7° WEBINÁRIO

USO DA MALWARE INFORMATION SHARING PLATFORM (MISP) NA REDE FEDERAL DE GESTÃO DE INCIDENTES CIBERNÉTICOS (REGIC)

Data: 24 Abr 25

Local: On-line - Plataforma Teams

GABINETE DE SEGURANÇA INSTITUCIONAL

GOVERNO FEDERAL BRASIL UNIÃO E RECONSTRUÇÃO

Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo
- CTIR Gov -

Uso da Malware Information Sharing Platform - MISP
na
Rede Federal de Gestão de Incidentes Cibernéticos - ReGIC

AGENDA

01 Contextualização

- Ameaças Cibernéticas
- Velocidade de propagação das Ameaças Cibernéticas

02 MISP e o cenário de ameaças

- O que é a Malware Information Sharing Platform MISP?
- Quais os benefícios do uso da MISP na minha organização?
- Quais os requisitos para a implementação da MISP na minha organização?

03 Projeto MISP ReGIC

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

04 Consumo de IOCs MISP na Rede

- Como a minha organização pode consumir IOCs sobre eventos do Projeto MISP ReGIC?
- Compartilhamento intra-rede
- Consumo via Feeds
- Consumo setorizado
- Caso de Uso Simulado

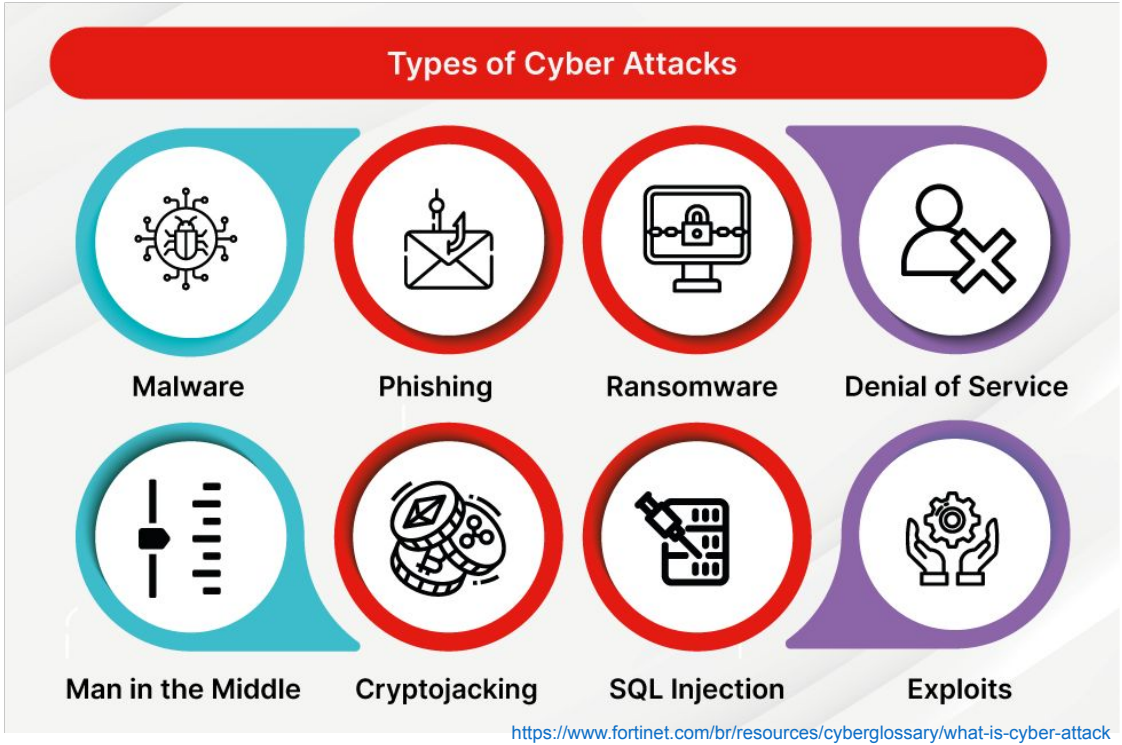
05 Fontes de consulta?

- Site do Projeto
- Notas disponibilizada pela comunidade

06 Perguntas

CONTEXTUALIZAÇÃO

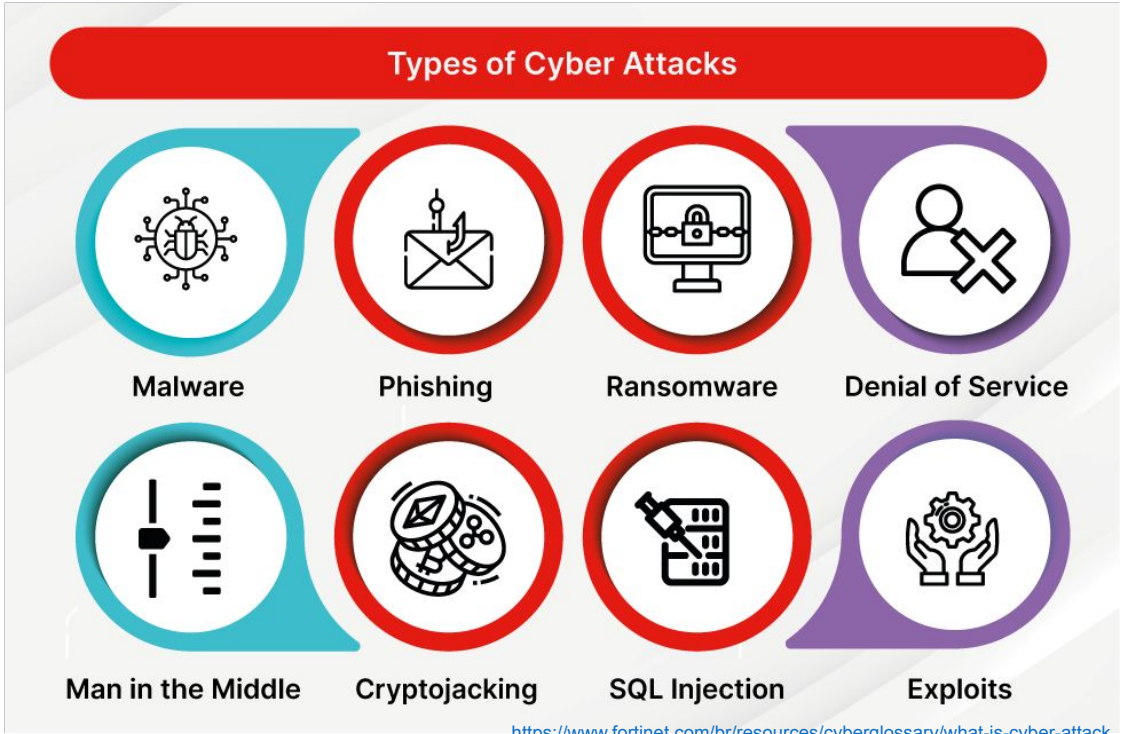
Ameaças Cibernéticas



https://www.fortinet.com/br/resources/cyberglossary/what-is-cyber-attack

CONTEXTUALIZAÇÃO

Ameaças Cibernéticas

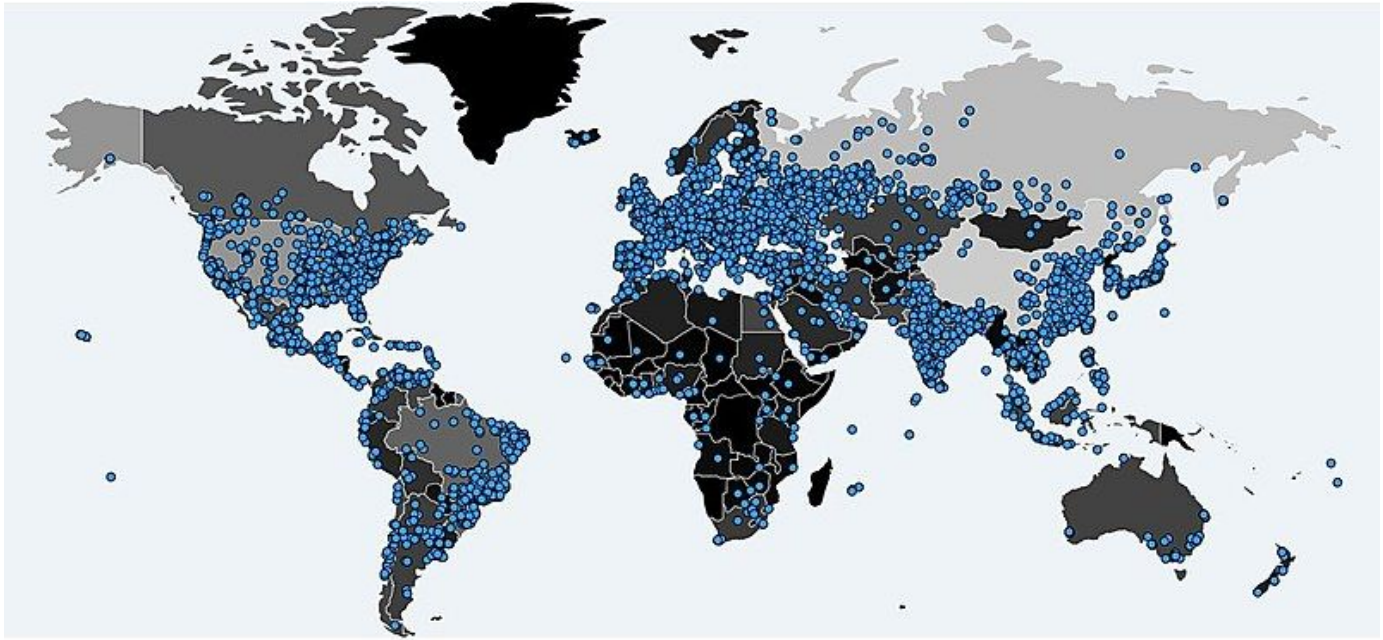


https://www.fortinet.com/br/resources/cyberglossary/what-is-cyber-attack

Qualquer ação maliciosa, intencional ou oportunista para roubar, danificar ou acessar ilegalmente dados, redes ou dispositivos de redes

CONTEXTUALIZAÇÃO

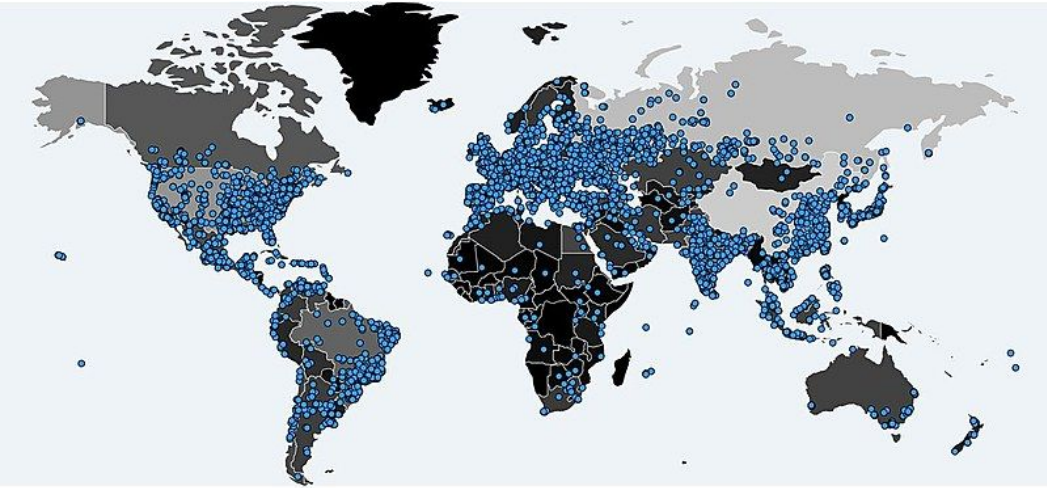
Velocidade de propagação das Ameaças Cibernéticas



CONTEXTUALIZAÇÃO

Velocidade de propagação das Ameaças Cibernéticas

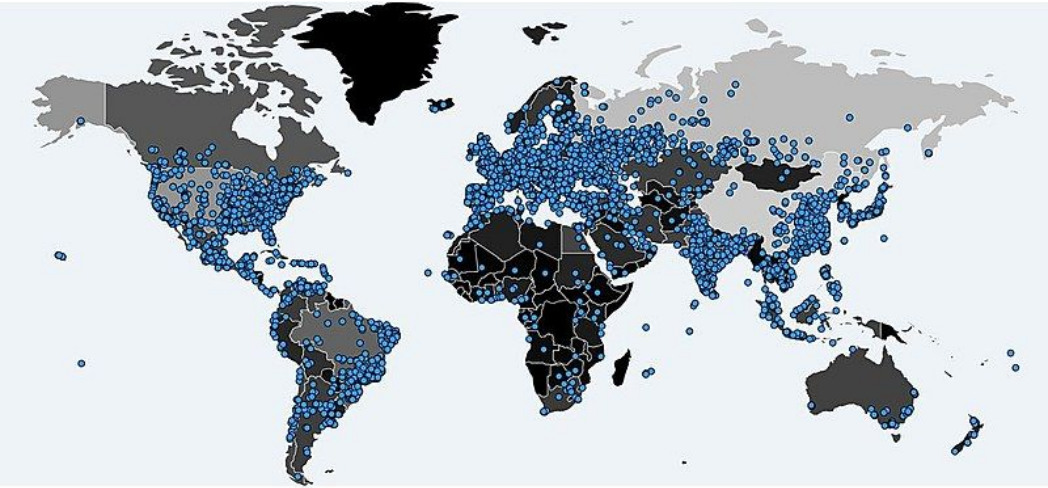
Ameaças cibernéticas como worms e ataques de ransomware, podem se espalhar globalmente em questão de minutos, explorando vulnerabilidades não corrigidas ou engenharia social



CONTEXTUALIZAÇÃO

Velocidade de propagação das Ameaças Cibernéticas

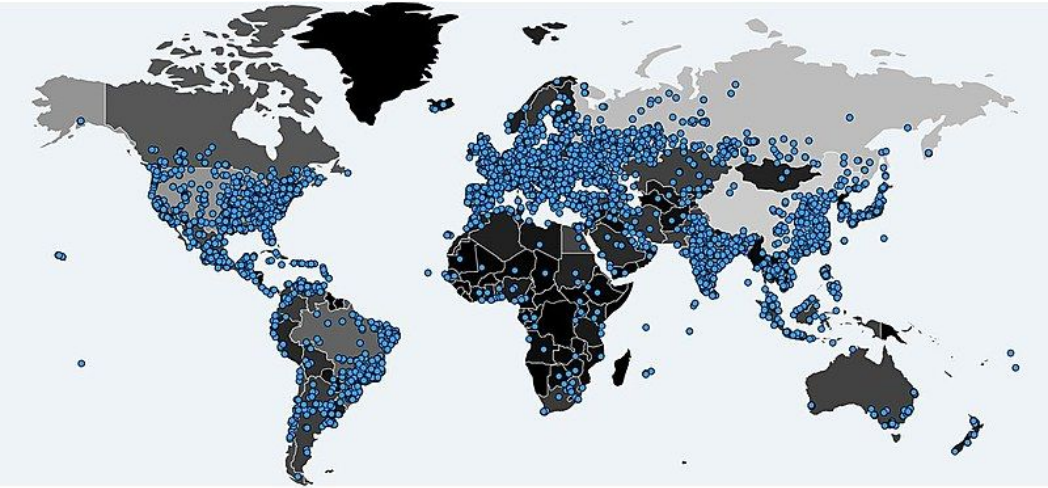
Mirai (2016) infectou mais de 400.000 de dispositivos IoT em 24 horas (Fonte:https://www.akamai.com/resources/other-resources/mirai-botnet-attack-dyn-analysis).



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).

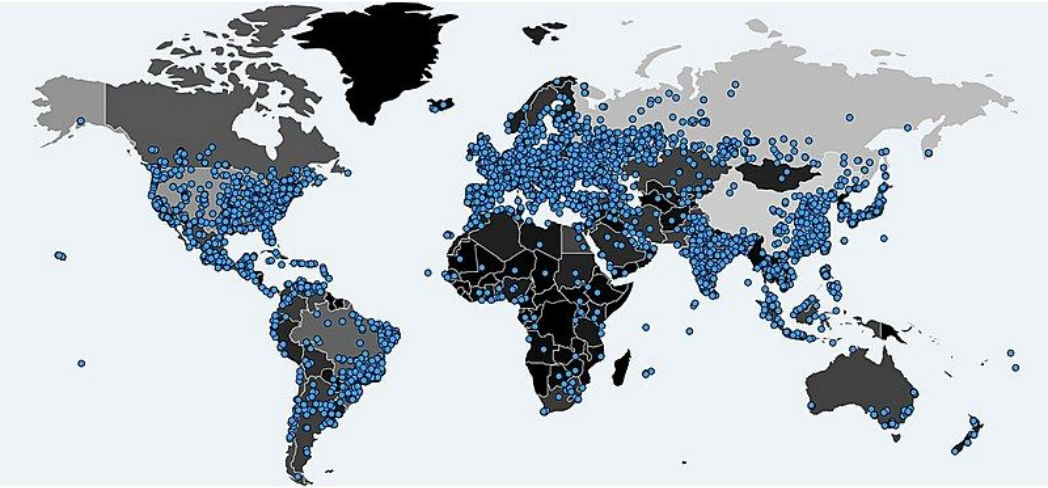


NotPetya (2017), Worm (disfarçado de ransomware), infectou mais de 10.000 sistemas em 1 hora (Ucrânia, Europa, EUA). (Fonte: https://istari-global.com/insights/spotlight/re-cap-the-untold-story-of-notpetya-the-most-devastating-cyberattack-in-history/)

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

MISP E O CENÁRIO DE AMEAÇAS

Quais os requisitos para a implementação da MISP na minha organização?

MISP E O CENÁRIO DE AMEAÇAS

Quais os requisitos para a implementação da MISP na minha organização?

Hardware

Servidor dedicado (físico ou virtual):

- CPU: Mínimo 4 núcleos (recomendado 8+ para grandes volumes de dados);
- RAM: Mínimo 8 GB (recomendado 16 GB ou mais);
- Armazenamento: 100 GB livre (SSD recomendado para desempenho);
- Rede: Conexão estável com banda suficiente para compartilhamento de feeds.

MISP E O CENÁRIO DE AMEAÇAS

Quais os requisitos para a implementação da MISP na minha organização?

Hardware

Servidor dedicado (físico ou virtual):

- CPU: Mínimo 4 núcleos (recomendado 8+ para grandes volumes de dados);
- RAM: Mínimo 8 GB (recomendado 16 GB ou mais);
- Armazenamento: 100 GB livre (SSD recomendado para desempenho);
- Rede: Conexão estável com banda suficiente para compartilhamento de feeds.

Software

Sistema Operacional:

- Linux (Ubuntu 22.04 LTS / Debian 11+ recomendados).

Dependências:

- Apache/Nginx, MySQL/MariaDB, PHP (8.1+), Redis.
- Python 3.x e ferramentas como Git.

MISP E O CENÁRIO DE AMEAÇAS

Quais os requisitos para a implementação da MISP na minha organização?

Segurança

Acesso Restrito:

- Firewall para limitar tráfego (portas 443/HTTPS e SSH apenas para IPs autorizados).
- Autenticação de dois fatores (2FA) para usuários administrativos.

Proteção de Dados:

- Criptografia em repouso (ex.: LUKS para discos) e em trânsito (SSL/TLS).
- Backup diário dos bancos de dados e configurações (em local seguro/offline).

Monitoramento:

- Ferramentas como Auditd (Linux) para logs de acesso e alterações.
- SIEM integrado para alertas de atividades suspeitas.

PROJETO MISP REGIC

O que é o Projeto?

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?

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?

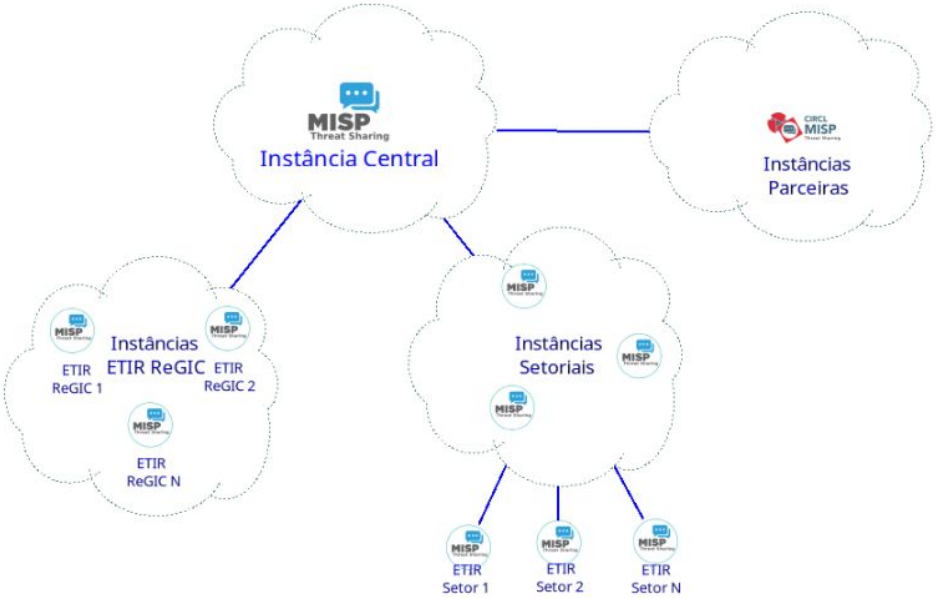
- Facilitar o compartilhamento de IoCs entre as ETIR, otimizando o tráfego de informações relevantes
- Capacitar equipes técnicas para instalar e operar a plataforma com eficiência
- Automatizar o consumo de IoCs em soluções de segurança
- Fortalecer a segurança cibernética nacional por meio de análise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

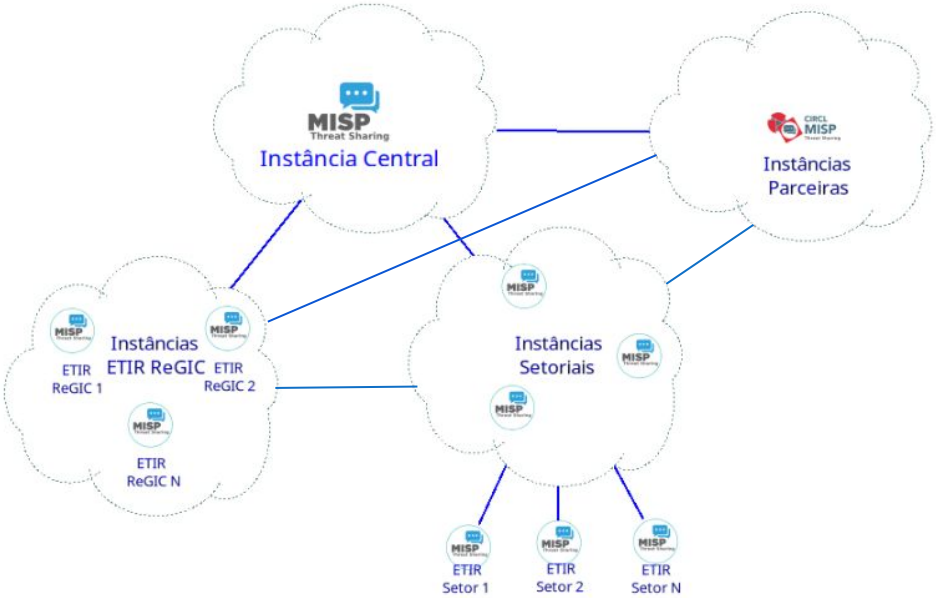
Como será estruturada a Rede MISP do Projeto ReGIC?



PROJETO MISP REGIC

Como será estruturada a Rede MISP do Projeto ReGIC?

Uma estrutura como esta é incentivada pelo CTIR Gov



CONSUMO DE IOCs MISP NA REDE

Como a minha organização pode consumir IOCs sobre eventos do Projeto MISP ReGIC?

CONSUMO DE IOCs MISP NA REDE

Como a minha organização pode consumir IOCs sobre eventos do Projeto MISP ReGIC?

Firewalls/IDS/IPS

Integração com Ativos de Segurança

CONSUMO DE IOCs MISP NA REDE

Como a minha organização pode consumir IOCs sobre eventos do Projeto MISP ReGIC?

Firewalls/IDS/IPS

Integração com Ativos de Segurança

Endpoint Detection and Response - EDR
Extended Detection and Response - XDR

CONSUMO DE IOCs MISP NA REDE

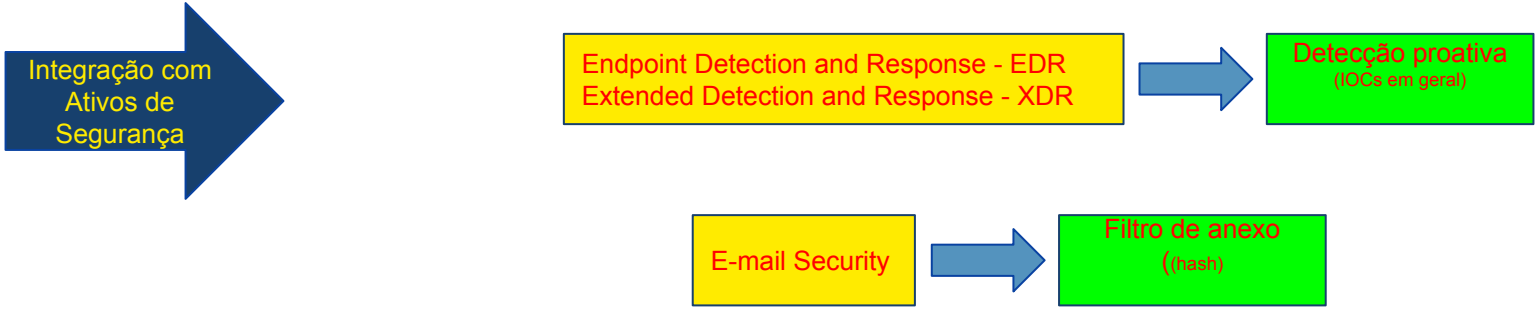
Como a minha organização pode consumir IOCs sobre eventos do Projeto MISP ReGIC?

Integração com Ativos de Segurança

- Firewalls/IDS/IPS
- Endpoint Detection and Response - EDR
  Extended Detection and Response - XDR
- E-mail Security

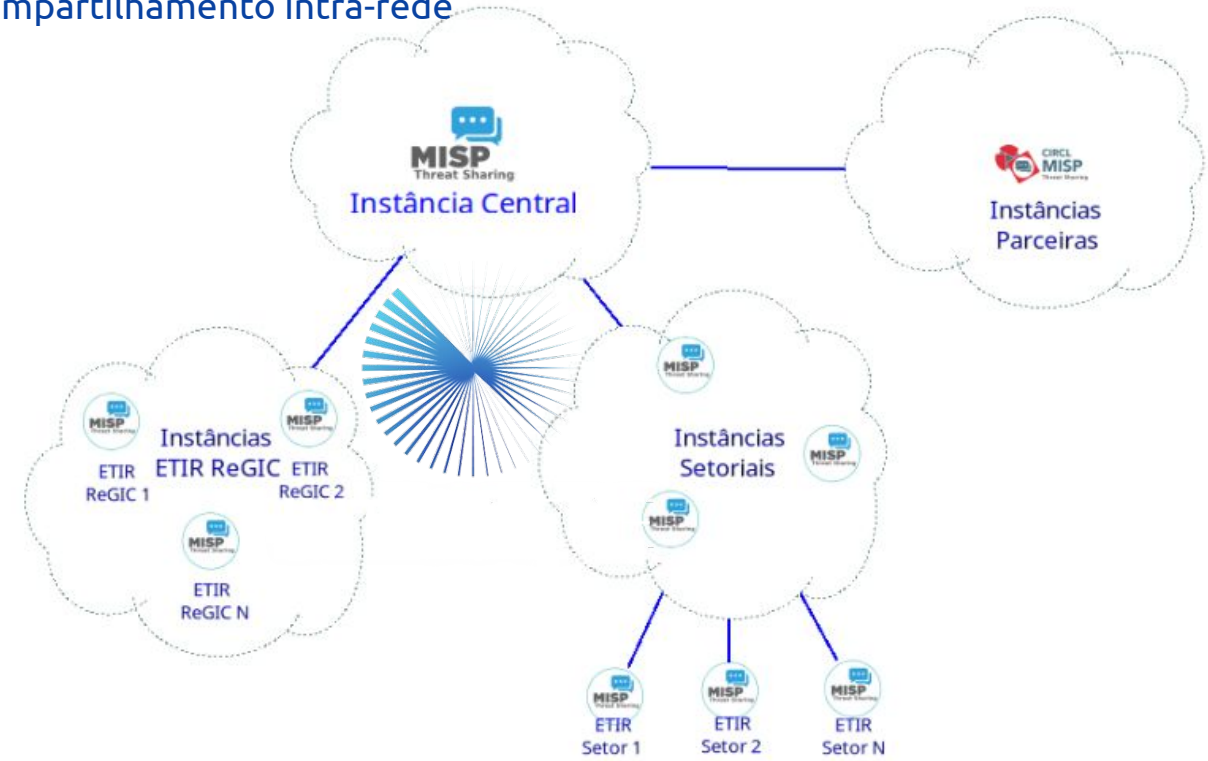
CONSUMO DE IOCs MISP NA REDE

Como a minha organização pode consumir IOCs sobre eventos do Projeto MISP ReGIC?



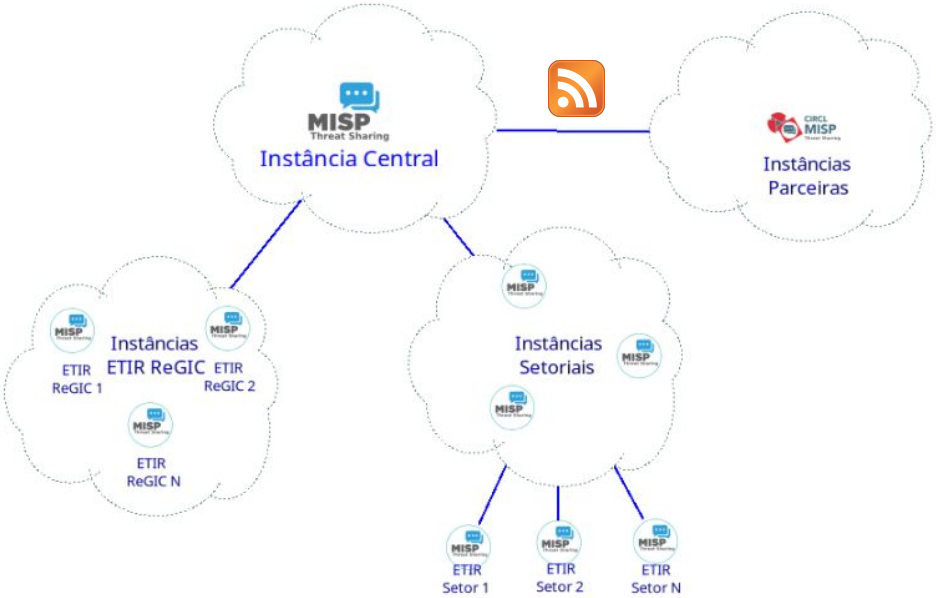
CONSUMO DE IOCs MISP NA REDE

Compartilhamento intra-rede



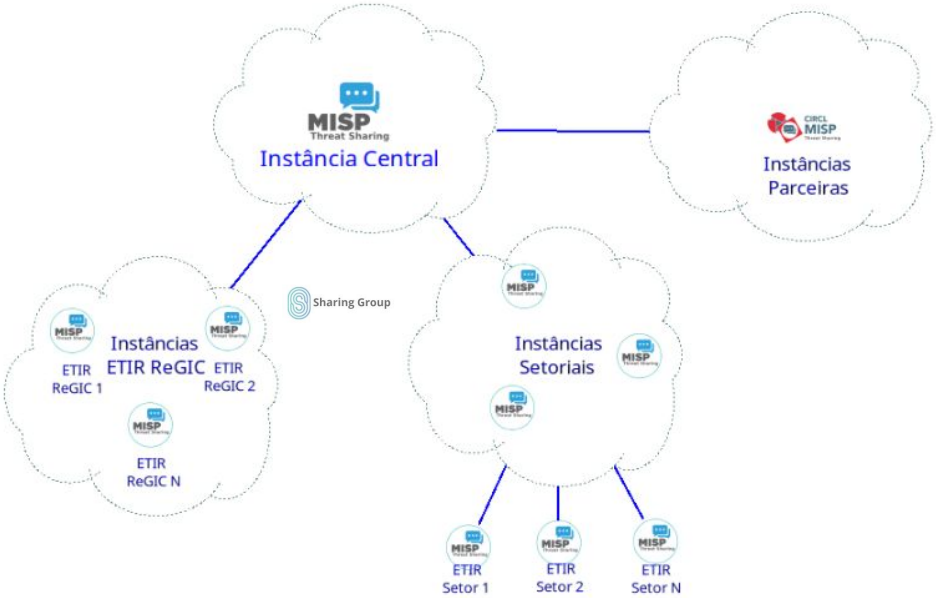
CONSUMO DE IOCs MISP NA REDE

Consumo via Feeds



CONSUMO DE IOCs MISP NA REDE

Consumo setorizado



CONSUMO DE IOCs MISP NA REDE

Caso de uso simulado

MISP/**PyMISP**

Python library using the MISP Rest API

pfsense®

FONTES DE CONSULTA

Site Oficial

FONTES DE CONSULTA

Site Oficial
- https://www.misp-project.org/

Git
- https://github.com/MISP/MISP

CIRCL
- https://www.circl.lu/services/misp-malware-information-sharing-platform/
- https://www.youtube.com/@CIRCLLuxembourg

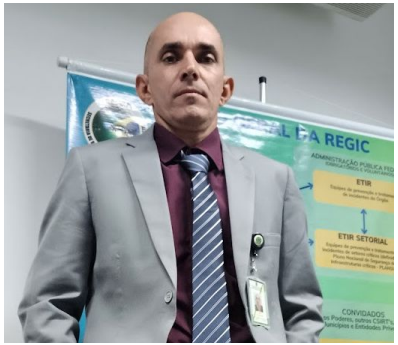
FONTES DE CONSULTA

Notas técnicas

Fonte:https://csirtamericas.org/en/resources

PERGUNTAS

CONTATOS



CERT
Incident Response Process Professional
Certificate Holder

CISSP Certified

OFFENSIVE SECURITY OSCE

OFFENSIVE SECURITY OSCP

C|EH Certified Ethical Hacker

C|HFI

www.gov.br/ctir

ctir@ctir.gov.br

ctirgov@presidencia.gov.br

adao.santos@presidencia.gov.br

linkedin.com/in/adaosantos

AVALIAÇÃO 7º WEBINÁRIO

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