Desafios e Perspectivas do Projeto MISP ReGIC sob a Óptica do Coordenador da Rede Federal de Gestão de Incidentes Cibernéticos

AGENDA

01 Contextualização

- O que é CTIR Gov?
- O que é a ReGIC?
- Quais os objetivos da ReGIC?
- Velocidade de propagação das ameaças cibernéticas

02 Projeto MISP ReGIC

- O que é o Projeto MISP ReGIC?
- Quais os objetivos do Projeto MISP ReGIC?
- Como será estruturada a Rede MISP do Projeto ReGIC?

03 Desafios do Projeto

- De Governança
- Técnicos

04 Perspectivas do Projeto

- Melhoria na curadoria dos IoCs
- Ampliação da Rede MISP para todos os Setores Críticos para o Governo
- Aumentar os acordos de parcerias

05 Considerações Finais

CONTEXTUALIZAÇÃO

O que é o CTIR Gov?

Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo

CONTEXTUALIZAÇÃO

O que é o CTIR Gov?

Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo

CSIRT de governo para coordenação, tratamento e resposta a incidentes cibernéticos no âmbito da Administração Pública Federal

CONTEXTUALIZAÇÃO

O que é o CTIR Gov?

Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo

Competências Legais e Acessórias

Portaria Ministerial nº 91, de 26 de julho de 2017

Dec nº 10.748, de 16 de julho de 2021

CONTEXTUALIZAÇÃO

O que é a ReGIC?

Dec nº 10.748, de 16 de julho de 2021
Institui a Rede Federal de Gestão de Incidentes Cibernéticos

CONTEXTUALIZAÇÃO

O que é a ReGIC?

Dec nº 10.748, de 16 de julho de 2021
Institui a Rede Federal de Gestão de Incidentes Cibernéticos

É uma estrutura colaborativa no Brasil que visa coordenar a prevenção, detecção, resposta e recuperação de incidentes cibernéticos envolvendo órgãos e entidades membros da rede.

CONTEXTUALIZAÇÃO

Quais os objetivos da ReGIC?

CONTEXTUALIZAÇÃO

Quais os objetivos da ReGIC?

I - divulgar medidas de prevenção, tratamento e resposta a incidentes cibernéticos

CONTEXTUALIZAÇÃO

Quais os objetivos da ReGIC?

I - divulgar medidas de prevenção, tratamento e resposta a incidentes cibernéticos

II - compartilhar alertas sobre ameaças e vulnerabilidades cibernéticas

CONTEXTUALIZAÇÃO

Quais os objetivos da ReGIC?

I - divulgar medidas de prevenção, tratamento e resposta a incidentes cibernéticos

II - compartilhar alertas sobre ameaças e vulnerabilidades cibernéticas

III - divulgar informações sobre ataques cibernéticos

CONTEXTUALIZAÇÃO

Quais os objetivos da ReGIC?

I - divulgar medidas de prevenção, tratamento e resposta a incidentes cibernéticos

II - compartilhar alertas sobre ameaças e vulnerabilidades cibernéticas

III - divulgar informações sobre ataques cibernéticos

IV - promover a cooperação entre os participantes da Rede

CONTEXTUALIZAÇÃO

Quais os objetivos da ReGIC?

I - divulgar medidas de prevenção, tratamento e resposta a incidentes cibernéticos

II - compartilhar alertas sobre ameaças e vulnerabilidades cibernéticas

III - divulgar informações sobre ataques cibernéticos

IV - promover a cooperação entre os participantes da Rede

V - promover a celeridade na resposta a incidentes cibernéticos

CONTEXTUALIZAÇÃO

Quais os objetivos da ReGIC?

I - divulgar medidas de prevenção, tratamento e resposta a incidentes cibernéticos

II - compartilhar alertas sobre ameaças e vulnerabilidades cibernéticas

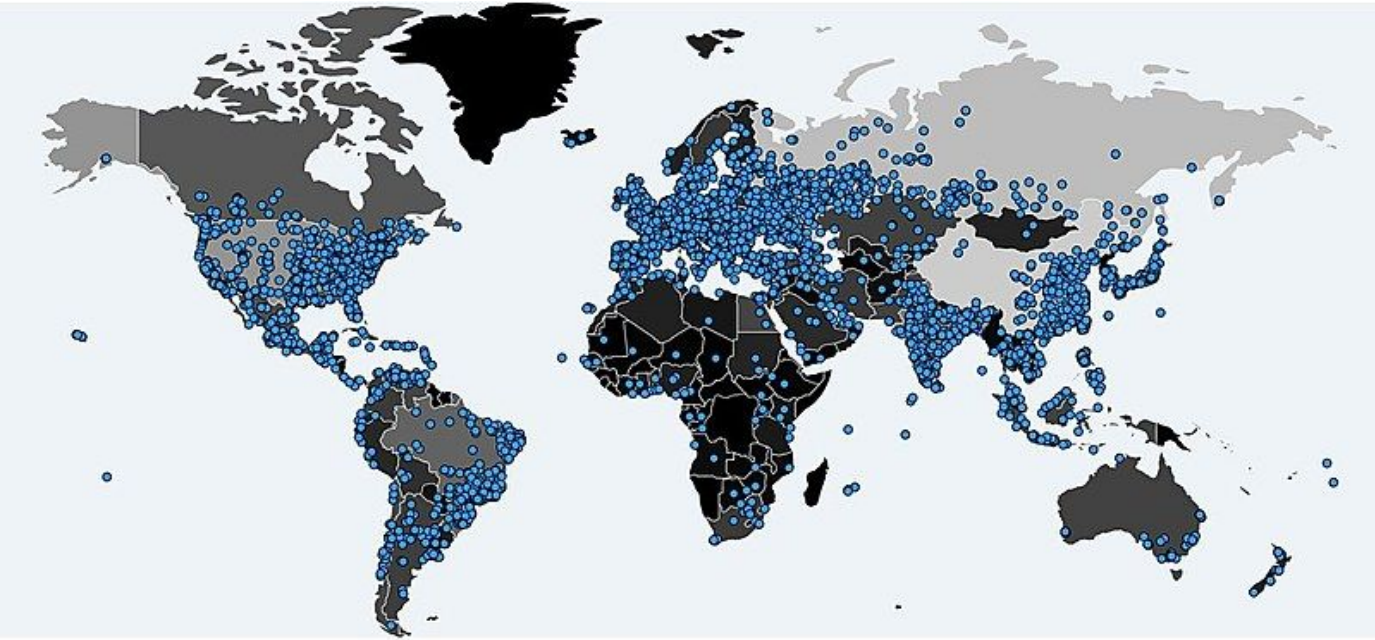
III - divulgar informações sobre ataques cibernéticos

IV - promover a cooperação entre os participantes da Rede

V - promover a celeridade na resposta a incidentes cibernéticos

CONTEXTUALIZAÇÃO

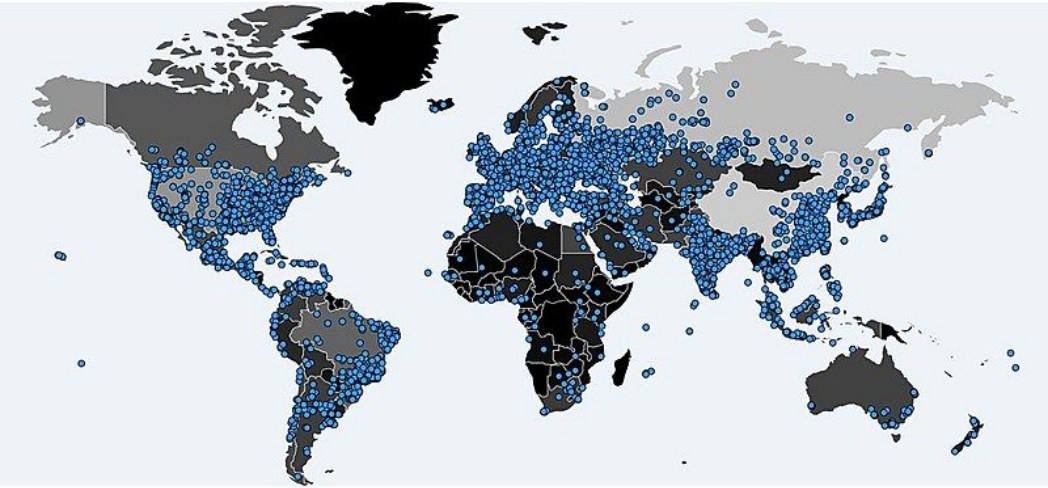
Velocidade de propagação das Ameaças Cibernéticas



CONTEXTUALIZAÇÃO

Velocidade de propagação das Ameaças Cibernéticas

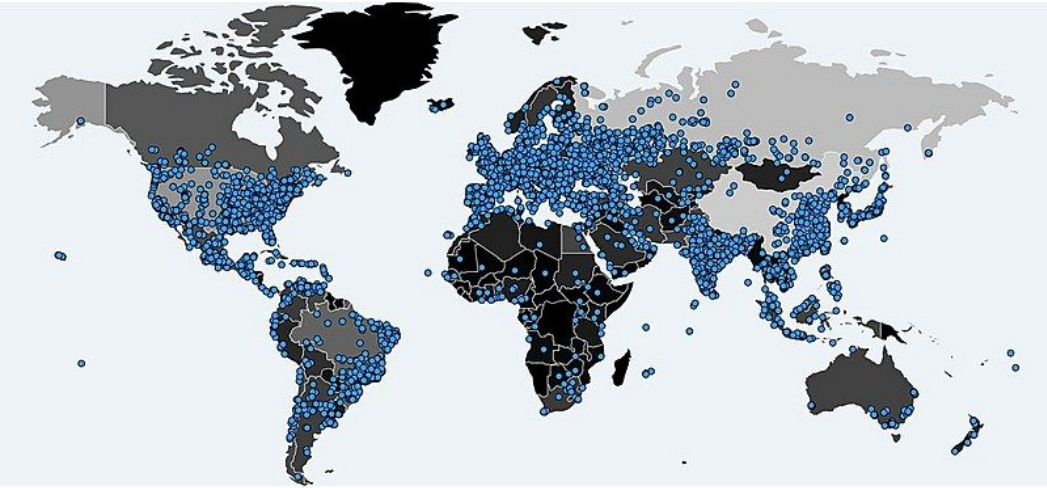
Ameaças cibernéticas podem, explorando diversos vetores ataque, se espalhar globalmente em questão de minutos



CONTEXTUALIZAÇÃO

Velocidade de propagação das Ameaças Cibernéticas

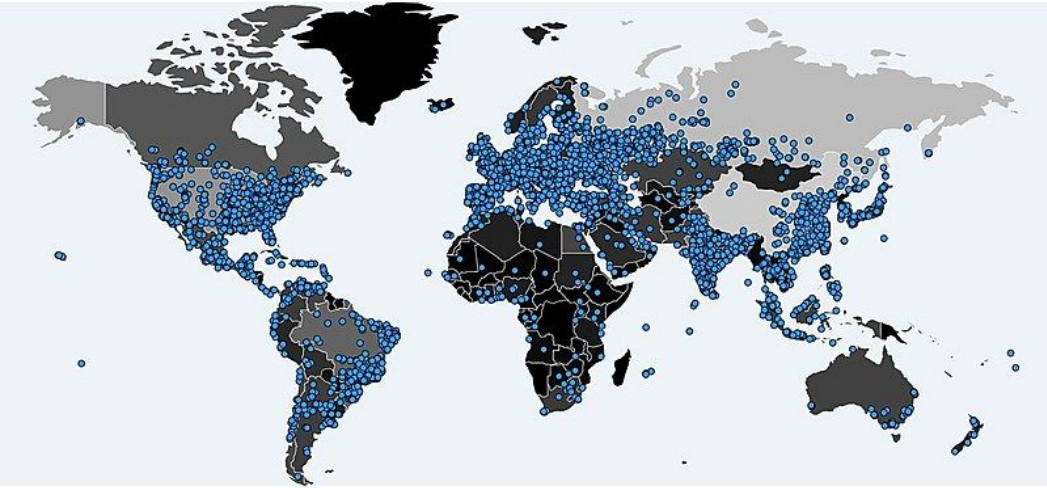
Mirai (2016) infectou mais de 400.000 de dispositivos IoT em 24 horas (Fonte:https://www.akamai.com/resources/other-resources/mirai-botnet-attack-dyn-analysis).



CONTEXTUALIZAÇÃO

Velocidade de propagação das Ameaças Cibernéticas

Mirai (2016) infectou mais 400.000 dispositivos IoT em 24 horas (Fonte:https://www.akamai.com/resources/other-resources/mirai-botnet-attack-dyn-analysis).

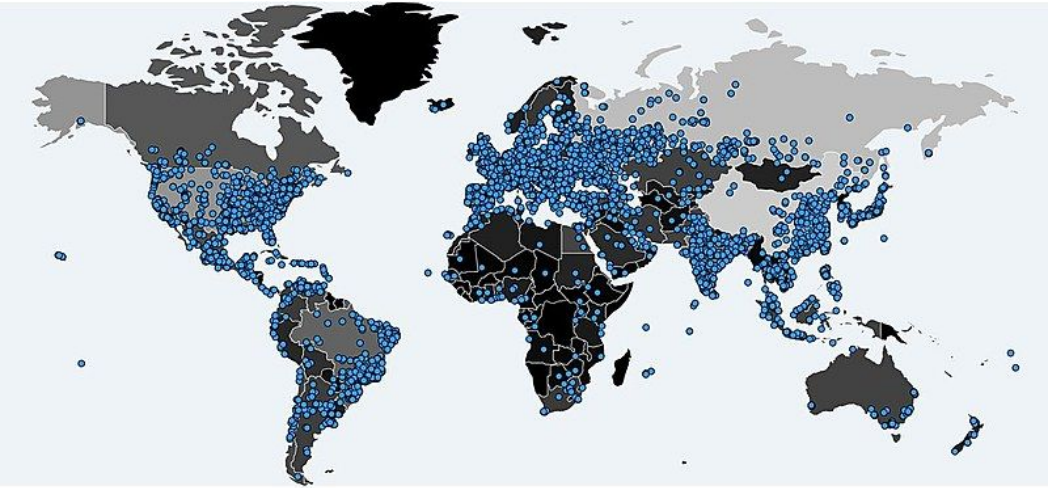


NotPetya (2017), Worm (disfarçado de ransomware), infectou mais de 10.000 sistemas em 1 hora (Ucrânia, Europa, EUA). (Fonte: https://istari-global.com/insights/spotlight/re-cap-the-untold-story-of-notpetya-the-most-devastating-cyberattack-in-history/)

CONTEXTUALIZAÇÃO

Velocidade de propagação das Ameaças Cibernéticas

Mirai (2016) infectou mais de 400.000 dispositivos IoT em 24 horas (Fonte:https://www.akamai.com/resources/other-resources/mirai-botnet-attack-dyn-analysis).



WannaCry (2017) infectou mais de 200.000 sistemas em 150 países em apenas 4 horas (Fonte: Europol, 2017).

NotPetya (2017), Worm (disfarçado de ransomware), infectou mais de 10.000 sistemas em 1 hora (Ucrânia, Europa, EUA). (Fonte: https://istari-global.com/insights/spotlight/re-cap-the-untold-story-of-notpetya-the-most-devastating-cyberattack-in-history/)

MISP E O CENÁRIO DE AMEAÇAS

O que é a Malware Information Sharing Platform MISP?

MISP E O CENÁRIO DE AMEAÇAS

O que é a Malware Information Sharing Platform MISP?

Plataforma open-source para coleta, armazenamento, distribuição e análise colaborativa de indicadores de ameaças cibernéticas (threat intelligence), como malwares, vulnerabilidades, ataques e campanhas. (Fonte: https://misp-project.org)

MISP E O CENÁRIO DE AMEAÇAS

O que é a Malware Information Sharing Platform MISP?

O MISP é uma ferramenta essencial para a inteligência colaborativa contra ameaças cibernéticas, pois permite o compartilhamento rápido de indicadores de comprometimento IoCs, ajudando organizações a se protegerem de forma proativa e a reagirem a ameaças em tempo real.

MISP E O CENÁRIO DE AMEAÇAS

Quais os benefícios do uso da MISP na minha organização?

- Inteligência de Ameaças em Tempo Real

MISP E O CENÁRIO DE AMEAÇAS

Quais os benefícios do uso da MISP na minha organização?

- Inteligência de Ameaças em Tempo Real
- Colaboração e Padronização

MISP E O CENÁRIO DE AMEAÇAS

Quais os benefícios do uso da MISP na minha organização?

- Inteligência de Ameaças em Tempo Real
- Colaboração e Padronização
- Eficiência Operacional

MISP E O CENÁRIO DE AMEAÇAS

Quais os benefícios do uso da MISP na minha organização?

- Inteligência de Ameaças em Tempo Real
- Colaboração e Padronização
- Eficiência Operacional
- Conformidade e Mitigação de Riscos

MISP E O CENÁRIO DE AMEAÇAS

Quais os benefícios do uso da MISP na minha organização?

- Inteligência de Ameaças em Tempo Real
- Colaboração e Padronização
- Eficiência Operacional
- Conformidade e Mitigação de Riscos
- Comunidade Ativa e Atualizações Contínuas

PROJETO MISP REGIC

O que é o Projeto MISP ReGIC?

A implantação da plataforma MISP surgiu como uma solução estratégica para potencializar os objetivos da Rede Federal de Gestão de Incidentes Cibernéticos - ReGIC. Esta solução permitirá não apenas a ampliação da capacidade de monitoramento e resposta, mas também fortalecerá a cooperação entre os diferentes órgãos-membros, promovendo uma abordagem proativa e coordenada frente às ameaças cibernéticas.

PROJETO MISP REGIC

Quais os requisitos para adesão ao Projeto?

Ser membro da Rede Federal de Gestão de Incidentes Cibernéticos

PROJETO MISP REGIC

Quais os requisitos para adesão ao Projeto?

- Ser membro da Rede Federal de Gestão de Incidentes Cibernéticos
- Solicitar via e-mail ao CTIR Gov (ctirgov@presidencia.gov.br)

PROJETO MISP REGIC

Quais os objetivos do Projeto?

PROJETO MISP REGIC

Quais os objetivos do Projeto?

Implementar a plataforma MISP na ReGIC, a fim de aumentar a eficiência na prevenção e resposta a incidentes cibernéticos, facilitar o compartilhamento de IoCs e promover integração com ferramentas de segurança na infraestrutura de segurança das Equipes de Tratamento e Respostas a Incidentes - ETIR integrantes da ReGIC.

PROJETO MISP REGIC

Quais os objetivos do Projeto?

Facilitar o compartilhamento de IoCs entre as ETIR, otimizando o tráfego de informações relevantes

PROJETO MISP REGIC

Quais os objetivos do Projeto?

- Facilitar o compartilhamento de IoCs entre as ETIR, otimizando o tráfego de informações relevantes
- Capacitar equipes técnicas para instalar e operar a plataforma com eficiência

PROJETO MISP REGIC

Quais os objetivos do Projeto?

- Facilitar o compartilhamento de IoCs entre as ETIR, otimizando o tráfego de informações relevantes
- Capacitar equipes técnicas para instalar e operar a plataforma com eficiência
- Automatizar o consumo de IoCs em soluções de segurança

PROJETO MISP REGIC

Quais os objetivos do Projeto?

- Facilitar o compartilhamento de IoCs entre as ETIR, otimizando o tráfego de informações relevantes
- Capacitar equipes técnicas para instalar e operar a plataforma com eficiência
- Automatizar o consumo de IoCs em soluções de segurança
- Fortalecer a segurança cibernética nacional por meio de análise colaborativa de eventos

PROJETO MISP REGIC

Quais os objetivos do Projeto?

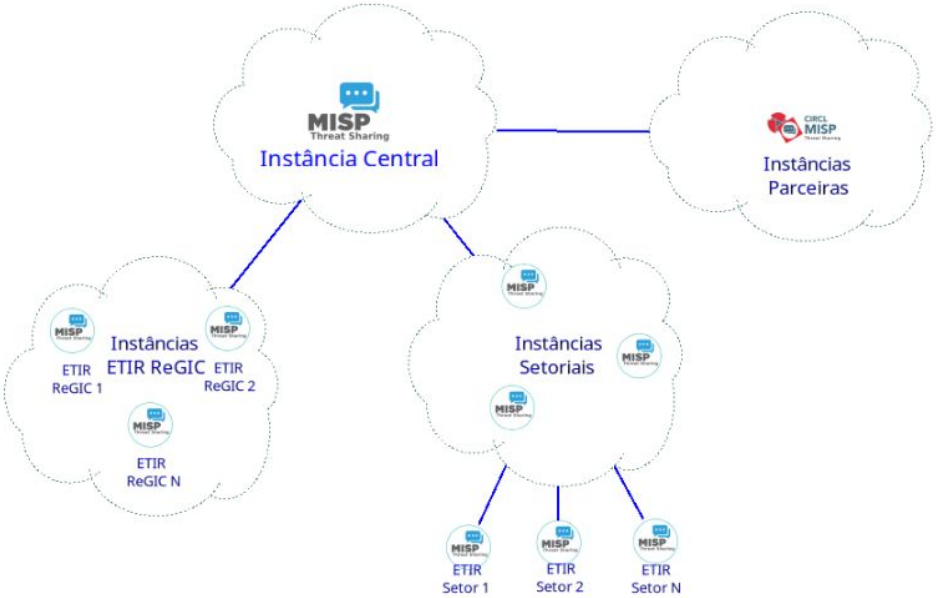
- Facilitar o compartilhamento de IoCs entre as ETIR, otimizando o tráfego de informações relevantes
- Capacitar equipes técnicas para instalar e operar a plataforma com eficiência
- Automatizar o consumo de IoCs em soluções de segurança
- Fortalecer a segurança cibernética nacional por meio de análise colaborativa de eventos
- Estabelecer comunidades específicas e gerais para feeds de inteligência cibernética

PROJETO MISP REGIC

Como será estruturada a Rede MISP do Projeto ReGIC?

PROJETO MISP REGIC

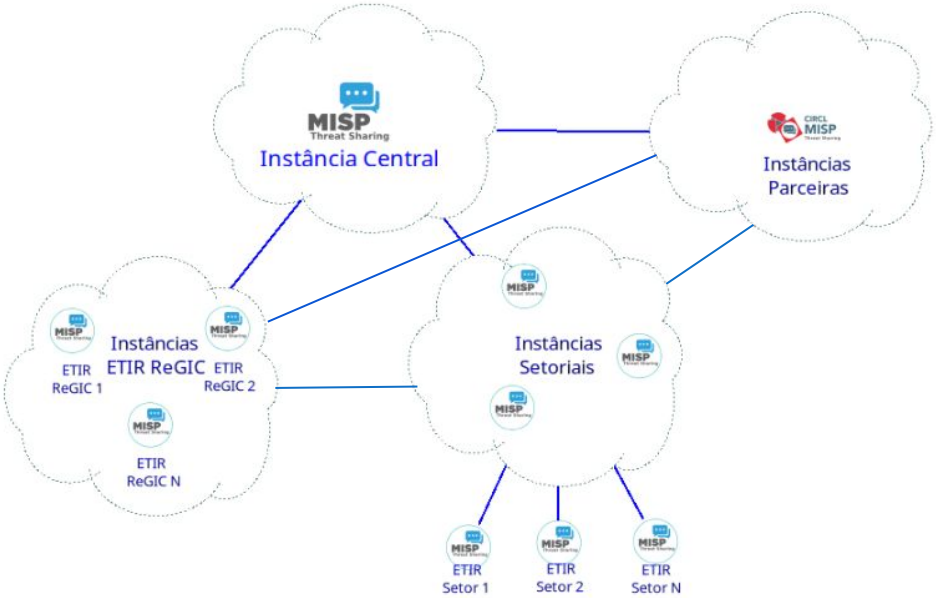
Como será estruturada a Rede MISP do Projeto ReGIC?



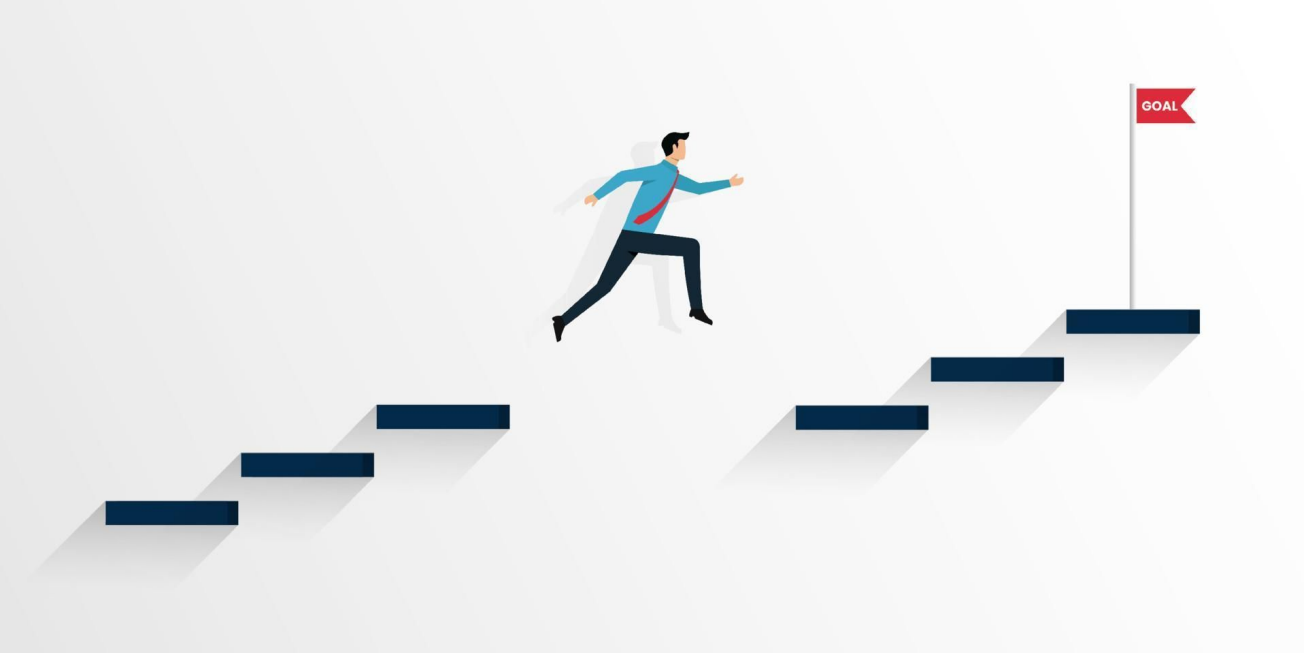
PROJETO MISP REGIC

Como será estruturada a Rede MISP do Projeto ReGIC?

Uma estrutura como esta é incentivada pelo CTIR Gov



DESAFIOS DO PROJETO



DESAFIOS DO PROJETO

De Governança

Coordenação multissetorial e alinhamento de interesses

DESAFIOS DO PROJETO

De Governança

- Coordenação multissetorial e alinhamento de interesses
- Adoção e engajamento dos participantes

DESAFIOS DO PROJETO

De Governança

- Coordenação multissetorial e alinhamento de interesses
- Adoção e engajamento dos participantes
- Gestão de dados

DESAFIOS DO PROJETO

De Governança

- Coordenação multissetorial e alinhamento de interesses
- Adoção e engajamento dos participantes
- Gestão de dados
- Sustentabilidade financeira e recursos

DESAFIOS DO PROJETO

De Governança

- Coordenação multissetorial e alinhamento de interesses
- Adoção e engajamento dos participantes
- Gestão de dados
- Sustentabilidade financeira e recursos
- Diferentes níveis de maturidade entre ETIRs da Rede

DESAFIOS DO PROJETO

Técnicos

Conhecimento técnico acerca da plataforma

DESAFIOS DO PROJETO

Técnicos

- Conhecimento técnico acerca da plataforma
- Curadoria de IoCs

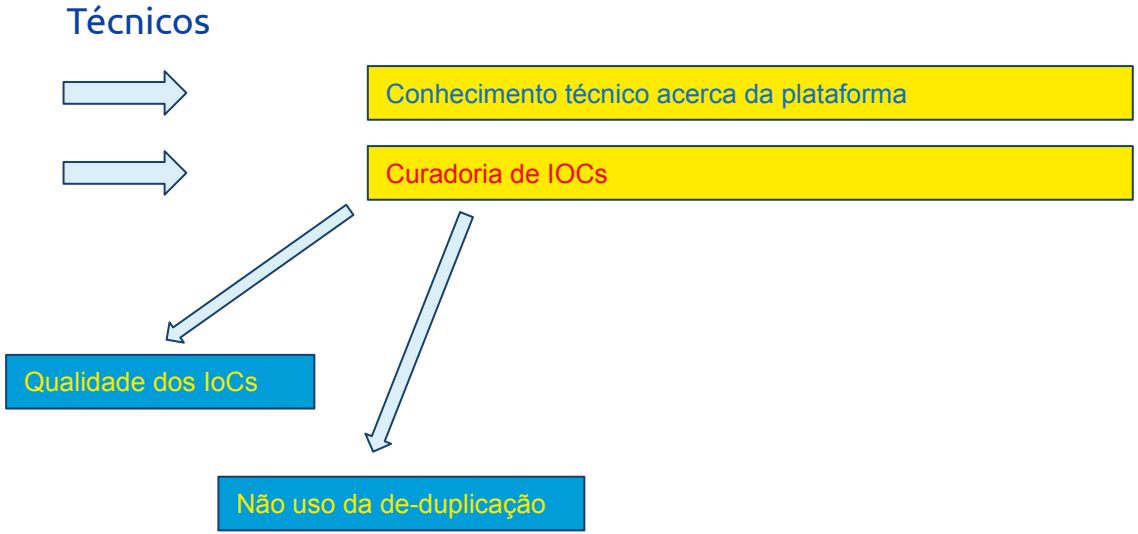
DESAFIOS DO PROJETO

Técnicos

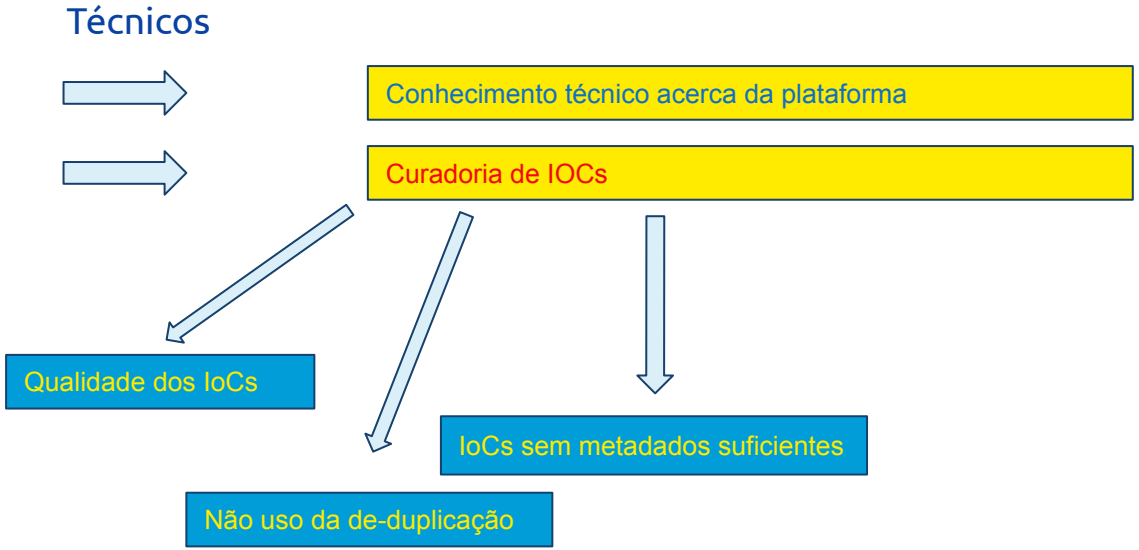
- Conhecimento técnico acerca da plataforma
- Curadoria de IOCs

Qualidade dos IoCs

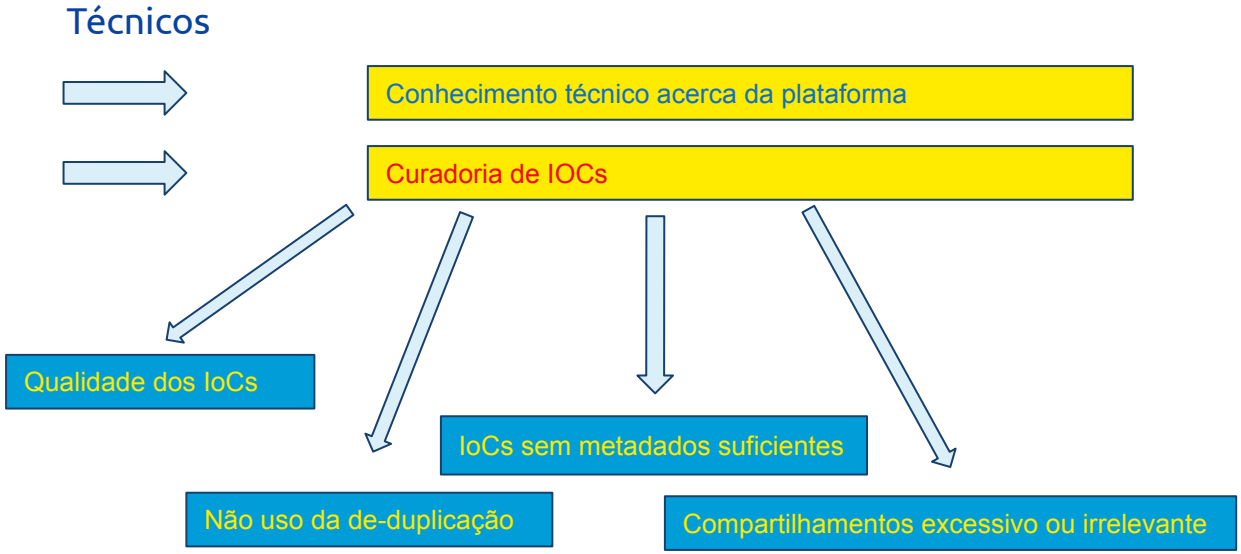
DESAFIOS DO PROJETO



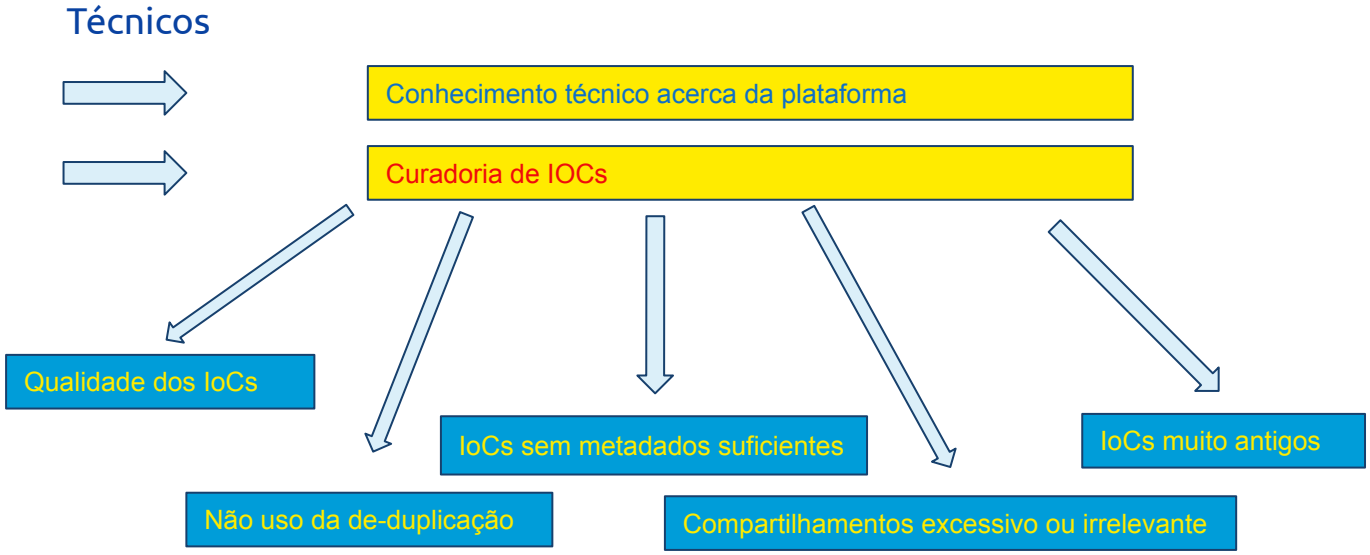
DESAFIOS DO PROJETO



DESAFIOS DO PROJETO



DESAFIOS DO PROJETO



DESAFIOS DO PROJETO

Técnicos

- Conhecimento técnico acerca da plataforma
- Curadoria de IOCs
- Dificuldade em entender as formas de consumo de IOCs

DESAFIOS DO PROJETO

Técnicos

- Conhecimento técnico acerca da plataforma
- Curadoria de IOCs
- Dificuldade em entender as formas de consumo de IOCs
- Dificuldades na automatização

DESAFIOS DO PROJETO

Técnicos

- Conhecimento técnico acerca da plataforma
- Curadoria de IOCs
- Dificuldade em entender as formas de consumo de IOCs
- Dificuldades na automatização
- Dificuldades na integração com ativos de segurança

DESAFIOS DO PROJETO

Técnicos

- Conhecimento técnico acerca da plataforma
- Curadoria de IOCs
- Dificuldade em entender as formas de consumo de IOCs
- Dificuldades na automatização
- Dificuldades na integração com ativos de segurança
- Dificuldades com troubleshoot

PERSPECTIVAS DO PROJETO

PERSPECTIVAS DO PROJETO

- Aumentar o engajamento dos membros da ReGIC e parceiros

PERSPECTIVAS DO PROJETO

- Aumentar o engajamento dos membros da ReGIC e parceiros
- Melhorar a coordenação

PERSPECTIVAS DO PROJETO

- Aumentar o engajamento dos membros da ReGIC e parceiros
- Melhorar a coordenação
- Estabelecer um nível adequado e útil de gestão de dados

PERSPECTIVAS DO PROJETO

- Aumentar o engajamento dos membros da ReGIC e parceiros
- Melhorar a coordenação
- Estabelecer um nível adequado e útil de gestão de dados
- Estabelecer um padrão aceitável de curadoria de IoCs

PERSPECTIVAS DO PROJETO

- Aumentar o engajamento dos membros da ReGIC e parceiros
- Melhorar a coordenação
- Estabelecer um nível adequado e útil de gestão de dados
- Estabelecer um padrão aceitável de curadoria de IoCs
- Oferecer capacitação técnica para operação do MISP e consumo de IoCs

PERSPECTIVAS DO PROJETO

- Aumentar o engajamento dos membros da ReGIC e parceiros
- Melhorar a coordenação
- Estabelecer um nível adequado e útil de gestão de dados
- Estabelecer um padrão aceitável de curadoria de IoCs
- Oferecer capacitação técnica operação do MISP e consumo de IoCs
- Ter um instância MISP em toda ETIR Setorial

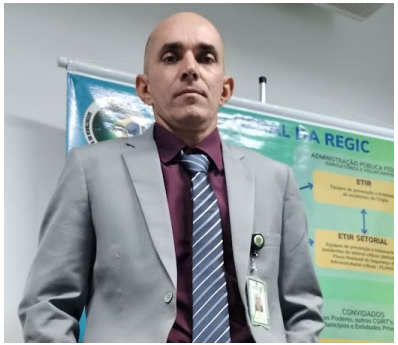
PERSPECTIVAS DO PROJETO

- Aumentar o engajamento dos membros da ReGIC e parceiros
- Melhorar a coordenação
- Estabelecer um nível adequado e útil de gestão de dados
- Estabelecer um padrão aceitável de curadoria de IoCs
- Oferecer capacitação técnica operação do MISP e consumo de IoCs
- Ter um instância MISP em toda ETIR Setorial
- Construir mais acordos e parcerias com foco no compartilhamento de informação

Considerações Finais

O projeto de implantação da MISP na ReGIC apresenta grande potencial estratégico, mas enfrenta desafios relacionados à comunicação, engajamento e capacidade técnica. Para garantir seu sucesso, é fundamental que haja uma estratégia integrada de comunicação, suporte técnico robusto e que se busque parcerias estratégicas que fortaleçam tecnicamente as ETIRs integrantes da ReGIC.

CONTATOS



CERT
Incident Response Process Professional
Certificate Holder

Colaborar para o aumento da resiliência cibernética nas instituições brasileiras é a nossa missão!