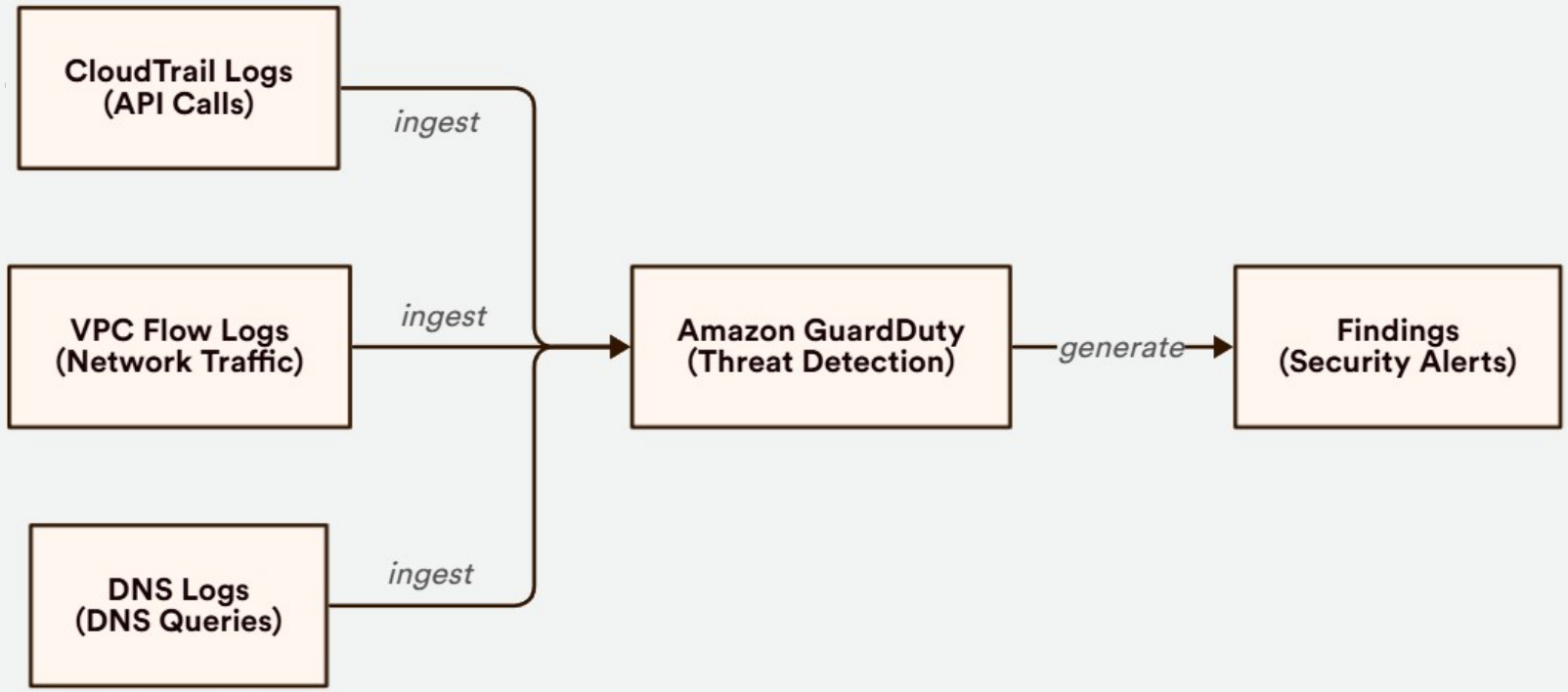


Fontes de Dados do GuardDuty

- CloudTrail: ações na conta, incluindo chamadas suspeitas via API
- VPC Flow Logs: tráfego de rede suspeito (port scanning, mineração, etc.)
- DNS Logs: resolução de domínios maliciosos ou incomuns

Findings e Integrações de Resposta

- Findings são alertas categorizados por severidade e tipo de ameaça (ex: acesso de IPs maliciosos)
- Integra com EventBridge, Security Hub, Lambda, SIEMs e automações de resposta
- Permite ações [illegible] revogação de



Boas Práticas e Dicas de Prova

- GuardDuty ≠ Macie: GuardDuty detecta ameaças; Macie detecta dados sensíveis
- Sempre aparece em questões de segurança automatizada, detecção de uso indevido e comportamento anômalo
- Não exige instalação nem configuração de coleta de logs — basta ativar
- Complementa outros serviços como Security Hub, Config, CloudTrail e IAM
- A prova pode citar ataques simulados (ex: port scan) ou acesso fora do padrão