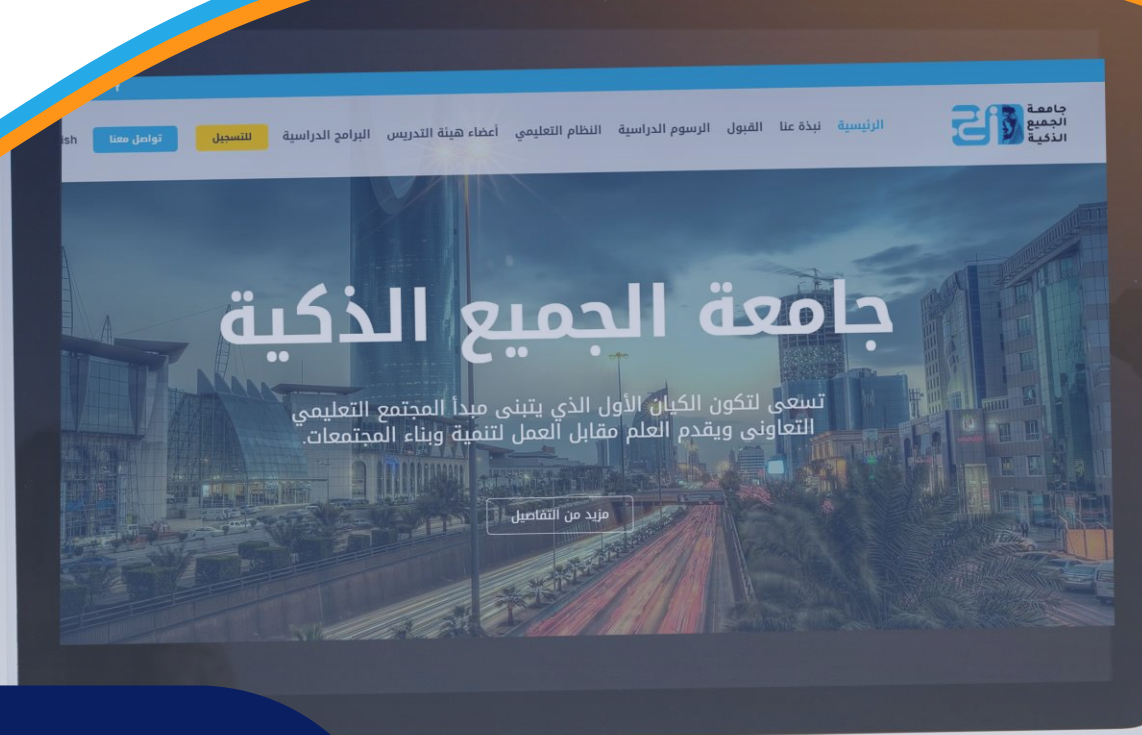




جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY



HCIA Security
Prepared by Eng. Abdelrhman Ahmed
Lecture 10

Cyber Security Emergency
Response

- The Internet of Things (IoT), mobile Internet, cloud computing, and big data are booming. Emerging technologies are reshaping the world. However, cyber security incidents are still on the rise, increasing people's concerns about cyber safety.
- In 2017, global cyber attacks, such as WannaCry ransomware, occurred at a high rate. It is difficult to effectively monitor and provide alerts for unexpected global security incidents. Furthermore, nations tend to be reactive instead of proactive when it comes to security incidents. This slide provides references for security incident responses.

- **Upon completion of this course, you will be able to:**
 - ❑ **Understand the background of cyber security emergency response.**
 - ❑ **Describe the handling process of cyber security emergency response.**
 - ❑ **Understand new trends in cyber security emergency response.**

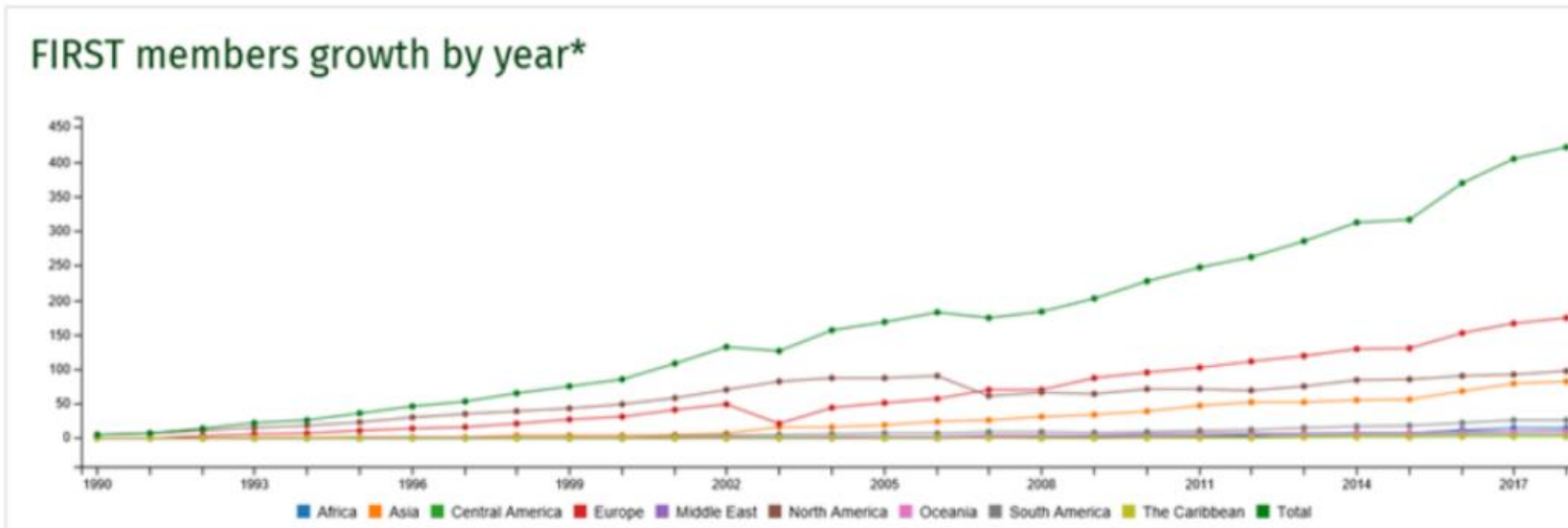
Background of Information Security Emergency Response

- The Morris Worm Incident, which occurred in November 1988, forced over 10% of Internet systems to stop working. This incident shocked the world and deeply concerned computer science professionals.
- A Computer Emergency Response Team (CERT) and the CERT Coordination Center (CERT/CC) for Internet security was founded in 1989 following the Morris worm incident. At that time, the Defense Advanced Research Projects Agency (DARPA) tasked Carnegie Mellon University's Software Engineering Institute (SEI) with developing a communication coordination center to connect experts during security emergencies and to help prevent future intrusion

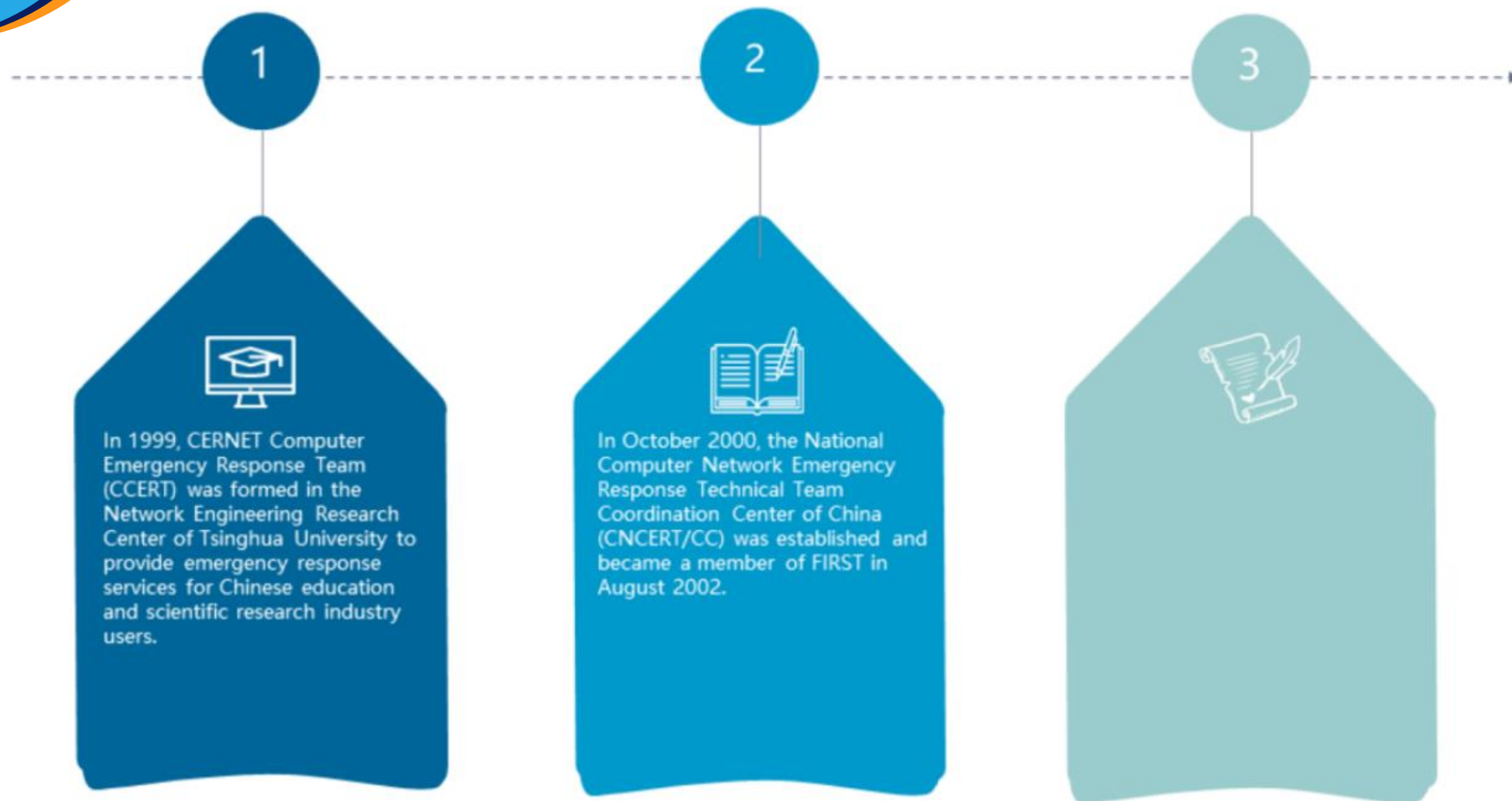


FIRST Background

- Security emergency response organizations in different countries face communication and cooperation difficulties because they use different languages and time zones and serve different user groups.
- The Forum of Incident Response and Security Teams (FIRST), founded in 1990, was initially formed by 11 security emergency response organizations, and currently has more than 400 members worldwide.



Emergency Response Organizations in China



CNCERT/CC

- Founded in September 2002, CNCERT/CC is a non-governmental and non-profit cyber security technical center. It is a core organization that helps to coordinate the cyber security emergency system in China.
- CNCERT has actively established international cooperation on cyber security. As of 2017, CNCERT had established "CNCERT International Cooperation Partnership" with 211 organizations in 72 nations and regions.



Forum of Incident Response
and Security Teams



Anti-Phishing
Working Group



Asia Pacific Computer Emergency Response
Team

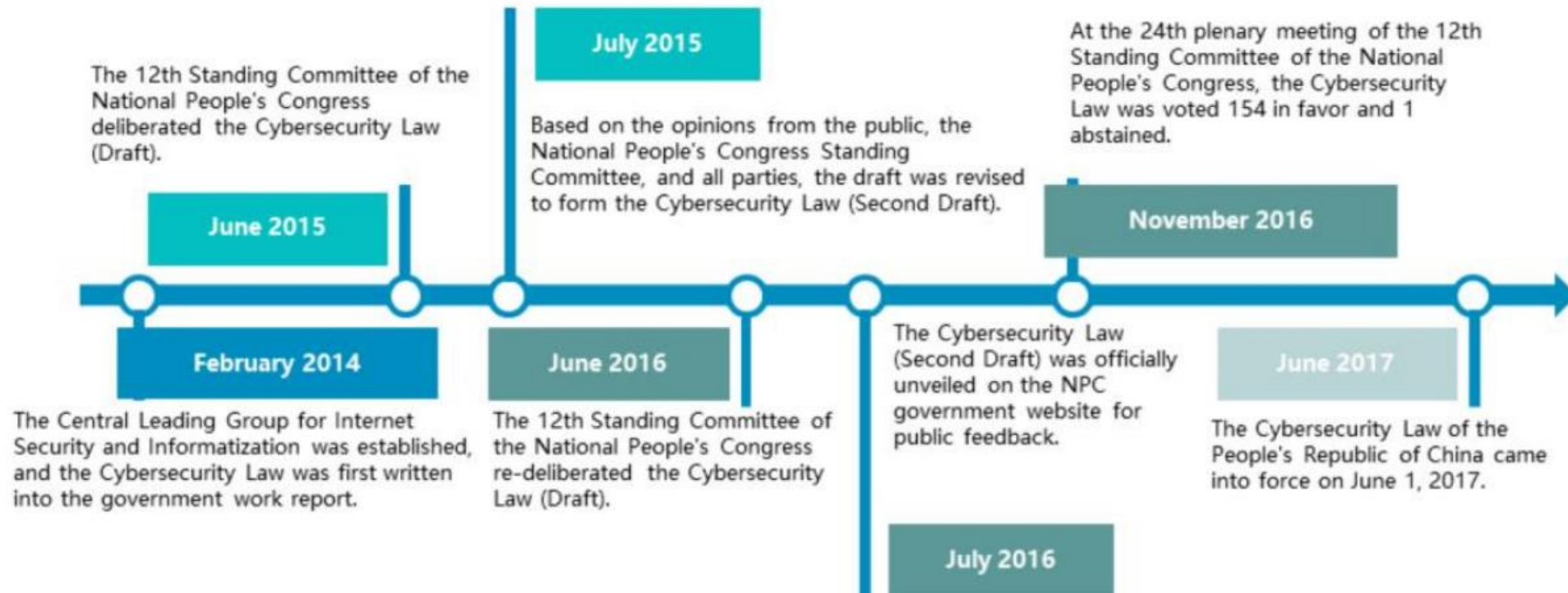


Cymru

CNCERT International Cooperation Partnership

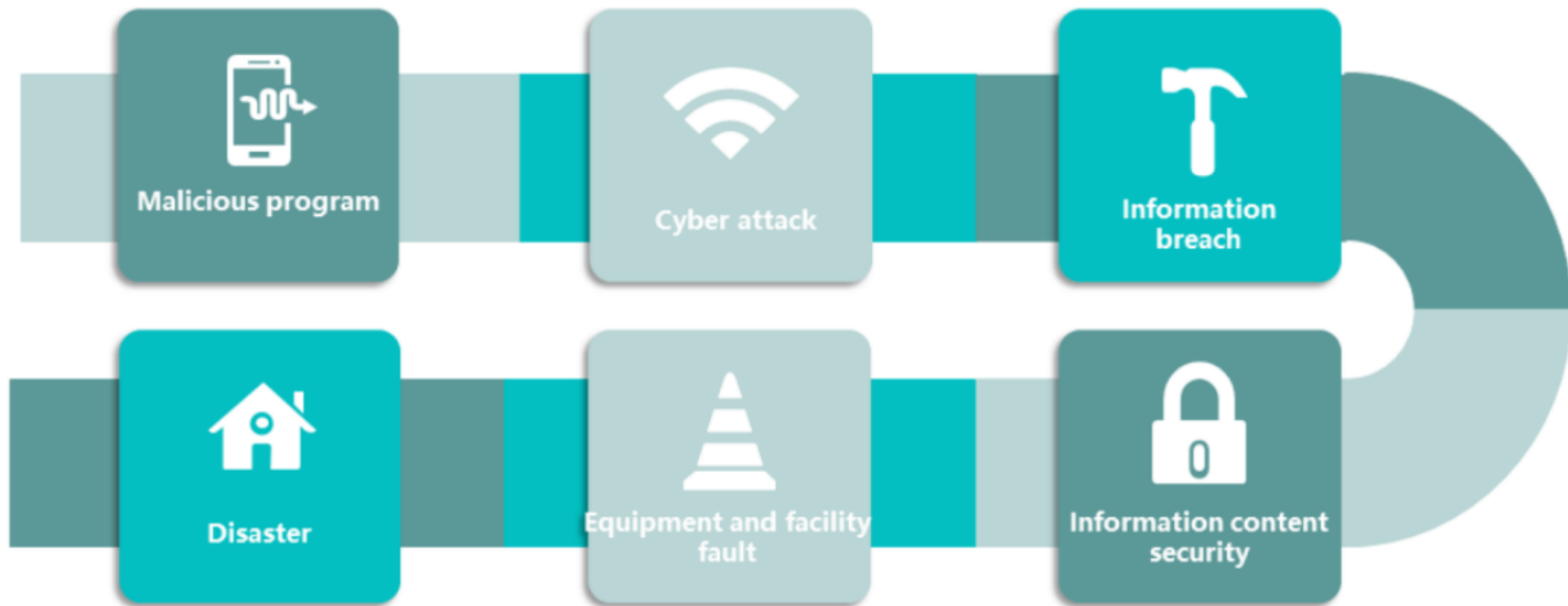
Cyber Security Laws and Regulations in China

- The Cybersecurity Law of the People's Republic of China was adopted by the Standing Committee of the National People's Congress (NPC) in November, 2016, and came into force on June 1, 2017. The Cybersecurity Law is China's first to provide guidelines on cyber security.
- The Cybersecurity Law underwent three years of deliberation before its final release.



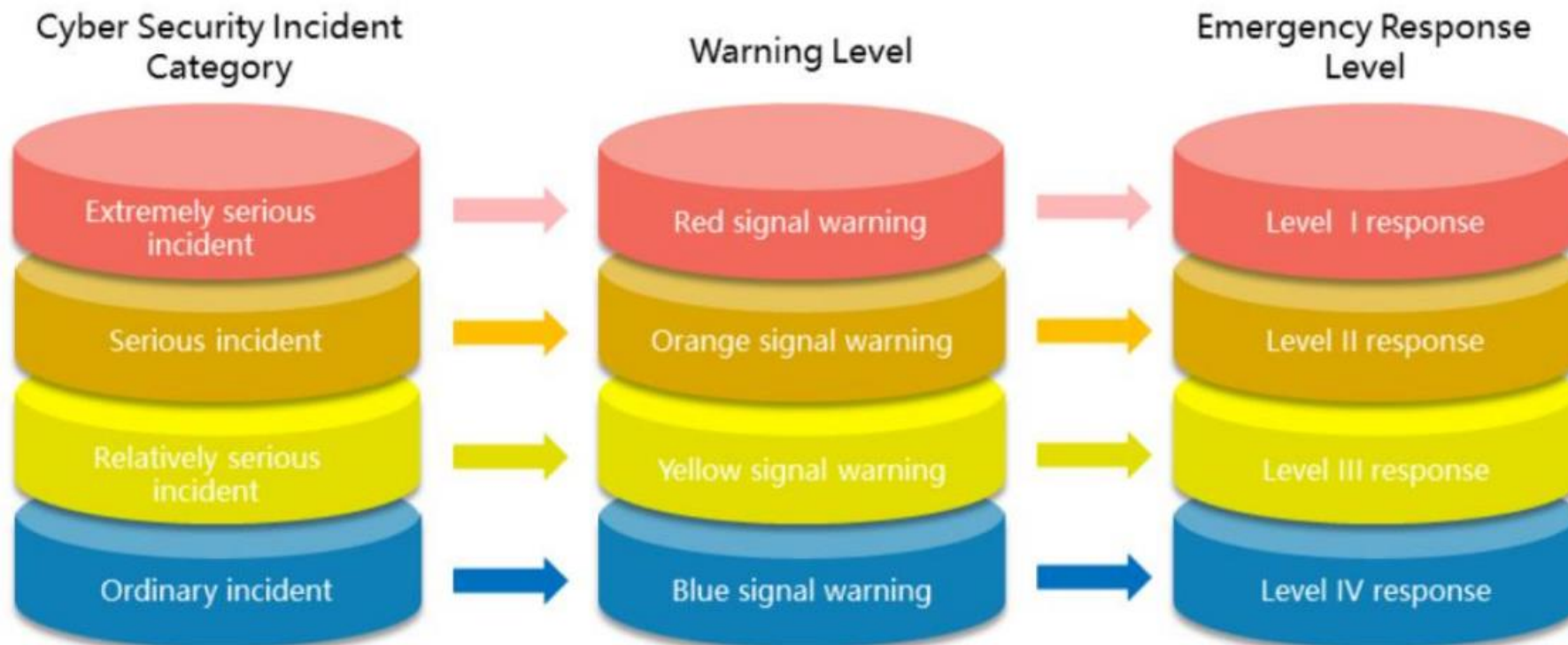
Cyber Security Incident Classification

- Cyber security incidents are classified as follows in the National Emergency Plan for Cyber Security Incidents:



National Cyber Security Incident Categories

- The National Emergency Plan for Cyber Security Incidents clarifies the enforcement solution for Chapter V "Monitoring, Early Warnings, and Emergency Responses" of the PRC Cybersecurity Law. The Plan divides incidents into four categories, which correspond to four warning levels and emergency response levels.



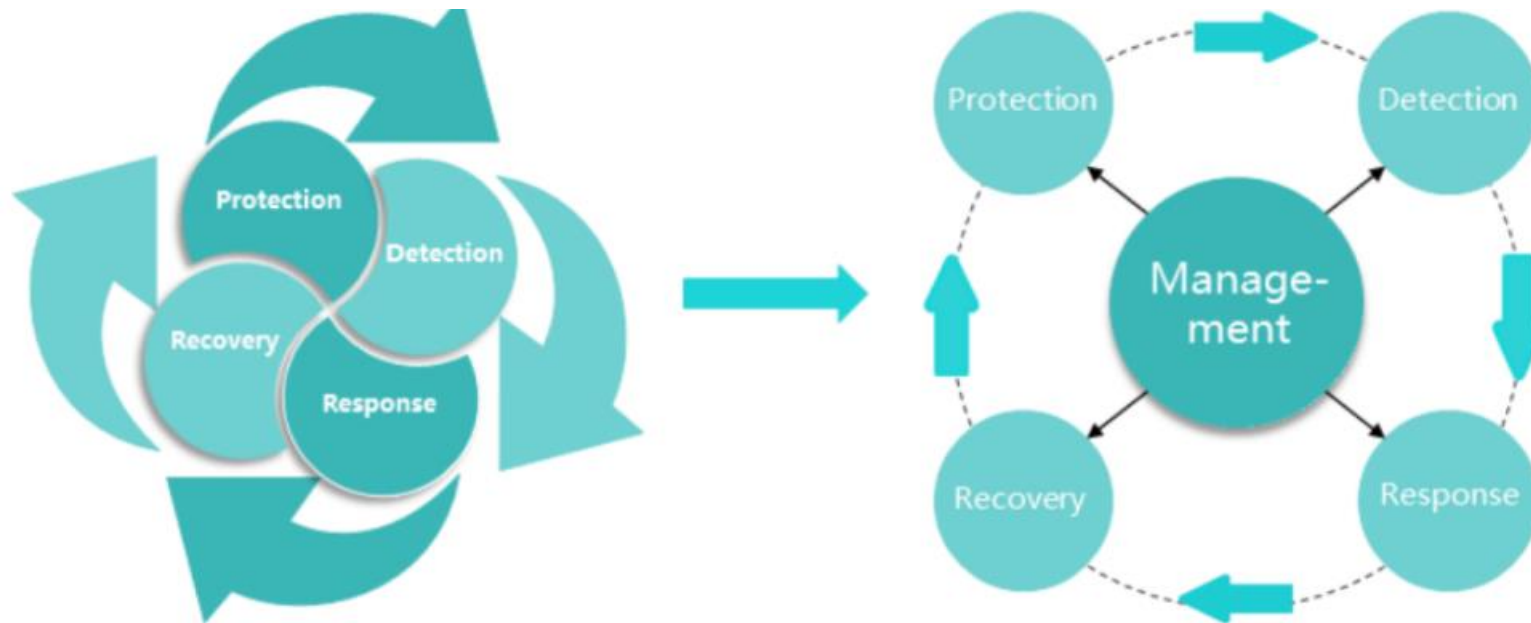
Concept of Incident Response/Emergency Response

- Incident response/emergency response refers to the preparations made by an organization to respond to emergencies and major information security incidents and the measures taken after the incident occurs.
- — GB/T 24363-2009 Information Security Emergency Response Plan Specifications
- The emergency response object of an information system security incident refers to the security incident of the information stored, transmitted, and processed by the information system. The incident subject may be caused by natural events, system faults, or manual attacks from internal or external personnel.
- —GA/T 708-2007 Architecture framework of security classification protection for information system



Cyber Security Emergency Response Model

- MPDRR is an acronym for management, protection, detection, reaction, and recovery. The MPDRR model is a common cyber security model with an in-depth defense system.
- The MPDRR model is developed based on the PDRR (protection, detection, recovery, response) model. It inherits the advantages of the PDRR model and adds security management to security technologies.



Cyber Security Emergency Response Types

- **Emergency response types:**

- ❑ **Remote emergency response (preferred):** Emergency response teams handle security incidents by telephone, email, or fax after receiving incident reports from customers.
- ❑ **Local emergency response:** Emergency response teams shortly arrive at the sites where cyber security incidents occur, locate the causes, resolve the issues, and create detailed emergency response reports.

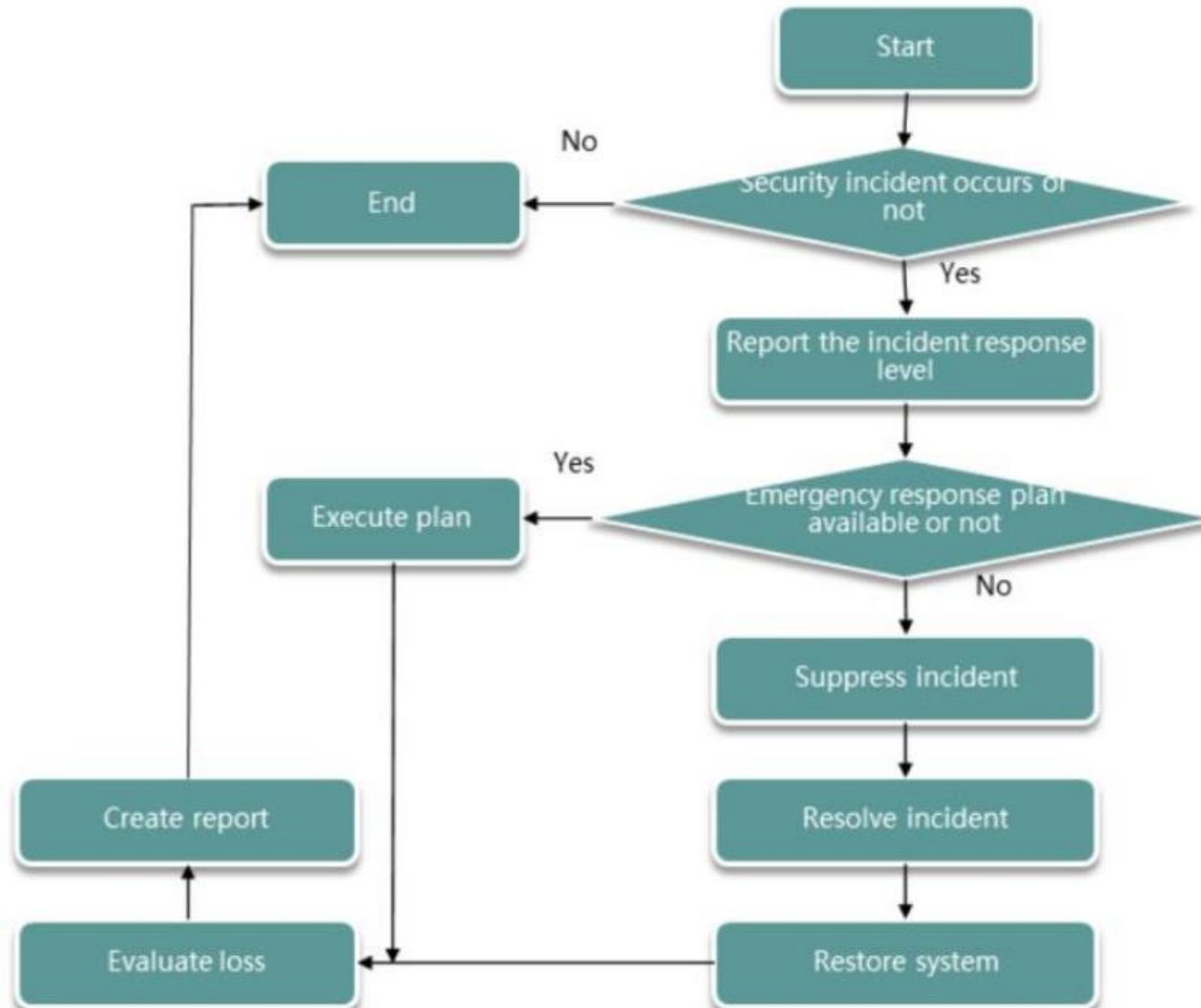


Remote emergency response



Local emergency response

Handling Process of Cyber Security Emergency Response



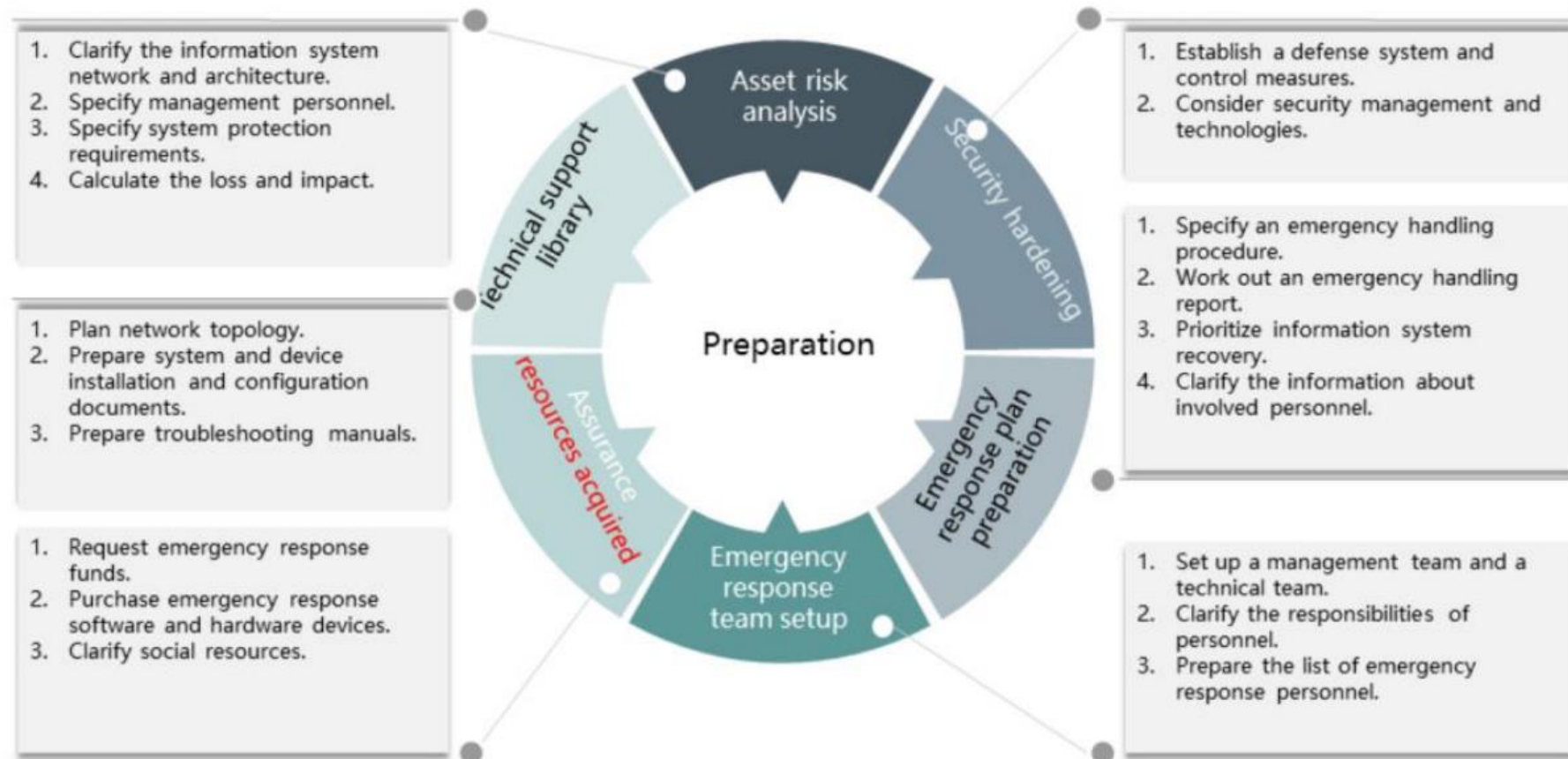
Cyber Security Emergency Response

- Cyber security emergency response plays an important role in tracing, handling, and preventing emerging cyber security incidents to ensure network information security. Currently, emergency response includes:



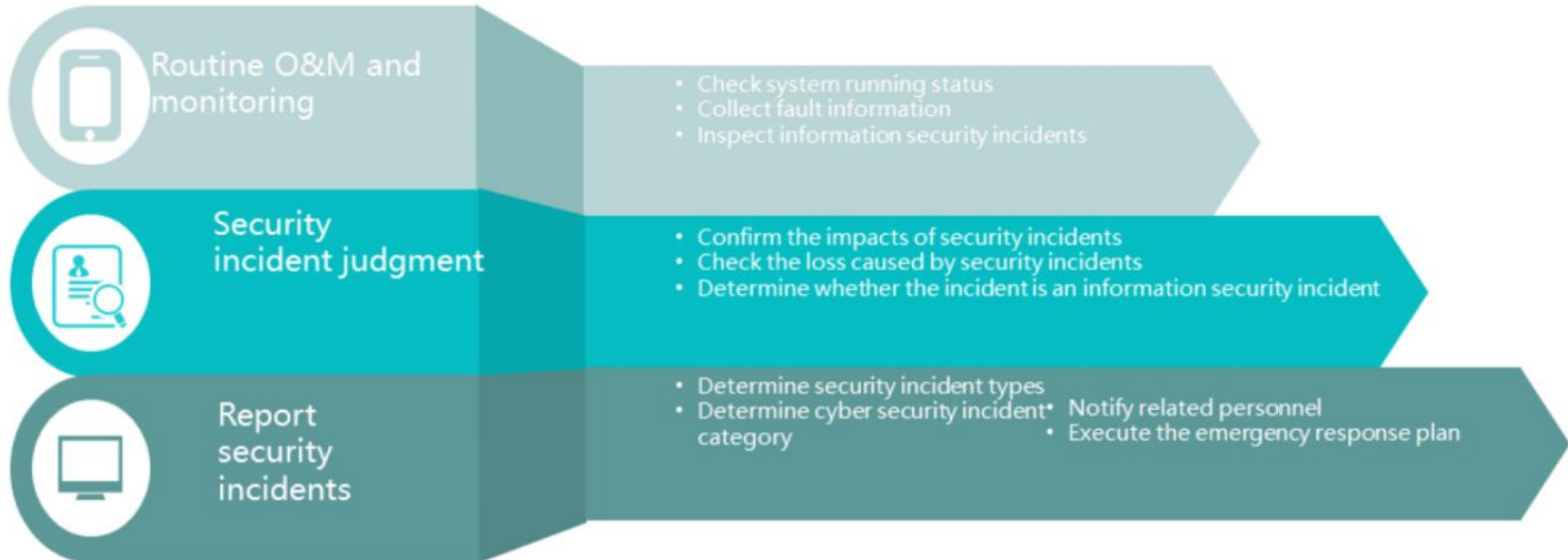
Preparation

Assess potential security incidents and formulate corresponding policies and assurance measures to suppress and resolve security incidents.



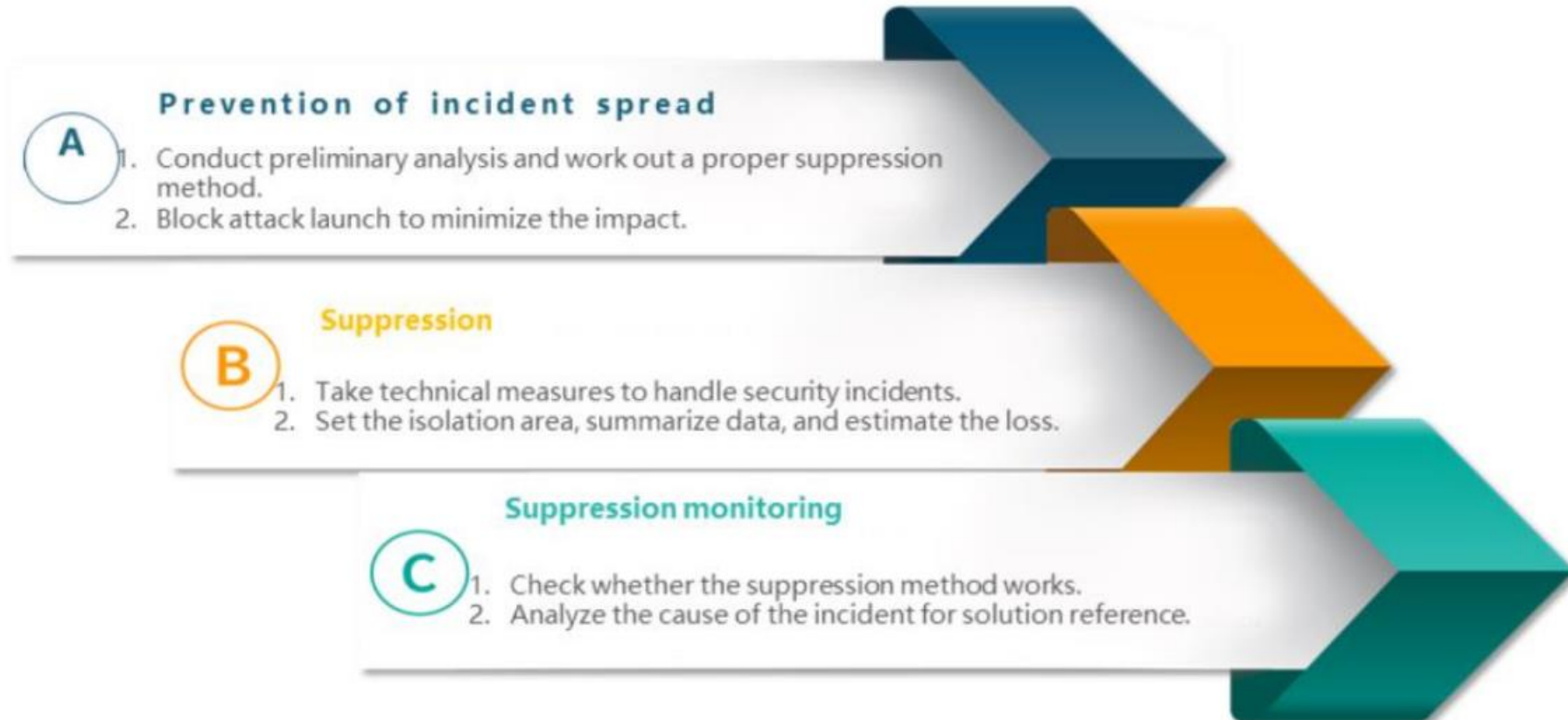
Detection

- Perform routine monitoring and collect system information. If a network security incident occurs, determine its impact and category, and report the incident



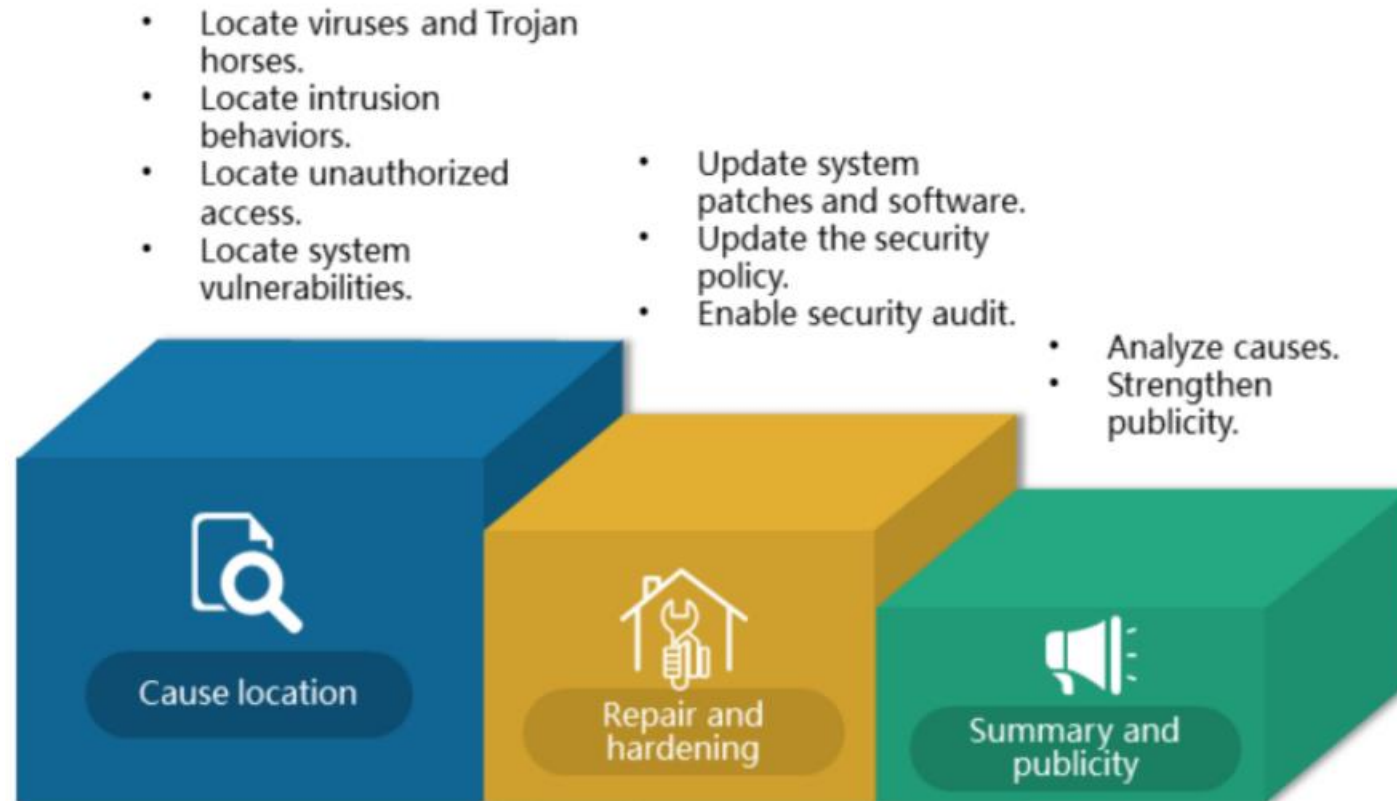
Suppression

- Restrict the scope of attacks and limit potential loss and damage. If an emergency incident is detected, start the emergency response process to minimize the impact of the incident.



Incident Resolving

- After the security incident is suppressed, locate the root cause to resolve the incident.



Recovery

- Restore all the compromised systems, applications, databases, and network devices to normal status.
- ☐ Restore network device configurations.
- ☐ Restore data or systems.
- ☐ Back up all changes.
- ☐ Check running status of the devices that recover.
- ☐ Check whether the isolation measures work. Remove isolation measures or short-term suppression defense measures if site situation improves.



Conclusion

- Learn lessons from security incident responses, and summarize information about security incidents.



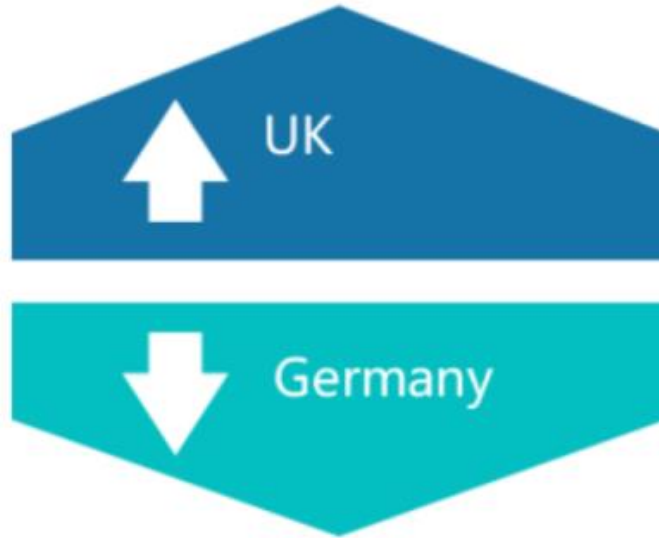
Global Major Security Incidents

- The IoT, mobile Internet, cloud computing, and big data are booming. Emerging technologies are reshaping the world. However, cyber security incidents are still on the rise, increasing people's concerns about cyber safety.



Cyber Security Laws/Regulations

- In 2017, global pilot projects focusing on cyber security laws and regulations were initiated in critical infrastructure, personal data security, and cyber emergency response. As a result, some countries have introduced trial security assurance regulations on autonomous driving.



The core Internet and automobile security principles have enforced cyber security responsibilities on each stakeholder of the automobile supply chain, requiring cyber security throughout the entire automobile lifecycle. Moreover, the principles have set the cyber security bottom line: Ensure basic automobile security even if the automobile is attacked.

The ethics code for autonomous and Internet vehicles gives clear description of controversial automated driving ethics. For example, it prohibits programming to dilemmas. Vendors shall be liable for the damages caused by their automation systems/products.

New Trend in Cyber Security Emergency Response

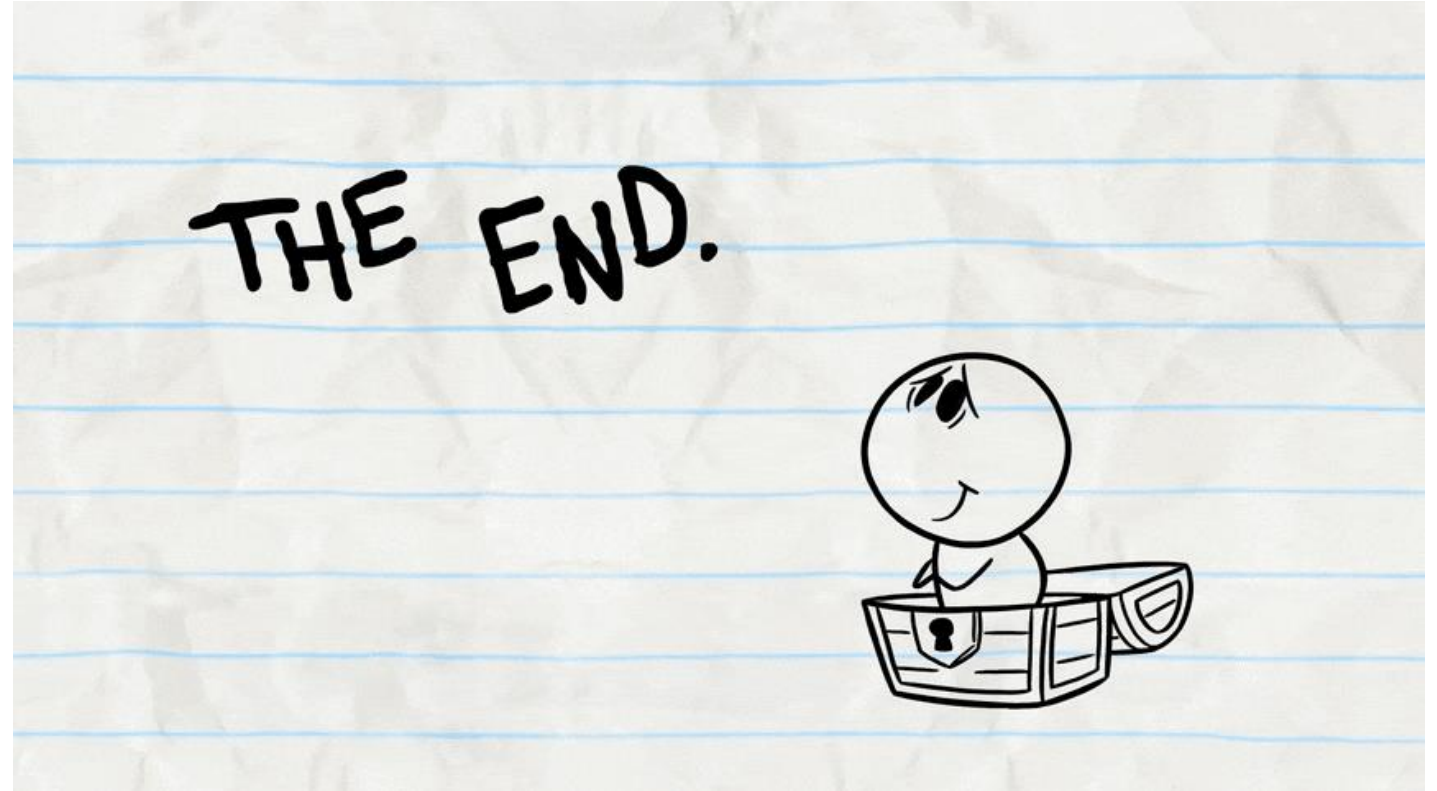
- In 2017, global cyber attacks, such as WannaCry ransomware, occurred at a high rate. It is difficult to effectively monitor and provide alerts for unexpected global security incidents. Furthermore, nations tend to be reactive instead of proactive when it comes to security incidents. The United States and Belgium, among others, have departed from the existing emergency response mechanism.



The End

Please feel free to contact me anytime if you have any questions

Abdelrhman Ahmed Refaat:
abdelrhmanahmedrefaat@gmail.com



جامعة القادسية
EVERYONE'S SMART UNIVERSITY