JPCERT/CC is an independent non-profit organization, acting as a national point of contact for the other CSIRTs in Japan. Since its establishment in 1992,the center has been gathering computer security incident and vulnerability information, issuing security alerts and advisories, and providing incident responses as well as education and training to raise awareness of security issues.

Setting CSIRTs in Africa Region

Yurie Ito
Director of Technical Operation
JPCERT/Coordination Center, Japan

@CSIRT Training in AfNOG tutorial, Morocco
1 June, 2008

What is CSIRT?

JPCERT CC®

CSIRT: Computer Security Incident Response Team
CERT: Computer Emergency Response Team

Many types of CSIRTs:

- *National POC CSIRT*
- *Organization CSIRT*
- *Government CSIRT*
- *Military CSIRT*
- *Academic Research CSIRT*
- *Vendor/Product CSIRT*
- *Regional CSIRT*

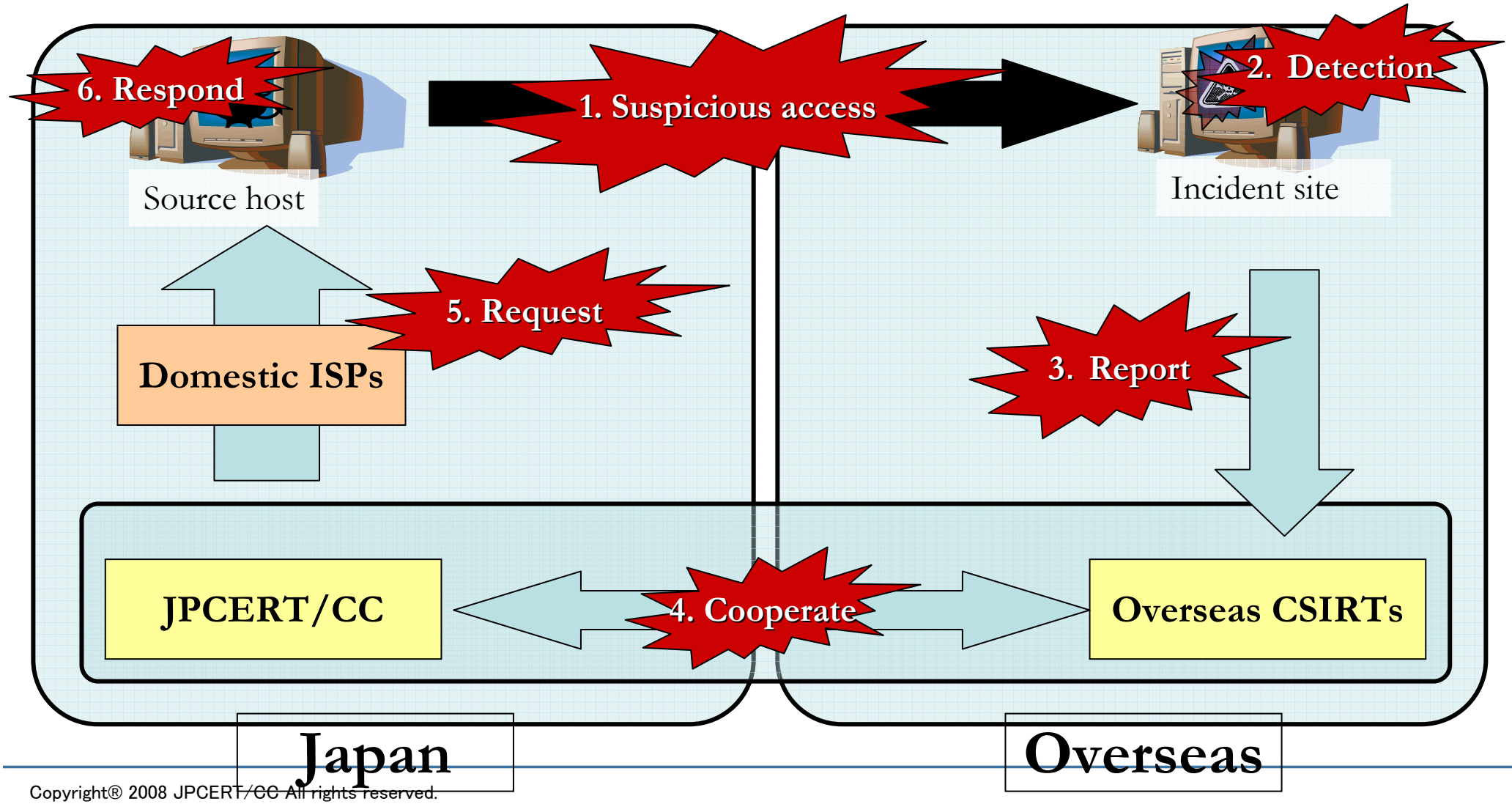
Why am I here:

I (on behalf of the international Cyber Security Incident Response Teams community) want National point of contact CSIRT at each of the African countries to be the focal point for the incident response coordination!

Why we need national POC?
International incident handlings

- *Cyber incident crosses boarder*
- *Overcome the differences between*
  - —*Languages: we don't speak French or Arabic.*
  - —*Security Cultures*
  - —*Rules, Laws, Regulations*
  - —*Time zones*

Incident Response Coordination



Cyber Incident

Who?

Attacker:
Professionals,
Criminals

Spyware
Botnets
Phishing
Troyjan
etc....

Tools
techniques

How?

Social engineering

Technical vulnerabilities

Why?

Money!!!

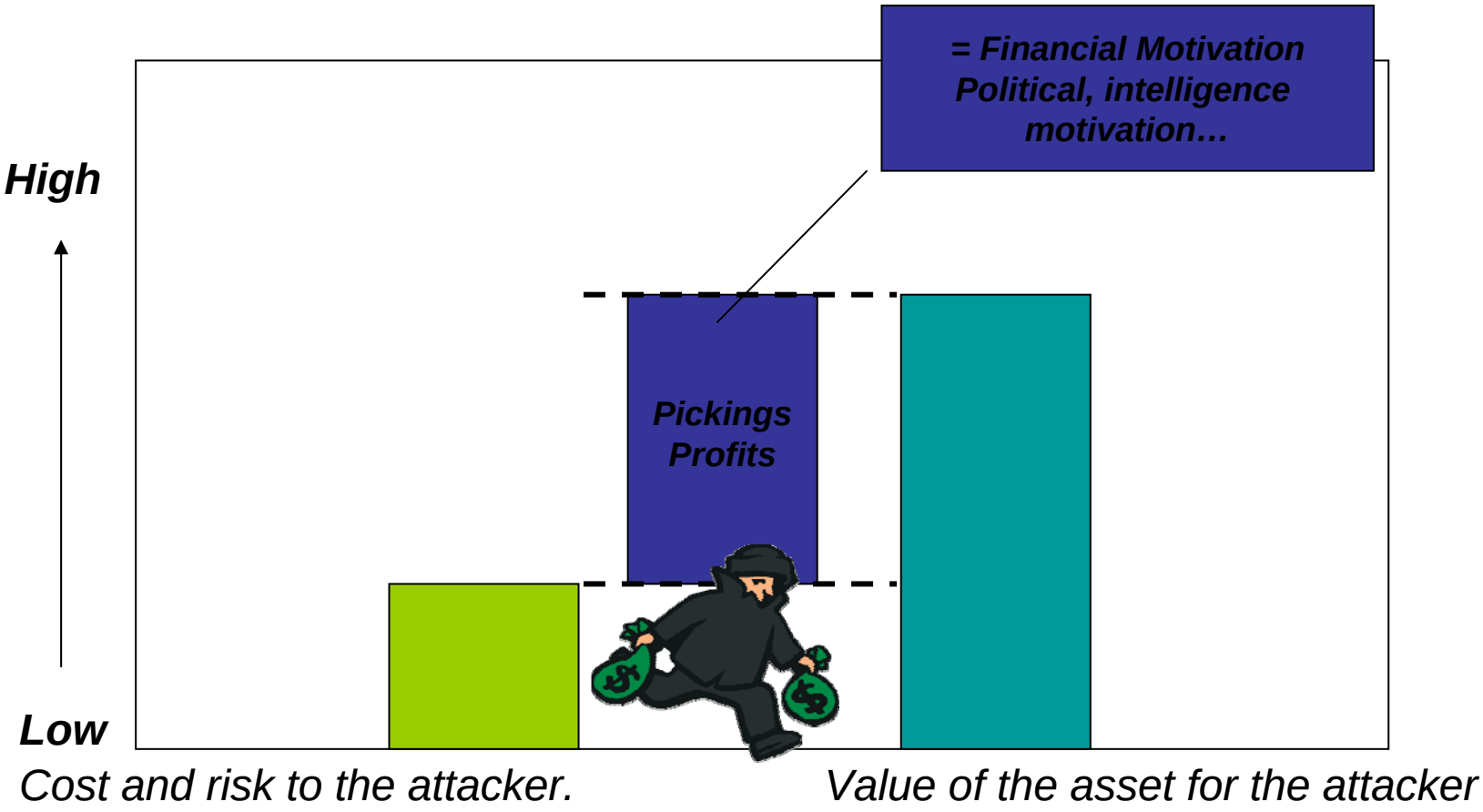
What?

Asset:
Any type of information,
PC, network resources

Where?

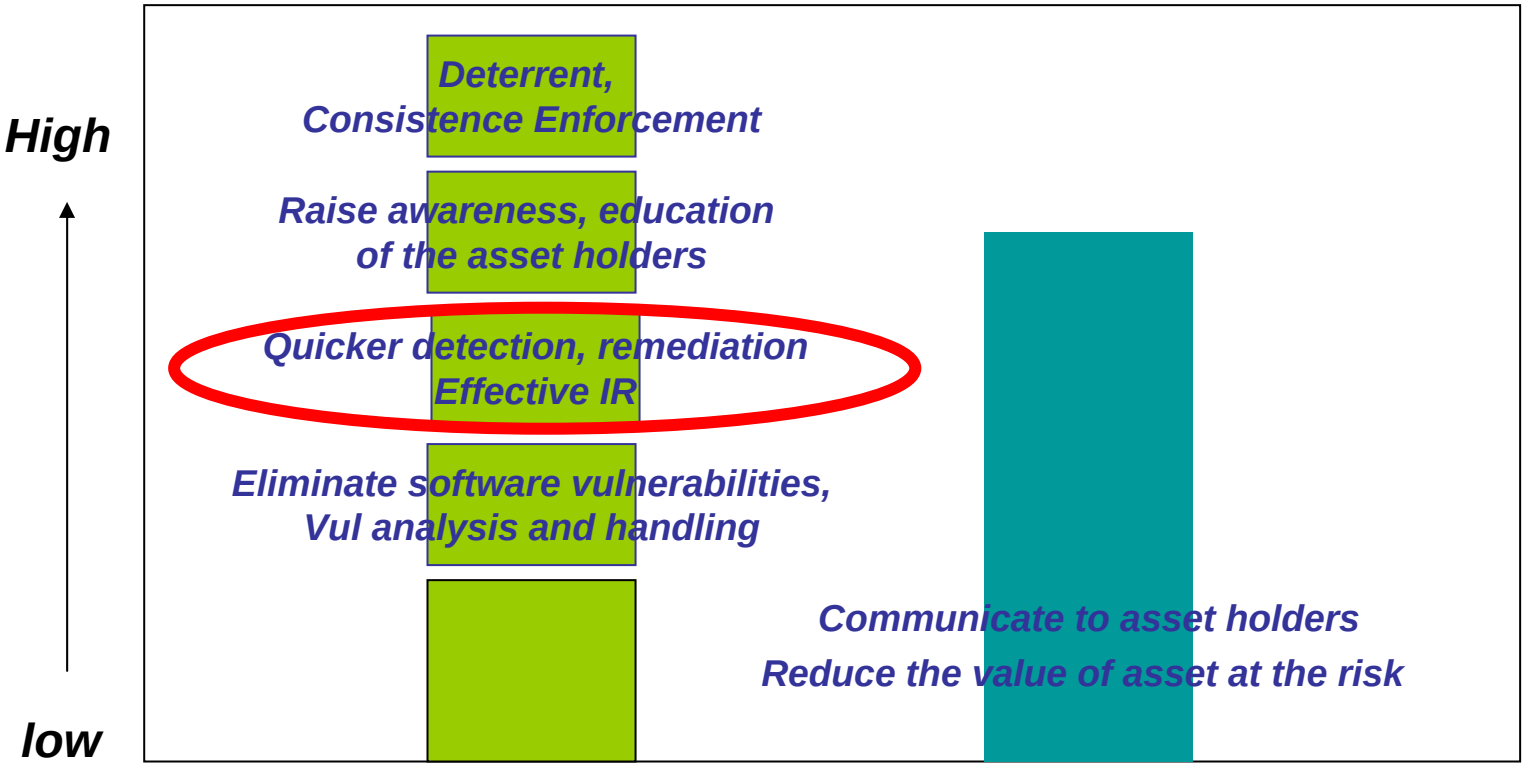
Attackers Cost and Assets Value
Low cost and Risk to the attacker

- *Current model*



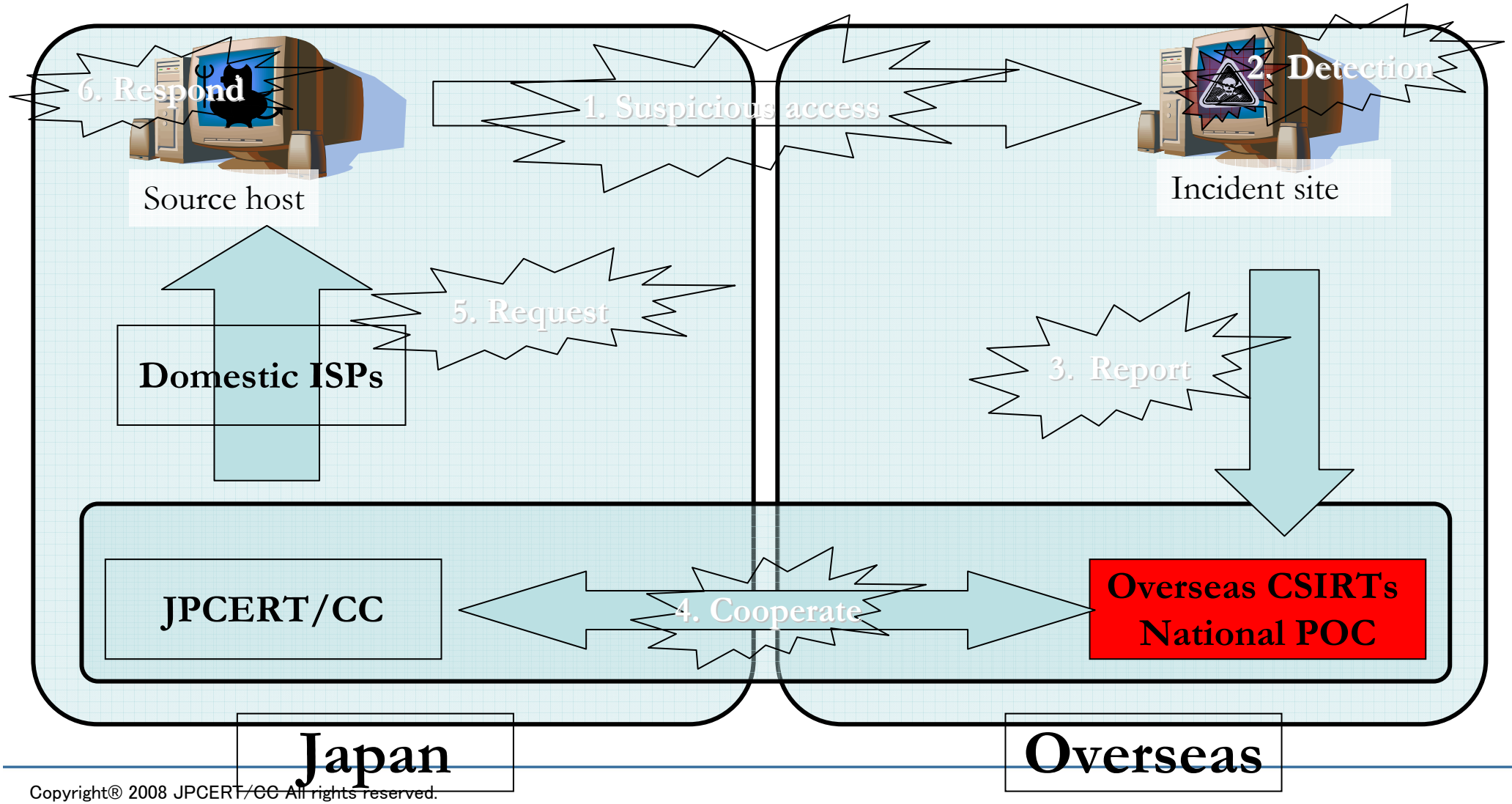
CSIRT Approach to impact the current model

- Raise the cost of the attackers

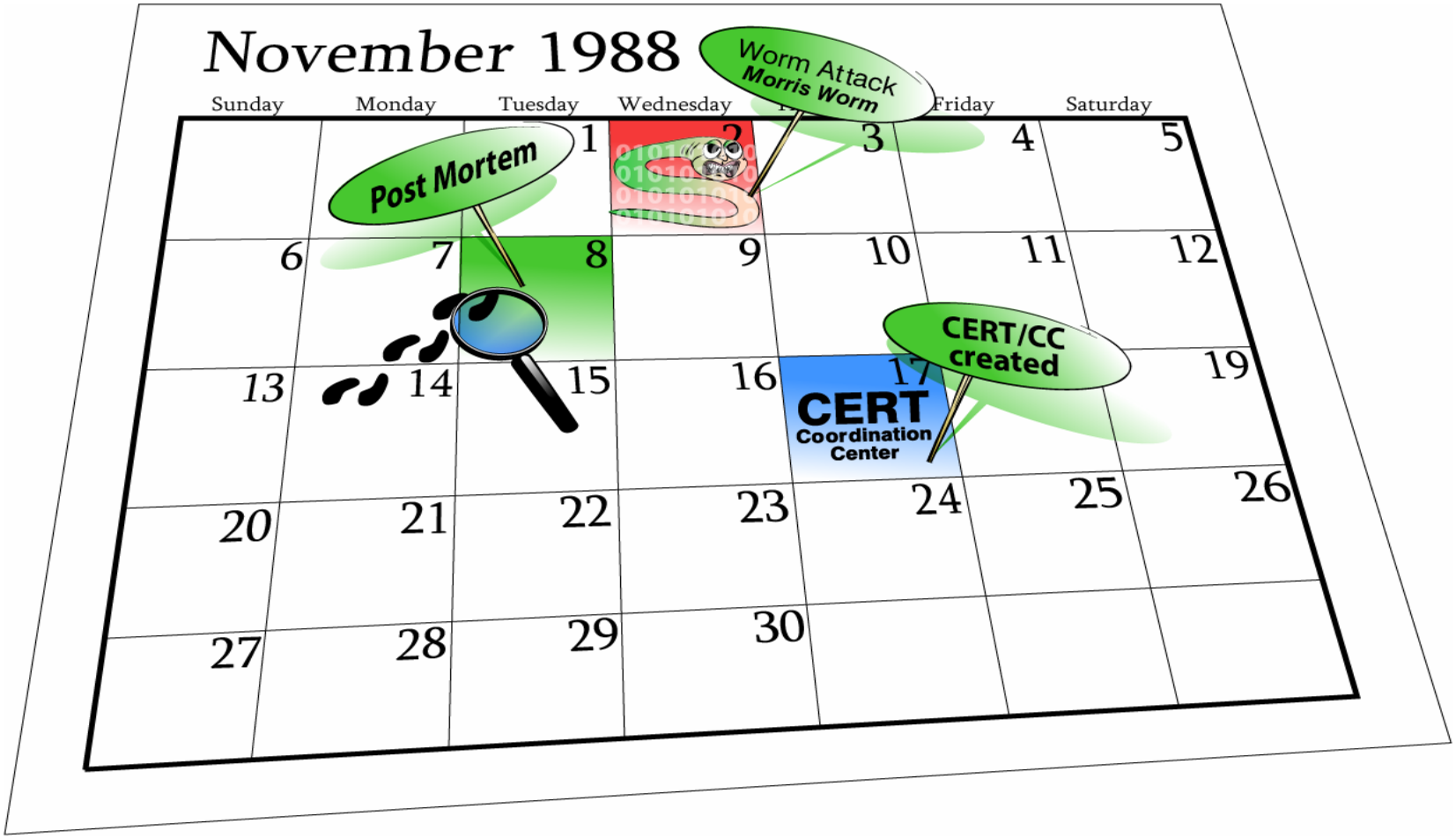


Incident Response Coordination

JPCERT CC®



Morris Worm

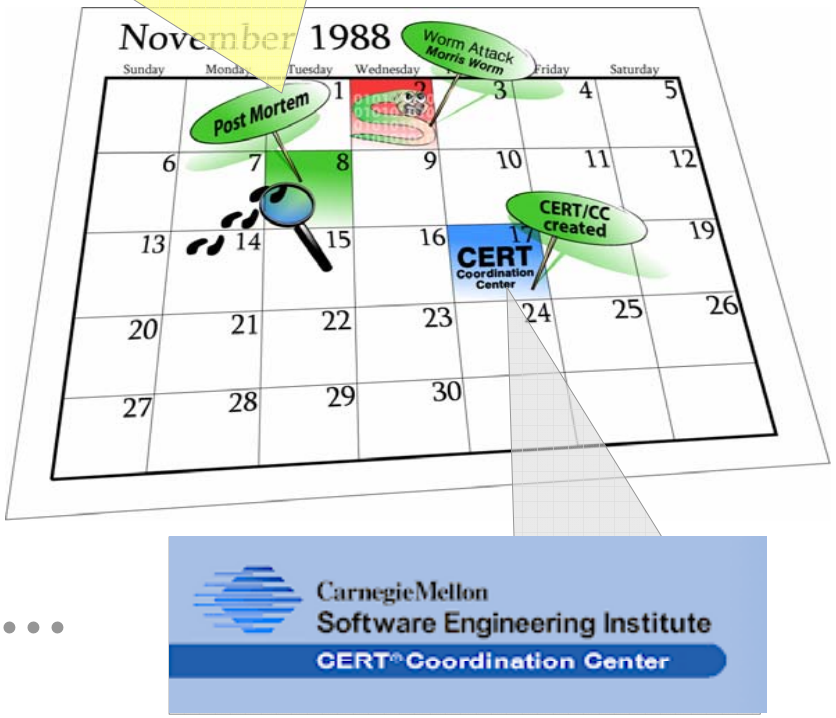


After Action

- *Effects of the worm*
  - *6,000 major Unix machine were infected*
    - *Someone guess that there were about 60,000 computer at that time.*
  - *Cost of the damage estimated at $10M-100M*

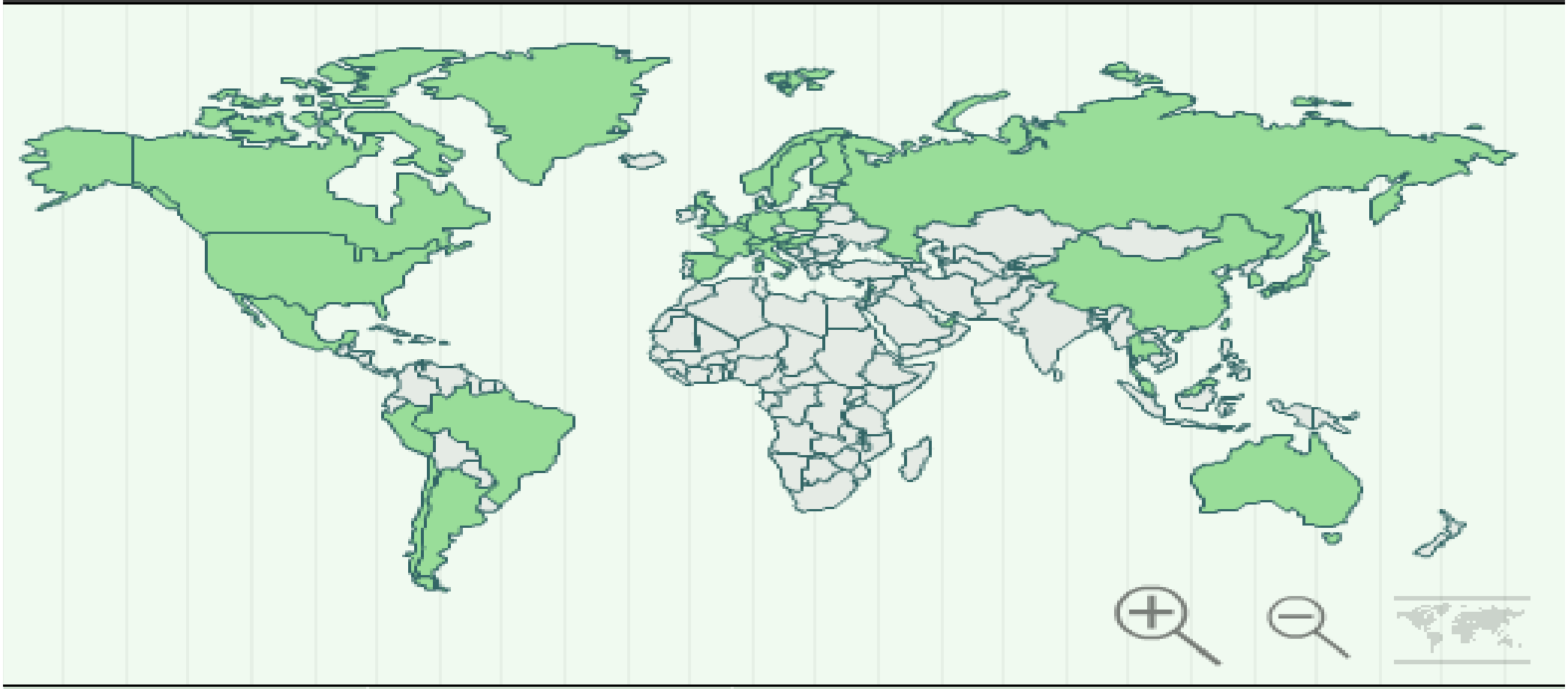
- *A call for a single point of contact to be established for Internet security problems*

To identify how to improve response to computer security incident…



JPCERT CC®

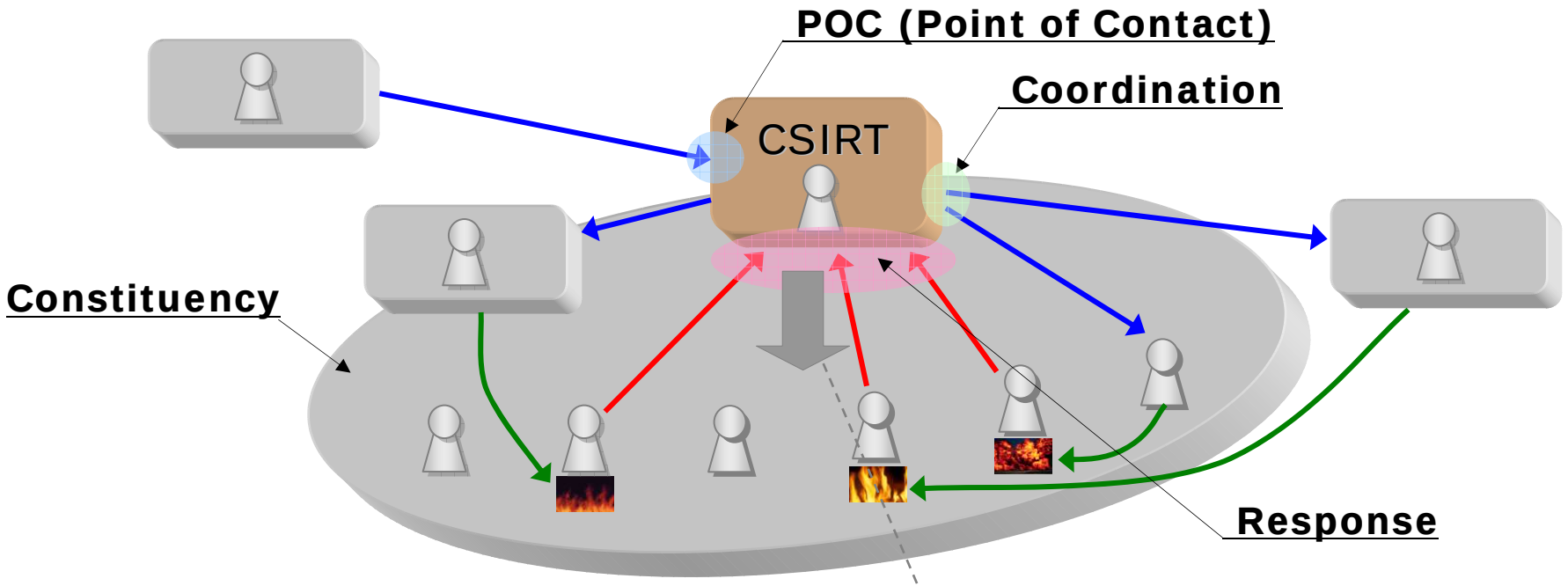
FIRST Teams around the world



By countries | By team name | 181 Teams across 36 countries

Why CSIRT

What is CSIRT? - JPCERT/CC model



- *Constituency? → Internet community in Japan*
- *Service? → Incident Response and Analysis, Security Alert, Coordination with other CSIRTs, Vendor Coordination, Education & Training, Research & Analysis*

Background

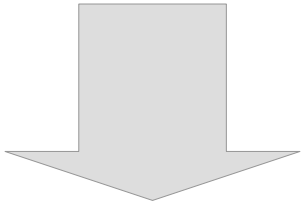
- *Many excuses for not planning for incident response, saying the following:*
  - *"We are NOT a target. I do NOT believe that who would want to compromise our network."*
  - *"We can NOT be hacked. We have best network defenses that proved very expensive."*
  - *"We thought we would just figure it out WHEN THE TIME CAME."*

Background

- *Infrastructures depending on the internet and Information Communication Technologies*
  - *Internet is vital for business and daily life*
- *Internet/Computer will help our activities in a cost-effective and efficient way*
- *The Operator of Critical [illegible]structure are concerned…*
  - *The computer system are vulnerable to attack or being used to further attacks to others.*

Background

- *Internet/Computer is complex and dynamic*
- *Interne is easily accessible to anyone with Computer and a network connection.*
  - *Less cross border than real world*
- *There is NOT perfect system or user.*
  - *Miss to configure, outdated/unpatched system, Vulnerabilities in software, and lack of security awareness of users.*



Possible intrusion/vulnerability
in your and your constituency system !

Why Do I Need a CSIRT?

- *Malicious acts will happen*
  - *Even the best information security infrastructure can NOT guarantee.*
  - *Attackers target to resources*
    - *What is their motivation ?*
      - *Technical interests → Money*

- *If Incidents occur, it is critical to have an effective means of responding.*

- *To limit the damage and lower the cost of recovery*
  - *Need to have the ability: Protect, Detect, Analyze and Respond to an incident.*
  - *Professional should respond to an Incident*

Multiple Disciplines Cooperation Motivation

- ***Need multiple communication network to share information timely and efficiently – CSIRT to bridge the gap:***
  - *Difficulties of communication between*
    - *Private sector and Public sector*
    - *Different function layers – CSIRT, Policy Makers, Law enforcement*
    - *competitors*
    - *International*
- ***Building a global distributed network of operational processes between CSIRT partners.***
  - *Systemic sharing of information and resources using the trusted network will minimize the coordination effort*
  - *Minimize potential for misunderstanding or mistakes when sharing sensitive information*
- ***Disclosing information as appropriate, as necessary***
  - *Keep working closely with private sectors, as independent neutral organization*
- ***Reducing the potential impact of incidents and vulnerabilities***

So, What does a CSIRT do?

- *Provides a single point of for reporting -*
  - *info@jpcert.or.jp for reporting incident*
  - *office@jpcert.or.jp for general contact*
  - *Vuls@jpcert.or.jp for vulnerability*

- *Assists the organizational constituency and general computing community in preventing and handling computer security incidents*

- *Share information and lesson learned with other CSIRT / response teams and appropriate organizations and sites.*

National POC CSIRT

JPCERT CC®

- *Service*
  - *National Focal point within a country to coordinate incident handling activities*
  - *Analyze incident and vulnerability information along with other teams, vendors, and technology experts to provide assessment for your constituency and communities*
  - *Bridging the gaps – brings together multiple different sectors (cross domain, cross public private sectors, cross boarder)*
  - *Developing mechanism for trusted communication for your community*

Security Culture in CSIRT Community

- *CSIRT Culture*
  - *My Security is depending on your security*

1. *Collaboration*
   - *Security is not competition*
   - *Share expertise/Resource*
   - *Best practices*

2. *Web of TRUST*
   - *most important thing for CSIRT*
   - *Reputation business – you live or die with this*

- ***You are part of the inter depending network***
- ***Let's work together to make the global infrastructure more safe place***