CIRT: Requirements and implementation

By : Muataz Elsadig

Sudan CERT

Joint ITU-ATU Workshop on Cyber-security Strategy in African Countries
Khartoum, Republic of Sudan,
24 – 26 July 2016

CERT or CSIRT

- There is no globally accepted definition of what a "National CSIRT" is, but for sure a national CSIRT is a security team with a national responsibilities; Its community normally include: Critical infrastructure - Government bodies – Other CSIRTs within the country - General public

- **There exist various abbreviations for this entity like:**
  - CERT (Computer Emergency Response Team)
  - CSIRT (Computer Security Incident Response Team)
  - IRT (Incident Response Team)
  - CIRT (Computer Incident Response Team)
  - SERT (Security Emergency Response Team)

National CSIRT Mandate

- Is to be the main focal point in the country(Provide Communication Channel);
- Watch and Worn service (announcements & alerts & warning);
- Capacity Building (training, conference, workshop, drills, …);
- Incident classification and reporting standards .
- Harmonization of legal frame work for information sharing and international Incident handling

National CSIRTs Key Partners

- Government
- Critical infrastructure /operators
- Law enforcement agencies
- Intelligence agencies
- ISPs
- Academia and researchers
- Anti-virus, Software & Hardware vendors
- Regional and international organizations
- International Peers
- Other CSIRTs within the country

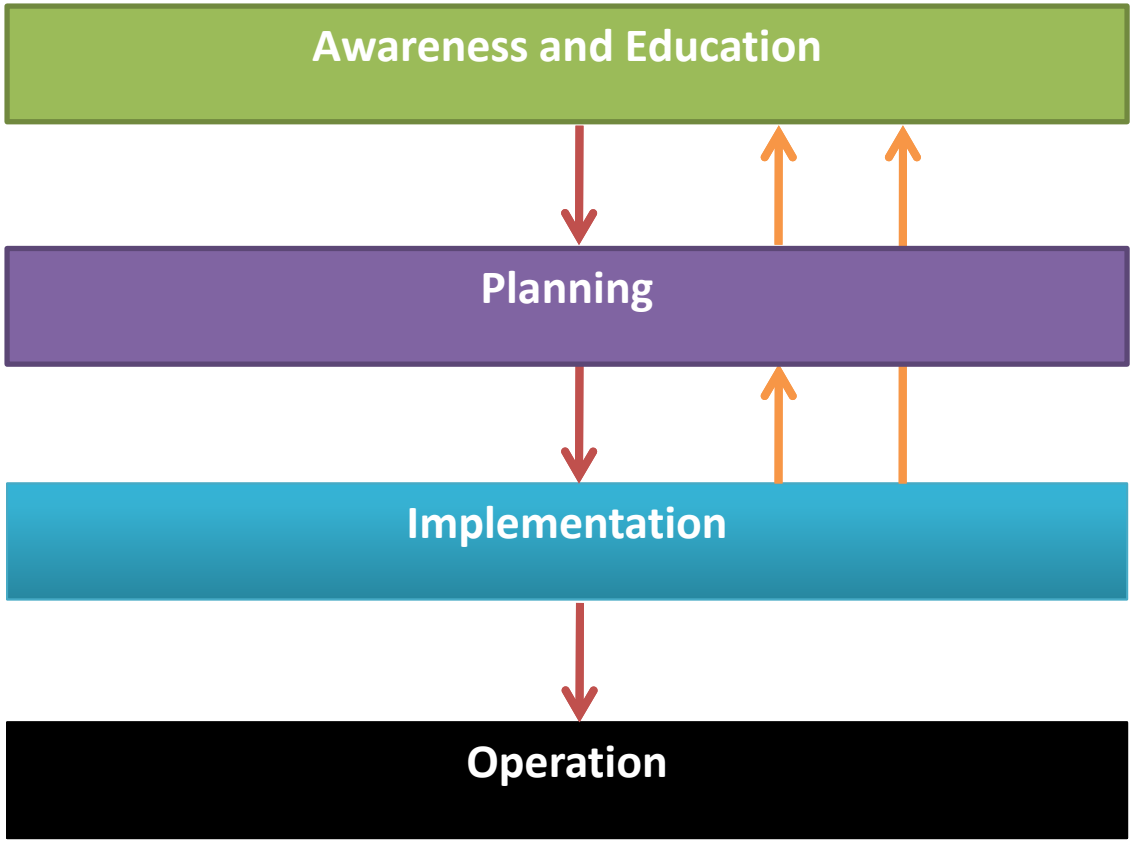
Trends in Internet

- A lot of misconfigured or outdated OSs, vulnerabilities in software, unpatched systems;
- Lack of security awareness by individual users;
- Steady increase in number of incidents;
- Growing dependency on the Internet;
- Easy connectivity to the Internet;

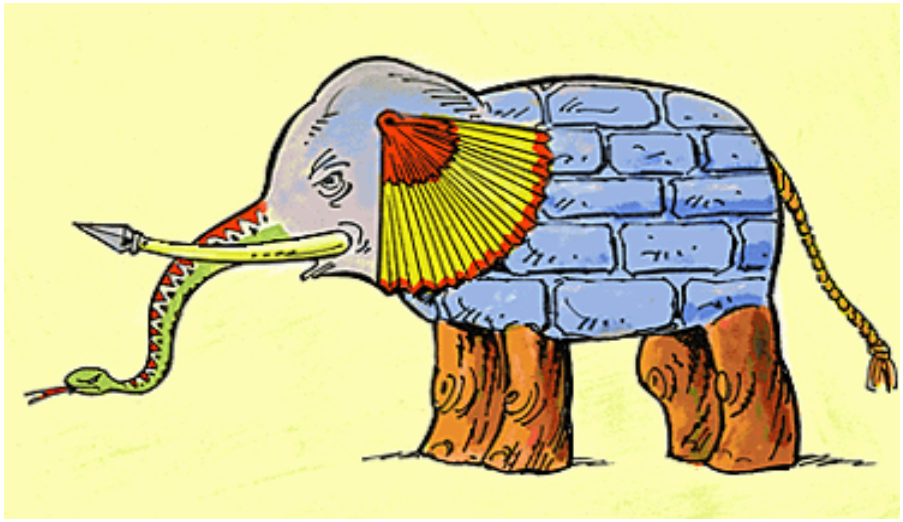
Fair Questions

- What are the basic requirements for establishing a CSIRT?
- What type of CSIRT will be needed?
- What type of services should be offered?
- How big should the CSIRT be?
- Where should the CSIRT be located in the organization?
- How much will it cost to implement a team?
- Are we ready to have one?
- What are the initial steps to follow to create a CSIRT?
- How much time does it take to implement CSIRT?
- And more ….

Steps (Stages)



Stage 1 – Education and Awareness



the decisions that must be made, the role the CSIRT will play (e.g., as a national focal point for incident reporting and response**), and the key issues that are likely to be faced (**management and staffing, developing trusted communications and coordination, effective processes, etc.)

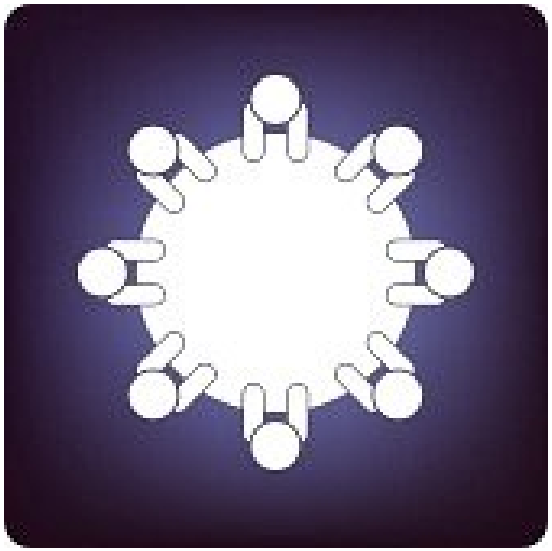
- What is this all about ?
- Why do we need CSIRT ?
- What is involved in establishing CSIRT?
- What decisions have to be made?

Meeting With Stakeholders To:

Laws, Regulations, and Other Policies

Core Services

Best Practices



Funding Strategies

Technology and NW

Understand Motivators

People to be Involved

What is Involved

Key Resources

Mission – Objectives - Expectations

Stage 2 – Planning and Design

Determine Main Items For National CSIRT

Project Plan (Road Map)

CSIRT Mission

Serve Whom??

What Services to Start by ??

Organizational Model

Where ?? CSIRT Location

Staff skills and knowledge

Equipment - Network

Budget and funding proposals

National (government) approval

Incident management processes

Roles and responsibilities

Methods for building trusted relationships

Stage 3 – Implementing the CSIRT

- Getting the funds
- Announcing broadly that a national CSIRT is being created and how to get more information
- Implementing the secure information systems
- Developing operational policies and procedures
- Implementing processes for the national CSIRT's interactions with its partener
- Identifying and hiring (or reassigning) personnel,
- Obtaining appropriate training for the CSIRT staff.

Stage 4 - Operating National CSIRT

- Ensure the national CSIRT has a basic incident management capability in place.
- So the team is actively receiving incident reports and coordinating responses to incidents.
- The national CSIRT has a vision with a framework that defines the mission, goals and objectives, structure, authority, funding, resources, and infrastructure to support and sustain the team.
- Policies and procedures have been developed and implemented.

Collaboration – Coordination – Cooperation

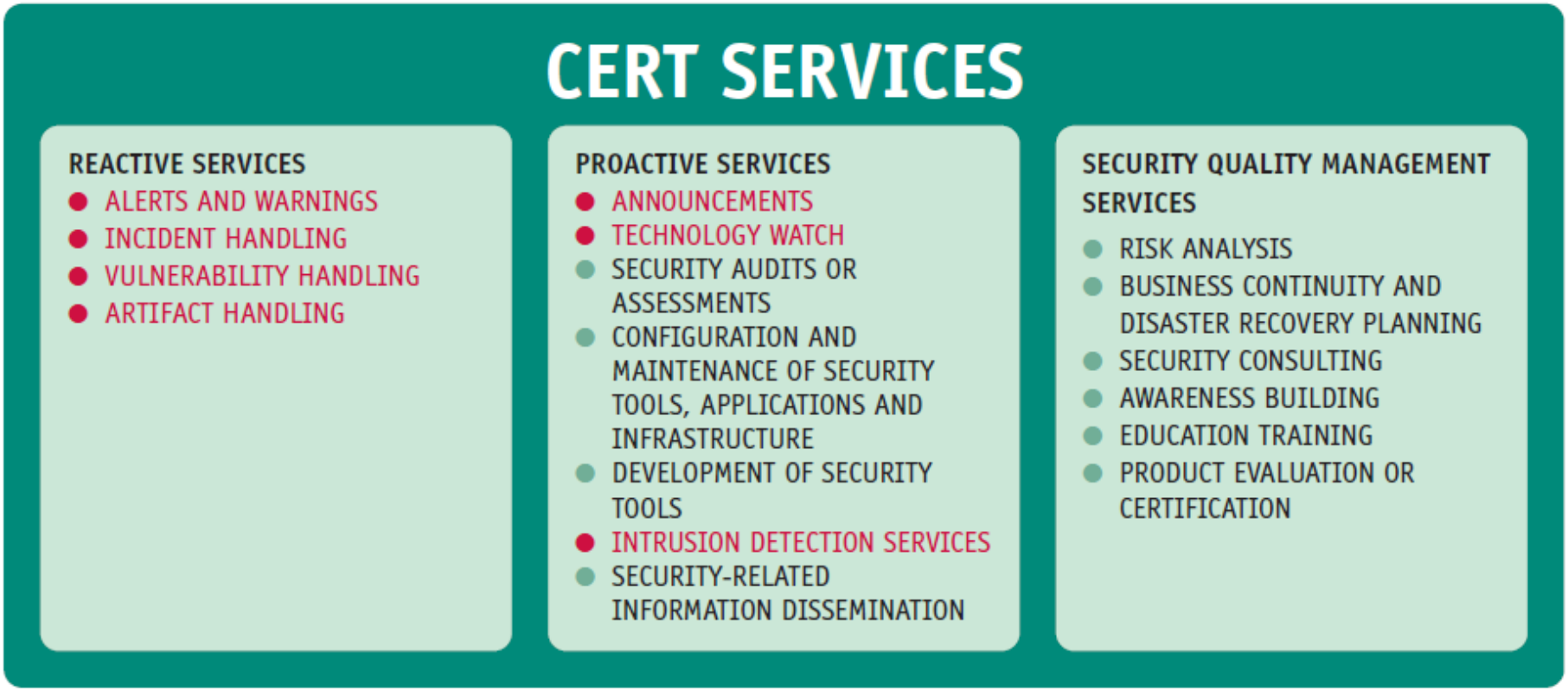
- Collaborate with all parties (inside)
- Participate in data and information sharing activities
- Participate in global “watch and warning” functions
- Cooperate with international entities (initiatives)
- You need partners – Regional communities – Peer CSIRTs
- Coordinate local efforts
- Work with community (ethical hackers, academia)

Common Problems

Failure To:

- Include all parties
- Reflect all items in Stages I and II
- Taking too many services
- Unrealistic expectations or perceptions
- Lack of time, staff and fund

CSIRT Possible Services



Over the years CSIRTs extended their capacities from being a reaction force to a complete security service provider, including preventative services such as alerts, security advisories, training and security management services.

National CSIRT Staff - Basic Skills

Personal Skills

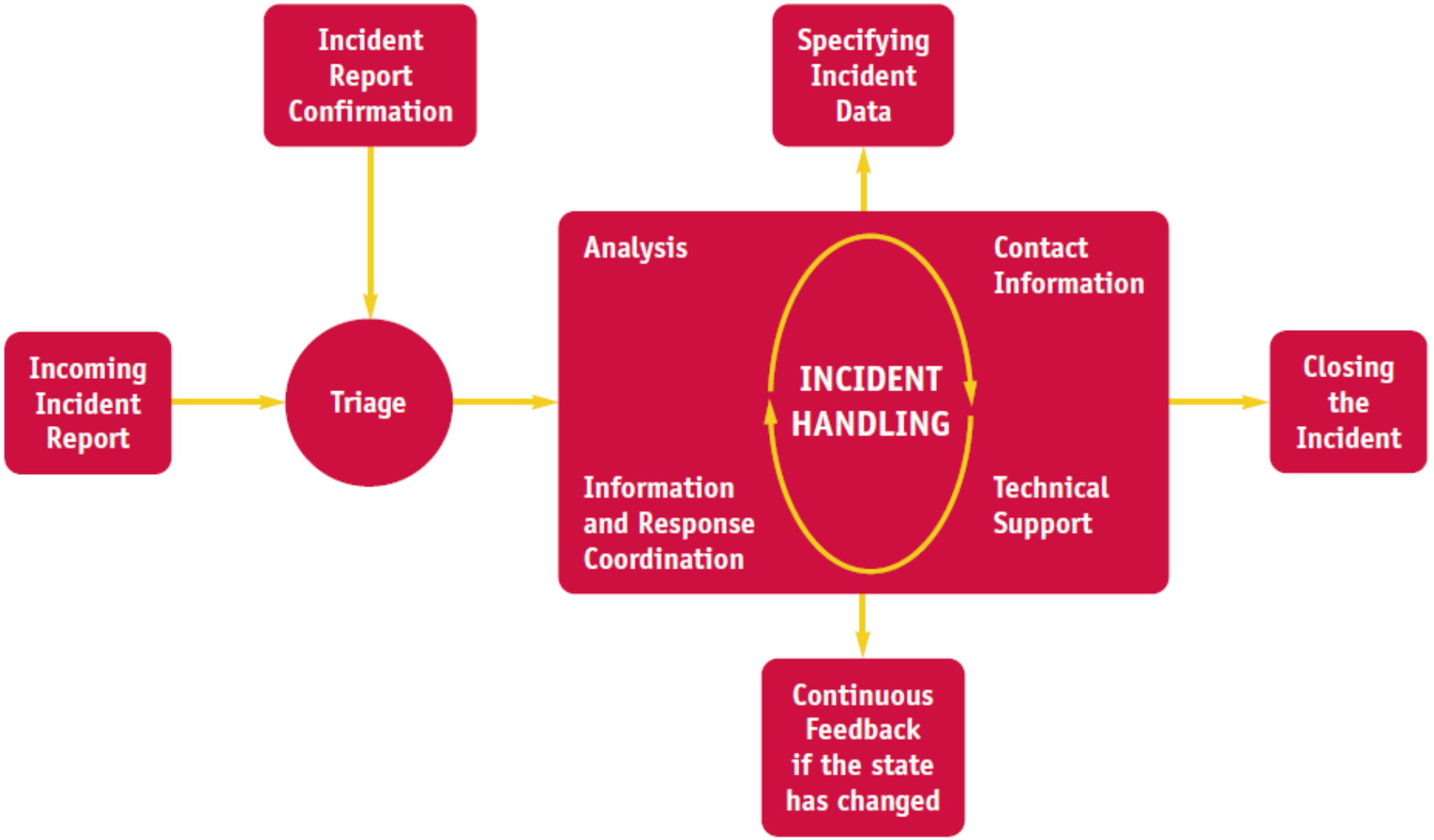
- Communication skills (oral and written)
- Diplomacy
- Ability to follow policies and procedures
- Ability to work as a contributing member of a team
- Knowing one's limits
- Ability to cope with stress
- Problem solving
- Time management
- Attention to detail

National CSIRT Staff - Basic Skills

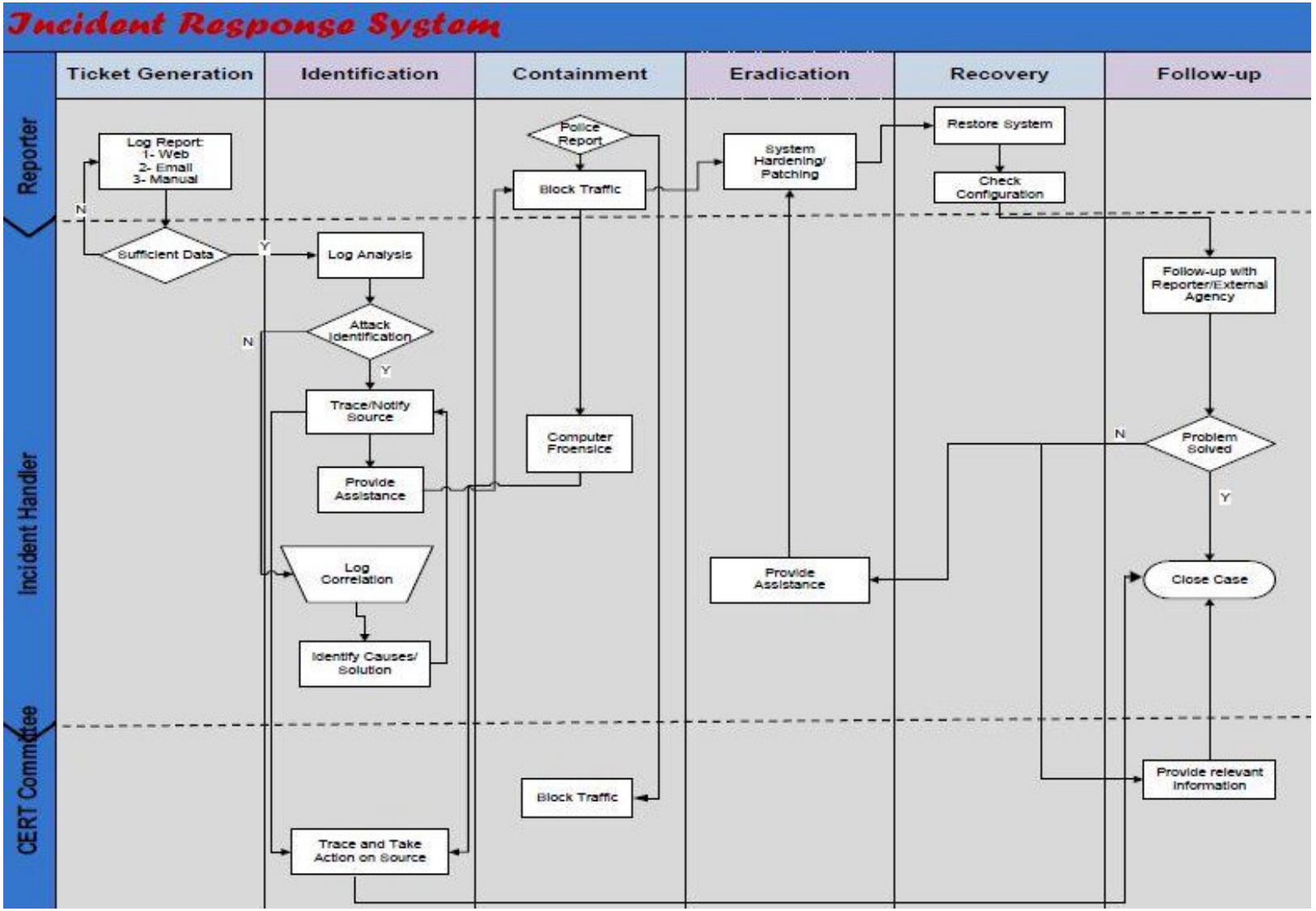
Technical Skills

- Security principles
- Security vulnerabilities, weaknesses and risks
- Physical security
- Internet/computer attacks (Smurf, POD, IPsweep, etc)
- Understanding and identifying intruder techniques
- Cryptography issues, algorithms, and tools
- Malicious code (e.g. viruses, worms, Trojan horses)
- Internet
- Network protocols (IP, TCP, ICMP, etc.)
- Domain Name System (DNS)
- Network services and applications
- Defensive security measures
- Basic programming skills

Incident Handling Process - Example



Incident Handling Process - Example



Incidents Categorization

Group	Severity	Examples
RED	Very High	DDoS, phishing site
YELLOW	High	Trojan distribution, unauthorised modification of information
ORANGE	Normal	Spam, copyright issue

CATEGORY	EXAMPLE OF INCIDENT	PRIORITY	RESPONSE TIME
HIGH	• Denial Of Service Attacks • Damage Of critical Systems • Web server compromised (Defacement) • Hack Threat	Red	24Hours
MEDIUM	• Internet Worm • System Intrusion • Data Loss • Harassment, Fraud • Root kit Activity • Vulnerability Exploit • Scan	Orange	3 days
LOW	• Spamming/Mail bomb • Virus • Phishing • Sniff	Yellow	1 Week

Thank You

- No need to start from Zer0
- Start small and grow (Brazil)(Tunisia)
- Best time is Now
- Others also need a CSIRT
- You may start coordinating only

Mutaz.ishag (at) ntc.gov.sd

Mutaz.ishag (at) cert.sd