nic.br cgi.br cert.br

LAC-CSIRTs Meeting
LACNIC 32 / LACNOG 2019
October 10, 2019 – Panamá

FIRST CSIRT Services Framework

Dr. Cristine Hoepers
General Manager
cristine@cert.br

cert.br nic.br cgi.br

About CERT.br

cert.br nic.br cgi.br

Incident Management

- Coordination
- Technical Analysis
- Support for recovery

Training and Awareness

- Courses
- Presentations
- Best Practices
- Meetings

Trend Analysis

- Distributed Honeypots
- SpamPots
- Processing of threat feeds

FIRST Improving Security Together MEMBER

APWG RESEARCH PARTNER www.antiphishing.org

CARNEGIE MELLON UNIVERSITY SOFTWARE ENGINEERING INSTITUTE | SEI Partner Network

The Honeynet PROJECT

Creation:

August/1996: report with a proposed model for incident management for the country is published by the Brazilian Internet Steering Committee – CGI.br[1]

June/1997: CGI.br creates CERT.br (at that time called NBSO – *NIC BR Security Office*) based on the report's recommendations[2]

[1] https://www.nic.br/grupo/historico-gts.htm | [2] https://www.nic.br/pagina/gts/157

Mission

To increase the level of security and incident handling capacity of the networks connected to the Internet in Brazil.

Focus of the Activities

- National focal point for security incident reports
- Support technical analysis and the understanding of attacks and threats
- Develop collaborative relationships with other entities
- Increase the capacity of incident detection, event correlation and trend analysis in the country
- Transfer the acquired knowledge through courses, best practices and awareness materials

FIRST CSIRT Services Framework

cert.br nic.br cgi.br

TLP:WHITE

FIRST CSIRT *Services Framework v2.0*

High level description of services that can be offered

- by a CSIRT
- by other teams that provide incident management services

It is the new “CSIRT Services” document

These are Best Practices from the FIRST perspective

- To help CSIRTs to
  - identify and choose main services
  - a starting point for standard’s terms and definitions to be used by the community
- What this document is **not**
  - it does not explain how to create a CSIRT
  - does not cover CSIRT maturity issues

Computer Security Inciden
Services Framework
Version 2.0 (Review Releas

FIRST.Org, Inc. (www.first.org)

Forum of Incident Response and Security Teams

Table of Contents

Version 2.0.1 (Review) 3

https://www.first.org/education/csirt_services_framework_v2.0

CSIRT *Services Framework v2.0:* Authors

TLP:WHITE

Editor

- Klaus-Peter Kossakowski, Hamburg University of Applied Science

Service Area Coordinators

- Olivier Caleff, OpenCSIRT Foundation (FR)
- Cristine Hoepers, CERT.br (BR)
- Amanda Mullens, CISCO (US)
- Samuel Perl, CERT/CC (US)
- Daniel Roethlisberger, Swisscom (CH)
- Robin M. Ruefle, CERT/CC (US)
- Mark Zajicek, CERT/CC (US)

Contributors

- Vilius Benetis, NRD CIRT (LT)
- Angela Horneman, CERT/CC (US)
- Allen Householder, CERT/CC (US)
- Art Manion, CERT/CC (US)
- Sigitas Rokas, NRD CIRT (LT)
- Mary Rossell, Intel (US)
- Désirée Sacher, Finanz Informatik (DE)
- Krassimir T. Tzvetanov, Fastly (US)

TLP:WHITE

CSIRT *Services Framework v2.0*: Service Areas

Information Security Event Management

- Monitoring and Detection
- Analyzing

Information Security Incident Management

- Accepting Reports
- Analyzing Incidents
- Analyzing artefacts and forensic evidence
- Mitigation and recovery
- Coordination

Vulnerability Management

- Vulnerability Discovery
- Report Intake
- Analysis
- Coordination
- Disclosure
- Response

Situational Awareness

- Data Acquisition
- Analysis and Synthesis
- Communication

Knowledge Transfer

- Awareness Building
- Training and Education
- Exercises
- Technical and Policy Advisory

TLP:WHITE

CSIRT *Services Framework v2.0*: Service Areas and Functions

SERVICE AREA 1
INFORMATION SECURITY EVENT MANAGEMENT

Monitoring and Detection
- Log and Sensor Management
- Detection Use Case Management
- Contextual Data Management

Analyzing
- Correlation
- Qualification

SERVICE AREA 2
INFORMATION SECURITY INCIDENT MANAGEMENT

Accepting information security incident reports
- Information Security Incident Report Receipt
- Information Security Incident Triage and Processing
- Information Security Incident Report Handling

Analyzing information security incidents
- Information security incident triage (prioritization and categorization)
- Information collection
- Coordinate any more detailed analysis
- Information security incident root cause analysis
- Cross-incident correlation

Analyzing artifacts and forensic evidence
- Media or surface analysis
- Reverse engineering
- Runtime or dynamic analysis
- Comparative analysis

Mitigation and recovery
- Establishing a response plan
- Applying ad-hoc measures and containment
- Returning all systems back to normal operation
- Supporting other information security entities
- Coordination
- Communication
- Sending notifications
- Distributing relevant information
- Coordinating activities
- Reporting
- Communicating with media

Supporting crisis management
- Distributing information to constituents
- Reporting on cyber security status
- Communicating strategic decisions

SERVICE AREA 3
VULNERABILITY MANAGEMENT

Vulnerability Discovery/Research
- Incident Response Vulnerability Discovery
- Public Source Vulnerability Discovery
- Vulnerability Research

Vulnerability Report Intake
- Vulnerability Report Receipt
- Vulnerability Report Triage and Processing

Vulnerability Analysis
- Vulnerability Triage (Validation and Categorization)
- Vulnerability Root Cause Analysis
- Vulnerability Remediation Development

Vulnerability Coordination
- Vulnerability Notification/Reporting
- Vulnerability Stakeholder Coordination

Vulnerability Disclosure
- Maintain Vulnerability Disclosure Policy and Infrastructure
- Vulnerability Announcement/ Communication/Dissemination
- Post-Vulnerability Disclosure Feedback

Vulnerability Response
- Vulnerability Detection
- Vulnerability Remediation

SERVICE AREA 4
SITUATIONAL AWARENESS

Data Acquisition
- Policy Aggregation, Distillation, and Guidance
- Mappings of assets to functions, roles, actions and key risks
- Collection
- Data Processing and Preparation

Analysis and Synthesise
- Projection and Inference
- Event Detection (through Alerting and/or Hunting)
- Situational Impact

Communication
- Internal and External Communication
- Reporting and Recommendations
- Implementation

SERVICE AREA 5
KNOWLEDGE TRANSFER

Awareness Building
- Research and Information Aggregation
- Development of Reports and Awareness Materials
- Dissemination of Information
- Outreach

Training and Education
- Knowledge, Skill, and Ability Requirements Gathering
- Development of Educational and Training Materials
- Delivery of Content
- Mentoring
- CSIRT Staff Professional Development

Exercises
- Requirements Analysis
- Format and Environment Development
- Scenario Development
- Executing Exercises
- Exercise Outcome Review

Technical and Policy Advisory
- Risk Management Support
- Business Continuity and Disaster Recovery Planning Support
- Policy Support
- Technical Advice

Next Steps

- The document is currently being reviewed to
  - incorporate first round of reviews
  - include graphical representations of service areas relationship

- It will be opened again for a final public review until the end of year

- Further work will be carried out as part of the CSIRT Framework Development SIG

  The state-of-the-art for CSIRTs could still improve considerably by extending and improving the available set of foundational frameworks and materials. The SIG will seek to involve experts interested in that work and provide a community to discuss improvements in need, existing gaps and (potential) new developments – taking into account, and collaborating where appropriate, initiatives from within FIRST and other entities/communities aiming for similar objectives (like APCERT, ENISA, GFCE, ITU, LACNIC, OCF, OAS, TF-CSIRT, etc.).

  https://www.first.org/global/sigs/csirt/

Thank You

cristine@cert.br

Incident reports to: cert@cert.br @certbr

www.cert.br

October 10, 2019

nic.br cgi.br

www.nic.br | www.cgi.br