Information Sharing in Taiwan & Intelligence Add-on from Globe

Kun-Hsien Shih

TWNCERT

National Center for Cyber Security Technology

TWNCERT / NCCST

- TWNCERT ➔ Taiwan National Computer Emergency Response Team
  - https://www.twncert.org.tw
- NCCST ➔ National Center for Cyber Security Technology
  - https://www.nccst.nat.gov.tw/Default?lang=en

Outline

Information Sharing in Taiwan

- The Cyber Security Management Act
- The CIS Architecture
- The N-ISAC

Intelligence Add-on from Globe

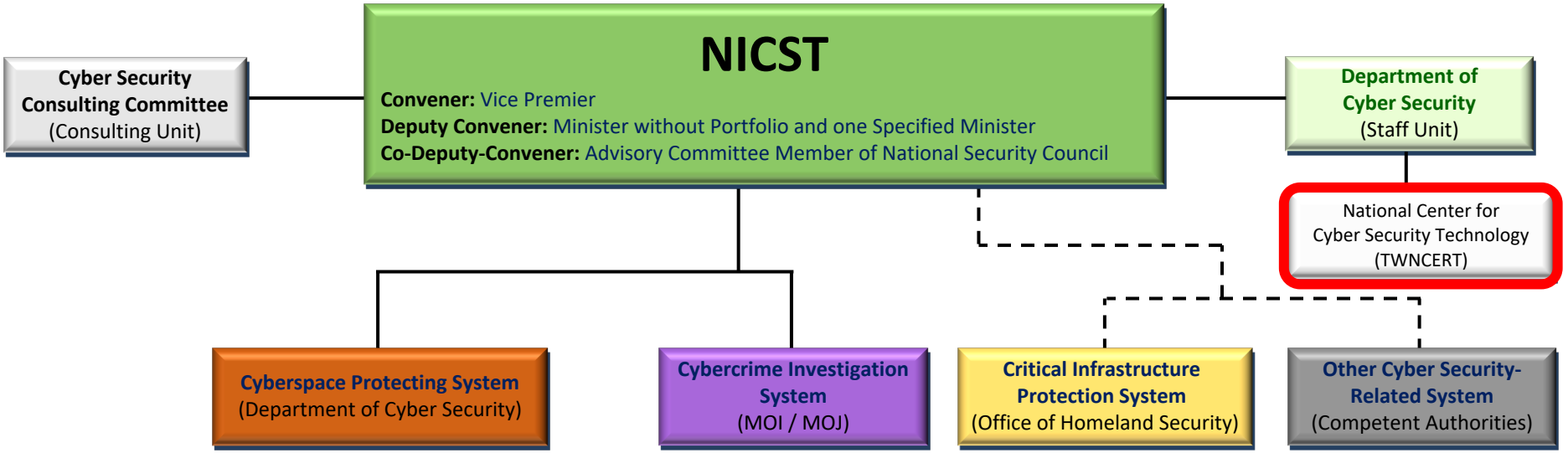
- CERT/CSIRT Community
- OSINT and Non-OSINT

Information Sharing in Taiwan

>>> The Cyber Security Management Act

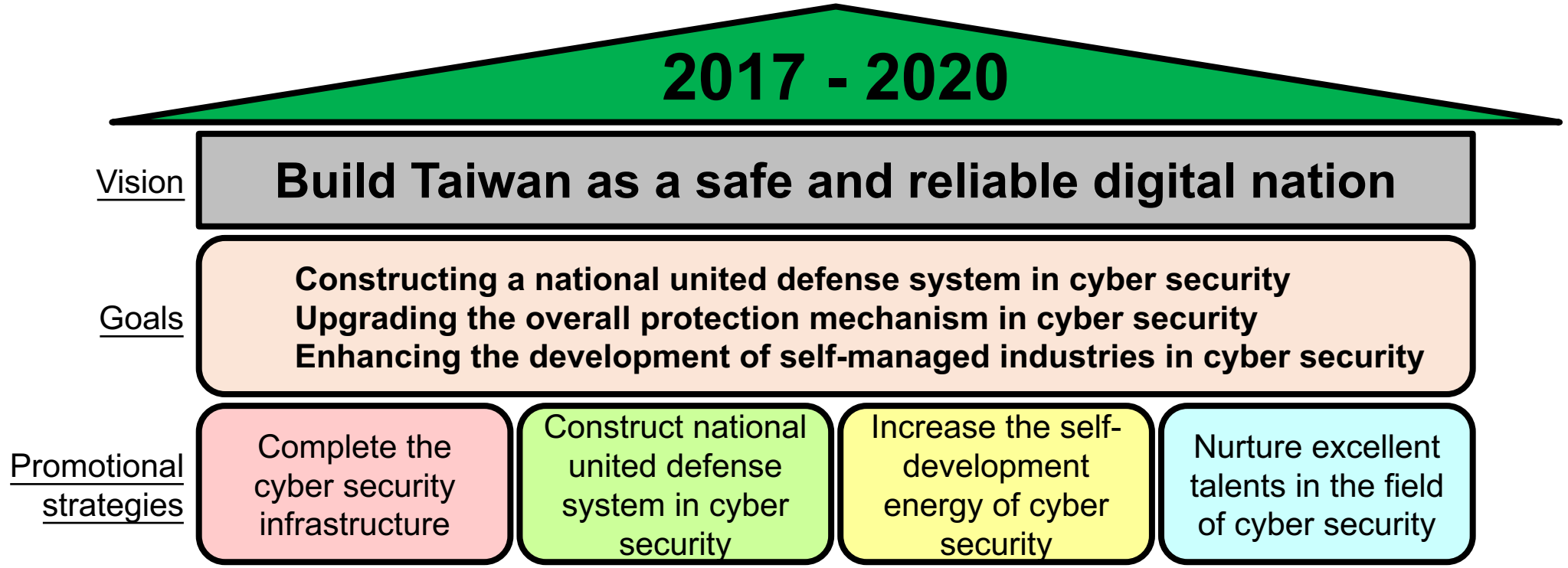
Cabinet Level Taskforce

- National Information & Communication Security Taskforce (NICST) was established in 2001, to actively promote national cyber security infrastructure tasks



National Cyber Security Program

TWNCERT
Taiwan National Computer Emergency Response Team
國家電腦事件處理中心



Cyber Security Management Act

TWNCERT
Taiwan National Computer Emergency Response Team
國家電腦事件處理中心

- Mission
  - Actively promote national cyber security policies
  - Safeguard national security
  - Drive development of cyber security industry
  - Maintain social and public interests
  - Accelerate construction of domestic cyber security environment
- Target Ordinance

Government Agencies

- **Central and Local Agencies**
- **Public Institutions Exercising Public Authorities**

Specific Non-Government Agencies

- **Critical Infrastructure Providers**
- **Government-Owned Enterprises**
- **Government-Founded Institutes**

Cyber Security Management Act

- The objective of the Act is to build a secure information environment to protect national security and public interests

Cybersecurity Management Act

Chapter 1
General Provision (§1~§9)

Chapter 2
Cyber Security Management of Government Agencies (§10~§15)

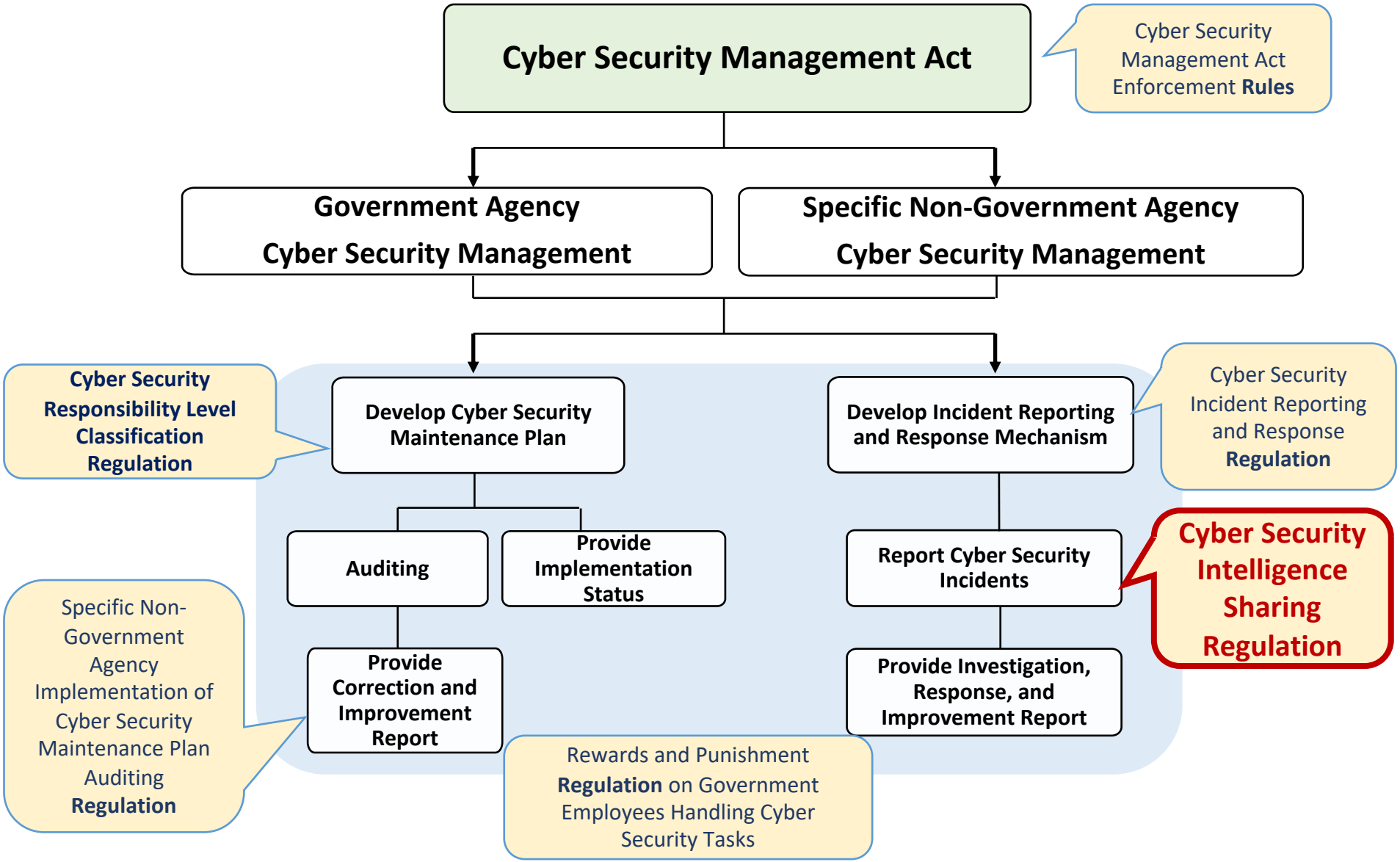
Chapter 3
Cyber Security Management of Specific Non-Government Agencies (§16~§18)

Chapter 4 Penalties (§19~§21)

Chapter 5 Appendix (§22~§23)

Purpose of Act, Terminologies, Industry Development, Authorities and Duties Delegation of Competent Authorities, Responsibility Ranking, **Information Sharing**, Outsourcing, etc.

Further Rules and Regulations

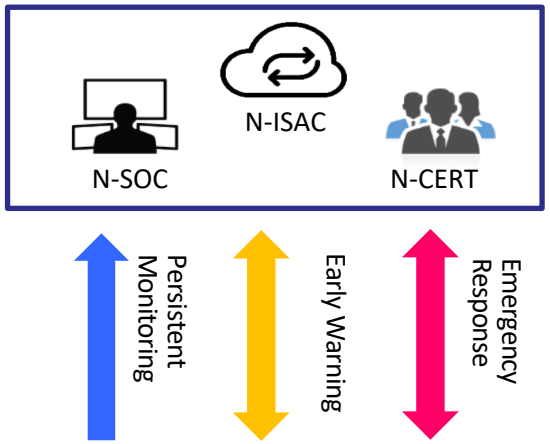


Information Sharing in Taiwan

>>> The CIS Architecture

>>> The N-ISAC

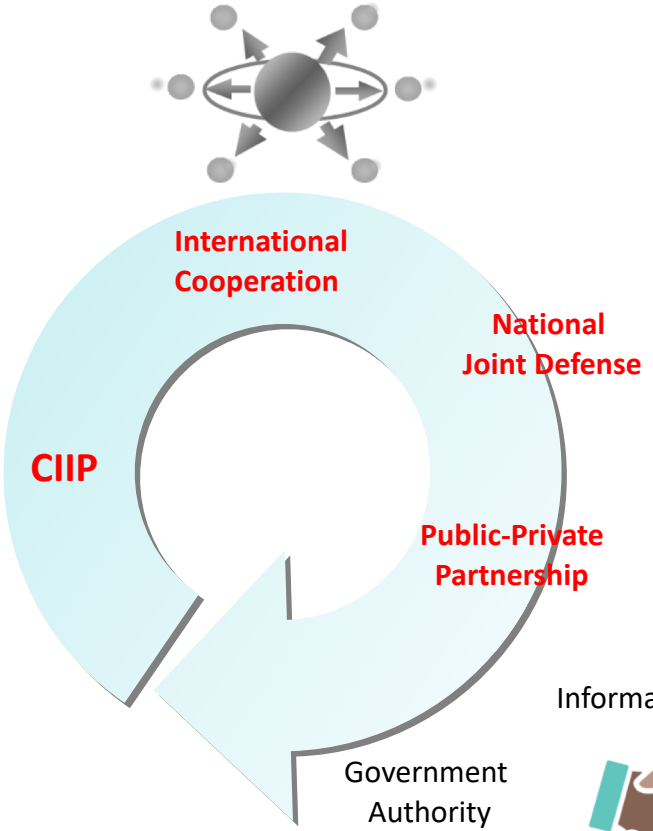
National Cyber Security Defense

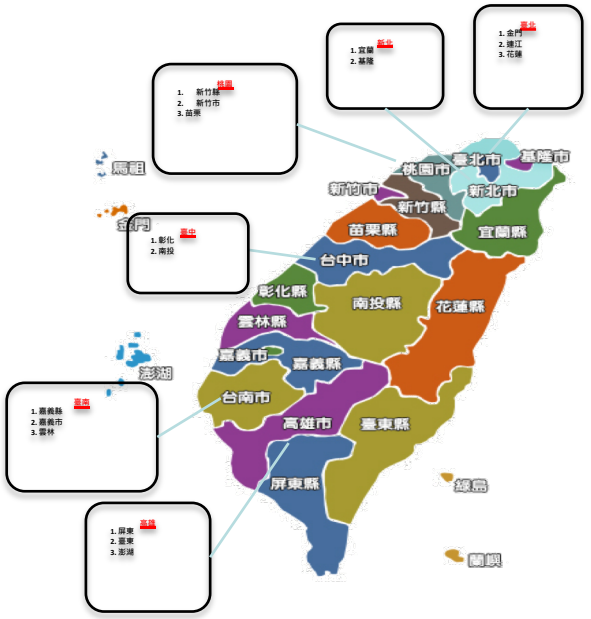


8 Domestic Critical Infrastructures

- Communications Commission
- Hygiene
- Financial Service
- Transportation
- Energy
- Water Resource
- High-Tech Park
- Government Authority

International Cyber Security Organization

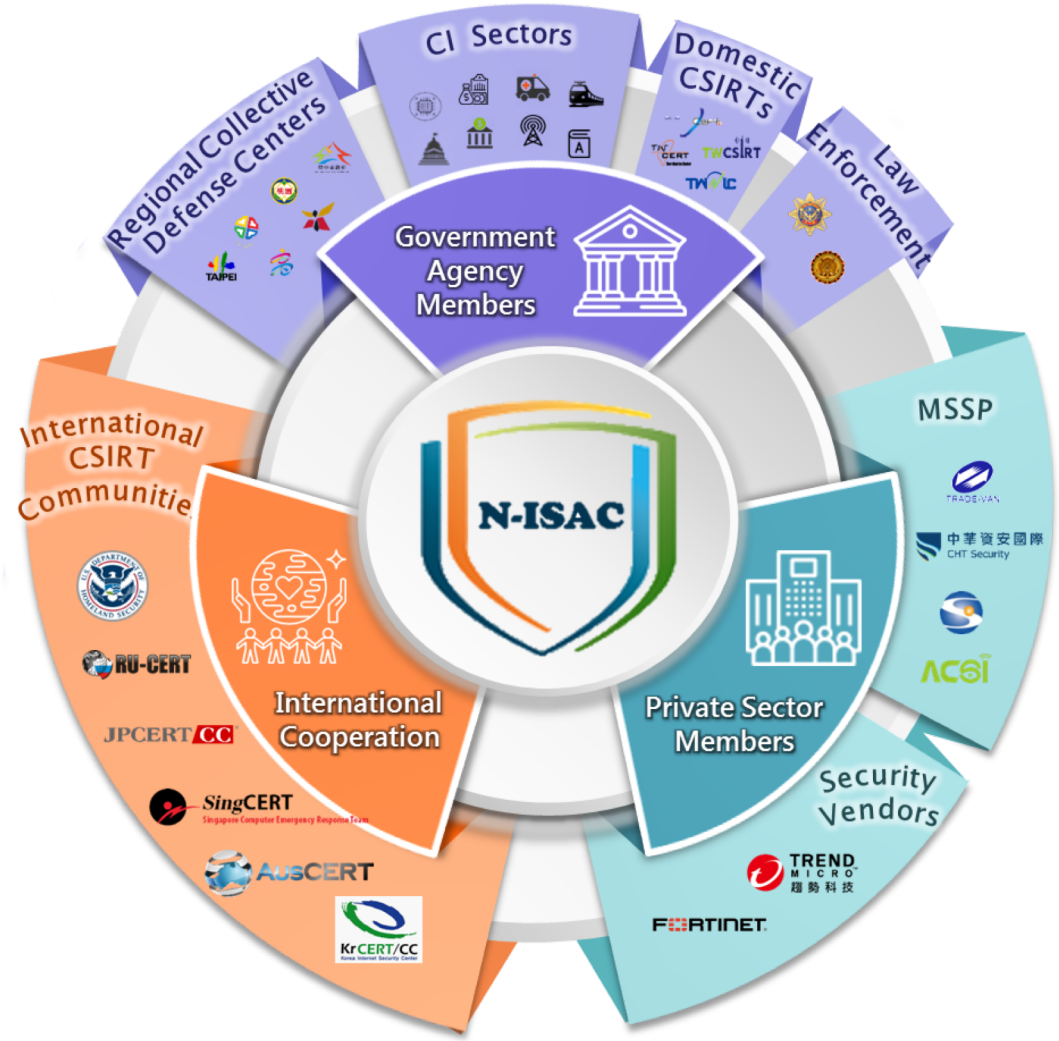




Information Exchange

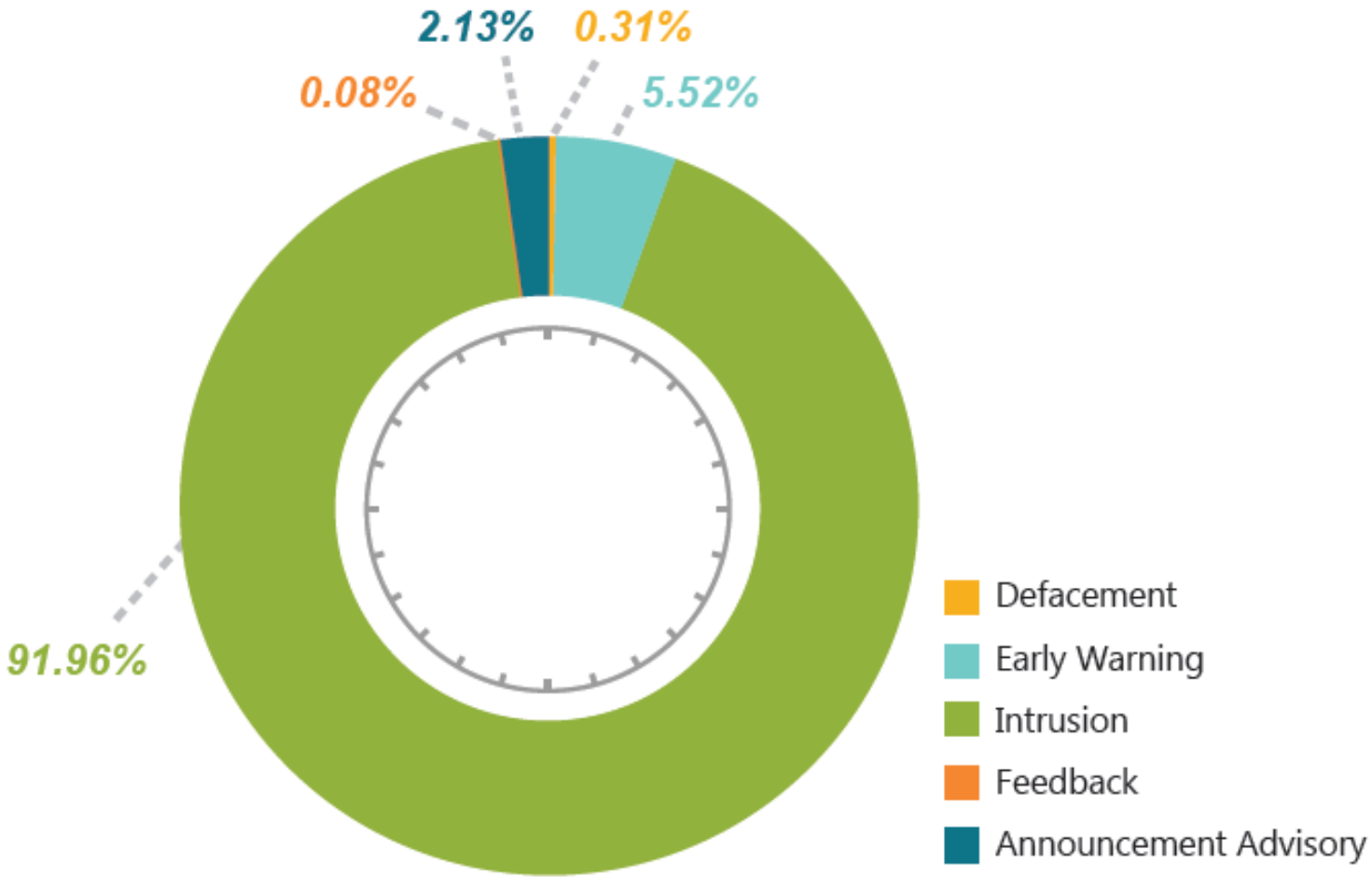
Cyber Security Organization,
Research Institute
or Software/Hardware
Application Developer

National Information Sharing & Analysis Center



Information Shared via N-ISAC

- N-ISAC members shared 178,454 information in 2018



Intelligence Add-on from Globe

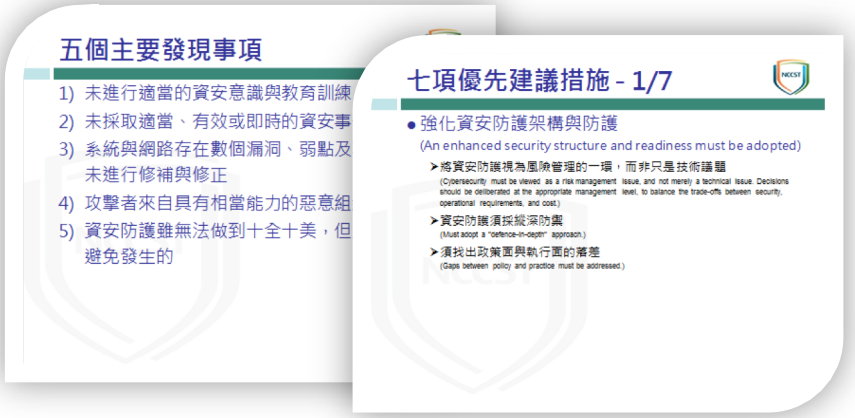
SingHealth Report

- From SingCERT to TWNCERT

PUBLIC REPORT OF THE COMMITTEE OF INQUIRY
INTO THE CYBER ATTACK ON
SINGAPORE HEALTH SERVICES PRIVATE LIMITED'S
PATIENT DATABASE
ON OR AROUND 27 JUNE 2018

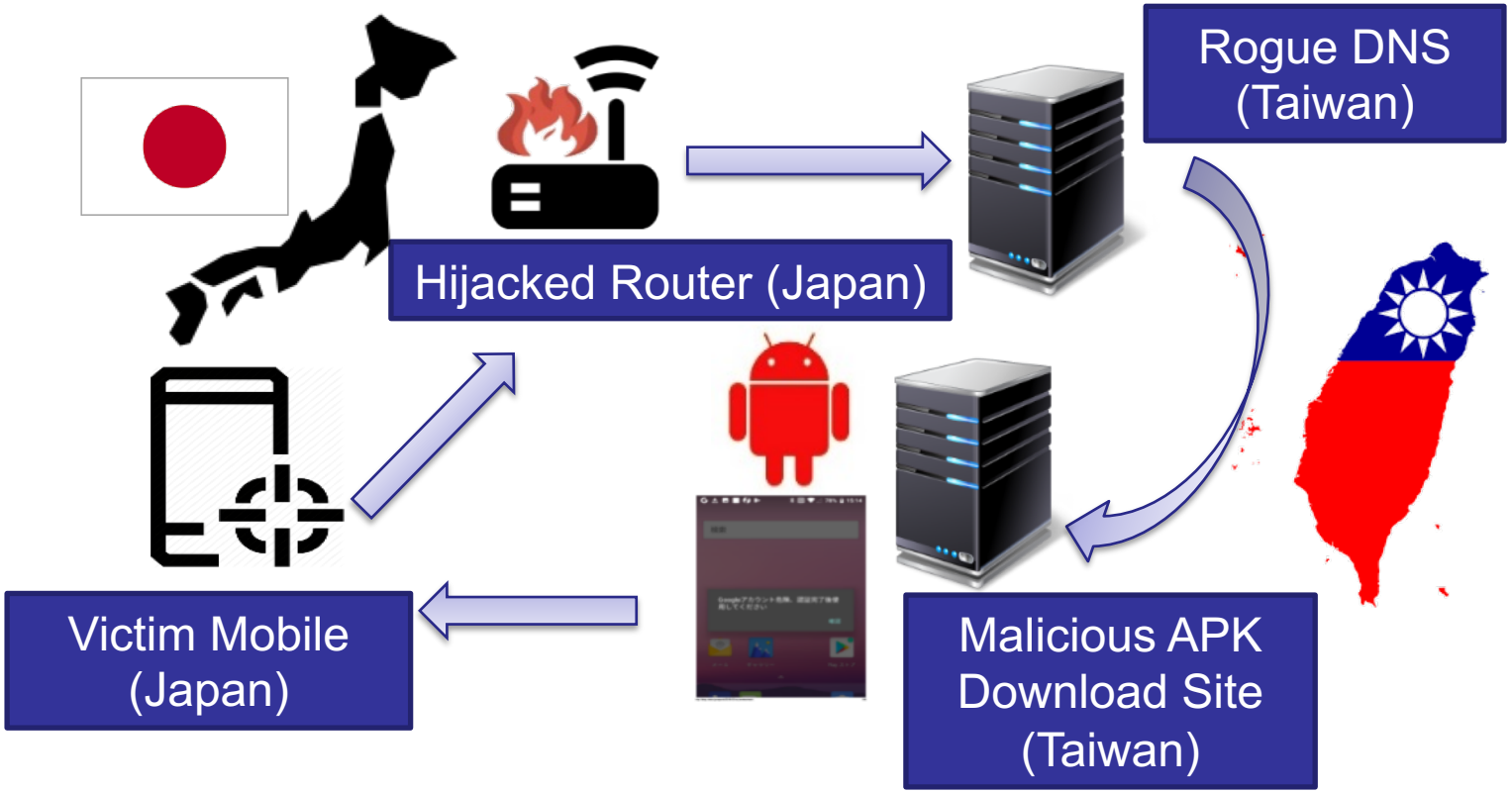
10 JANUARY 2019

N-ISAC

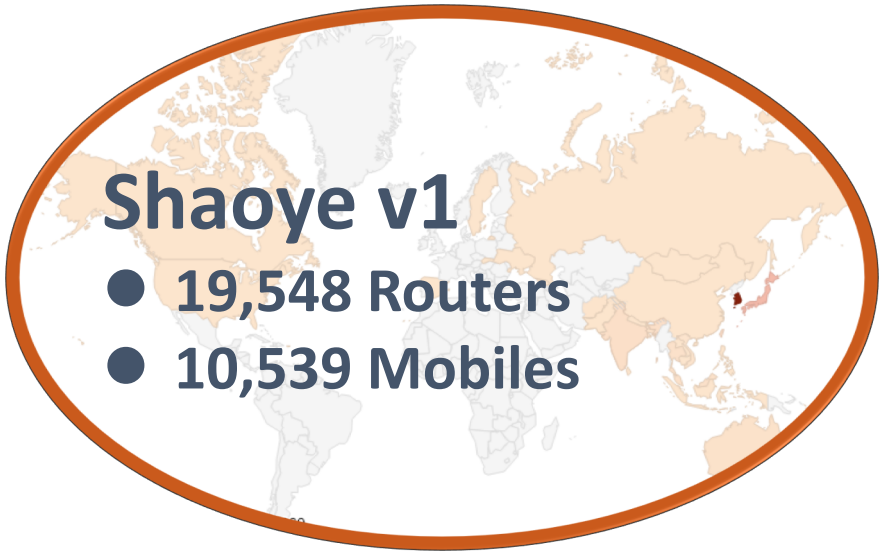


Abnormal Home Router DNS

- From JPCERT/CC to TWNCERT
- XLoader / Shaoye / FakeSpy



Share to the Globe



Shaoye v1

- 19,548 Routers
- 10,539 Mobiles

Shaoye v2

- 867 Mobiles

ACSC AUSTRALIAN CYBER SECURITY CENTRE

ANSSI

KrCERT/CC Korea Internet Security Center

CNCERT/CC

certin Handling Computer Security Incidents

CyberSecurity MALAYSIA

RU-CERT

SingCERT Singapore Computer Emergency Response Team

id-SIRTII/CC

JPCERT CC® Japan Computer Emergency Response Team Coordination Center

US-CERT UNITED STATES COMPUTER EMERGENCY READINESS TEAM

HKCERT

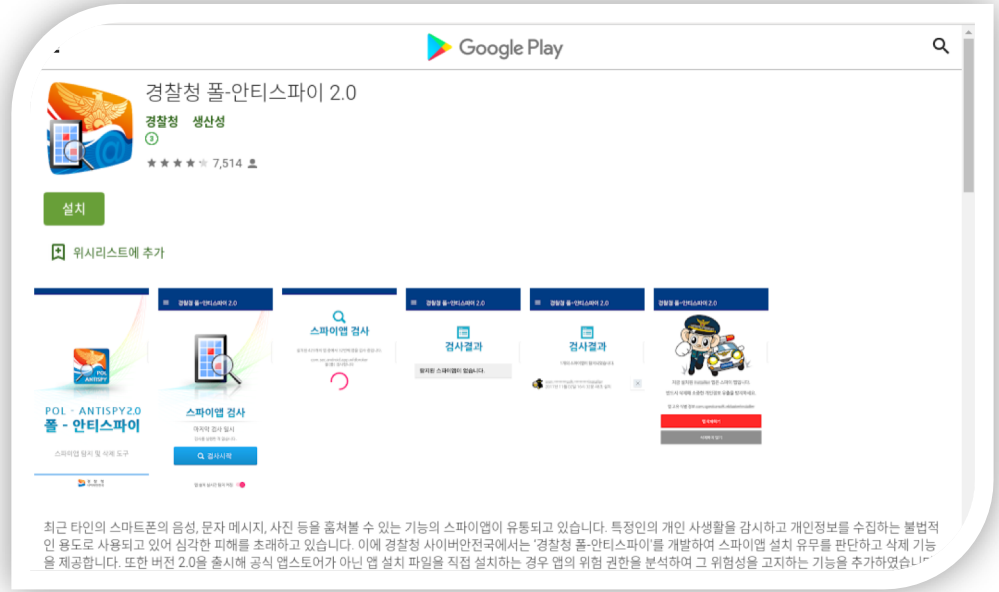
CERT Bund

computer emergency response team CERT-EU for the EU institutions, bodies and agencies

ThaiCERT Thailand Computer Emergency Response Team a member of ETDA

Phishing / Fake Google Play

- From KrCERT/CC to TWNCERT
- Phishing Page ➔ Fake Google Play, Malicious Police APK



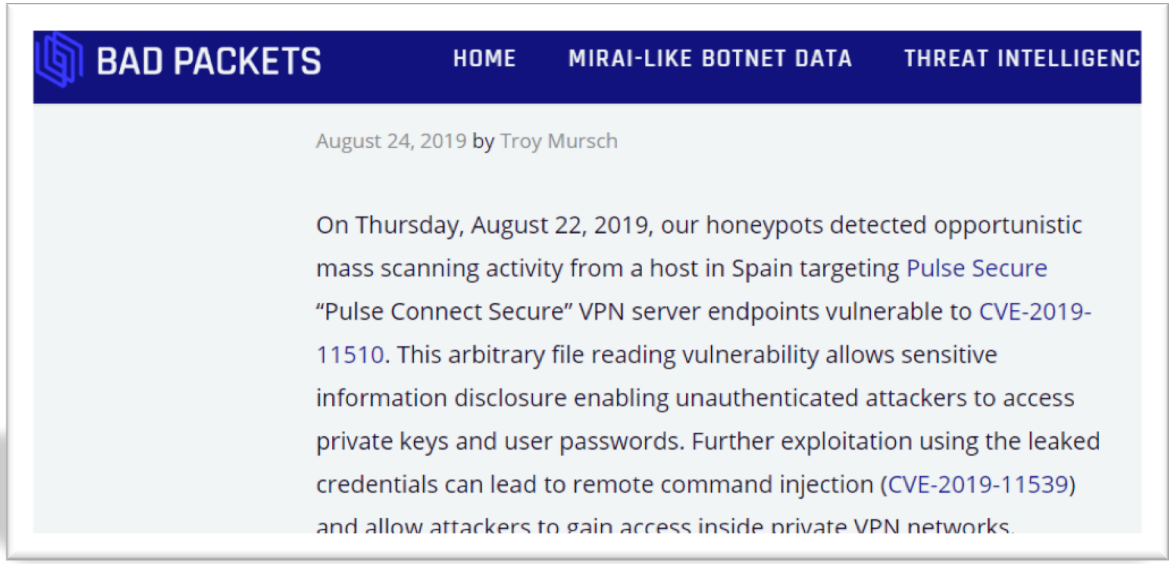
Share with KrCERT/CC

May 17th
➔Received phishing sites and verified them

May 22nd
➔Police malicious APKs on fake Google Play
➔Shared two Malicious APKs and two C2s

July 3rd
➔Finance and Banking malicious APKs on fake Google Play
➔Shared twelve C2s

Pulse Secure VPN Vulnerable



BAD PACKETS HOME MIRAI-LIKE BOTNET DATA THREAT INTELLIGENC

August 24, 2019 by Troy Mursch

On Thursday, August 22, 2019, our honeypots detected opportunistic mass scanning activity from a host in Spain targeting Pulse Secure "Pulse Connect Secure" VPN server endpoints vulnerable to CVE-2019-11510. This arbitrary file reading vulnerability allows sensitive information disclosure enabling unauthenticated attackers to access private keys and user passwords. Further exploitation using the leaked credentials can lead to remote command injection (CVE-2019-11539) and allow attackers to gain access inside private VPN networks.

N-ISAC

Aug. 28th

- ✓ ANA to all members
- ✓ EWA to specific members

Vulnerable Devices in Taiwan

Aug. 26th
217

Aug. 31st
25% 163

Sep. 16th
49% 111

From the Globe & To the Globe

APCERT Theme

Fostering A Safer Cyberspace Through Partnerships and Collaboration

Share to Better Cyber Security

Contact TWNCERT

TWNCERT
Taiwan National Computer Emergency Response Team
國家電腦事件處理中心

Taiwan National Computer Emergency Response Team

- Service Hotline: +886-2-2739-1000
- Fax hotline: +886-2-2733-1655
- Email: twncert@twncert.org.tw
- Report an Incident:irr@twncert.org.tw

Thank You