SONDA®
make it easy

DESCRITIVO PROFESSIONAL SERVICES TRUSTED ADVISOR PARA CLOUD PÚBLICA

ÍNDICE

1. Versão do Produto

Versão	Escopo	Data de Atualização
Versão 01	Criação do documento	-

2. Descrição Resumida

A **SONDA** conta com uma equipe especializada e certificada para prover consultoria dos mais diversos ambientes de Cloud, proporcionando uma gestão adequada e aderente às melhores práticas do mercado, para ajudar as empresas a serem mais produtivas atuando de maneira preventiva e com soluções completas que melhoram a produtividade do seu negócio, seja qual for o porte da empresa e a complexidade dos processos.

3. Objetivo

O serviço tem como objetivo oferecer uma avaliação de conformidade e utilização de melhores práticas dos ambientes em cloud, apresentando para o **CLIENTE** o resultado das conformidades com o resultado dos testes aprovados, alertas, vulnerabilidades e recomendações necessárias.

4. Benefícios

Os benefícios do serviço são:

- Sugestão de soluções integradas de segurança corporativa desenvolvidas para funcionar em diferentes plataformas e em ambientes na nuvem;
- Priorizar os riscos certos com ferramentas de gerenciamento unificadas criadas para maximizar os conhecimentos dentro de sua organização;
- A automação e o conhecimento de especialistas da **SONDA** ajudam o **CLIENTE** a detectar ameaças com rapidez, responder de forma efetiva e fortalecer a postura de segurança através das melhores práticas em ambientes em nuvem.

4.1. Diferenciais Comerciais

- Conhecimento técnico avançado das principais plataformas em nuvem como AWS, Azure, Google Cloud, OCI, IBM Cloud, entre outras;
- Experiência com serviços e recursos específicos da nuvem, incluindo computação, armazenamento, rede, bancos de dados, serviços gerenciados, entre outros. Além de experiência em implementar as melhores práticas de segurança na nuvem com implementação de políticas de controle de acesso, gerenciamento de identidade e soluções de autenticação segura;
- Habilidade em automação de processos e provisionamento de recursos utilizando as práticas de IaC para provisionar e gerenciar recursos de maneira automatizada;
- Habilidade para projetar e implementar arquiteturas eficientes na nuvem e experiência em arquiteturas baseadas em microsservices e em containers, como por exemplo, Docker e Kubernetes;
- Conhecimento em design de soluções escaláveis, seguras e resilientes, além de habilidade para projetar soluções que possam escalar automaticamente em resposta às demandas variáveis;
- Conhecimento dos modelos de preços e capacidade de analisar detalhadamente os custos associados aos serviços em nuvem para propor otimizações;
- Conhecimento em regulamentações e conformidade relevantes utilizando os melhores frameworks de compliance, como GDPR, HIPAA, ISO 27001;

- Capacidade de atender o **CLIENTE** de forma integrada com as demais soluções digitais da **SONDA**.

5. Escopo de Atuação

A **SONDA** realizará a análise da vulnerabilidade do ambiente de maneira detalhada em todas as camadas e auxiliará o **CLIENTE** a implementar as melhores práticas de segurança identificando falhas e ameaças de exposição de dados.

Diagnóstico do ambiente

- **Configuração de segurança da Conta**
  - Certificar de que as configurações de segurança da conta, como MFA (Autenticação de Multifator) para usuários e contas de root, estejam configuradas corretamente;
  - Avaliar a política de senha e a periodicidade de rotação de credenciais.
- **Análise de Configurações de Segurança**
  - Avaliar a configuração da infraestrutura em busca de possíveis vulnerabilidades e configurações de segurança inadequadas.
- **Controle de Acesso**
  - Revisar as políticas de IAM (Identity and Access Management - IAM) para garantir que as permissões concedidas estejam mínimas e sigam o princípio do menor privilégio;
  - Verificar se há usuários ou contas com permissões excessivas.
- **Auditoria e Monitoramento**
  - Confirmar que os registros de auditoria estão habilitados e configurados corretamente;
  - Avaliar as práticas de monitoramento em tempo real e alertas para atividades suspeitas.
- **Segurança de Dados**
  - Verificar se há dados sensíveis sendo armazenados de forma segura, utilizando criptografia apropriada;
  - Avaliar políticas de retenção de dados e processos de exclusão.
- **Rede e Segurança de Tráfego**
  - Avaliar as configurações de segurança de grupo de segurança e listas de controle de acesso (ACL) para garantir que apenas o tráfego necessário seja permitido;
  - Considerar a utilização de serviços como WAF (Web Application Firewall) para proteger aplicações web.
- **Atualização e Patch**
  - Verificar se as instâncias e serviços estão atualizados com os patches de segurança mais recentes.
- **Resiliência e Recuperação de Desastres**
  - Avaliar as práticas de backup e recuperação para garantir a resiliência contra falhas.
- **Conformidade e Certificações**
  - Verificar se as práticas de segurança estão em conformidade com regulamentações relevantes e indicar certificações, se aplicável.
- **Automação e Orquestração**
  - Indicar a utilização de ferramentas de automação para configurar e monitorar continuamente a conformidade.
- **Produtividade e Colaboração (E-mail Security):** Avaliar a utilização de ferramentas de colaboração com insights e informações que melhoram a segurança do ambiente.
  - Advanced Threat Protection for protection against malware and zero day attacks;
  - Data Loss Prevention to monitor sensitive data from being transmited;
  - Email restrictions link “Do Not Forward” or “Encrypt E-mail”;

- Políticas de Segurança: Antimalware, filtro de spam, proteger e armazenar arquivos confidenciais, tratar a classificação da informação no e-mail conforme a política existente do **CLIENTE**, journaling entre outros.

- **Documentação de Procedimentos:** Criar documentação detalhada de novos procedimentos de segurança;

Implementação de melhorias e Repasse de Conhecimento (Contratação Opcional)

- **Implementação de Melhorias**
  - Implementação das recomendações identificadas na fase de diagnóstico do ambiente;
- **Repasse de Conhecimento**
  - **Repasse de conhecimento da Equipe de TI:** Treinar a equipe de TI sobre novas políticas e ferramentas de segurança;
  - **Workshop:** Oferecer workshop de práticas seguras de uso de recursos em nuvem;

6. Ofertas

O Professional Services de Trusted Advisor é oferecido para os principais provedores de nuvem pública como o Amazon Web Services (AWS), Google Cloud Plataform (GCP), Huawei Cloud , OCI , IBM Cloud e Microsoft Azure e pode ser contratado com em conjunto com a contratação do provedor de nuvem através da **SONDA** ou somente o serviço, quando o **CLIENTE** já possui suas subscrições;

Ao final do serviço, será entregue ao **CLIENTE**:

Diagnóstico do ambiente

- **Elaboração de um Plano de Ação:** Desenvolvimento de um plano detalhado para implementar as recomendações identificadas, incluindo cronograma, recursos necessários e prioridades;
- **Relatórios e Recomendações:** Ao final do assessment, serão entregues para o **CLIENTE** relatórios detalhados com os resultados da avaliação, análise de lacunas e recomendações para melhorias.

Implementação de melhorias e Repasse de Conhecimento (Contratação Opcional)

- Implementação das recomendações identificadas na fase se diagnóstico e repasse do conhecimento;

7. Premissas e Requisitos

- O serviço contempla a avaliação do ambiente do **CLIENTE**, para atividades de habilitação, implementação e configuração devem ser contratadas horas adicionais do serviço;
- O resultado das Análises de Conformidade podem recomendar a contratação e/ou upgrade de licenças que devem ser contratadas a parte e descritas na Proposta Técnica Comercial. A responsabilidade da **SONDA** se restringe às licenças de softwares discriminadas e quantificadas na Proposta Técnica Comercial, bem como pela respectiva manutenção e renovação de suporte destas durante a vigência do Contrato. A **SONDA** também garantirá a conformidade das licenças por ela fornecidas com a infraestrutura disponibilizada na prestação dos serviços ora contratados;
- O serviço não contempla execução de melhorias ou aplicação de recomendações idenificadas.

8. Matriz de Responsabilidade

Para um melhor entendimento a matriz de responsabilidade será classificada com base na metodologia RASICO, onde: **R** - Responsável; **A** - Aprovador; **S** - Suporte; **I** – Informado; **C** – Consulta e **O** - Opcional.

Contratação Opcional?	Atividades	SONDA	CLIENTE
Não	Analisar o ambiente e realizar as recomendações	R	I
Sim	Execução das recomendações (Quando contratado pelo **CLIENTE**)	R	I

Nota: Na Matriz de Responsabilidade existem atividades que são opcionais para o **CLIENTE**, ou seja, é permitido ao mesmo que escolha a **SONDA** como prestadora do serviço ou um outro parceiro. Para essas atividades a coluna "Contratação opcional" é preenchida com "Sim". Portanto, toma-se como premissa, essas atividades como escopo padrão, sendo de responsabilidade do **CLIENTE** sinalizar caso não queira que elas sejam de responsabilidade da **SONDA**.

9. Nível de Serviço

O SLA das plataformas de nuvem, são fornecidos pelos seus respectivos fabricantes.

Antes do início do projeto, será realizada uma reunião inicial entre a equipe **SONDA** e o **CLIENTE** para definir claramente os objetivos do projeto, metas mensuráveis e expectativas em relação aos serviços a serem prestados. Os objetivos e expectativas serão documentados em um plano de trabalho detalhado, que servirá como referência ao longo do projeto.

Será estabelecido um plano de comunicação que inclui canais entre a equipe **SONDA** e o **CLIENTE,** em que a comunicação será realizada regularmente para fornecer atualizações sobre o andamento do projeto, identificando e resolvendo os problemas e solicitando feedback do **CLIENTE**.

A **SONDA** adota uma abordagem proativa para identificar e resolver problemas que possam surgir durante a prestação dos serviços, além de implementar medidas corretivas rapidamente, em colaboração com o **CLIENTE**, para minimizar o impacto nos resultados do projeto.

O tempo de planejamento, execução e reporte serão determinados pelo escopo contratado e dimensionamento da infraestrutura a ser avaliada. Os tempos serão documentados no plano de trabalho detalhado, citado acima.


SONDA
make it easy