SONDA®
make it easy

DESCRITIVO PROFESSIONAL SERVICES SEGURANÇA DA INFORMAÇÃO

ÍNDICE

1. Versão do Produto

Versão	Escopo	Data de Atualização
Versão 01	Criação do documento	-

2. Descrição Resumida

Atualmente, existem milhões de ameaças que podem danificar os ambientes de TI das organizações, o que afeta a integridade e a continuidade do negócio, gerando perdas monetárias significativas devido à indisponibilidade dos serviços afetados. Nesse sentido, as organizações devem estar preparadas para enfrentar as ameaças ou violações de seus ambientes de TI, mas geralmente não possuem os recursos ou ferramentas para atingir esse objetivo.

Nesse contexto, a **SONDA** gerencia a segurança dos ambientes de TI de nossos **CLIENTES** por meio do serviço de gerenciamento de segurança de TI. Neste serviço, a **SONDA** é responsável por fornecer, gerenciar e suportar as ferramentas necessárias para proteger os ambientes de TI, apoiando a continuidade e integridade dos mesmos para que nossos **CLIENTES** se sintam seguros, permitindo o desenvolvimento ideal de suas atividades diárias de negócios.

3. Objetivo

O Professional Services da Segurança da Informação é uma solução que integra as tecnologias de segurança essenciais com especialistas no gerenciamento do serviço para prover controle e políticas altamente eficazes contra:

- Proteção contra vírus, spywares, cavalos de tróia, worms, bots e rootkits;
- Segurança contra hackers;
- Proteção contra intrusões do host, através de análise baseado em assinaturas;
- Segurança do navegador da Web, identificando sites não confiáveis e perigosos já nos resultados da pesquisa;
- Configuração de políticas de antivírus, IPS, firewall e de exceções específicas para o **CLIENTE** ou para grupo de máquinas;

Objetivando assim:

- Melhorar a confidencialidade, integridade e segurança dos ambientes de TI;
- Aumentar o controle sobre as plataformas através do gerenciamento de segurança dos ambientes de TI de nossos **CLIENTES;**
- Reduzir incidentes de segurança por meio de gerenciamento especializado;
- Fornecer recomendações de segurança aos nossos **CLIENTES**.

4. Benefícios

Os benefícios do serviço são:

- Detectar e agir contra ameaças ou vulnerabilidades de segurança de forma mais eficiente;
- Reduzir incidentes de segurança e riscos em ambientes de TI;
- Disponibilizar especialistas em segurança em ambientes de TI;
- Suporte a conformidade com regulamentações legais e padrões do setor em questões de segurança (ISO / IEC 27001, SOX, PCI, Basiléia II e outros);
- Suporte a disponibilidade de serviços e ambientes de TI.

4.1. Diferenciais Comerciais

- Equipe qualificada e certificada em produtos líderes no mercado;
- Vasta experiência em ambientes distintos (Nuvem ou Local);
- Equipe Multidisciplinar em produtos de segurança.

5. Escopo de Atuação

- Gestão de Endpoint Security;
- Gestão de AntiSpam;
- Gestão de Ferramenta de Análise de Vulnerabilidade;
- Gestão de Sistema de Cofre de Senhas;
- Integração de Monitoramento de Logs de Segurança de Soluções de Firewall;
- Melhores práticas para regras de Sistema de Detecção de Intrusão;
- Gerenciamento de Ferramenta de Anti-DDoS com Emissão de Relatórios.

6. Ofertas

O Professional Services de segurança da informação engloba suporte especializado, avaliações de riscos, implementação de soluções de segurança, monitoramento proativo, resposta a incidentes e atendimento para proteger os dados e sistemas dos **CLIENTES** contra ameaças cibernéticas, garantindo conformidade regulatória e tranquilidade para os **CLIENTES**.

7. Monitoramento

Para atuar de forma preventiva e preditiva, a **SONDA** oferece o serviço de Monitoramento que coleta dados dos itens monitorados e identifica condições que indicam a saúde do ambiente, sinalizando possíveis riscos ou sucessos operacionais.

O **CLIENTE** tem acesso ao portal da ferramenta de monitoramento, onde pode visualizar dados e relatórios detalhados, garantindo total transparência e a certeza de que o ambiente está sendo continuamente gerido e acompanhado pela equipe **SONDA**.

Além disso, o serviço conta com integração entre nosso ITSM e o Monitoramento por meio da ferramenta de Enterprise Application Integration (EAI), permitindo a abertura automática de chamados sempre que uma anomalia for detectada. Isso reduz significativamente o tempo de resposta a qualquer irregularidade no ambiente.

8. Premissas e Requisitos

- Licenciamento de Softwares;
    - Endpoint Security;
    - AntiSpam;
    - Ferramenta de Análise de Vulnerabilidade;
    - Cofre de Senhas;
    - SIEM;
    - IPS;
    - Anti-DDoS.
- Suporte vigente com os fabricantes das ferramentas descritos acima.

9. Matriz de Responsabilidade

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

Atividades	SONDA	CLIENTE
Gerar relatórios do ambiente do **CLIENTE**	R	
Gerar lista de logs do ambiente do **CLIENTE**	R	
Criar e alterar políticas	R	
Apresentar os requisitos de negócio para as políticas de Proteção de Segurança		R
Apresentar os requisitos de negócio para as políticas de Segurança		R
Criar e alterar políticas de Prevenção contra Intrusões	R	
Apresentar os requisitos de negócio para as políticas de Prevenção contra Intrusões		R
Criar e alterar políticas de Firewall	R	
Apresentar os requisitos de negócio para as políticas de Firewall		R
Criar e alterar políticas de Prevenção contra Intrusões	R	
Apresentar os requisitos de negócio para as políticas de Prevenção contra Intrusões		R
Criar e alterar políticas de Controle de dispositivos e aplicativos	R	
Apresentar os requisitos de negócio para as políticas de Controle de dispositivos e aplicativos		R
Criar e alterar políticas de LiveUpdate	R	
Apresentar os requisitos de negócio para as políticas de LiveUpdate		R
Criar e alterar políticas de exceções	R	
Apresentar os requisitos de negócio para as políticas de exceções		R
Alterar configurações gerais dos servidores	R	

10.Requisição de Serviço

A tabela abaixo lista as requisições de serviços disponíveis para solicitações dos **CLIENTES** assim como seu tempo de solução e horário de cobertura.

Requisição	Classificação	Tempo de Solução
Administração de Antivírus – criar usuário	D	Conforme TS contratado
Administração de Antivírus – bloquear usuário	D	Conforme TS contratado
Administração de Antivírus – reset de senha	D	Conforme TS contratado
Administração de Antivírus – criar política	A	Conforme TS contratado
Administração de Antivírus – remover política	A	Conforme TS contratado
Administração de Antivírus – alterar política	A	Conforme TS contratado
Administração de Antivírus – liberar arquivo bloqueado	A	Conforme TS contratado
Administração de Antivírus – configuração de manager	C	Conforme TS contratado
Administração de Antivírus – atualização da aplicação	F	Conforme TS contratado
Administração de Antivírus – analisar computador infectado	A	Conforme TS contratado
Administração de Antivírus – gerar relatório	F	Conforme TS contratado


SONDA
make it easy