SIDKRON

ESPECIALISTAS EM GESTÃO DE RISCO CIBERNÉTICO

A Sidkron é uma empresa brasileira especializade em Segurança Cibernética, com **atuação nacional e internacional**, apoiando organizações na proteção de seus ambientes digitais contra ameaças cada vez mais sofisticadas.

Atuamos com foco estratégico em **Gestão de Risco Cibernético**, integrando tecnologia, inteligência ofensiva e visão de negócio para entregar soluções alinhadas à realidade operacional de cada empresa.

Nosso diferencial está na combinação entre expertise técnica, metodologia própria e atendimento consultivo, permitindo que nossos clientes tenham **visibilidade real sobre seus riscos** e maior capacidade de resposta diante de vulnerabilidades críticas.

Contamos com profissionais altamente qualificados, experiência prática em ambientes corporativos complexos e metodologias alinhadas às **principais referências internacionais de segurança.**

A SIDKRON AJUDA EMPRESAS A:

IDENTIFICAR
vulnerabilidades críticas antes que sejam exploradas por atacantes.

REDUZIR
riscos operacionais, financeiros e de conformidade.

FORTALECER
a maturidade em segurança cibernética e a resiliência digital da organização.

APOIAR
requisitos de compliance, LGPD e normas do seu segmento.

TOMAR DECISÕES
com mais segurança, clareza e previsibilidade.

CIBERSEGURANÇA NÃO É APENAS PROTEÇÃO TECNOLÓGICA.

É CONTINUIDADE, REPUTAÇÃO E ESTRATÉGIA DE NEGÓCIO.

A Sidkron é sua parceira estratégica para transformar segurança em vantagem competitiva e proteger o que realmente importa: **seus dados, sua operação e o futuro da sua empresa.**

SIDKRON

PENTEST SIDKRON

Sua empresa pode estar exposta neste exato momento — sem perceber.

Ataques cibernéticos deixaram de ser uma possibilidade distante. Hoje, empresas de todos os portes convivem diariamente com riscos invisíveis capazes de **comprometer operações, dados, reputação e continuidade do negócio.**

O Pentest da Sidkron vai além de uma simples análise técnica. Simulamos **ataques reais** para identificar vulnerabilidades exploráveis antes que criminosos digitais façam isso.

Nossa abordagem combina inteligência ofensiva, metodologia própria e visão estratégica de risco cibernético para entregar **clareza, priorização e segurança** para a tomada de decisão.

Mais do que identificar falhas, ajudamos organizações a fortalecerem sua **resilência digital**, protegerem dados sensíveis e **reduzem impactos financeiros, operacionais e reputacionais.**

IDENTIFICAMOS VULNERABILIDADES ANTES QUE SEJAM EXPLORADAS.

REDUZIMOS RISCOS OPERACIONAIS, FINANCEIROS E LEGAIS.

PROTEGEMOS DADOS, SISTEMAS E A REPUTAÇÃO DA SUA EMPRESA.

FORTALECEMOS A MATURIDADE EM CIBERSEGURANÇA E A CONTINUIDADE DO NEGÓCIO.

Empresas maduras
não esperam sofrer um ataque
para descobrir suas vulnerabilidades.

SIDKRON

BENEFÍCIOS DO PENTEST

Mais do que identificar falhas, o Pentest entrega **clareza** sobre seus riscos e fortalece sua empresa para enfrentar ameaças com **inteligência, prevenção** e **estratégia**.

01 GERENCIAR VULNERABILIDADES E AMEAÇAS

Identifique, priorize e trate riscos de forma inteligente, antes que sejam explorados por atacantes.

02 ATENDER NORMAS REGULATÓRIAS

Apoie iniciativas de compliance como PCI-DSS, LGPD e outras normas, demonstrando governança e responsabilidade.

03 PRESERVAÇÃO DA IMAGEM CORPORATIVA

Reduza riscos de incidentes que podem impactar sua reputação, marca e confiança do mercado.

04 INSIGHTS PARA LÍDERES E GESTORES

Relatórios executivos claros e objetivos que apoiam decisões estratégicas e investimentos assertivos.

05 FORTALECE A CONFIANÇA E FIDELIDADE DO CLIENTE

Demonstre compromisso com a proteção de dados e a segurança da informação, gerando mais confiança e competitividade.

06 AVALIA O IMPACTO DE UM ATAQUE REAL

Entenda como sua empresa seria impactada em um cenário real e prepare-se para minimizar danos.

TIPOS DE PENTEST

Avaliamos seu ambiente sob diferentes perspectivas para entregar uma visão completa dos seus riscos.

EXTERNAL
Avaliação do acesso a dados ou sistemas críticos a partir da internet.

INTERNAL
Avaliação do ambiente de TI da empresa sob o ponto de vista da rede interna.

MOBILE APPLICATION
Testes em aplicativos móveis (Android, iOS) e componentes de back-end (APIs, Web Services, etc).

WEB APPLICATION E API
Avaliação da resiliência de aplicações web e APIs por um atacante dedicado.

WI-FI
Avaliação do acesso a dados e sistemas críticos a partir da rede de acesso Wi-Fi.

FÍSICO
Identificação e exploração de vulnerabilidades em estruturas físicas e controles de acesso.

DESKTOP
Avaliação de resiliência de aplicações desktop instaladas em estações de trabalho.

VISIBILIDADE. PROTEÇÃO. CONTINUIDADE. RESULTADOS.

O Pentest da Sidkron entrega o conhecimento que sua empresa precisa para se antecipar às ameaças e evoluir sua postura de segurança.

Empresas maduras não esperam sofrer um ataque para descobrir suas vulnerabilidades. **Elas se antecipam.**

SIDKRON

MODALIDADES DE PENTEST

Três abordagens. Três níveis de visibilidade. Um único objetivo: proteger seu negócio.

WHITE BOX

- Todas as informações do cliente sobre a rede, servidores, banco de dados e sistemas que estão inclusos no escopo do teste de invasão, e demais informações de acesso aos mesmos, são fornecidas para que possam ser realizados **testes extensivos e com mais abrangência.**

INVESTIMENTO MENOR

GRAY BOX

- Esse tipo de análise o Pentester recebe alguma **informação do cliente,** como dados da infraestrutura da rede ou acesso a determinado serviço web.
- Um bom exemplo de teste Gray Box são aqueles direcionados para analisar possíveis falhas de segurança em uma aplicação vinda através de um **usuário credenciado**, como níveis de permissões de acesso e alterações não autorizadas.

INVESTIMENTO INTERMEDIÁRIO

BLACK BOX

- É o tipo de análise mais próximo de um ataque externo, pois nenhuma informação vinda do cliente é fornecida ao analista de teste. Sendo assim toda e qualquer informação é adquirida através de **técnicas específicas de hacking sobre os serviços disponíveis do alvo.**

INVESTIMENTO MAIS ALTO

"A Sidkron possui **metodologia própria, qualificação técnica** e **diferenciais** no mercado para realizar qualquer uma das **três modalidades de Pentest.**

- Metodologia própria
- Qualificação técnica
- Diferenciais no mercado
- Segurança em todas as perspectivas

SIDKRON

COMO FUNCIONA NOSSO PENTEST

Seguimos um processo estruturado, ético e controlado, garantindo segurança na execução, comunicação transparente e resultados que realmente geram impacto para o seu negócio.

Do planejamento ao relatório final, cada etapa é conduzida com foco em identificar riscos críticos e apoiar sua empresa na tomada de decisões estratégicas.

O QUE ESTÁ INCLUSO

Um serviço completo, do início ao fim, com entregas claras e acionáveis.

01 — PLANEJAMENTO E ALINHAMENTO
Entendimento do ambiente, definição do escopo, objetivos, regras de engajamento e janelas de execução.

02 — RECONHECIMENTO E COLETA DE INFORMAÇÕES
Mapeamento do ambiente e coleta de informações públicas e técnicas para identificar possíveis vetores de ataque.

03 — ANÁLISE E IDENTIFICAÇÃO DE VULNERABILIDADES
Varredura, análise manual e identificação de falhas exploráveis que podem ser utilizadas por um atacante.

04 — EXPLORAÇÃO E TESTES DE INTRUSÃO
Execução controlada de técnicas de ataque para validar as vulnerabilidades e avaliar o impacto real no ambiente.

05 — PÓS-EXPLORAÇÃO E MOVIMENTAÇÃO
Avaliação de escalação de privilégios, movimentação lateral e acesso a dados sensíveis.

06 — RELATÓRIO TÉCNICO E EXECUTIVO
Entrega de relatórios claros, com evidências, nível de risco, impacto e recomendações práticas para correção.

07 — APRESENTAÇÃO E RECOMENDAÇÕES
Reunião de apresentação dos resultados e alinhamento do plano de ação para mitigar os riscos identificados.

NOSSO COMPROMISSO COM SEU NEGÓCIO

- Execução ética, segura e autorizada, sem impacto na operação do ambiente.
- Confidencialidade total em todas as etapas do projeto.
- Relacionamento próximo, com comunicação clara e transparente.
- Foco em entregar valor real e apoiar decisões estratégicas.
- Compromisso com a melhoria contínua da segurança e maturidade da sua empresa.

Visibilidade completa. Riscos identificados.
Decisões seguras. Negócio protegido.

Entregamos mais do que relatórios.
Entregamos clareza, prioridade e segurança para o que realmente importa:
a continuidade do seu negócio.

SIDKRON

NOSSO PROCESSO EM 6 ETAPAS

Um fluxo estruturado para garantir que cada avaliação seja completa, profunda e gere valor real para o seu negócio.

01 PLANEJAMENTO

Entendemos o seu negócio, definimos objetivos, escopo, regras de engajamento e alinhamos expectativas.

02 COLETA DE INFORMAÇÕES

Mapeamos o ambiente, pessoas, tecnologias e processos para identificar pontos de exposição e possíveis vetores de ataque.

03 ANÁLISE E IDENTIFICAÇÃO DE VULNERABILIDADES

Realizamos varreduras, análise manual e testes para identificar falhas exploráveis e avaliar o nível de risco.

04 EXPLORAÇÃO E TESTES DE INTRUSÃO

Exploramos de forma controlada as vulnerabilidades identificadas para validar impactos e comprovar riscos reais.

05 PÓS-EXPLORAÇÃO E MOVIMENTAÇÃO

Avaliamos a escalada de privilégios, movimentação lateral e acesso a dados sensíveis para medir o impacto potencial completo.

06 RELATÓRIO E RECOMENDAÇÕES

Entregamos um relatório técnico e executivo detalhado, com evidências, análise de risco e um plano de ação priorizado.

O QUE VOCÊ RECEBE

RELATÓRIO TÉCNICO COMPLETO
Detalhamento das descobertas, evidências, impacto, nível de risco e recomendações de correção.

RELATÓRIO EXECUTIVO
Visão clara e estratégica para líderes e gestores, com os principais riscos e prioridades.

PLANO DE AÇÃO PRIORITÁRIO
Recomendações práticas e priorizadas para mitigação dos riscos identificados.

APRESENTAÇÃO DE RESULTADOS
Reunião de alinhamento para apresentação dos resultados, esclarecimentos e próximos passos.

SUPORTE PÓS-TESTE
Esclarecimento de dúvidas e apoio na priorização das correções após a entrega do relatório.

NÍVEIS DE RISCO

Classificamos as vulnerabilidades com base no impacto e na probabilidade de exploração.

CRÍTICO
Exploração fácil e alto impacto. Ação imediata necessária.

ALTO
Exploração possível com impacto significativo. Correção prioritária.

MÉDIO
Exploração moderada e impacto limitado. Correção recomendada.

BAIXO
Exploração difícil e impacto reduzido. Correção conforme disponibilidade.

INFORMATIVO
Achados informativos que não representam risco direto, mas podem ajudar na melhoria contínua.

UM PROCESSO RIGOROSO, TRANSPARENTE E FOCADO EM PROTEGER O QUE MAIS IMPORTA: SEU NEGÓCIO.

- Foco no que realmente importa
- Segurança com excelência
- Transparência em cada etapa
- Resultados que geram impacto

SIDKRON

AFINAL, QUANTAS VEZES É NECESSÁRIO REALIZAR O PENTEST?

O Pentest deve ser realizado **regularmente** para garantir um gerenciamento de segurança de rede e dos negócios;

A equipe da Sidkron busca revelar como ameaças recém descobertas podem ser potencialmente utilizadas por invasores. Além de análises regularmente agendadas, os testes também devem ser executados sempre que uma **nova estrutura ou aplicação** for inserida na rede; houver **atualizações ou modificações significativas** aplicadas à infraestrutura de rede e sistemas; **novos escritórios** forem construídos; as **políticas de segurança** forem modificadas ou houver **troca de colaboradores**.

Contratar uma **Análise de Vulnerabilidades** é diferente de se contratar um **Pentest.** Infelizmente algumas empresas têm vendido Análise de Vulnerabilidades como sendo Pentest para poder oferecer um custo mais acessível para o cliente, seja por desconhecimento ou intencionalmente.

Mas, não é a mesma coisa!

Por isso, a Sidkron elaborou uma tabela comparativa para explicar melhor as principais diferenças existentes e "**não comprar gato por lebre**". E em se tratando de Segurança Digital, isso é muito sério. A empresa pode contratar apenas uma Análise de Vulnerabilidades, mas precisa estar claro para ela o que de fato vai receber.

TESTES REGULARES GARANTEM:

- Gestão contínua de riscos
- Identificação de ameaças recentes
- Adaptação a mudanças na infraestrutura
- Proteção em novos cenários
- Segurança para o seu negócio

SIDKRON

TABELA COMPARATIVA ENTRE ANÁLISE DE VULNERABILIDADES X PENTEST

CATEGORIAS	ANÁLISE DE VULNERABILIDADES	PENTEST
OBJETIVOS	Identificar e listar as falhas de redes e sistemas; Detectar o maior número possível de riscos, sem necessariamente analisar profundamente cada um deles.	Simular um ataque hacker para identificar vulnerabilidades de segurança e apontar soluções; Identificar vulnerabilidades específicas e avaliar as defesas do sistema.
EXECUÇÃO	• O processo é todo automatizado com o uso de software que busca pontos de falha. Exemplos: Qualys, Nessus, Openvas, entre outros; • Scanners de vulnerabilidades ativos funcionam por demanda, varrendo sistemas, máquinas e redes em busca de pontos sensíveis; • Scanners passivos realizam varreduras ocasionais em períodos predeterminados.	• Testagem de sistemas, redes, aplicações web e mobile em busca de vulnerabilidades exploráveis por cibercriminosos; • Exposição de informações e dados sujeitos a roubos e outras falhas; • Avaliação da eficácia dos mecanismos de proteção e apontamento das soluções; • Busca por vazamentos de dados possivelmente expostos na Internet; • Utilização da engenharia social para obtenção de credenciais e outras informações.
PRINCIPAIS TIPOS	✓ Estática; ✓ Dinâmica.	✓ **White Box**: fornece muitas informações à equipe de testes; ✓ **Black Box**: não fornece informações prévias sobre o sistema; ✓ **Gray Box**: combina elementos de White Box e Black Box.
PRÓS	✓ Não exige conhecimento avançado; ✓ Menor tempo de execução do projeto; ✓ Custo mais baixo.	✓ Utiliza mão-de-obra mais qualificada; ✓ É uma abordagem mais prática e interativa para avaliar a segurança de um sistema, simulando ataques reais; ✓ Relatório mais detalhado; ✓ A saída típica é um relatório detalhado que descreve as técnicas utilizadas, as vulnerabilidades exploradas, o impacto social de um ataque bem-sucedido e recomendações para melhorar a segurança.
CONTRAS	✗ As falhas identificadas não são exploradas a fundo para determinar seu impacto total ou se são realmente exploráveis; ✗ Ocorrência de muitos falsos positivos; ✗ Os cibercriminosos não utilizam ferramentas de análise de vulnerabilidades para comprometer a segurança de uma empresa, logo fica distante do que seria um ataque real.	✗ Custo maior, variando conforme o tipo de Pentest escolhido; ✗ Maior tempo de execução do projeto; ✗ Escassez de mão-de-obra qualificada no mercado para execução do serviço.

QUAL ESCOLHER?

A **Análise de Vulnerabilidades** é ideal para identificar o maior número possível de falhas de forma rápida, preventiva e com **menor custo**.

O **Pentest** é ideal para entender como as falhas podem ser exploradas por **atacantes reais** e como melhorar a segurança de forma efetiva.

Ambas as abordagens são **complementares** e **essenciais** para uma estratégia de segurança completa e eficaz.

SIDKRON

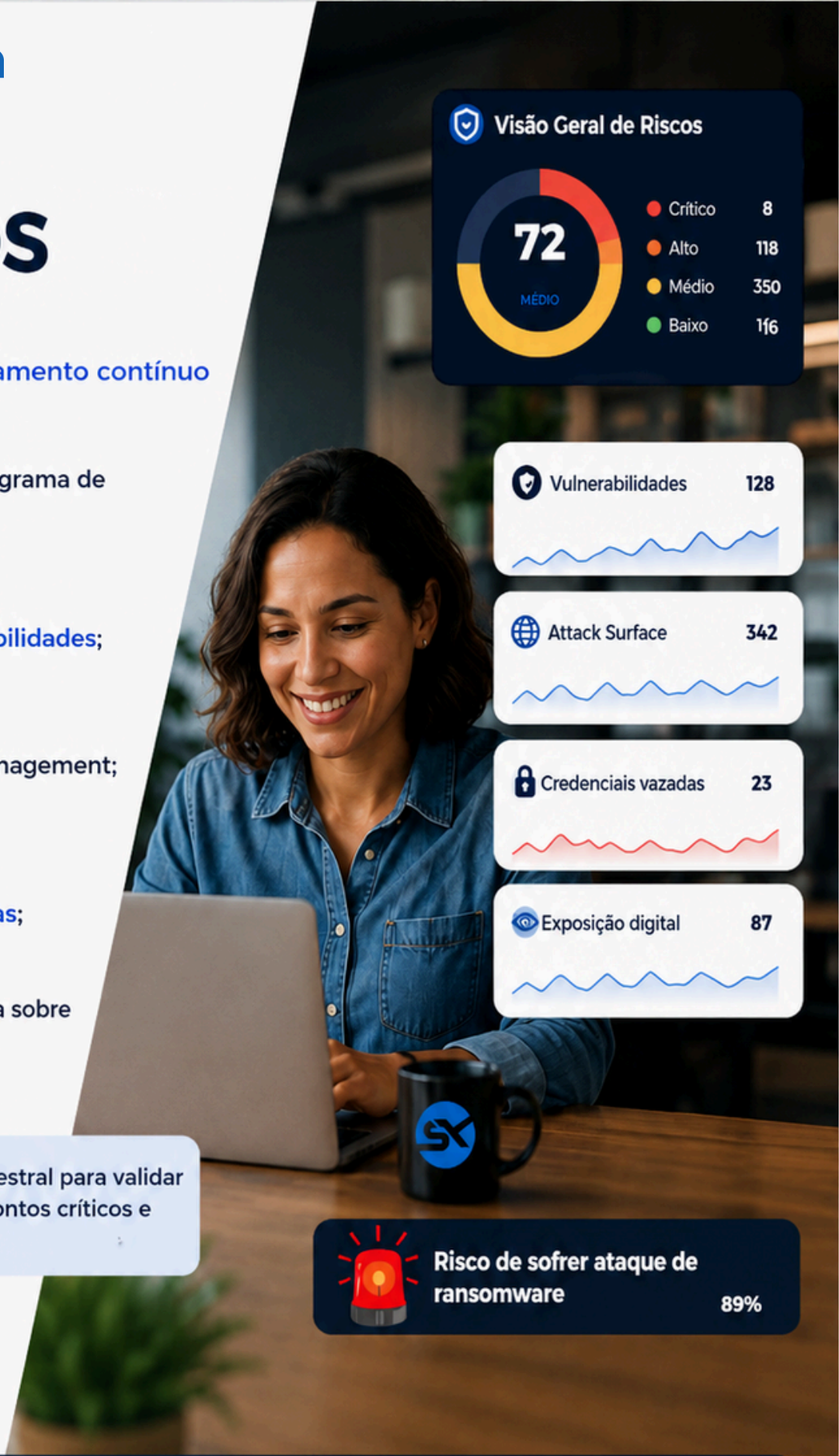
OUTROS SERVIÇOS

Um programa de monitoramento contínuo de riscos cibernéticos.

A Sidkron desenvolve um programa de gestão que centraliza:

- Gestão de vulnerabilidades;
- Attack Surface Management;
- Monitoramento de credenciais vazadas;
- Visibilidade contínua sobre riscos digitais.

Pentest anual ou semestral para validar a LGPD e identificar pontos críticos e vulnerabilidades.



Transformamos cibersegurança em algo acessível para empresas que antes estavam desassistidas.

SIDKRON

Sua próxima decisão protege o futuro do seu negócio.

A cibersegurança não precisa ser complexa para ser eficaz.

Com estratégia, tecnologia e parceria, transformamos risco em confiança e proteção em vantagem competitiva.

Vamos construir juntos um ambiente digital mais seguro para o seu negócio.

Fale com a gente!

+55 62 99403-5858

sidkron.com

contato@sidkron.com.br

Escaneie e fale conosco.

Juntos, vamos tomar o ambiente digital mais seguro para todos.

A segurança da informação é mais do que tecnologia.
É confiança, continuidade e crescimento sustentável.