CENTRO DE DEFESA CIBERNÉTICA

3º Fórum Brasileiro de CSIRTS

Cel QEM José Ricardo Souza **CAMELO**

Centro de Defesa Cibernética - CDCiber

CDCIBER
CENTRO DE DEFESA CIBERNÉTICA

OBJETIVO

Discutir aspectos técnicos e Lições Aprendidas na Copa do Mundo FIFA 2014.

- **SUMÁRIO**
  - CDCiber e o Tratamento de Incidentes de Redes (TIR).
  - Estratégia adotada para a Operação Copa do Mundo FIFA 2014.
  - Números da Copa no escopo do CDCiber.
  - Eventos de destaque.
  - Comentários sobre Lições Aprendidas.
  - Conclusão.

CDCIBER EM 4 FRASES

- Organização Militar do Exército Brasileiro.
- Órgão Central do Sistema Militar de Defesa Cibernética (*).
- Coordena e Integra as atividades de Defesa Cibernética no âmbito do Ministério da Defesa (MD).
- Nos Grandes Eventos, Coordena e Integra as atividades de Segurança e Defesa Cibernéticas em apoio a Segurança do Evento.

CDCIBER CENTRO DE DEFESA CIBERNÉTICA

CDCIBER E O "TIR"

O CDCiber é um CSIRT?

MODELO TÉCNICO NOS GRANDES EVENTOS

- Ações de coordenação e integração eminentementes técnicas aplicadas à Operação Copa do Mundo FIFA 2014:
  - inventario de ativos de informação críticos ligados à Operação;
  - avaliação e análise (*) dos riscos dos ativos críticos de maior prioridade, conforme apontado por seus possuidores;
  - acompanhamento da divulgação de novas vulnerabilidades ligadas ao inventário;

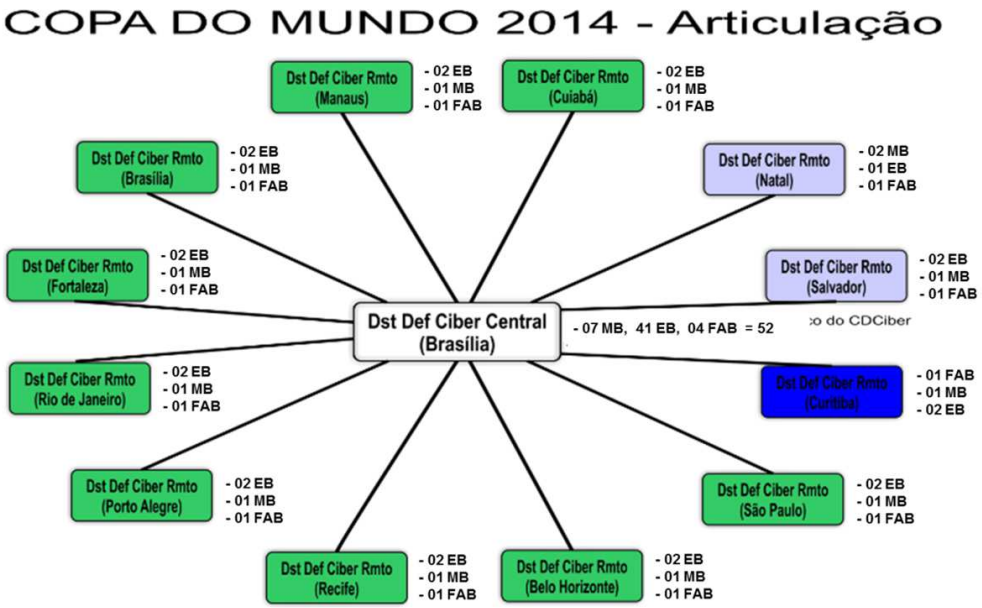
CDCIBER E O "TIR"

- acompanhamento da divulgação de supostos ataques ou mobilização para ataques a infraestruturas de informação de interesse;
- monitoração técnica da disponibilidade de sítios de interesse;
- mobilização de meios nas Forças Armadas e implementação de uma **Seção de Tratamentos de Incidentes de Redes**, em seu Centro de Operações, para gestão dos eventos de segurança ligados às redes computacionais de relevância para a Copa do Mundo FIFA 2014;

CDCIBER CENTRO DE DEFESA CIBERNÉTICA

ESTRATÉGIA ADOTADA

Operar com 13 Destacamentos de Defesa Cibernética



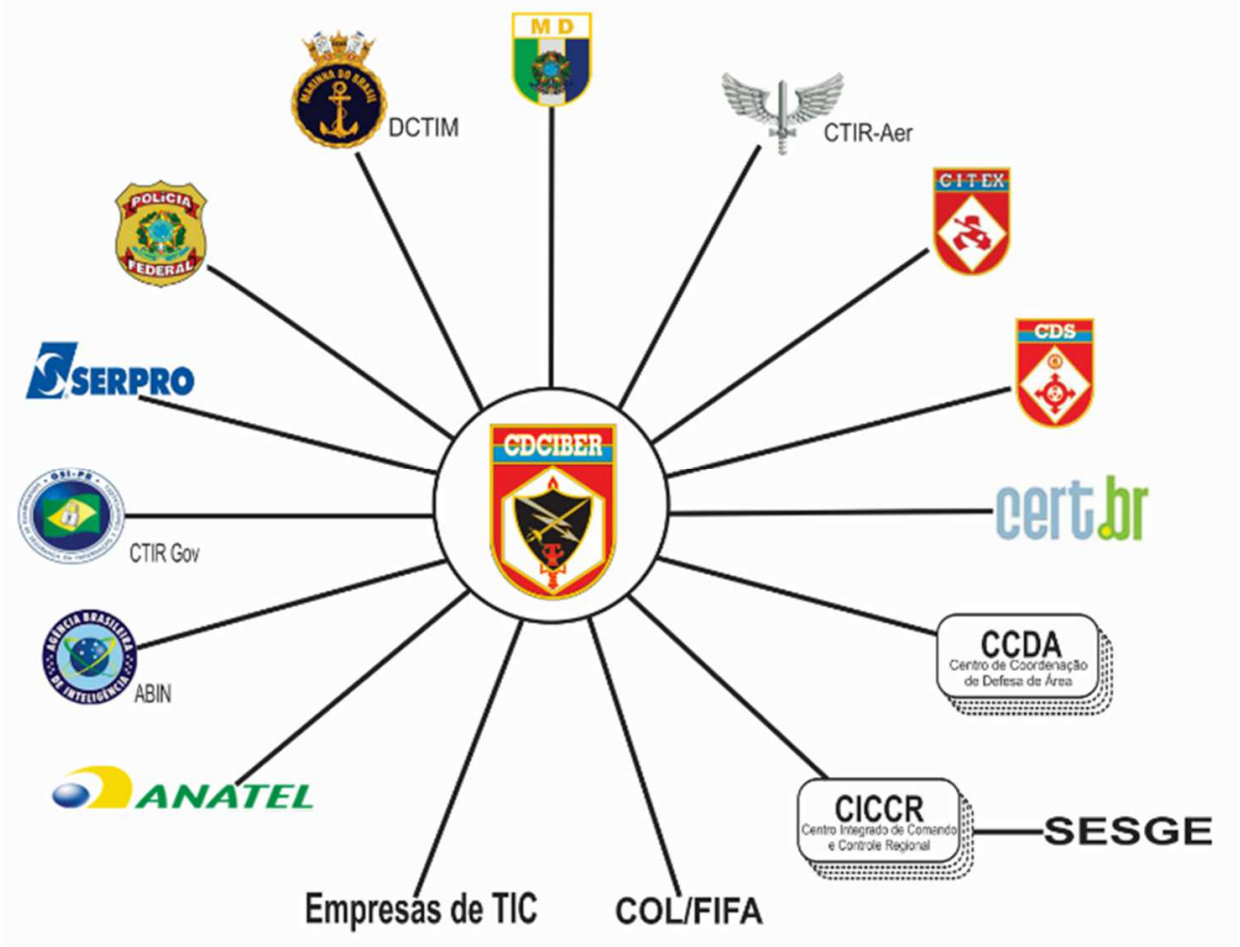
CDCIBER
CENTRO DE DEFESA CIBERNÉTICA

MSSÃO

Coordenar e integrar as ações de defesa e segurança cibernéticas contra ações cibernéticas hostis, colaborando com as medidas de segurança do Grande Evento

CDCIBER
CENTRO DE DEFESA CIBERNÉTICA

ATUAÇÃO COLABORATIVA NA COPA



CDCIBER
CENTRO DE DEFESA CIBERNÉTICA

NÚMEROS DA COPA DO MUNDO 2014

ITEM	QUANTIDADE
Análises de Riscos realizadas	15
Relatórios de Riscos Emitidos	30
Visitas Técnicas realizadas	60
Ativos identificados	1.592
Eventos de Segurança Tratados	756
Notificações de Segurança Enviadas	258
Eventos de Segurança tratados que envolveram análise de logs	3

CDCIBER
CENTRO DE DEFESA CIBERNÉTICA

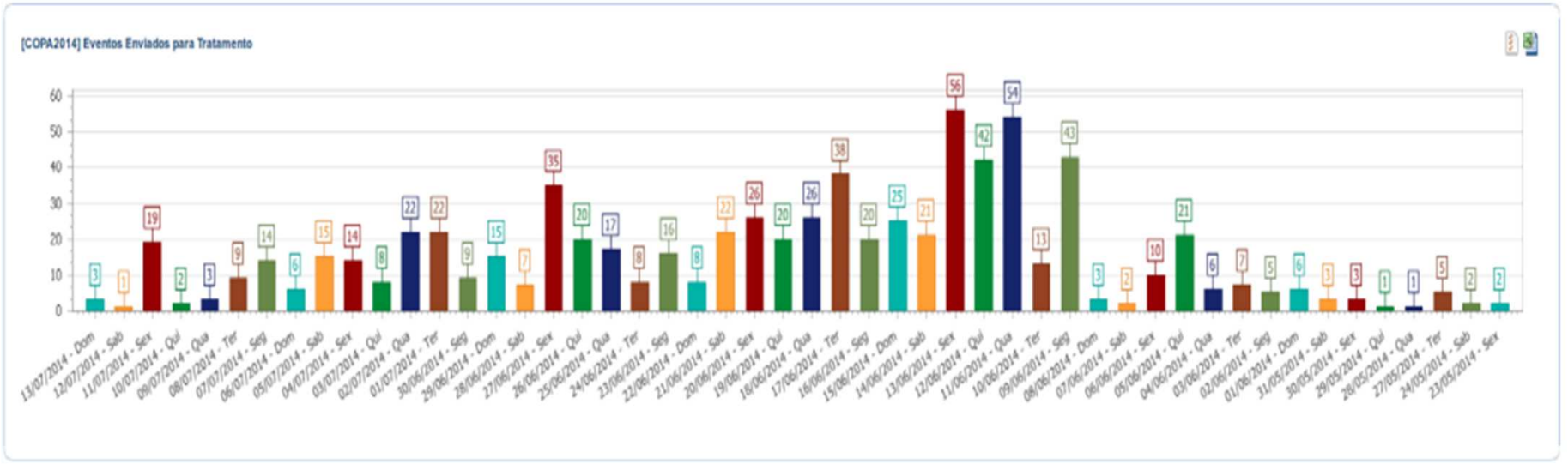
NÚMEROS DA COPA DO MUNDO 2014

ITEM	QUANTIDADE
Militares e Civis empregados	112
Pessoal capacitado	79
Cursos de Capacitação	2
Novas Vulnerabilidades Alertadas	12

CDCIBER
CENTRO DE DEFESA CIBERNÉTICA

NÚMEROS DA COPA DO MUNDO 2014

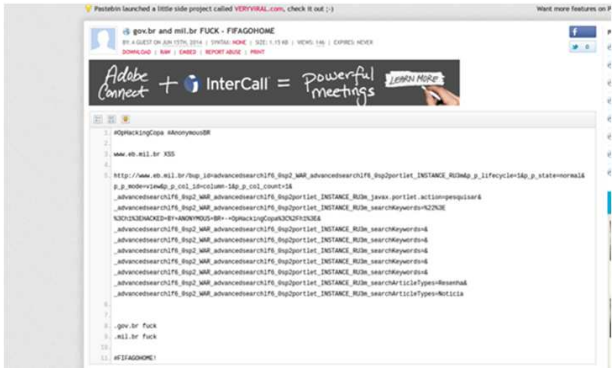
Eventos de Segurança



CDCIBER
CENTRO DE DEFESA CIBERNÉTICA

ALGUNS EVENTOS(*) DE DESTAQUE

- Vazamento de informações da rede do Itamaraty.
- Comprometimento de conta do Twitter da Polícia Federal.
- Ataques à página do Exército.
- (*) eventos de conhecimento público



CDCIBER CENTRO DE DEFESA CIBERNÉTICA

ALGUMAS LIÇÕES APRENDIDAS

- Canal técnico x "Ação de Comando".
- Antecipação propiciada pelas ações combinadas inventariação de ativos, gestão de riscos, inteligência mostrou-se pertinente e deve ser aprimorada.
- Operar presencialmente reduz tempo de reação aos incidentes e potencializa a proatividade nas ações.

ALGUMAS LIÇÕES APRENDIDAS

- O aumento da atuação colaborativa e o aprofundamento das **relações de confiança** entre as instituições não é simplesmente relevante: é essencial.
- O "hacktivismo" possui potencial para promover ataques com impactos muito maiores que o demonstrado. Tal comportamento merece atenção e análise?

ALGUMAS LIÇÕES APRENDIDAS

- As ameaças que estão além do hacktivismo, além de atuarem "silenciosamente", possuem potencial e motivação, a princípio, muito maiores, no entanto, não foram identificadas, de forma explícita, ações dessa ordem vinculadas aos Grandes Eventos no Brasil. Essa visão é pertinente? O que isso pode significar?

QUAIS SÃO AS VERDADEIRAS AMEAÇAS?...

Hacktivismo...

Espionagem cibernética ...

Terrorismo cibernético ...

Crime Cibernético ...

CDCIBER CENTRO DE DEFESA CIBERNÉTICA

OBRIGADO!