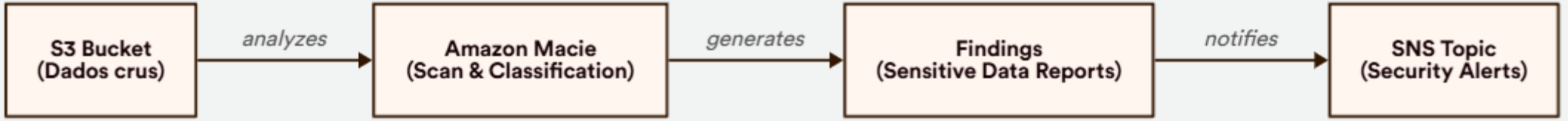
Amazon Macie – Descoberta de Dados Sensíveis

Marlon Brehmer Anesi • Arquiteto de Soluções

O que é o Amazon Macie?

- Serviço gerenciado que usa ML para identificar dados sensíveis em buckets S3
- Detecta padrões como CPF, cartão de crédito, e-mails, tokens e dados pessoais
- Classifica os dados por sensibilidade e gera alertas de segurança
- PII (Personally Identifiable Information): dados que podem identificar uma pessoa (CPF, número de cartão, email e etc...) o Macie automatiza a detecção e classificação de PII em buckets



Como o Macie Funciona

- Varre objetos armazenados em S3 de forma automatizada ou sob demanda
- Usa classificadores baseados em machine learning e regras definidas
- Gera achados (findings) que podem ser exportados ou integrados a sistemas de resposta

Casos de Uso do Macie

- Identificar exposição indevida de dados sensíveis em buckets públicos ou mal configurados
- Auditoria e conformidade com LGPD, GDPR, HIPAA, etc.
- Integração com AWS Security Hub, CloudWatch Events, Lambda e workflows de segurança

Boas Práticas e Dicas de Prova

- Macie é voltado exclusivamente para análise de dados em buckets S3
- Reforça segurança e conformidade — aparece em questões com LGPD/PII
- Pode agir proativamente sobre exposição de dados sensíveis
- Achados podem ser enviados para automações via EventBridge e Security Hub
- A prova cobra distinção entre Macie (dados sensíveis) e GuardDuty (ameaças na conta)