OpenAI e DevSec

Como Automatizar a Correção de Vulnerabilidades

Luiz Machado - 2024

Segurança em ambientes AWS

Mitigando Riscos

Luiz Machado - 2024

Luiz Machado 

- Head Cloud Cilia Tecnologia
- Instrutor/DevSecOps CloudFaster Academy
- 4x AWS Cert
- AWS Community Builder (Sec)
- Lider de comunidade (GYNSec)

AWS User Groups Goiânia

Responsabilidade compartilhada

Responsabilidade compartilhada

AWS

O que você não tem acesso

Serviços Gerenciados

Serverless

Cliente

O que você tem acesso

Liberação de acessos

Sistemas Operacionais

AWS User Groups Goiânia

AWS IAM

Luiz Machado - 2024

AWS IAM

Como os serviços da AWS se comunicam ?

Luiz Machado - 2024

AWS IAM

API

API

AWS IAM

Politica de acesso

API

Lambda

API

DynamoDB

AWS User Groups Goiânia

AWS IAM

AWS User Groups Goiânia

AWS IAM

Politica de acesso

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "dynamodb:GetItem",
            ],
            "Resource": [
                "arn:aws:dynamodb:us-east-1:AccountId:table/minhaTabela"
            ],
            "Effect": "Allow"
        }
    ]
}
```

AWS User Groups Goiânia

AWS IAM

Regra / Role

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "lambda.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Politica de acesso

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "dynamodb:GetItem",
            ],
            "Resource": [
                "arn:aws:dynamodb:us-east-1:AccountId:table/minhaTabela"
            ],
            "Effect": "Allow"
        }
    ]
}
```

AWS IAM

Regra / Role

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "lambda.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

AWS User Groups Goiânia

AWS IAM

Regra / Role

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "lambda.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Regra / Role

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::AccountId:role/LambdaExecutionRole"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

AWS User Groups Goiânia

AWS IAM

Liberação de acessos

- Cria usuários ✔
- Politica de senhas ✔
- MFA ✔
- Politicas de acesso ✔
- Regras de acesso ✔

AWS User Groups Goiânia

Pontos de atenção na AWS

Pontos de atenção na AWS

Gestão de acessos a conta
Gestão de acessos a recursos
Serviços de borda (ex: ELB, API GW)
Subnets Publicas e Privadas
Imagens de container

Serviços AWS

Luiz Machado - 2024

Serviços AWS

AWS User Groups Goiânia

Serviços AWS

GuardDuty

Detective

Inspector

CloudTrail

AWS User Groups Goiânia

Serviços AWS

Certificate Manager

KMS

Secrets Manager

AWS User Groups Goiânia

Principais recomendações

Nunca utilizar a conta root no dia a dia
Ativar o MFA da conta root
Aplique o menor privilégio
Ative camadas de acesso aos recursos
Ative os serviços de segurança da AWS

Dúvidas

Obrigado

@luizmachadoaws

AWS User Groups Goiânia

AWS User Groups Goiânia