Amazon Q

Amazon Q: Transformando a Automação em Segurança da Informação

Potencializando a segurança com inteligência artificial

Anny Ribeiro

WHOAMI

- 9 anos na área de tecnologia
- Analista de Infraestrutura na Cilia tecnologia com foco em segurança da informação
- Bacharela em Sistemas de Informação
- Técnica em Informática
- Pós graduanda em Cibersegurança
- fã de coisinhas de nerd e dO NERDOLA
- Participante ativa de comunidades de tecnologia
  - coordenadora PyLadies Goiânia
  - coordenadora GYNSec
  - membro da organização da AWS UG Goiânia

Contexto Atual

- **Volume crescente de alertas**
  - sobrecarregando equipes de segurança
- **Complexidade das configurações**
  - segurança na nuvem
  - muitas ferramentas
  - mais ameaças
  - IA
- **Necessidade de respostas rápidas a**
  - incidentes de segurança
- **Escassez de profissionais qualificados**
  - segurança da informação
  - outras equipes

O que é esse Amazon Q

- Assistente de IA desenvolvido pela AWS para aumentar a produtividade
- Processamento de linguagem natural para interações conversacionais
- Integração com serviços AWS de desenvolvimento
- Foco em assistência técnica segurança e ferramentas e automação de segurança
- Pode ser usado via linha de código ou integrado a sua IDE

A pergunta de ouro

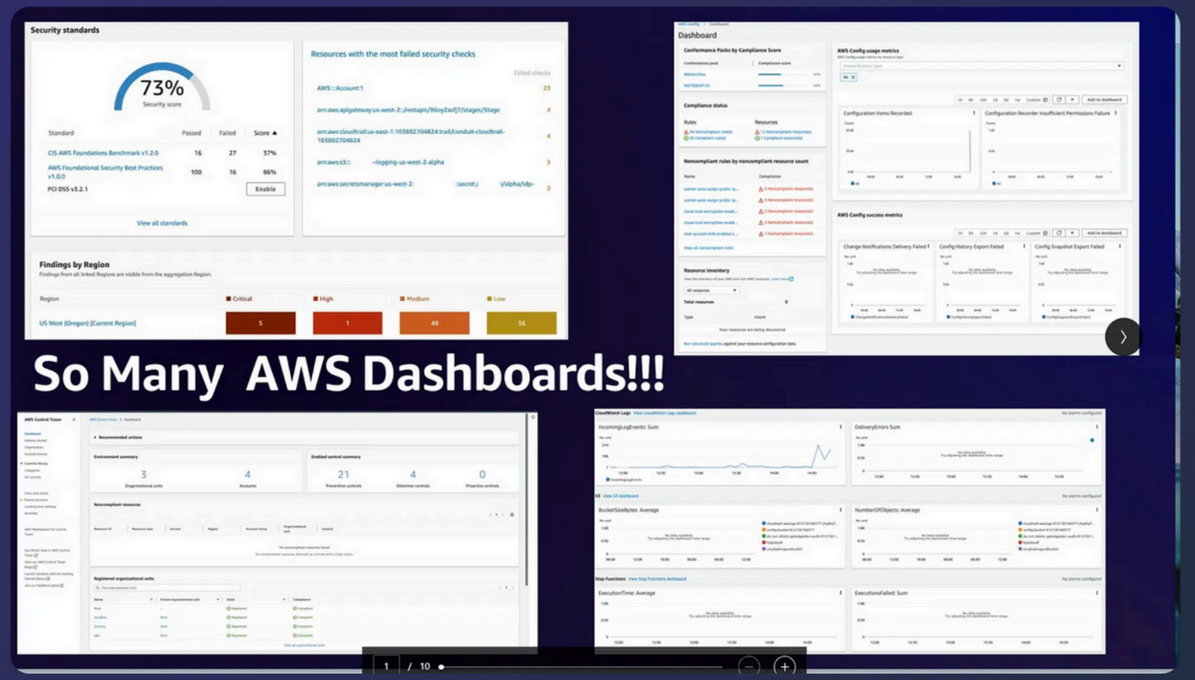
- **Então a IA vai me substituir? Fazer meu trabalho por mim?**

Casos de Uso

- **Análise de configurações de segurança**
  - para identificar vulnerabilidades
- **Automação de tarefas**
  - tarefas repetitivas de verificação e remediação
- **Resposta a incidentes**
  - sugestões de contenção com análise rápida
- **Análise de código e infraestrutura**
  - para detectar falhas de segurança

Análise de Configurações

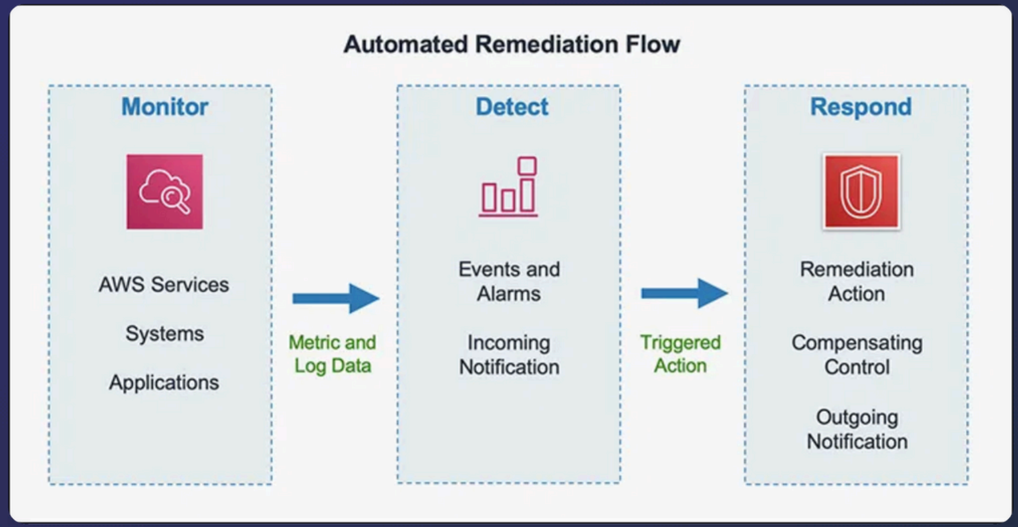
- Verificação de políticas IAM para garantir acesso adequado
- Identificação de recursos mal configurados em tempo real
- Recomendações de melhores práticas baseadas em padrões AWS



Exemplo: *"Amazon Q, verifique se minhas configurações de S3 seguem as melhores práticas de segurança"*

Automação de Tarefas

- Geração de scripts para remediação de problemas de segurança
- Automação de verificações periódicas conformidade e segurança
- Criação de relatórios de conformidade e status de segurança



"Amazon Q, crie um script para identificar EC2 instances sem patches de segurança"

Otimizar tempo de POCs

- Software de scan de vulnerabilidade
  - IDE
  - códigos em linguagens x e y (phyton, java, ruby on rails...)
  - tempo de POC geralmente 7-10 dias
  - diferentes ferramentas de gerenciamento de código
  - poder testar especificamente uma lista de coisas (vulnerabilidades mais conhecidas ou mais encontradas)

"Amazon Q, use o Loki para gerar vulnerabilidade de código baseadas na OWASP Top 10 em phyton e injete no projeto X."

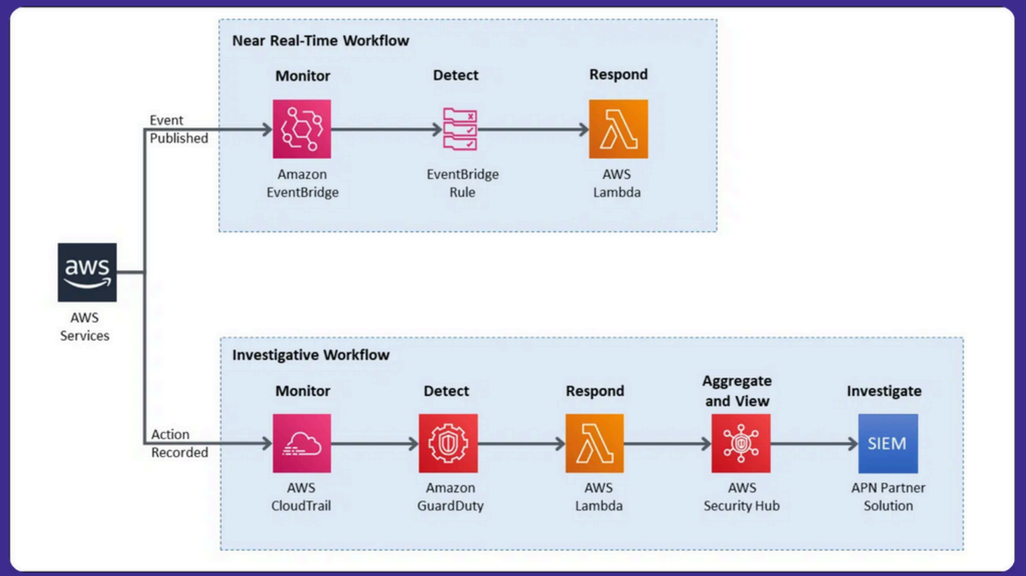
Criar suas próprias ferramentas

- Análise de detecções, arquivos suspeitos, emails...
  - manual, demorado
  - muitas ferramentas
  - personalizável

"Amazon Q, preciso..."

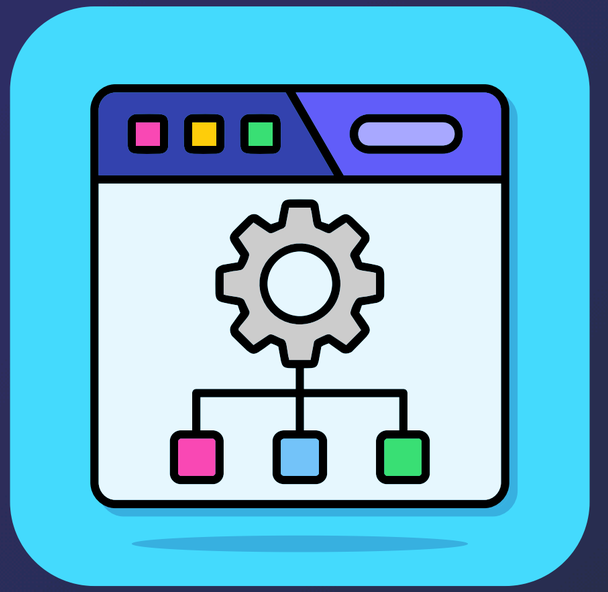
Resposta a Incidentes

- Análise rápida de logs para identificação de padrões suspeitos
- Sugestões de contenção automáticas baseadas no tipo de incidente
- Documentação de incidentes estruturada e detalhada
- Redução do tempo de resposta através de automação inteligente



Exemplo: *"Amazon Q, analise este log do CloudTrail e identifique atividades suspeitas nas últimas 24 horas"*

Demonstração: Análise de Configuração



1. **Comando inicial:** Solicitar análise de configurações de segurança
2. **Análise automática:** O Amazon Q examina políticas IAM e configurações de bucket
3. **Interpretação dos resultados:** Identificação de vulnerabilidades e riscos
4. **Implementação:** Aplicação das recomendações de segurança sugeridas

"Amazon Q, verifique se minhas configurações de S3 seguem as melhores práticas de segurança"

Demonstração: Automação de Verificações

1. **Criação de script:** Solicitar geração de script para verificação automática

```
"Amazon Q, crie um script para verificar patches de segurança em todas as instâncias EC2"
```

2. **Integração com AWS CLI:** O script é configurado para usar comandos AWS nativos

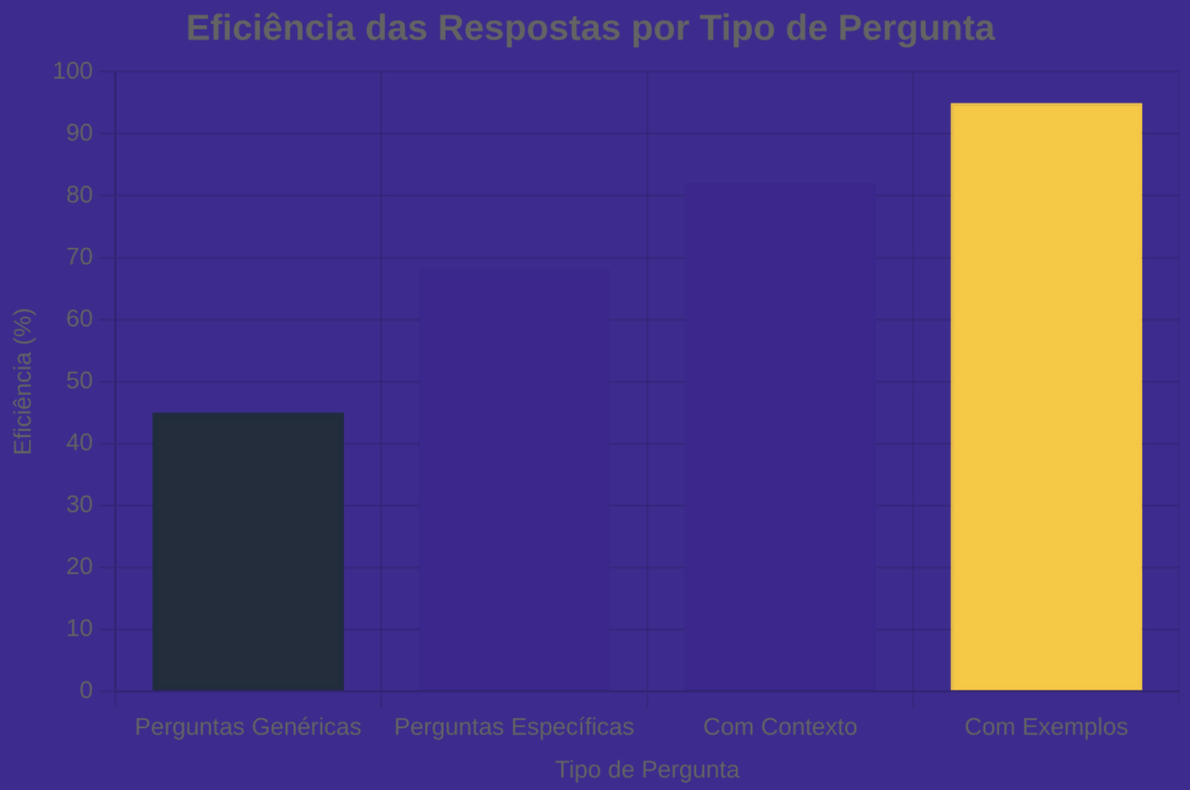
3. **Agendamento:** Configuração de verificações periódicas usando CloudWatch Events

4. **Alertas e notificações:** Sistema automatizado de notificações via SNS

Melhores Práticas

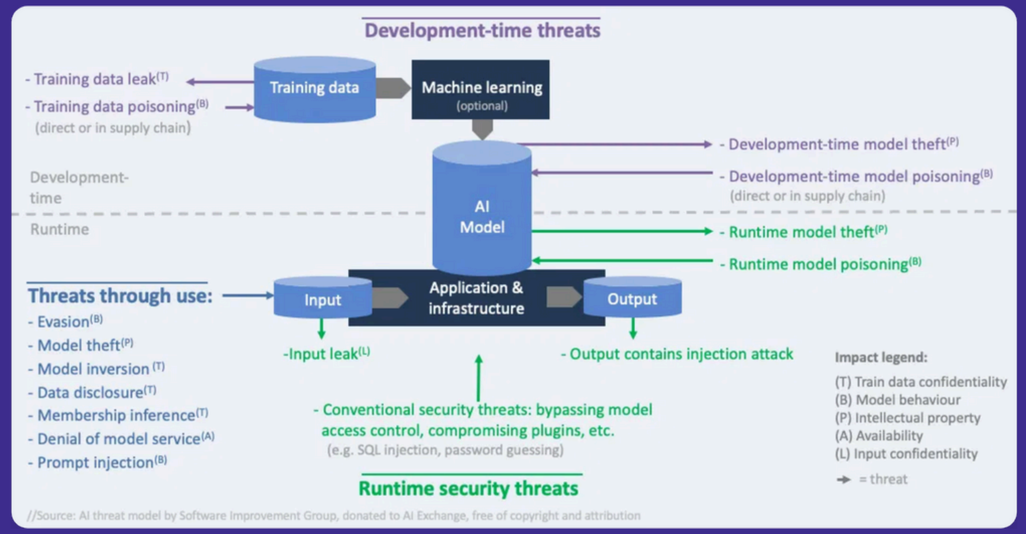
- **Formular perguntas específicas e claras** para obter respostas mais precisas
- **Validar recomendações** antes da implementação em ambientes críticos
- **Integrar com fluxos de trabalho existentes** para maximizar a eficiência
- **Documentar soluções geradas** para referência futura e auditoria

Dica: Comece com perguntas simples e vá aumentando a complexidade à medida que se familiariza com as capacidades do Amazon Q.



Considerações de Segurança

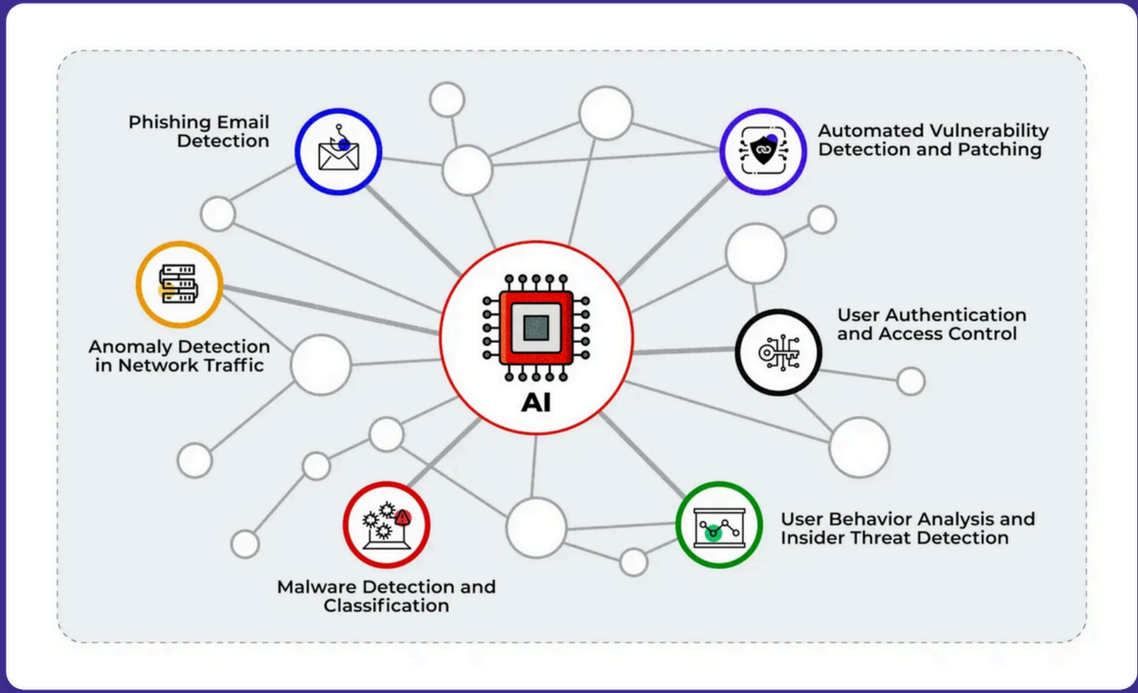
- **Gerenciamento de informações sensíveis**- Evitar compartilhar dados confidenciais
- **Limitações do Amazon Q** em contextos de segurança crítica
- **Validação humana especializada** para decisões críticas de segurança
- **Governança e políticas de uso** para implementação responsável



Próximos Passos

- **Como começar a usar o Amazon Q** para segurança em sua organização
- **Recursos de aprendizado adicionais** e documentação oficial da AWS
- **Comunidades e fóruns** para suporte e troca de experiências
- **Tendências futuras** na integração de IA com segurança da informação

Comece hoje mesmo a transformar sua segurança com Amazon Q!



Obrigada

@cybersecwonderwoman

GYNSEC

AWS User Groups Goiânia

pyladies Goiânia