



2º WEBINÁRIO

PARA EQUIPES DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS (ETIR) DOS ÓRGÃOS PERTENCENTES À REDE FEDERAL DE GESTÃO DE INCIDENTES CIBERNÉTICOS (REGIC)

Data: 3 Set 24
Local: On-line - Plataforma Teams

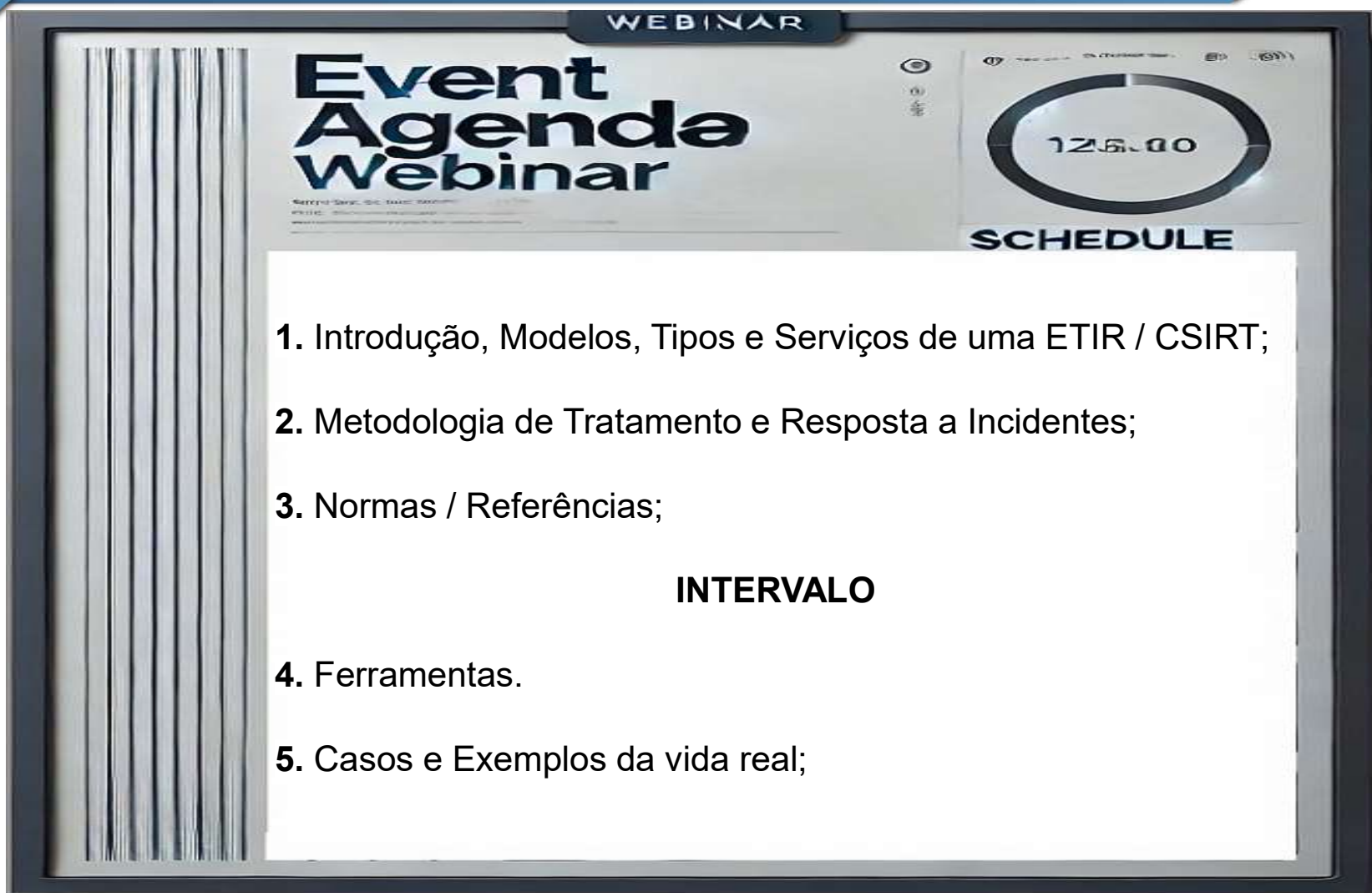
2º Webinar
Sessões virtuais para as ETIRs pertencentes à ReGIC

CABINETE DE SEGURANÇA INSTITUCIONAL

GOVERNO FEDERAL
BRASIL
UNIÃO E RECONSTRUÇÃO

Maurício Leite Ferreira
Analista de Incidentes

2º WEBINAR – CTIR Gov 2024



WEBINAR

Event Agenda Webinar

125.00
SCHEDULE

1. Introdução, Modelos, Tipos e Serviços de uma ETIR / CSIRT;
2. Metodologia de Tratamento e Resposta a Incidentes;
3. Normas / Referências;

INTERVALO

4. Ferramentas.
5. Casos e Exemplos da vida real;

ETIR / CSIRT

TLP: CLEAR

Grupo de agentes com a responsabilidade de prestar serviços relacionados à segurança cibernética para o órgão ou a entidade, em observância à política de segurança da informação e aos processos de gestão de riscos de segurança da informação do órgão ou da entidade.

A principal função dessas equipes é: prevenir, identificar, analisar, mitigar e resolver os incidentes de maneira eficaz para minimizar impactos e restaurar a normalidade o mais rápido possível.



TLP: CLEAR

MODELOS DE ETIRs / CSIRTs

Modelo 1 – Utilizando a equipe de Tecnologia da Informação – TI:

Não existirá um grupo dedicado exclusivamente. A Equipe será formada a partir dos membros das equipes de TI do próprio órgão ou entidade.

Modelo 2 – Centralizado:

A Equipe será estabelecida de forma centralizada no âmbito da organização e será composta por pessoal com dedicação exclusiva às atividades de tratamento e resposta aos incidentes em redes computacionais.

Modelo 3 – Descentralizado:

A Equipe será composta por colaboradores distribuídos por diversos locais dentro da Organização, podendo atuar operacionalmente de forma independente, porém alinhadas com as diretrizes estabelecidas pela coordenação central.

Modelo 4 – Combinado ou Misto:

Trata-se da junção dos modelos Descentralizado e Centralizado, neste modelo existirá uma Equipe central e Equipes distribuídas pela organização.



TLP: CLEAR

TIPOS DE ETIRs / CSIRTs

CSIRTs Corporativos ou Privados:

São equipes especializadas que atuam dentro de organizações privadas ou empresas.

CSIRTs Governamentais:

Operam no âmbito de entidades governamentais e estão focados em proteger a infraestrutura crítica do estado.

CSIRTs Nacionais:

São equipes de resposta a incidentes que operam a nível nacional e coordenam esforços entre o setor público e privado para proteger a segurança cibernética do país.

CSIRTs Regionais:

Focados em uma região geográfica específica, podem ser parte de uma rede mais ampla de CSIRTs nacionais.

CSIRTs Setoriais:

Especializados em setores específicos, como finanças, saúde ou energia.



TLP: CLEAR

TIPOS DE ETIRs / CSIRTs

CSIRTs Acadêmicos ou de Pesquisa:

Operam no âmbito acadêmico ou de pesquisa.

Investigam ameaças emergentes, desenvolvem novas ferramentas e técnicas para segurança e colaboram com outras instituições acadêmicas e de pesquisa.

CSIRTs Internacionais:

Trabalham a nível global e facilitam a cooperação entre diferentes CSIRTs e organizações internacionais.

Facilitam a colaboração transnacional, compartilham inteligência sobre ameaças e coordenar respostas a incidentes internacionais.

PSIRTs: (Product Security Incident Response Team) é um grupo dentro de uma organização, geralmente uma empresa de tecnologia ou de software, responsável por gerenciar e responder a incidentes de segurança relacionados a seus produtos.

OT CSIRTs: (Operational Technology Computer Security Incident Response Team) respondem a incidentes de segurança cibernética relacionados a sistemas de tecnologia operacional (OT).



TLP: CLEAR

PROPÓSITO DO CSIRT

CSIRTs Operacionais, internos de uma organização: Ex. CSIRT BB, Telefônica;

CSIRTs de Coordenação, coordenam outros CSIRTs: Ex: CTIR Gov, CAIS/RNP, ComDCiber ;

CSIRTs de Responsabilidade nacional, respondem pelo País: Ex: CERT.br, CTIR Gov.

TLP: CLEAR

CSIRTs com Responsabilidade Nacional



Fonte: www.first.org



TLP: CLEAR

NORMAS COMPLEMENTARES E DECRETO

NC 5 - CRIAÇÃO DE EQUIPES DE TRATAMENTO E RESPOSTA A INCIDENTES EM REDES COMPUTACIONAIS – ETIR:

<https://www.gov.br/gsi/pt-br/ssic/legislacao/NC05.pdf>

NC 8 - GESTÃO DE ETIR: DIRETRIZES PARA GERENCIAMENTO DE INCIDENTES EM REDES COMPUTACIONAIS NOS ÓRGÃOS E ENTIDADES DA ADMINISTRAÇÃO PÚBLICA FEDERAL:

<https://www.gov.br/gsi/pt-br/ssic/legislacao/NC08.pdf>

NC 21 - DIRETRIZES PARA O REGISTRO DE EVENTOS, COLETA E PRESERVAÇÃO DE EVIDÊNCIAS DE INCIDENTES DE SEGURANÇA EM REDES :

<https://www.gov.br/gsi/pt-br/ssic/legislacao/NC21.pdf>

REGIC :

O Decreto n.º 10.748, de 16 de julho de 2021, instituiu a Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC).

O objetivo da ReGIC é fortalecer a cooperação e a parceria entre o governo federal e os entes federativos, e sensibilizar os órgãos e a população em geral.

<https://www.in.gov.br/en/web/dou/-/decreto-n-10.748-de-16-de-julho-de-2021-332610022>

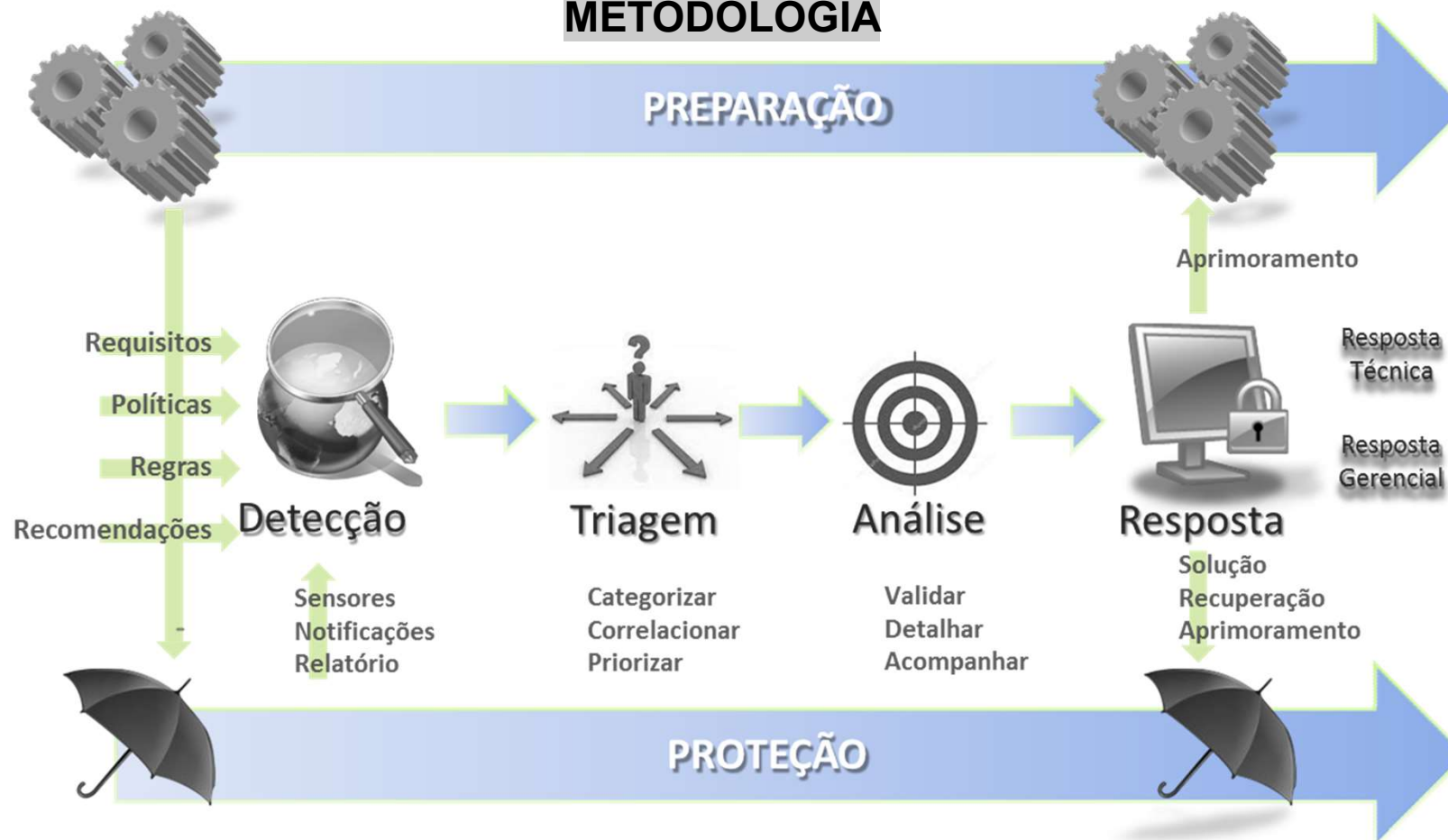


RFC 2350
Descrição do CSIRT, de acordo com a RFC 2350 (também conhecida como BCP 21), incluindo informações de contato, missão, políticas e serviços.

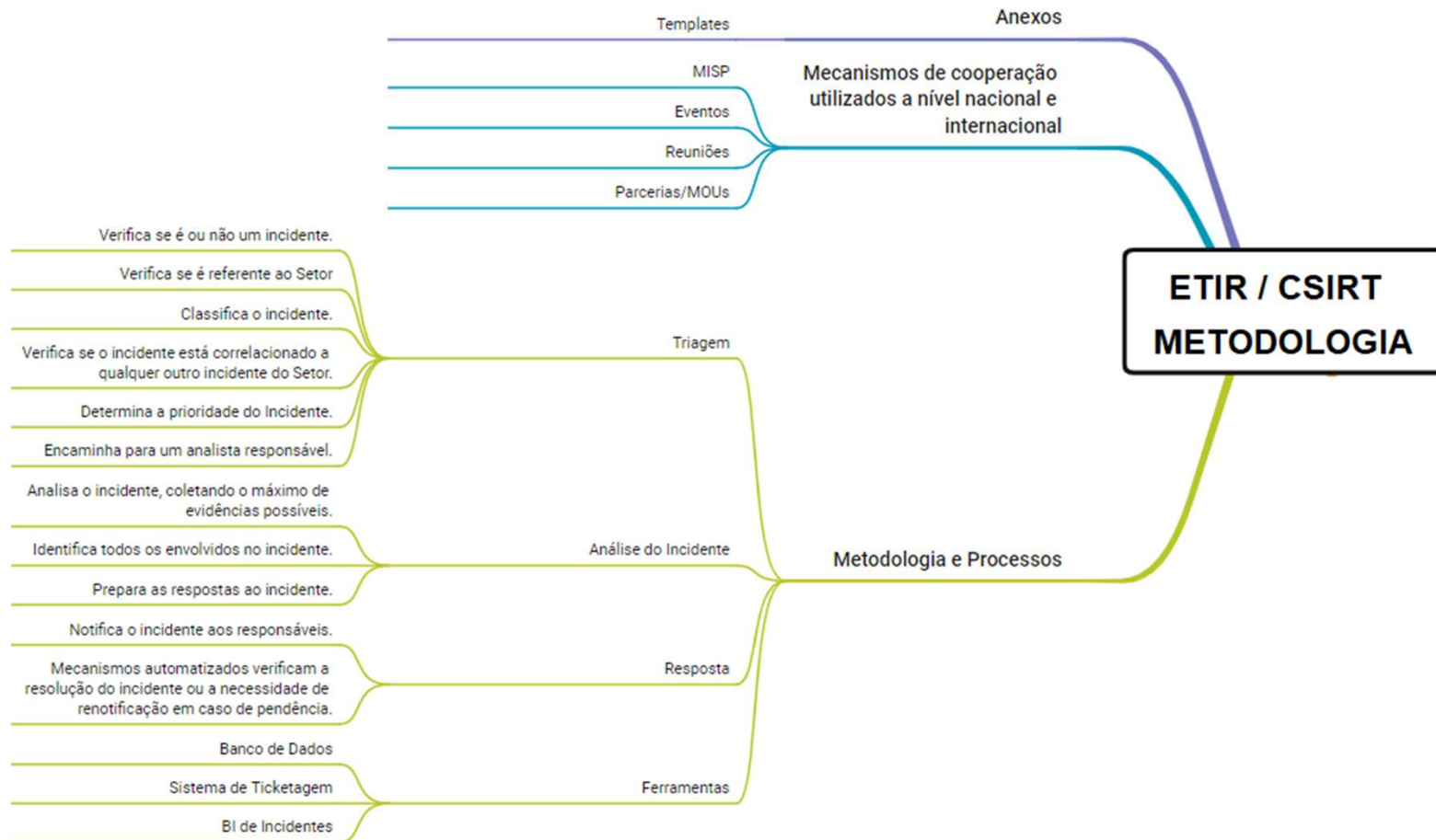


TLP: CLEAR

METODOLOGIA



TLP: CLEAR



TLP: CLEAR



2º WEBINAR – CTIR Gov 2024

TLP: CLEAR FERRAMENTAS



Log Collection: Representa a coleta de logs de diversas fontes para monitoramento contínuo dos sistemas de TI e identificação de atividades suspeitas ou anômalas.

Reporting: Envolve a criação de relatórios que documentam incidentes, desempenho e métricas de segurança. Isso é essencial para fornecer informações úteis à gestão e para o aprimoramento de estratégias de segurança.

Research & Development: Foco em pesquisa e desenvolvimento para inovar e melhorar as tecnologias e metodologias de segurança, adaptando-se a novas ameaças.

Threat Intelligence: Coleta e análise de informações sobre ameaças para entender as táticas, técnicas e procedimentos (TTPs) dos atacantes e assim melhorar a detecção e resposta a incidentes.

Knowledge Base: Manutenção de uma base de conhecimento que inclui procedimentos, documentação de incidentes anteriores e outras informações úteis para a operação do SOC.

Ticketing: Sistema de gestão de tickets para rastrear e gerenciar incidentes de segurança, garantindo que todos os problemas sejam endereçados de maneira ordenada.

SIEM (Security Information and Event Management): Integração e análise em tempo real de eventos de segurança para detectar e responder rapidamente a incidentes.

Aggregation/Correlation: Ação de agregar e correlacionar dados de múltiplas fontes para identificar padrões que possam indicar ameaças de segurança.

Destacando que todas essas atividades convergem para o SOC e que cada um desses elementos trabalha de forma integrada para fortalecer a postura de segurança cibernética da organização, possibilitando uma resposta rápida e eficaz a incidentes de segurança.


2º WEBINAR – CTIR Gov 2024

TLP: CLEAR

Issue Tracking System - Request Tracker (RT)

“Issue Tracking Systems (ITS) são sistemas destinados a controlar e registrar o andamento de cada atividade desenvolvida por uma dada equipe.”

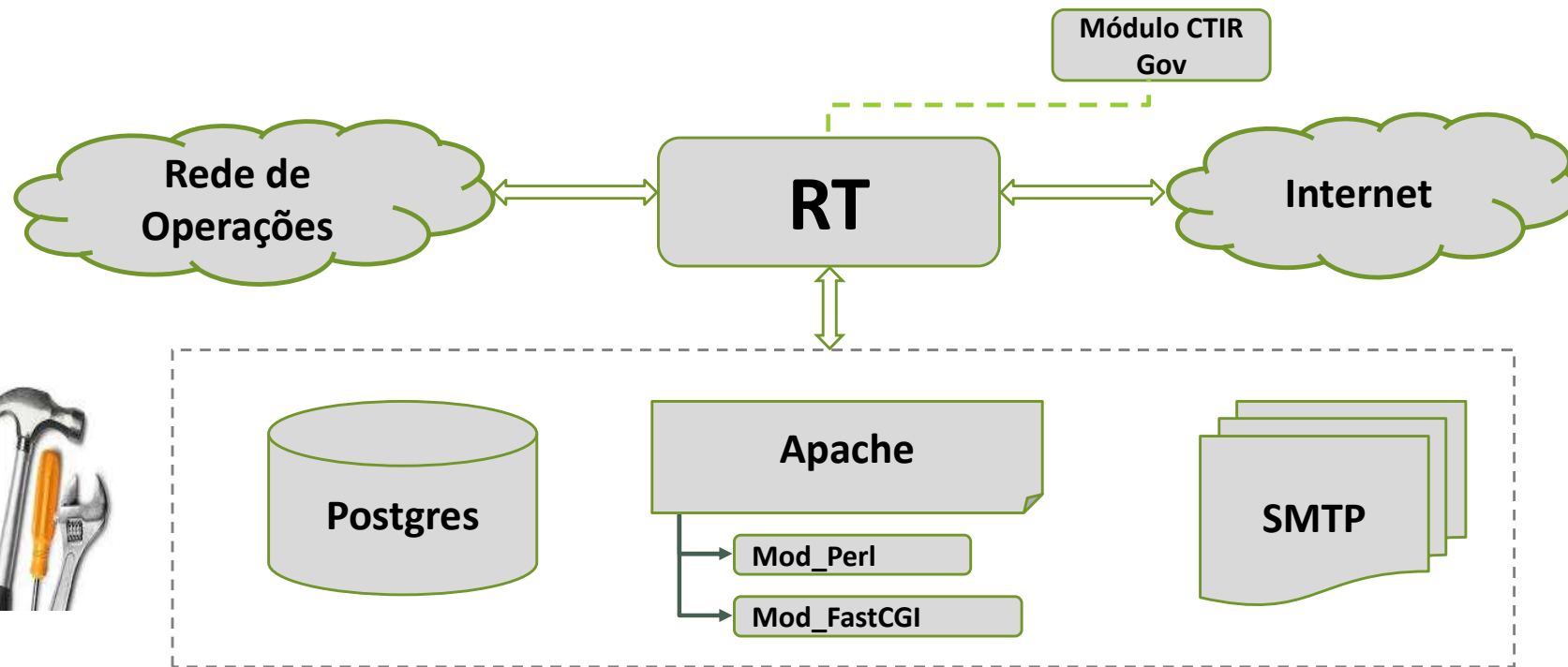
Destinam-se principalmente a:

- 
- Registrar um evento (notificação);
 - Atribuir um responsável pela atividade;
 - Determinar as partes envolvidas; e
 - Rastrear as mudanças ocorridas.

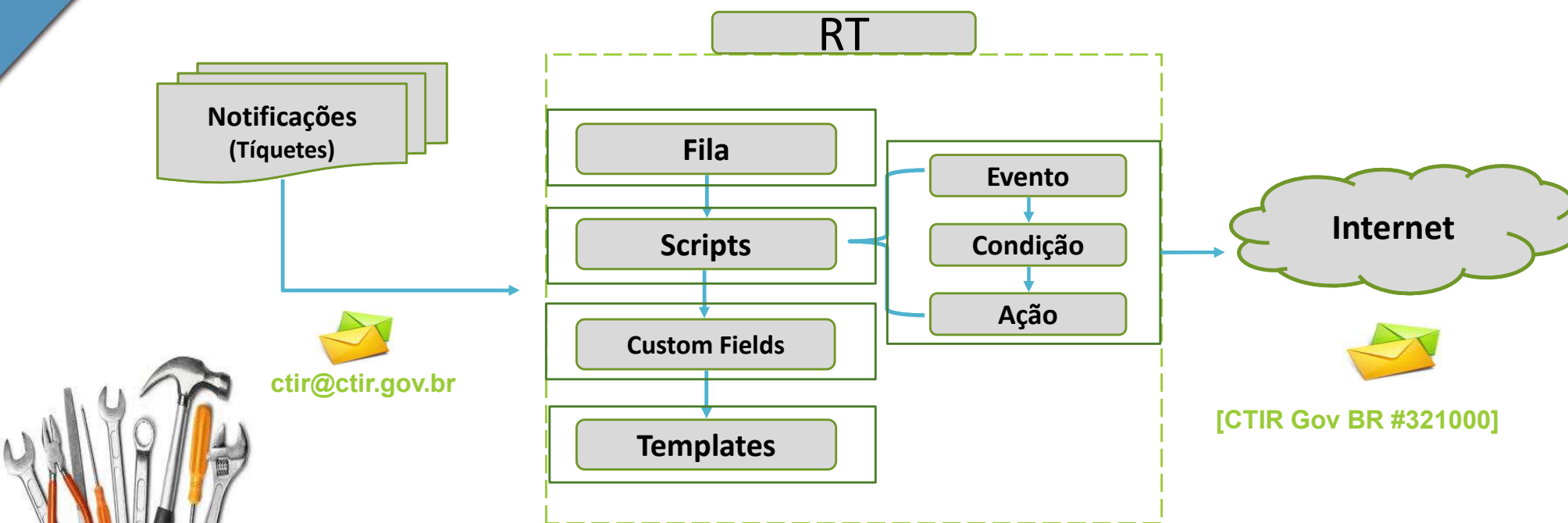
No contexto de uma ETIR:

- Automatizar e padronizar etapas;
- Criar modelos de notificação;
- Aumentar a produtividade; e
- Reduzir erros nas notificações.

TLP: CLEAR



TLP: CLEAR



TLP: CLEAR

sex., 14 de jan. de 2022 18:36:57 echo (Fernando Borges) - Correspondência adicionada Copiar Responder Comentar Reencaminhar

[TLP:GREEN] Baixar (sem título) / com cabeçalhos text/plain 3.4KIB

Prezados,

1. Informamos que o(s) endereço(s) IP/Domínio(s) listado(s) abaixo, está(ão) configurado(s) como "servidor DNS recursivo aberto":

.....
8.197.74
.....

2. Um servidor DNS recursivo é considerado aberto quando aceita consultas recursivas de modo indiscriminado, de qualquer rede. Essa falha de configuração permite que terceiros utilizem o(s) referido(s) servidor(es) para ataques de negação de serviço.

2.1 Recomendações, dicas de configuração e maiores detalhes sobre o ataque podem ser encontradas em:

.....
<http://www.cert.br/docs/whitepapers/dns-recursivo-aberto>
<https://labs.opendns.com/2014/03/17/dns-amplification-attacks/>
.....

3. Solicitamos que o problema seja verificado com urgência e que sejam realizados os ajustes de configuração necessários.

3.1 Você pode verificar se o seu servidor está respondendo recursivamente no sítio abaixo, o qual faz parte de um projeto que reúne instituições de ensino e pesquisa da Holanda. Um botão verde ("Geen reactie van server via IPv4") indica que seu DNS está configurado corretamente:

.....
<http://www.openresolver.nl/>
.....

6. Caso este tipo de problema não seja de sua responsabilidade, solicitamos que esta mensagem seja encaminhada aos responsáveis por tal tarefa.

7. Solicitamos que referências futuras a esta notificação preservem o "Assunto" desta mensagem.

Colocamo-nos à disposição para auxiliá-los no que for necessário.

--
Atenciosamente,

Equipe CTIR Gov <ctir@ctir.gov.br>
www.ctir.gov.br
INOC-DBA (VOIP): 266031*800

--
O Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo - CTIR Gov, subordinado ao Departamento de Segurança da Informação - DSI, do Gabinete de Segurança Institucional da Presidência da República, tem como finalidade atender aos incidentes de segurança de redes computacionais do governo (domínios gov.br, jus.br, leg.br, mil.br, mp.br, def.br e tc.br).

CTIR Gov [312601]



TLP: CLEAR

^ 300 tíquetes de mais alta prioridade que eu possuo

Editar

# Assunto	Prioridade	Fila	Estado
321068 Re: Abuse from 131.72.....52	101	Alert	novo
321115 Atividade Suspeita/Maliciosa [redacted df.gov.br 131.....52]	101	Scan	aberto
321345 [TLP:WHITE] Malware Analysis of LAPSUS\$ Hacking Group	10	General	aberto
322156 [TLP:AMBER] Trickbot IOCs 31 Março - 04 Abril	10	IOCs e TTPs	aberto
321868 Site falso	10	General	aberto
319016 Re: [TLP:RED] Government site access credentials obtained via Stealer malware [GSEG5 #2069]	10	General	novo
318635 Re: [TLP:RED] Government site access credentials obtained via Stealer malware [GSEG5 #2069]	10	Administration	aberto
318636 Re: [TLP:RED] Government site access credentials obtained via Stealer malware [GSEG5 #2069]	10	Administration	novo
319673 Re: [TLP:RED] Government site access credentials obtained via Stealer malware [GSEG5 #2069]	10	General	novo
321604 Fake Website [redacted webmail@... cloudapp.azure.com 20.....96]	10	Phishing_Site	aberto
316203 Conta utilizada em campanhas de phishing	10	General	aberto
322302 BRICS CERT Cyber Security Online Seminar	10	General	aberto
321578 [TLP:GREEN] Problema de postmaster com o contato etir@... gov.br	0	Administration	aberto
322296 Tickets do periodo de 2022-04-06 22:00:00 ate o dia 2022-04-07 22:00:00	0	Administration	aberto
317636 E-mails do Coordenador do CTIR Gov	0	Administration	novo



TLP: CLEAR

[README](#) [Code of conduct](#) [AGPL-3.0 license](#) [Security](#)



[chat on discord](#) [Build status](#) [license AGPL-3.0](#)

TheHive is a scalable 3-in-1 open source and free Security Incident Response Platform designed to make life easier for SOCs, CSIRTs, CERTs and any information security practitioner dealing with security incidents that need to be investigated and acted upon swiftly. It is the perfect companion to [MISP](#). You can synchronize it with one or multiple MISP instances to start investigations out of MISP events. You can also export an investigation's results as a MISP event to help your peers detect and react to attacks you've dealt with. Additionally, when TheHive is used in conjunction with [Cortex](#), security analysts and researchers can easily analyze tens if not hundred of observables.

Title	Severity	Tasks	Observables	Assignee	Date	Actions
#34 - [MALSPAM] Malspam 2016-10-06 (.js in .zip) - campaign: "Your Order"	High	5 Tasks	824	[Avatar]	03/20/19 10:56	[Icons]
#27 - [CTI] [Vulnerability] This is a case created from a template	High	5 Tasks	3	[Avatar]	02/28/19 14:55	[Icons]
#24 - [MISP] #3329 OSINT - ASERT Threat Intelligence Report 2016-03 The Four-Element Sword Engagement	High	5 Tasks	53	[Avatar]	02/09/17 12:03	[Icons]





Home » Tecnologia » Ferramentas » Whois

Whois

ctir.gov.br



[Exibir resultado completo](#)

Copyright © NIC.br

A utilização dos dados abaixo é permitida somente conforme descrito na Política de Privacidade, sendo proibida a sua distribuição, comercialização ou reprodução, em particular para fins publicitários ou propósitos similares.
2024-08-20 14:35:26 -03:00 - IP: 170.246.252.4

Domínio **ctir.gov.br**

TITULAR	PRESIDÊNCIA DA REPÚBLICA
DOCUMENTO	00.394.411/0001-09
RESPONSÁVEL	SECRETARIA DE ADMINISTRAÇÃO
PAIS	BR
CONTATO DO TITULAR	MAR79
CONTATO TÉCNICO	GCTGS
SERVIDOR DNS	luminol.ctir.gov.br 200.160.7.164 2001:12ff:0:7::164 v

CASOS
REAIS

TLP: CLEAR

Domain Dossier Investigate domains and IP addresses

domain or IP address

domain whois record
 DNS records
 traceroute
 network whois record
 service scan

user: anonymous [170.246.252.4]
 balance: 48 units
[log in](#) | [account info](#)

[Control Ips.net](#)

To obtain Whois data redacted because of the GDPR or privacy services, try ICANN's RDRS. [\[more information\]](#)

Address lookup

canonical name [presidencia.gov.br.](#)

aliases

addresses [170.246.255.9](#)

Domain Whois record

Queried [whois.nic.br](#) with "presidencia.gov.br"...

```

domain:      presidencia.gov.br
owner:       PRESIDENCIA DA REPUBLICA
registrant:  MART9
tech-c:      MART9
nservers:    alpha.planalto.gov.br
nsstat:      20240815 AA
nslastaa:    20240815
nservers:    alpha2.planalto.gov.br
nsstat:      20240815 AA
nslastaa:    20240815
dsrecord:    11146 RSA-SHA-1 0D3389EDA3D950B7616F91F88EE413AB04A96D1D7142D10AC6ED038BDD81AF879
dsstatus:    20240815 DSOK
dslastok:    20240815
dsrecord:    11146 RSA-SHA-1 75554E982E2D418C9DC98E8E3C8FB0ACDARCF86C
dsstatus:    20240815 DSOK
dslastok:    20240815
created:     20000903 #276288
changed:     20210225
status:      published

nic-hdl-br:  MART9
person:      Coord. Tecnologia de Rede
created:     19990524
changed:     20210225

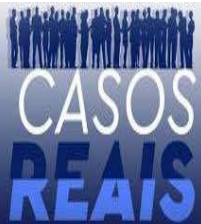
# Security and mail abuse issues should also be addressed to
# cert.br, http://www.cert.br/, respectively to cert@cert.br
# and mail-abuse@cert.br
#
# whois.registro.br accepts only direct match queries. Types
# of queries are: domain (.br), registrant (tax ID), ticket,
# provider, CIDR block, IP and ASN.
    
```

Network Whois record

Queried [whois.lacnic.net](#) with "170.246.255.9"...

```

inetnum:     170.246.252.0/22
aut-num:     AS266031
abuse-c:     MART9
owner:       PRESIDENCIA DA REPUBLICA
    
```





TLP: CLEAR

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

O que você procura?



Últimos Alertas e Recomendações

Alertas

ALERTA 15/2024

Vulnerabilidades na plataforma Zimbra Collaboration

ALERTA 14/2024

Falha crítica no sistema operacional Windows

ALERTA 13/2024

Vulnerabilidade crítica no produto Zabbix

ALERTA 12/2024

Recomendações

RECOMENDAÇÃO 04/2024

Configuração de controles recomendados pelas boas práticas para serviços Web, E-mail e DNS

RECOMENDAÇÃO 03/2024

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

RECOMENDAÇÃO 02/2024

Informações sobre o Ransomware Black Basta

TLP: CLEAR

501 Membros

Seção de administração da lista de discussão ETIR-GOV Gerenciamento de membros...

- | | | |
|--|---|---|
| <ul style="list-style-type: none"> • Opções Gerais • Senhas • opções de idioma • Gerenciamento de membros... <ul style="list-style-type: none"> ◦ [Lista de membros] ◦ Inscrição em massa ◦ Remoção em massa ◦ Alterar Endereço • Opções não digest • Opções digest | <p>Categorias de Configuração</p> <ul style="list-style-type: none"> • Opções de Privacidade... • Processamento de Retorno • Opções de Arquivamento • Email<->Notícias gateways • Auto-Resposta • Filtragem de Conteúdo • Tópicos | <p>Outras Atividades Administrativas</p> <ul style="list-style-type: none"> • Supervisionar requisições administrativas de moderação que estão pendentes • Ir para a página de informações gerais da lista • Editar as páginas HTML, públicas e arquivos de texto • Ir para os arquivos da lista • Sair |
|--|---|---|

Faça suas modificações nas seções seguintes, então submeta as modificações usando o botão *Enviar suas modificações*.

Lista de Membros

Encontrar membro [\(ajuda\)](#):

[Clique aqui para incluir a legenda para esta tabela.](#)

470 membros no total, 30 mostrados											
[A] B C D E F G H I J K L M N O P Q R S T U V W Y Z											
desinscr	endereço do membro nome do membro	moderado	ocultar	sem mensagens [razão]	notif	menos eu	sem duplicados	digest	plano	idioma	
<input type="checkbox"/>	abuse@cgu.gov.br	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Português (Brasil) ▾	
<input type="checkbox"/>	abuse@cni.jus.br	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Português (Brasil) ▾	



Maurício Leite Ferreira
Analista de Incidentes – CTIR Gov

mauricio.leite@presidencia.gov.br

Site: <https://www.gov.br/ctir>

Comunicação de Incidentes: ctir@ctir.gov.br

Linkedin: <https://www.linkedin.com/company/ctirgov/>

Twitter: <https://twitter.com/CtirGov>

TLP: CLEAR

CSIRT SETORIAL

