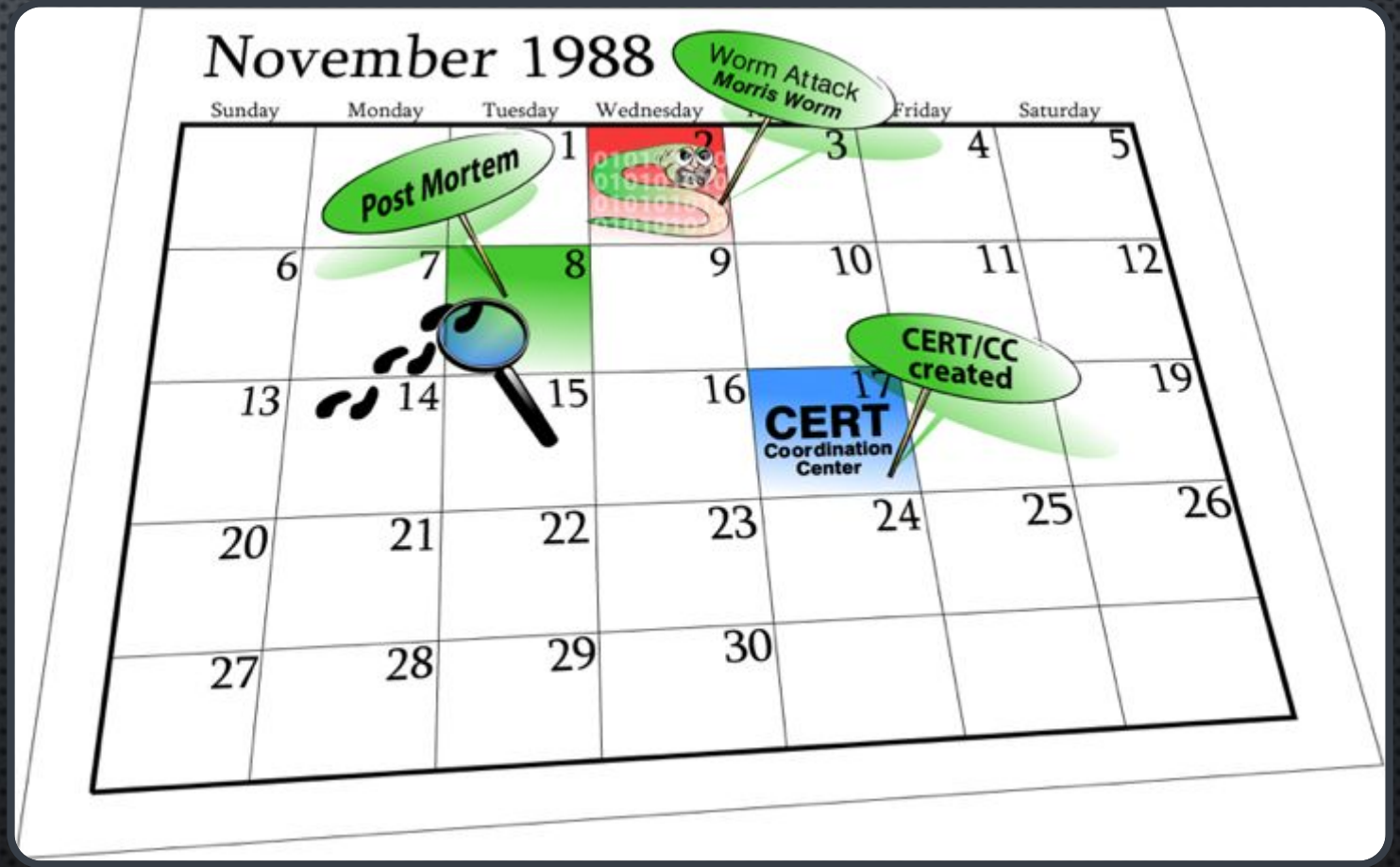
JPCERT CC®

Dr. Koichiro Komiyama
JPCERT/CC
global-cc@jpcert.or.jp

# FULL CIRCLE: ROLE OF CERT/CSIRT AFTER 35 YEARS.

# MORRIS WORM AND THE FIRST CSIRT WAS MADE

- A CSIRT IS LIKE "FIRE BRIGADE, FIRE FIGHTER" (ENISA 2008)



# NORM AGREED BY STATES

- 11 RECOMMENDATION OF UNGGE REPORT (JULY 2015)
  - (K) STATES SHOULD NOT CONDUCT OR KNOWINGLY SUPPORT ACTIVITY TO HARM THE INFORMATION SYSTEMS CSIRTS OF ANOTHER STATE.
  - STATE SHOULD NOT USE CSIRTS TO ENGAGE IN MALICIOUS INTERNATIONAL ACTIVITY.
  - QUASI-DIPLOMATIC FUNCTION.



(Photo by Andrew Burton/Getty Images)

# What people expect to CSIRT community

- Additional roles such as …
  - Attribution
  - Censorship
  - Surveillance
  - Offensive cyber
- Work as information sharing clearing house(EU NIS Directive, 2018)
- CSIRTs "should not be part of an intelligence or law enforcement agency" and "should not engage in control of content and the censorship of free speech, nor collect digital intelligence" (Morgus et al, 2015)

# Back to Framework:

# SOC, CERT/CSIRT and then Cyber Defense Center

# Secret Reciepe to protect the Game in 2021


## Issues Japan faced:

1. Only four years to prepare
2. Different work style, organization structure, luck of common terminology
3. People come and go

## Framework helped us:

1. A jump start
2. More comprehensive approach

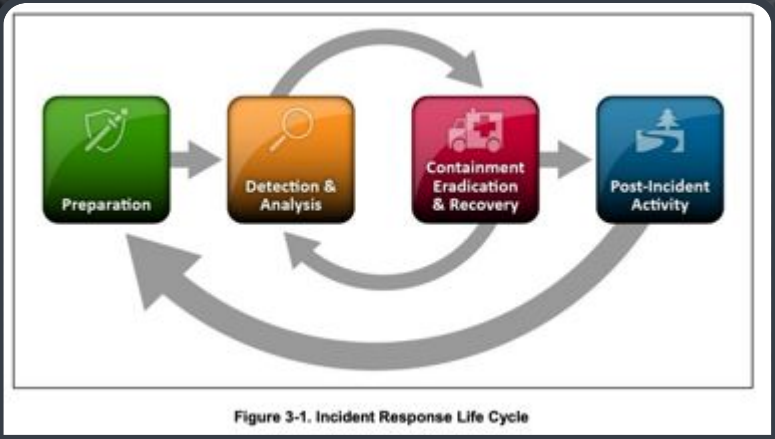
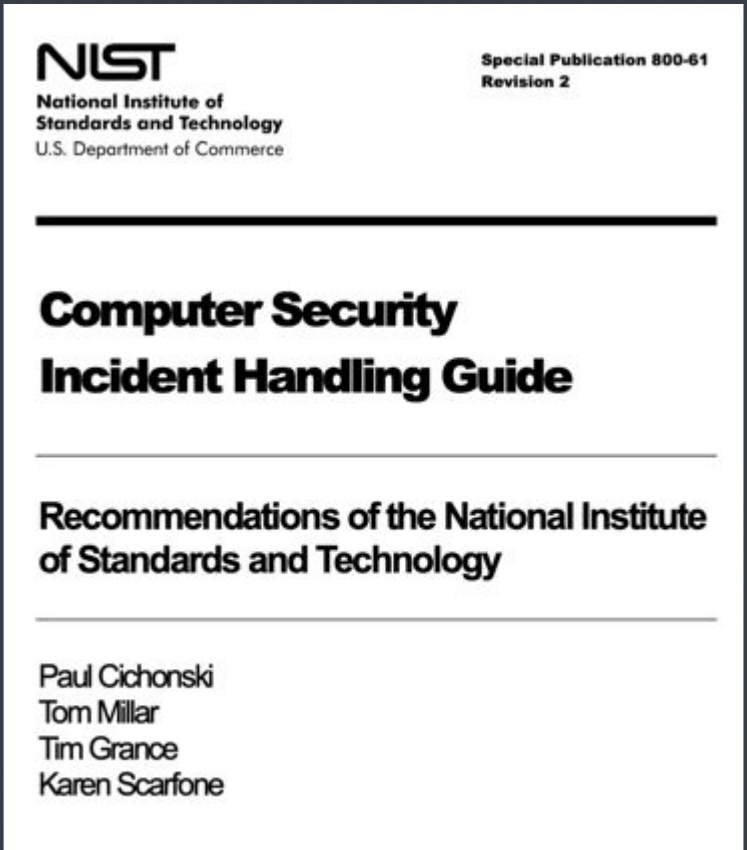


Figure 3-1. Incident Response Life Cycle


NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-61
Revision 2

**Computer Security Incident Handling Guide**

Recommendations of the National Institute of Standards and Technology

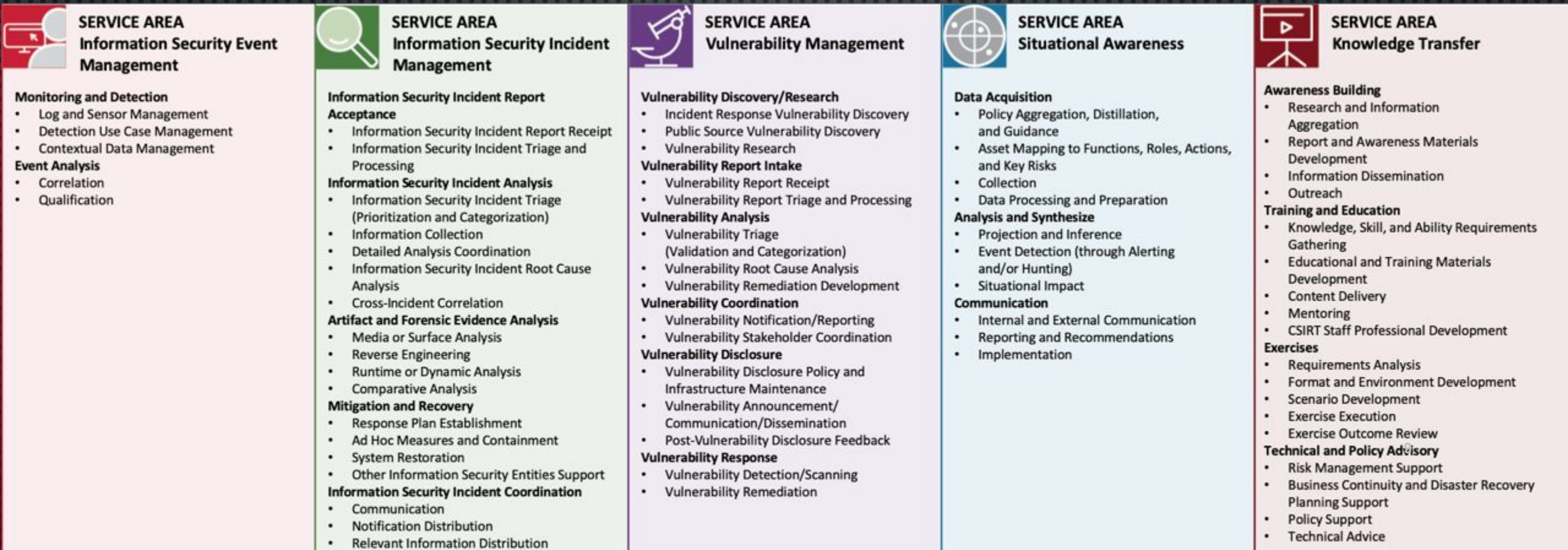
Paul Cichonski
Tom Millar
Tim Grance
Karen Scarfone

# NIST SP800-61 REV2

- PUBLISHED IN 2012
- GUIDANCE ON COMPUTER SECURITY INCIDENT HANDLING, INCLUDING THE ORGANIZATION AND MANAGEMENT OF INCIDENT RESPONSE TEAMS
- GENERIC ENOUGH TO BE USED IN INCIDENT RESPONSE ORGANIZATIONS OF ALL SIZES AND ALL TYPES

# FIRST CSIRT SERVICES FRAMEWORK V2.1

- Updated 2018 by FIRST members
- Available in seven languages(Fr, Arabic, Es, Chinese, Ru, Japanese)
- stemmed from a discussion at FIRST, it reflects  observations from  on the response operation.



**SERVICE AREA**
**Information Security Event Management**

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

**Event Analysis**
- Correlation
- Qualification

**SERVICE AREA**
**Information Security Incident Management**

**Information Security Incident Report Acceptance**
- Information Security Incident Report Receipt
- Information Security Incident Triage and Processing

**Information Security Incident Analysis**
- Information Security Incident Triage (Prioritization and Categorization)
- Information Collection
- Detailed Analysis Coordination
- Information Security Incident Root Cause Analysis
- Cross-Incident Correlation

**Artifact and Forensic Evidence Analysis**
- Media or Surface Analysis
- Reverse Engineering
- Runtime or Dynamic Analysis
- Comparative Analysis

**Mitigation and Recovery**
- Response Plan Establishment
- Ad Hoc Measures and Containment
- System Restoration
- Other Information Security Entities Support

**Information Security Incident Coordination**
- Communication
- Notification Distribution
- Relevant Information Distribution

**SERVICE AREA**
**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**
- Vulnerability Disclosure Policy and Infrastructure Maintenance
- Vulnerability Announcement/ Communication/Dissemination
- Post-Vulnerability Disclosure Feedback

**Vulnerability Response**
- Vulnerability Detection/Scanning
- Vulnerability Remediation

**SERVICE AREA**
**Situational Awareness**

**Data Acquisition**
- Policy Aggregation, Distillation, and Guidance
- Asset Mapping to Functions, Roles, Actions, and Key Risks
- Collection
- Data Processing and Preparation

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

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

**SERVICE AREA**
**Knowledge Transfer**

**Awareness Building**
- Research and Information Aggregation
- Report and Awareness Materials Development
- Information Dissemination
- Outreach

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

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

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

# ITU-T X.1060 CYBER DEFENCE CENTRE

- LESSONS LEARNED FROM TOKYO 2020
- ITU-T STANDARDIZE IT AS X.1060 IN 2021.
- **CSIRT + SOC + STRATEGY = CYBER DEFENCE CENTRE**
- 64 DIFFERENT SERVICES IN 9 DIFFERENT CATEGORIES

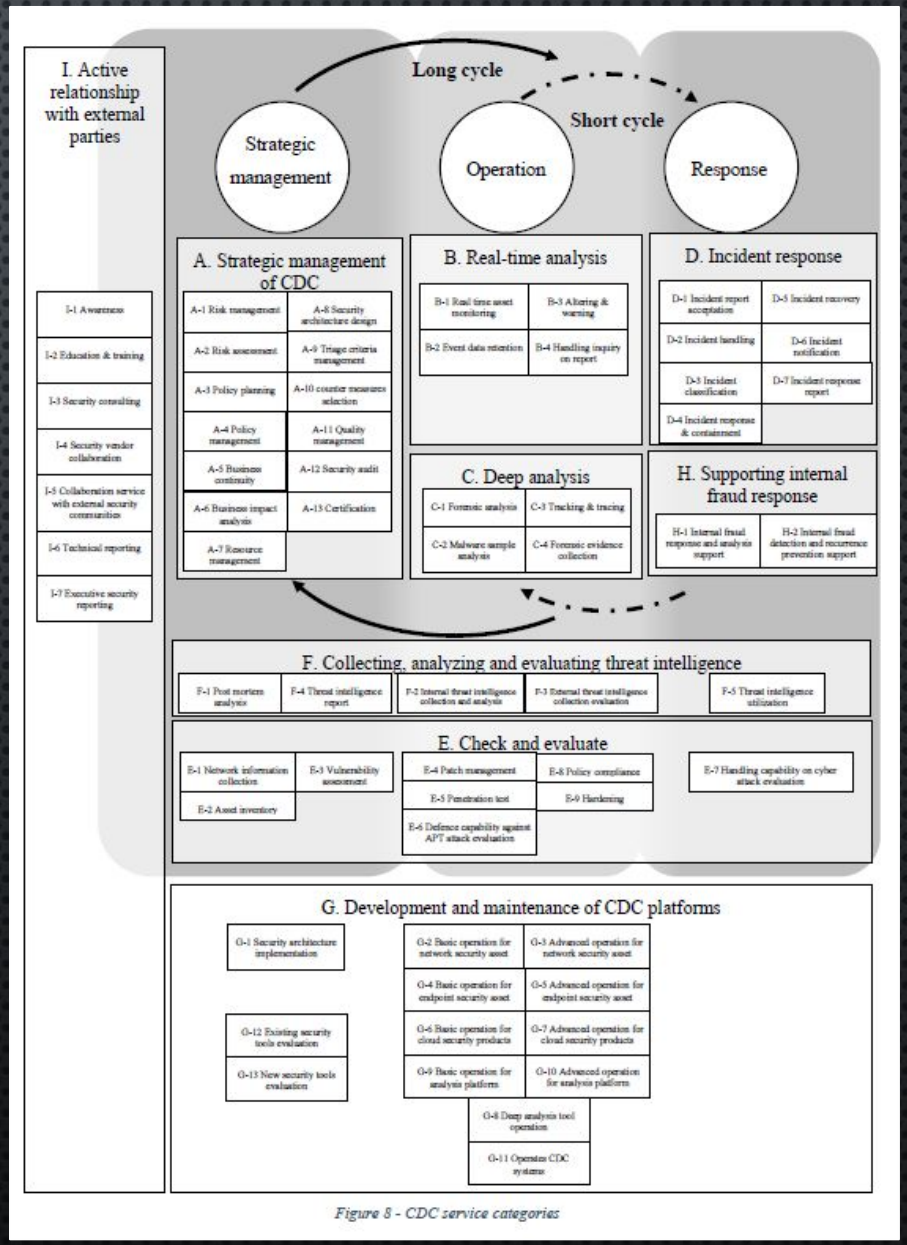



Figure 8 - CDC service categories

# Summary:

1. Role of CERT/CSIRTs are evolving Rapidly
2. Take advantage of Existing Frameworks!
3. Especially in a case, you need to build a large team in a short period of time.

Thank you