

# I3P Project: What Makes a Good CSIRT?



## Cyber Security Division 2012 Principal Investigators' Meeting

**Shari Lawrence Pfleeger**  
**Research Director**  
**Institute for Information Infrastructure Protection**  
**[pfleeger@dartmouth.edu](mailto:pfleeger@dartmouth.edu)**  
**603 729 6023**

# What is the I3P?

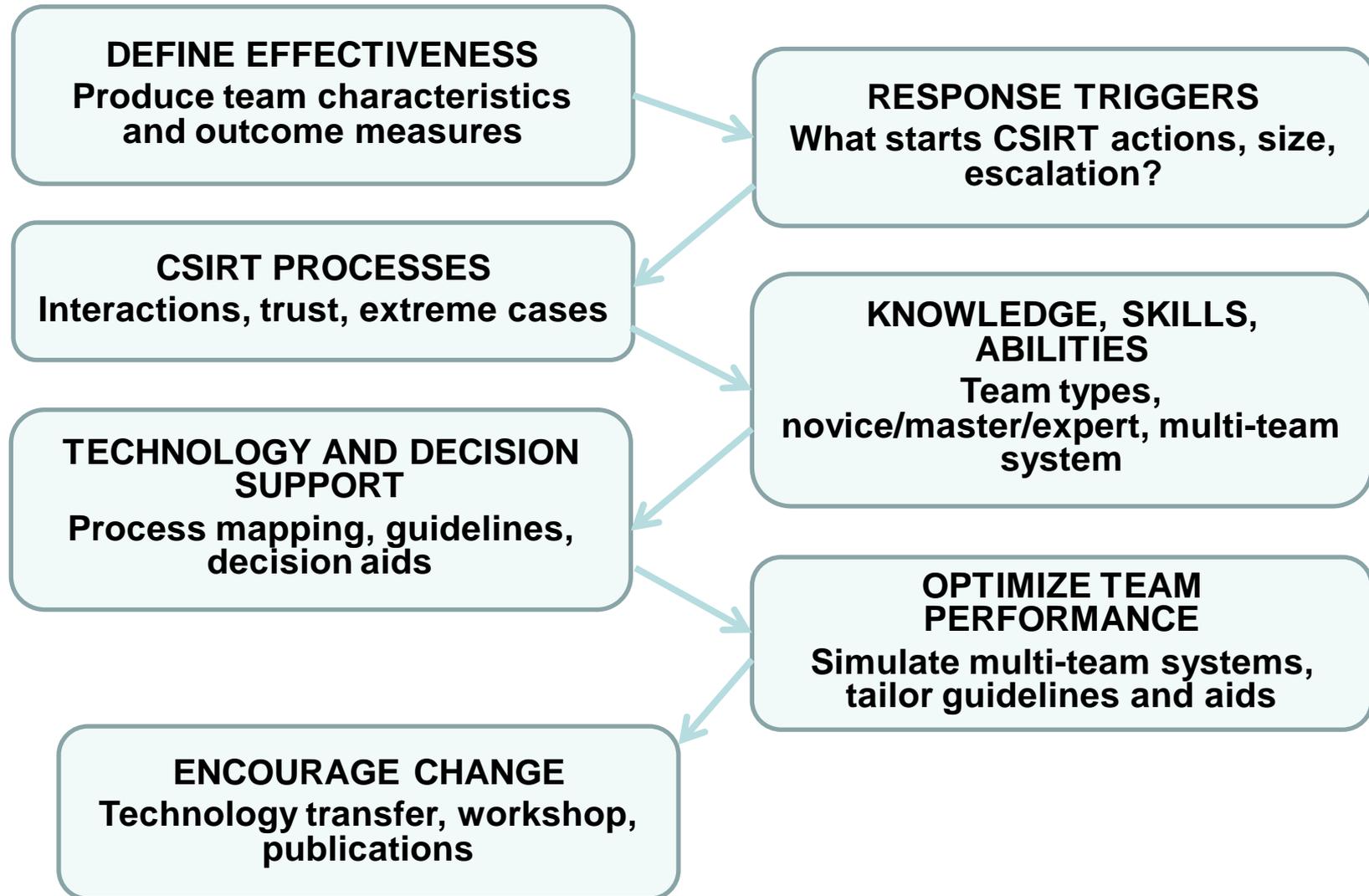


- A national consortium of 28 universities, national labs and non-profits doing cyber security research
- 10 years of impact
- Focus on multi-institution, multidisciplinary projects to strengthen the nation's information infrastructure

# What Makes a Good CSIRT?

- Duration: October 2012 for 3 years
- George Mason U: Organizational psychologists will look at knowledge, skills and abilities; teams; interactions
- Hewlett-Packard: Runs Navy-Marine Corps Intranet (NMCI); will provide access to CSIRT, network analysts, help desk, etc. (NMCI is the largest internal computer network in the world: 363,000 computers, 707,000 sailors, 620 locations)
- Dartmouth: Will analyze costs and benefits

# Project Activities



# Generating Taxonomy of CSIRT Criteria

## Top-Down

- Review existing taxonomies
  - Domain-general
  - Domains “similar” to CSIRTs
- Adapt to CSIRT setting
  - Test extant dimensions
    - Focus groups
    - Archival information

## Bottom-Up

- CSIRT “critical incidents”
  - Focus groups
  - Archival information
- Develop taxonomy of CSIRT criteria
  - Obtain dimensions

# CSIRT Services

## 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



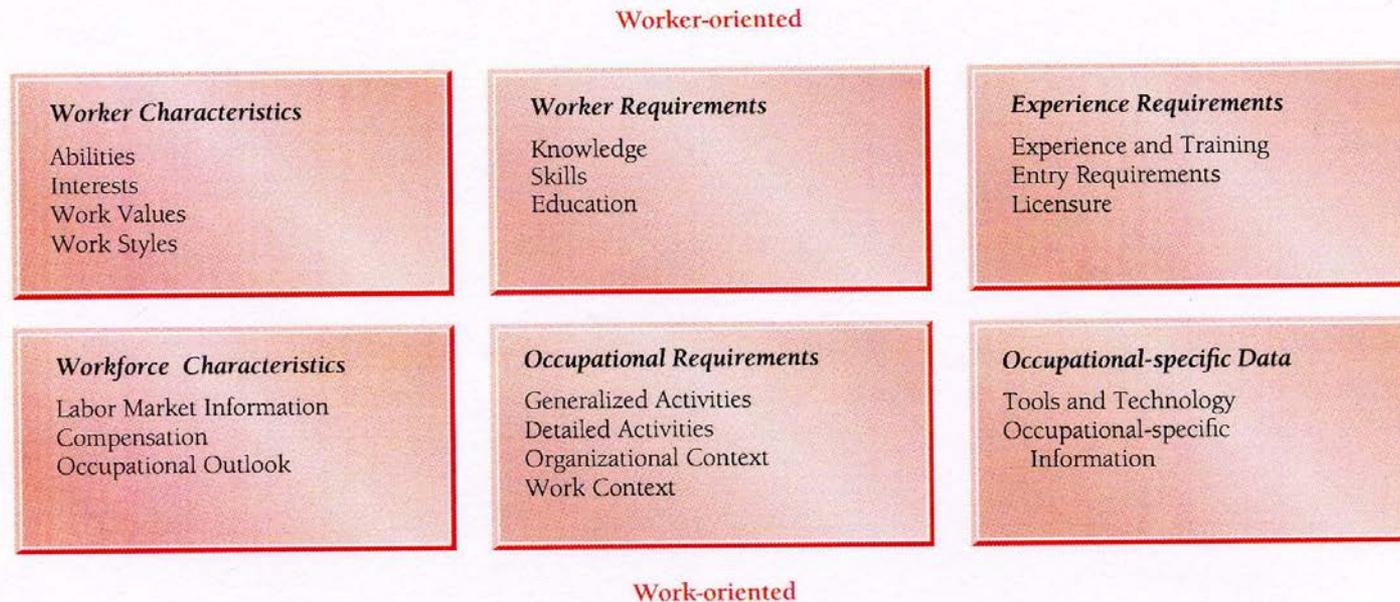
- ↻ Announcements
- ↻ Technology Watch
- ↻ Security Audit or Assessments
- ↻ Configuration & Maintenance of Security Tools, Applications, & Infrastructures
- ↻ Development of Security Tools
- ↻ Intrusion Detection Services
- ↻ Security-Related Information Dissemination

## Security Quality Management Services



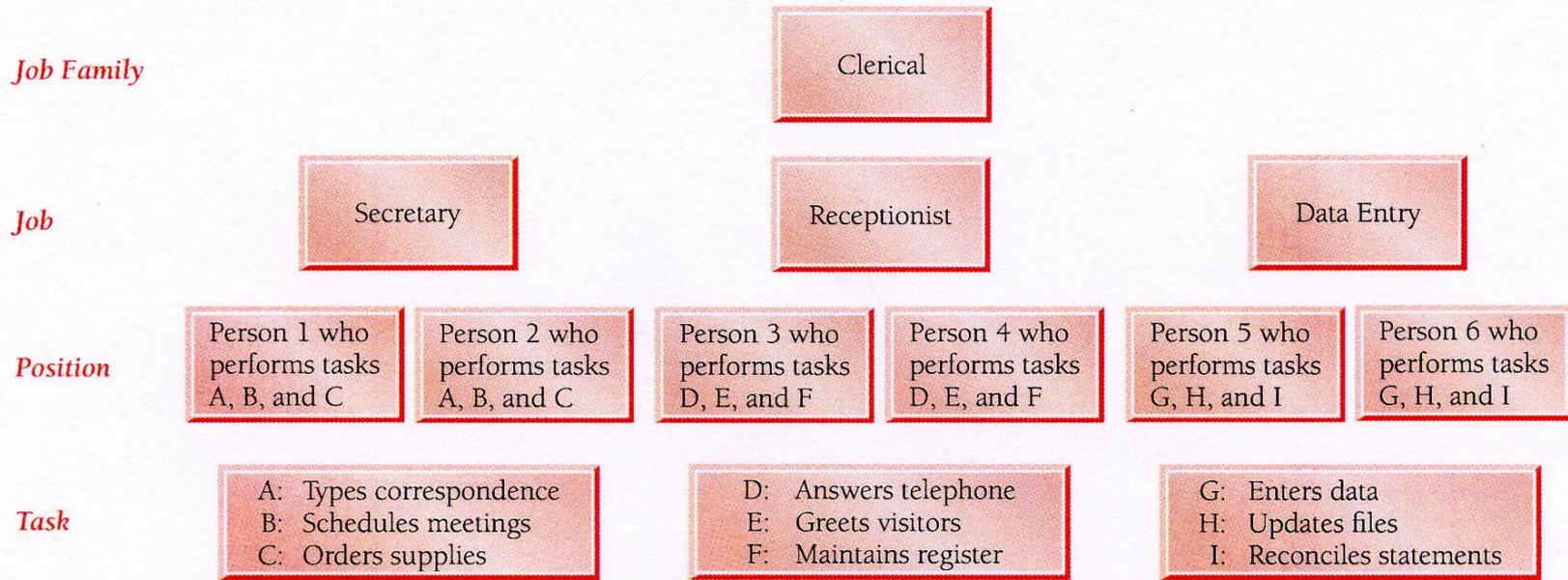
- ✓ Risk Analysis
- ✓ Business Continuity & Disaster Recovery Planning
- ✓ Security Consulting
- ✓ Awareness Building
- ✓ Education/Training
- ✓ Product Evaluation or Certification

# Task Analysis: What Do CSIRT Team Members Do?



**Figure 3-4** Content model for the Occupational Information Network

# How Do Tasks Interact?



**Figure 3-2** Relationships among tasks, positions, jobs, and job families

# How Do People Interact?

## Relationships with Other Persons

This section deals with different aspects of interaction between people involved in various kinds of work.

Code	Importance to this job
DNA	Does not apply
1	Very minor
2	Low
3	Average
4	High
5	Extreme

### 4.1 Communications

Rate the following in terms of how important the activity is to the completion of the job. Some jobs may involve several or all of the items in this section.

#### 4.1.1 Oral (communicating by speaking)

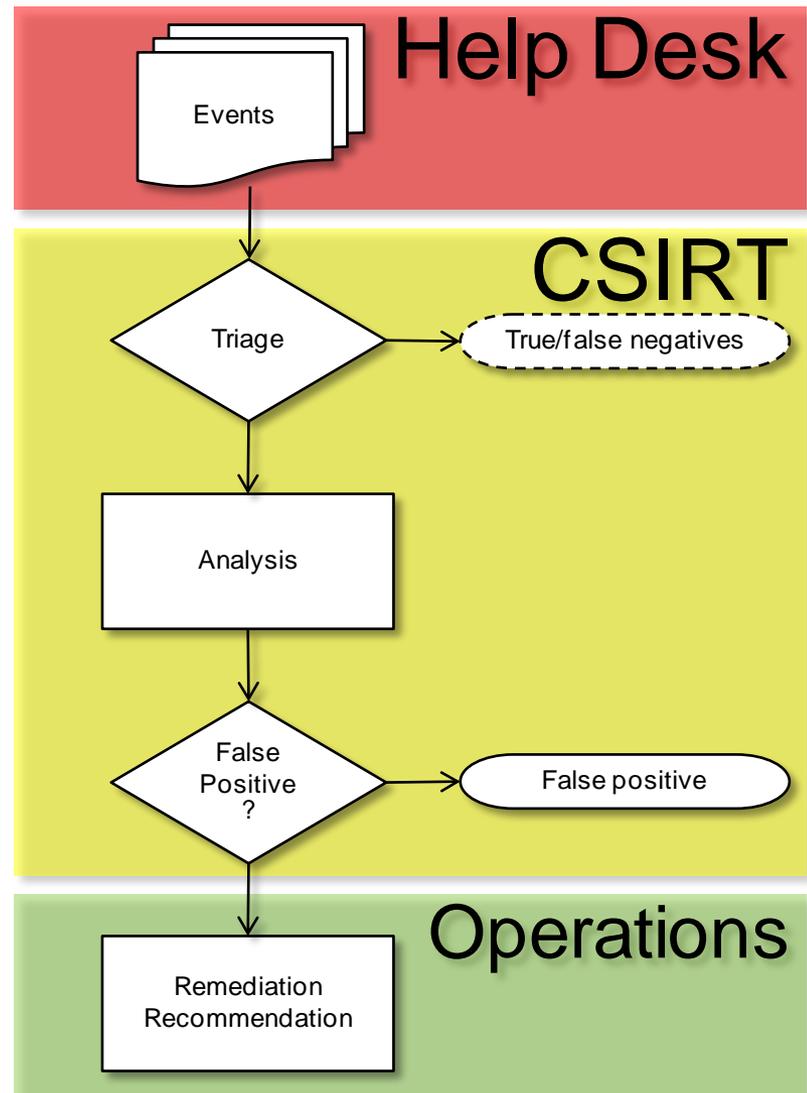
99	Advising (dealing with individuals in order to counsel and/or guide them with regard to problems that may be resolved by legal, financial, scientific, technical, clinical, spiritual, and/or other professional principles)
100	Negotiating (dealing with others in order to reach an agreement or solution; for example, labor bargaining, diplomatic relations, etc.)
101	Persuading (dealing with others in order to influence them toward some action or point of view; for example, selling, political campaigning, etc.)
102	Instructing (the teaching of knowledge or skills, in either an informal or a formal manner, to others; for example, a public school teacher, a journeyman teaching an apprentice, etc.)
103	Interviewing (conducting interviews directed toward some specific objective; for example, interviewing job applicants, census taking, etc.)

**Figure 3-3** Sample items from the PAQ

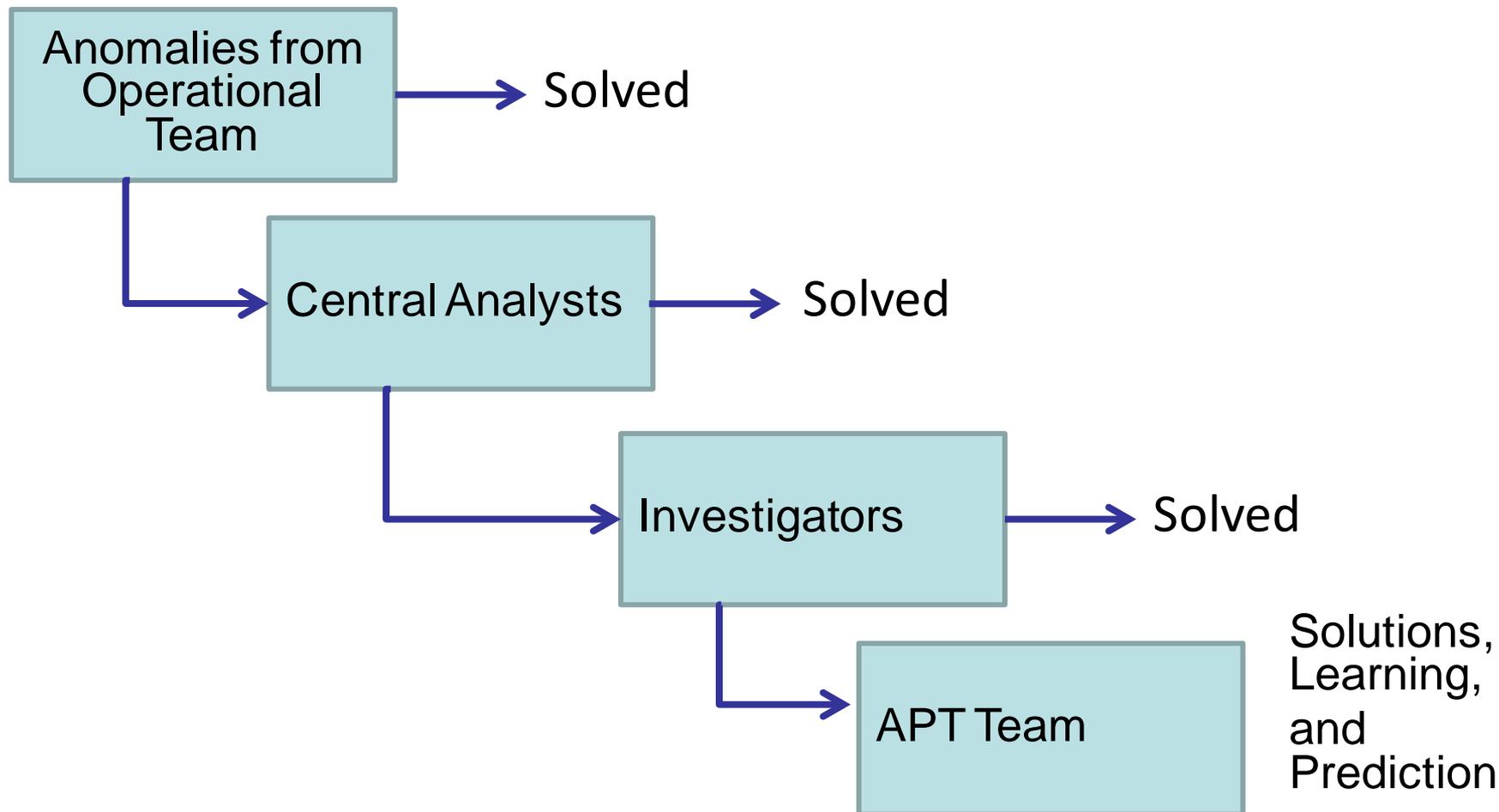
From *Position Analysis Questionnaire* by E. J. McCormick, P. R. Jeanneret, and R. C. Mecham. Copyright © 1989. All rights reserved. Reprinted by permission of PAQ Services.

# Process Modeling

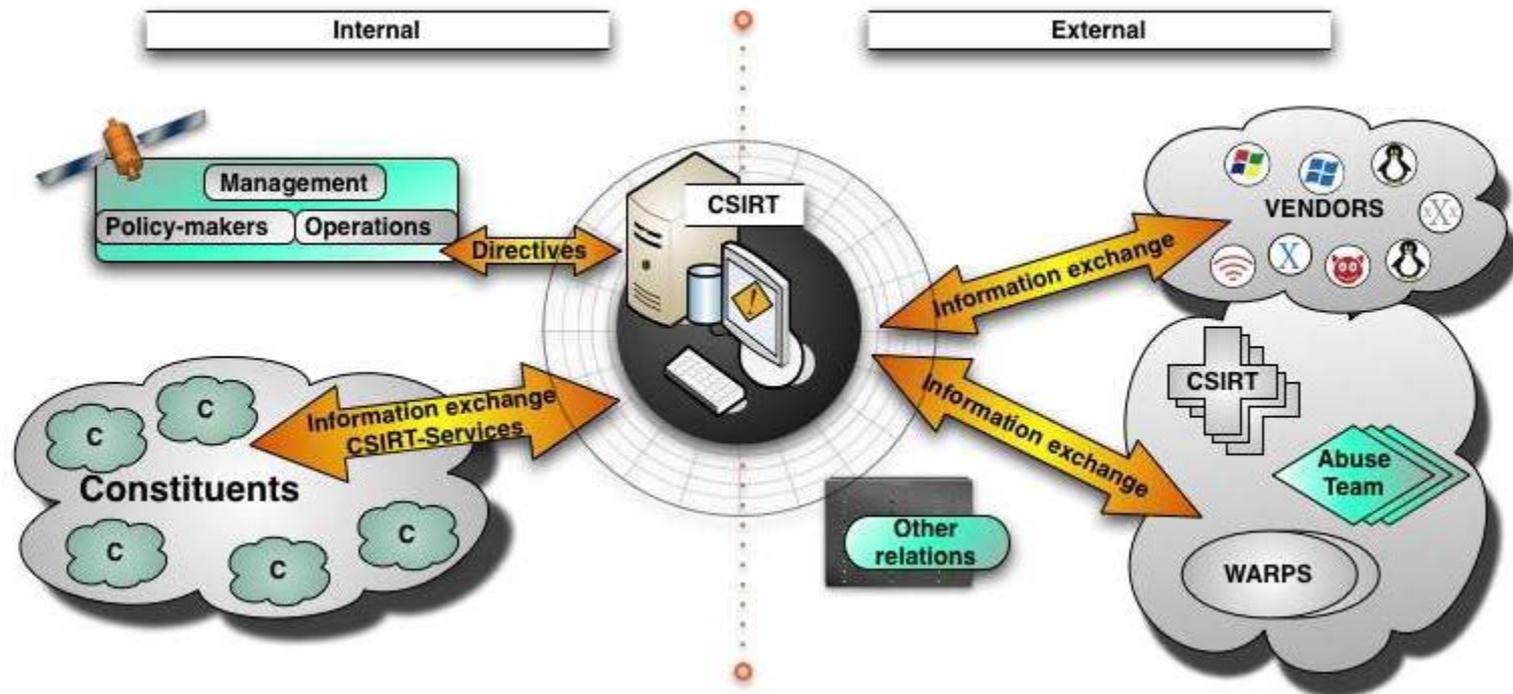
- Develop models of CSIRT processes
  - Analyze and improve business process efficiency, quality and cost
  - Facilitate understanding and communication
  - Support process management
  - Seek ways to introduce automation
  - Develop best practices
- Focus on process models that capture interactions between teams



# Skills and Escalation

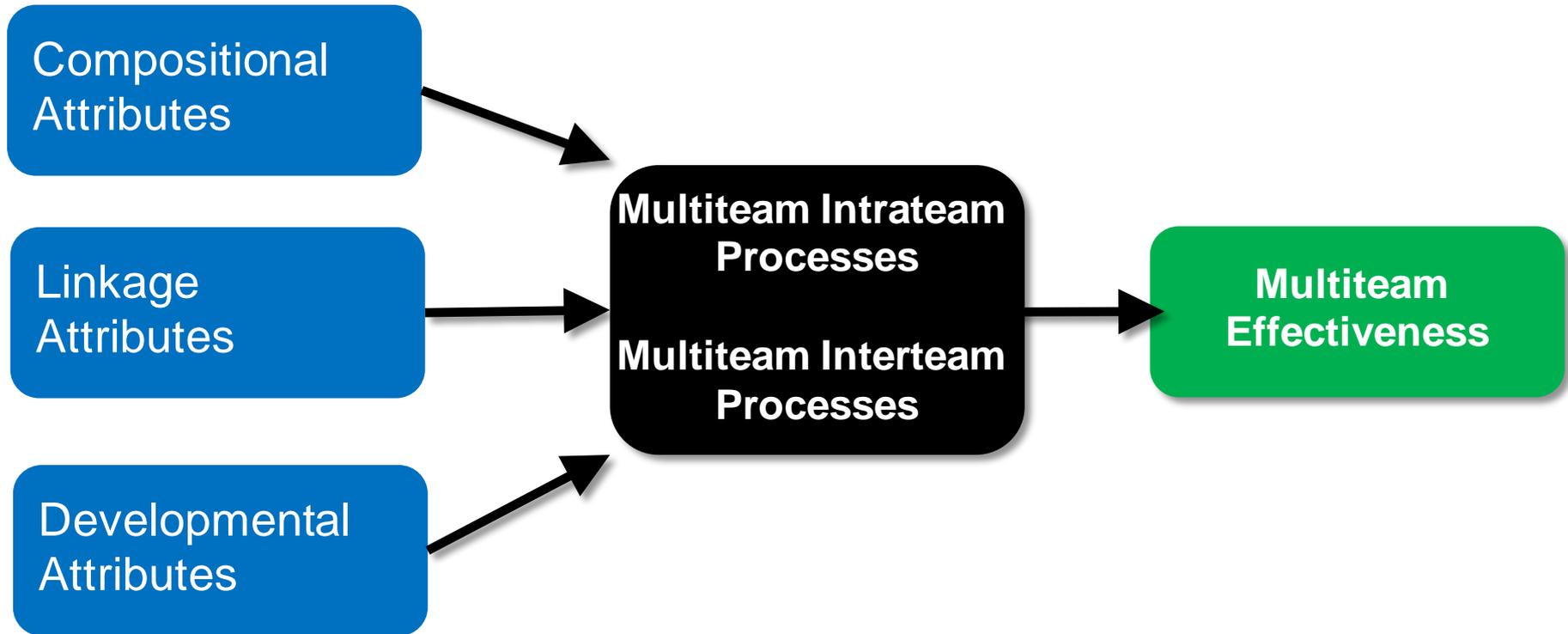


# How Do Teams Interact?

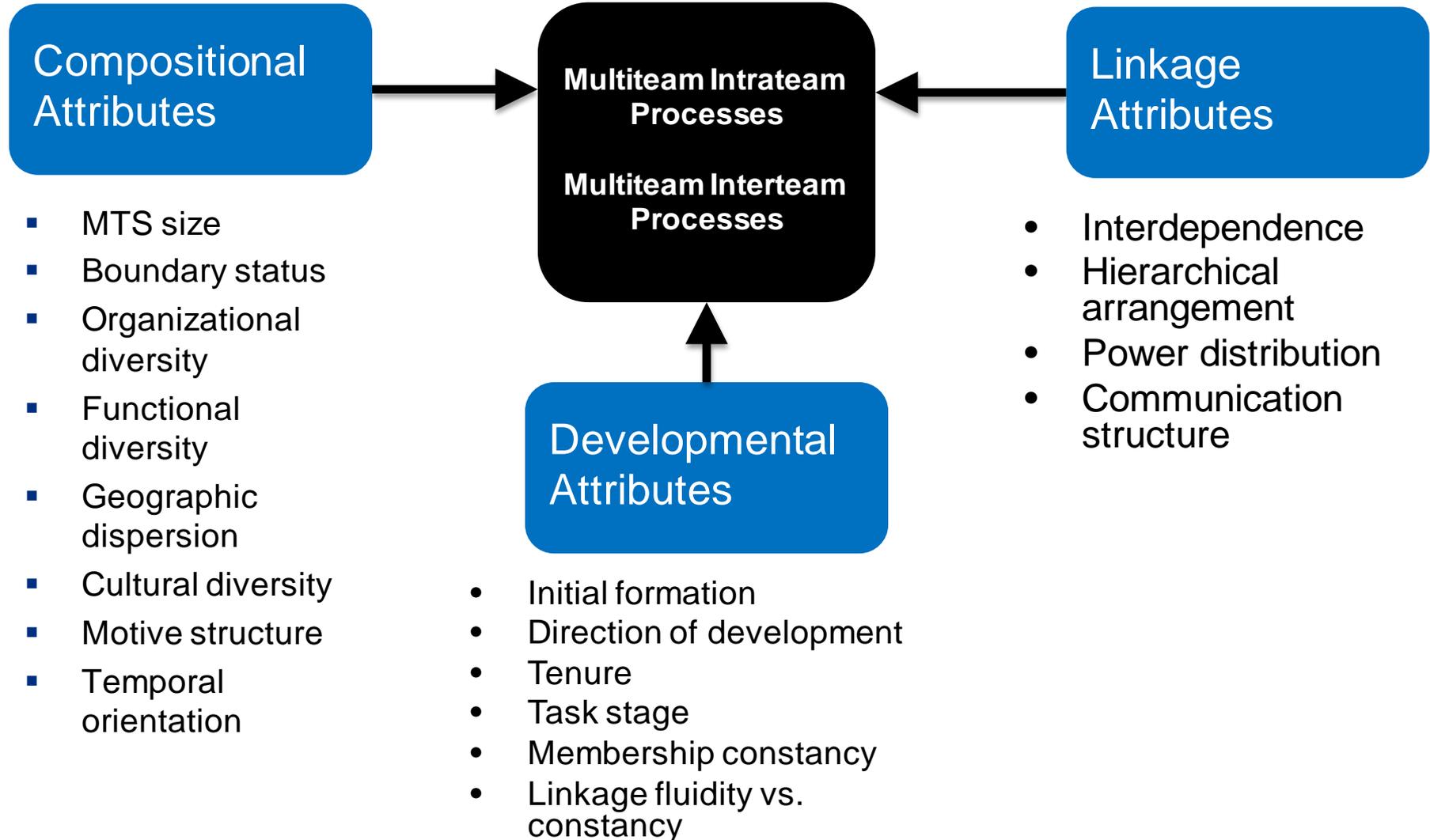


Bronk, H., Thorbruegge, M., & Hakkaja M. (2007). *A Basic Collection of Good Practices for Running a CSIRT*. Heraklion, Greece: European Network and Information Security Agency.

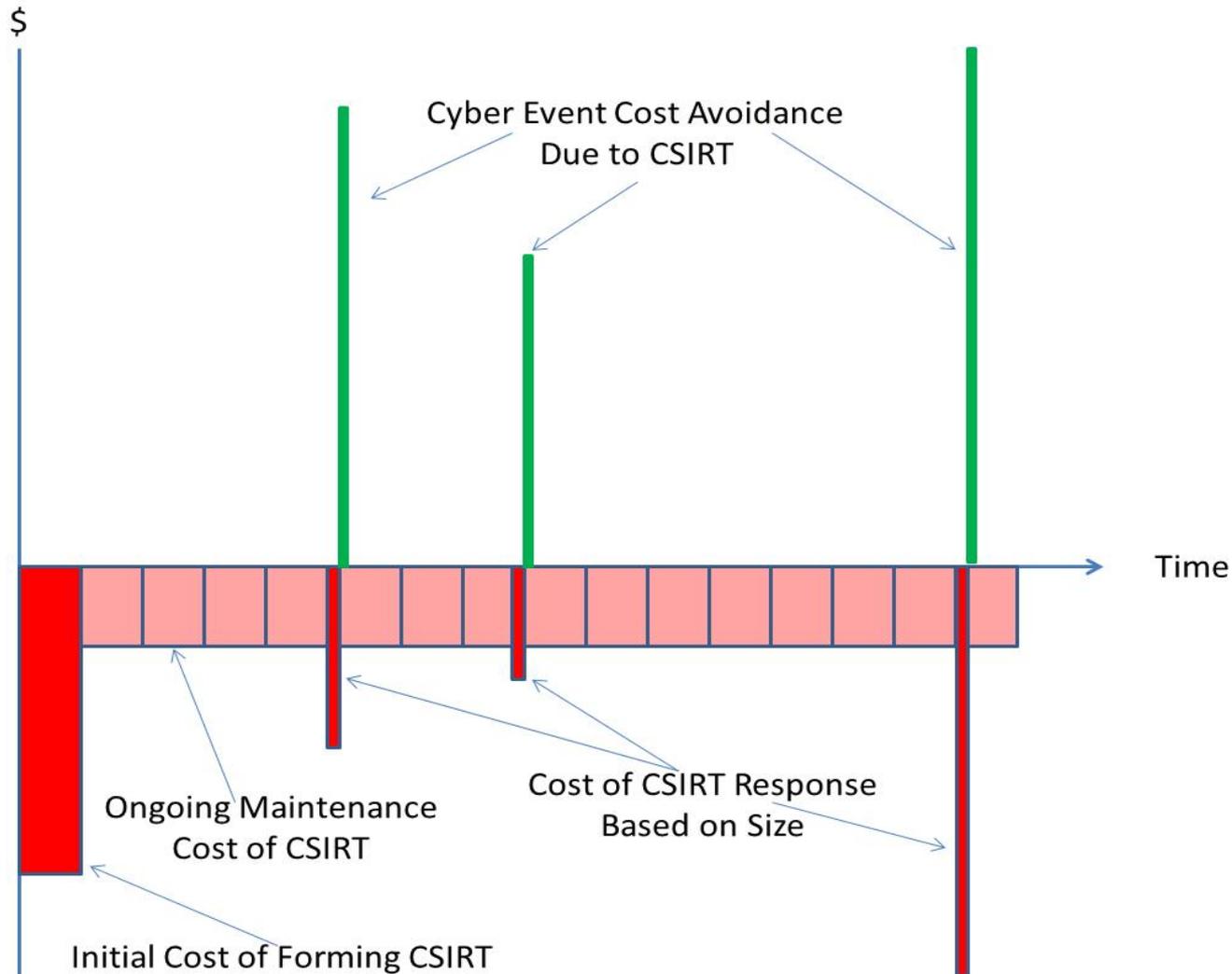
# Model Multiteam System Effectiveness



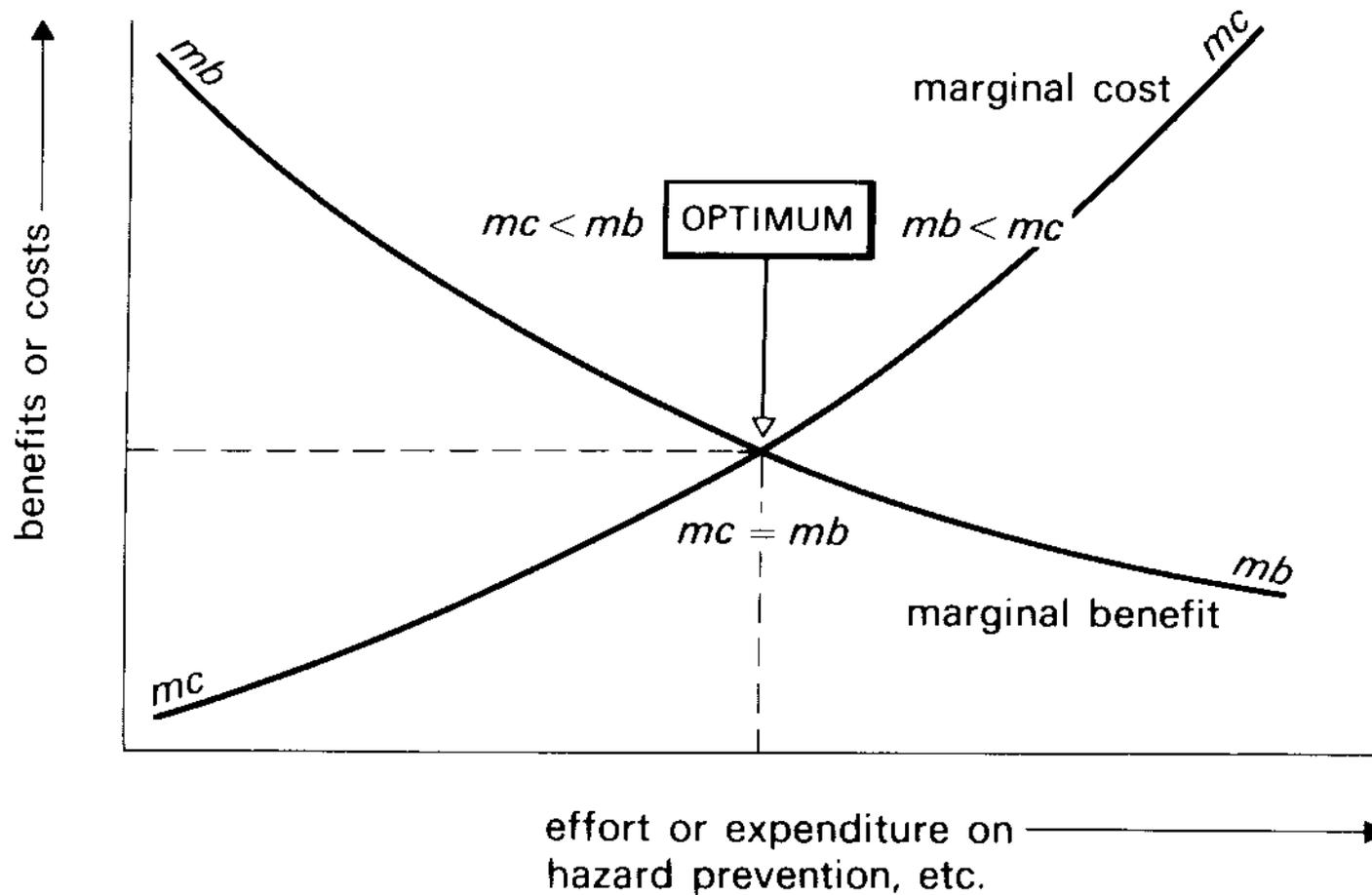
# Attributes Inform Processes



# CSIRT Cash Flows



# Cost-Benefit Analysis: Trade-offs



# Deliverables

- Basic principles of
  - Team composition
  - Training
  - Support
- Decision aids
- Guidelines for optimized processes
- Results from
  - Interviews
  - Focus groups
  - Observation



# Questions?

