■ Relatório STRIDE – Arquitetura: aws_multi_az_web

Descrição: Arquitetura "aws_multi_az_web" com os seguintes componentes identificados no diagrama: Cloudfront, Aws Waf, Aws Shield, Application Load Balancer, Auto Scaling, Rds, Elasticache, Cloudwatch, Ses.

■ Componente: Cloudfront

- Ameaça (Information Disclosure): Conteúdo de cache privado pode ser exposto.
  Contramedida: Signed URLs e cache-key restrictive.
- Ameaça (Denial of Service): Ataques DDoS podem saturar borda.
  Contramedida: Shield Standard + limitações de taxa.

■ Componente: Aws Waf

- Ameaça (Tampering): Regras podem ser desativadas acidentalmente.
  Contramedida: Controle de mudança via IaC (Terraform/CloudFormation).
- Ameaça (Information Disclosure): Falsos negativos expõem endpoints.
  Contramedida: Alertas CloudWatch para mudanças em ACL.

■ Componente: Aws Shield

- Ameaça (Availability): Se não configurado, ataques DDoS podem afetar serviço.
  Contramedida: Ativar Shield Advanced em ALB e Route 53.

■ Componente: Application Load Balancer

- Ameaça (Information Disclosure): Headers revelando detalhes internos.
  Contramedida: Strip Server headers, HTTPS only.
- Ameaça (Denial of Service): Saturação de listeners.
  Contramedida: WAF rules + Auto Scaling listeners.

■ Componente: Auto Scaling

- Ameaça (Denial of Service): Configuração inadequada pode não escalar e causar falha.
  Contramedida: Alarmes CloudWatch dretransport and proper scaling policies.
- Ameaça (Cost Impact): Escala excessiva gerando custos inesperados.
  Contramedida: Limites de capacidade máxima e verificação de autoscaling.

■ Componente: Rds

- Ameaça (Information Disclosure): Backup público ou snapshots compartilhados acidentalmente.
  Contramedida: Snapshots privados + KMS encriptação.
- Ameaça (Tampering): Queries maliciosas podem alterar dados.
  Contramedida: IAM roles + SQL firewall rules.

■ Componente: Elasticache

- Ameaça (Information Disclosure): Dados em cache sem TLS.
  Contramedida: TLS in-flight, AUTH token requerido.
- Ameaça (Tampering): Comandos não autenticados podem alterar cache.
  Contramedida: IAM auth e Security Groups restritivos.

■ **Componente: Cloudwatch**

- Ameaça (Repudiation): Logs podem ser apagados ou desabilitados.
  Contramedida: KMS-encrypted log groups e retenção imutável.
- Ameaça (Information Disclosure): Logs sensíveis não criptografados.
  Contramedida: Mascaramento de dados sensíveis nos logs.

■ **Componente: Ses**

- Ameaça (Spoofing): Phishing via domínios não verificados.
  Contramedida: DKIM, SPF e DMARC configurados.
- Ameaça (Information Disclosure): Conteúdo de e-mails interceptado.
  Contramedida: TLS obrigatório para SMTP/API.