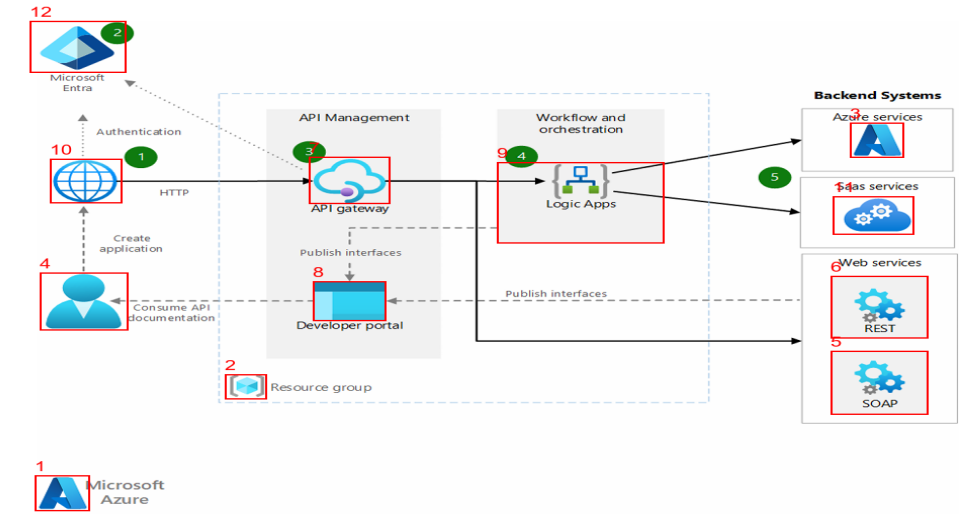
Relatório para: arch_azure.png



1: Azure_services (0.98)
2: Azure_resource_group (0.97)
3: Azure_services (0.96)
4: Azure_users (0.96)
5: Azure_api (0.95)
6: Azure_api (0.95)
7: Azure_api_gateway (0.95)
8: Azure_management-portal (0.92)
9: Azure_integration-204-Logic-Apps (0.92)
10: Azure_http (0.86)
11: Azure_cloud_services (0.76)
12: Azure_microsoft_entra (0.66)

Azure_services

• **Spoofing**: Serviço falso se passa por oficial.
• **Tampering**: Alteração de parâmetros de serviço.
• **Repudiation**: Falta de rastreabilidade.
• **Information Disclosure**: Dados internos expostos.
• **Denial of Service**: Sobrecarga proposital do serviço.
• **Elevation of Privilege**: Configuração incorreta dá acesso total.

Azure_resource_group

• **Spoofing**: Recurso falso dentro do grupo.
• **Tampering**: Alteração não autorizada de recursos.
• **Repudiation**: Ações não registradas.
• **Information Disclosure**: Dados de configuração expostos.
• **Denial of Service**: Criação massiva de recursos esgota limites.
• **Elevation of Privilege**: Permissões excessivas em recursos críticos.

Azure_services

• **Spoofing**: Serviço falso se passa por oficial.
• **Tampering**: Alteração de parâmetros de serviço.
• **Repudiation**: Falta de rastreabilidade.
• **Information Disclosure**: Dados internos expostos.
• **Denial of Service**: Sobrecarga proposital do serviço.
• **Elevation of Privilege**: Configuração incorreta dá acesso total.

Azure_users

• **Spoofing**: Usuário falso se passa por legítimo.
• **Tampering**: Alteração de credenciais.
• **Repudiation**: Negação de ações.
• **Information Disclosure**: Dados pessoais expostos.
• **Denial of Service**: Múltiplas tentativas de login.
• **Elevation of Privilege**: Usuário comum obtém privilégios administrativos.

Azure_api

• **Spoofing**: Chaves ou tokens de API falsificados.
• **Tampering**: Manipulação das requisições/respostas.
• **Repudiation**: Falta de logs detalhados de chamadas.
• **Information Disclosure**: Respostas de API contendo informações sensíveis.
• **Denial of Service**: Flood de chamadas para exaurir recursos.
• **Elevation of Privilege**: API mal configurada permite comandos administrativos.

Azure_api

• **Spoofing**: Chaves ou tokens de API falsificados.
• **Tampering**: Manipulação das requisições/respostas.
• **Repudiation**: Falta de logs detalhados de chamadas.
• **Information Disclosure**: Respostas de API contendo informações sensíveis.
• **Denial of Service**: Flood de chamadas para exaurir recursos.
• **Elevation of Privilege**: API mal configurada permite comandos administrativos.

Azure_api_gateway

• **Spoofing**: Cliente falso burla autenticação.
• **Tampering**: Alteração de rotas e payloads.
• **Repudiation**: Logs insuficientes de acessos.
• **Information Disclosure**: Erros expõem detalhes internos.
• **Denial of Service**: Excesso de requisições sobrecarrega APIs.

• **Elevation of Privilege**: Configuração incorreta dá acesso irrestrito.

Azure_management-portal

• **Spoofing**: Login falso imita portal oficial.
• **Tampering**: Alteração de configurações críticas.
• **Repudiation**: Ações administrativas não rastreadas.
• **Information Disclosure**: Dados de gestão expostos.
• **Denial of Service**: Sobrecarga de acessos ao portal.
• **Elevation of Privilege**: Usuário comum vira administrador.

Azure_integration-204-Logic-Apps

• **Spoofing**: Aplicativo falso executa workflows.
• **Tampering**: Alteração de fluxos automatizados.
• **Repudiation**: Execuções não rastreadas.
• **Information Disclosure**: Dados processados expostos.
• **Denial of Service**: Execuções massivas sobrecarregam serviço.
• **Elevation of Privilege**: Workflow concede acesso indevido.

Azure_http

• **Spoofing**: Requisições forjadas com headers falsos.
• **Tampering**: Manipulação de tráfego HTTP.
• **Repudiation**: Logs de requisições ausentes.
• **Information Disclosure**: URLs expõem parâmetros sensíveis.
• **Denial of Service**: Flood de conexões HTTP.
• **Elevation of Privilege**: Headers permitem escalonamento de acesso.

Azure_cloud_services

• **Spoofing**: Serviço falso imita instância Azure.
• **Tampering**: Alteração de código implantado.
• **Repudiation**: Atividades não rastreadas.
• **Information Disclosure**: Dados de configuração expostos.
• **Denial of Service**: Falha proposital no balanceamento.
• **Elevation of Privilege**: Usuário comum acessa funções administrativas.

Azure_microsoft_entra

• **Spoofing**: Identidade falsa burla autenticação.
• **Tampering**: Manipulação de tokens de identidade.

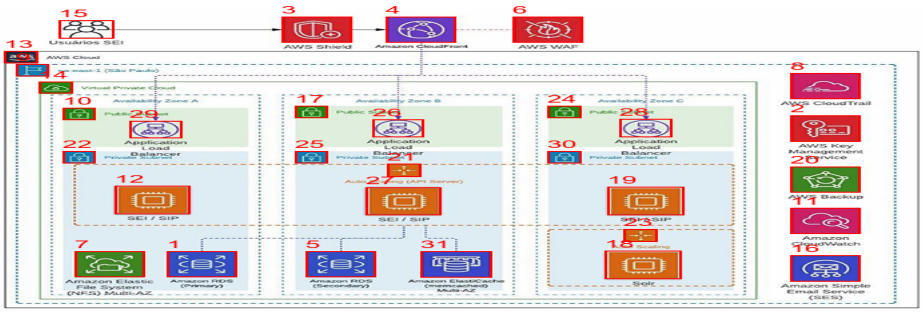
• **Repudiation**: Atividades de login não rastreadas.

• **Information Disclosure**: Dados de identidade expostos.

• **Denial of Service**: Tentativas massivas de login.

• **Elevation of Privilege**: Escalonamento de privilégios via identidade.

Relatório para: arch_aws.png



1: AWS-RDS (0.99)
2: AWS-Key-Management-Service (0.98)
3: AWS-Shield (0.98)
4: AWS-CloudFront (0.98)
5: AWS-RDS (0.98)
6: AWS-WAF (0.97)
7: AWS-EFS (0.97)
8: AWS-CloudTrail (0.96)
9: AWS-Region (0.96)
10: AWS-Public-subnet (0.95)
11: AWS-CloudWatch (0.94)
12: AWS-Category_Compute (0.94)
13: AWS-Cloud-logo (0.94)
14: AWS-Private_vpc (0.94)
15: AWS-Res_Users (0.92)
16: AWS-Simple-Email-Service (0.91)
17: AWS-Public-subnet (0.91)
18: AWS-Category_Compute (0.91)
19: AWS-Category_Compute (0.90)
20: AWS-Backup (0.89)
21: AWS-Scaling-group (0.88)
22: AWS-Private-subnet (0.86)
23: AWS-Scaling-group (0.85)
24: AWS-Public-subnet (0.84)
25: AWS-Private-subnet (0.84)
26: AWS-Res_Elastic-Load-Balancing_Application-Load-Balancer (0.81)
27: AWS-Category_Compute (0.78)
28: AWS-Res_Elastic-Load-Balancing_Application-Load-Balancer (0.73)
29: AWS-Res_Elastic-Load-Balancing_Application-Load-Balancer (0.72)
30: AWS-Private-subnet (0.67)
31: AWS-ElastiCache (0.63)

AWS-RDS

• **Spoofing**: Uso de credenciais de banco falsificadas.

• **Tampering**: Injeção de SQL ou alteração de registros.

• **Repudiation**: Ausência de trilhas de auditoria.

• **Information Disclosure**: Exposição de dados confidenciais.

• **Denial of Service**: Exaustão de conexões por queries pesadas.

• **Elevation of Privilege**: Usuário comum ganha privilégios de admin.

AWS-Key-Management-Service

• **Spoofing**: Solicitação falsa de chaves de criptografia.

• **Tampering**: Alteração de políticas de chave.

• **Repudiation**: Dificuldade em rastrear operações de chave.
• **Information Disclosure**: Exposição de chaves privadas.
• **Denial of Service**: Excesso de requisições KMS paralisa apps.
• **Elevation of Privilege**: Usuário comum consegue gerar/excluir chaves.

AWS-Shield

• **Spoofing**: Relatórios falsos de ataques.
• **Tampering**: Modificação de regras de proteção.
• **Repudiation**: Negação de incidentes registrados.
• **Information Disclosure**: Dados de mitigação expostos.
• **Denial of Service**: Falha proposital da proteção contra DoS.
• **Elevation of Privilege**: Configuração incorreta dá acesso a defesas críticas.

AWS-CloudFront

• **Spoofing**: CDN falsa interceptando tráfego.
• **Tampering**: Modificação de conteúdo em cache.
• **Repudiation**: Logs de distribuição incompletos.
• **Information Disclosure**: Cabeçalhos expondo origem ou tokens.
• **Denial of Service**: Ataques volumétricos contra edge locations.
• **Elevation of Privilege**: Configuração incorreta permite bypass de restrições.

AWS-RDS

• **Spoofing**: Uso de credenciais de banco falsificadas.
• **Tampering**: Injeção de SQL ou alteração de registros.
• **Repudiation**: Ausência de trilhas de auditoria.
• **Information Disclosure**: Exposição de dados confidenciais.
• **Denial of Service**: Exaustão de conexões por queries pesadas.
• **Elevation of Privilege**: Usuário comum ganha privilégios de admin.

AWS-WAF

• **Spoofing**: Requisições falsas burlam o WAF.
• **Tampering**: Alteração de regras de filtragem.
• **Repudiation**: Logs de bloqueio inconsistentes.
• **Information Disclosure**: Cabeçalhos expostos em respostas.
• **Denial of Service**: Ataques não mitigados sobrecarregam serviços.
• **Elevation of Privilege**: Configuração incorreta permite bypass total.

AWS-EFS

• **Spoofing**: Acesso indevido a sistemas de arquivos.
• **Tampering**: Alteração maliciosa de arquivos compartilhados.
• **Repudiation**: Dificuldade em rastrear modificações.
• **Information Disclosure**: Arquivos confidenciais expostos.
• **Denial of Service**: Bloqueio por consumo de IOPS.
• **Elevation of Privilege**: Usuário sem permissão obtém leitura/escrita.

AWS-CloudTrail

• **Spoofing**: Logs forjados por invasores.
• **Tampering**: Alteração ou deleção de trilhas de auditoria.
• **Repudiation**: Falta de integridade em eventos registrados.
• **Information Disclosure**: Exposição de logs com chaves/tokens.
• **Denial of Service**: Sobrecarga por excesso de eventos.
• **Elevation of Privilege**: Usuário malicioso desativa auditoria.

AWS-Region

• **Spoofing**: Tráfego redirecionado para região falsa.
• **Tampering**: Alteração de configuração de replicação.
• **Repudiation**: Logs inconsistentes entre regiões.
• **Information Disclosure**: Exposição de dados replicados.
• **Denial of Service**: Ataques em massa a uma região específica.
• **Elevation of Privilege**: Acesso indevido a recursos inter-regionais.

AWS-Public-subnet

• **Spoofing**: Serviço falso na subnet pública.
• **Tampering**: Alteração de tráfego público.
• **Repudiation**: Logs incompletos de acessos externos.
• **Information Disclosure**: Exposição de portas/serviços desnecessários.
• **Denial of Service**: Sobrecarga em serviços públicos.
• **Elevation of Privilege**: Serviço exposto usado como pivô de ataque.

AWS-CloudWatch

• **Spoofing**: Agente falso envia métricas manipuladas.
• **Tampering**: Alteração de alarmes e dashboards.
• **Repudiation**: Dificuldade em atribuir origem de métricas.
• **Information Disclosure**: Logs contendo dados confidenciais.
• **Denial of Service**: Excesso de métricas gerando custos altos.

• **Elevation of Privilege**: Usuário comum altera alertas críticos.

AWS-Category_Compute

• **Spoofing**: VMs falsas se passando por instâncias legítimas.
• **Tampering**: Alteração da imagem base ou do código implantado.
• **Repudiation**: Falta de registros de execução.
• **Information Disclosure**: Dados em memória ou logs expostos.
• **Denial of Service**: Exaustão de CPU/RAM por workloads maliciosos.
• **Elevation of Privilege**: Exploração para acesso root/admin.

AWS-Cloud-logo

• **Spoofing**: Uso de logotipo para phishing.
• **Tampering**: Alteração não autorizada da identidade visual.
• **Repudiation**: Dificuldade em provar autoria de modificações.
• **Information Disclosure**: Exposição de design interno de marca.
• **Denial of Service**: Uso abusivo para confundir usuários.
• **Elevation of Privilege**: Uso indevido da marca para enganar stakeholders.

AWS-Private_vpc

• **Spoofing**: Invasor imita dispositivo autorizado.
• **Tampering**: Alteração maliciosa nas rotas da VPC.
• **Repudiation**: Logs de tráfego ausentes.
• **Information Disclosure**: Rotas internas expostas.
• **Denial of Service**: Flood de tráfego interno.
• **Elevation of Privilege**: VM comprometida obtém acesso privilegiado.

AWS-Res_Users

• **Spoofing**: Usuário falso se passa por legítimo.
• **Tampering**: Modificação de dados enviados ao sistema.
• **Repudiation**: Negação de ações realizadas.
• **Information Disclosure**: Dados pessoais expostos.
• **Denial of Service**: Tentativas massivas de login.
• **Elevation of Privilege**: Usuário comum ganha acesso de administrador.

AWS-Simple-Email-Service

• **Spoofing**: Envio de e-mails falsos (phishing).
• **Tampering**: Alteração de mensagens em trânsito.

• **Repudiation**: Remetente nega envio de mensagens.
• **Information Disclosure**: Exposição de listas de contatos.
• **Denial of Service**: Flood de envios até bloquear SES.
• **Elevation of Privilege**: Usuário comum envia em nome de domínios restritos.

AWS-Public-subnet

• **Spoofing**: Serviço falso na subnet pública.
• **Tampering**: Alteração de tráfego público.
• **Repudiation**: Logs incompletos de acessos externos.
• **Information Disclosure**: Exposição de portas/serviços desnecessários.
• **Denial of Service**: Sobrecarga em serviços públicos.
• **Elevation of Privilege**: Serviço exposto usado como pivô de ataque.

AWS-Category_Compute

• **Spoofing**: VMs falsas se passando por instâncias legítimas.
• **Tampering**: Alteração da imagem base ou do código implantado.
• **Repudiation**: Falta de registros de execução.
• **Information Disclosure**: Dados em memória ou logs expostos.
• **Denial of Service**: Exaustão de CPU/RAM por workloads maliciosos.
• **Elevation of Privilege**: Exploração para acesso root/admin.

AWS-Category_Compute

• **Spoofing**: VMs falsas se passando por instâncias legítimas.
• **Tampering**: Alteração da imagem base ou do código implantado.
• **Repudiation**: Falta de registros de execução.
• **Information Disclosure**: Dados em memória ou logs expostos.
• **Denial of Service**: Exaustão de CPU/RAM por workloads maliciosos.
• **Elevation of Privilege**: Exploração para acesso root/admin.

AWS-Backup

• **Spoofing**: Acesso indevido fingindo ser um sistema autorizado.
• **Tampering**: Alteração ou exclusão de backups críticos.
• **Repudiation**: Falta de rastreabilidade em operações de restauração.
• **Information Disclosure**: Exposição de dados sensíveis em backups.
• **Denial of Service**: Sobrecarga de processos de backup.
• **Elevation of Privilege**: Usuário comum acessa backups de nível restrito.

AWS-Scaling-group

• **Spoofing**: Instâncias falsas entram no grupo.
• **Tampering**: Alteração de políticas de escalonamento.
• **Repudiation**: Falta de logs de escalonamento.
• **Information Disclosure**: Exposição de métricas sensíveis.
• **Denial of Service**: Escalonamento excessivo consome recursos.
• **Elevation of Privilege**: Política incorreta gera acesso indevido.

AWS-Private-subnet

• **Spoofing**: Máquina maliciosa dentro da subnet privada.
• **Tampering**: Alteração de regras internas.
• **Repudiation**: Falta de registros de tráfego interno.
• **Information Disclosure**: Dados internos expostos sem VPN.
• **Denial of Service**: Exaustão de recursos internos.
• **Elevation of Privilege**: Máquina sem privilégio acessa rede restrita.

AWS-Scaling-group

• **Spoofing**: Instâncias falsas entram no grupo.
• **Tampering**: Alteração de políticas de escalonamento.
• **Repudiation**: Falta de logs de escalonamento.
• **Information Disclosure**: Exposição de métricas sensíveis.
• **Denial of Service**: Escalonamento excessivo consome recursos.
• **Elevation of Privilege**: Política incorreta gera acesso indevido.

AWS-Public-subnet

• **Spoofing**: Serviço falso na subnet pública.
• **Tampering**: Alteração de tráfego público.
• **Repudiation**: Logs incompletos de acessos externos.
• **Information Disclosure**: Exposição de portas/serviços desnecessários.
• **Denial of Service**: Sobrecarga em serviços públicos.
• **Elevation of Privilege**: Serviço exposto usado como pivô de ataque.

AWS-Private-subnet

• **Spoofing**: Máquina maliciosa dentro da subnet privada.
• **Tampering**: Alteração de regras internas.
• **Repudiation**: Falta de registros de tráfego interno.
• **Information Disclosure**: Dados internos expostos sem VPN.
• **Denial of Service**: Exaustão de recursos internos.

• **Elevation of Privilege**: Máquina sem privilégio acessa rede restrita.

AWS-Res_Elastic-Load-Balancing_Application-Load-Balancer

• **Spoofing**: Cliente falso finge ser legítimo.
• **Tampering**: Alteração maliciosa do tráfego roteado.
• **Repudiation**: Falta de logs confiáveis de requisições.
• **Information Disclosure**: Cabeçalhos ou erros expondo dados.
• **Denial of Service**: Ataques volumétricos (DoS/DDoS).
• **Elevation of Privilege**: Configuração incorreta permite bypass de regras.

AWS-Category_Compute

• **Spoofing**: VMs falsas se passando por instâncias legítimas.
• **Tampering**: Alteração da imagem base ou do código implantado.
• **Repudiation**: Falta de registros de execução.
• **Information Disclosure**: Dados em memória ou logs expostos.
• **Denial of Service**: Exaustão de CPU/RAM por workloads maliciosos.
• **Elevation of Privilege**: Exploração para acesso root/admin.

AWS-Res_Elastic-Load-Balancing_Application-Load-Balancer

• **Spoofing**: Cliente falso finge ser legítimo.
• **Tampering**: Alteração maliciosa do tráfego roteado.
• **Repudiation**: Falta de logs confiáveis de requisições.
• **Information Disclosure**: Cabeçalhos ou erros expondo dados.
• **Denial of Service**: Ataques volumétricos (DoS/DDoS).
• **Elevation of Privilege**: Configuração incorreta permite bypass de regras.

AWS-Res_Elastic-Load-Balancing_Application-Load-Balancer

• **Spoofing**: Cliente falso finge ser legítimo.
• **Tampering**: Alteração maliciosa do tráfego roteado.
• **Repudiation**: Falta de logs confiáveis de requisições.
• **Information Disclosure**: Cabeçalhos ou erros expondo dados.
• **Denial of Service**: Ataques volumétricos (DoS/DDoS).
• **Elevation of Privilege**: Configuração incorreta permite bypass de regras.

AWS-Private-subnet

• **Spoofing**: Máquina maliciosa dentro da subnet privada.
• **Tampering**: Alteração de regras internas.

• **Repudiation**: Falta de registros de tráfego interno.
• **Information Disclosure**: Dados internos expostos sem VPN.
• **Denial of Service**: Exaustão de recursos internos.
• **Elevation of Privilege**: Máquina sem privilégio acessa rede restrita.

AWS-ElastiCache

• **Spoofing**: Cliente falso acessa cache.
• **Tampering**: Alteração de chaves e valores em cache.
• **Repudiation**: Falta de trilhas de auditoria no cache.
• **Information Disclosure**: Dados sensíveis armazenados sem criptografia.
• **Denial of Service**: Exaustão de memória por chaves maliciosas.
• **Elevation of Privilege**: Acesso root ao cluster Redis/Memcached.