COMUNIDADE MISP ABEP-TIC

INTELIGÊNCIA DE AMEAÇAS PARA OS ESTADOS BRASILEIROS

GT-SI ABEP-TIC

JULHO 25

TLP:CLEAR

AGENDA

- ABEP-TIC, CONSAD e GTD;
- Objetivos GT-SI;
- Estados membros;
- Comunidade MISP ABEP-TIC de Inteligência de ameaças;
- Cases:
  - CODATA - PB
  - PRODEMGE - MG
  - PRODAM - AM
- Desafios;
- Próximos passos;
- Integração com a rede ReGIC

TLP:CLEAR

OBJETIVOS DO GT-SI

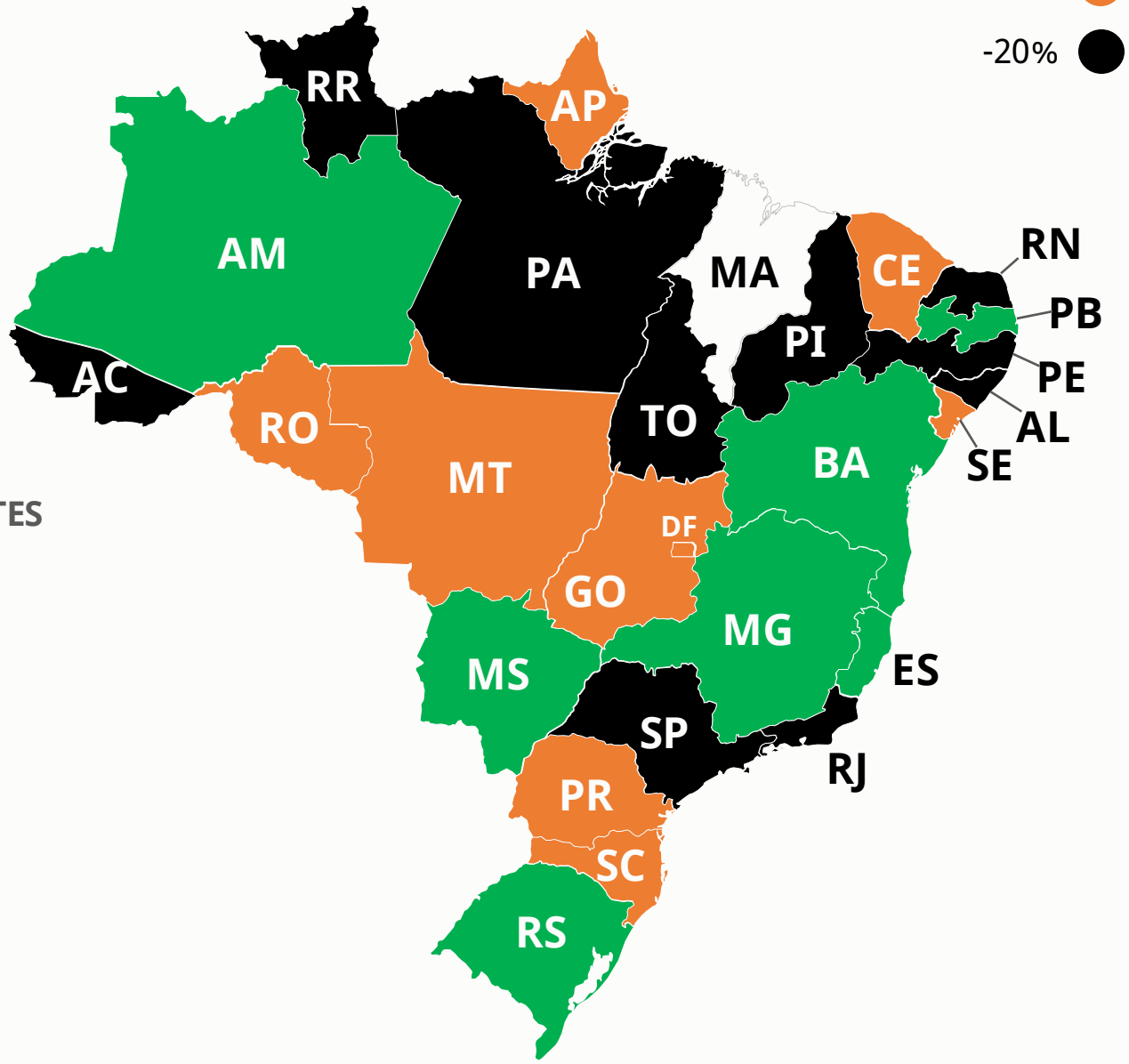
- Contribuir para a melhoria da maturidade de Segurança das associadas ABEP-TIC;
- Propor treinamentos e participação em eventos de SI;
- Realizar diagnósticos de SI e PRIVACIDADE;
- Apoiar as necessidades de SI e LGPD;
- Elaborar documentos de SI e Termos de Referência para as associadas;

GTD

- Integrar com iniciativas de SI do governo federal e internacionais;
- Estender o diagnóstico aos estados e futuramente aos municípios;
- Viabilizar treinamentos e participação em eventos de SI;
- Viabilizar o acesso a ferramentas de SI através de convênios;

MEMBROS EM 2025

+50% PRESENÇA E ENTREGAS
20-49% PRESENÇA
-20% PRESENÇA



61 PARTICIPANTES

15 FREQUENTES

25 + DF

TLP:CLEAR

PROJETO COMUNIDADE MISP ABEP-TIC

- Objetivo: Estabelecer uma rede de troca de informações de inteligência de ameaças entre as associadas ABEP-TIC, segmentos estaduais, parceiros nacionais e internacionais.
  - Secundário
    - Fomentar a formalização das equipes de segurança da informação e/ou tratamento de incidentes de SI (ETIR) nas associadas;
    - Compartilhar informações sobre ameaças, vulnerabilidades e incidentes entre as associadas e outras ETIRs;
    - Fomentar a participação das associadas na ReGIC.

TLP:CLEAR

COMUNIDADE MISP ABEP-TIC

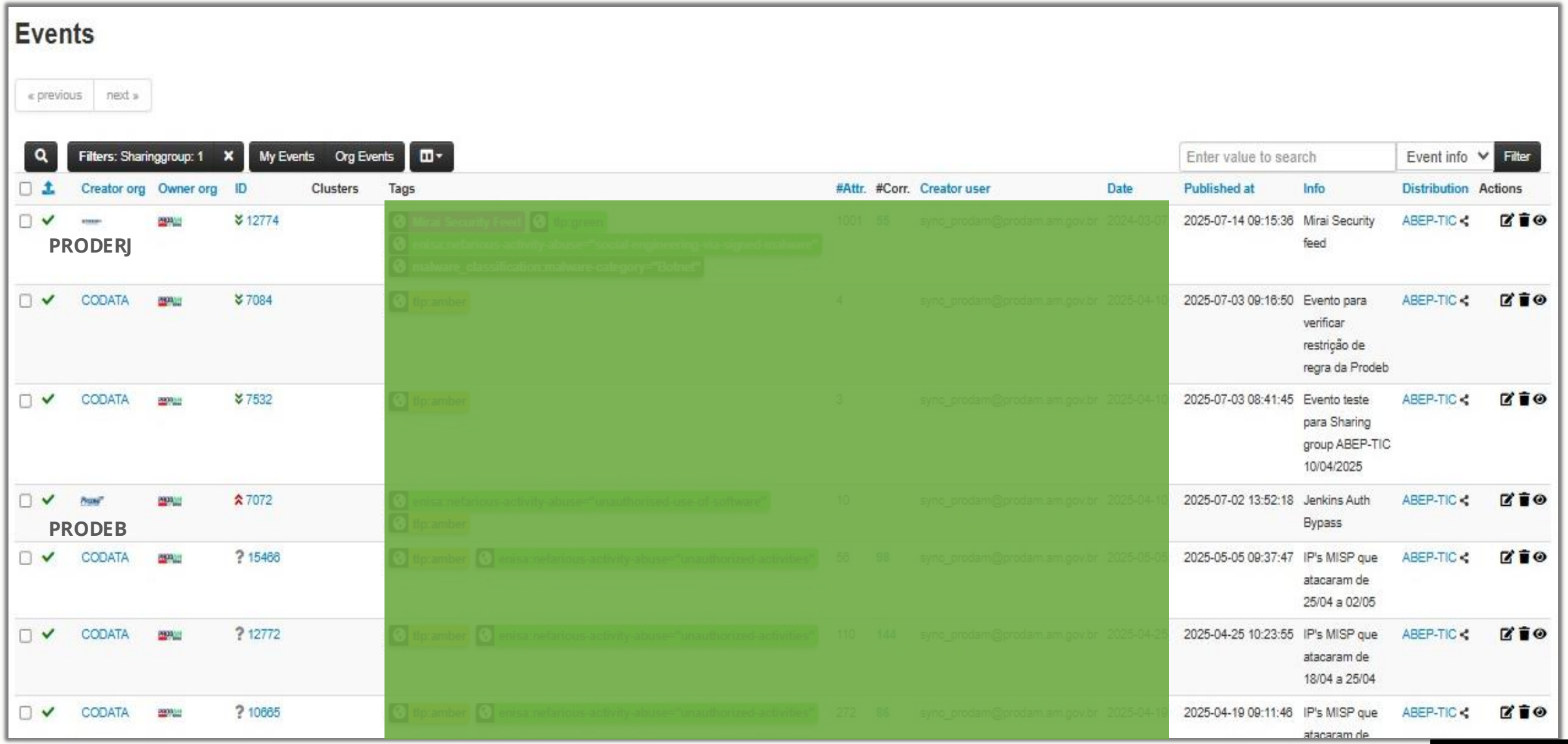
- Treinamento em formato de workshop: novembro / dezembro de 2024
  - Patrocinado pelo BID através do GTD;
  - Voltado à instalação e configuração do MISP;
  - 20 estados participantes;
    - 69 colaboradores concluíram a parte teórica;
  - 36hs de gravação;
  - Manual de instalação e configuração.

TLP:CLEAR

COMUNIDADE MISP

TLP:CLEAR

COMUNIDADE MISP ABEP-TIC



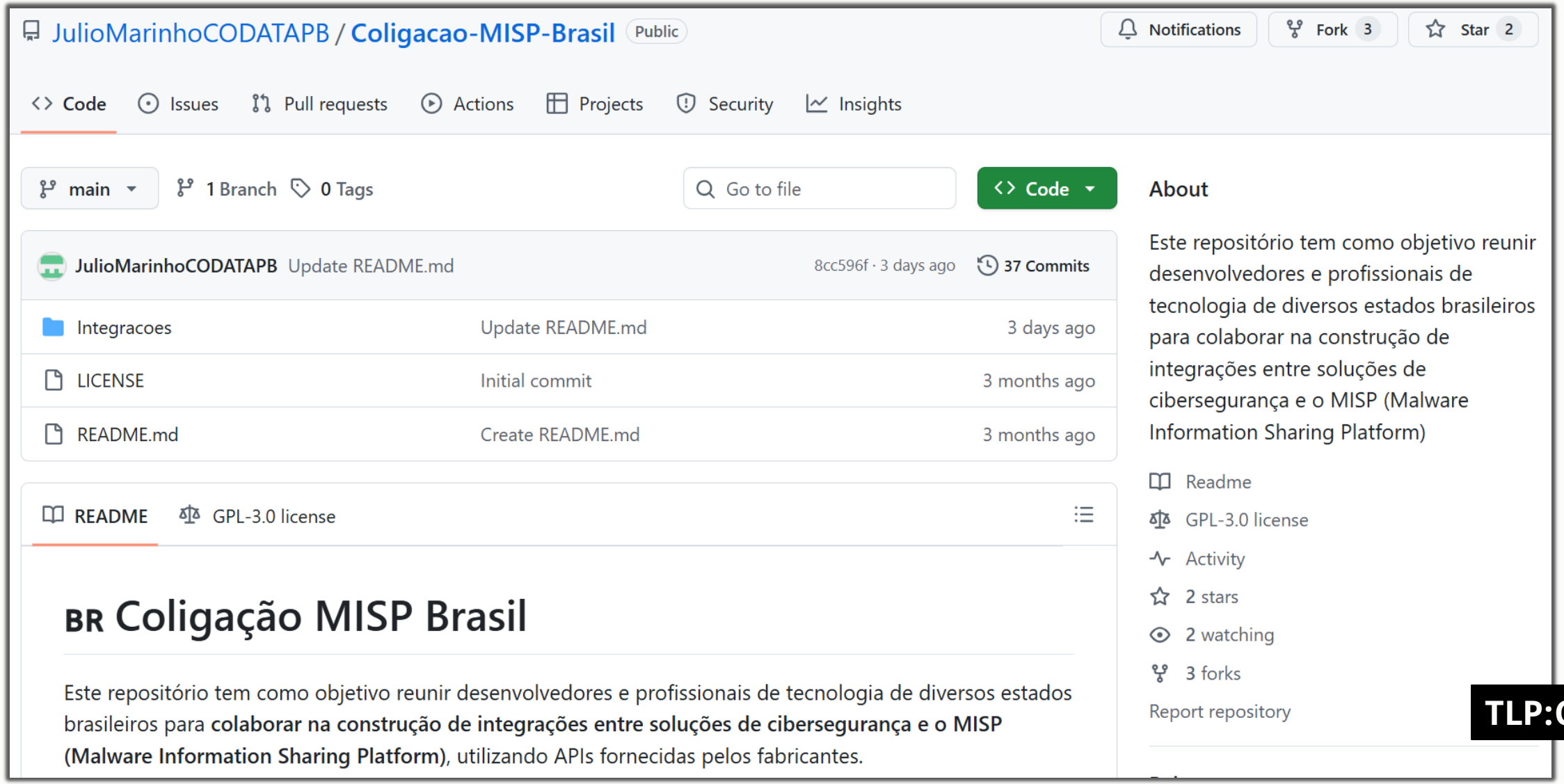
TLP:CLEAR

CASE **CODATA**

- Participa da comunidade ABEP-TIC desde 30 março de 2025
  - Conectado ao CTIR.GOV;
  - Integrou o MISP às ferramentas de SI e monitoramento
    - SIEM – confirma eventos suspeitos com IOCs do MISP;
    - *Firewall* de borda – bloqueio automático de eventos recebidos do SIEM;
    - *HoneyPot;*
  - Criou repositório GITHUB para compartilhamento das integrações MISP com outras ferramentas.

TLP:CLEAR

CASE CODATA **INTEGRAÇÕES MISP**



JulioMarinhoCODATAPB / **Coligacao-MISP-Brasil** Public

Notifications | Fork 3 | Star 2

Code | Issues | Pull requests | Actions | Projects | Security | Insights

main | 1 Branch | 0 Tags | Go to file | Code

JulioMarinhoCODATAPB Update README.md — 8cc596f · 3 days ago — 37 Commits

Integracoes	Update README.md	3 days ago
LICENSE	Initial commit	3 months ago
README.md	Create README.md	3 months ago

README | GPL-3.0 license

BR Coligação MISP Brasil

Este repositório tem como objetivo reunir desenvolvedores e profissionais de tecnologia de diversos estados brasileiros para **colaborar na construção de integrações entre soluções de cibersegurança e o MISP (Malware Information Sharing Platform)**, utilizando APIs fornecidas pelos fabricantes.

About

Este repositório tem como objetivo reunir desenvolvedores e profissionais de tecnologia de diversos estados brasileiros para colaborar na construção de integrações entre soluções de cibersegurança e o MISP (Malware Information Sharing Platform)

Readme
GPL-3.0 license
Activity
2 stars
2 watching
3 forks
Report repository

GitHub

TLP:CLEAR

CASE **CODATA**

- Próximos passos:
  - Monitorar a saída dos *Firewalls*;
  - Integrar os IOC de *hash* ao SIEM;
  - Integrar os IOC de domínios ao filtro de DNS.

TLP:CLEAR

CASE **PRODEMGE**

- Implementou MISP em 2018
  - Participa da comunidade MISP ABEP-TIC;
  - Conectado ao CERT.BR e CTIR.GOV;
  - Integrou o MISP às ferramentas de SI e monitoramento de rede internas:
    - XDR;
    - SIEM;
    - Anti-DDOS.

TLP:CLEAR

CASE **PRODAM**

- Participa da Comunidade MISP ABEP-TIC desde 14 março de 2025
  - Integrado ao CTIR.GOV;
  - Integrou o MISP às ferramentas de SI e monitoramento;
    - SIEM – confirma eventos suspeitos com IOCs do MISP;
    - Firewall de borda – bloqueio automático de eventos recebidos do SIEM.

TLP:CLEAR

DESAFIOS ENFRENTADOS PELA COMUNIDADE MISP ABEP-TIC

- Formalização de ETIRs;
- Capacitação;
- Ampliação da Comunidade para outros seguimentos;
- Integração com soluções de SI e monitoramento;
- Desenvolvimento de automações;
- Agilizar o uso do MISP na análise e compartilhamento de informações sobre ameaças.

TLP:CLEAR

COMUNIDADE ABEP-TIC DE INTELIGÊNCIA DE AMEAÇAS DE SI

- Próximas fases:
  - Capacitação avançada;
  - Integrações internacionais;
  - Integração com MISP Cert.br.

TLP:CLEAR

VISÃO GERAL DA **REDE REGIC**

ADMINISTRAÇÃO PÚBLICA FEDERAL

(OBRIGATÓRIOS E VOLUNTÁRIOS)

ETIR

Equipe de prevenção e tratamento de incidentes do Órgão

ETIR SETORIAL

Equipe de prevenção e tratamento de incidentes de setores críticos (definidos no Plano Nacional de Segurança de Infraestruturas críticas - PLANSIC

CONVIDADOS

(outros Poderes, outros CSIRT'S, Estados, Municípios e entidades Privadas)

ETIR

Equipe de prevenção e tratamento de incidentes do Órgão

TLP:CLEAR

INTEGRAÇÃO COM A **REDE REGIC**

PRODS PARTICIPANTES












13 CONVIDADAS ESTADUAIS – TREINAMENTOS **CSIRT** MENSAIS – **9** WEBINÁRIOS

TLP:CLEAR

GT-SI ABEP-TIC

PRODAM

https://prodam.am.gov.br

lilian@prodam.am.gov.br

prodemge

https://www.prodemge.gov.br

brunomcb@prodemge.gov.br

PRODEB

TECNOLOGIA, INFORMAÇÃO E SEGURANÇA.

https://www.prodeb.ba.gov.br

walter.junior@prodeb.ba.gov.br

CODATA

https://codata.pb.gov.br

juliomarinho@codata.pb.gov.br

TLP:CLEAR