



Ministério da Fazenda

Serviço Federal de Processamento de Dados (SERPRO)

A Resposta a Incidentes no Processo de Desenvolvimento Seguro

Daniel Araújo Melo - daniel.melo@serpro.gov.br

1o. Fórum Brasil-Amazônia de TIC - 11/11/2011



Ligado nas
Comunidades

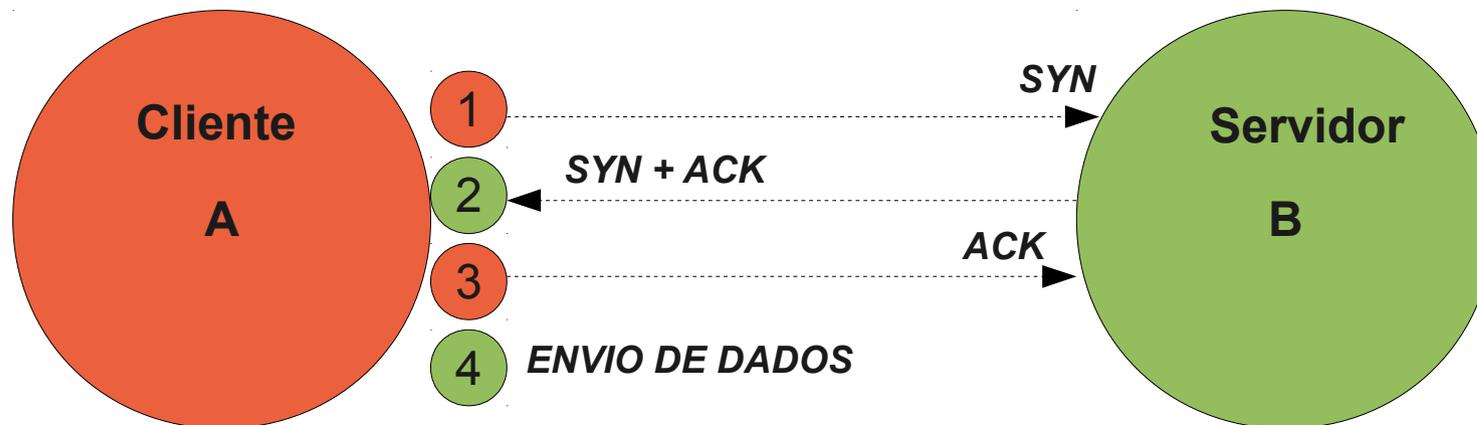
 **SERPRO**
Serviço Federal de Processamento de Dados

Agenda

- **Segurança em TIC**
- **Resposta a Incidentes**
- **Processo de Resposta a Incidentes**
- **Resposta a Ataques no SERPRO**

História

- **1996 – 14.000 computadores conectados à Internet**
- **TCP - Principal Protocolo**
- **1 de setembro – Phrack Magazine publica exploit que explora característica do Destinatário**
 - Destinatário aloca recursos ao receber (1)



Ciclo de Vida das Vulnerabilidades

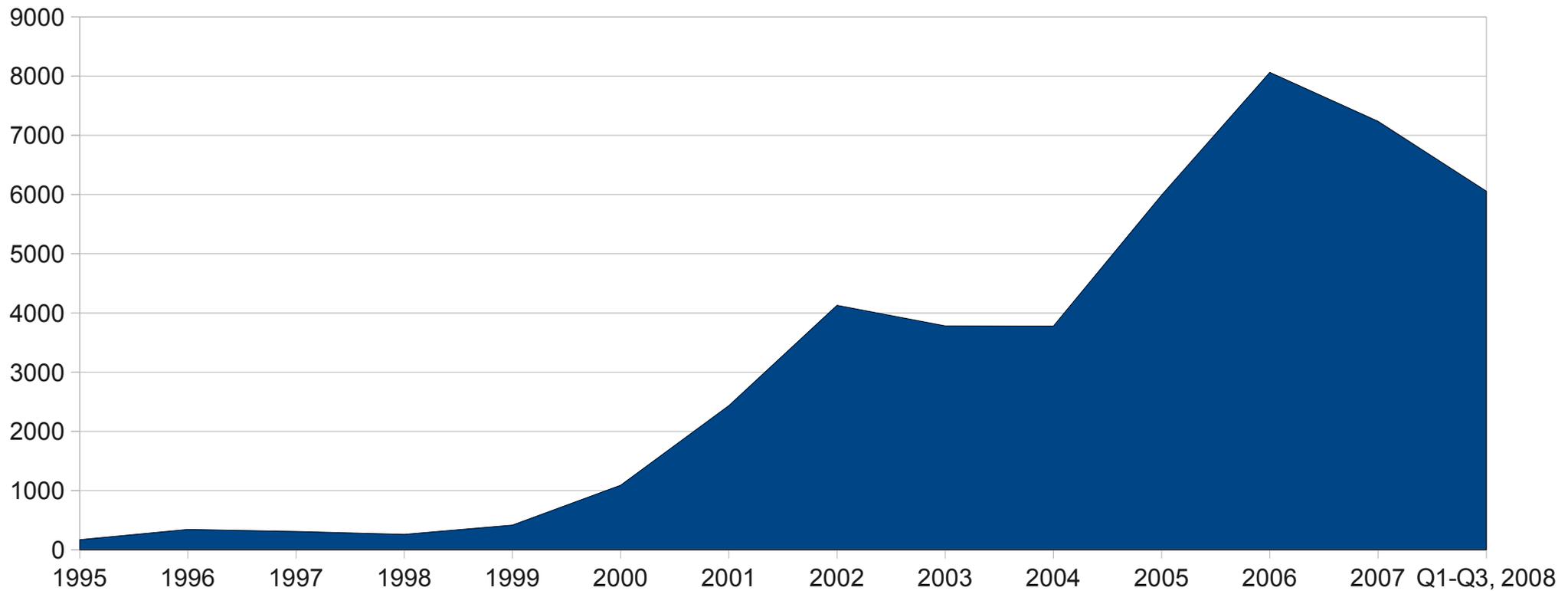
- **Alguém descobre a vulnerabilidade;**
- **Atacantes analisam e produzem exploits;**
- **Ataques ocorrem;**
- **Defensores buscam correção;**
- **Soluções paliativas são propostas;**
- **Correção é publicada;**
- **Após alguns meses, malware é lançado.**



Vulnerabilidades Reportadas



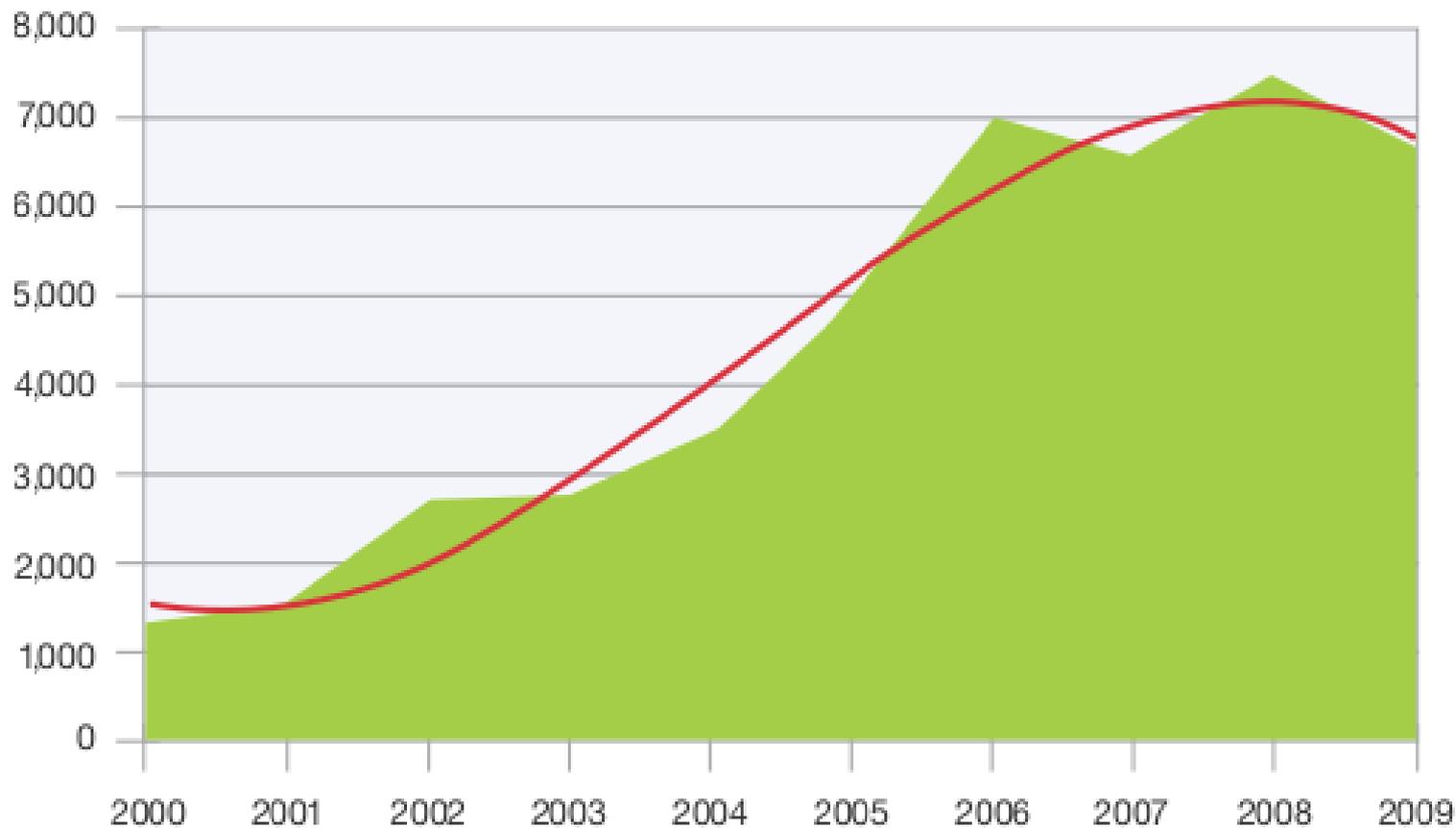
Vulnerabilidades Reportadas ao Cert/CC



Vulnerabilidades Reportadas



Vulnerability Disclosures 2000-2009



Fonte: IBM X-Force 2009 Trend and Risk Report

Quanto é muito?



- **3784 vulnerabilidades reportadas em 2003**
 - $3784 * 20$ minutos para ler = 158 dias
 - Supondo que você seja afetado por 10%
 - $378 * 1$ hora para instalar correção = 47 dias para instalar todas as correções em 1 sistema.
 - Para ler notícias de segurança e corrigir 1 sistema
 - $158 + 47 = 205$ dias

Quanto é muito?

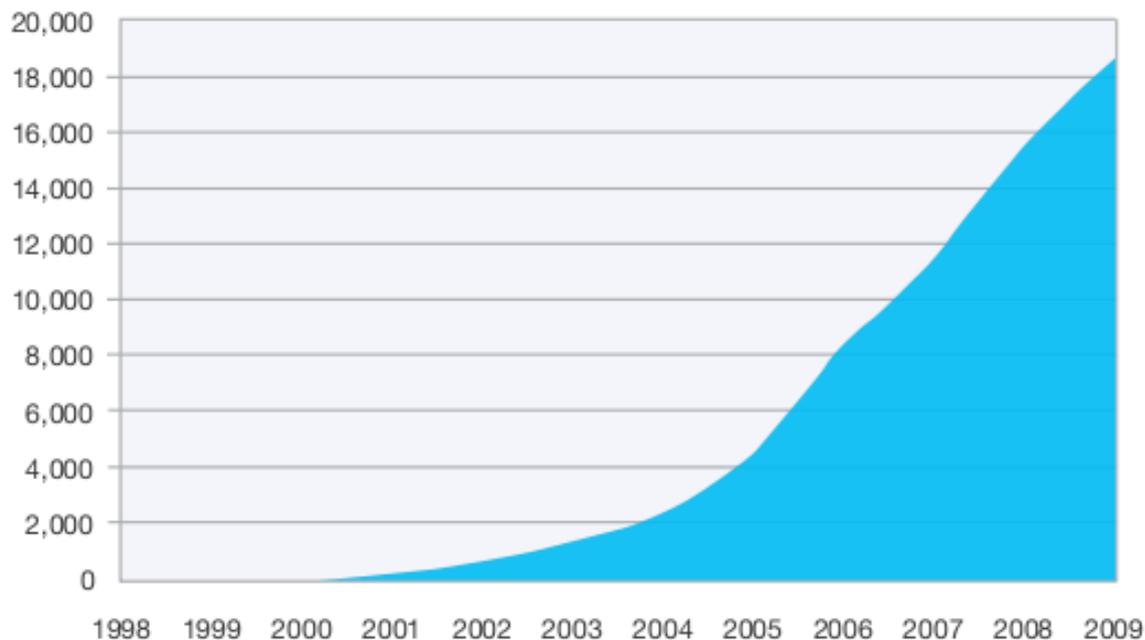


- **Wietse Venema estima que em geral existe 1 falha de segurança por 1000 linhas de código**
 - Kernel Linux ultrapassou 13 milhões de linhas
 - <http://www.h-online.com/open/features/What-s-new-in-Linux-2-6-36-1103009.html?page=6>
 - Um sistema desktop pode possuir mais de 100 milhões de linhas de código
- **Necessários 20 anos para identificar todas as falhas de um sistema desktop;**
- **10% a 15% das correções inserem novas vulnerabilidades.**

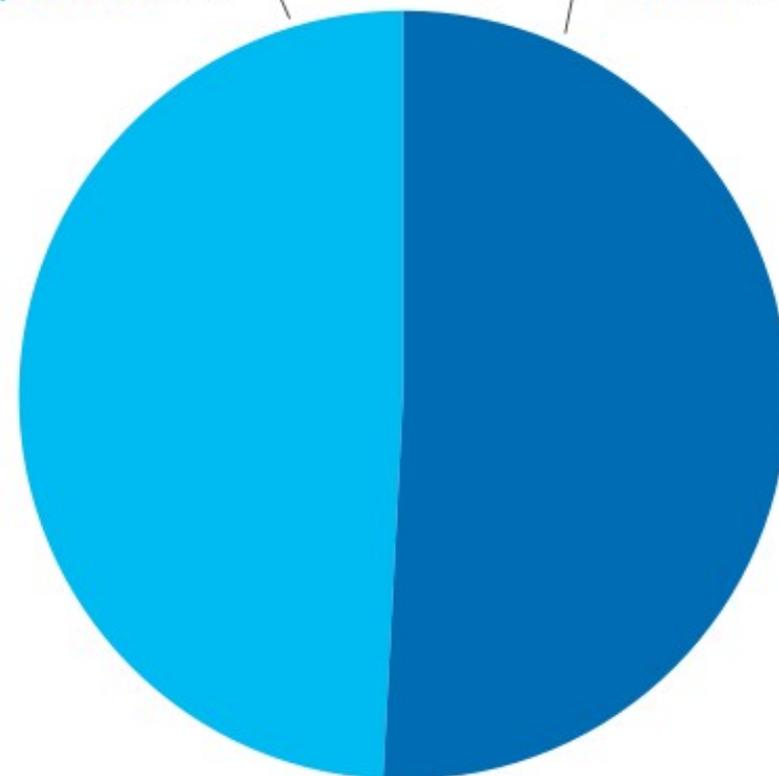
Vulnerabilidades WEB



**Cumulative Count of Web Application
Vulnerability Disclosures
1998-2009**



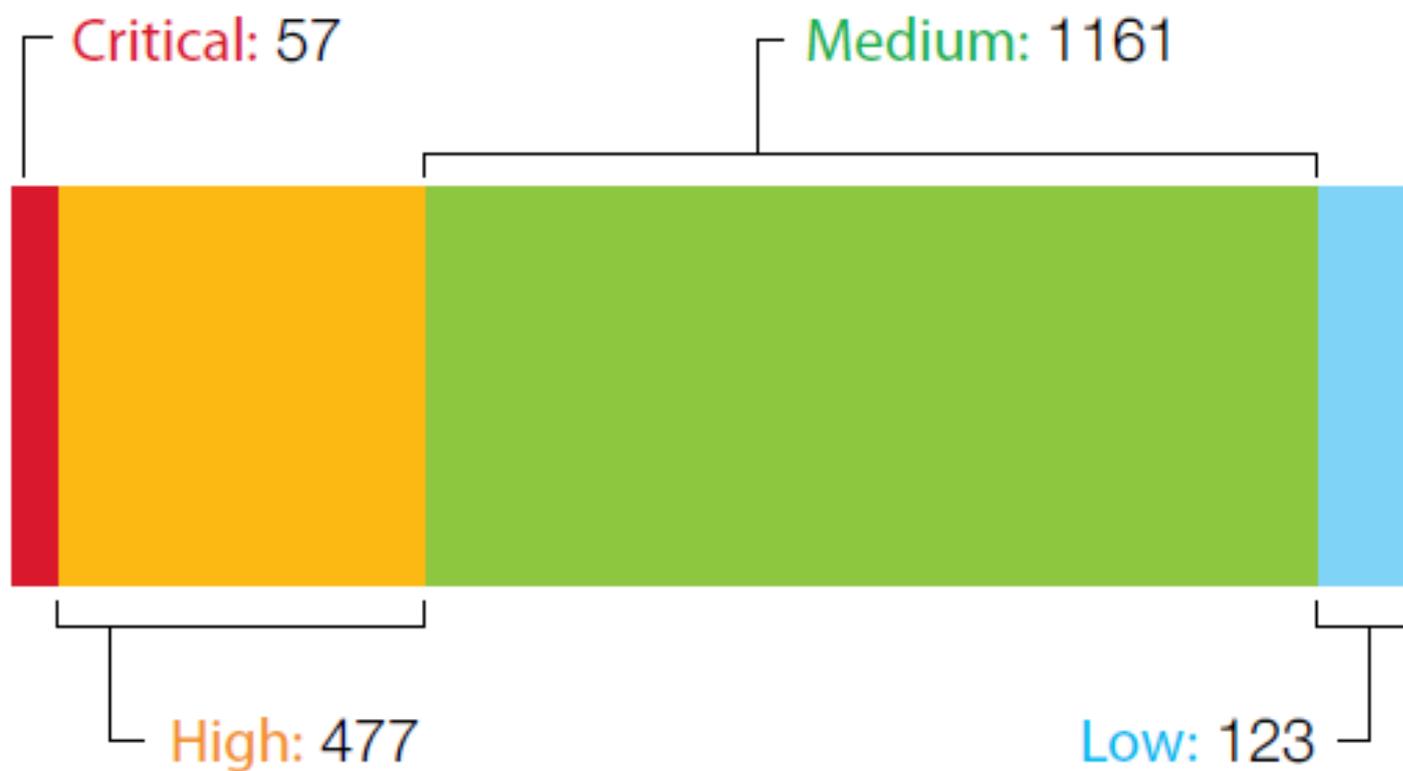
Web Applications: 49% **Others: 51%**



Fonte: IBM X-Force 2009 Trend and Risk Report



Total Vulnerabilities in Q1 2011: 1818



Source: IBM X-Force



Novas Vulnerabilidades
+
Nenhum mecanismo de segurança é 100% confiável!
=
Incidentes de Segurança podem ocorrer...



Como responder a um Incidente?



Empiricamente percebe-se que:

Quanto mais ágil for a recuperação de um incidente,
menor será o prejuízo.

Resposta a Incidentes



- **RFC 2350 – BCP 21**
 - Expectations for Computer Security Incident Response

Network Working Group
Request for Comments: 2350
BCP: 21
Category: Best Current Practice

N. Brownlee
The University of Auckland
E. Guttman
Sun Microsystems
June 1998

Expectations for Computer Security Incident Response

Status of this Memo

This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (1998). All Rights Reserved.

Abstract

The purpose of this document is to express the general Internet community's expectations of Computer Security Incident Response Teams (CSIRTs). It is not possible to define a set of requirements that would be appropriate for all teams, but it is possible and helpful to list and describe the general set of topics and issues which are of concern and interest to constituent communities.

Resposta a Incidentes



- **RFC 2350**
 - Expectations for Computer Security Incident Response

Network Working Group
Request for Comments: 2350
BCP: 21

N. Brownlee
The University of Auckland
E. Guttman
Sun Microsystems
June 1998

N. Brownlee
The University of Auckland
E. Guttman
Sun Microsystems
June 1998

Computer Security Incident Response

Current Practices for the
Commission and suggestions for
is unlimited.

Copyright (C) The Internet Society (1998). All Rights Reserved.

Abstract

The purpose of this document is to express the general Internet community's expectations of Computer Security Incident Response Teams (CSIRTs). It is not possible to define a set of requirements that would be appropriate for all teams, but it is possible and helpful to list and describe the general set of topics and issues which are of concern and interest to constituent communities.

Resposta a Incidentes



- **RFC 2350**
 - Expectations for Computer Security Incident Response

Network Working Group
Request for Comments: 2350

N. Brownlee
The University of Auckland

This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements. Distribution of this memo is unlimited.

Status of this Memo

This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (1998). All Rights Reserved.

Abstract

The purpose of this document is to express the general Internet community's expectations of Computer Security Incident Response Teams (CSIRTs). It is not possible to define a set of requirements that would be appropriate for all teams, but it is possible and helpful to list and describe the general set of topics and issues which are of concern and interest to constituent communities.

Resposta a Incidentes



- **RFC 2350**
 - Expectations for Computer Security Incident Response

Network Working Group
Request for Comments: 2350
BCP: 21
Category: Best Current Practice

N. Brownlee
The University of Auckland
E. Guttman
Sun Microsystems
June 1998

The purpose of this document is to express the general Internet community's expectations of Computer Security Incident Response Teams (CSIRTs). It is not possible to define a set of requirements that would be appropriate for all teams, but it is possible and helpful to list and describe the general set of topics and issues which are of concern and interest to constituent communities.

Copyright Notice

Copyright (C) The Internet Society (1998). All Rights Reserved.

Abstract

The purpose of this document is to express the general Internet community's expectations of Computer Security Incident Response Teams (CSIRTs). It is not possible to define a set of requirements that would be appropriate for all teams, but it is possible and helpful to list and describe the general set of topics and issues which are of concern and interest to constituent communities.

Programa CERT



Software Engineering Institute
Carnegie Mellon

search



[Publications Catalog](#)

[HOME](#) | [Software Assurance](#) | [Secure Systems](#) | [Organizational Security](#) | [Coordinated Response](#) | [Training](#)

information for

[System Administrators](#)

[Developers](#)

[Researchers](#)

[Managers](#)

[Prospective Employees](#)

Welcome to CERT

about us

CERT, the home of the well-known [CERT@ Coordination Center](#), is located at Carnegie Mellon University's Software Engineering Institute. We study internet security vulnerabilities, research long-term changes in networked systems, and develop information and training to help you improve security.

Our areas of focus

- software assurance
- secure systems
- organizational security
- coordinated response
- training

[Take the tour](#)

CERT Spotlight: XNET

How can you ensure that your staff is prepared?

Responding to critical cyber events requires technical knowledge and skills, decision-making abilities, and effective coordination. The best way to prepare your staff is to have them practice under realistic conditions; however, it can be difficult and expensive to create and administer these types of training scenarios.

Our [CERT® Exercise Network \(XNET\)](#) solves these problems. This platform allows organizations to create customized, realistic, interactive simulations on an isolated network. Through a web-based interface, participants across multiple locations can work together to analyze and respond to the latest



Announcements

October 17, 2011

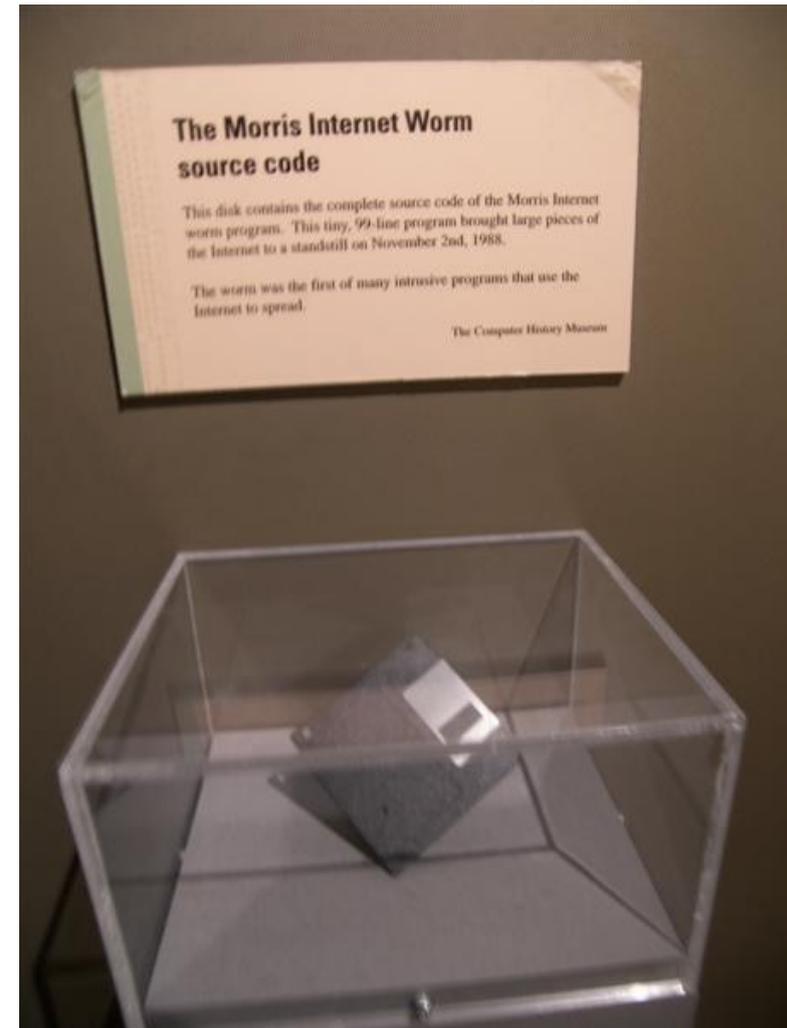
[New Insider Threat Blog Entry](#)
The entry "Data Exfiltration and Output Devices - An Overlooked Threat" has been posted.

October 14, 2011

[CERT Oracle Secure Coding Standard for Java Book Published](#)
The CERT Oracle Secure Coding Standard for Java has been published by Addison-Wesley Professional.

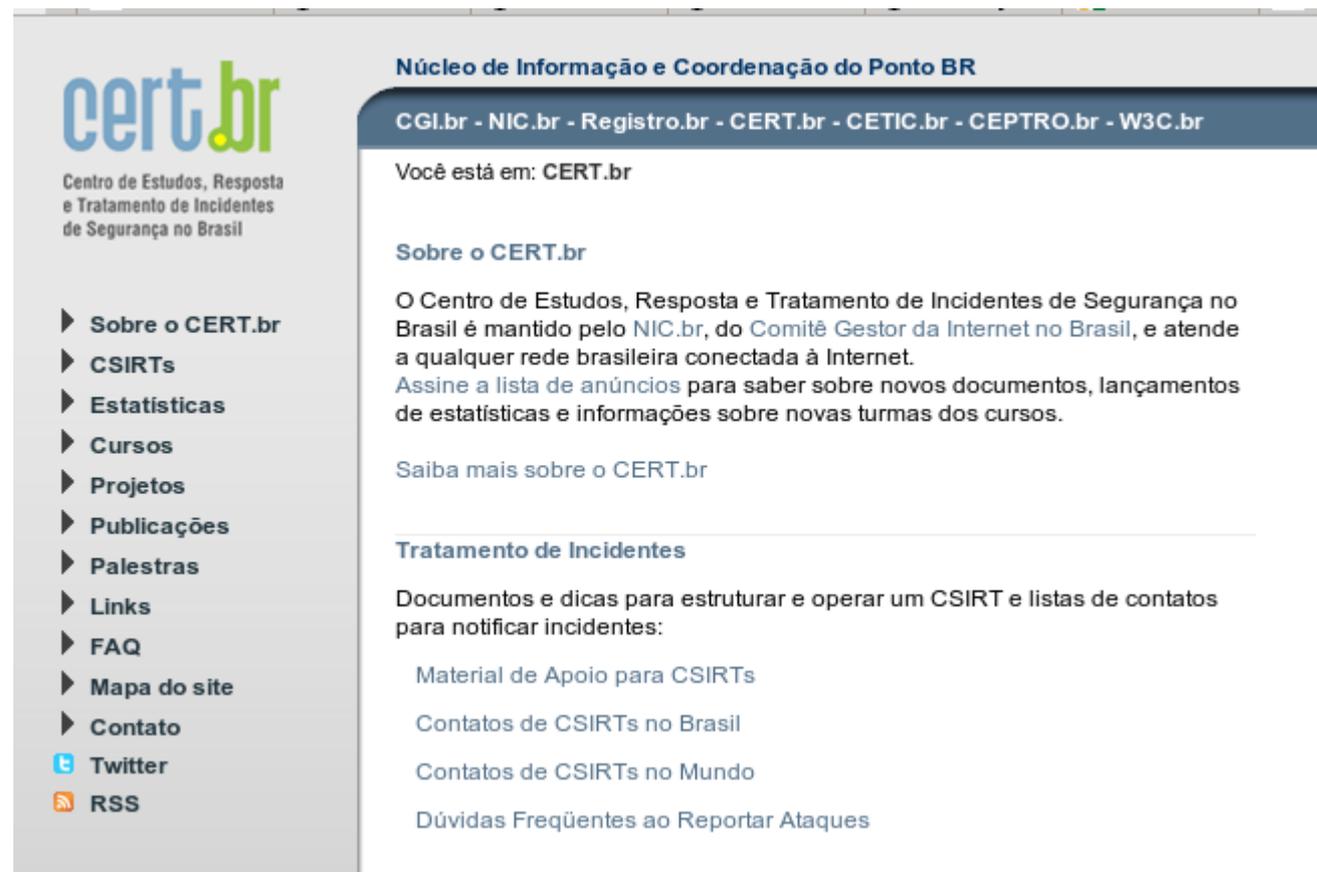
Programa CERT

- **Criado em 1988**
- **Motivação:**
 - Incidente com o Worm de Morris
 - 10% da Internet foi afetada
 - Explorava múltiplas vulnerabilidades
- **Fianciado pela DARPA**
 - Defense Advanced Research Projects Agency
- **CSIRT Handbook**
 - Computer Security Incident Response Team Handbook



http://en.wikipedia.org/wiki/Morris_worm

- **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**
- **Equipe de Resposta a Incidentes mantida pelo Comitê Gestor de Internet**

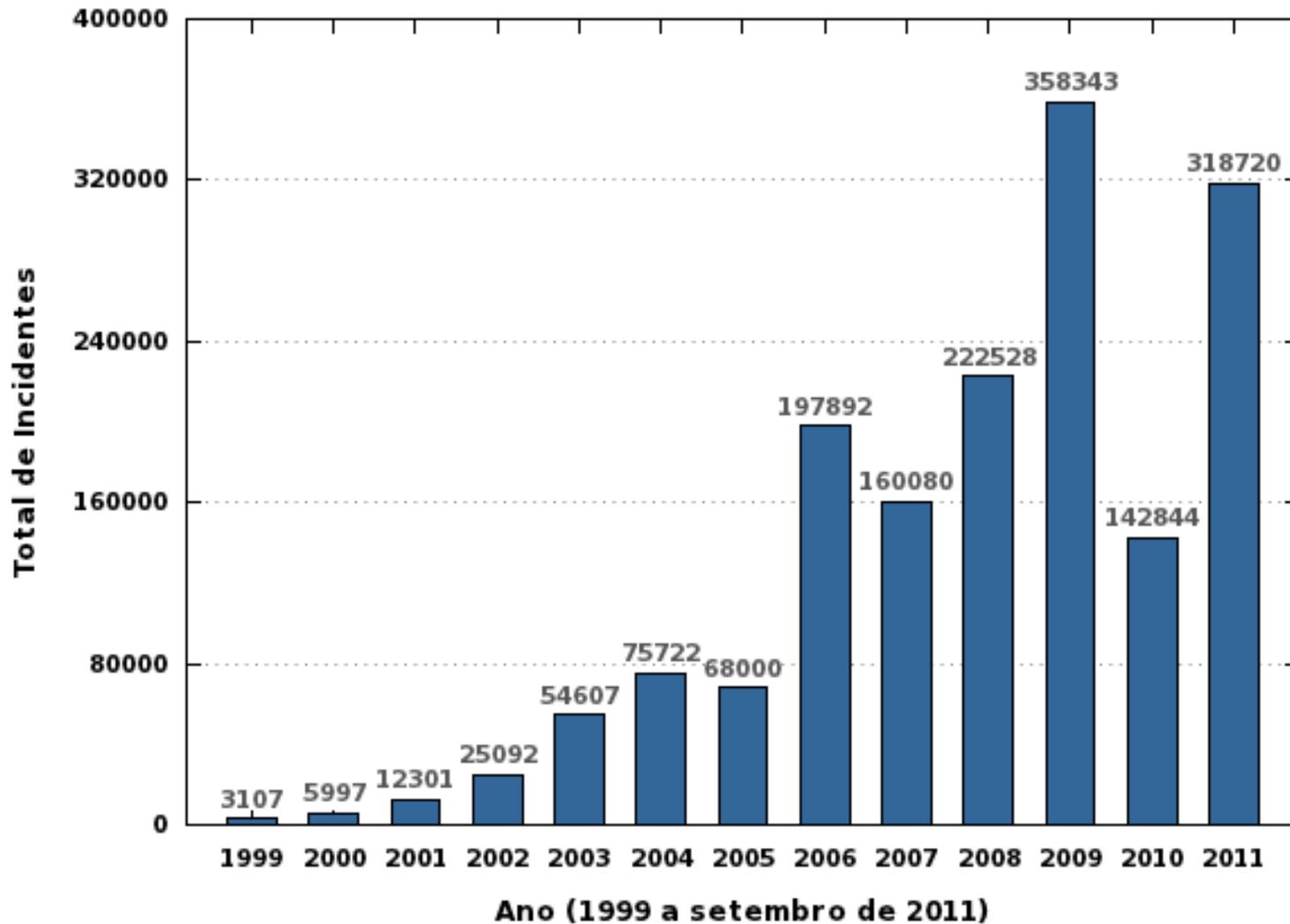


The screenshot shows the CERT.br website. On the left is a navigation menu with the following items: Sobre o CERT.br, CSIRTs, Estatísticas, Cursos, Projetos, Publicações, Palestras, Links, FAQ, Mapa do site, Contato, Twitter, and RSS. The main content area has a header for 'Núcleo de Informação e Coordenação do Ponto BR' and a sub-header listing various domains: CGI.br - NIC.br - Registro.br - CERT.br - CETIC.br - CEPTRO.br - W3C.br. Below this, it states 'Você está em: CERT.br'. The main section is titled 'Sobre o CERT.br' and contains the following text: 'O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil é mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil, e atende a qualquer rede brasileira conectada à Internet. Assine a lista de anúncios para saber sobre novos documentos, lançamentos de estatísticas e informações sobre novas turmas dos cursos.' Below this is a link 'Saiba mais sobre o CERT.br'. A section titled 'Tratamento de Incidentes' lists 'Documentos e dicas para estruturar e operar um CSIRT e listas de contatos para notificar incidentes:' followed by links for 'Material de Apoio para CSIRTs', 'Contatos de CSIRTs no Brasil', 'Contatos de CSIRTs no Mundo', and 'Dúvidas Frequentes ao Reportar Ataques'.



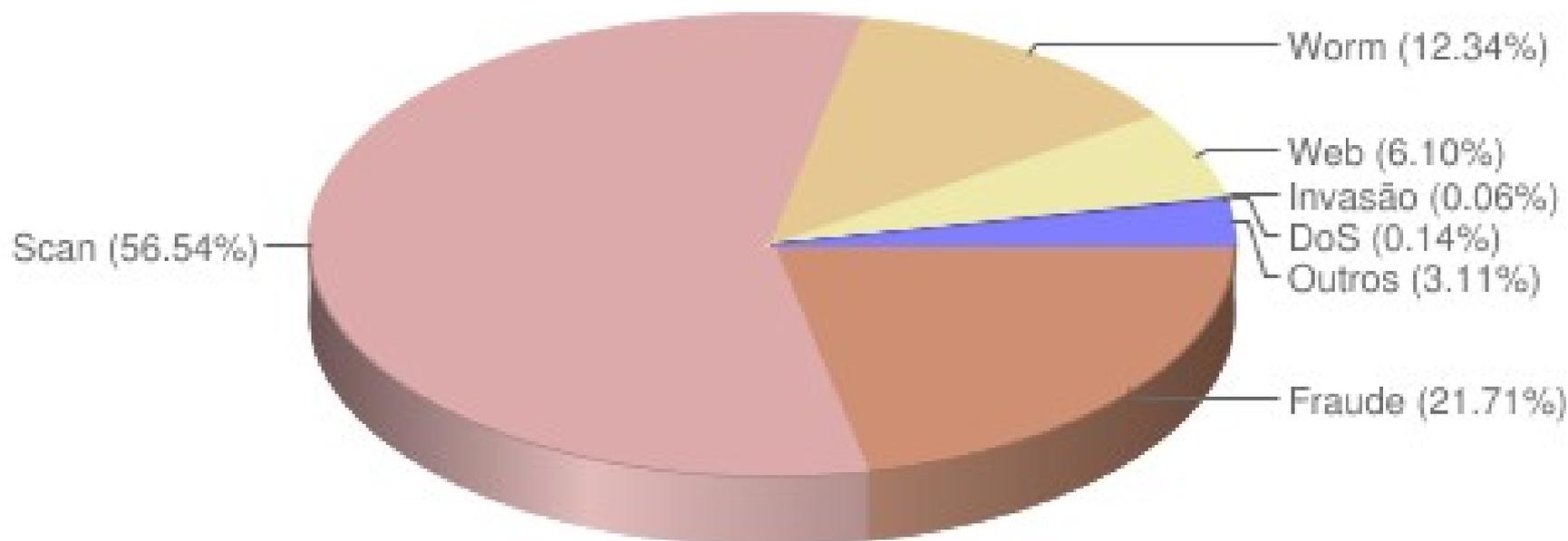
- **Estatísticas**

Total de Incidentes Reportados ao CERT.br por Ano





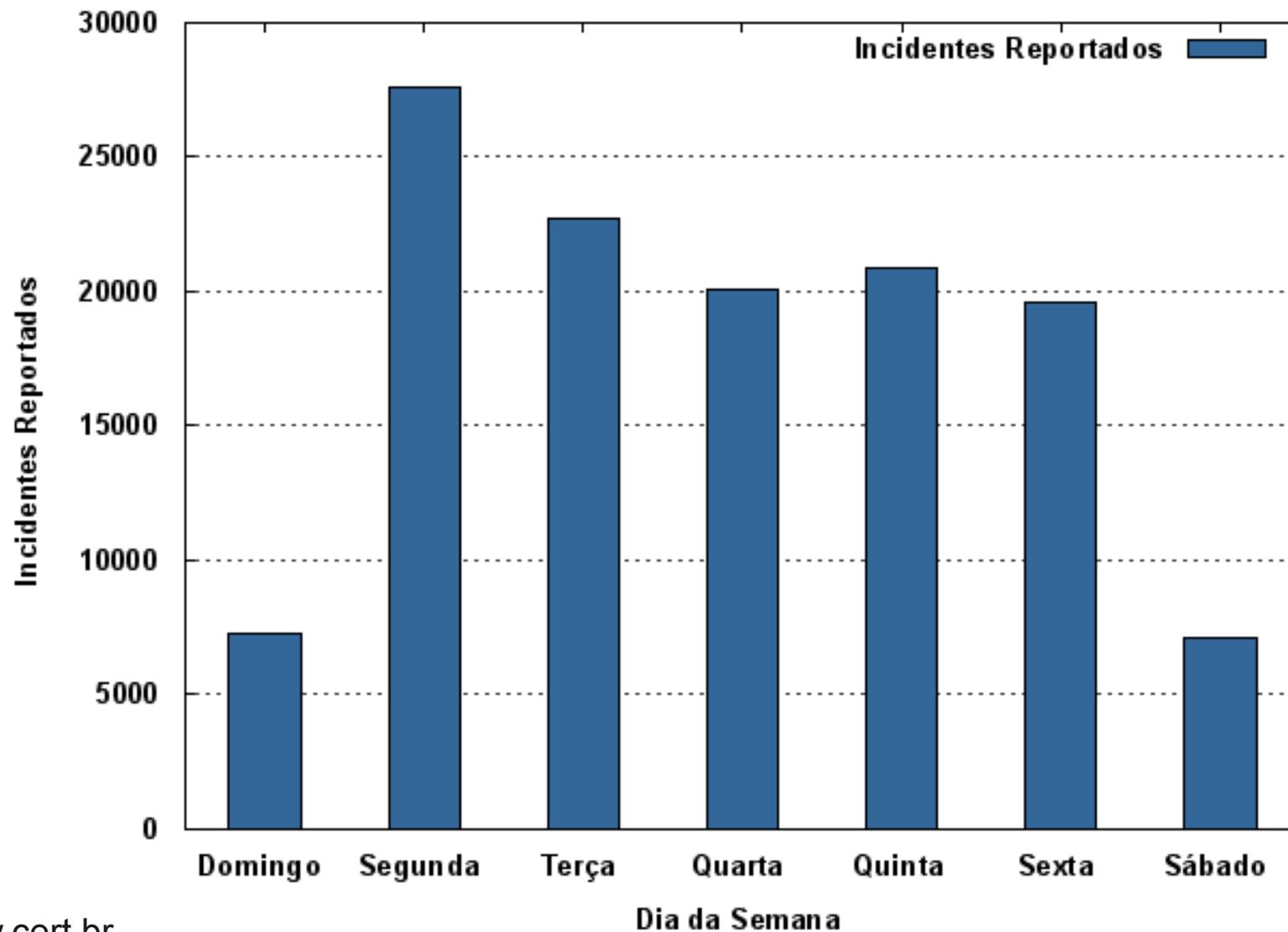
Incidentes reportados (Tipos de ataque)



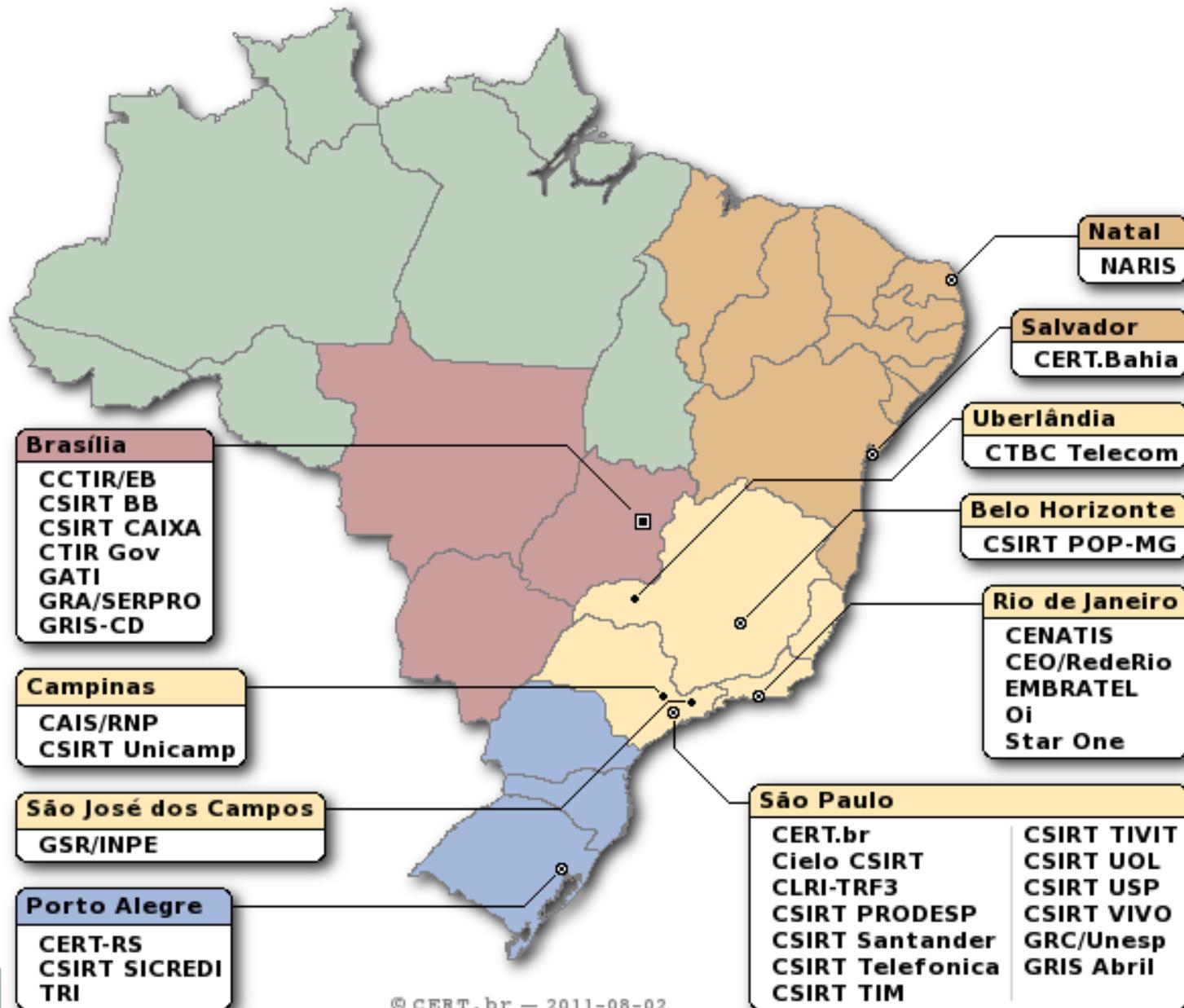
Fonte: www.cert.br



CERT.br: Incidentes Reportados (por dia da semana)



Csirts no Brasil

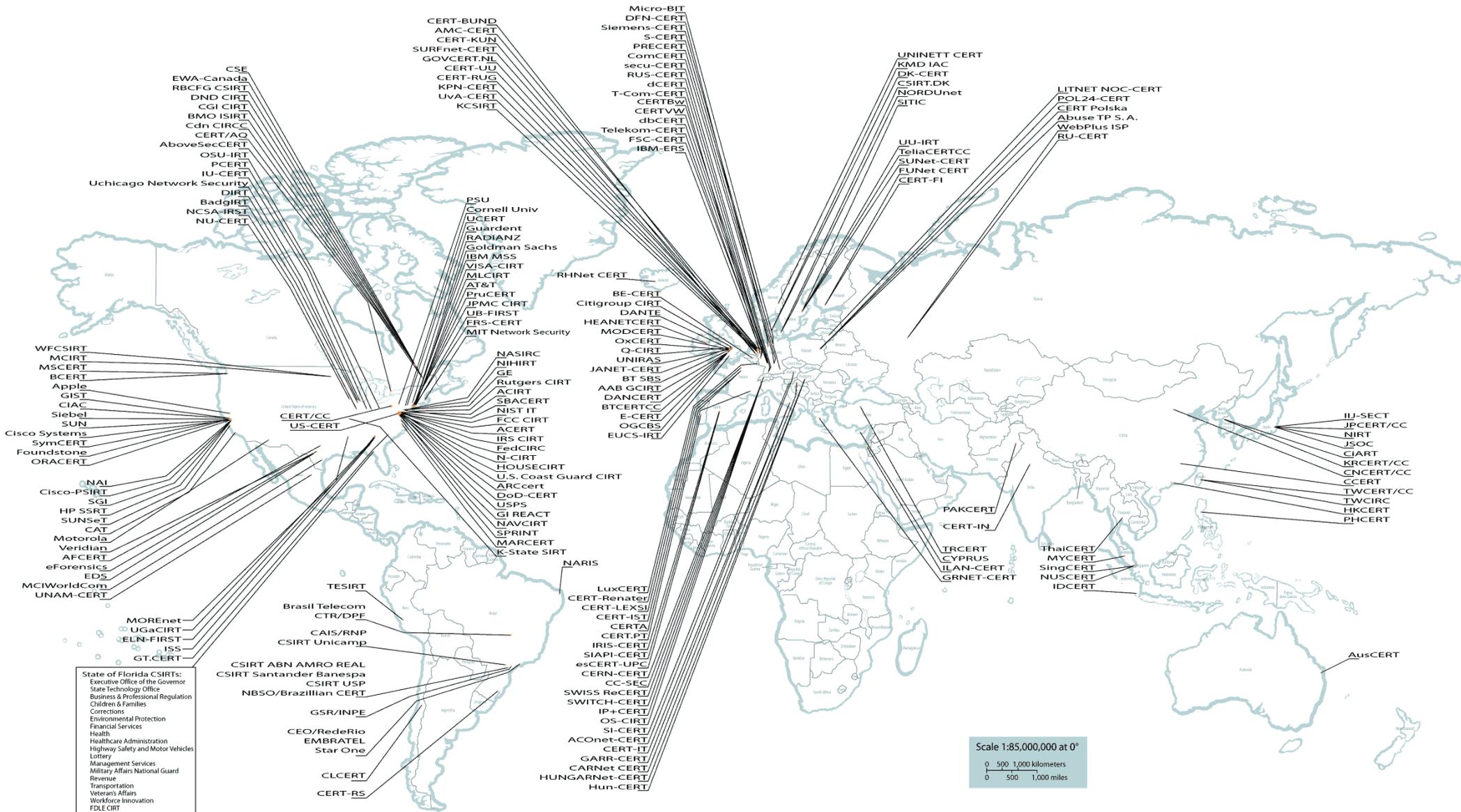


Csirts no Mundo - FIRST



Incident Response Teams Around the World

International cooperation speeds response to Internet security breaches.



Framework Csirt



- **Processo Genérico e Adaptável;**
- **Difundido mundialmente;**
- **Apresenta como estabelecer e manter uma equipe de resposta a incidentes**
 - Analogia com corpo de bombeiros
- **Serviços que podem ser oferecidos**
 - 3 categorias
 - Reativos
 - Proativos
 - Gestão de qualidade

Serviços



Reactive Services



- + Alerts and Warnings
- + Incident Handling
 - Incident analysis
 - Incident response on site
 - Incident response support
 - Incident response coordination
- + Vulnerability Handling
 - Vulnerability analysis
 - Vulnerability response
 - Vulnerability response coordination
- + Artifact Handling
 - Artifact analysis
 - Artifact response
 - Artifact response coordination

Proactive Services



- Announcements
- Technology Watch
- Security Audit or Assessments
- Configuration & Maintenance of Security Tools, Applications, & Infrastructures
- Development of Security Tools
- Intrusion Detection Services
- Security-Related Information Dissemination

Security Quality Management Services



- ✓ Risk Analysis
- ✓ Business Continuity & Disaster Recovery Planning
- ✓ Security Consulting
- ✓ Awareness Building
- ✓ Education/Training
- ✓ Product Evaluation or Certification

Serviços



Reactive Services



- + Alerts and Warnings
- + Incident Handling
 - Incident analysis
 - Incident response on site
 - Incident response support
 - Incident response coordination
- + Vulnerability Handling
 - Vulnerability analysis
 - Vulnerability response
 - Vulnerability response coordination
- + Artifact Handling
 - Artifact analysis
 - Artifact response
 - Artifact response coordination

Proactive Services



- Announcements
- Technology Watch
- Security Audit or Assessments
- Configuration & Maintenance of Security Tools, Applications, & Infrastructures
- Development of Security Tools
- Intrusion Detection Services
- Security-Related Information Dissemination

Security Quality Management Services



- ✓ Risk Analysis
- ✓ Business Continuity & Disaster Recovery Planning
- ✓ Security Consulting
- ✓ Awareness Building
- ✓ Education/Training
- ✓ Product Evaluation or Certification

Serviços



Reactive Services



- + Alerts and Warnings
- + Incident Handling
 - Incident analysis
 - Incident response on site
 - Incident response support
 - Incident response coordination
- + Vulnerability Handling
 - Vulnerability analysis
 - Vulnerability response
 - Vulnerability response coordination
- + Artifact Handling
 - Artifact analysis
 - Artifact response
 - Artifact response coordination

Proactive Services



- Announcements
- Technology Watch
- Security Audit or Assessments
- Configuration & Maintenance of Security Tools, Applications, & Infrastructures
- Development of Security Tools
- Intrusion Detection Services
- Security-Related Information Dissemination

Security Quality Management Services



- ✓ Risk Analysis
- ✓ Business Continuity & Disaster Recovery Planning
- ✓ Security Consulting
- ✓ Awareness Building
- ✓ Education/Training
- ✓ Product Evaluation or Certification

Serviços



Reactive Services



- + Alerts and Warnings
- + Incident Handling
 - Incident analysis
 - Incident response on site
 - Incident response support
 - Incident response coordination
- + Vulnerability Handling
 - Vulnerability analysis
 - Vulnerability response
 - Vulnerability response coordination
- + Artifact Handling
 - Artifact analysis
 - Artifact response
 - Artifact response coordination

Proactive Services



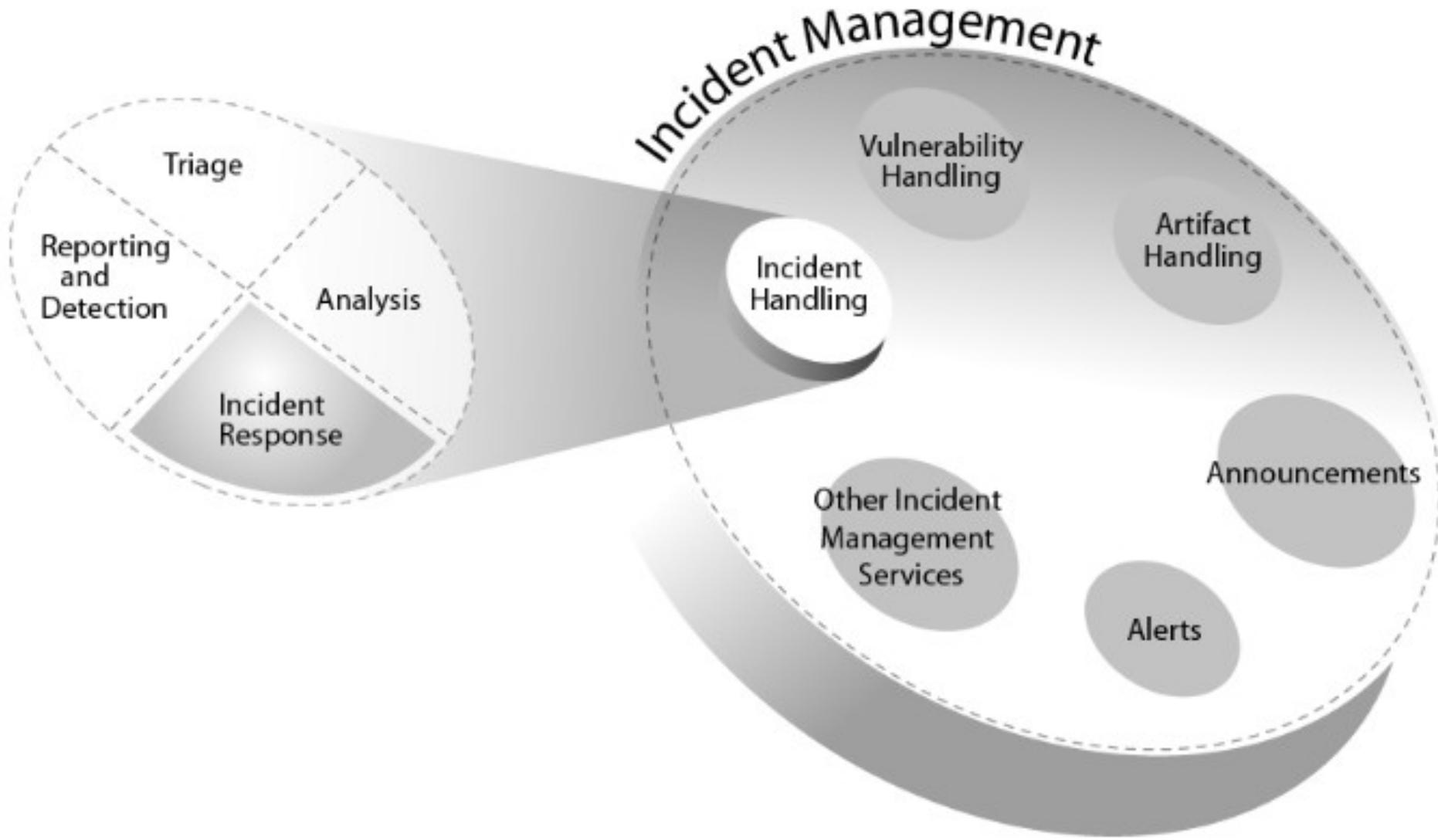
- Announcements
- Technology Watch
- Security Audit or Assessments
- Configuration & Maintenance of Security Tools, Applications, & Infrastructures
- Development of Security Tools
- Intrusion Detection Services
- Security-Related Information Dissemination

Security Quality Management Services

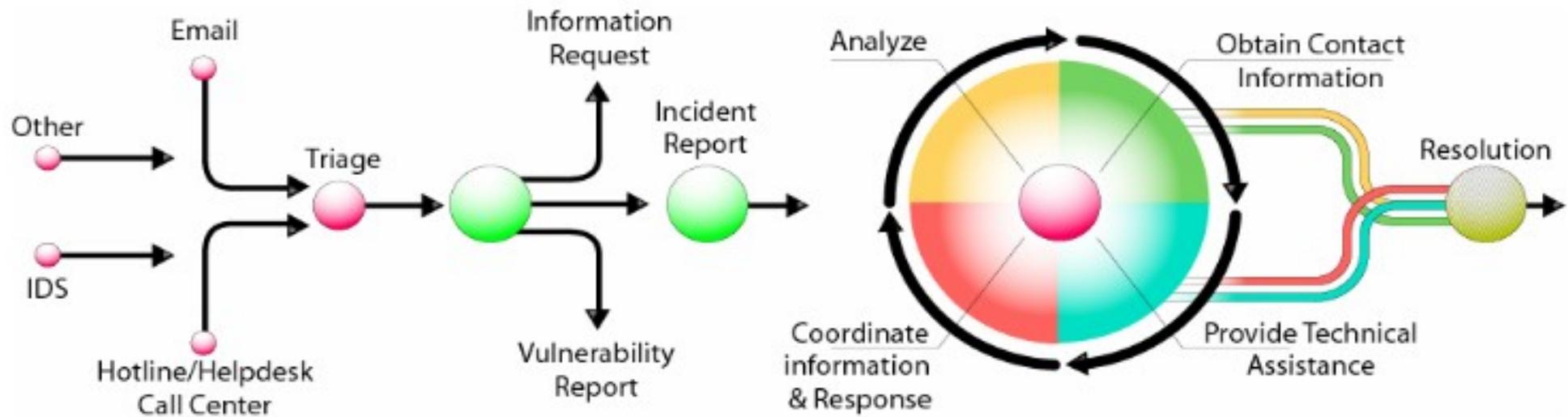


- ✓ Risk Analysis
- ✓ Business Continuity & Disaster Recovery Planning
- ✓ Security Consulting
- ✓ Awareness Building
- ✓ Education/Training
- ✓ Product Evaluation or Certification

Incident Management



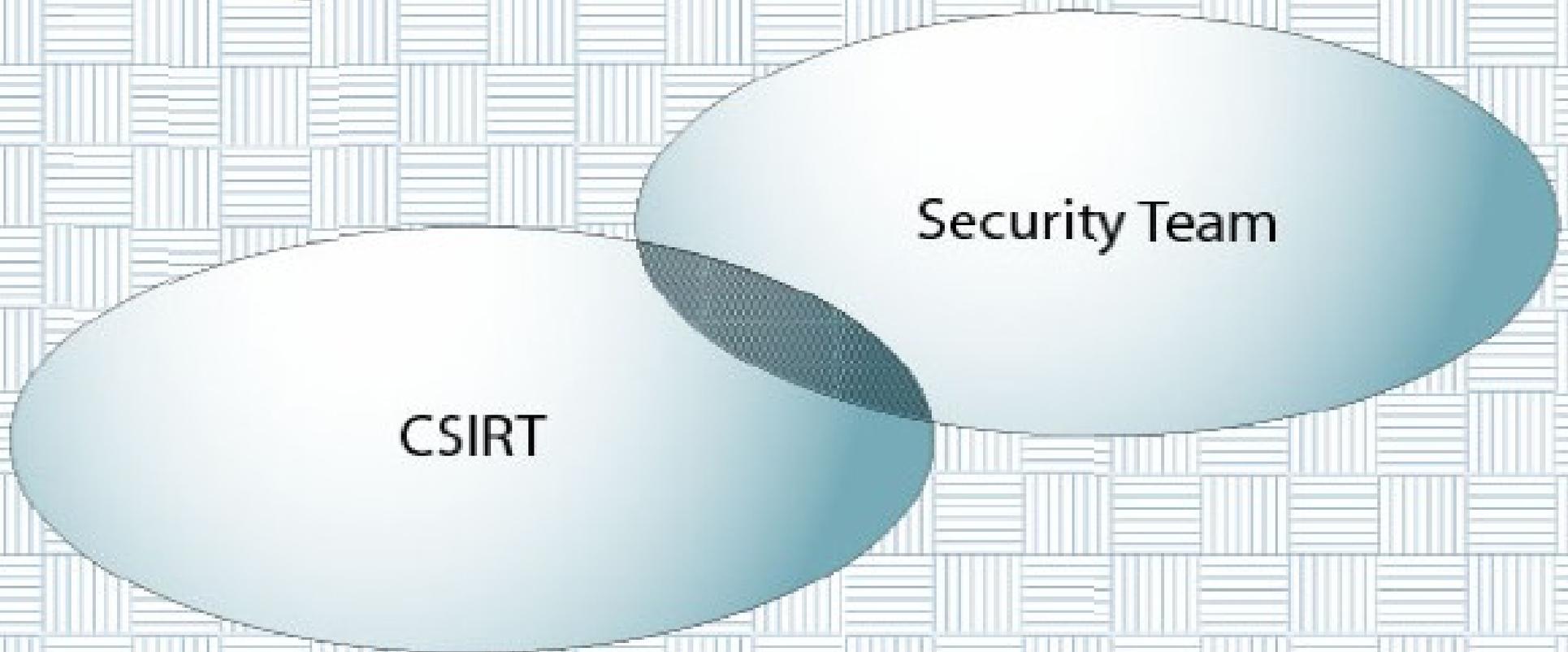
Processo de Resposta a Incidentes



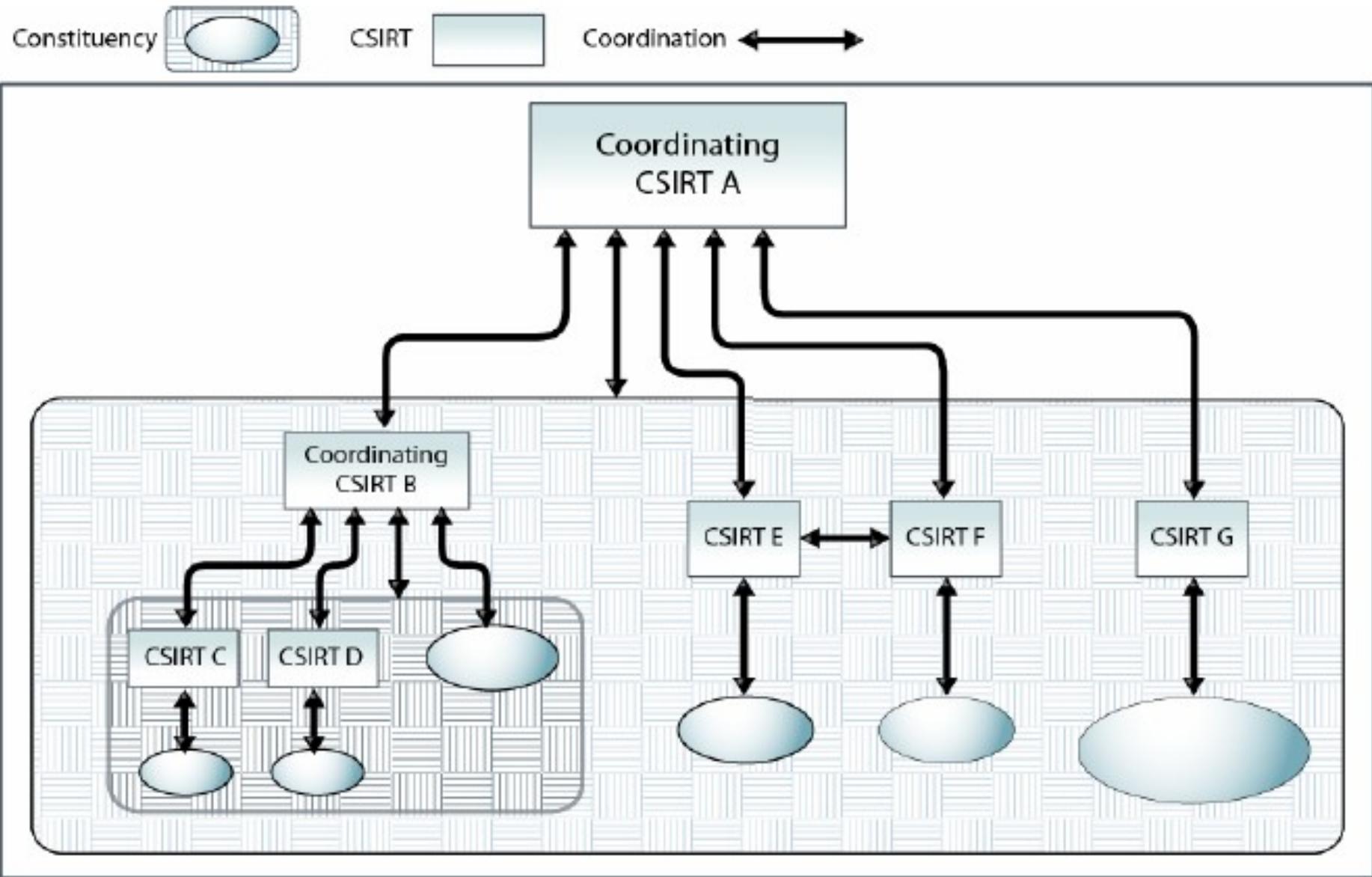
Equipe



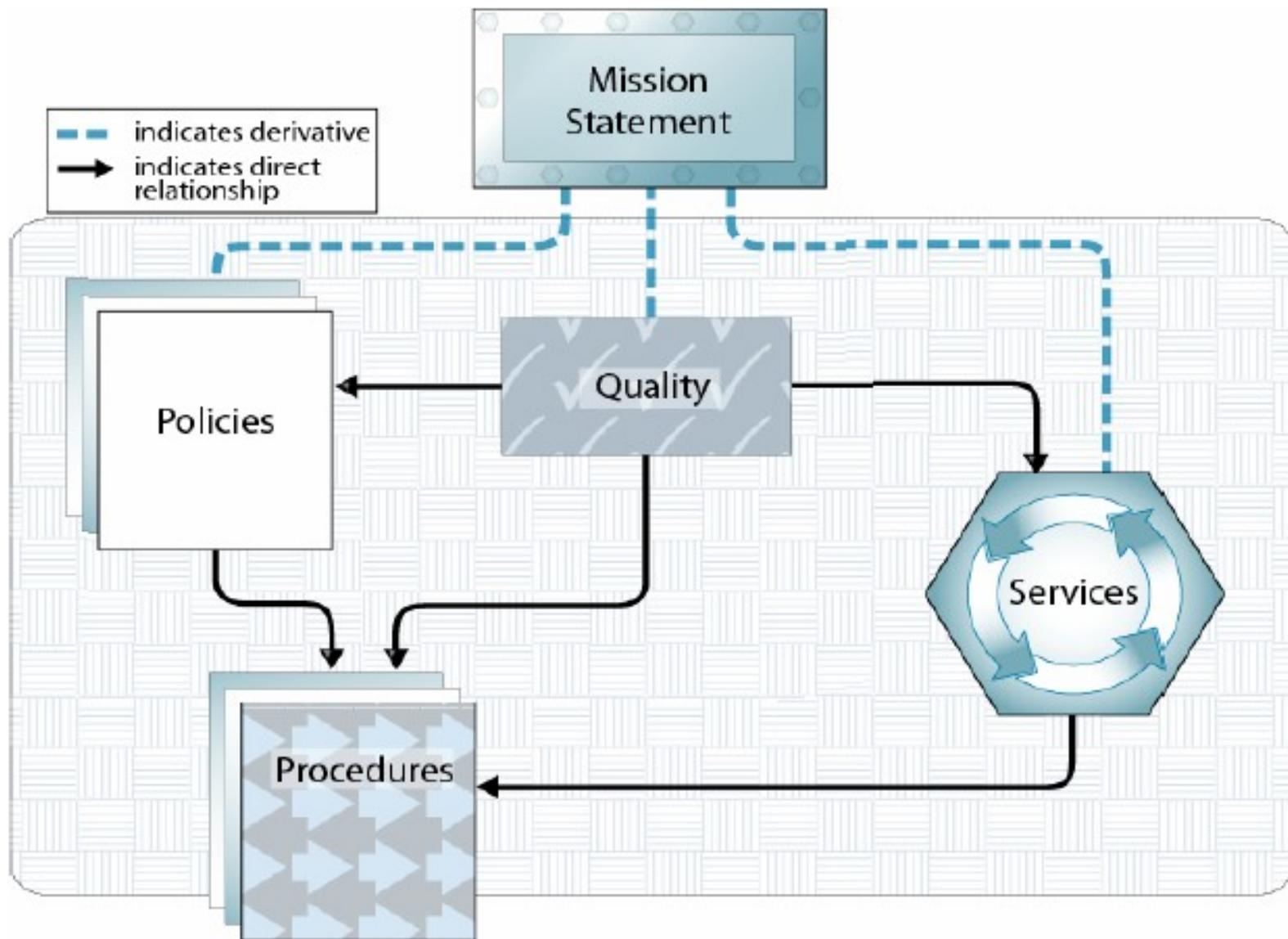
Parent Organization



Relações entre CSIRTs



Relação entre missão e serviços



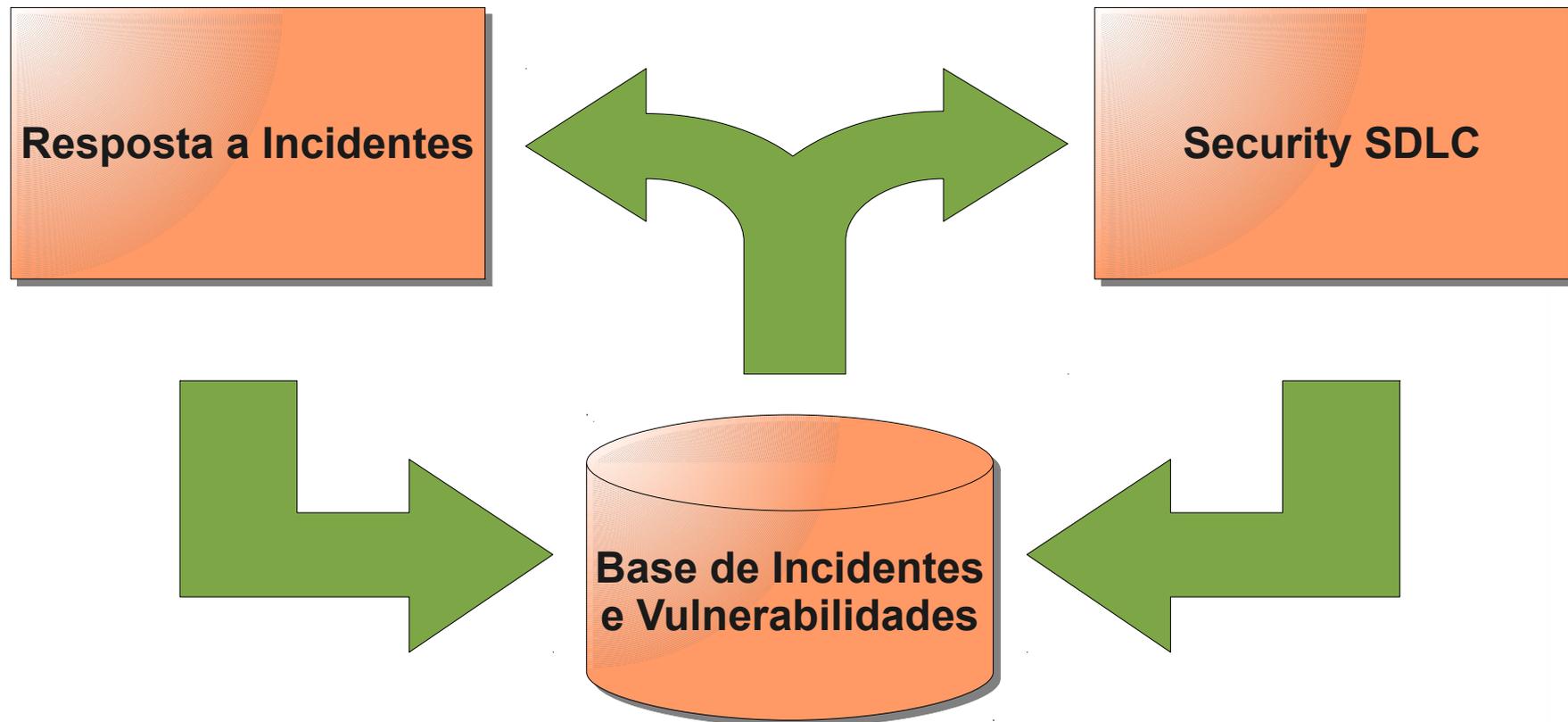
Modelos Organizacionais



- **Coordenação**
- **Ad-hoc**
- **Centralizado**
- **Distribuído**
- **Distribuído com Coordenação Centralizada**

Integração com SDLC

- **Resposta a Incidentes fornece subsídios que podem ser utilizados no início do SDLC;**





Microsoft Security Response Center

[HOME](#)[WHAT WE DO](#)[REPORT A VULNERABILITY](#)[COMMUNITY COLLABORATION](#)

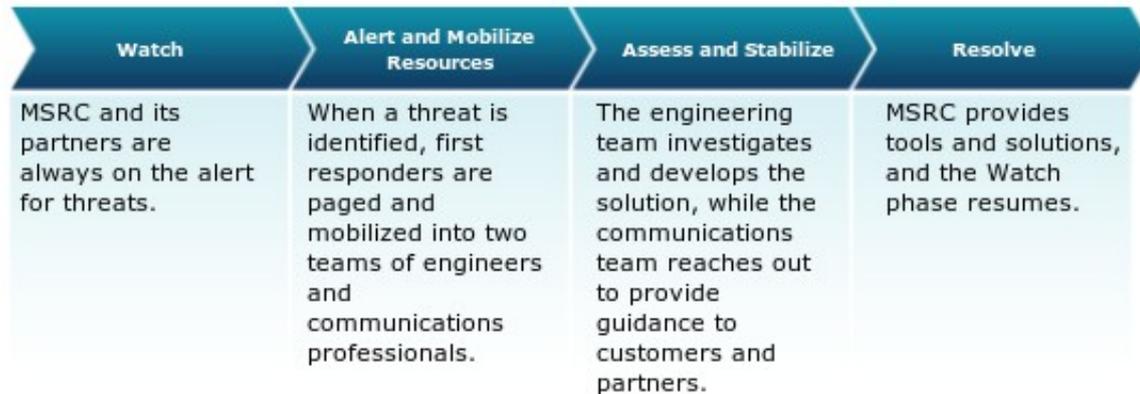
Responding to Security Incidents



The Microsoft Security Response Center (MSRC) uses Microsoft's worldwide Software Security Incident Response Process (SSIRP) to understand security incidents quickly, and then investigate, analyze, and resolve those incidents. Security incidents are situations that arise when malicious users exploit vulnerabilities. The MSRC provides customers with the necessary information, guidance, mitigation steps, and tools to react appropriately.

Software Security Incident Response Process (SSIRP)

The SSIRP is defined by four phases:



Security Update Guide

The Security Update Guide was created to help IT professionals better understand and use Microsoft security release information, processes, communications, and tools. [Check out the summary or download the Guide now.](#)



Related Links

[Releasing Security Updates, Bulletins, and Advisories](#)[Conducting Technical Investigations](#)

IBM Product Security Incident Response

Public Blogs

Search

Browse Blogs

My Blog

My Updates

▼ Vulnerability severity ratings

[Low-severity](#)

[Medium-severity](#)

[High-severity](#)

▼ IBM Brands

[Application Integration](#)

[Middleware \(WebSphere\)](#)

[Business Analytics](#)

[IBM Collaboration Solutions \(Lotus\)](#)

[IBM Security Systems](#)

[IBM System Storage](#)

[IBM Power Systems](#)

[IBM System x](#)

[IBM Systems Software](#)

IBM Product Security Incident Response Blog

This page contains important information regarding security vulnerabilities that may affect IBM products and solutions. IBM PSIRT follows the NIST guidelines for determining the severity rating of the reported vulnerability - see "[NVD Vulnerability Severity Ratings](#)" for details. Please use this information to take the appropriate actions.

In our effort to serve you better, we recommend that you subscribe to RSS feed for notification of future IBM Security Bulletins and advisories posted on this blog. The short URL for this blog is <https://www.ibm.com/blogs/PSIRT>

1 - 15 of 26

Page 1 | 2

[Previous](#) | [Next](#)

Sort by: [Date](#) | [Title](#) | [Most Recommendations](#) | [Most Comments](#) | [Most Visits](#)

Security Bulletin: Potential security vulnerability when using Web based applications on IBM WebSphere Application Server due to Java HashTable implementation vulnerability (PM53930) (CVE-2012-0193)

IBM PSIRT | Tuesday 4:53 PM | Tags: [websphere](#) [psirtmedium](#) [java](#) [psirtaim](#)

[Comments \(0\)](#) | [Visits \(104\)](#)

IBM WebSphere Application Server is susceptible to a potential denial of service condition when using Web based applications due to a JavaHashTable implementation vulnerability. CVE(s): CVE-2012-0193 Affected product(s): IBM WebSphere Application Server Affected version(s): 6.0, 6.0.0.2,

▼ Resources

[→ IBM Secure Engineering Practices](#)

[→ About IBM PSIRT](#)

[→ IBM PSIRT Process](#)

[→ Report Security Issue](#)

▼ Feeds

[Feed for Blog Entries](#)

[Feed for Blog Comments](#)

▼ Archive

[January 2012](#)

[December 2011](#)

[November 2011](#)



Software Engineering Institute
Carnegie Mellon

search



[Publications Catalog](#)

[HOME](#) | [Software Assurance](#) | [Secure Systems](#) | [Organizational Security](#) | [Coordinated Response](#) | [Training](#)

Software Assurance

- [Secure Coding](#)
- [Vulnerability Analysis](#)
- [Function Extraction \(FX\)](#)

related links

- [Publications Catalog](#)
- [Historical Documents](#)
- [CERT Coordination Center](#)
- [CERT/CC Blog](#)
- [US-CERT Vulnerability Notes Database](#)
- [Vulnerability Disclosure Policy](#)
- [Courses](#)
- [Build Security In](#)

US-CERT
www.us-cert.gov

Secure Coding

Easily avoided software defects are a primary cause of commonly exploited software vulnerabilities. CERT staff has observed, through an analysis of thousands of vulnerability reports, that most vulnerabilities stem from a relatively small number of common programming errors. By identifying insecure coding practices and developing secure alternatives, software developers can take practical steps to reduce or eliminate vulnerabilities before deployment.

As part of the CERT Secure Coding Initiative, members of the Secure Coding team work with software developers and software development organizations to reduce vulnerabilities resulting from coding errors before they are deployed. We strive to identify common programming errors that lead to software vulnerabilities, establish standard secure coding standards, educate software developers, and to advance the state of the practice in secure coding.

Areas of Work

Secure Coding Standards

The CERT Program is working with the software development and security communities to develop standards for commonly used programming languages. We

Podcasts and Videos

ROBERT C. SEACORD | senior vulnerability analyst - CERT/CC

Secure Coding Initiative: Project - 12.02.2008 - Featuring Robert S

Casos de Sucesso do SERPRO



- **Sem infecções em larga escala desde Agobot (2005);**
- **Resistência ao Conficker;**
- **Resistência aos ataques de DDOS em 2011;**
- **Nenhuma invasão aos sítios desenvolvidos pelo SERPRO e sistemas críticos durante os ataques de 2011;**
- **Assinatura do IDS SNORT, capaz de detectar o Ultrasurf, distribuída na comunidade internacional;**



O fator humano é fundamental.

Nenhuma tecnologia foi capaz de substituir o Analista



Obrigado!

daniel.melo@serpro.gov.br

Bibliografia

- **Secure Coding – Principles and Practices. Mark G. Graff, Kenneth Wyk. Editora O'reilly.**
- **CSIRT – Handbook - www.cert.org.**