Amazon Q

# Protegendo EC2 em Tempo Real

com Amazon Q e Open Source

**Anny Ribeiro**

AWS
User Groups
Goiânia

# WHOAMI

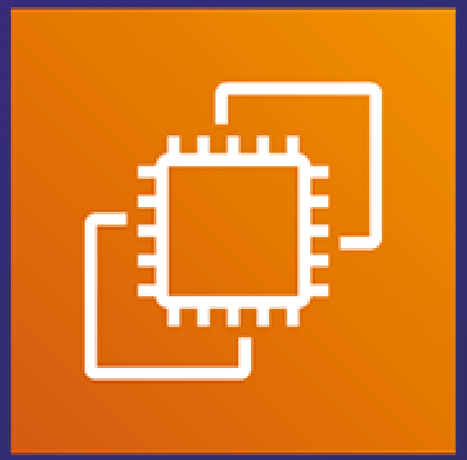
- 9 anos na área de tecnologia
- Analista de Infraestrutura na Cilia tecnologia com foco em segurança da informação
- Bacharela em Sistemas de Informação
- Técnica em Informática
- Pós graduanda em Cibersegurança
- fã de coisinhas de nerd e dO NERDOLA
- Participante ativa de comunidades de tecnologia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

# Por que a segurança em tempo real é a nova linha de frente?


- 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

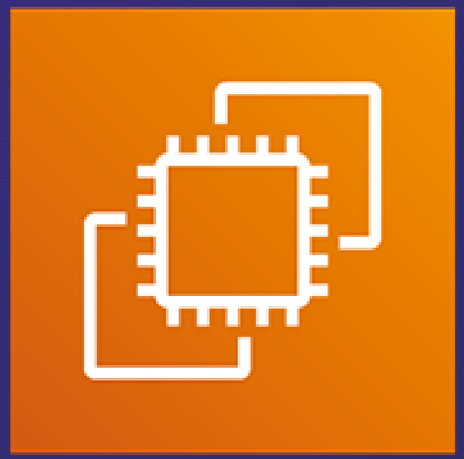
AWS User Groups Goiânia

# Amazon EC2 (Elastic Compute Cloud)



- É um dos serviços mais fundamentais da AWS
  - fornecendo capacidade de computação segura e redimensionável na nuvem.
  - Ele permite que você alugue máquinas virtuais, conhecidas como instâncias EC2, para executar suas aplicações, com total controle sobre o sistema operacional.

# O Desafio da Segurança de EC2

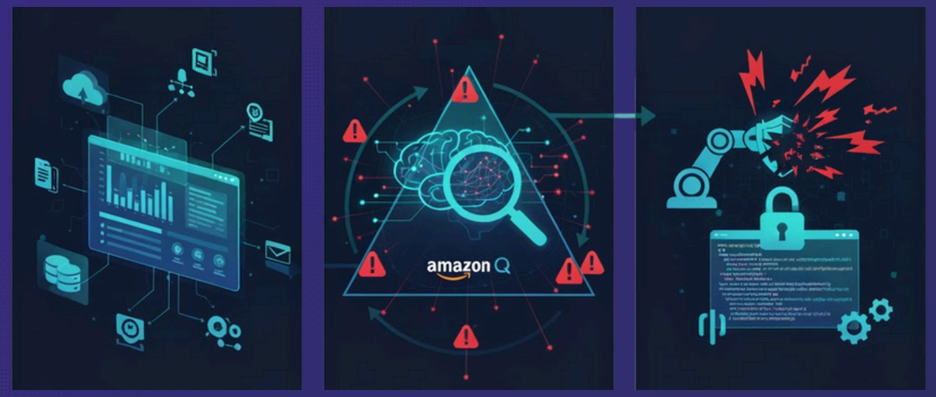


Amazon EC2

- Realidade: Ameaças dinâmicas e o alto risco de intrusão em VMs.
- Modelo de Responsabilidade Compartilhada: Reforçar a responsabilidade do cliente (Security in the Cloud).
- Foco: Não é mais sobre "prevenir", mas sim "detectar e responder" em tempo real.

AWS User Groups Goiânia

# A Tríade de Proteção em Tempo Real




- Monitoramento Contínuo: Logs, Métricas e Eventos.
- Detecção Inteligente: IA/ML para identificar anomalias (Amazon Q entra aqui).
- Resposta Automatizada: Agir imediatamente para conter a ameaça (Automação/Open Source).

# Apresentando a Solução Híbrida


- AWS Nativa (Amazon Q + Serviços): Inteligência, automação de diagnóstico e segurança de plataforma.

- Open Source (OS):
  - é um modelo de desenvolvimento e licença onde o código-fonte de um software é livremente acessível, utilizável, modificável e distribuível por qualquer pessoa.

  - Flexibilidade, baixo custo e controle profundo no nível da instância (Host-Based Security).

# Por Que Open Source no EC2?

- Visibilidade de Host (Endpoint): A AWS não vê o que acontece dentro da VM. O OS preenche essa lacuna.
- Controle Fino: Agentes leves para monitoramento de arquivos, processos e usuários.
- Custo-Benefício e Flexibilidade: Adaptação a ambientes híbridos ou com restrições orçamentárias.

# Amazon Q no Contexto de Segurança


- O que é Amazon Q Developer/Business?
  - Um assistente de IA para desenvolvimento e operações.
- Segurança como Copiloto:
  - Ajuda na análise de segurança, diagnóstico operacional (alarme em CloudWatch → investigação automática) e até mesmo com a escrita de regras seguras (ex: Security Groups).

# Amazon Q e a Investigação de Incidentes


- Diagnóstico em Tempo Quase Real: Q pode receber um alarme (ex: alto uso de CPU) e correlacionar com eventos recentes (ex: novo usuário, alteração no Security Group).
- Proatividade: Usar o Q para consultar e otimizar regras de segurança do EC2 (ex: "Me mostre todas as regras de SG abertas para o mundo na porta 22").

# Serviços AWS Nativos

- GuardDuty: Detecção de ameaças (incluindo Malware Protection para EC2 via EBS snapshots).
- Security Hub: Centralização de findings. Config: Monitoramento de conformidade em tempo real.

AWS User Groups Goiânia

# Combinando o Melhor dos Mundos

## AMAZON Q

AGILIZA A INVESTIGAÇÃO, OTIMIZA AS CONFIGURAÇÕES DA PLATAFORMA (SGS, IAM), ATUA COMO UM ANALISTA DE SEGURANÇA GENAI.

## OPEN SOURCE

OFERECE VISIBILIDADE GRANULAR DE PROCESSOS, ARQUIVOS E USUÁRIOS (PROTEÇÃO HOST-LEVEL).

## RESULTADO

UM CICLO DE PROTEÇÃO MAIS RÁPIDO (DETECÇÃO → DIAGNÓSTICO (Q) → RESPOSTA AUTOMATIZADA (OS/LAMBDA)).

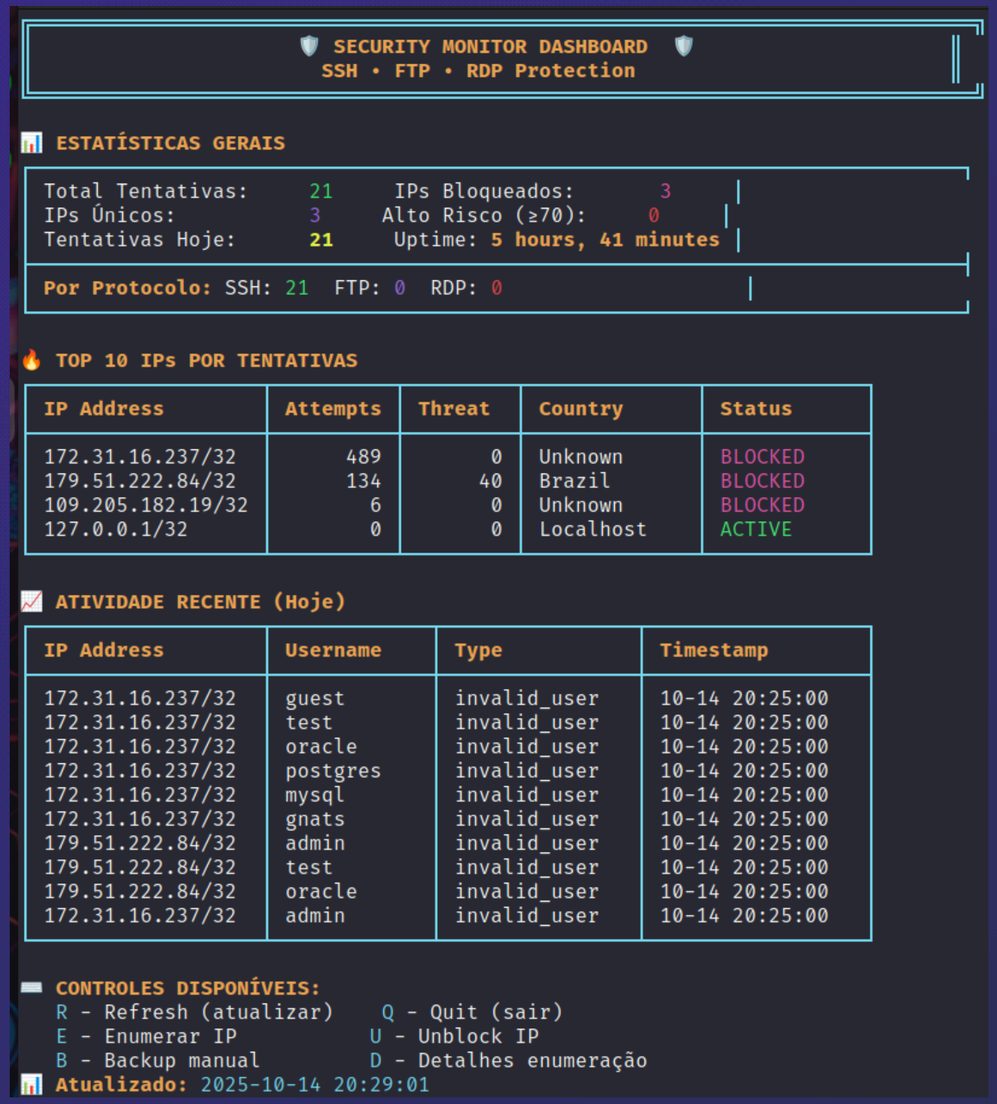
AWS User Groups Goiânia

# Cenário de Uso do Amazon Q



AWS User Groups
Goiânia

# Cenário de Uso do Amazon Q



🛡️ SECURITY MONITOR DASHBOARD 🛡️
SSH • FTP • RDP Protection

📊 ESTATÍSTICAS GERAIS

| | | | |
|---|---|---|---|
| Total Tentativas: | 21 | IPs Bloqueados: | 3 |
| IPs Únicos: | 3 | Alto Risco (≥70): | 0 |
| Tentativas Hoje: | 21 | Uptime: | 5 hours, 41 minutes |

Por Protocolo: SSH: 21 FTP: 0 RDP: 0

🔥 TOP 10 IPs POR TENTATIVAS

| IP Address | Attempts | Threat | Country | Status |
|---|---|---|---|---|
| 172.31.16.237/32 | 489 | 0 | Unknown | BLOCKED |
| 179.51.222.84/32 | 134 | 40 | Brazil | BLOCKED |
| 109.205.182.19/32 | 6 | 0 | Unknown | BLOCKED |
| 127.0.0.1/32 | 0 | 0 | Localhost | ACTIVE |

📈 ATIVIDADE RECENTE (Hoje)

| IP Address | Username | Type | Timestamp |
|---|---|---|---|
| 172.31.16.237/32 | guest | invalid_user | 10-14 20:25:00 |
| 172.31.16.237/32 | test | invalid_user | 10-14 20:25:00 |
| 172.31.16.237/32 | oracle | invalid_user | 10-14 20:25:00 |
| 172.31.16.237/32 | postgres | invalid_user | 10-14 20:25:00 |
| 172.31.16.237/32 | mysql | invalid_user | 10-14 20:25:00 |
| 172.31.16.237/32 | gnats | invalid_user | 10-14 20:25:00 |
| 179.51.222.84/32 | admin | invalid_user | 10-14 20:25:00 |
| 179.51.222.84/32 | test | invalid_user | 10-14 20:25:00 |
| 179.51.222.84/32 | oracle | invalid_user | 10-14 20:25:00 |
| 172.31.16.237/32 | admin | invalid_user | 10-14 20:25:00 |

⌨️ CONTROLES DISPONÍVEIS:
R - Refresh (atualizar) Q - Quit (sair)
E - Enumerar IP U - Unblock IP
B - Backup manual D - Detalhes enumeração
📊 Atualizado: 2025-10-14 20:29:01

AWS User Groups
Goiânia

# Cenário de Uso do Amazon Q

```
● Completed in 4.844s
Para executar o teste:

1. Conecte na EC2 de ataque:
bash
ssh -i /home/anny-ribeiro/Downloads/key-labs-aws.pem ubuntu@3.143.224.25

2. Instale dependências necessárias:
bash
sudo apt update
sudo apt install -y nmap sshpass netcat-openbsd traceroute

3. Execute o script:
bash
chmod +x attack_simulation.sh
./attack_simulation.sh

4. Monitore os resultados na EC2 de defesa:
bash
ssh -i /home/anny-ribeiro/Downloads/key-labs-aws.pem ubuntu@13.59.241.156
docker logs linuxsecmonitor-monitor-1 -f


O script simula: port scanning, brute force SSH, web scanning, connection flooding, file system probing,
process enumeration, network reconnaissance e comandos suspeitos.
```

```
ubuntu@ip-172-31-16-237:~$ ls
advanced_attack.sh  attack_simulation.sh  attack_simulation_v2.sh
```

AWS User Groups
Goiânia

# Boas Práticas e Próximos Passos

- Princípio do Privilégio Mínimo Privílegio (Zero Trust): O ponto de partida para tudo.
- Automatize a Resposta: Use ferramentas SOAR ou Lambda para ações como quarentena de EC2.
- Mantenha os Agentes OS Atualizados: Essencial para novas assinaturas de detecção.

AWS
User Groups
Goiânia

# Obrigada

@cybersecwonderwoman

GYNSEC

MULHERESGO

Outras informações, material da palestra, minhas redes e contatos.