RNP
ORGANIZAÇÃO SOCIAL DO MCTI

GT-Periscope

GT-PERISCOPE: Uma Ferramenta para Predição de Ataques DDoS por Meio da Identificação Precoce de Botnets

Wagner Monteverde - Coordenador

Sherlock-X
Cyber Security Platform.

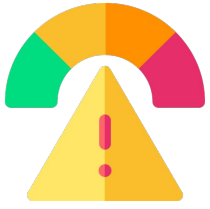
Apresentação Final dos GTs para RNP
Ciclo 2020-2021

EARLYSEC

UFPR
UNIVERSIDADE FEDERAL DO PARANÁ

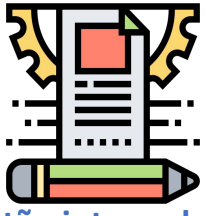
Sherlock-X

Detecção e Gestão de Vulnerabilidades



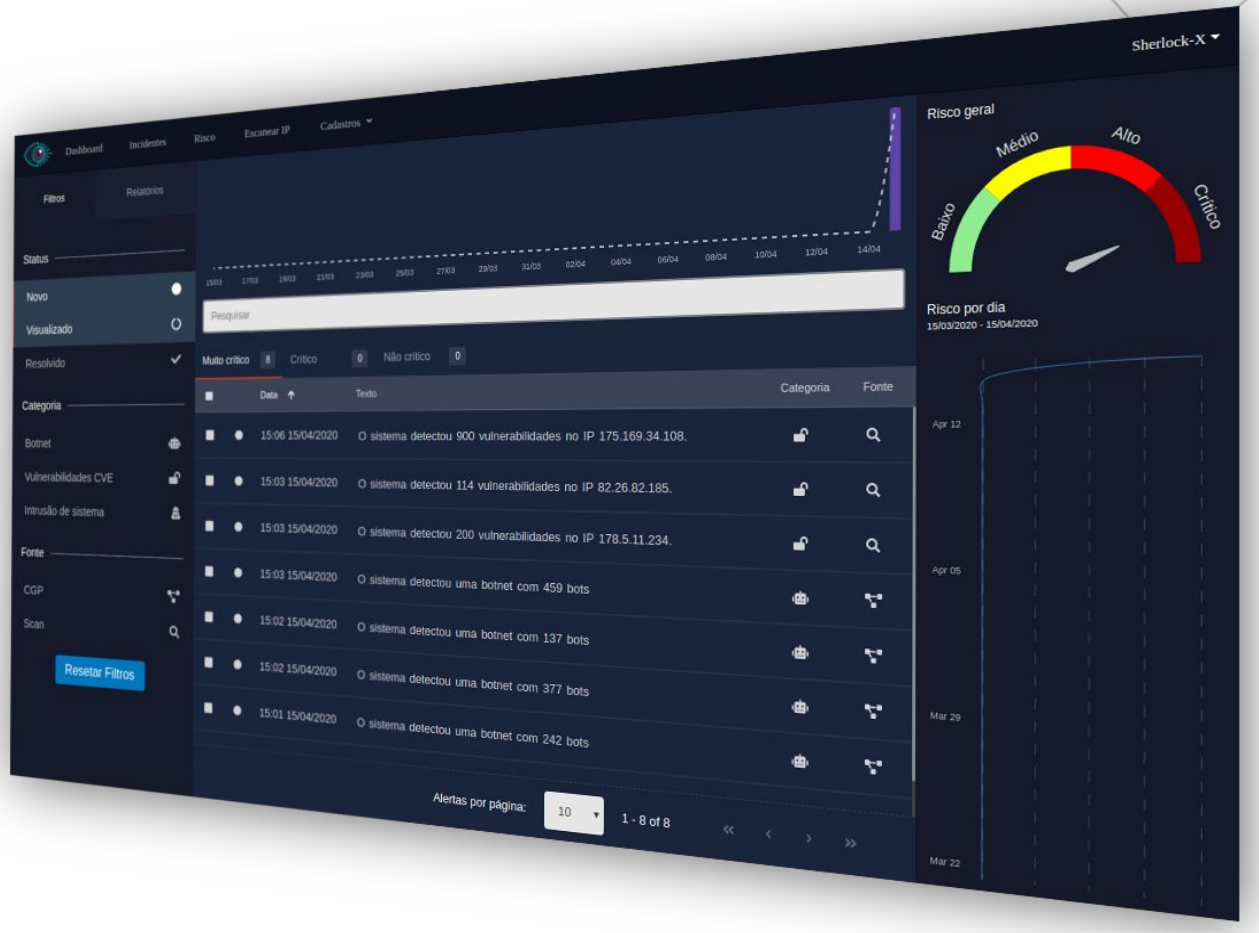
Índice de risco

Detecção de tráfego malicioso (bots)



Gestão integrada de incidentes

Recomendações de soluções



ISO 27001

PCI Security Standards Council

NIST National Institute of Standards and Technology U.S. Department of Commerce

LGPD Lei Geral de Proteção de Dados Pessoais

RNP 30 anos
ORGANIZAÇÃO SOCIAL DO MCTIC

Evoluções do Produto

GT-Periscope

Sherlock-X
Cyber Security Platform.

Sherlock-X
Arquitetura

Recursos

Interface WEB

Middleware

Módulos da inteligência

Amazon Cloud

EC2

WAF

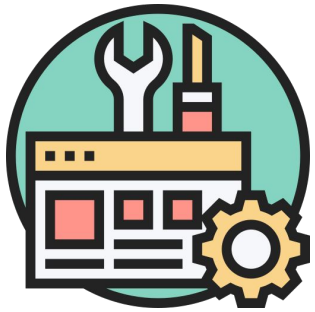
VPC

Cloud Front

Fonte dos ícones: flaticon.com

GT-Periscope Fase 2

Evolução MVP

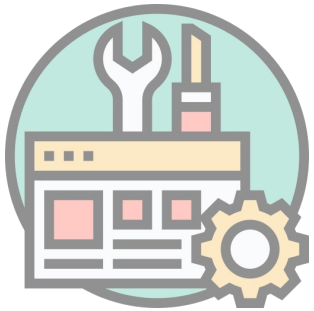


Recomendações paras as vulnerabilidades

Fonte dos ícones: flaticon.com

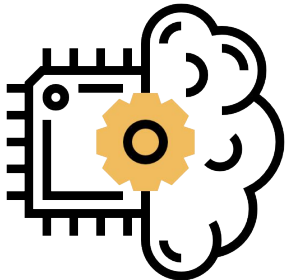
GT-Periscope Fase 2

Evolução MVP



Recomendações paras as vulnerabilidades

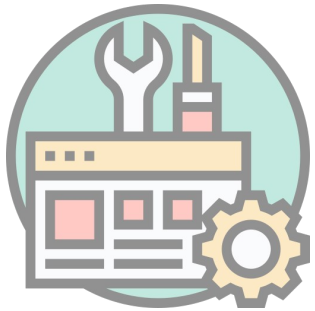
Otimização motor de vulnerabilidades



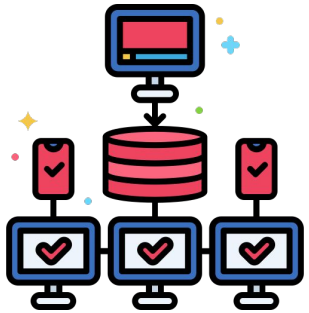
Fonte dos ícones: flaticon.com

GT-Periscope Fase 2

Evolução MVP

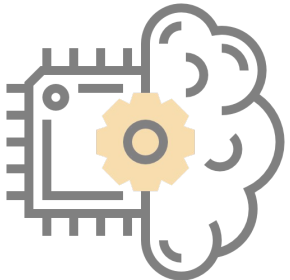


Recomendações paras as vulnerabilidades



Otimização do sensor de análise de botnets

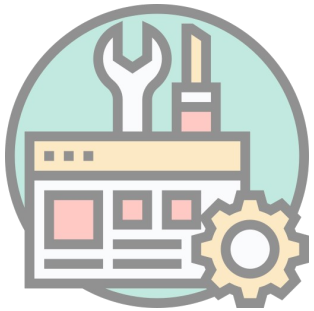
Otimização motor de vulnerabilidades



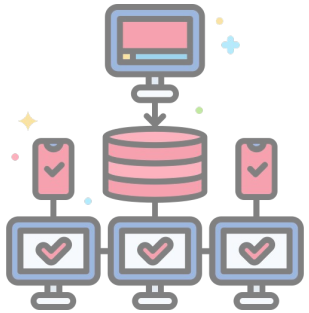
Fonte dos ícones: flaticon.com

GT-Periscope Fase 2

Evolução MVP

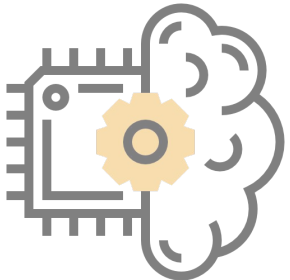


Recomendações paras as vulnerabilidades



Otimização do sensor de análise de botnets

Otimização motor de vulnerabilidades



Lançamento da landing page

Fonte dos ícones: flaticon.com

GT-Periscope Fase 2

Comparação entre soluções similares

Ativo	Shodan	OpenVAS	Sherlock-X
1	0	0	2
2	18	14	28
3	61	0	34
4	0	0	2
5	46	2	20
6	0	0	0
7	61	13	34
8	57	10	20
9	0	0	0
10	0	0	0
11	60	15	56

GT-Periscope Fase 2

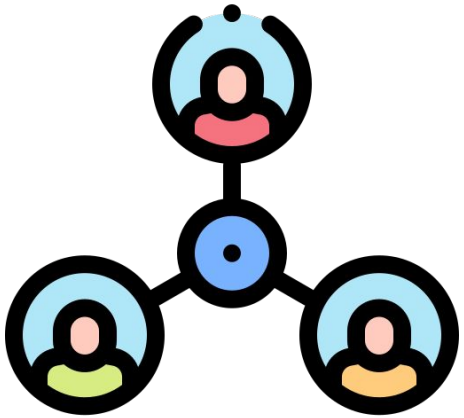
Comparação entre soluções similares

Índice médio de FP Shodan (%)	Índice médio de FN Shodan (%)	Índice médio de FP OpenVAS (%)	Índice médio de FN Openvas (%)	Índice médio de FP Sherlock-x (%)	Índice médio de FN Sherlock-x (%)
46%	26%	0%	53%	0%	3%

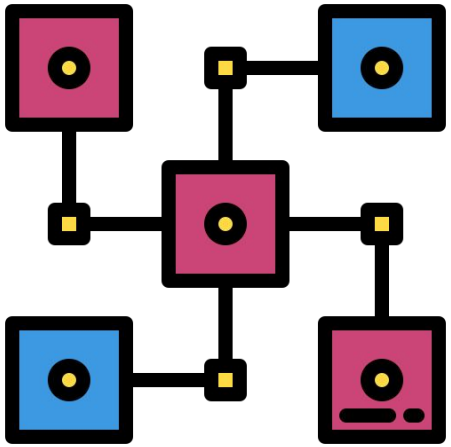
FP: Falsos Positivos
FN: Falsos Negativos

GT-Periscope Fase 2

Principais diferenciais

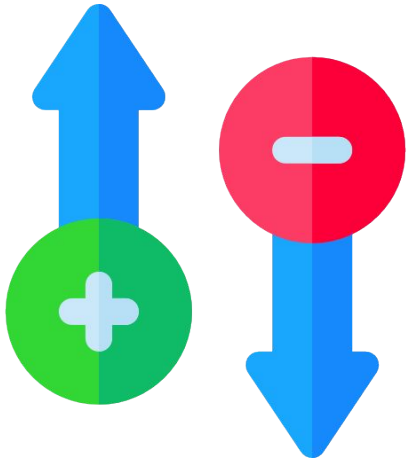


Plataforma multi-organização



Sistema Distribuído

Solução Nacional



Resultados melhores ou equivalentes

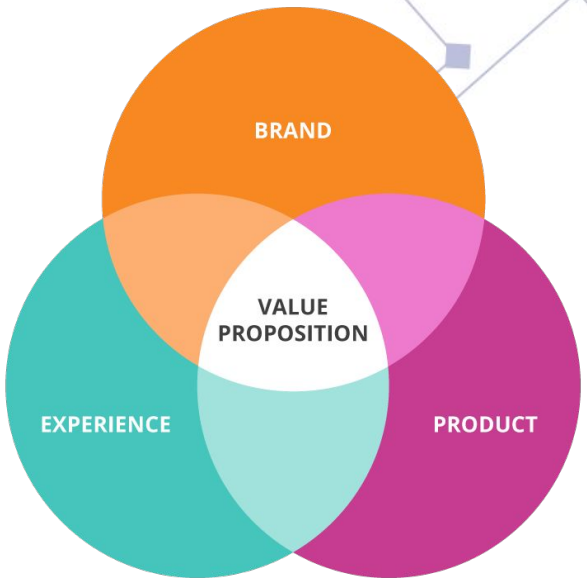
RNP 30 anos
ORGANIZAÇÃO SOCIAL DO MCTIC

Evoluções do Modelo de Negócios

GT-Periscope

Sherlock-X
Cyber Security Platform.

Visão de Negócio
Proposta de valor



Antecipar e **prevenir** ataques

Automatizar a descoberta de vulnerabilidades e botnets

Proporcionar a gestão de vulnerabilidades e resposta a incidentes

Evitar perdas financeiras e de reputação

Contribuir para adequação à legislação de proteção de dados pessoais

O Mercado de Segurança Cibernética no Brasil

Micromarket Monitor

SEGURANÇA DE REDES

SERVIÇOS DE SEGURANÇA

GERENCIAMENTO DE IDENTIDADE, AUTENTICAÇÃO E ACESSO (IAAM)

PROTEÇÃO DE INFRAESTRUTURA

O Mercado de Segurança Cibernética no Brasil

Micromarket Monitor

SEGURANÇA DE REDES

SERVIÇOS DE SEGURANÇA

GERENCIAMENTO DE IDENTIDADE, AUTENTICAÇÃO E ACESSO (IAAM)

PROTEÇÃO DE INFRAESTRUTURA

O Mercado de Segurança Cibernética no Brasil

Micromarket Monitor

US$ 7.29 Bilhões

Mercado total de segurança da informação (TAM)

US$ 1.93 Bilhões

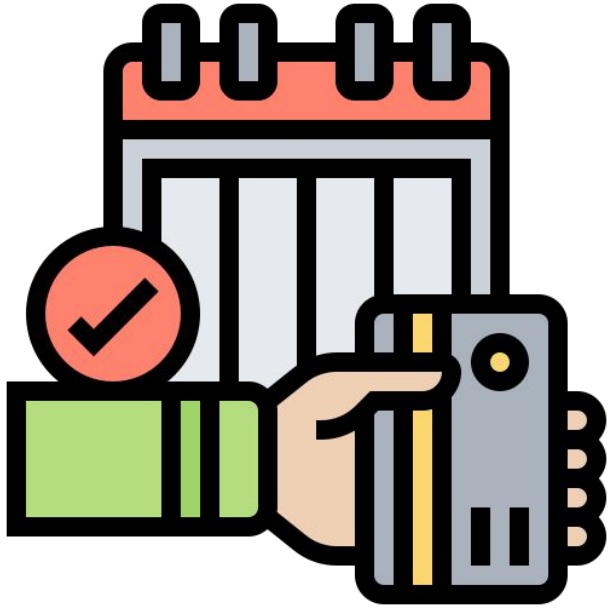
Mercado endereçável (SAM)

US$ 583.2 Milhões

Mercado acessível (SOM)

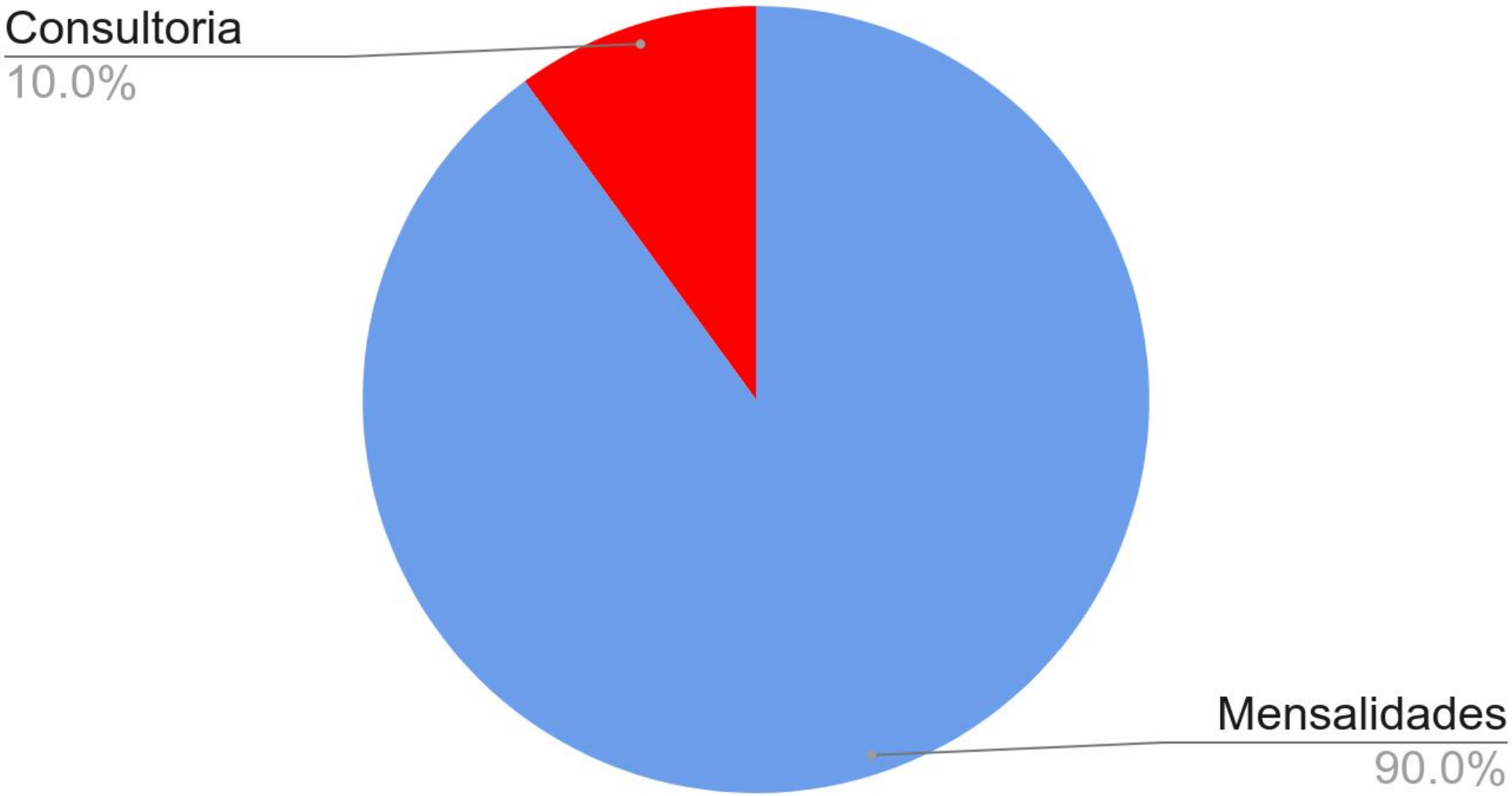
Modelo de Negócio
Monetização

Entrega como um serviço em nuvem SaaS



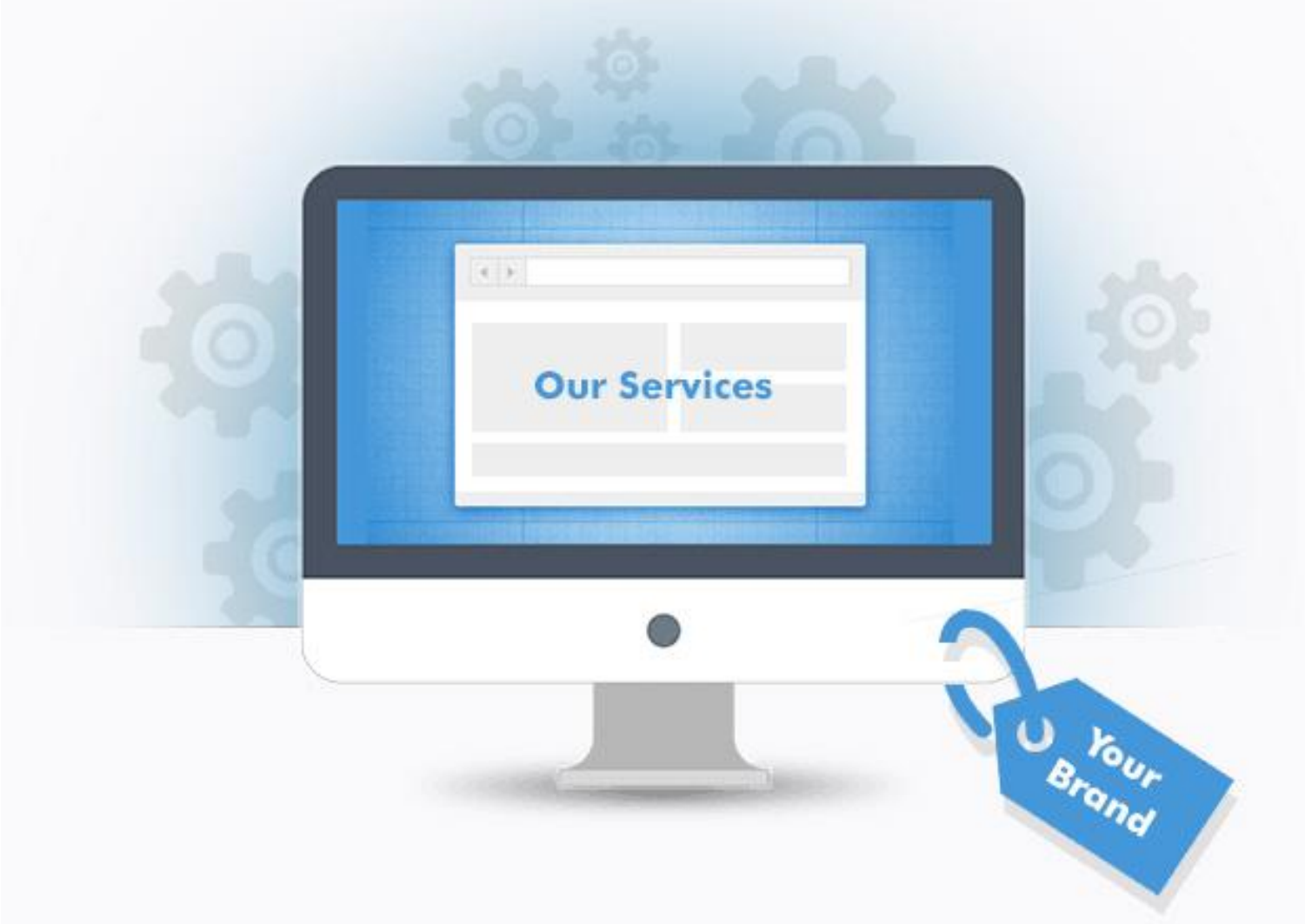
Monetização através de mensalidades

Visão de Negócio
Modelo de receitas



Visão de Negócio

Novo modelo de negócios em testes - White Label



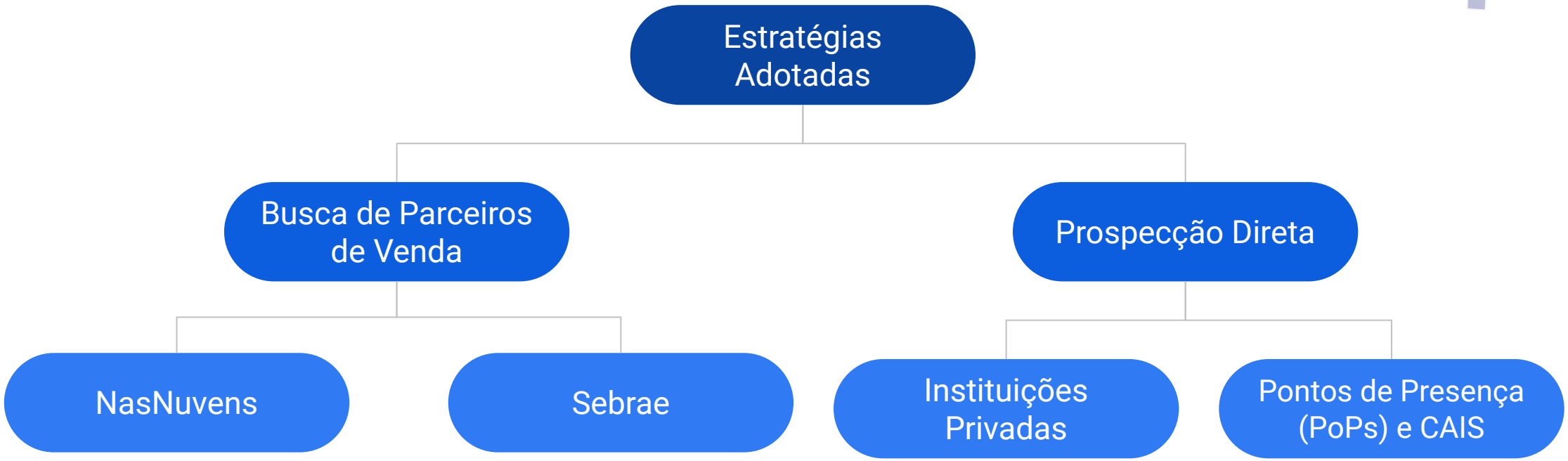
RNP 30 anos
ORGANIZAÇÃO SOCIAL DO MCTIC

Uso da solução e experimentos realizados ao longo da Fase 2

GT-Periscope

Sherlock-X
Cyber Security Platform.

Prospecção
Mercado



Estratégia adotada para o mercado:
Busca de parceiros de venda

SEBRAE

ApexBrasil

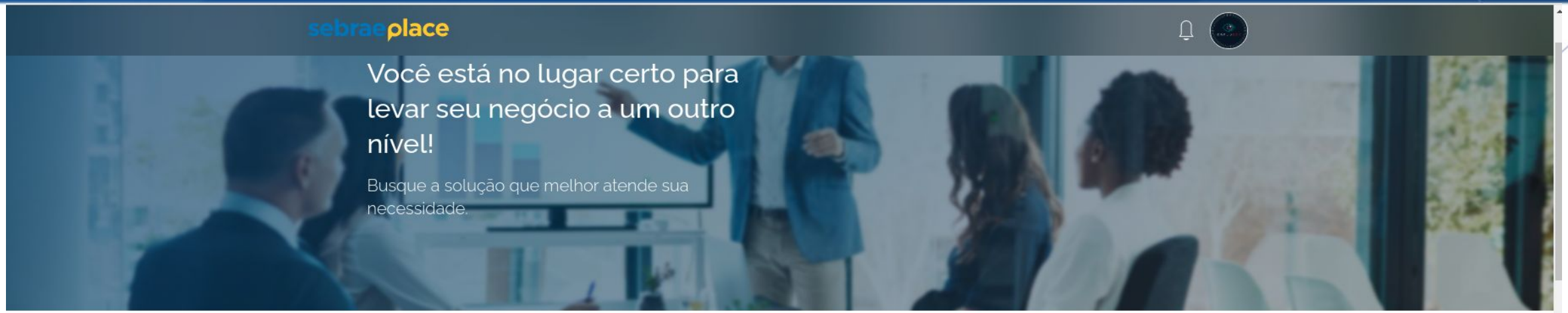
BIOPARK

nas nuvens

DISTRITO

rtm

Prospecção
Mercado



Busque a melhor solução para seu negócio

Ex: consultoria em marketing

Organizar anúncios

- Mais relevantes
- Menor preço
- Maior preço
- Melhor avaliado

- Todas as datas
- Esta semana
- Próxima semana
- Este mês

Início | Término

Preço

Modalidades

Quero Soluções Digitais

Solução Digital

Plataforma SoluQ RH

ATRAÇÃO, QUALIFICAÇÃO e CONTRATAÇÃO de talentos e...

Avaliações 5.0

Planos a partir de [redacted] | Escolher um plano

Solução Digital

Sherlock-X Plataforma de Segurança Cibernética para...

A plataforma que traz Segurança da Informação para...

Avaliações 5.0

Planos a partir de R[redacted] | Escolher um plano

Estratégia adotada:
Prospecção direta

Estratégia adotada no sistema RNP:
Conversa com gestores e atores das pontas do sistema RNP

PoP-PR

PoP-CE
Ponto de Presença da RNP no Ceará

CAIS

nas nuvens

Usuários implantados e em implantação no sistema RNP

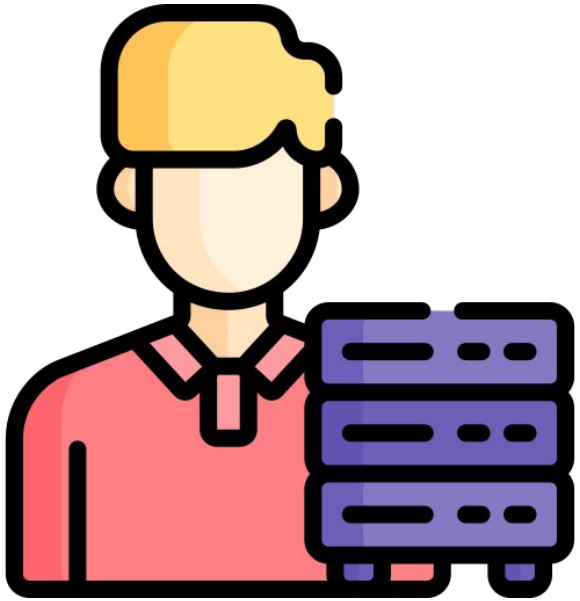
PoP-PR

PoP-CE
Ponto de Presença da RNP no Ceará

Experimentos Sistema RNP

Persona

Gestores de TI do sistema RNP (3x)

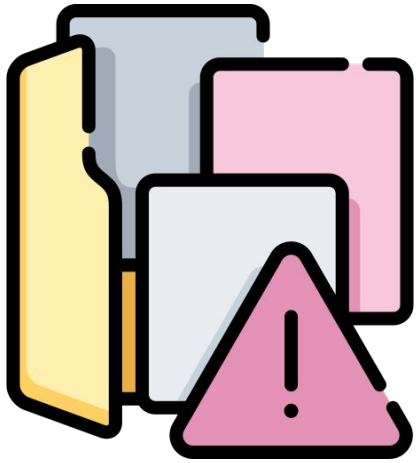


Responsável pela infraestrutura no sistema RNP (3x)

Experimentos Sistema RNP

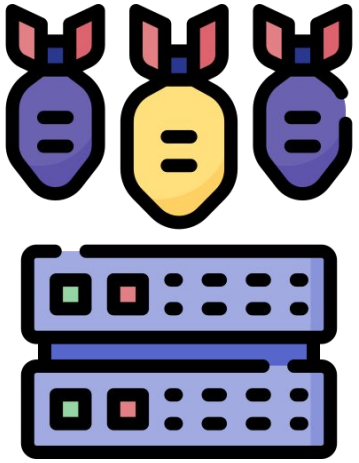
Dor

Adequação a LGPD



Insegurança (2x)

Ataque cibernético (2x)

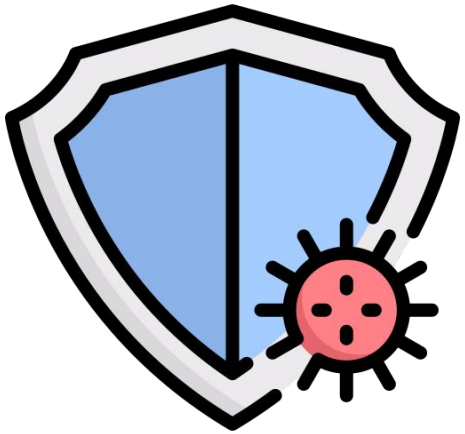


Desconhecimento sobre segurança infraestrutura

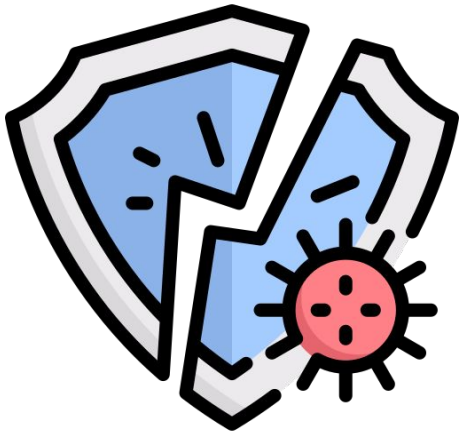
Experimentos Sistema RNP

Momento

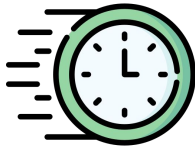
Entrada em vigor da LGPD



Prevenção contra ataques (4x)



Ações pós ataque



Experimentos Sistema RNP

Ação

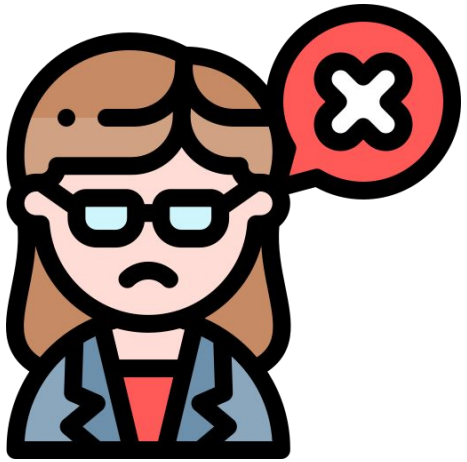
Workshop (2x)

Linkedin (2x)

Risco

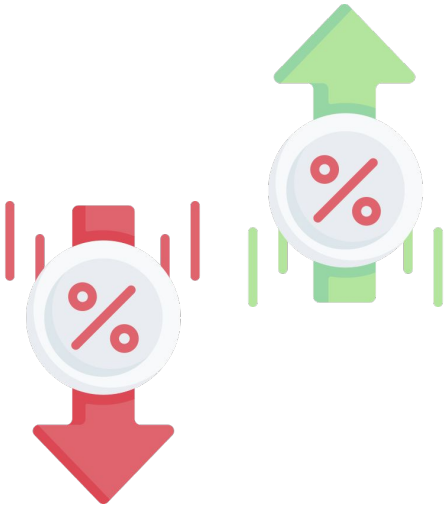
Avaliação das redes

Experimentos Sistema RNP
Resultados



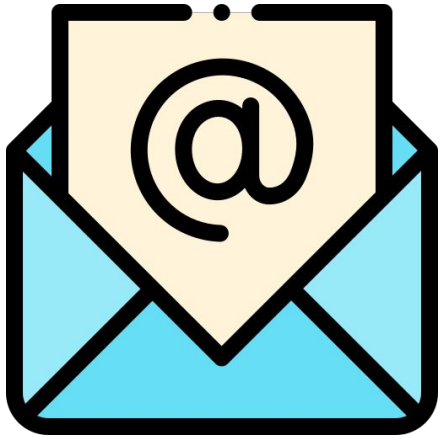
Persona principal não foi atingida

A persona não utiliza o Linkedin



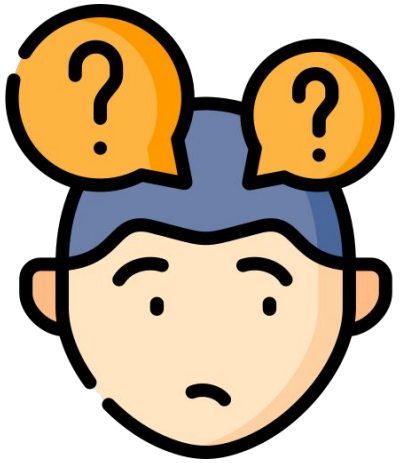
Personas mostraram interesse em usar a ferramenta

Experimentos Sistema RNP
Aprendizados



Lista de email e assunto devem ser melhor qualificados

Linkedin não é o canal ideal



Leads confusos com a proposta do sistema

Revisitar a definição da persona

PoP-PR

Palestra técnica

Persona: Responsável por infraestrutura

RNP 30 anos
ORGANIZAÇÃO SOCIAL DO MCTIC

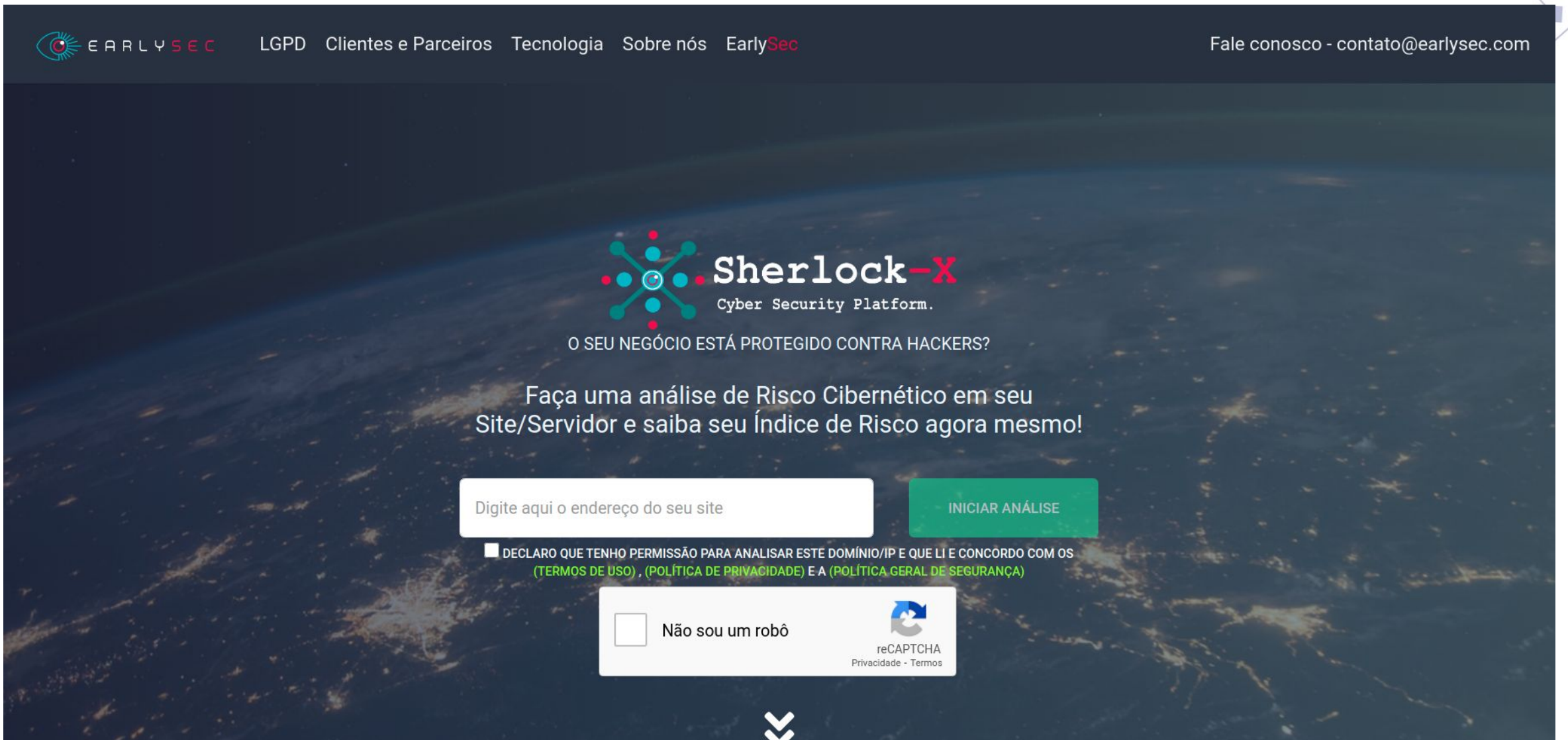
Oferta no NasNuvens

GT-Periscope

Sherlock-X
Cyber Security Platform.

GT-Periscope

NasNuvens - Oferta gratuita



Oferta Sistema RNP
NasNuvens

STARTUP

- Detecção e Gestão de Vulnerabilidades externa (IPs públicos)
- Detecção de má configuração de portas e serviços
- Gestão de incidentes
- Índice de risco
- Limite de 20 ativos
- Limite de 1 usuário

Mensal

Por **R$ 500,00**/Mês

Assine agora

BASIC

- Detecção e Gestão de Vulnerabilidades externa (IPs públicos)
- Detecção de má configuração de portas e serviços
- Gestão de incidentes
- Índice de risco
- Limite de 50 ativos
- Limite de 2 usuários

Mensal

Por **R$ 900**/Mês

Assine agora

PRO

- Detecção e Gestão de Vulnerabilidades externa (IPs públicos)
- Detecção de má configuração de portas e serviços
- Gestão de incidentes
- Índice de risco
- Detecção e Gestão de Vulnerabilidades rede Interna
- Limite de 100 ativos
- Limite de 4 usuários

Mensal

Por **R$ 1.655,00**/Mês

Assine agora

ENTERPRISE

- Detecção e Gestão de Vulnerabilidades externa (IPs públicos)
- Detecção de má configuração de portas e serviços
- Gestão de incidentes
- Índice de risco
- Detecção e Gestão de Vulnerabilidades rede Interna
- Detecção de Dispositivos infectados (bots)
- Implantação e Suporte técnico
- Limite de 200 ativos
- Limite de 6 usuários

Mensal

Por **R$ 2.600,00**/Mês

Assine agora

RNP 30 anos
ORGANIZAÇÃO SOCIAL DO MCTIC

Estrutura da Startup para tocar o negócio

GT-Periscope

Sherlock-X
Cyber Security Platform.

Estrutura da Startup
Infraestrutura

START UP brasil

STARTUP ACELERADA
INOVATIVA 2017.1
Melhor Aceleradora do Brasil

EARLYSEC

unimake SOFTWARE

GRUPO Integrado

baita

CNPq

MCTIC

amazon web services

RNP

CAIS

GT-Periscope

EARLYSEC

UFPR
UNIVERSIDADE FEDERAL DO PARANÁ

Sherlock-X
Cyber Security Platform.

Wagner Monteverde
Especialista em Segurança da Informação e Privacidade (Startup EarlySec)

wagner@earlysec.com

(44) 9 9953 9690

SCAN ME

www.sherlock-x.com.br

RNP ORGANIZAÇÃO SOCIAL DO MCTI

MINISTÉRIO DO TURISMO

MINISTÉRIO DA DEFESA

MINISTÉRIO DA SAÚDE

MINISTÉRIO DA EDUCAÇÃO

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÕES

PÁTRIA AMADA BRASIL GOVERNO FEDERAL