RNP 30 anos
ORGANIZAÇÃO SOCIAL DO MCTIC

GT-ARQUIMEDES: Uma Ferramenta para se Esquivar de Vazamentos de Informação na Transmissão de Mensagens de Rede

Michele Nogueira - Coordenadora Acadêmica
Wagner Monteverde - Assistente de Inovação

03 de Fevereiro de 2021

UFPR
UNIVERSIDADE FEDERAL DO PARANÁ

EARLYSEC

RNP 30 anos
ORGANIZAÇÃO SOCIAL DO MCTIC

Você sabe mensurar a vulnerabilidade de segurança gerada pelos dispositivos IoT na sua rede?

Introdução

Tudo Conectado!

Hospitais

Introdução

Tudo Conectado!

Agroindústria

Hospitais

Introdução

Tudo Conectado!

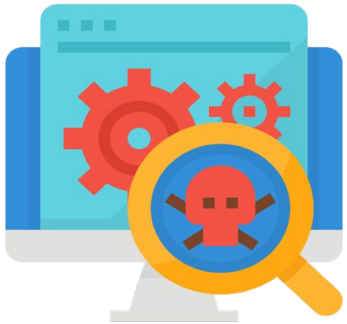
Agroindústria

Automotivo

Hospitais

Introdução

Aumento dos Ataques na IoT



8 em cada 10 organizações dos EUA sofreram ataques IoT

WELIVE SECURITY, 2019

82% de hospitais já sofreram ataques provenientes da IoT

FIERCE HEALTHCARE, 2019

32,7% de dispositivos IoT infectados

NOKIA, 2019-2020

Introdução

Objetivo Inicial

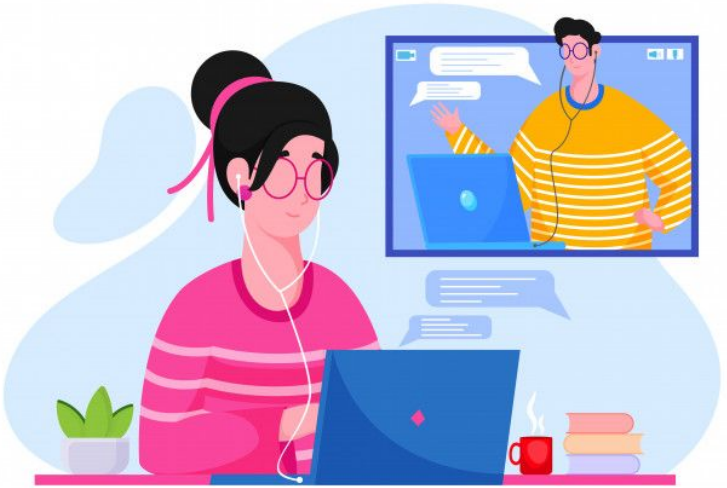
Privacidade às informações e prevenção da descoberta de **dados** e **comportamentos de dispositivos** pela análise de tráfego de rede

Introdução

Entrevistas

Começaram as Entrevistas ...

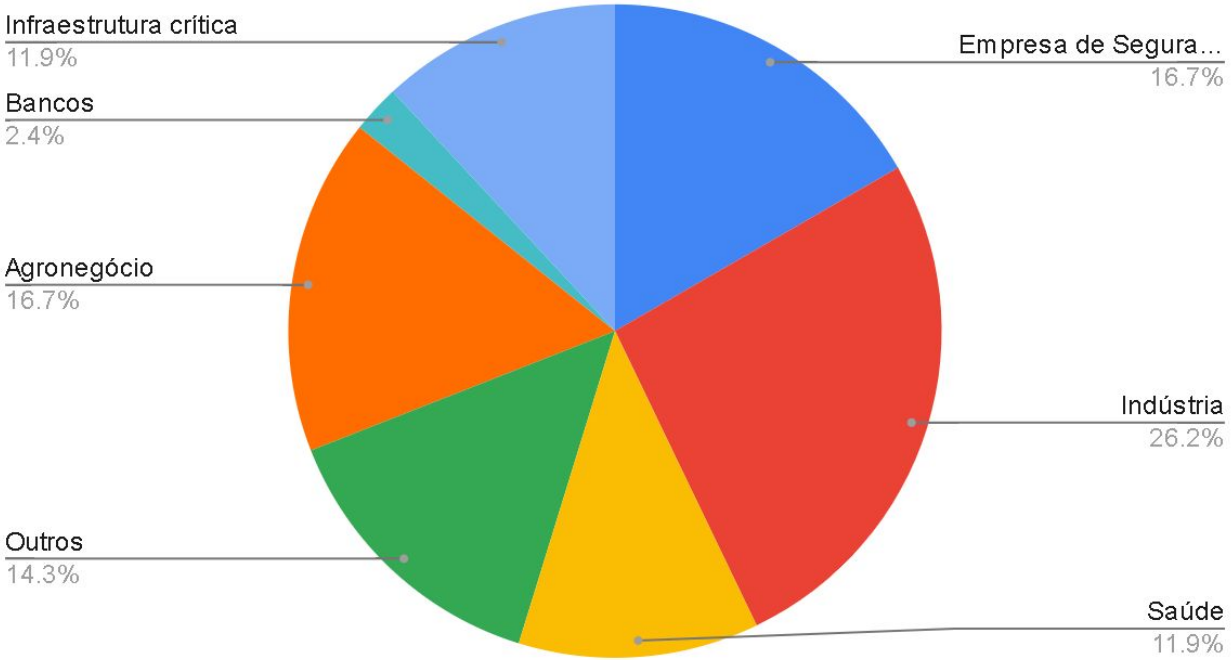
- ➔ Empresas de Segurança
- ➔ Segurança Nacional
- ➔ Agroindústria
- ➔ Hospitais



Introdução

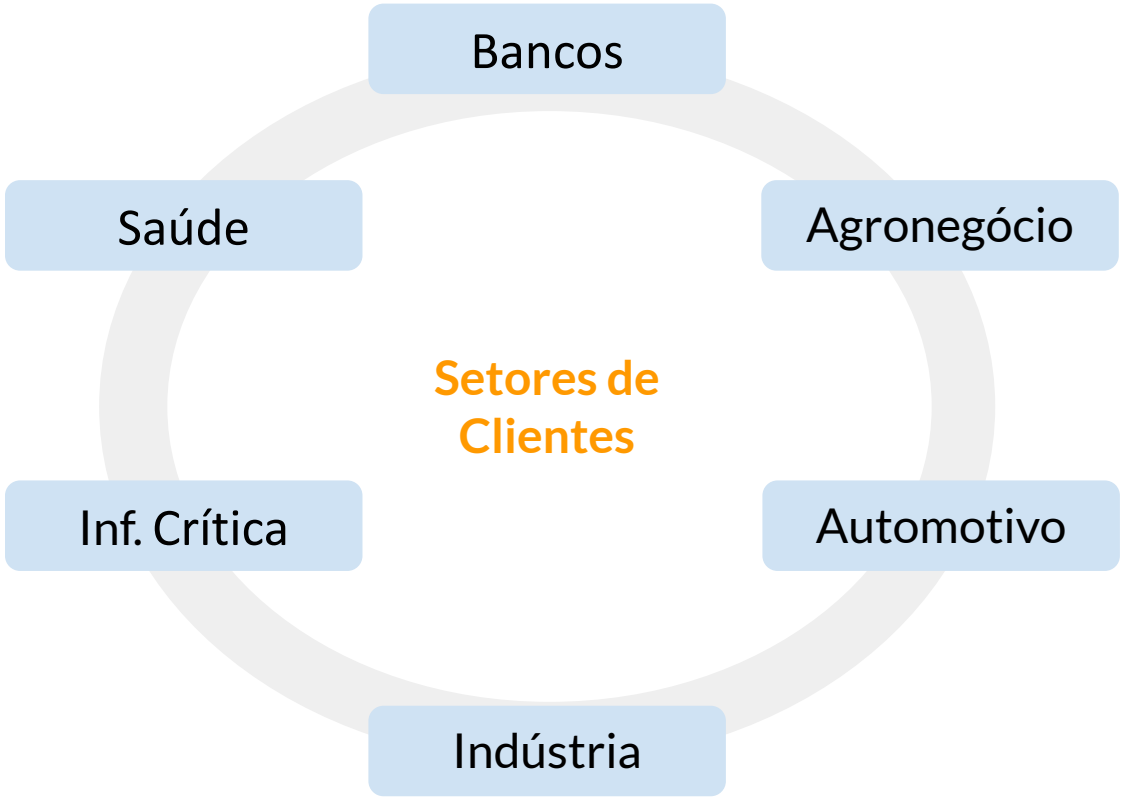
Entrevistas

53 Entrevistas



Introdução

Entrevistas



Introdução

Entrevistas - Aprendizado

Bancos

- Conservadores
- Segurança rigorosa
- Pouca digitalização IoT

Itaú

Banco do Nordeste

Introdução

Entrevistas - Aprendizado

Agronegócio

- Avançado na transformação digital
- Fazendas conectadas
- Segurança não é tão importante!

JOHN DEERE

Embrapa

São Martinho

Introdução

Entrevistas - Aprendizado

- Advento 5G
- Baixa Latência
- Número de dispositivos conectados

Automotivo

RENAULT

Introdução

Entrevistas - Aprendizado

- IoT para monitoramento
- Automação
- Indústria 4.0 crescendo
- Pouca segurança

Indústria

WEG
VAISALA

Introdução

Entrevistas - Aprendizado

- Conservadoras
- Modelo Itaipu c/ prédio inteligente
- Não possuem segurança para IoT

Inf. Crítica

Claro
ITAIPU BINACIONAL
CEMIG

Introdução

Entrevistas - Aprendizado

Saúde

- Adesão de tecnologias
- Segurança rigorosa
- Não possuem segurança para IoT/5G

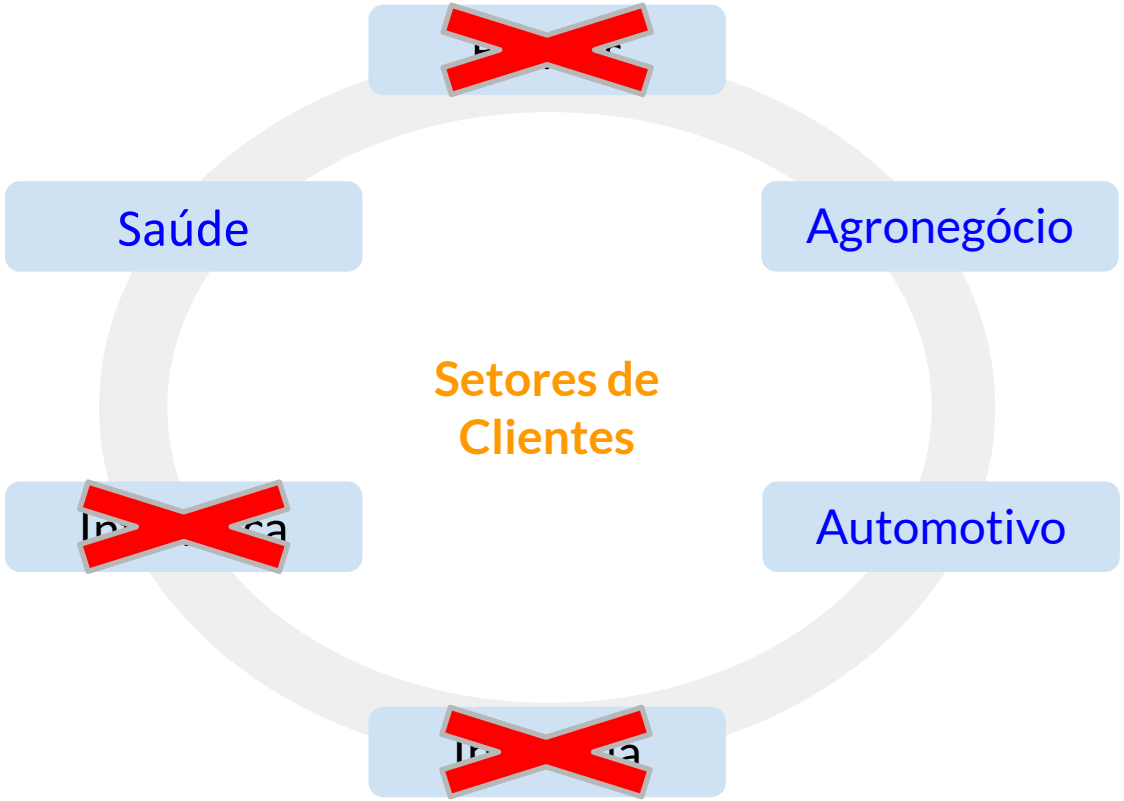
UHG

Unimed

HOSPITAL ISRAELITA ALBERT EINSTEIN

Introdução

Entrevistas - Aprendizado



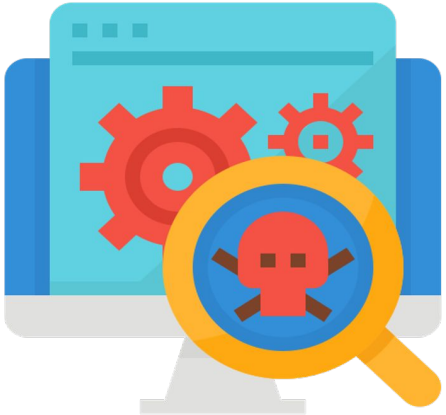
RNP 30 anos
ORGANIZAÇÃO SOCIAL DO MCTIC

O que fazer?
Novo objetivo?

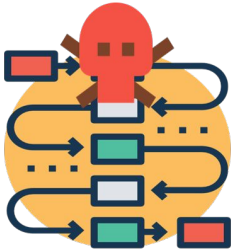
RNP 30 anos
ORGANIZAÇÃO SOCIAL DO MCTIC

Falhas de Segurança! (Vulnerabilidades)

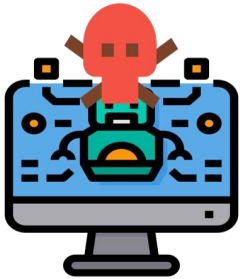
Vulnerabilidades de segurança nos dispositivos: porta de entrada para atacantes



Pessoas



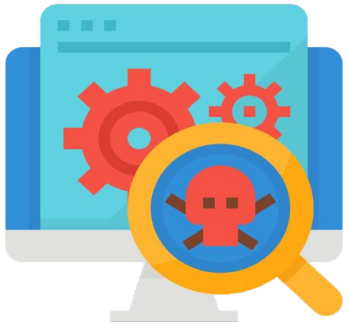
Processos



Organizações

Motivação

Problemas



Vulnerabilidades em dispositivos IoT

Acesso indevido, roubo de dados e informações

Monitoramento de atividades e ataques

RNP 30 anos
ORGANIZAÇÃO SOCIAL DO MCTIC

Solução

GT-Arquimedes

Uma Ferramenta para Detectar Vulnerabilidades nos Dispositivos IoT

Nossa Ferramenta

GT-Arquimedes

- ➔ Mapeamento da rede e identificação dos dispositivos IoT
- ➔ Localização das vulnerabilidades e quantificação de riscos
- ➔ Controle e remoção das vulnerabilidades
- ➔ Proteção contra ataques

Visão de Negócio

Proposta de valor

Proporcionar conhecimento sobre o comportamento e as vulnerabilidades de segurança, quantificar os riscos e prevenir perda financeira na infraestrutura digital formada por dispositivos IoT e 5G.

Visão de Negócio

Proposta de valor

Conhecimento das Vulnerabilidades

Visão de Negócio

Proposta de valor

Conhecimento das Vulnerabilidades

Quantificação de Riscos

Visão de Negócio

Proposta de valor

Conhecimento das Vulnerabilidades

Quantificação de Riscos

Prevenção de Perda Financeira

Canvas

Versão Final

Key Partners Insert

- RNP
- NasNuvens
- Sebrae
- Sherlock-x
- UFPR

Key Activities Insert

- Monitoramento 24x7
- Ofuscar os dados na rede
- Mapeamento do comportamento de dispositivos na rede em relação a privacidade.
- Implantação

Key Resources Insert

- Código fonte/solução
- Servidores em nuvem
- Equipe especializada
- Acesso remoto a uma máquina virtual na infraestrutura digital
- Máquina virtual local para coleta do tráfego

Value Proposition Insert

Proporcionar o conhecimento do comportamento/vulnerabilidades, quantificação dos riscos e prevenção de perda financeira/econômica na infraestrutura digital

Quantificação do risco de comprometimento e negação da infraestrutura digital

Identificação de vulnerabilidades de segurança nos dispositivos IoT

Preservação dos serviços críticos e comunicação 5G/4G/3G da infraestrutura digital

Customer Relationships Insert

- Plataforma agradável e fácil de usar
- Service Desk

Channels Insert

- Palestras/eventos
- Telefone
- Redes sociais
- Telefone
- Redes sociais
- Email
- Palestras
- Site do produto
  Landing page
- Lista de email

Customer Segments Insert

Clientes com preocupação (imediata) com vulnerabilidades de segurança em aplicações da IoT

Saúde (sistema RNP)
Automotivo (foco para a StartUp)

Clientes com preocupação (não imediata) com vulnerabilidades de segurança em aplicações da IoT

Agronegócio (validar com o sistema RNP)

Cost Structure Insert

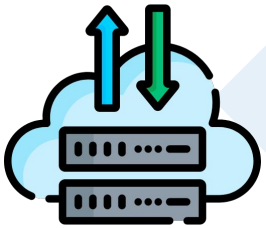
- Servidores/infraestrutura
- Equipe
- Marketing
- Treinamento

Revenue Streams Insert

- Mensalidade - Planos
  Planos anuais, bianuais (com desconto), trianuais (com desconto).
- Implantação
- Consultorias

Visão de Negócio

Arquitetura do Produto



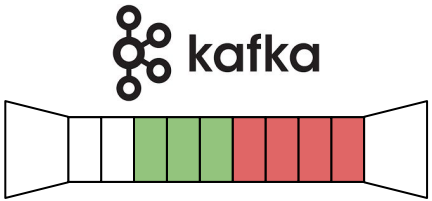
1 - Coletor

2 - Mapeamento dos Dispositivos IoT

Visão de Negócio

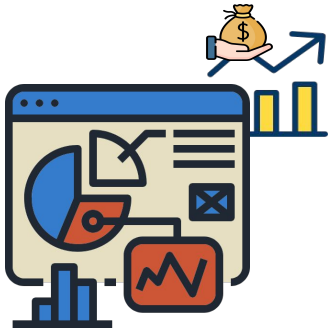
Arquitetura do Produto

3 - Gerenciador de Filas



4 - Centro de Inteligência

5 - Visualizações



Visão de Negócio

Arquitetura do Produto

Coletor | Mapeamento | Gerenciador de Filas | Centro de Inteligência | Visualização

python

WIRESHARK

python

NEURAL NETWORK

kafka

python

Java

NEURAL NETWORK

ANGULAR

spring

Bootstrap

Visão de Negócio

Parceiros Chaves

Sherlock-X

EARLYSEC

UFPR
UNIVERSIDADE FEDERAL DO PARANÁ

SEBRAE

nas nuvens

RNP

Visão de Negócio

Fontes de Receita

Mensalidades

Implantação

Consultoria

Equipe GT-Arquimedes

Coordenadores, desenvolvedores e mentores

Michele Nogueira
Coordenadora
UFPR/UFMG

Wagner Monteverde
Assistente de Inovação
EarlySec

Fausto Vetter
Coordenador de P&D
RNP

Ricardo T. Macedo
Pesquisador
UFSM

Andressa Vergütz
Desenvolvedora
UFPR

Bruna V. Santos
Desenvolvedora
UFSM

Fábio L. Carneiro
Desenvolvedor
UFPB

Thiago A. N. França
Desenvolvedor
UTFPR

Alex Julian
Mentor
UHG/RNP

Michele Nogueira
Doutora em Ciência da Computação
Universidade Federal do Paraná (UFPR) e
Universidade Federal de Minas Gerais (UFMG)

Wagner Monteverde
Especialista em Segurança da Informação
e Privacidade (Startup EarlySec)
wagner@earlysec.com

gt.arquimedes@gmail.com