Introduction to Computer Security Incident Response Team (CSIRT)

October 10 – 12, 2016 Republic of Guinee

By

Marcus K. G. Adomey

OVERVIEW

- CSIRT Definition
- CSIRT Brief History
- CSIRT in the World
- CSIRT in Africa
- CSIRT Constituency
- CSIRT Types
- CSIRT Services
- CSIRT Mission
- CSIRT Policies and Procedures
- CSIRT Tools
- CSIRT Organizational Placement
- CSIRT Organizational Models
- CSIRT Authority
- CSIRT Relationships with Other Teams
- CSIRT Staffing
- CSIRT Funding and Cost

CSIRT Definition

CSIRT Definition

A Computer Security Incident Response Team (CSIRT) is an organization or team that provides, to a well-defined constituency, services and support for both preventing and responding to computer security incidents

CSIRT Definition

CSIRT Acronyms

Various acronyms and titles have been given to CSIRT organizations over the years. These titles include

- CERT - Computer Emergency Response Team
- CSIRC - Computer Security Incident Response Capability or Center
- CIRC - Computer Incident Response Capability or Center
- CIRT - Computer Incident Response Team
- IHT - Incident Handling Team
- IRC - Incident Response Center or Incident Response Capability
- IRT - Incident Response Team
- SERT - Security Emergency Response Team
- SIRT - Security Incident Response Team

Brief History of CSIRT

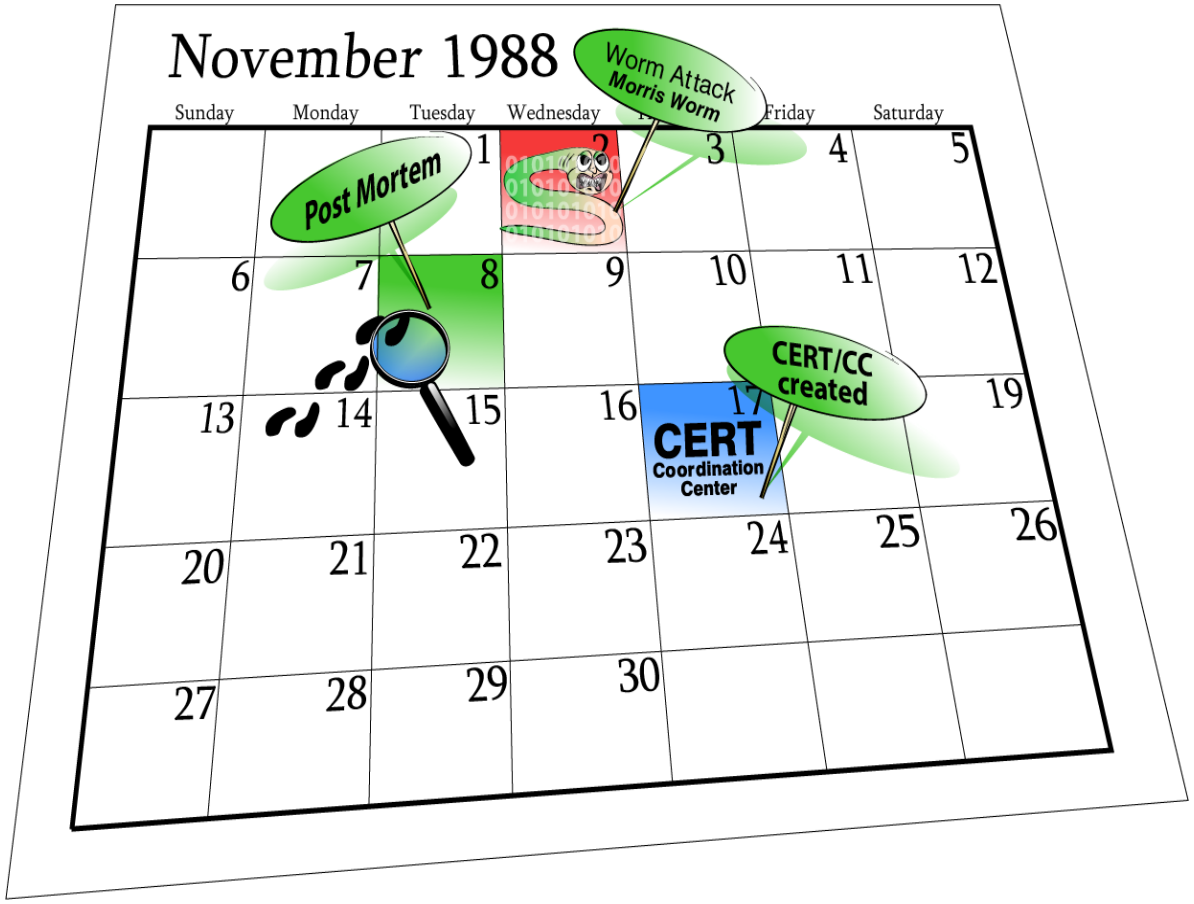
Brief History of CSIRT

- Robert Tappan Morris then student at Cornell University launched on November 2, 1988 from MIT the first and fast self-replicating computer worms via the Internet
- Crippled almost 10% (6000) of the computer connected to the Internet in Nov 1988.
- He was sentenced to three years probation, 400 hours of community service, a fine of $10,050 plus the costs of his supervision.

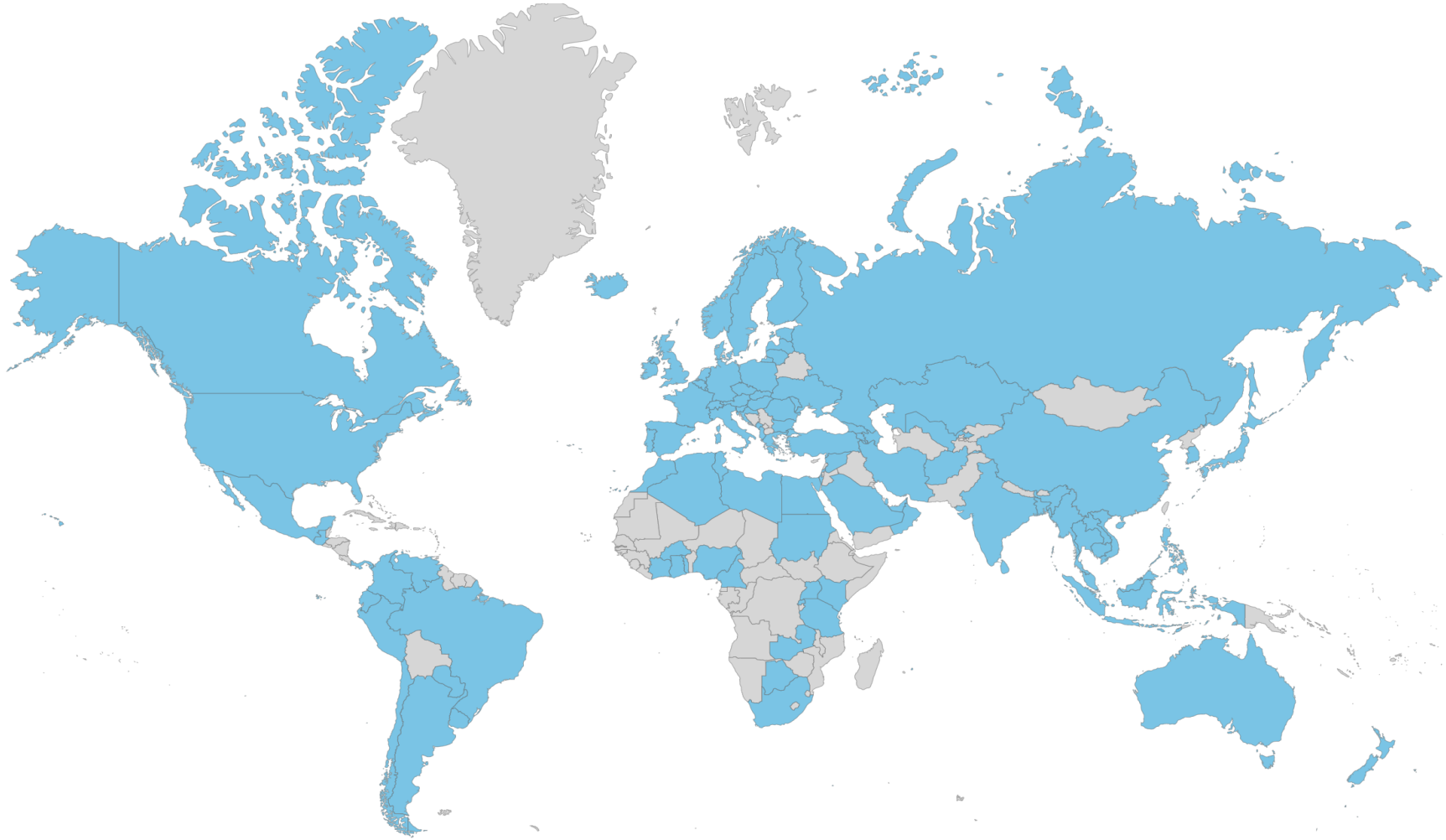
Morris is accompanied by his mother, Anne, left, and his father, Robert Sr., at right rear, after a day of jury selection in his trial on charges of infiltrating a nationwide computer network in Nov. 1988

Brief History of CSIRT

- By on the 7th November 1988, the resolution of this incident was done through an international collaboration
- Characterized by duplication of effort and waste of resources
- To face any future form of such attack, avoid the duplication of effort, waste of resources and collectively resolve, the first CERT was created on the 17 November 1988.



CSIRT in the World

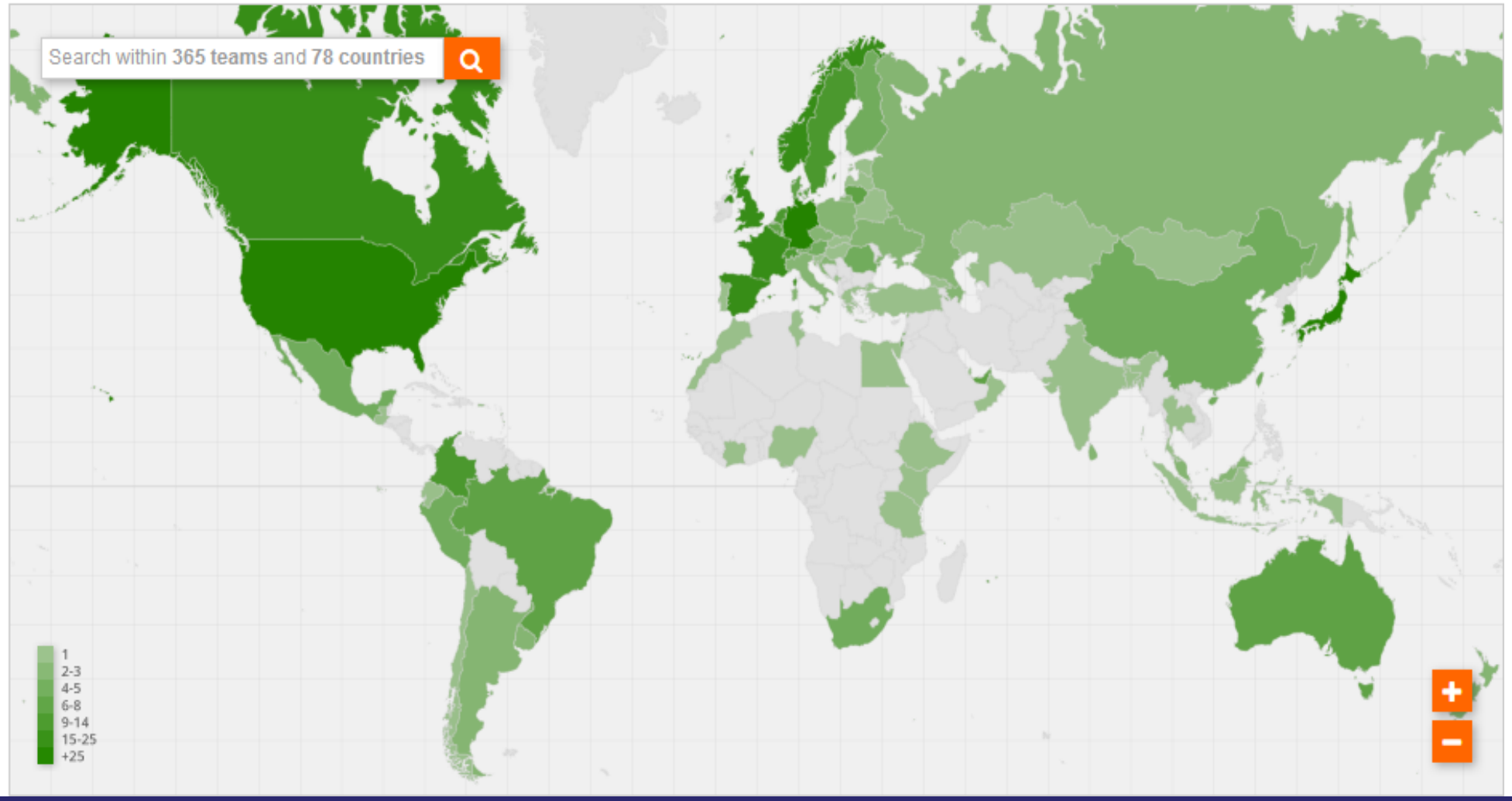


ITU

ORGANISATION INTERNATIONALE DE la francophonie

AfricaCERT
United in promoting cyber security in Africa

CSIRT in the World – From FIRST Perspective



ITU

ORGANISATION INTERNATIONALE DE la francophonie

AfricaCERT
United in promoting cyber security in Africa

CSIRT Framework

CSIRT FRAMEWORK

- Constituency
- Mission
- CSIRT Authority
- CSIRT Organizational Placement
- Policy and procedures
- Models and Legal Basis of Cooperation

CSIRT Constituency

CSIRT Framework

Constituency

The constituency is the organization (or group of organizations) and/or people whose incidents CSIRT handles (or coordinates)

A Constituency could be

- An army
- National Security
- A Police
- University
- Banks
- Heath System
- ISP
- Telcos
- Grids Power
- Ministry of Finance (Accountant General)
- Software Development Company
- Etc.

CSIRT Services

- ❑ **Reactive**
- ❑ **Proactive**
- ❑ **Security Quality Management**

CSIRT Framework

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*

CSIRT Framework

Proactive Services

- Announcements
- Technology Watch
- Security Audits or Assessments
- Configuration and Maintenance of Security
- Development of Security Tools
- Intrusion Detection Services
- Security-Related Information Dissemination

CSIRT Framework

Security Quality Management

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

Type of CSIRTs

Type of CSIRT

There could be some of the following CSIRT:

- Government CSIRT
  - Military CSIRT
  - Police CSIRT
  - National Security CSIRT
  - Finance CSIRT
  - Health CSIRT
  - Etc.
- Academic CSIRT
- ISP CSIRT
- Bank CSIRT
- Industry CSIRT

CSIRT Mission

CSIRT Mission

- A mission statement is a statement that defines the essence or purpose of a company or organization. It answers the question, "Why do we exist?“
- Consist of at least three or four sentences used by an organization to explain, in simple and concise terms, their purposes for being.
- be non-ambiguous
- be imperative to enable the CSIRT to establish a service and quality framework, including the nature and range of services provided, the definition of its policies and procedures, and the quality of service.

If the team is housed within a large organization or is funded from an external body, the CSIRT mission statement must complement the mission of those organizations

CSIRT Mission

Example of Mission Statement

SingCERT's Mission Statement:

"One Point of Trusted Contact

Facilitate Security Threats Resolution

Increase National Competency in IT Security"

Fictitious CERT mission statement:

"Fictitious CERT provides information and assistance to the staff of its hosting company to reduce the risks of computer security incidents as well as responding to such incidents when they occur."

Vision Statement

- Must be clear to **project the end goal of the CSIRT**
- Must **complement** the **mission statement of the CSIRT**.
- It should **reflect what the CSIRT aims to attain**.
- **Be realistic**

Sample Vision Statement:

1. X-CIRT's vision is to be a trusted global leader in cybersecurity - collaborative, agile, and responsive in a complex environment.
2. Y-CIRT will work to help create a safe, clean and reliable cyber space in its Region through global collaboration

CSIRT Policies and Procedures

Policies and Procedures

All services and CSIRT functions should be supported by well-defined policies and procedures.

A documented set of policies and procedures is vital to

- ✓ ensure that team activities support the CSIRT mission
- ✓ set expectations for confidentiality
- ✓ provide the framework for day-to-day operational needs
- ✓ maintain consistency and reliability of service

Policies and Procedures

Example Policies

- security policy
- open reporting environment policy
- incident reporting policy
- incident handling policy
- external communications policy
- media relations policy
- information disclosure policy
- information distribution policy
- human error policy
- training and education policy
- CSIRT acceptable use policy

Policies and Procedures

Example Procedures

- standard operating procedures (SOPs)
- accepting and tracking incident reports
- answering the hotline
- incident and vulnerability handling
- gathering, securing, and preserving evidence
- configuration of CSIRT networks and systems
- system and network monitoring and intrusion detection
- backing up and storing incident data
- notification processes (how information is packaged, distributed, archived, etc.)
- training and mentoring

CSIRT Organizational Placement

CERT Organizational Placement

CSIRT Organizational Placement

- The place that a CSIRT holds in its parent organization is tightly coupled to its stated mission, its constituency and to its Organizational model.

- There is no clear standard or consistent placement or location of a CSIRT within the organizational reporting structure of a host or parent organization.

CSIRT Organizational Models

Organizational Models for CSIRT

- ❑ Security Team
- ❑ Internal Distributed CSIRT
- ❑ Internal Centralized CSIRT
- ❑ Combined Distributed & Centralized CSIRT
- ❑ Coordinating CSIRT

CSIRT ORGANIZATIONAL MODEL

Security Team

- CSIRT has not been established
- No group or section of the organization has been given the formal responsibility for all incident handling activities
- Incident response efforts are not necessarily coordinated or standardized across the organization
- Network or security administrators at the local or division level handle security events on an ad hoc and sometimes isolated basis as part of their overall responsibilities or job assignments

IT Support Staff

IT Security Team

CSIRT ORGANIZATIONAL MODEL

Internal Distributed CSIRT

- Structured on geographical location or functional responsibilities
- Distributed CSIRT
- Distributed security team(s) perform(s) CSIRT duties
- There is a manager who oversees and coordinates activities

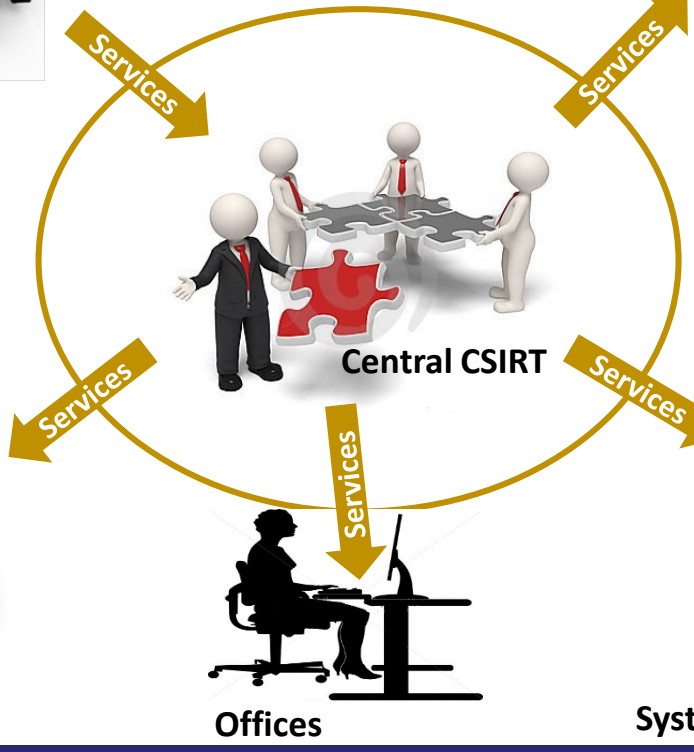
CSIRT ORGANIZATIONAL MODEL

Internal Centralized CSIRT

- The team is centrally located in the organization
- There is a CSIRT manager who reports to high-level management
- CSIRT provides the incident handling services for an organization.
- The CSIRT serves as the single point of contact into the organization
- Staff are full time workers of the CSIRT;

IT Support Unit

End Users



Management

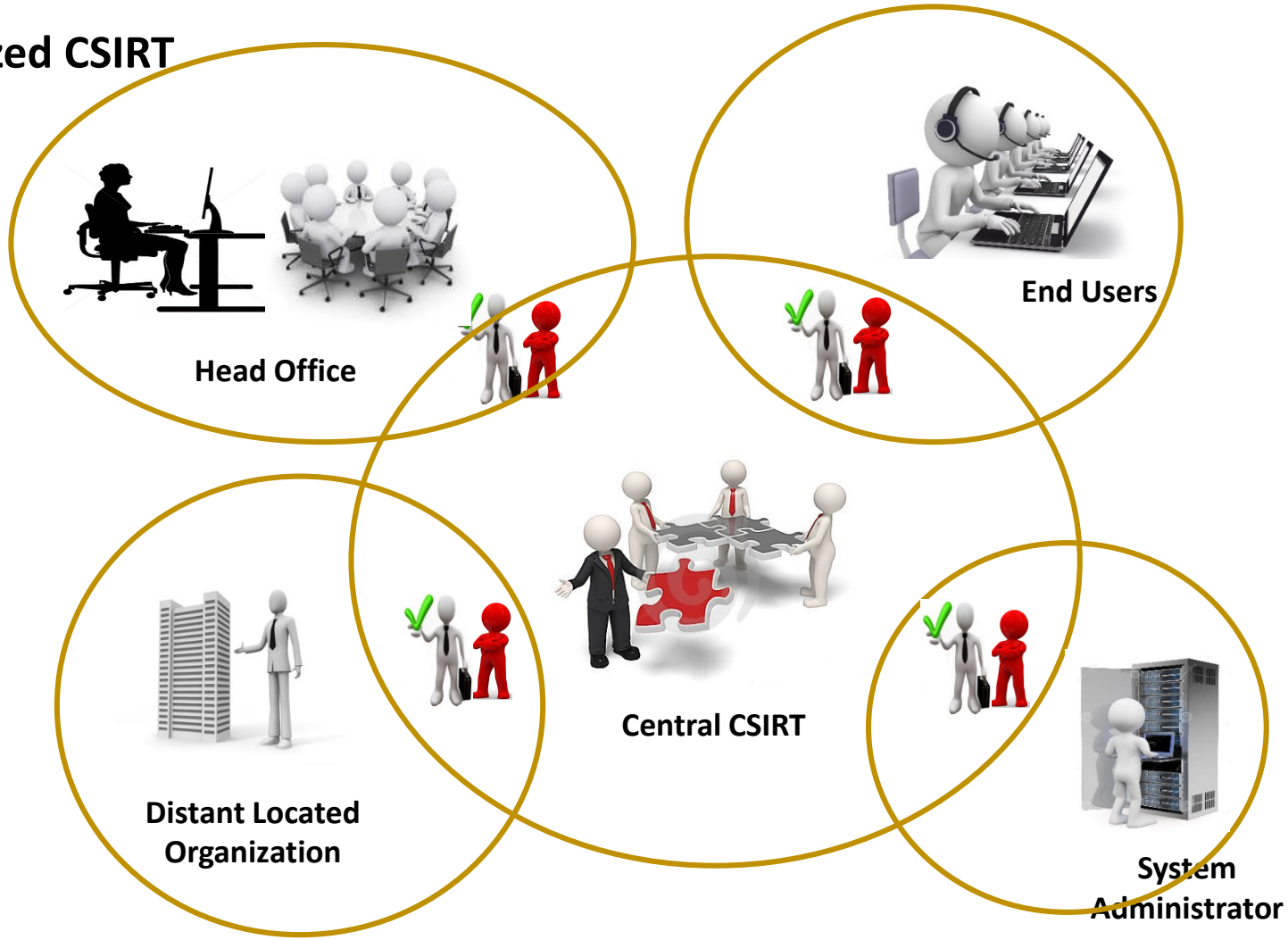
Offices

System Administrator

CSIRT ORGANIZATIONAL MODEL

Internal Combined Distributed and Centralized CSIRT

- This model represents a combination of the distributed CSIRT and the centralized CSIRT
- Uses existing staff in strategic locations throughout the organization with the centrally located coordinating capabilities



CSIRT Authority

CSIRT Authority

There are three levels of authority or relationships that a CSIRT can have with its constituency

- **Full authority**: The CSIRT can make decisions, without management approval, to direct response and recovery actions.
- **Shared authority**: The CSIRT participates in the decision process regarding what actions to take during a computer security incident, but can only influence, not make the decision.
- **No authority**: The CSIRT cannot make any decisions or take any actions on its own. The CSIRT can only act as an advisor to an organization, providing suggestions, mitigation strategies, or recommendations.

CSIRT ORGANIZATIONAL MODEL

Non-Authoritative CSIRT

Advisories, Alerts and Recommendations

Information Feedback

Security Team | Functional Unit | CSIRT | CSIRT

Authoritative CSIRT

Direction and Delegation

Reports

Security Team | Functional Unit | CSIRT | CSIRT

CSIRT Relationships with Other Teams

RELATIONSHIP TO OTHER TEAMS

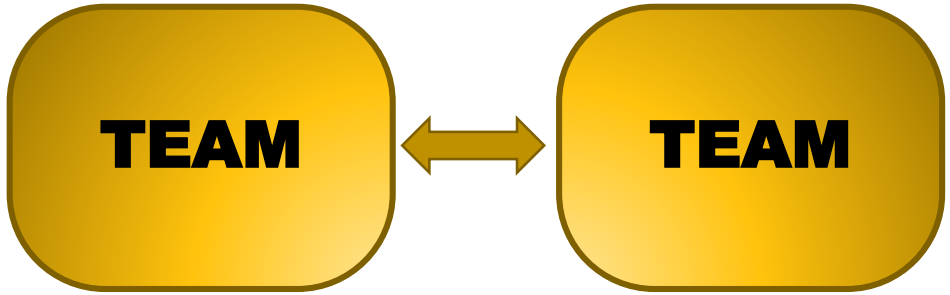
- The realm of CERTs is the Internet, and therefore the world
- There are many constituencies and CERT around the world
- At some level these CERTs have to inter-operate in order to get their job done.
- This cooperation and coordination effort is at the very heart of the CERT framework

RELATIONSHIP TO OTHER TEAMS

Models of cooperation

Bilateral team-team cooperation

- This is a model of a bilateral cooperation between two teams only.
- It is based on the trust between particular teams and their members, usually built over years, for example through joined participation in security projects.
- This kind of cooperation is often stimulated by common goals for future development and similar team missions.

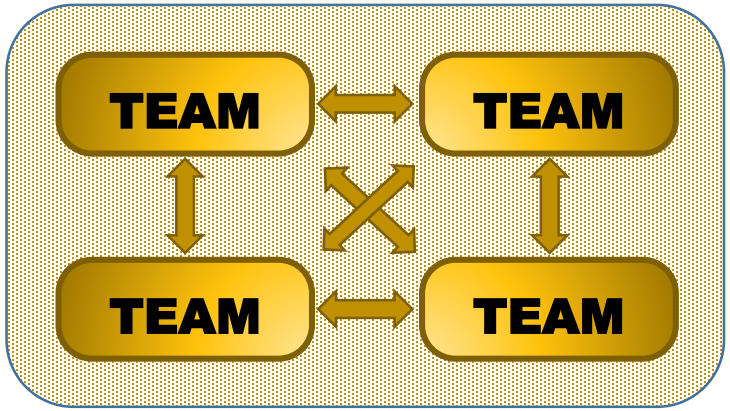


RELATIONSHIP TO OTHER TEAMS

Models of cooperation

Association

- The association is a model of cooperation between many teams which have common interests and goals.
- The framework for this kind of cooperation might be set by a common geographical area (like in the national cooperation activities), common sets of services, similar constituencies, sector of operations etc.
- The association model comes with different names: forum, taskforce, group, coalition, alliance etc.

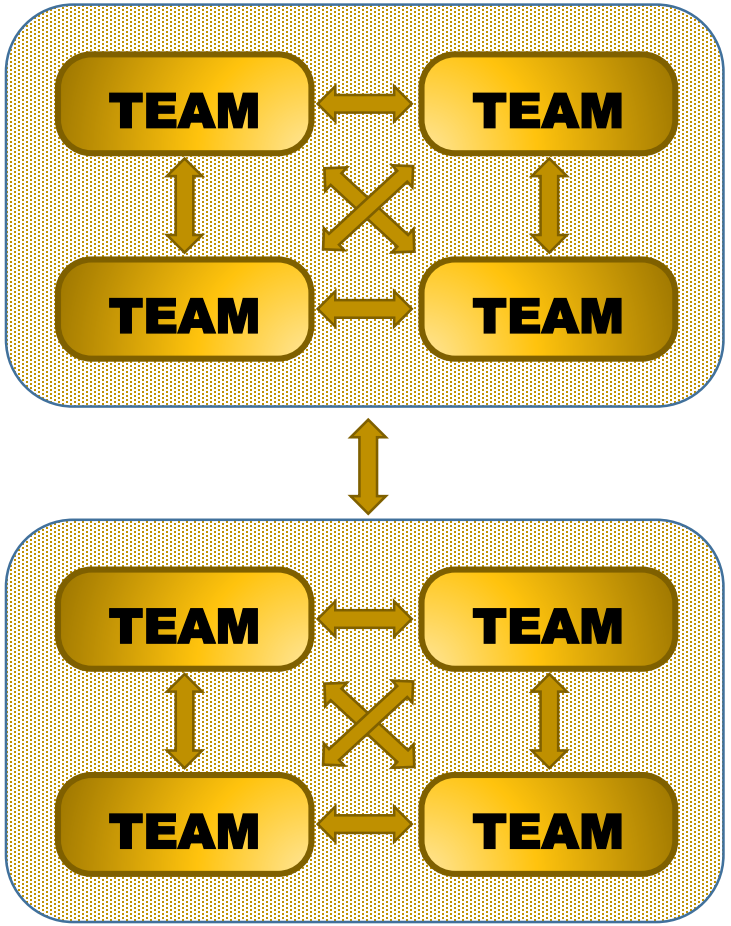


RELATIONSHIP TO OTHER TEAMS

Models of cooperation

Cooperation between associations

- This model depicts cooperation among two or more associations.
- It is usually based on the common goals of both organizations and shared benefits.
- This kind of cooperation is very often realized by exchanging experiences (for example delegates on the organization's meetings) and formulation of common goals and rules of cooperation (for example Memorandum of Understanding)



RELATIONSHIP TO OTHER TEAMS

Legal basis for cooperation

Non-disclosure agreement

- A non-disclosure agreement (NDA), sometimes also called a confidential disclosure agreement (CDA), confidentiality agreement or secrecy agreement, is a legal contract between at least two parties which outlines confidential materials or knowledge the parties wish to share with one another for certain purposes, but wish to restrict from generalized use.
- In other words, it is a contract through which the parties agree not to disclose information covered by the agreement.
- An NDA creates a confidential relationship between the parties to protect any type of trade secret.
- As such, an NDA can protect non-public business information.

RELATIONSHIP TO OTHER TEAMS

Legal basis for cooperation

Memorandum of Understanding

A Memorandum of Understanding (MOU) is a legal document describing a bilateral agreement between parties. It expresses a convergence of will between the parties, indicating an intended common line of action, rather than a legal commitment. It is a more formal alternative to a gentlemen's agreement, but generally lacks the binding power of a contract.

RELATIONSHIP TO OTHER TEAMS

Legal basis for cooperation

Contract

A contract is a "promise" or an "agreement" made of a set of promises. Breach of this contract is recognized by the law and legal remedies can be provided. In civil law, contracts are considered to be part of the general law of obligations. The law generally sees performance of a contract as a duty

RELATIONSHIP TO OTHER TEAMS

Legal basis for cooperation

Terms of Reference

Creating a detailed Terms of Reference is critical to the success of an association, as it defines its purpose of existence:

- Vision, objectives, scope and deliverables (i.e. what has to be achieved)
- Stakeholders, roles and responsibilities (i.e. who will take part in it)
- Resource, financial and quality plans (i.e. how it will be achieved)
- Work breakdown structure and schedule (i.e. when it will be achieved)

Quelques CIRTs

https://tuncert.ansi.tn/publish/content/

http://cert-mu.govmu.org/English/Pages/default.aspx

http://www.cicert.ci/

http://www.cirt.bf/

http://certgh-web.cert-gh.org/index.php/holder/cirt-implementation-in-ghana/

http://www.egcert.eg/


Thank
you