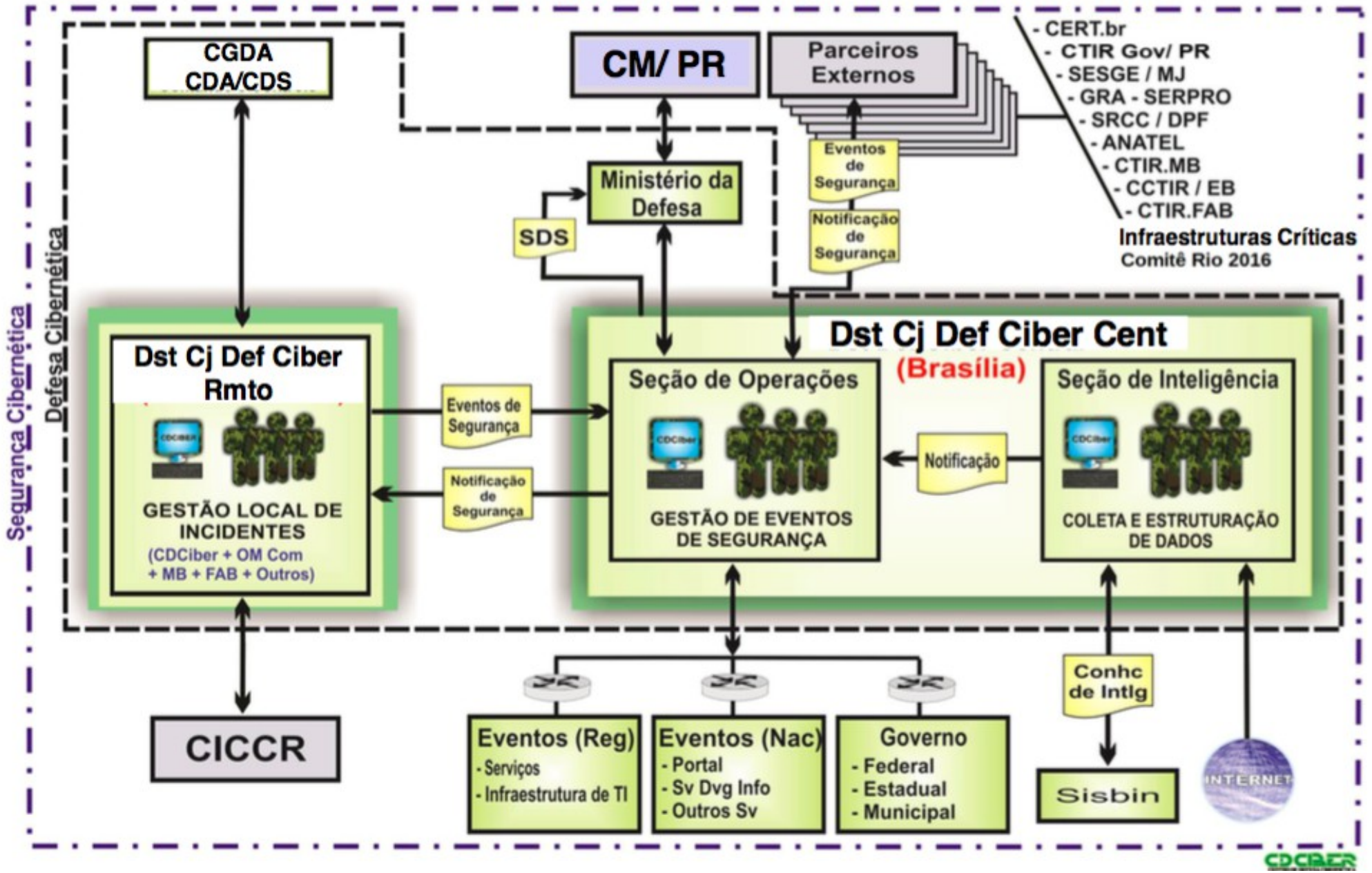
# PROCESSOS DE TRATAMENTO DE INCIDENTES EMPREGADOS PELO CDCIBER NOS JOGOS OLÍMPICOS E PARALÍMPICOS RIO 2016


# SUMÁRIO

1) Missão do CCSDCIBER para os JOP Rio 2016
2) Ações do CCSDCIBER para os JOP Rio 2016
3) Lições aprendidas da Copa do Mundo FIFA 2014
4) Avaliação do RT e RTIR
5) Implantação do RT
6) Customização do RT
7) Integração com soluções de segurança
8) Sumário Diário de Situação
9) Estatísticas sobre incidentes de segurança durante os Jogos Olímpicos e Paralímpicos Rio 2016
10) Ações futuras (ETIR de Coordenação)

# JO RIO 2016

## COORDENAÇÃO E INTEGRAÇÃO DA SEGURANÇA E DEFESA CIBERNÉTICAS



# CCSDCIBER

- O Centro de Coordenação de Segurança e Defesa Cibernética (CCSDCIBER) foi articulado em:
- 01 (um) Dst Cj Def Ciber Central (CDCiber)
- 10 (dez) Dst Cj Def Ciber Remotos, a saber:
  - 01 (um) no CGDA (CML - RJ);
  - 05 (cinco) nos CDAs (SP, BH, SV, MN e BR);
  - 04 (quatro) Centros de Defesa Setoriais (Maracanã, Deodoro, Barra e Copacabana).

**Início das operações em 11JUL16, com o regime de trabalho em período integral (h24), a partir de 15JUL16.**

# CCSDCIBER

- Capacitação dos militares e civis integrantes dos Dst Def Ciber:
- Curso do CERT.br – Overview sobre resposta e tratamento de incidentes de segurança. (40 horas)
- Estágio CDCiber – Soluções de segurança e de gestão de tíquetes . (40 horas)

# AÇÕES DO CCSDCIBER

O CCSDCiber **realiza a coordenação** da resposta e o tratamento dos Incidentes de Segurança Cibernéticos que representam violações de segurança nas redes de interesse para o MD na Op JO Rio 2016, bem como **colabora** com parceiros institucionais públicos e privados visando o compartilhamento da Consciência Situacional.

# AÇÕES DO CCSDCIBER

- Estabelecer recomendações de segurança **(caderno)**.
- Realizar análise e gestão de risco das redes de interesse (**inventário de ativos, identificação de vulnerabilidades e projeto de risco**).
- Implantar melhorias nos processos de resposta e tratamento a incidentes de segurança **(solução para gestão de tíquetes)**.
- Implantar soluções de segurança prospectadas.
- Realizar a distribuição de alertas e a consolidação de estatísticas.

# ESCOPO DE TRABALHO

- Recomendações de segurança e análise/gestão de risco das redes de interesse: CGDA, CDS e CDA (todos).
- Processos de resposta e tratamento a incidentes de segurança: CGDA, CDS e CDA (todos), Centro de Tecnologia dos JO Rio 2016 (TOC), CERT.br, CTIR.Gov, parceiros institucionais públicos e privados.
- Soluções de segurança: CDCiber, Ministério da Defesa, CGDA (2 CTA), CDS e CDA (todos).

# LIÇÕES APRENDIDAS
# COPA DO MUNDO FIFA 2014

- Implantação de um sistema de gestão de tíquetes **(específico)** para tratamento de incidentes de segurança.

- Elaboração de um dashboard (CS) que proporcionasse ao CDCiber as seguintes informações:

  a) estatística de incidentes e geração de alertas provenientes das redes de interesse;

  b) possível impacto no cenário cibernético;

  c) nível de alerta cibernético.

# RT vs RTIR

*“RT for Incident Response helps your CERT or CSIRT efficiently track computer security incidents. Designed collaboratively with top Incident Response teams, we built RTIR on top of RT to help manage your entire workflow from report to incident to investigation and resolution.*

*RTIR is the premise open source incident handling system targeted for computer security teams. We worked with over a dozen CERT and CSIRT teams around the world to help you handle the ever-increasing volume of incident reports.”*

*(Best Pratical, 2010)*

# RT vs RTIR

- O RTIR foi personalizado em excesso (processos, metodologia, características técnicas do incidente, constituência, dentre outros fatores)
- O RT fornece a possibilidade de personalização de forma bastante flexível. Embora seja necessário o **desenvolvimento de códigos** e modelos específicos, além da grande oferta de plugins.

# Especificações Técnicas RT

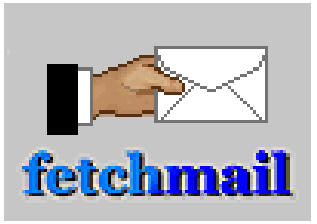
*“RT is a server-side, database-backed web application which works with any modern browser, including many popular mobile devices, and the email interface works with* ***any mail client****, from Outlook to Apple Mail to Thunderbird to Gmail to Mutt. On the server side, RT requires a Unix-like or* ***Linux operating system, SQL database, web server, and Perl.****"*

*(Best Pratical, 2010)*

# Especificações Técnicas RT



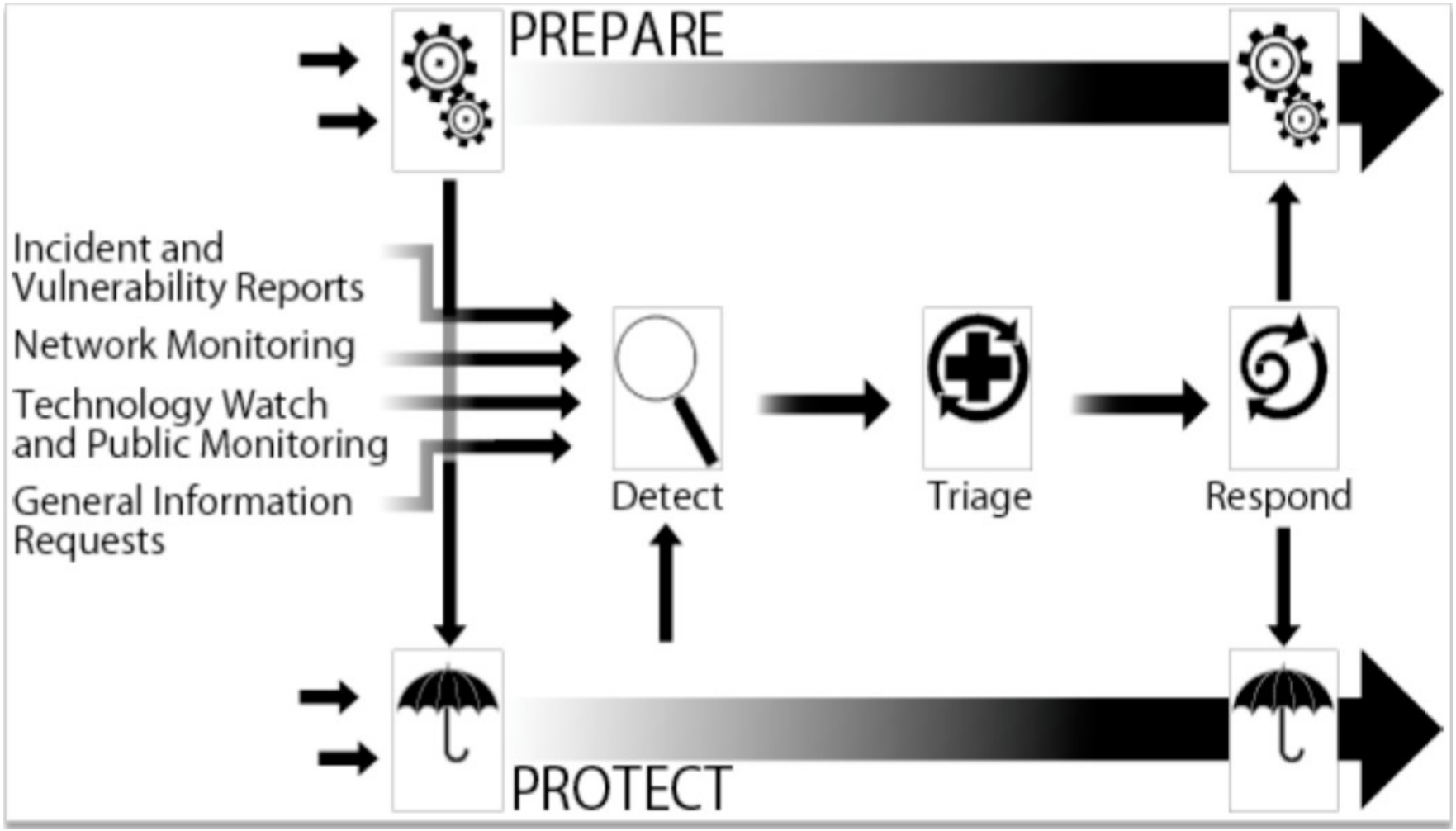



# SUPORTE PGP

- Diretório onde são colocadas todas as chaves públicas (confiáveis) no servidor.
- Arquivo de configuração contém a chave privada do CDCIBER.
- Opções de **assinar e encriptar**.

# PROCESSO DE RESPOSTA E TRATAMENTO




FONTE CERT.BR

# CUSTOMIZAÇÕES

- **Criação** de **filas**, de **grupos de usuários,** de **campos personalizados** e **ciclo de vida específico.**
- **Ações customizadas**
- **Finalizar análise**: Em análise para Analisado
- **Notificar**: Analisado para Notificado
- **Enviar para análise**: Aberto para Em análise

# TRANSIÇÕES ENTRE ESTADOS

- **Novo**: Aberto, Rejeitado, Em análise
- **Aberto**: Rejeitado, Pendente, Em análise, Analisado, Resolvido
- **Em análise**: Aberto, Pendente, Analisado, Rejeitado
- **Pendente**: Em análise, Rejeitado, Analisado, Notificado, Resolvido
- **Resolvido**: Aberto, Em análise, Pendente, Rejeitado
- **Rejeitado**: Aberto, Pendente, Em análise
- **Analisado**: Notificado, Pendente, Resolvido, Rejeitado
- **Notificado**: Resolvido, Em análise,  Pendente, Rejeitado

# Plugins RT

## 1. RT Extension PriorityAsString

Apresenta prioridades como "strings" ao invés de números. Exemplo: **muito alta, alta, média, baixa, muito baixa**

## 2. RT Extension MandatoryOnTransition

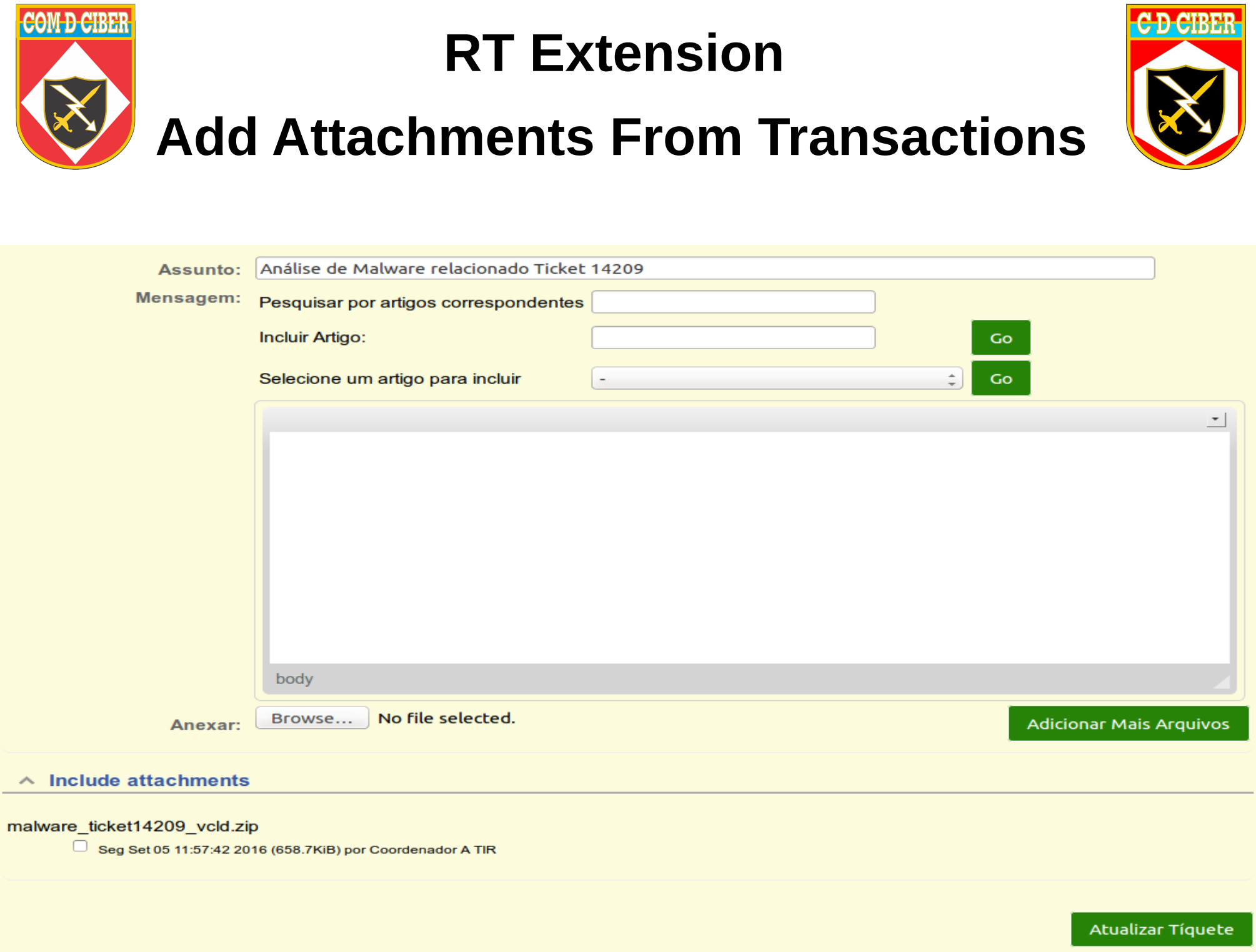
Impõe que determinados campos sejam preenchidos antes de mudar de/para estado ou a partir de estado específico. Exemplo: De qualquer estado para o estado **"Resolvido"**, o campo "Ações" é mandatório.

## 3. RT Extension CustomField HideEmptyValues

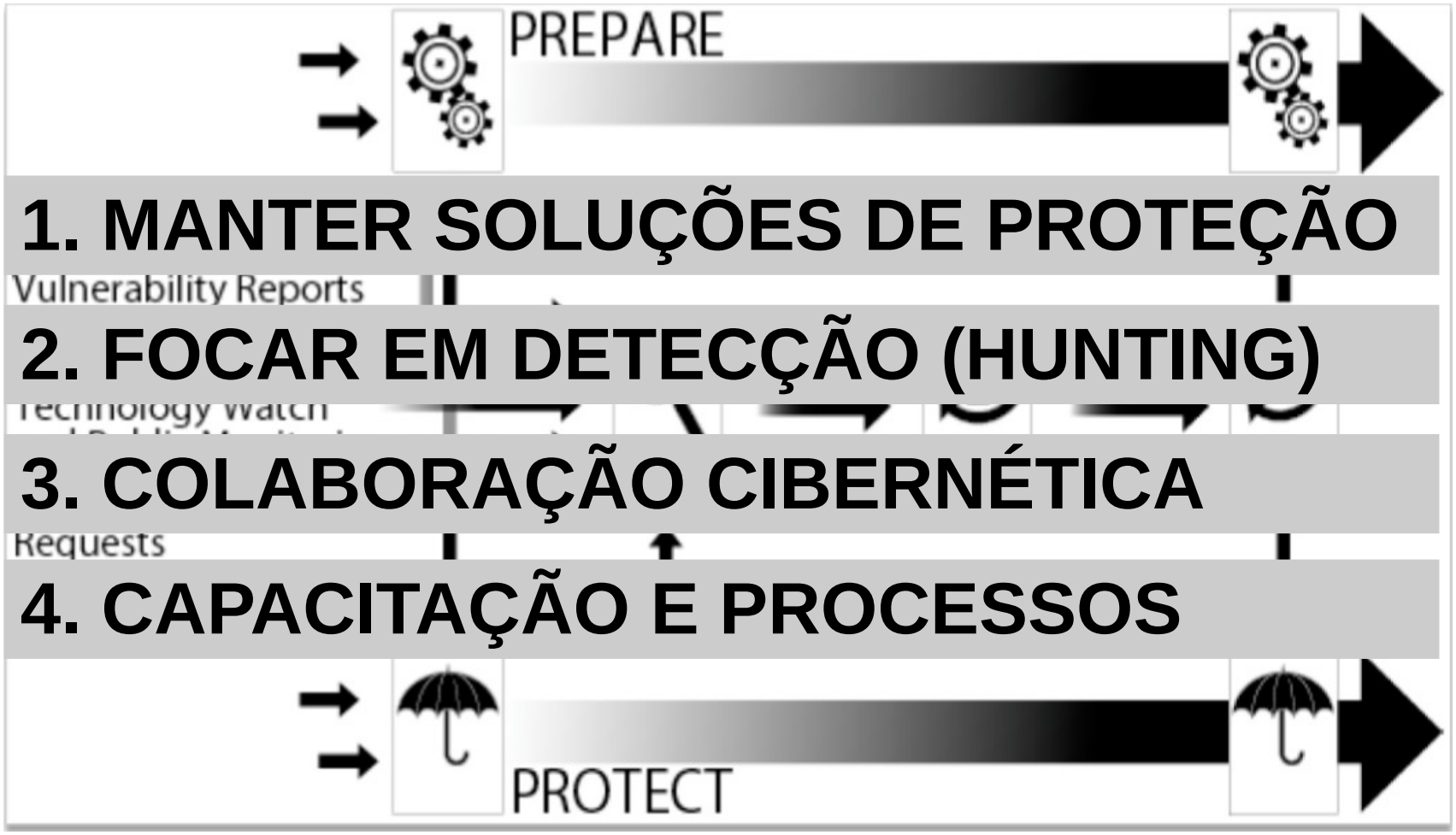
Permite esconder campos personalizados sem valores na interface do usuário do RT quando está visualizando um tíquete.

# RT Extension

# Add Attachments From Transactions



# CONCLUSÃO




FONTE CERT.BR