Prevenção a incidentes no contexto da Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC)

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

Apresentação

Fernando Borges

Analista no CTIR Gov desde 2020

Equipe de Operações

Roteiro

TLP:CLEAR

01 CTIR Gov

RFC 2350
Constituency
Papel no GSI

02 ReGIC

Decreto
Objetivos e foco
Atividades

03 Processos e fontes de dados

Aquisição e processamento
Coordenação e compartilhamento

04 Prevenção

SSIC
Alertas e Recomendações
Mailing list

05 Parcerias

Parceiros nacionais e internacionais
Exemplos de parceria
Casos reais
Tendências e CTIR Gov em Números

06 Conclusão

Tempestividade
Proatividade
Importância da ReGIC no contexto

CTIR Gov - 18 anos

TLP:CLEAR

2024

↑

2006

Roteiro

TLP:CLEAR

CTIR Gov
01

RFC 2350
Constituency
Papel no GSI

ReGIC
02

Decreto
Objetivos e foco
Atividades

Processos e fontes de dados
03

Aquisição e processamento
Coordenação e compartilhamento

Prevenção
04

SSIC
Alertas e Recomendações
Mailing list

Parcerias
05

Parceiros nacionais e internacionais
Exemplos de parceria
Casos reais
Tendências e CTIR Gov em Números

Conclusão
06

Tempestividade
Proatividade
Importância da ReGIC no contexto

RFC 9116 - security.txt

TLP:CLEAR

Sua organização publica o security.txt?

www.gov.br/ctir/pt-br/well-known/security.txt

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

# Canonical URI
Canonical: https://www.gov.br/ctir/pt-br/security.txt

# Our security address
Contact: mailto:ctir@ctir.gov.br

# Our OpenPGP key
Encryption: https://www.gov.br/ctir/pt-br/media/ctir-site.asc

# List of preferred languages for security reports
Preferred-Languages: pt-br, en

# Date and time after which this file is considered stale
Expires: 2025-05-18T23:59:00z

# EOF
-----BEGIN PGP SIGNATURE-----

iQIzBAEBCgAdFiEEK77LSew61P5cTZ/5vQ8v8CIb/3gFAmSHXZMACgkQvQ8v8CIb
/3hRyQ/9HHnCaN31Bjinn7qn+tkgXi9mB0Mo5XWoR7AUV5F5UCSlPmULLLOPzV1P
2polgI8txuBrDkYvOgKgLeRRWPnuooxTvU/F6oGx3LLAKRoiiC12vqT2gS49taIO
I8mz2yJ2IaW1mnwFgiAT0aK8zx50mPZEPcRHWJoC8KAHAzBbO91C2sJDbPly4jnL
vpbc+2pVxKFmJTa7on+lSIGDJ8l8G+/bgcuNqkUgIt7xZOCT+KGaclZIODbX5W3v
G9REPTRoUztRn0VHaAHTtg8aVTnh0qjVHummV1e25tFZK8puHokhopZrELMNOgS6
34GXutB3PT5ix7tQvkdO8HprqqFNvElmm+HqfsSAKYpeqnIWFNDNLW0gJZB9yBAF
CEyJMIBZe9eIudxi28GGW/jg44Wu5GS2hpNvnQ7w+N0ov+FzcqJPSIY2ptjQLtPi
rmyN8KCpn0NVIVTCcTezYwu3hVCQQ5w0nv+5S01AIlZgompXGqOZ+N/wGfgT8lUj
u14jRXw5MCmMtpWE3Y4MY9gJs3HZvHVcaXsBEfYsAPTxikhmyqOFWzcmS8bFLAx+
7fAMt8JUT2H1V0fyjOLf9zp165uMOfDjPyY5IFDg1vNAKTczCOZyKoa4hTee04J1
VO/zyHXvXD3Z1TnTlg5oXnaKeYwIIjg67Tqbwu0cRzFldqyjLH0=
=r3hm
-----END PGP SIGNATURE-----
```

RFC 9116 - security.txt

TLP:CLEAR

Internet Engineering Task Force (IETF) E. Foudil
Request for Comments: 9116
Category: Informational Y. Shafranovich
ISSN: 2070-1721 Nightwatch Cybersecurity
April 2022

A File Format to Aid in Security Vulnerability Disclosure

Abstract

When security vulnerabilities are discovered by researchers, proper reporting channels are often lacking. As a result, vulnerabilities may be left unreported. This document defines a machine-parsable format ("security.txt") to help organizations describe their vulnerability disclosure practices to make it easier for researchers to report vulnerabilities.

https://www.rfc-editor.org/rfc/rfc9116

Criando um security.txt

TLP:CLEAR

Tyler Hall Tech's security.txt Generator

Create an security.txt file for your website

UThis tool is designed to help website administrators create a security.txt file, a proposed standard that enables websites to define their security policies clearly and concisely. The security.txt file makes it easier for security researchers to report security vulnerabilities.

https://tylerhalltech.com/security-txt-generator/

O CTIR Gov - RFC 2350

TLP:CLEAR

gov.br Gabinete de Segurança Institucional da Presidênci...

Órgãos do Governo | Acesso à Informação | Legislação | Acessibilidade | Entrar com o gov.br

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

O que você procura?

Assuntos > RFC 2350

RFC 2350

Descrição do CTIR Gov, de acordo com a RFC 2350 (também conhecida como BCP 21), incluindo informações de contato, missão, políticas e serviços.

Publicado em 24/03/2023 14h16 | Atualizado em 21/06/2024 14h38

Compartilhe:

RFC 2350 (English) | RFC 2350 (Português BR)

O CTIR Gov - RFC 2350

TLP:CLEAR

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

O que você procura?

3. Apresentação

3.1 Declaração da Missão

O Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) coordena respostas a incidentes de segurança cibernética relacionados a redes pertencentes aos membros da Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC).

3.2 Abrangência Operacional (Constituency)

Órgãos aderentes à Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC), instituída pelo Decreto 10.748, de 16 de julho de 2021.

3.3 Patrocínio e/ou Filiação

O CTIR Gov foi formalmente criado em 2006, por iniciativa do Governo Brasileiro por meio do Gabinete de Segurança Institucional (GSI). GSI é o gabinete executivo do governo federal do Brasil responsável pela política de segurança e defesa nacional. As atividades desempenhadas pelo CTIR Gov estão de acordo com as atribuições da Secretaria de Segurança da Informação e Cibernética do GSI (antigo Departamento de Segurança da Informação), conforme definido no Decreto Presidencial 10.748 [1], de 2021:

I - coordenar as atividades das equipes de prevenção, tratamento e resposta a incidentes cibernéticos do membros da Rede Federal de Gestão de Incidentes Cibernéticos (REGIC) relacionados à prevenção, tratamento e resposta a incidentes cibernéticos;

II - articular-se com as ETIR de Governo para prevenção, tratamento e resposta a que se refere o inciso I, utilizando plataforma computacional dedicada para coordená-las;

O CTIR Gov - RFC 2350

TLP:CLEAR

RECOMENDAÇÃO 03/2024

Utilização da RFC 2350 por Equipes de Tratamento de Incidentes de Redes

Publicado em 21/06/2024 15h53 | Atualizado em 25/07/2024 09h23

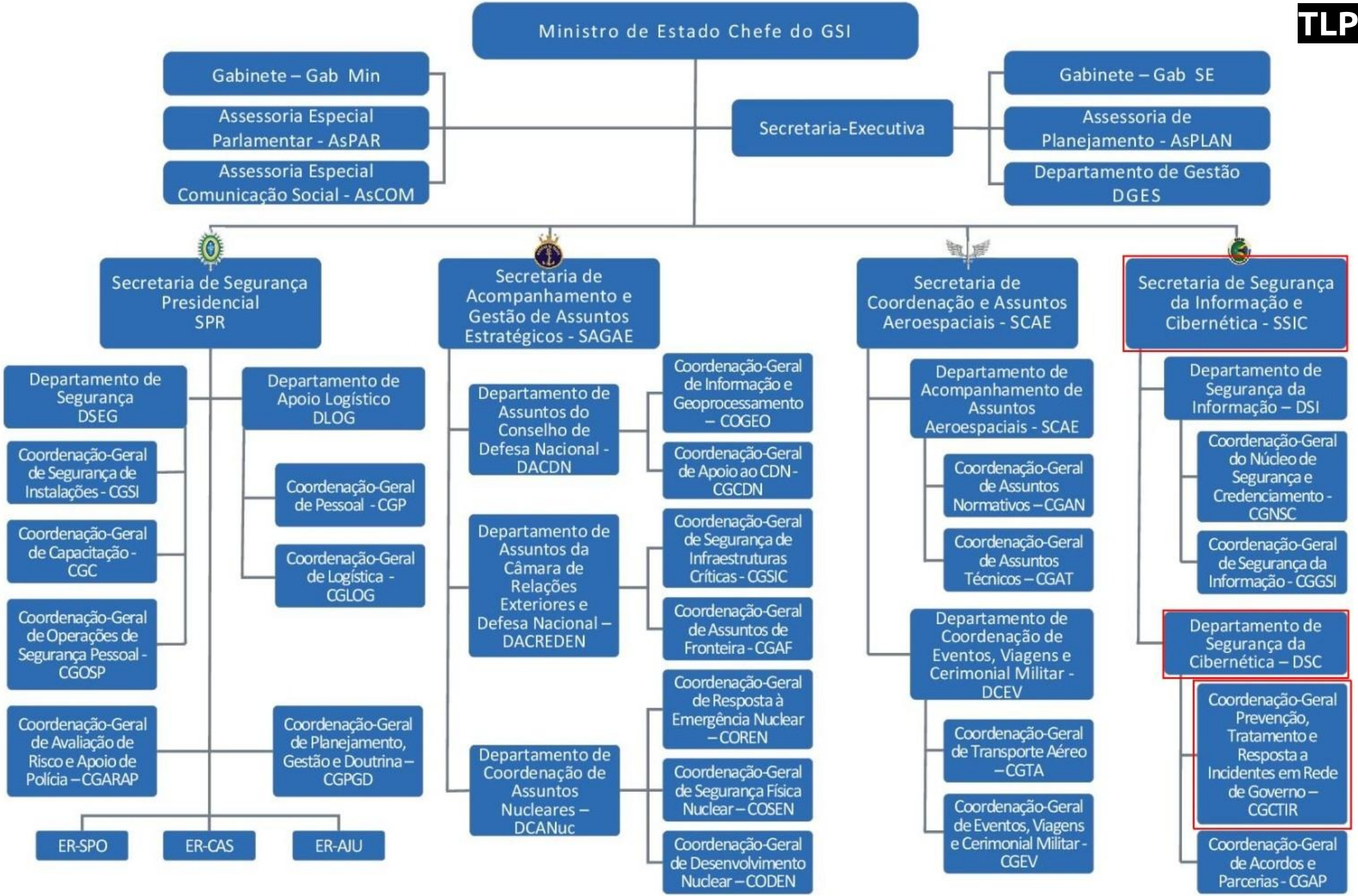
Compartilhe:

[TLP:CLEAR]

1. A Request for Comments (RFC) 2350 estabelece padrões para a descrição de Equipes de Tratamento e Resposta a Incidentes. O documento estabelece a forma como as Equipes devem apresentar suas informações e capacidades ao público e a outras entidades, conforme publicado em:

- https://datatracker.ietf.org/doc/html/rfc2350

2. O principal objetivo da RFC 2350 é definir um formato consistente para a documentação das operações, serviços e políticas das ETIR, disponibilizando informações sobre suas funções, tipos de incidentes que lidam, formas de contato e outros dados relevantes.


Ministro de Estado Chefe do GSI
Gabinete – Gab Min
Assessoria Especial Parlamentar - AsPAR
Assessoria Especial Comunicação Social - AsCOM
Secretaria-Executiva
Gabinete – Gab SE
Assessoria de Planejamento - AsPLAN
Departamento de Gestão DGES
Secretaria de Segurança Presidencial SPR
Departamento de Segurança DSEG
Coordenação-Geral de Segurança de Instalações - CGSI
Coordenação-Geral de Capacitação - CGC
Coordenação-Geral de Operações de Segurança Pessoal - CGOSP
Coordenação-Geral de Avaliação de Risco e Apoio de Polícia – CGARAP
Departamento de Apoio Logístico DLOG
Coordenação-Geral de Pessoal - CGP
Coordenação-Geral de Logística - CGLOG
Coordenação-Geral de Planejamento, Gestão e Doutrina – CGPGD
ER-SPO
ER-CAS
ER-AJU
Secretaria de Acompanhamento e Gestão de Assuntos Estratégicos - SAGAE
Departamento de Assuntos do Conselho de Defesa Nacional - DACDN
Coordenação-Geral de Informação e Geoprocessamento – COGEO
Coordenação-Geral de Apoio ao CDN - CGCDN
Departamento de Assuntos da Câmara de Relações Exteriores e Defesa Nacional – DACREDEN
Coordenação-Geral de Segurança de Infraestruturas Críticas - CGSIC
Coordenação-Geral de Assuntos de Fronteira - CGAF
Departamento de Coordenação de Assuntos Nucleares – DCANuc
Coordenação-Geral de Resposta à Emergência Nuclear – COREN
Coordenação-Geral de Segurança Física Nuclear – COSEN
Coordenação-Geral de Desenvolvimento Nuclear – CODEN
Secretaria de Coordenação e Assuntos Aeroespaciais - SCAE
Departamento de Acompanhamento de Assuntos Aeroespaciais - SCAE
Coordenação-Geral de Assuntos Normativos – CGAN
Coordenação-Geral de Assuntos Técnicos – CGAT
Departamento de Coordenação de Eventos, Viagens e Cerimonial Militar - DCEV
Coordenação-Geral de Transporte Aéreo – CGTA
Coordenação-Geral de Eventos, Viagens e Cerimonial Militar - CGEV
Secretaria de Segurança da Informação e Cibernética - SSIC
Departamento de Segurança da Informação – DSI
Coordenação-Geral do Núcleo de Segurança e Credenciamento - CGNSC
Coordenação-Geral de Segurança da Informação - CGGSI
Departamento de Segurança da Cibernética – DSC
Coordenação-Geral Prevenção, Tratamento e Resposta a Incidentes em Rede de Governo – CGCTIR
Coordenação-Geral de Acordos e Parcerias - CGAP

O CTIR Gov - Apoio ao processo decisório

TLP:CLEAR

1. Consciência situacional
2. Coordenação do tratamento de incidentes
3. Prevenção a incidentes
4. Apoio para a definição de normativos

Roteiro

TLP:CLEAR

CTIR Gov
01
RFC 2350
Constituency
Papel no GSI

ReGIC
02
Decreto
Objetivos e foco
Atividades

Processos e fontes de dados
03
Aquisição e processamento
Coordenação e compartilhamento

Prevenção
04
SSIC
Alertas e Recomendações
Mailing list

Parcerias
05
Parceiros nacionais e internacionais
Exemplos de parceria
Casos reais
Tendências e CTIR Gov em Números

Conclusão
06
Tempestividade
Proatividade
Importância da ReGIC no contexto

ReGIC - Decreto 10.748: Finalidade

TLP:CLEAR

DA REDE FEDERAL DE GESTÃO DE INCIDENTES CIBERNÉTICOS

Art. 1º Fica instituída a Rede Federal de Gestão de Incidentes Cibernéticos, nos termos do disposto no inciso VII do **caput** do art. 15 do Decreto nº 9.637, de 26 de dezembro de 2018.

§ 1º A participação dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional na Rede Federal de Gestão de Incidentes Cibernéticos será obrigatória.

§ 2º A participação das empresas públicas e das sociedades de economia mista federais e das suas subsidiárias na Rede Federal de Gestão de Incidentes Cibernéticos será voluntária e ocorrerá por meio de adesão.

§ 3º A Secretaria de Governo Digital da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia participará da Rede Federal de Gestão de Incidentes Cibernéticos na condição de órgão central do Sistema de Administração dos Recursos de Tecnologia da Informação - Sisp do Poder Executivo federal.

Art. 2º A Rede Federal de Gestão de Incidentes Cibernéticos tem por finalidade aprimorar e manter a coordenação entre órgãos e entidades da administração pública federal direta, autárquica e fundacional para prevenção, tratamento e resposta a incidentes cibernéticos, de modo a elevar o nível de resiliência em segurança cibernética de seus ativos de informação.

Rede Federal de Gestão de Incidentes Cibernéticos - Objetivos

TLP:CLEAR

01

Divulgar

Medidas de prevenção

02

Compartilhar

Alertas, Recomendações

03

Alertar

Informações de ataques

04

Incentivar

Trabalho cooperativo

05

Promover

Celeridade e tempestividade

Elevar o nível de resiliência em Segurança Cibernética

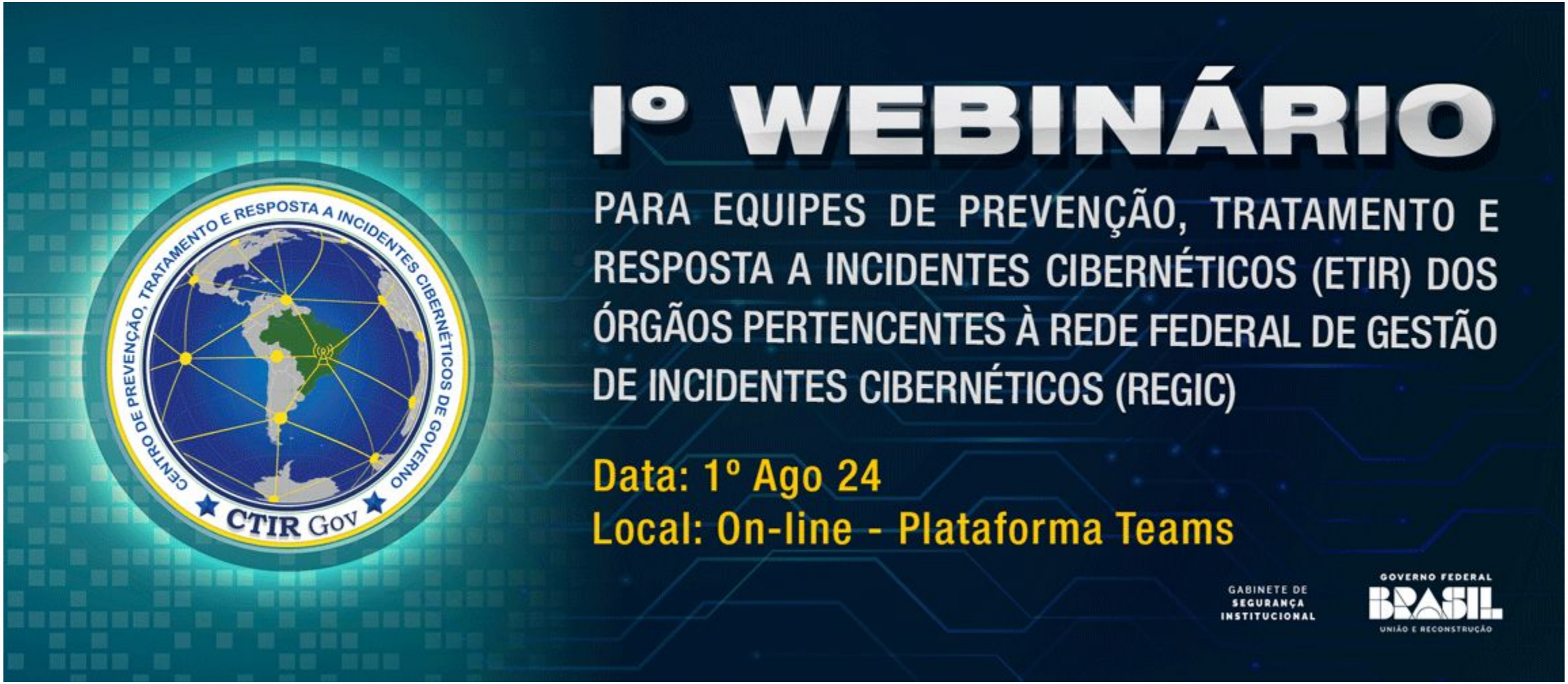
Rede Federal de Gestão de Incidentes Cibernéticos - Foco

TLP:CLEAR

Melhorar a coordenação ampliando o trabalho colaborativo

Evento on-line

TLP:CLEAR



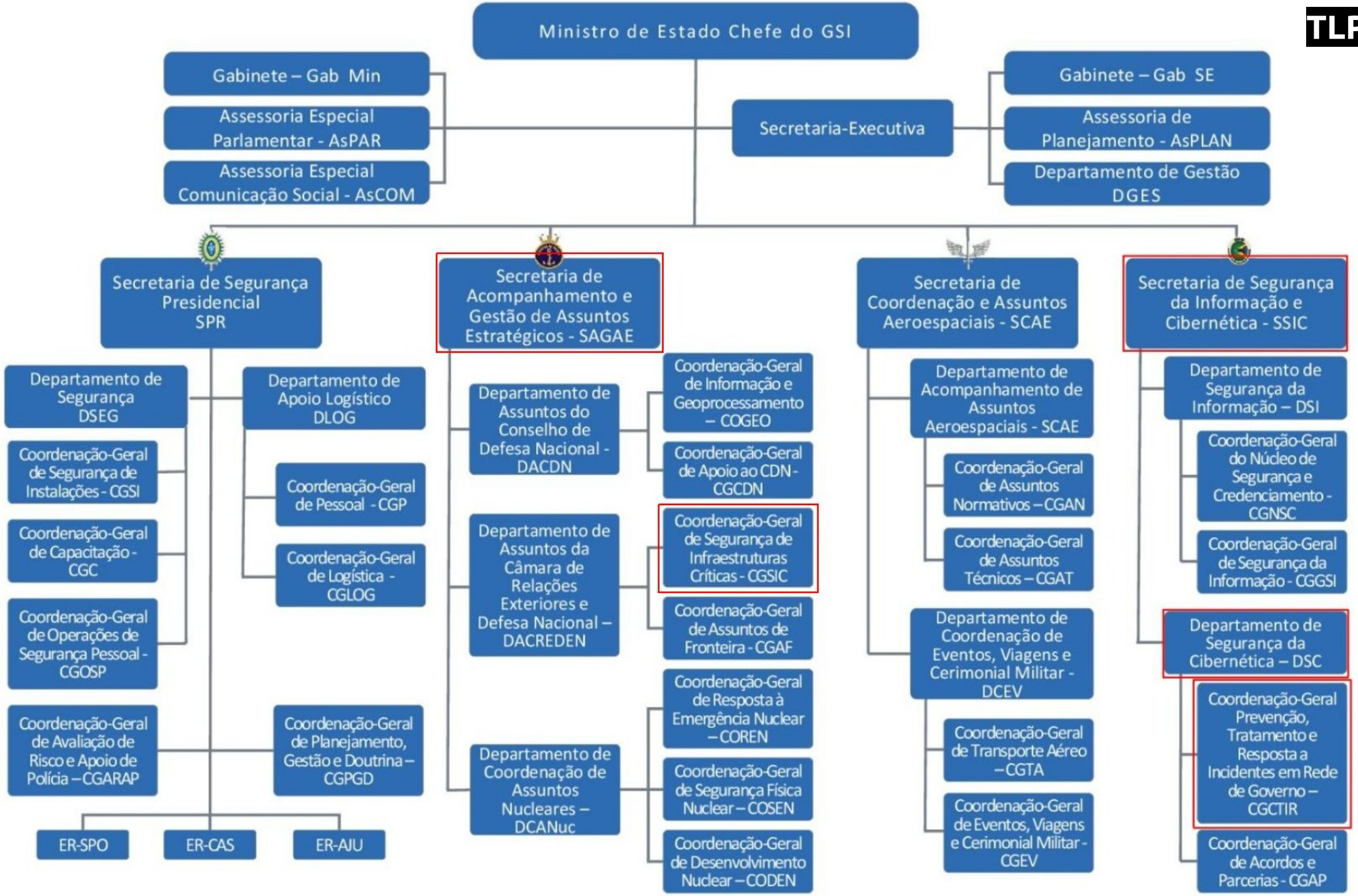
Caravanas Federativas

TLP:CLEAR

Gabinete de Segurança Institucional

O que você procura?

Neste sentido, a SSIC por meio do CTIR Gov realizou atendimentos aos representantes de instituições e municípios do estado do Rio de Janeiro e apresentou, além da estrutura da Secretaria, a Rede Federal de Gestão de Incidentes Cibernéticos - REGIC, destacando a importância do envolvimento e da adesão à REGIC das três esferas governamentais bem como instituições de outros Poderes e entidades de relevância estratégica.


Ministro de Estado Chefe do GSI
Gabinete – Gab Min
Assessoria Especial Parlamentar - AsPAR
Assessoria Especial Comunicação Social - AsCOM
Secretaria-Executiva
Gabinete – Gab SE
Assessoria de Planejamento - AsPLAN
Departamento de Gestão DGES
Secretaria de Segurança Presidencial SPR
Departamento de Segurança DSEG
Coordenação-Geral de Segurança de Instalações - CGSI
Coordenação-Geral de Capacitação - CGC
Coordenação-Geral de Operações de Segurança Pessoal - CGOSP
Coordenação-Geral de Avaliação de Risco e Apoio de Polícia – CGARAP
Departamento de Apoio Logístico DLOG
Coordenação-Geral de Pessoal - CGP
Coordenação-Geral de Logística - CGLOG
Coordenação-Geral de Planejamento, Gestão e Doutrina – CGPGD
ER-SPO
ER-CAS
ER-AJU
Secretaria de Acompanhamento e Gestão de Assuntos Estratégicos - SAGAE
Departamento de Assuntos do Conselho de Defesa Nacional - DACDN
Coordenação-Geral de Informação e Geoprocessamento – COGEO
Coordenação-Geral de Apoio ao CDN - CGCDN
Departamento de Assuntos da Câmara de Relações Exteriores e Defesa Nacional – DACREDEN
Coordenação-Geral de Segurança de Infraestruturas Críticas - CGSIC
Coordenação-Geral de Assuntos de Fronteira - CGAF
Departamento de Coordenação de Assuntos Nucleares – DCANuc
Coordenação-Geral de Resposta à Emergência Nuclear – COREN
Coordenação-Geral de Segurança Física Nuclear – COSEN
Coordenação-Geral de Desenvolvimento Nuclear – CODEN
Secretaria de Coordenação e Assuntos Aeroespaciais - SCAE
Departamento de Acompanhamento de Assuntos Aeroespaciais - SCAE
Coordenação-Geral de Assuntos Normativos – CGAN
Coordenação-Geral de Assuntos Técnicos – CGAT
Departamento de Coordenação de Eventos, Viagens e Cerimonial Militar - DCEV
Coordenação-Geral de Transporte Aéreo – CGTA
Coordenação-Geral de Eventos, Viagens e Cerimonial Militar - CGEV
Secretaria de Segurança da Informação e Cibernética - SSIC
Departamento de Segurança da Informação – DSI
Coordenação-Geral do Núcleo de Segurança e Credenciamento - CGNSC
Coordenação-Geral de Segurança da Informação - CGGSI
Departamento de Segurança da Cibernética – DSC
Coordenação-Geral Prevenção, Tratamento e Resposta a Incidentes em Rede de Governo – CGCTIR
Coordenação-Geral de Acordos e Parcerias - CGAP

Programa Ascender Defesas

TLP:CLEAR

Histórico de Incidentes

TLP:CLEAR

Rússia	Austrália	China	Alemanha	Arábia Saudita	Índia	Brasil
Phishing	Spear-Phishing	DDoS	Phishing	DDoS	DDoS	?
Interceptação	Hacktivismo		Malware		Defacement	
Malware			Ciberespionagem		Hacktivismo	

Apoio ao G20 - Infraestruturas Críticas

TLP:CLEAR

Gabinete de Segurança Institucional

O que você procura?

GSI/PR atua na segurança de Infraestruturas Críticas durante o G20

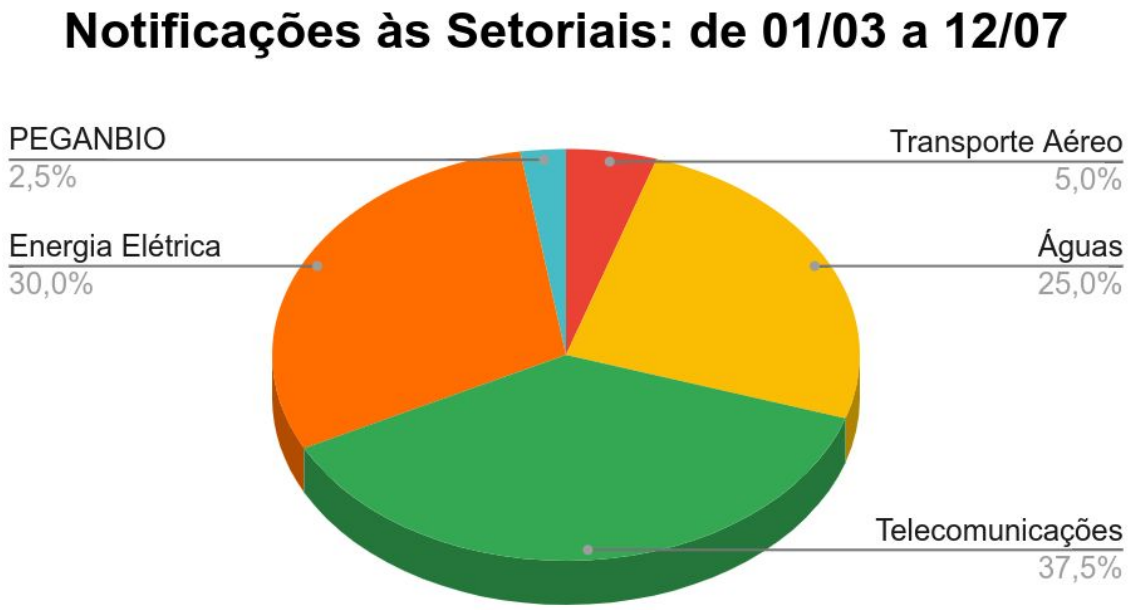
Evento ocorreu dias 25, 26 e 27 de junho em Maceió/AL

Publicado em 27/06/2024 14h24 | Atualizado em 27/06/2024 14h48

Compartilhe:

Prevenção no contexto do G20

TLP:CLEAR



Roteiro

TLP:CLEAR

CTIR Gov
01
RFC 2350
Constituency
Papel no GSI

ReGIC
02
Decreto
Objetivos e foco
Atividades

Processos e fontes de dados
03
Aquisição e processamento
Coordenação e compartilhamento

Prevenção
04
SSIC
Alertas e Recomendações
Mailing list

Parcerias
05
Parceiros nacionais e internacionais
Exemplos de parceria
Casos reais
Tendências e CTIR Gov em Números

Conclusão
06
Tempestividade
Proatividade
Importância da ReGIC no contexto

Processo de aquisição de dados

TLP:CLEAR

Agências Internacionais

IoC's, Alertas...

CSIRTs Nacionais e Internacionais

Notificações, Feeds, MISP...

Fóruns Internacionais

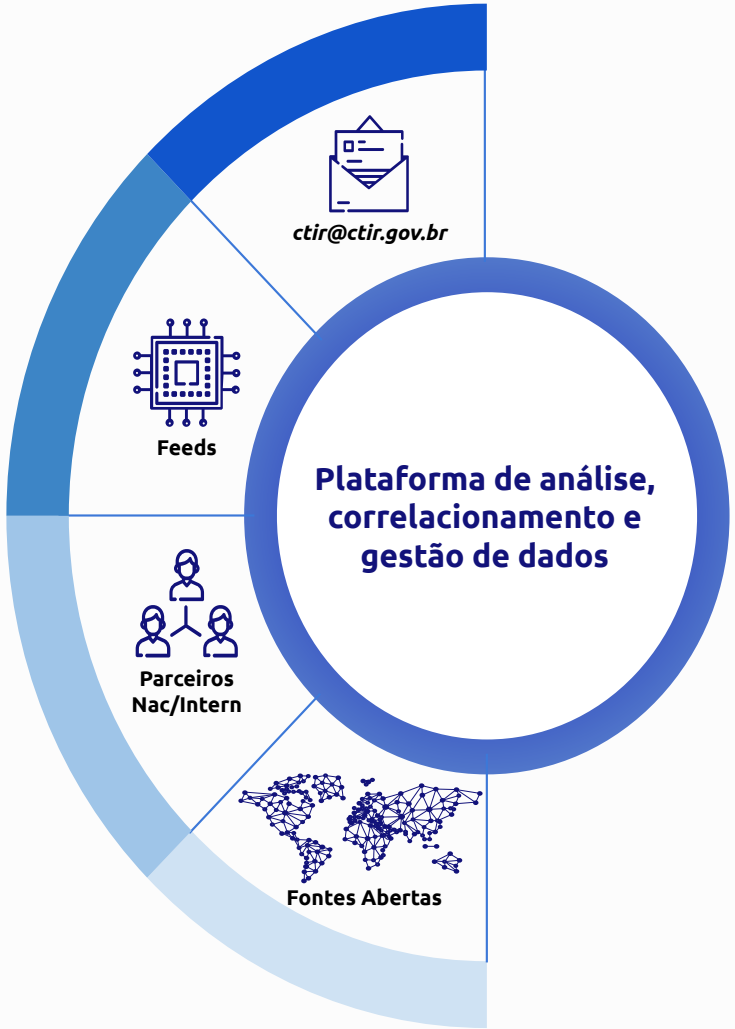
Feeds...

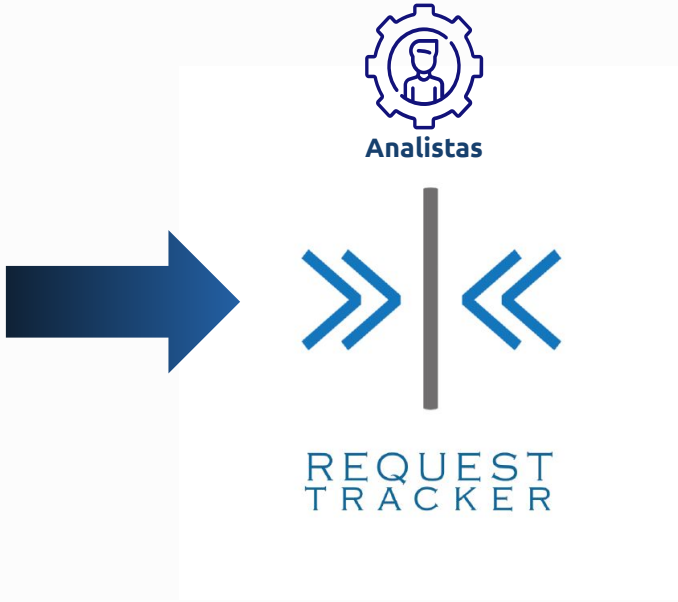
Colaboradores

Notificações...

Processamento de dados e criação de notificações

TLP:CLEAR





[CTIR Gov BR #XXXX]
[TLP:AMBER] NOTIFICAÇÃO

Coordenação

TLP:CLEAR

Processo de coordenação e compartilhamento de dados

TLP:CLEAR

Roteiro

TLP:CLEAR

CTIR Gov
01
RFC 2350
Constituency
Papel no GSI

ReGIC
02
Decreto
Objetivos e foco
Atividades

Processos e fontes de dados
03
Aquisição e processamento
Coordenação e compartilhamento

Prevenção
04
SSIC
Alertas e Recomendações
Mailing list

Parcerias
05
Parceiros nacionais e internacionais
Exemplos de parceria
Casos reais
Tendências e CTIR Gov em Números

Conclusão
06
Tempestividade
Proatividade
Importância da ReGIC no contexto

Secretaria de Segurança da Informação e Cibernética - Publicações

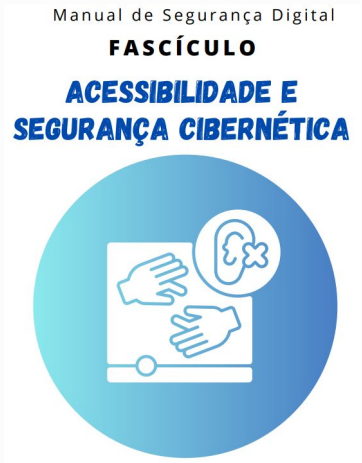
TLP:CLEAR

Gabinete de Segurança Institucional

O que você procura?

SSIC - Fascículos

TLP:CLEAR



CTIR Gov - Alertas e Recomendações

TLP:CLEAR

gov.br Gabinete de Segurança Institucional da Presidênci... Órgãos do Governo Acesso à Informação Legislação Acessibilidade Entrar com o gov.br

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

O que você procura?

Assuntos > Alertas e Recomendações

Alertas e Recomendações

Alertas

Recomendações

Mais recentes publicações

TLP:CLEAR

ALERTA 01/2024 — última modificação 12/01/2024 13h58
Vulnerabilidades críticas em produtos Volexity Ivanti

ALERTA 02/2024 — última modificação 02/02/2024 17h28
Atualizações sobre vulnerabilidades em produtos Volexity Ivanti

ALERTA 03/2024 — última modificação 08/03/2024 17h47
Vulnerabilidades críticas no software Jenkins

ALERTA 04/2024 — última modificação 16/03/2024 15h11
Aplicativos maliciosos com temática "IRPF"

ALERTA 05/2024 — última modificação 03/04/2024 09h10
Vulnerabilidade crítica na ferramenta XZ

ALERTA 06/2024 — última modificação 12/04/2024 11h21
Vulnerabilidade no Sistema Operacional Palo Alto Networks (PAN-OS)

ALERTA 07/2024 — última modificação 19/04/2024 19h52
Aumento de casos de vazamentos de credenciais de acesso a sistemas de governo

ALERTA 08/2024 — última modificação 04/06/2024 10h29
Vulnerabilidade no Check Point Security Gateway

ALERTA 09/2024 — última modificação 01/07/2024 16h12
Vulnerabilidade crítica no OpenSSH

ALERTA 10/2024 — última modificação 25/07/2024 10h17
Falha em atualização de produto CrowdStrike

RECOMENDAÇÃO 01/2024 — última modificação 26/03/2024 17h42
Relatório sobre ataques de negação de serviço (DoS e DDoS)

RECOMENDAÇÃO 02/2024 — última modificação 20/06/2024 17h12
Informações sobre o Ransomware Black Basta

RECOMENDAÇÃO 03/2024 — última modificação 25/07/2024 09h23
Utilização da RFC 2350 por Equipes de Tratamento de Incidentes de Redes

RECOMENDAÇÃO 04/2024 — última modificação 25/07/2024 15h34
Configuração de controles recomendados pelas boas práticas para serviços Web, E-mail e DNS.

ETIR-Gov - Mailing list

TLP:CLEAR

ETIR-GOV -- Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo

Sobre ETIR-GOV

Ver esta página em Português (Brasil)

Esta lista de discussão é destinada a membros de Equipes de Tratamento de Incidentes de Redes – ETIR.
Por meio dela serão disponibilizadas informações referentes a prevenção a incidentes cibernéticos de interesse da Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC), sob coordenação do Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo - CTIR Gov.

Para ver a coleção de postagens anteriores a lista, visite os arquivos da ETIR-GOV . (*O arquivo atual somente está disponível para os membros da lista.*)

Usando ETIR-GOV

Para postar uma mensagem a todos os membros da lista, envie um email para etir-gov@listas.planalto.gov.br.

Você poderá se inscrever na lista ou modificar sua inscrição existente, nas seções abaixo.

Inscrevendo-se na ETIR-GOV

Inscreva-se na lista ETIR-GOV preenchendo o seguinte formulário. Você receberá uma mensagem de confirmação de inscrição, para prevenir que outros o inscrevam sem sua permissão. Uma vez que a confirmação for recebida, sua requisição será posta para aprovação pelo moderador da lista. Você será notificado da decisão do moderador por email. Esta é também uma lista oculta, que significa que a lista de membros está somente disponível para o administrador da lista.

Seu endereço de email:	
Seu nome (opcional):	

Você poderá entrar com uma senha privativa abaixo. Isto oferece somente uma segurança média, mas deve prevenir outras pessoas de obter sua inscrição. **Não utilize uma senha válida** pois ela provavelmente será lhe encaminhada de volta em formato texto plano.

Caso tenha escolhido não entrar com uma senha, uma senha será gerada automaticamente para você, e lhe será enviada assim que confirmar sua inscrição. Você pode sempre requisitar um reenvio de sua senha quando editar suas opções pessoais.

Selecione uma senha:	
Reentre com a senha para confirmar:	
EM que idiomas prefere exibir suas mensagens?	Português (Brasil)
Deseja receber e-mails da lista enviados uma vez por dia em um único email (digest)?	Não Sim

Inscrever

https://www1.planalto.gov.br/mailman/listinfo/etir-gov

Roteiro

TLP:CLEAR

CTIR Gov
01
RFC 2350
Constituency
Papel no GSI

ReGIC
02
Decreto
Objetivos e foco
Atividades

Processos e fontes de dados
03
Aquisição e processamento
Coordenação e compartilhamento

Prevenção
04
SSIC
Alertas e Recomendações
Mailing list

Parcerias
05
Parceiros nacionais e internacionais
Exemplos de parceria
Casos reais
Tendências e CTIR Gov em Números

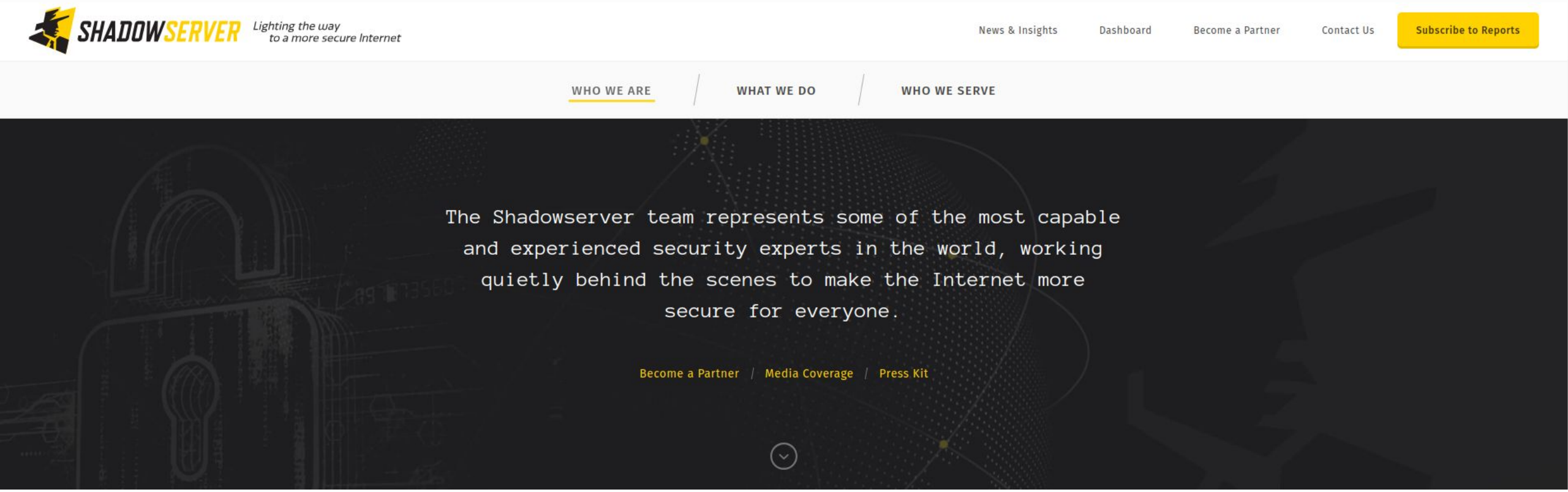
Conclusão
06
Tempestividade
Proatividade
Importância da ReGIC no contexto

Parceiros Nacionais e Internacionais

TLP:CLEAR

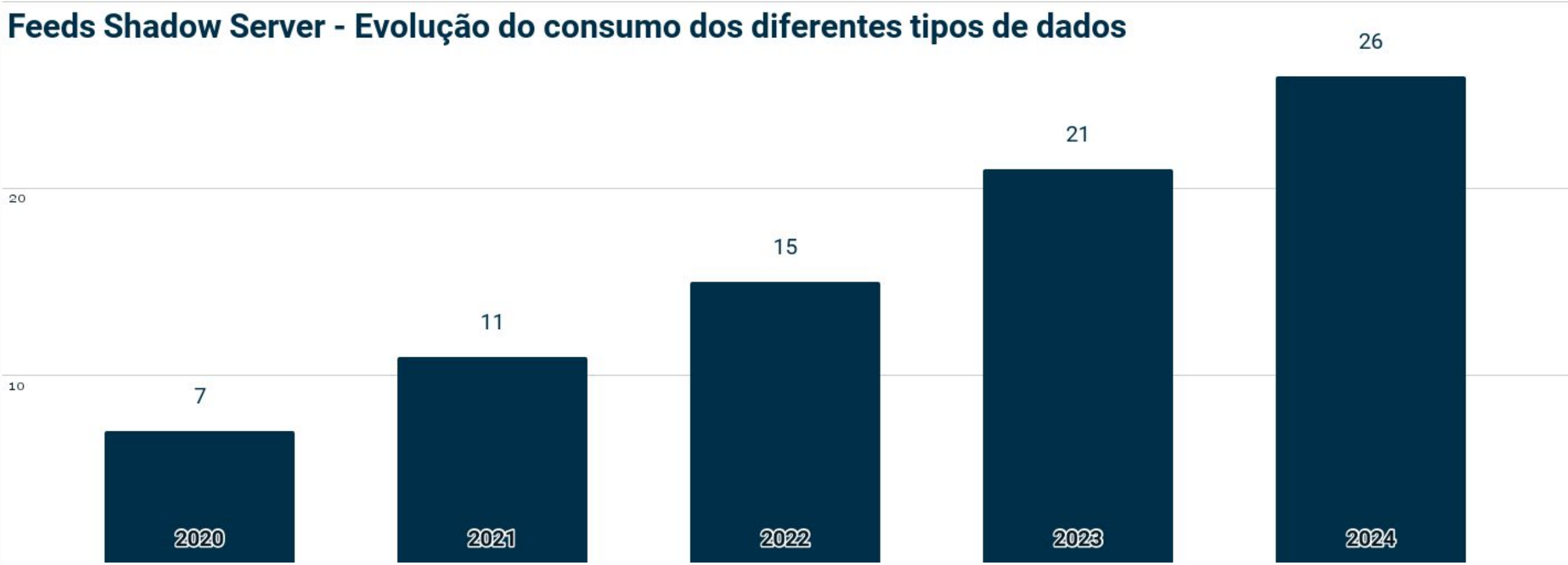
Dados para ações de prevenção

TLP:CLEAR



Aumento do consumo de feeds - Impacto e utilização

TLP:CLEAR



Rede de CSIRTS de Governo dos Estados Membros da Organização dos Estados Americanos (OEA)

CSIRTAmericas Network acts as the main promoter of the Cybersecurity Program of the **Inter-American Committee against Terrorism (CICTE)** of the **Organization of American States (OAS)** in strengthening the capacities of CSIRTs in the region to respond to cyber incidents, and has the support of:

OAS | More rights for more people

Canada

CSIRTAmericas Network

Contact | Disclaimer | Partners

Membros

TLP:CLEAR

OEA | OAS | CSIRTAmericas Network

Community Services Resources Log in EN

Members

- Argentina
- Barbados
- Bolivia
- Brazil
- The Bahamas
- Canada
- Chile
- Colombia
- Costa Rica
- Dominican Republic
- Ecuador
- Guatemala
- Guyana
- Jamaica
- Mexico
- Panama
- Peru
- Paraguay
- Suriname
- Trinidad and Tobago
- United States of America
- Uruguay

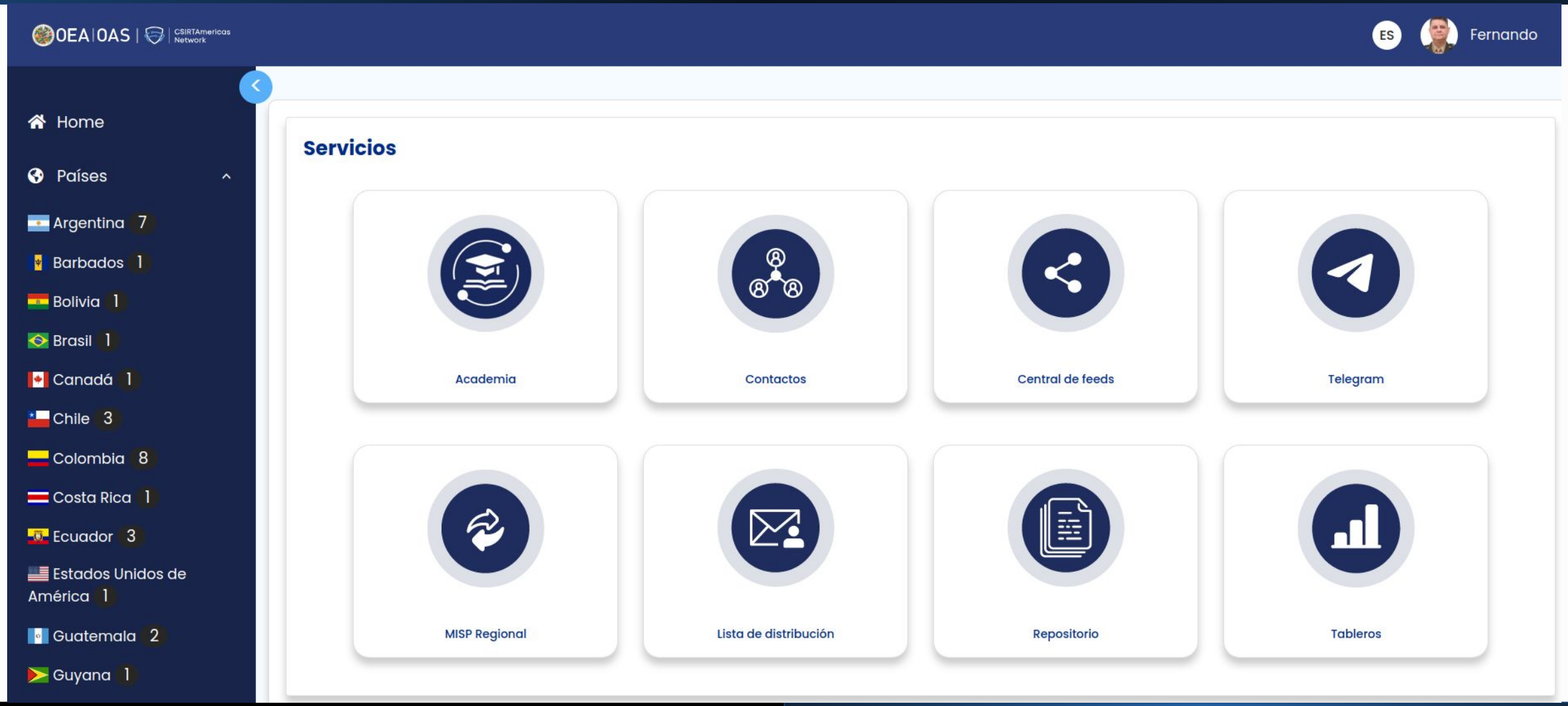
445 Specialists

50 CSIRTs

22 Countries

Recursos

TLP:CLEAR

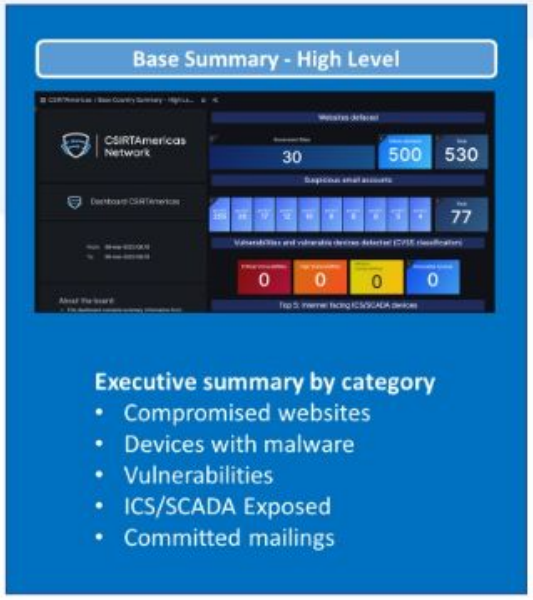


Visibilidade e consciência situacional

TLP:CLEAR

OEA CICTE | CSIRTAmericas Network

Executive dashboard



Executive summary by category

- Compromised websites
- Devices with malware
- Vulnerabilities
- ICS/SCADA Exposed
- Committed mailings

Operating dashboards

Defacement

Websites compromised by defacement attack.

Malicious Communications

Devices compromised with malware.

Vulnerabilities

Devices with vulnerabilities

Spam

Compromise of email accounts / servers

Critical Infrastructure

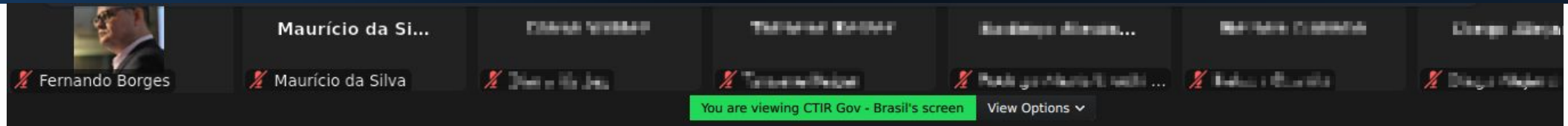
ICS/SCADA exposed to the Internet

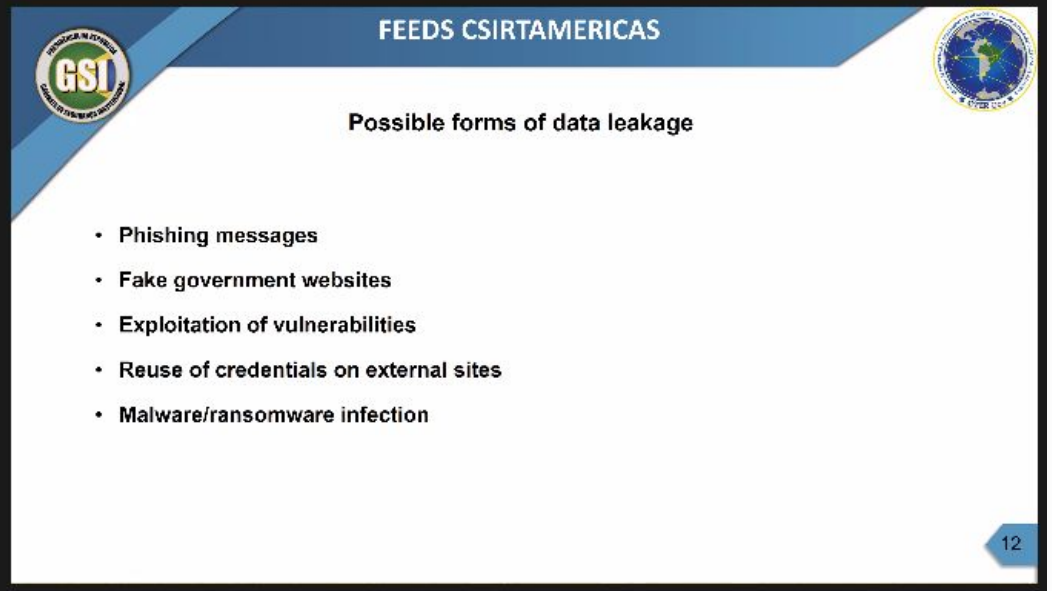
Initiative with financial support from:

UK Government

Caso de uso de dados do *CSIRTAmericas*

TLP:CLEAR

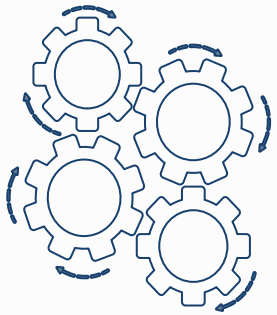




Processamento do feed *CSIRTAmericas*

TLP:CLEAR

Feed Credentials

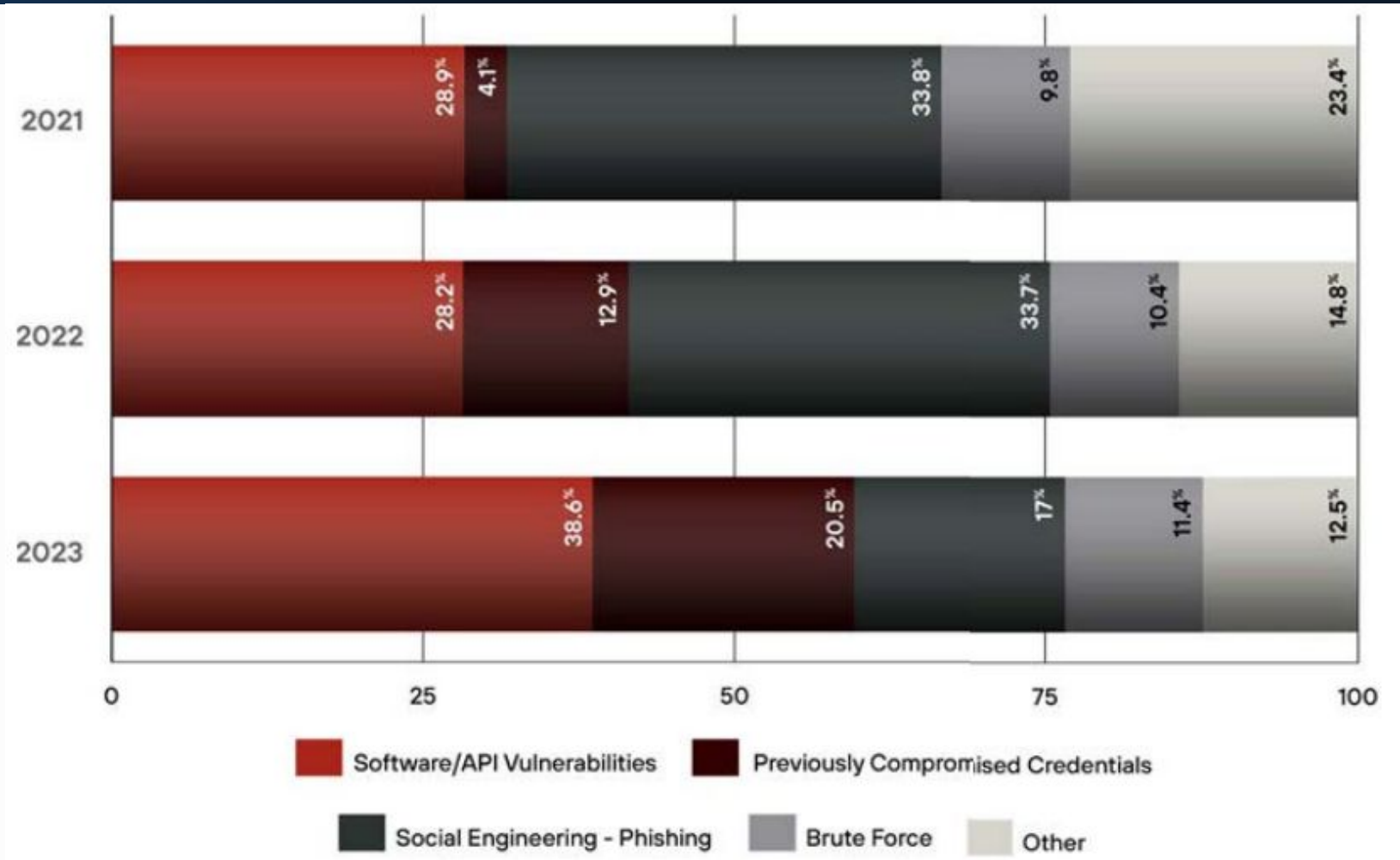


[CTIR Gov BR #XXXX]
[TLP:AMBER] Possível comprometimento de credenciais [xxx.gov.br]

Controle de repetições
Armazenamento do login
Agrupamento por domínios e subdomínios
Definição do melhor contato para notificação (ReGIC)

Vetor inicial de acesso

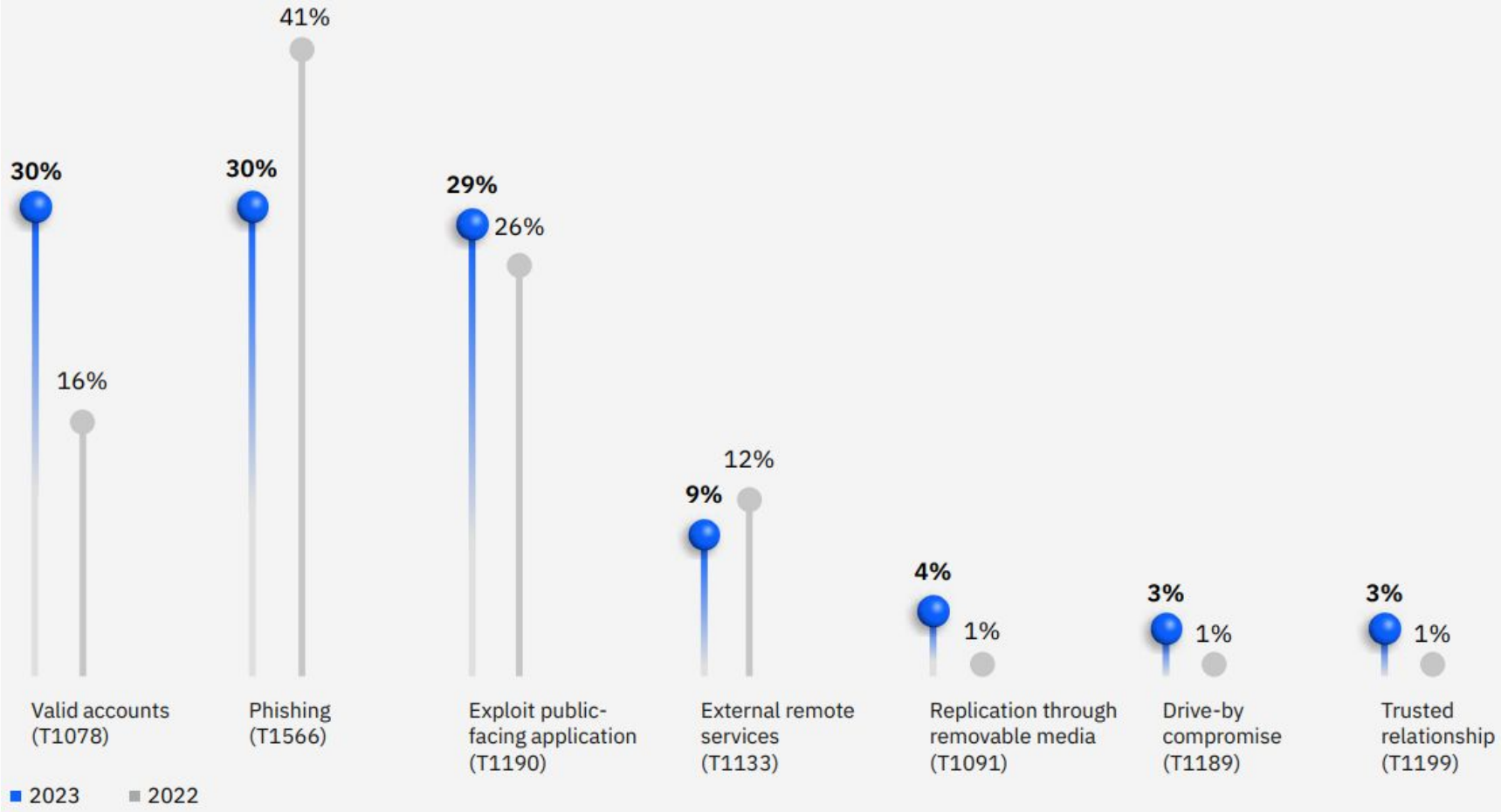
TLP:CLEAR



PaloAlto Incident Response Report 2024

Ataques com acesso inicial por contas válidas

TLP:CLEAR



IBM X-Force Threat Intelligence Index 2024

Múltiplo fator de autenticação

TLP:CLEAR

MFA não é uma panaceia! Mas...

A combinação de aplicação de updates, controle de credenciais, MFA e segmentação de rede evitaria mais de 80% dos ataques graves notificados ao CTIR Gov.

Alerta sobre o assunto

TLP:CLEAR

ALERTA 07/2024

Aumento de casos de vazamentos de credenciais de acesso a sistemas de governo

Publicado em 19/04/2024 19h52

Compartilhe:

[TLP:CLEAR]

1. O Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Governo (CTIR Gov), colaborativamente com o Centro Integrado de Segurança Cibernética do Governo Digital (CISC Gov.Br), tem verificado a tendência de aumento do número de credenciais válidas comercializadas de modo ilícito, com o objetivo de possibilitar acesso indevido e, como consequência, permitir outras ações maliciosas como disseminação de phishing, malwares, movimentação lateral e ataques de maior proporção, como Ransomware, por exemplo.

2. Ainda em 2023 foi publicada a Recomendação 02/2023, versando sobre "Credenciais de acesso como vetor de incidentes cibernéticos às infraestruturas de Governo", disponível em:

- https://www.gov.br/ctir/pt-br/assuntos/alertas-e-recomendacoes/recomendacoes/2023/recomendacao-02-2023

3. Atacantes têm empregado diferentes técnicas para obter credenciais de acesso válidas. Dentre elas, cabe citar: phishing, engenharia social, keyloggers e monitoramento de tráfego de rede. Diversas campanhas de obtenção de credenciais visando órgãos governamentais tem sido identificadas, impondo a necessidade de execução de medidas proativas de segurança cibernética para mitigar os riscos de explorações bem-sucedidas.

Estatísticas e tendências

TLP:CLEAR

gov.br Gabinete de Segurança Institucional da Presidênci... Órgãos do Governo Acesso à Informação Legislação Acessibilidade Entrar com o gov.br

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

O que você procura?

Assuntos > CTIR Gov Em Números

Estatísticas resultantes do trabalho de detecção, triagem, análise e resposta a incidentes cibernéticos

(Última atualização: 01 de julho de 2024)

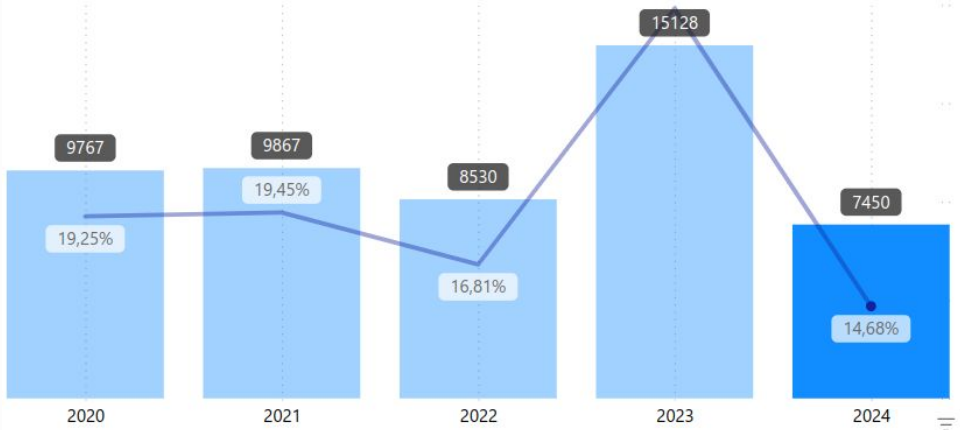
Um dos serviços providos pelo CTIR Gov consiste na disponibilização das estatísticas resultantes do trabalho de detecção, triagem, análise e resposta a incidentes cibernéticos.

O **CTIR Gov "Em Números"** é uma iniciativa criada com o objetivo de disponibilizar estatísticas gerais de interesse público relacionadas aos incidentes cibernéticos de governo, em um ambiente que simplifica o acesso e compreensão dos dados, utilizando-se de relatórios interativos e uma interface visual mais amigável.

O ambiente está em constante evolução e tem como meta tornar-se a principal referência de informações relativas à gestão de incidentes cibernéticos do Governo do Brasil. Suas informações podem ser utilizadas também para determinar tendências e padrões de atividades de ataques e para recomendar estratégias de prevenção adequadas.

Estatísticas e tendências

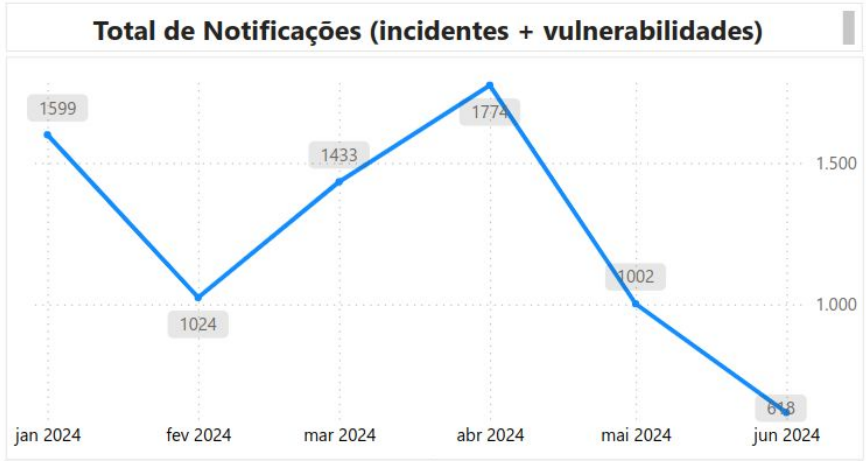
TLP:CLEAR

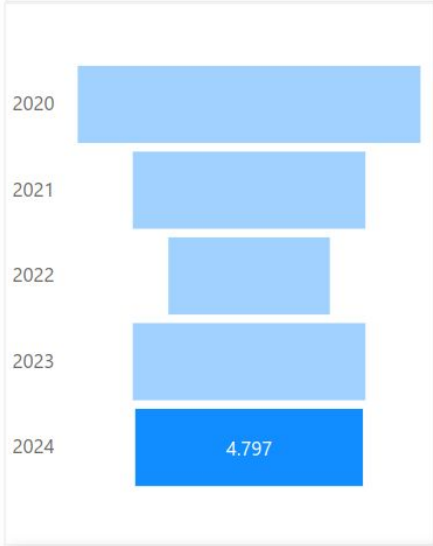


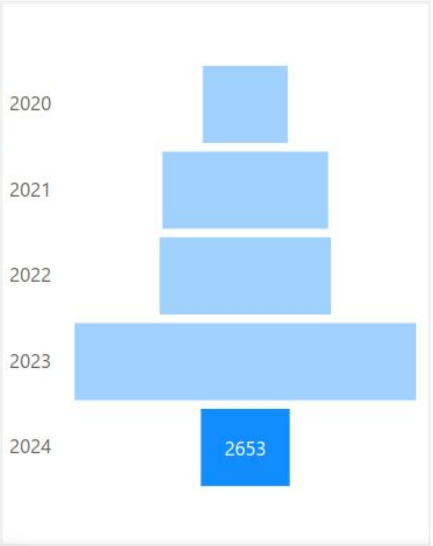
Ano	Vulnerabilidades	Incidentes	Total
2024	2653	4797	7450
Total	**2653**	**4797**	**7450**

Mês	Vulnerabilidades	Incidentes	Total
janeiro	546	1053	1599
fevereiro	447	577	1024
março	429	1004	1433
abril	514	1260	1774
maio	404	598	1002
junho	313	305	618
Total	**2653**	**4797**	**7450**

Trimestre	Vulnerabilidades	Incidentes	Total
Trim 1	1422	2634	4056
Trim 2	1231	2163	3394
Total	**2653**	**4797**	**7450**







Roteiro

TLP:CLEAR

01 CTIR Gov

RFC 2350
Constituency
Papel no GSI

02 ReGIC

Decreto
Objetivos e foco
Atividades

03 Processos e fontes de dados

Aquisição e processamento
Coordenação e compartilhamento

04 Prevenção

SSIC
Alertas e Recomendações
Mailing list

05 Parcerias

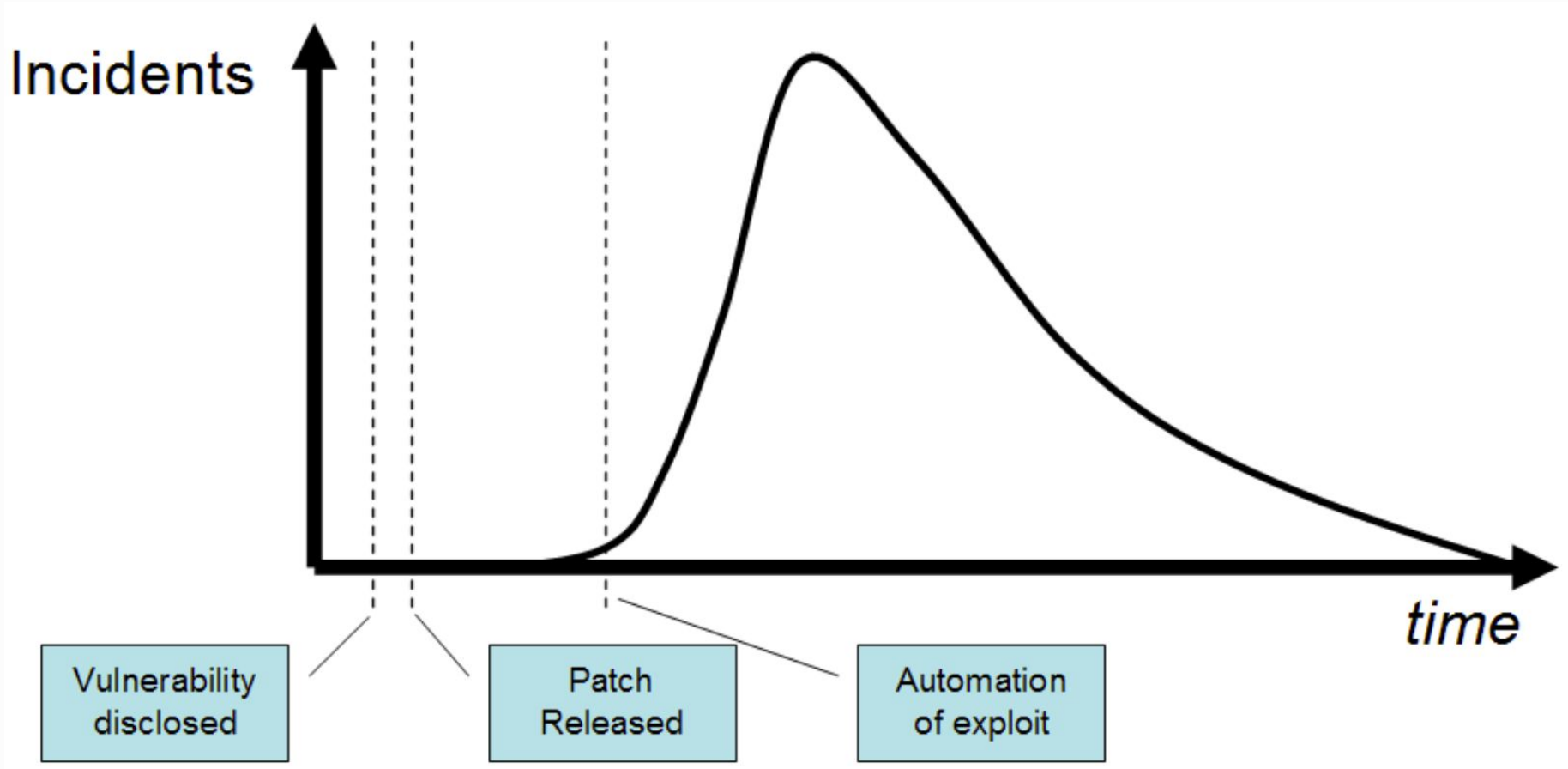
Parceiros nacionais e internacionais
Exemplos de parceria
Casos reais
Tendências e CTIR Gov em Números

06 Conclusão

Tempestividade
Proatividade
Importância da ReGIC no contexto

Janela de tempo...

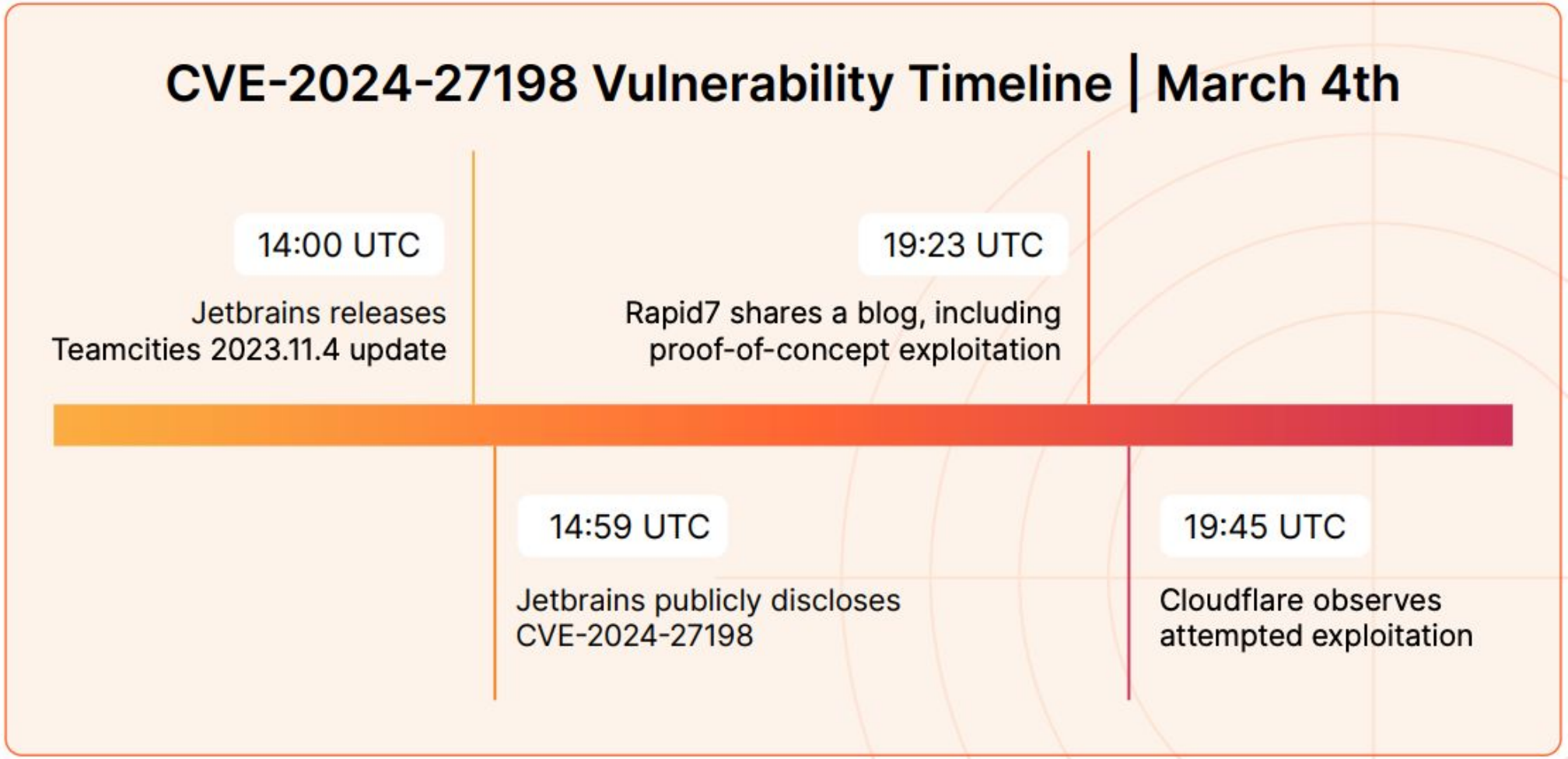
TLP:CLEAR



Effectiveness of Proactive CSIRT Services

Cada vez mais estreita!

TLP:CLEAR



2024 Cloudflare Application Security Report

Importância da coordenação e prevenção

TLP:CLEAR

Proatividade: Construção de uma cultura de segurança com a ReGIC

Tempestividade: Redução do tempo de exposição e do dano potencial

Trabalho Colaborativo: Compartilhamento de informações, dados e boas práticas

Obrigado!

TLP:CLEAR

https://www.gov.br/ctir

ctir@ctir.gov.br

fernando.borges@presidencia.gov.br