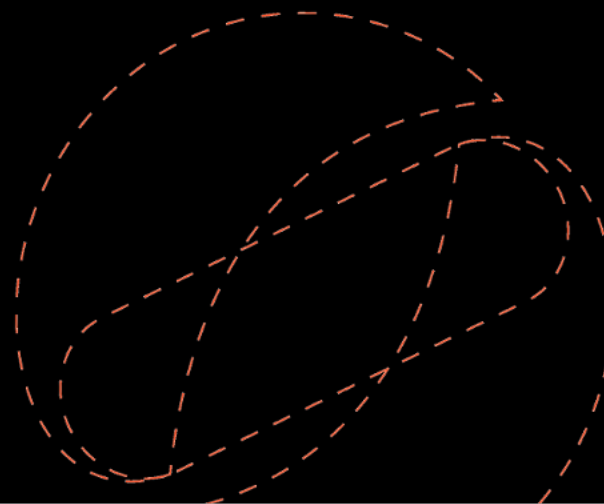


DIGITAL FOOTPRINT SECURITY RATING SMB

Conheça o nível da sua segurança, ou de terceiros, exposta na Internet e saiba como diminuir os riscos



BENEFÍCIOS

- ◆ Conhecimento do nível de segurança (própria e de terceiros) exposto na Internet, e a evolução no tempo
- ◆ Entendimento dos riscos relacionados
- ◆ Informações disponíveis para a melhor tomada de decisão
- ◆ Demonstração de diligência na condução dos negócios perante terceiros
- ◆ Avaliação independente das ações realizadas, processos implementados e tecnologias utilizadas

Visão geral

A presença na Internet, de qualquer organização, expõe publicamente suas fraquezas, sem qualquer necessidade de acesso privilegiado para verificá-las. Essas informações podem ser utilizadas por cibercriminosos, concorrentes, ou até mesmo clientes e fornecedores, ou em processos de M&A. Mas o mais importante é que ela seja utilizada por você para mitigar todos os riscos relacionados, inclusive os de imagem.

Empresas com *rating* baixo têm de 3 a 5 vezes maiores chances de sofrerem incidentes de segurança.

O serviço DIGITAL FOOTPRINT SECURITY RATING SMB foi desenvolvido para atender essa demanda crescente e recorrente do mercado, utilizando metodologia e tecnologia líderes.

Para quem é indicado

Empresas que necessitam avaliar ou reavaliar o seu nível de segurança, ou o de terceiros, exposto na Internet.

Produtos finais

- ◆ Relatório de avaliação do seu nível de segurança, ou o de terceiros, exposto na Internet, através de uma visão “outside-in”;
- ◆ Visão evolutiva e comparação com o mercado;
- ◆ Plano de ação para incrementar o nível de segurança exposto na Internet, de acordo com o diagnóstico apresentado.

CONTRATOS



On Demand



Managed Services



Umbrella



Retainer

Escopo Avaliado

O Serviço DIGITAL FOOTPRINT SECURITY RATING tem escopo de análise pré-definido:

- ◆ **Network Security:** avalia uso de portas e protocolos de alto risco, além de itens relacionados;
- ◆ **Endpoint Security:** analisa dados de segurança dos endpoints de acordo com dados públicos informados via sistema operacional, web browser e plugins;
- ◆ **Application Security:** verifica a presença de vulnerabilidades conhecidas em aplicações, via whitehat CVE databases, blackhat exploit databases, e outros;
- ◆ **Patching:** avalia quão rapidamente uma organização instala as correções de segurança disponibilizadas pelos fabricantes mundiais de tecnologia, como Microsoft e outros;
- ◆ **DNS Security:** valida a configuração pública do DNS e verifica se não ocorreram eventos maliciosos através da “passive DNS history” das organizações;
- ◆ **Malware Exposure:** verifica se a organização está contaminada por agentes maliciosos, através do uso de sinkhole, OSINT malware feeds e dados de inteligência de ameaças (deep, dark e clear web);
- ◆ **Information Leak:** analisa deep, dark e clear web para verificar o vazamento de credenciais ou dados da organização.

Mais informações em www.safontreis.com

SAFONT REIS

Av. Cauaxi, 370, Unid. 161 | Alphaville
Barueri/SP | CEP: 06454-020
info@safontreis.com.br
+55 11 97657-6777

Sobre nossa empresa

Somos independentes. Não trabalhamos com vendedores, mas com advisors. Não representamos ou estamos comprometidos com fabricantes, produtos ou soluções. Estamos do lado do cliente, somos os olhos do cliente. Entendemos o negócio e as necessidades, avaliamos a situação, e recomendamos os próximos passos, baseados em uma equipe com 25 anos de experiência, trabalhando com os maiores clientes e projetos do Brasil.