RNP
ORGANIZAÇÃO SOCIAL DO MCTI

GT-Periscope

Apresentação GT-PERISCOPE
Resultados parciais da Fase 2

Wagner Monteverde - Coordenador

Webinar do GTs para RNP – Ciclo 2020-2021

Sherlock-X
Cyber Security Platform.

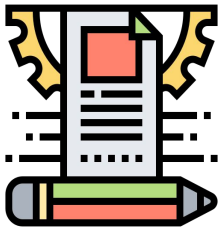
EARLYSEC

UFPR
UNIVERSIDADE FEDERAL DO PARANÁ

Sherlock-X

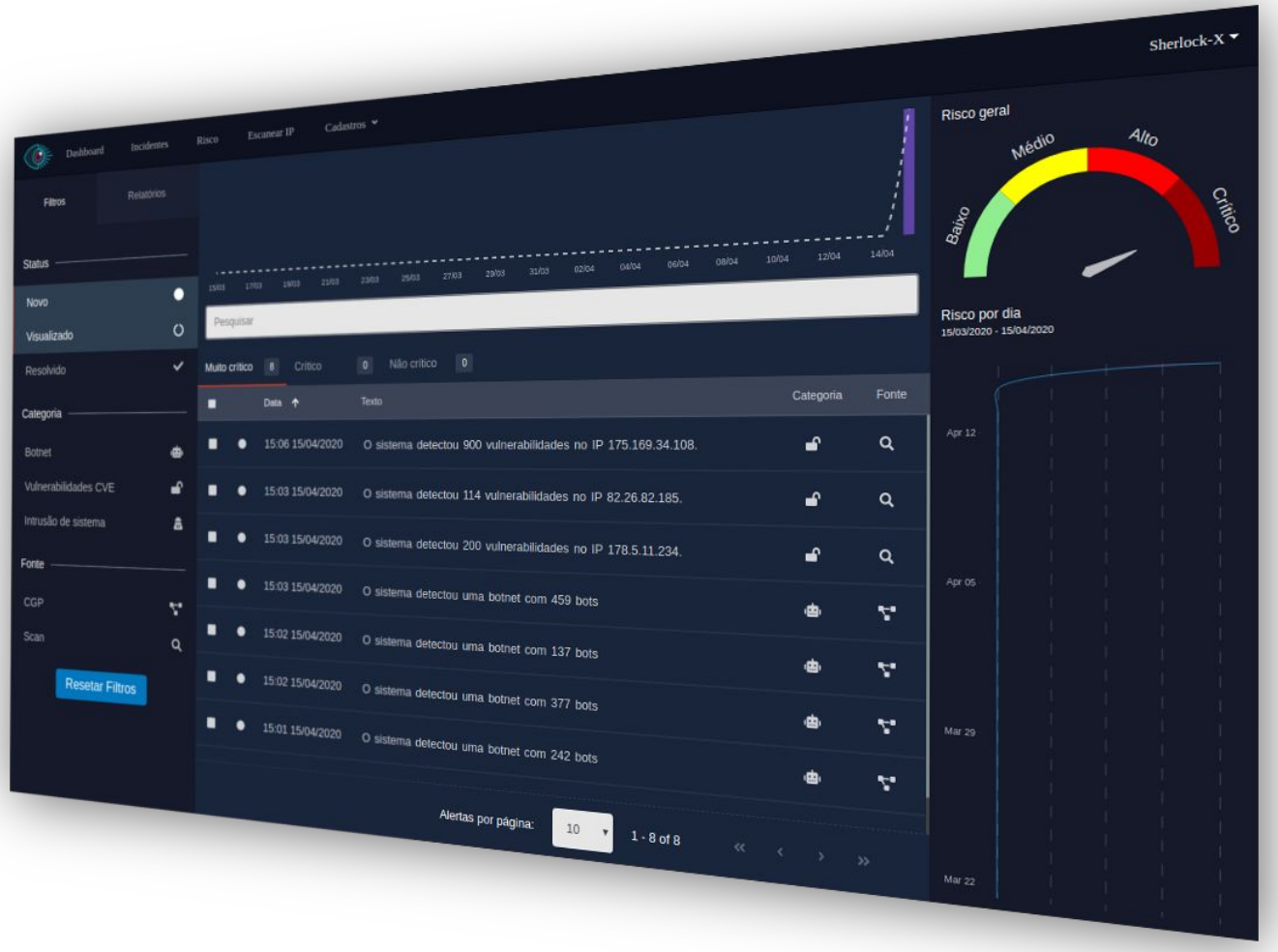
Detecção e Gestão de Vulnerabilidades

Detecção de Dispositivos infectados (bots)



Gestão integrada de incidentes

Índice de risco



Sherlock-X

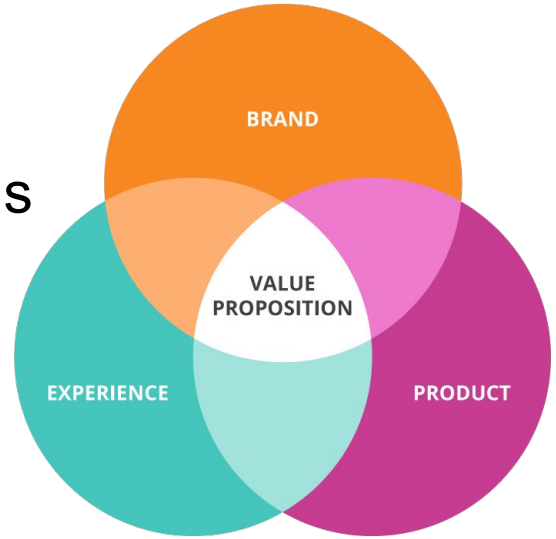
Antecipar e **prevenir** ciberataques

Automatizar a descoberta de vulnerabilidades e botnets

Proporcionar a gestão de vulnerabilidades e resposta a incidentes

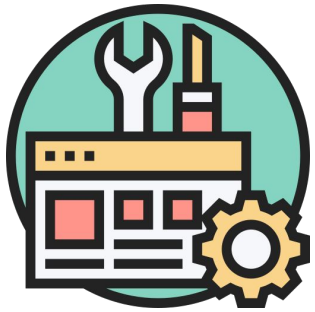
Evitar perdas financeiras e de reputação

Contribuir para adequação à Legislação de Proteção de Dados Pessoais



Fonte dos ícones: flaticon.com

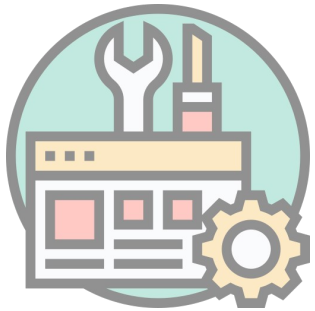
GT-Periscope Fase 2
Evolução MVP



Recomendações paras as vulnerabilidades

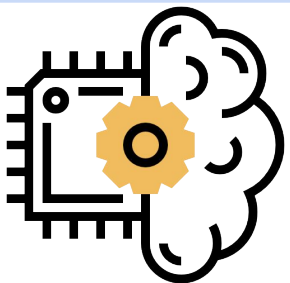
Fonte dos ícones: flaticon.com

GT-Periscope Fase 2
Evolução MVP



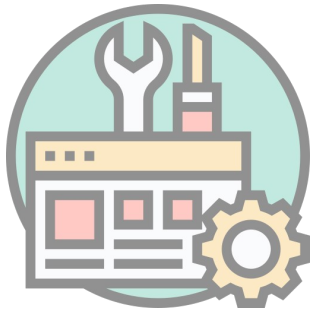
Recomendações paras as vulnerabilidades

Otimização motor de vulnerabilidades

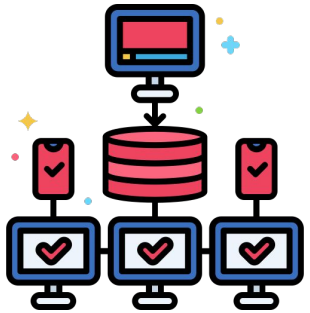


Fonte dos ícones: flaticon.com

GT-Periscope Fase 2
Evolução MVP

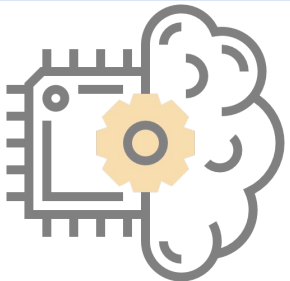


Recomendações paras as vulnerabilidades



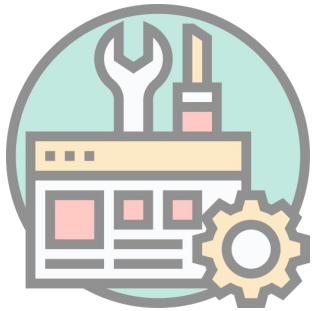
Otimização do sensor de análise de botnets

Otimização motor de vulnerabilidades

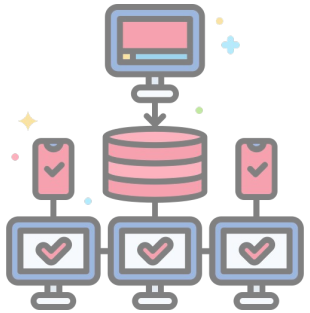


Fonte dos ícones: flaticon.com

GT-Periscope Fase 2
Evolução MVP

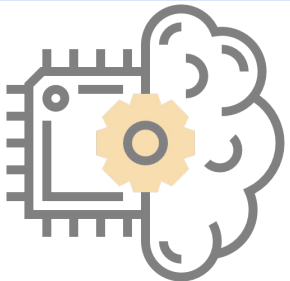


Recomendações paras as vulnerabilidades



Otimização do sensor de análise de botnets

Otimização motor de vulnerabilidades



Lançamento da landing page

Fonte dos ícones: flaticon.com

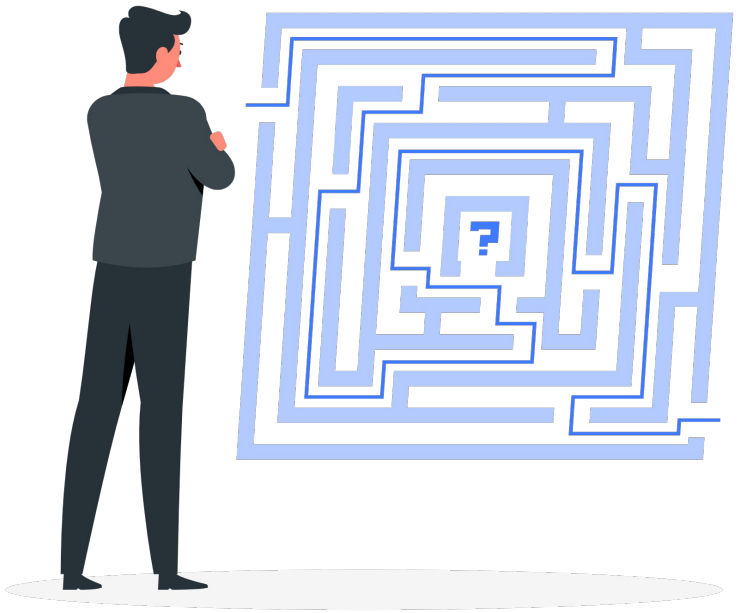
GT-Periscope Fase 2

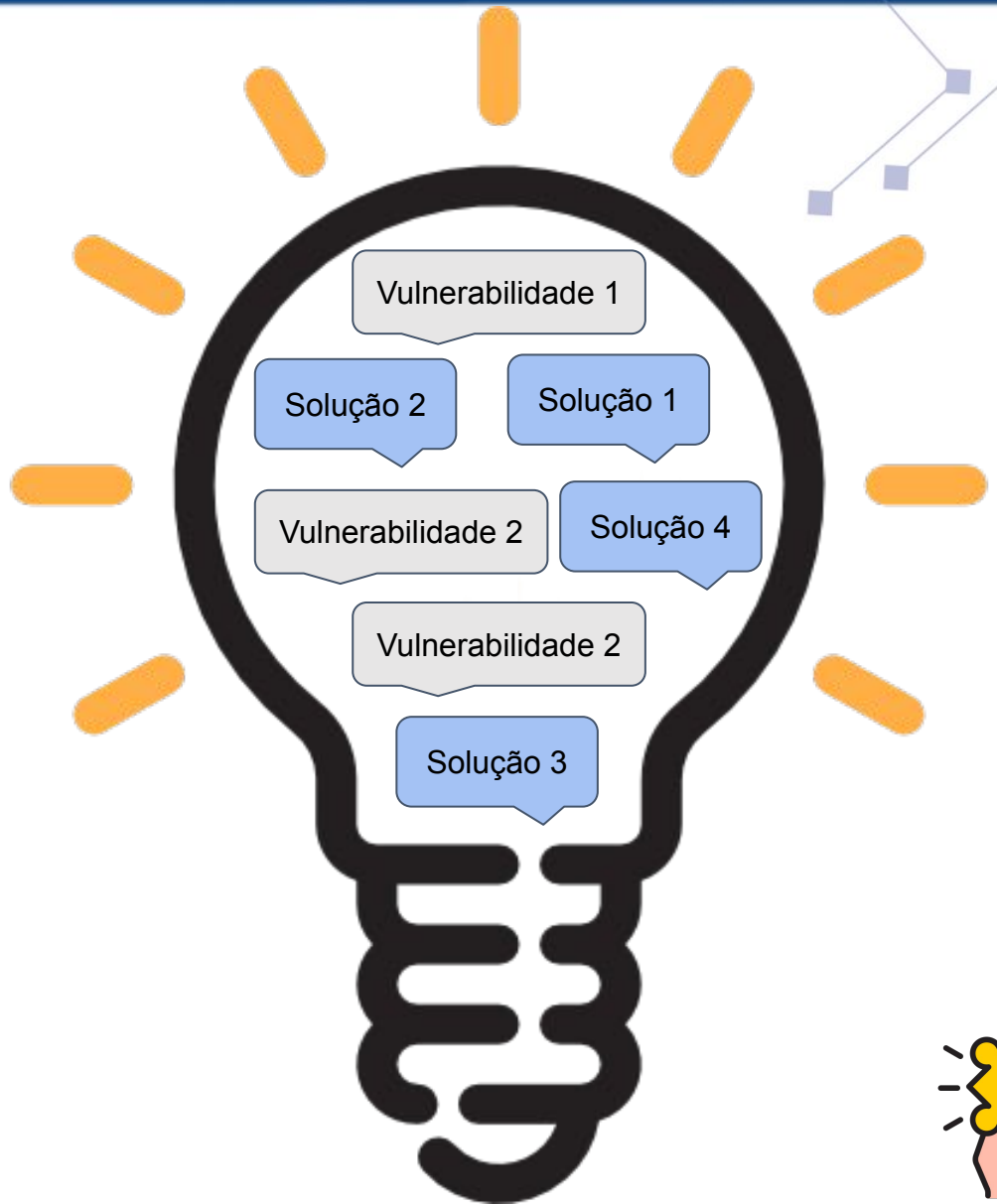
Soluções para as vulnerabilidades

Fonte dos ícones: storyset.com

GT-Periscope Fase 2

Recomendações para as vulnerabilidades





Fonte dos ícones: storyset.com, flaticon.com

GT-Periscope Fase 2

Otimização motor de vulnerabilidades

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

Otimização motor de vulnerabilidades

SHODAN

OpenVAS
Open Vulnerability Assessment System

Sherlock-X

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%	13%

GT-Periscope Fase 2

Otimização do sensor de análise de botnets

Cenário	Janelas (10 segundos)	Bots	Dispositivos normais (máximo)	Média Acurácia	Falso Positivo (máximo)	Falso Negativo (máximo)	Média tempo de processamento (por janela)
CTU-13 Cenário 10	878	10	739	99,49%	6	10	0,819 s
CTU-13 Cenário 11	97	2	885	99,94%	5	2	0,785 s

Fonte dos datasets: https://www.stratosphereips.org/datasets-ctu13

GT-Periscope Fase 2
Lançamento da landing page

Relatório da Análise de Riscos Tecnológicos do Ativo [redacted].113

Resumo Executivo

Olá **Marlon** [redacted], este é o relatório da análise de risco para o ativo [redacted].113. Nesta análise de risco foram verificados os seguintes itens: Detecção de portas abertas, Detecção de má configuração de portas e serviços em execução no ativo, e detecção de Vulnerabilidades de Software Profunda executados no ativo nas portas e serviços detectados.

Analisando esses itens, foram verificados que o índice de risco do ativo é: 7.8 considerado Crítico

Foram detectados 2 portas abertas, 24 vulnerabilidades e nenhum serviço com más práticas de configuração.

Mas o que isso quer dizer?

Quanto maior o nível de risco do ativo, maior é a chance de este sofrer um ataque cibernético, o risco calculado para o ativo é baseado na observação das melhores práticas de Segurança segundo a ISO/IEC 27001. Este procura verificar o real risco do ativo ser alvo de pessoas mal intencionadas (hackers), quanto maior o índice de risco menor é a expertise necessária para causar algum dano ou vazamento de informações dependendo do caso.

Este relatório de análise de riscos calcula o seu grau de risco e lhe dá detalhes sobre os problemas detectados, e ao final recomendações técnicas e recomendação geral para melhorar a segurança do ativo e baixar o índice de risco do mesmo.

Índice de Risco Geral do Ativo

7.8

Crítico

Este risco é calculado analisando todos os itens conforme o tipo da análise selecionada.

Informações Técnicas da Análise

Portas abertas e grau de risco por porta:

- **Porta:** 80 - **Produto:** Apache httpd
- **Porta:** 443 - **Produto:** Apache httpd

Níveis de Risco:

Os níveis de riscos tecnológicos são calculados utilizando a metodologia qualitativa, baseada nas vulnerabilidades encontradas e no seu índice de risco, e também, nas más configurações e quantidade de portas abertas no ativo.

GT-Periscope Fase 2
Sistema RNP

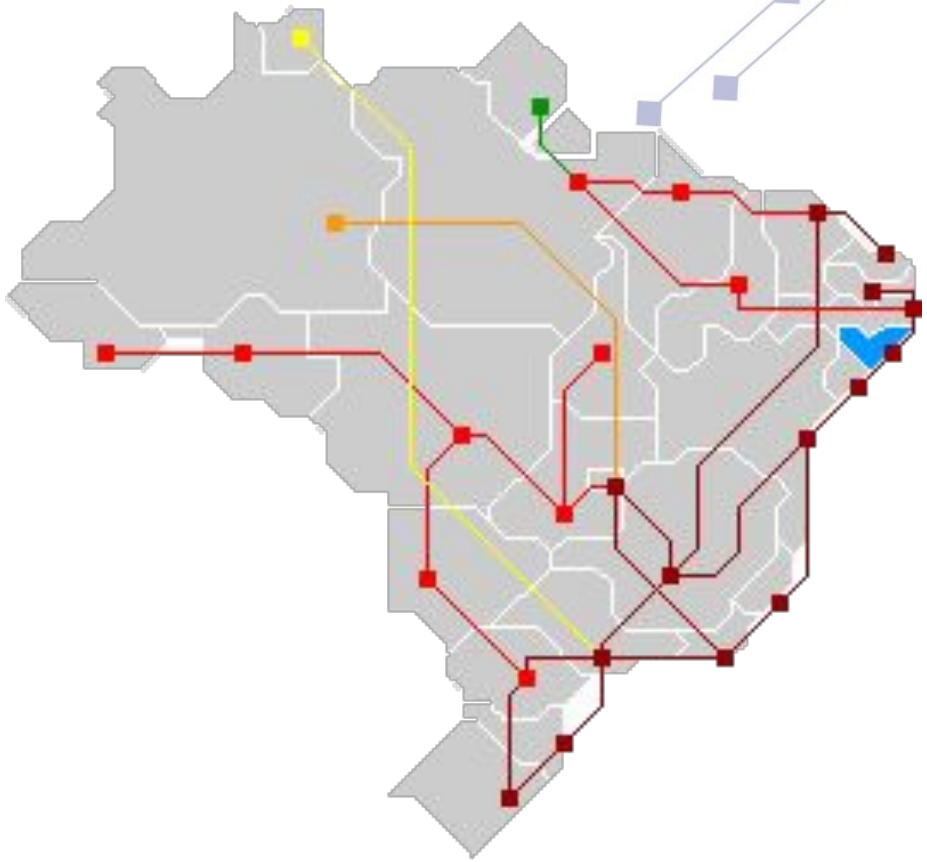
Instituições de educação e pesquisa

Empresas inovadoras

Ambientes promotores de inovação

Agências de fomento à pesquisa

Estabelecimentos de saúde com ensino e pesquisa



GT-Periscope Fase 2

Clientes externos à RNP (pequenas e médias empresas)

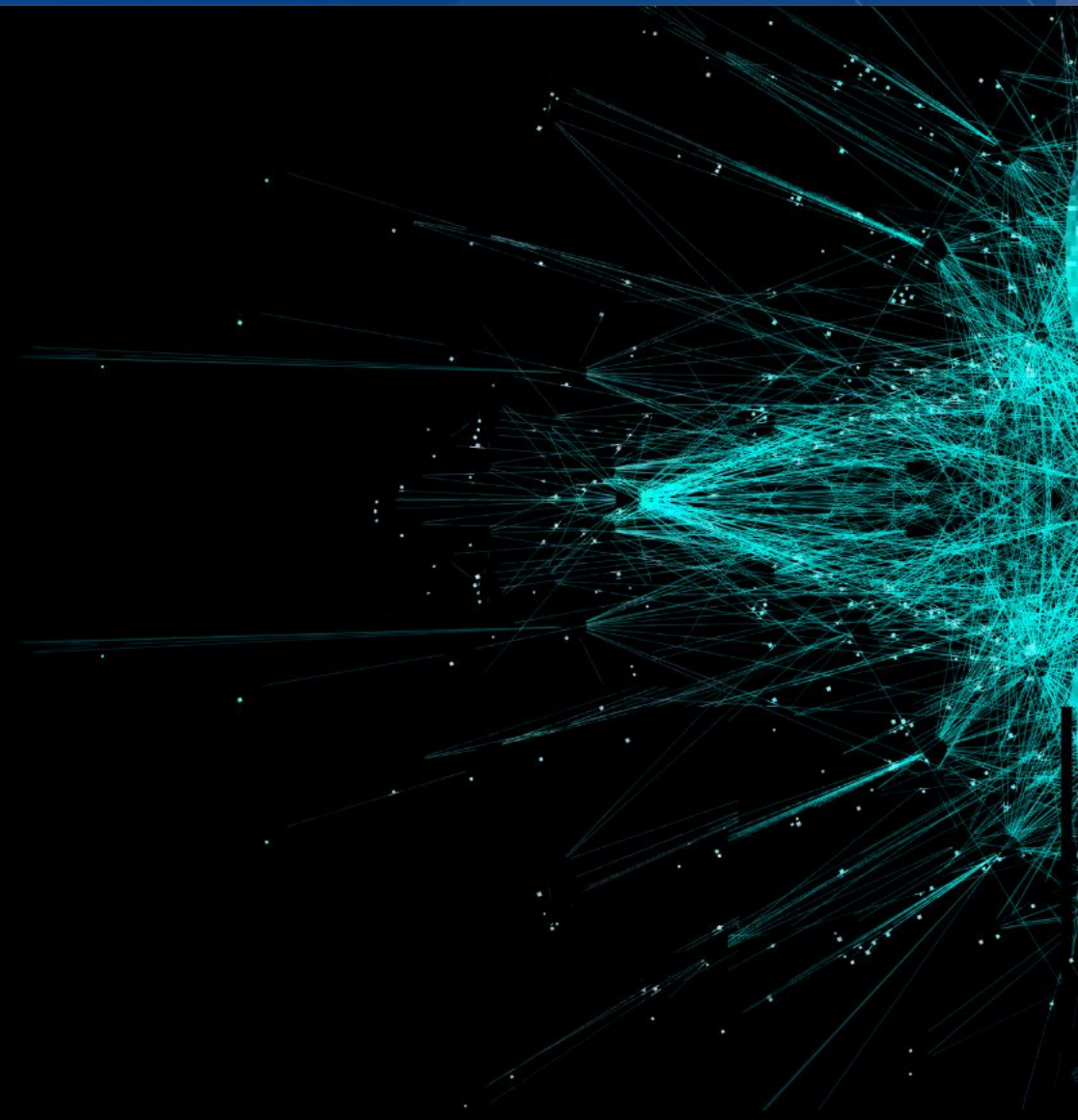
Fonte dos ícones: storyset.com


sebraeplace
Sherlock-X
Cyber Security Platform.
By
EARLYSEC
SEBRAE
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

EARLYSEC

Simplifying Cybersecurity

Pois Segurança da Informação deve ser acessível a todos!



Clientes e parceiros

STARTUP ACELERADA INOVATIVA 2017.1 Melhor Aceleradora do Brasil

START UP brasil

RNP
REDE NACIONAL DE ENSINO E PESQUISA

GRUPO Integrado

MCTIC

CNPq

Softex

VERIFACT

BFG ADVOGADOS | BARROSO, FERREIRA & GONÇALVES

ApexBrasil

SEBRAE

unimake SOFTWARE

baita

CAIS

UTFPR
UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

UFPR
UNIVERSIDADE FEDERAL DO PARANÁ

GT-Periscope Fase 2

Informações do Serviço no NasNuvens

Sherlock-X

Detecção e Gestão de Vulnerabilidades

Detecção de Dispositivos infectados (bots)

Índice de risco

Gestão integrada de incidentes

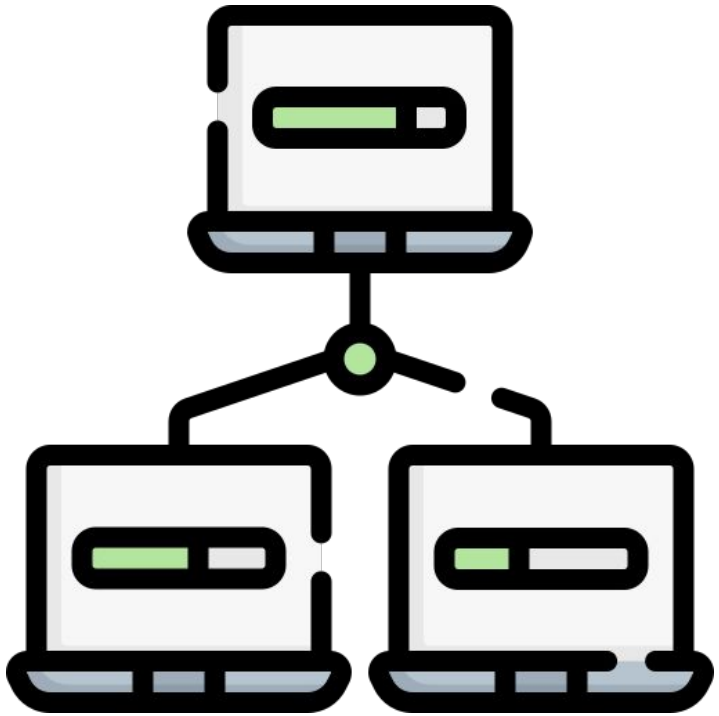
Recomendações de soluções

ISO 27001

PCI Security Standards Council

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

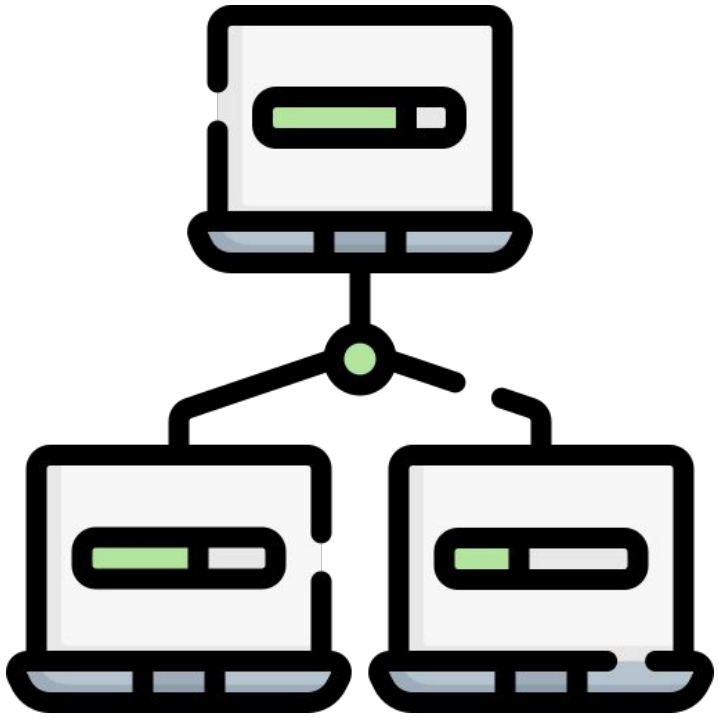
LGPD Lei Geral de Proteção de Dados Pessoais



Ativos de Rede Interna,
Computadores, Roteadores, etc ...

GT-Periscope Fase 2

Informações de Uso e Autenticação



Ativos de Rede Interna,
Computadores, Roteadores, etc ...

Ativos Externos, Sites, IPs Públicos,
servidores etc ...

Keycloak

Uma solução de gerenciamento de identidade e acesso.

GT-Periscope Fase 2

Informações de Uso e Autenticação

Keycloak

Uma solução de gerenciamento de identidade e acesso.

OAUTH 2.0

Padrão aberto para autorização.

GT-Periscope Fase 2

Informações de Uso e Autenticação

Keycloak

Uma solução de gerenciamento de identidade e acesso.

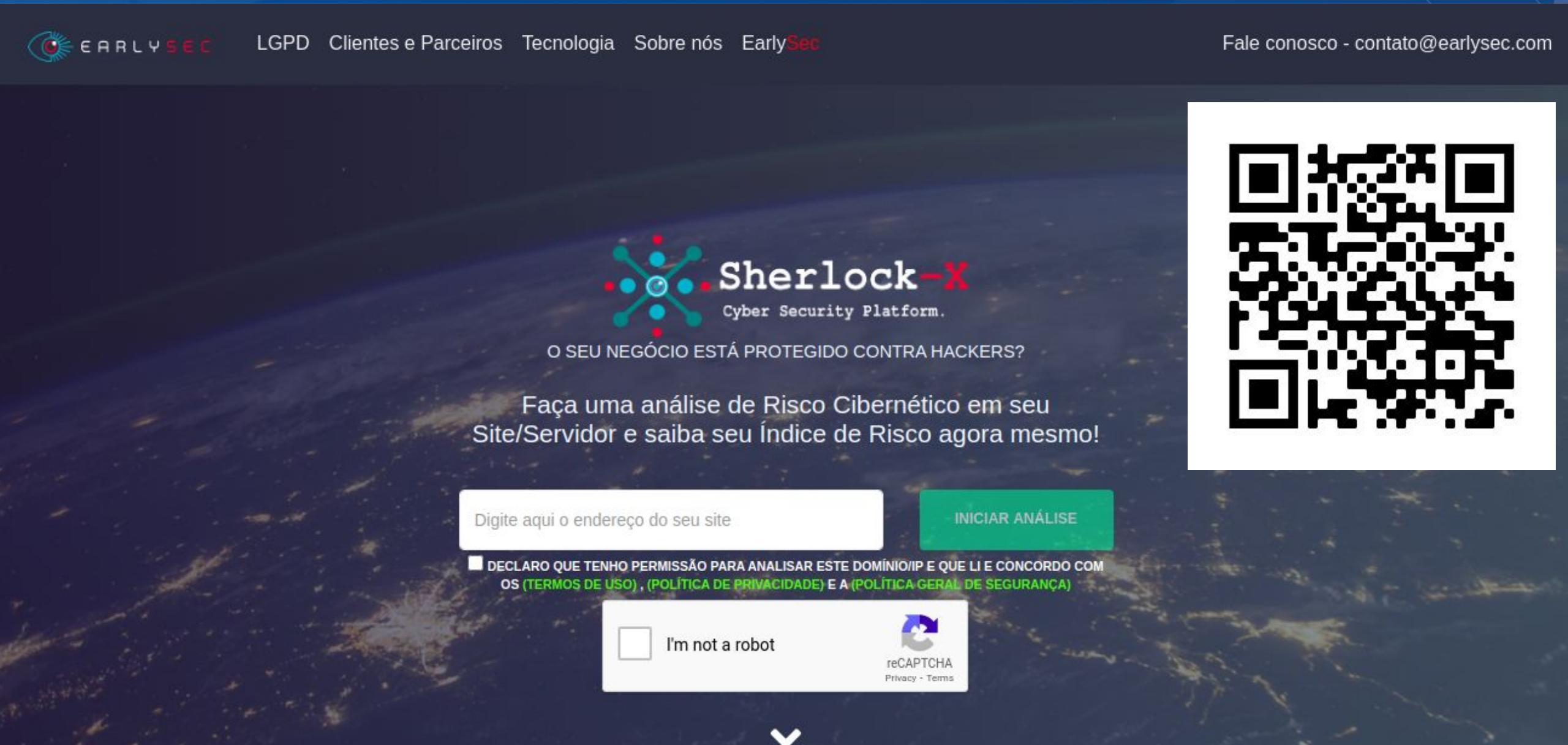
OAUTH 2.0

Padrão aberto para autorização.

Spring Security

Spring Security é um Framework Java / Java EE que fornece autenticação.

GT-Periscope Fase 2
Planos



RNP
ORGANIZAÇÃO SOCIAL DO MCTI

GT-Periscope Fase 2
Planos

Startup

Saiba Mais

- ✓ Detecção e Gestão de **Vulnerabilidades externa** (IPs públicos)
- ✓ Gestão de **incidentes**
- ✓ Índice de **risco**
- ✓ Limite de **20 ativos**
- ⊗ Detecção e Gestão de Vulnerabilidades rede Interna
- ⊗ Detecção de Dispositivos infectados (bots)
- ⊗ Implantação e Suporte técnico

Saiba Mais!

R$ 500,00 + taxas

Basic

Saiba Mais

- ✓ Detecção e Gestão de **Vulnerabilidades externa** (IPs públicos)
- ✓ Gestão de **incidentes**
- ✓ Índice de **risco**
- ✓ Limite de **50 ativos**
- ⊗ Detecção e Gestão de Vulnerabilidades rede Interna
- ⊗ Detecção de Dispositivos infectados (bots)
- ⊗ Implantação e Suporte técnico

Saiba Mais!

R$ 900,00 + taxas

Pro

Saiba Mais

- ✓ Detecção e Gestão de **Vulnerabilidades externa** (IPs públicos)
- ✓ Gestão de **incidentes**
- ✓ Índice de **risco**
- ✓ Limite de **100 ativos**
- ⊗ Detecção e Gestão de Vulnerabilidades rede Interna
- ⊗ Detecção de Dispositivos infectados (bots)
- ⊗ Implantação e Suporte técnico

Saiba Mais!

R$ 1.655,00 + taxas

GT-Periscope Fase 2

Planos

Enterprise

Saiba Mais

- Detecção e Gestão de **Vulnerabilidades externa** (IPs públicos)
- Gestão de **incidentes**
- Índice de **risco**
- Limite de **200 ativos**
- Detecção e Gestão de **Vulnerabilidades rede interna**
- Detecção de **Dispositivos infectados** (bots)
- Implantação e Suporte técnico

Saiba Mais!

R$ 2.600,00 + taxas

GT-Periscope Fase 2
Experimentos Tração On Line

Persona	Gestores de TI do sistema RNP
Dor	Adequação à LGPD das organizações relacionadas ao aspecto de controles de Segurança Cibernética.
Momento	Relacionado a entrada em vigor da LGPD.
North Star	Verificar o nível de preocupação em se adequar a nova Lei - objetivo : Marcar reuniões com possíveis clientes.
Ideia Nomeada	Workshop clientes RNP.
Descrição do Experimento (incluindo responsável e prazo)	Responsável pelo experimento: Wagner Monteverde. Prazo de execução: 1 mês e meio;
Critério de sucesso	Agendamento de pelo menos 2 reuniões com contatos adquiridos no workshop.
Métricas Chave	Número de inscritos, número de confirmações no Workshop através do participantes do workshop, número de reuniões marcadas através do workshop.

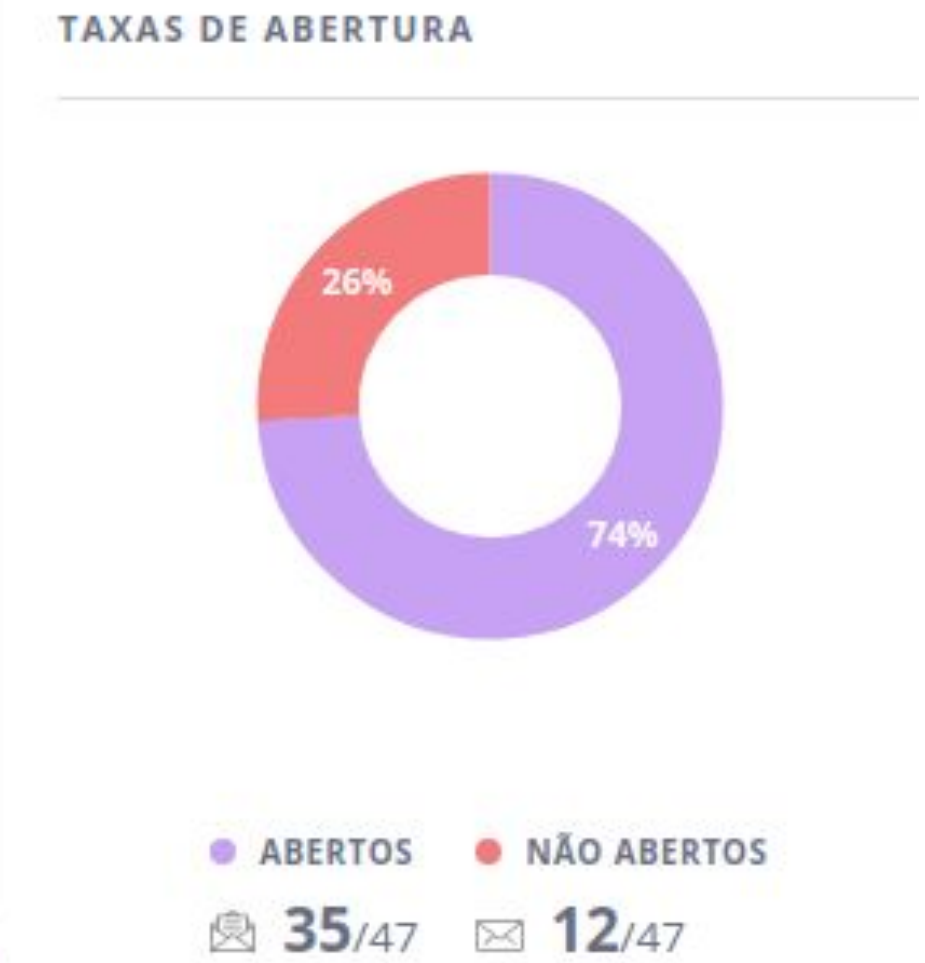
Experimento 01 - Resultados:
Envio para lista da RNP de gestores de TI

Número de inscritos	**55**
Número de confirmações	**20**
Número de Participantes	**11**
Número de reuniões marcadas	**3**

Experimento 01 - Resultados:
Envio para lista da RNP de gestores de TI

Número de inscritos	55
Número de confirmações	20
Número de Participantes	11
Número de reuniões marcadas	3

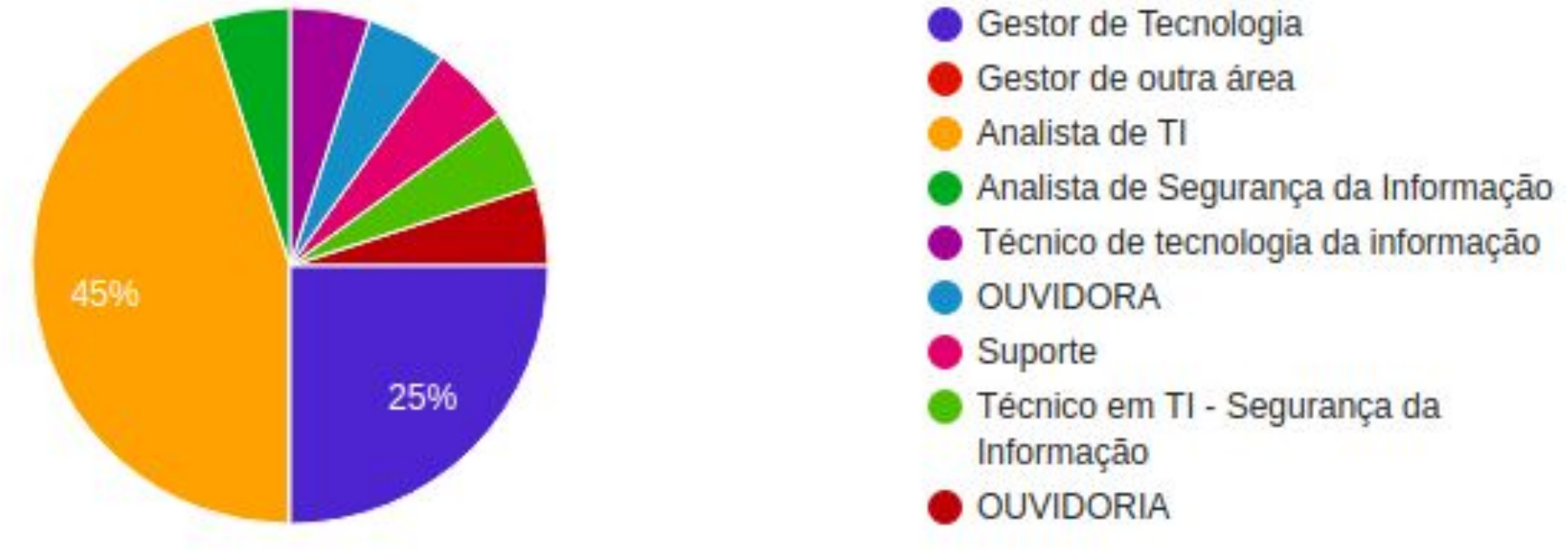
Critério de sucesso atingido!



Experimento 01 - Resultados:
Envio para lista da RNP de gestores de TI

Cargo que ocupa na instituição (Escolha a opção que melhor se enquadra no seu perfil).

20 responses



GT-Periscope Fase 2

Experimentos Tração On Line

Persona	Gestores de TI do sistema RNP
Dor	Insegurança e medo de sofrer ataques cibernéticos.
Momento	Vigoração da LGPD, antes do mesmo sofrer um ataque, ou roubo de dados.
North Star	Verificar o nível de preocupação dos gestores nas questões preventivas de com possível [illegible] após a nova Lei, objetivo principal marcar reuniões
Ideia Nomeada	Mineração de leads do Sistema RNP através do linkedin, nutrição do lead e realização de contato.
Descrição do Experimento (incluindo responsável e prazo)	Através da rede social Linkedin será minerado [illegible] do sistema RNP para [illegible] após o engajamento [illegible] será realizado um contato para agendamento de reunião. Responsável pelo experimento: Wagner Monteverde. Prazo de execução: 2 semanas;
Critério de sucesso	Ao menos 5 reuniões
Métricas Chave	Número de leads encontrados, número de leads contactados, número de leads que reuniões marcadas, número de leads que engajaram com o conteúdo, [illegible]

Experimento 02 - Resultados:
Mineração de leads do Sistema RNP no Linkedin

Número de leads encontrados	**31**
Número de solicitações de contato	**31**
Número de aceitações	**5**
Número de respostas no chat	**0**
Número de reuniões marcadas	**0**

GT-Periscope Fase 2

Experimentos Tração On Line

Persona	Responsável por infraestrutura da organização no sistema RNP.
Dor	A preocupação em sofrer um ataque cibernético que vaze algum dado.
Momento	Antes de sofrer um ataque cibernético, visto a vigoração da LGPD.
North Star	Avaliar o engajamento dos responsáveis por infraestruturas em buscar soluções [illegible] risco e abrir porta para produto de maior ticket [illegible] para a necessidade de detecção de
Ideia Nomeada	Experimento para detecção de interesse por situação do risco cibernético da organização.
Descrição do Experimento (incluindo responsável e prazo)	Através da utilização de uma app que calcula o score de risco de um ativo (site), [illegible] baixo), por sua vez poderá [illegible] uma análise grátis, mas também uma paga (valor Responsável pelo experimento: Wagner Monteverde. Prazo de execução: 2 semanas;
Critério de sucesso	5 Análises de risco
Métricas Chave	Número de análises grátis, número de análises pagas, número de desistências, número de pessoas interessadas em efetuar análise completa de sua infraestrutura.

Experimento 03 - Resultados:
Análise gratuita de vulnerabilidades App.

Número de análises free realizadas	**1**
Número de análises completas	**1**

URL	POSIÇÃO	PRIMEIRO CLIQUE
http://www.earlysec.com/	1	1
https://cyber-risk-analyzer.earlysec.com/	6	2
https://api.whatsapp.com/send?phone=5544988028242&text=Ol%C3%A1,%...	7	1

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