APCERT 2019
ANNUAL GENERAL MEETING & CONFERENCE

BADAN SIBER & SANDI NEGARA

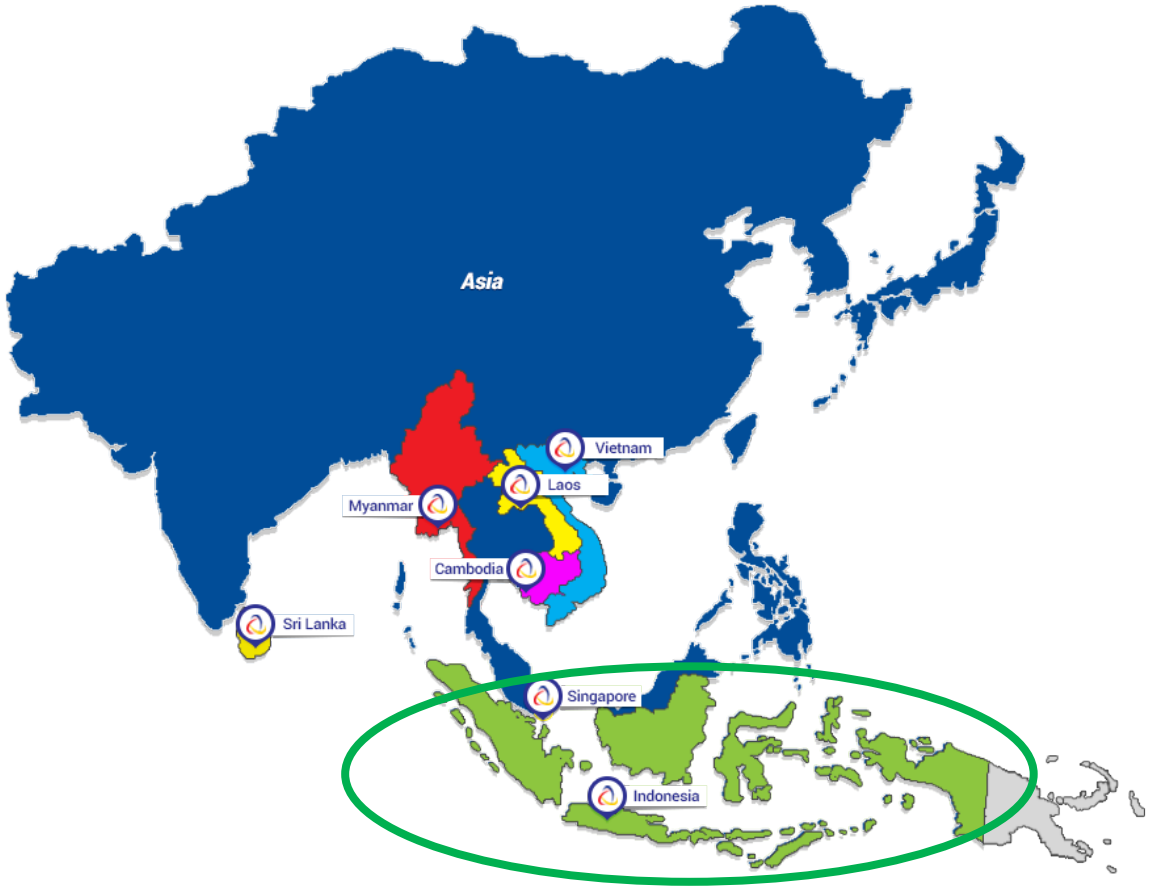
Hybrid Cyber Exercise :
The Indonesian Case Study

Mohamad Endhy Aziz
Arini Muhafidzah

October 2, 2019

Presented in 17TH APCERT Open Conference, Singapore

INDONESIA



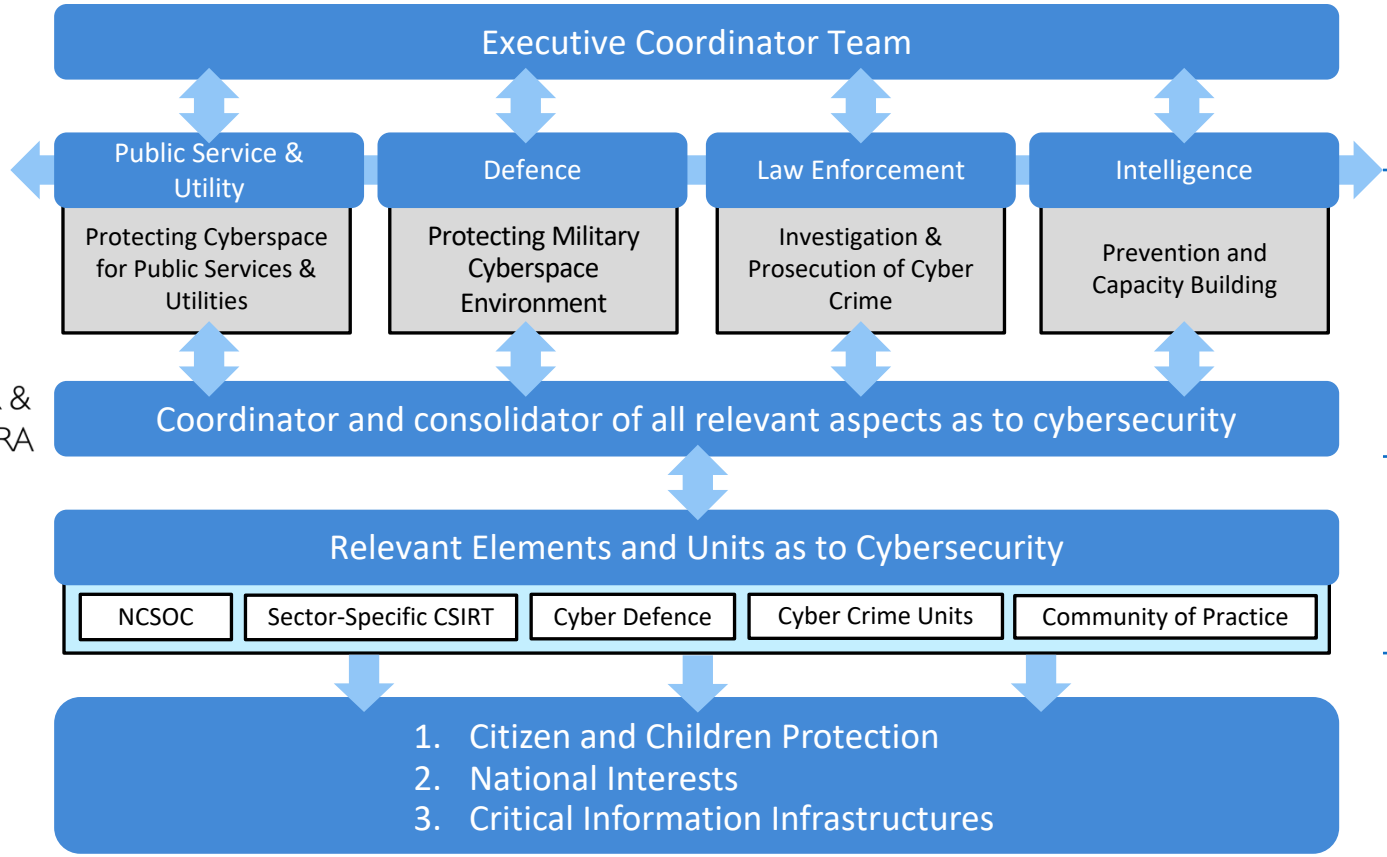
- Population : 264+ million people.
- Number of internet users : 171 million users (64,8 %).
- The government to connect all provinces and districts across the country through a massive fiber optic network construction with total sea cable length reaching 35,280 km, and a mainland cable length reaching as much as 21,807 km.
- The country has been working toward the goal to have 200 new startups across the 10 cities emerge from the funnel each year, starting from 2016 – which would amount to 1,000 startups by the end of 2020.

N.B. :
Consider visiting **Bali**.
It's the ultimate destination for travellers!
Whether you come for its culture, the beauty, the adventure, the food, or to surf.

INDONESIA CYBERSECURITY MANAGEMENT FRAMEWORK

BADAN SIBER & SANDI NEGARA

id-SIRTII/CC



Policy and Strategy Level
Coordinating Ministry, Ministers

Tactical Level
Cybersecurity Agency,
Senior Officers, Senior Experts, Academicians

Operational Level
Public Servants, Industry, Practitioners

ISSUES & CHALLENGES :

CYBER THREATS & INCIDENTS IN INDONESIA

ID-SIRTII/CC Traffic Monitoring & Attack Detection

2018

232.447.974
Attacks Detected

122.435.215
Malware Activities

1.872
Vulnerabilities Detected

2.885
Incident Reports

2017

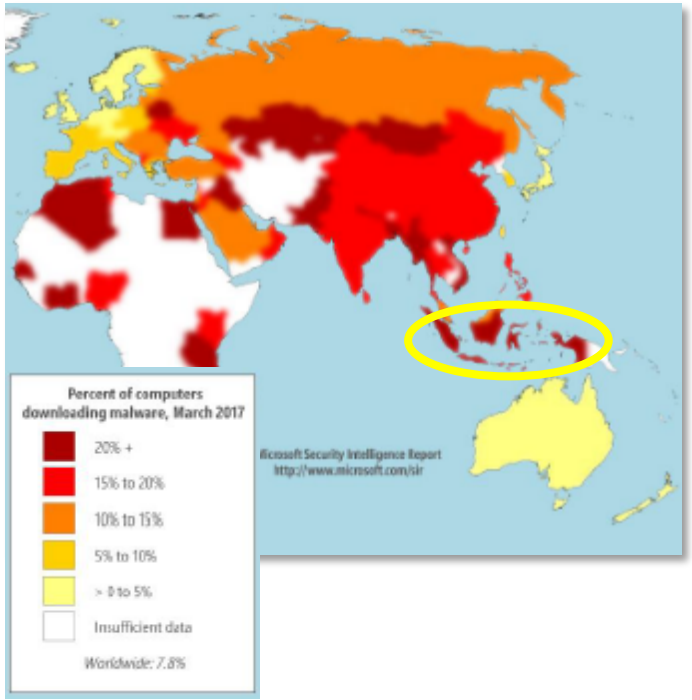
205.502.159
Attacks Detected

36.423.773
Malware Activities

98.787
Vulnerabilities Detected

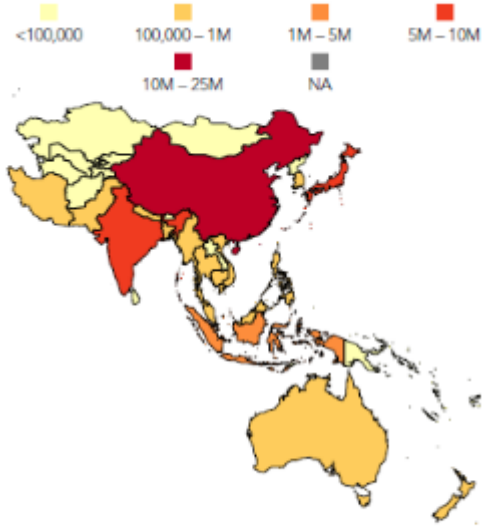
2.260
Incident Reports

Percentage of Computers Downloading Malware*



At average, about **22%** of the computers in Indonesia are infected by malware.

Web Application Attack**
Source Countries – Asia Pacific, Q1 2017



Country	Attacks Sourced	Global Rank
China	18,963,654	4
India	6,150,881	12
Japan	5,839,869	13
Singapore	4,285,527	15
Indonesia	3,248,604	17

*"The threat landscape is **evolving**, becoming more **sophisticated** and doing so at a **faster pace** than many organisations are able to keep up with."*

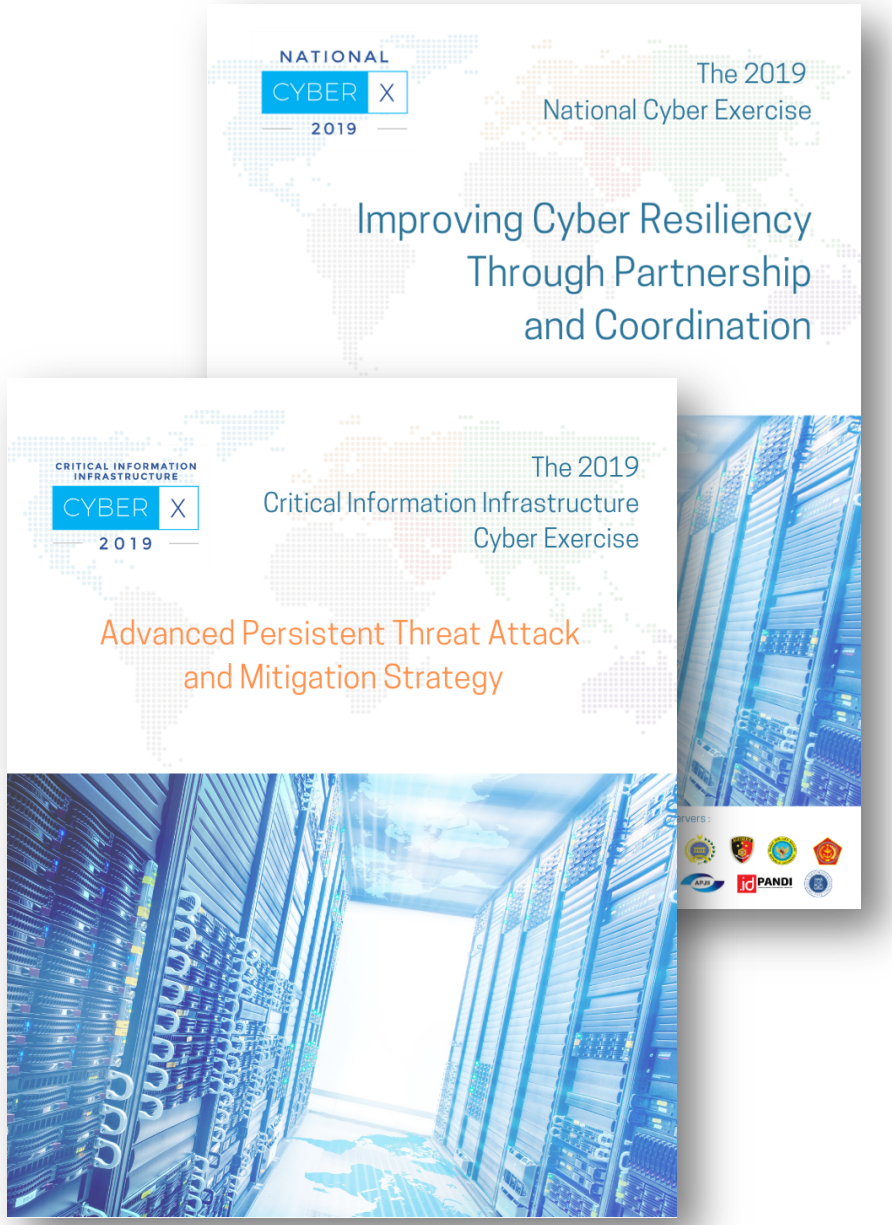
Source :
** Microsoft Security Intelligence Report*
*** Akamai's State Of The Internet]/Security Q1 2017 Report*

CYBER EXERCISES IN INDONESIA

- National Cyber Exercise (National Cyber-X)
  - Intended for decision makers.
  - Aims to generate discussions on various cyber issues, to enhance general awareness, validate plans and procedures, as well as to assess the types of systems needed to guide the prevention of, protection from, mitigation of, response to, and recovery from a significant cyber incident.
  - 36 participants from 14 institutions (2019).
- Critical Information Infrastructure Cyber Exercise (CII Cyber-X), Government Cyber Exercise (Gov Cyber-X)
  - Intended for IT operational staffs, IT administrators, or staffs responsible for cyber security operations and/or handling cyber incidents.
  - 205 participants from 95 institutions, 4 different industries (financial, energy, healthcare, defence & strategic industry).

"Exercising makes you stronger. Or prepared, at least."

Lauri Luht,
Head of the Cyber Defence Exercises,
NATO CCDCOE



CII CYBER-X
GOALS AND APPROACH

GOALS

- To continuously improve the capability and readiness of the CII operators in handling cyber incidents through exercise drills, and to promote the good practices.

APPROACH

1. Assess the ability of CII sectors in handling cyber incidents;
2. Evaluate weaknesses and shortcomings related to procedures and techniques possessed by the CII operators in handling cyber incidents;
3. Provide understanding and explanation of good practices in handling cyber security incidents.

KEY ASPECTS OF ASSESSMENT

- Cyber incident management structure.
- Incident reporting framework and escalation process.
- Logging requirement.
- Breach remediation.
- Communication with external and internal parties.
- Incident impact analysis and forensic investigation.
- Malware analysis.
- Post mortem analysis.
- Management reporting.

CYBER EXERCISE CLASSIFICATIONS

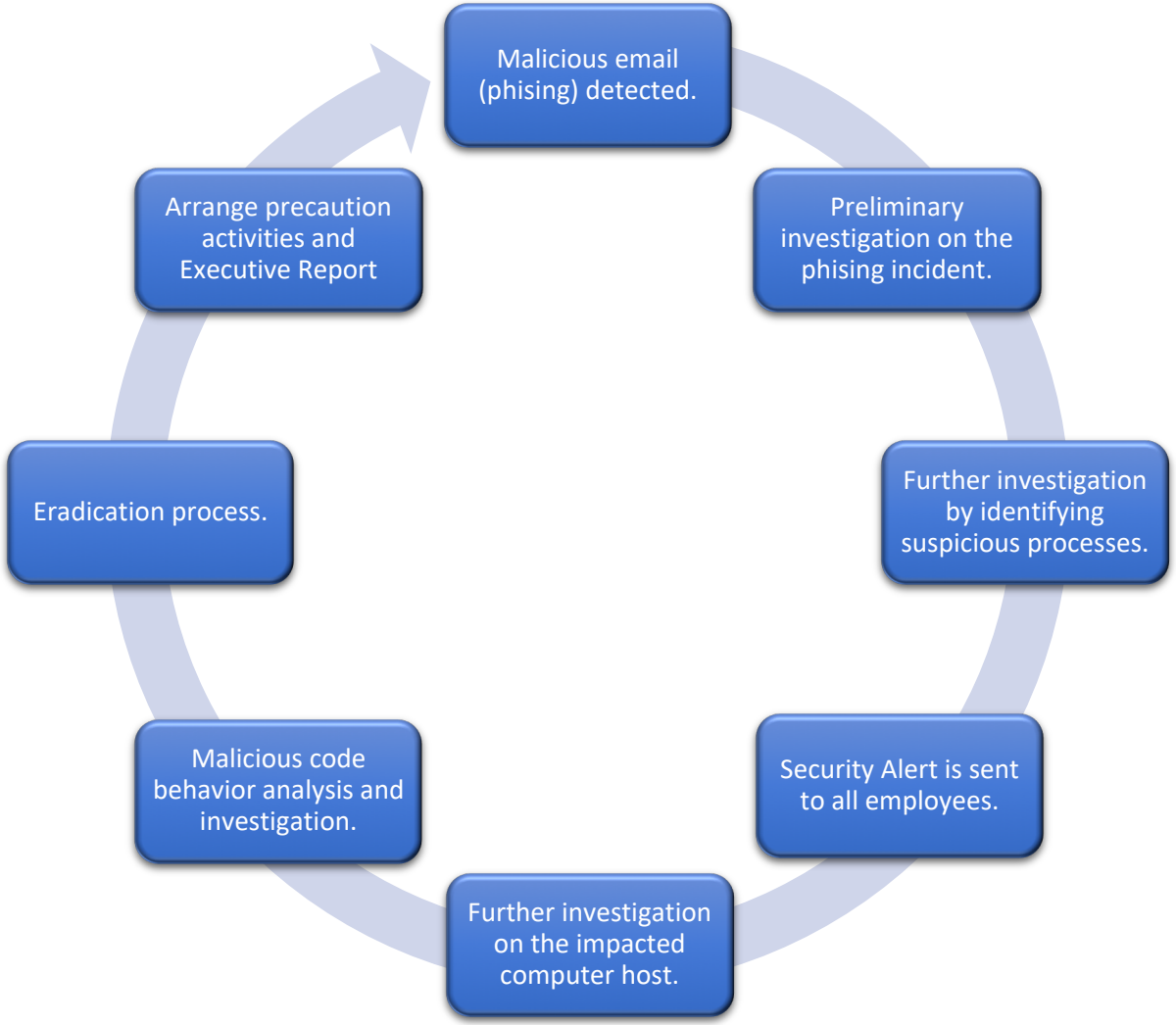
Style	Description	Complexity	Timing	Resources	Matches
Table Top	Paper-driven exercise with injects scripted by exercise planners and delivered via paper (cards/discussion). This type of exercise can be planned and executed quickly, depending on the number of organizations involved.	This type of exercise can be planned and executed quickly, depending on the number of organizations involved.	Planning: 1–2 months Execution: 1–3 days	Limited resources needed, depending on number of organizations.	Organizations new to exercises and to assessing organizational IA objectives. Organizations that need to validate processes/ train personnel in-between other exercises.
Hybrid	Paper injects with some live Scenarios facilitated by a RT for realism (probes, scans, e-mail spoofing, etc.)	This type of exercise requires more planning and longer execution times.	Planning: 3–6 months Execution: 3–5 days	Requires more people and time, real targets for scenarios, deconfliction contacts.	Organizations familiar with inter-organization exercises and a strong knowledge of their own objectives.
Full Live	Exercise plan incorporates real scenarios and injects into the exercise. Paper injects only used to stimulate if necessary	This type of exercise requires detailed coordination and planning.	Planning: 6–12 months Build up: 2–3 months Execution: 7–14 days	Large number of Organizational participants, IT resources, travel budget for meetings, deconfliction contacts	Organizations familiar with exercises, RTs, and their own organizational objectives.

WHY RUN HYBRID CYBER EXERCISE ?

Hybrid	Paper injects with some live Scenarios facilitated by a RT for realism (probes, scans, e-mail spoofing, etc.)	This type of exercise requires more planning and longer execution times.	Planning: 3–6 months Execution: 3–5 days	Requires more people and time, real targets for scenarios, deconfliction contacts.	Organizations familiar with inter-organization exercises and a strong knowledge of their own objectives.

- When it comes to what learning methods work best, everyone might be different, but hands-on exercise approach is favored by most Indonesian.
- People who practice what they're learning in a hands-on environment can often retain much more information when compared with only discussing the problem such as in Table Top Exercise.
- Enable the testing of procedures and ensure preparedness of staff to follow them.
- Laying out real reactions and behavior to exercise scenarios.

CII CYBER EXERCISE :
A HYBRID CYBER EXERCISE CASE IN INDONESIA



Exercise scenario :

- **8 injects** related to malicious code (APT) handling.

Approaches :

- Injection (cases of cyber incidents) and each questions are given in the Participants Handout document.
- The activity consisted of several stages (cases). Participants may proceed to the next stage if they were able to correctly answer each question in the given case.
- Participants can discuss only in his team. Exercise Assistants can provide technical assistance to Participants if needed.
- After the activity ends, a discussion, evaluation and conclusion of the activity's results are carried out.

Assumption :

- Participants are assumed to be Incident Response Teams / IRTs responsible for responding/handling incidents at each of your company's institutions.

CII CYBER EXERCISES :
THE PROCESSES

Identifying → Planning → Conducting → Evaluating

- **Identifying :**
  - Have a clear objectives for the exercise and what measures to test on the exercise.
  - Choose a high level scenario, a realistic scenario is critical to the success of the exercise.
  - Choose the type of exercise, fit the need you have identified and the measures that should be tested.
  - Identify key participants, involve their input into creating a realistic scenario and to ensure their enthusiastic participation.
  - Setting size and scope of the exercise.

- Key point to consider : Identify the measures to be tested, which includes the processes and the people involved in those processes.

- **Planning :**
  - *Concept Development Meeting*, discuss and get authorization on the activity, and determine the scenario being implemented.
  - *Initial Planning Meeting*, discuss inputs for developing the scenario.
  - *Mid-Term Planning Meeting*, discuss detailed scenario being implemented
  - *Final Planning Meeting*, and finalize the scenario and final technical meeting.

- Key point to consider : Ensure that scenarios are realistic, and that they include the necessary injects that drive the scenario along.

CII CYBER EXERCISES :
THE PROCESSES

- **Conducting :**
  - Prepare the participants with some training material, so they have understanding of how they should act.
  - The scenario needs to be managed and adapted in response to the actions of participants and pre-planned injects of new information.
  - Provide a dashboard for controlling the scenario and receive updates on actions taken by participants.

- Key point to consider : Injects should simulate real-world communication about an incident.

- **Evaluating :**
  - Evaluation ensures that lessons are learned, interdependencies identified, and that these are communicated effectively back to participants for them to take action.

- Key point to consider : Working closely with the stakeholders to reach consensus ensures the evaluation conclusions and recommendations will be accepted by stakeholders and gives greater chance the recommendations will be acted upon.

DEVELOPING THE SCENARIO :
SOME TIPS

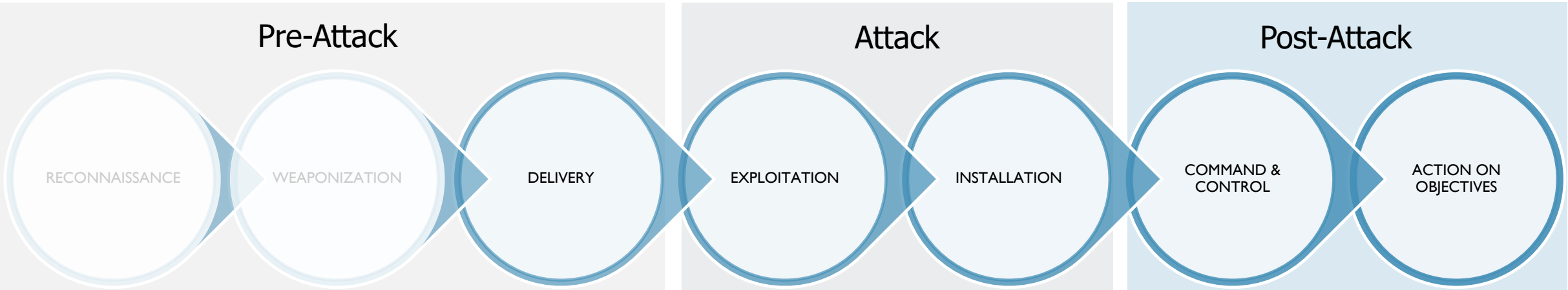
- Aligning from a real attack to the exercise scenario and the measurements is tricky. However, it is crucial to make the scenario as realistic as possible.
- Have a good understanding of the participating organizations function, and how they will respond to incidents.
- Sometimes participants will act differently than expected, so you need to allow for multiple responses and actions of the participants.

DEVELOPING THE SCENARIO :

RED TEAM ACTIONS EXAMPLE FOR THE EXERCISE

ELABORATING THE SCENARIO :

1. Define Red Team (RT) actions.
2. Align each RT actions into exercise goals and measurements.
3. Elaborate/create detailed actions of RT.
4. Create timeline of RT actions.
5. Execute RT actions, based on the planned actions and timeline defined.
6. Record every RT actions for the exercise materials, i.e. evidence for incident response.



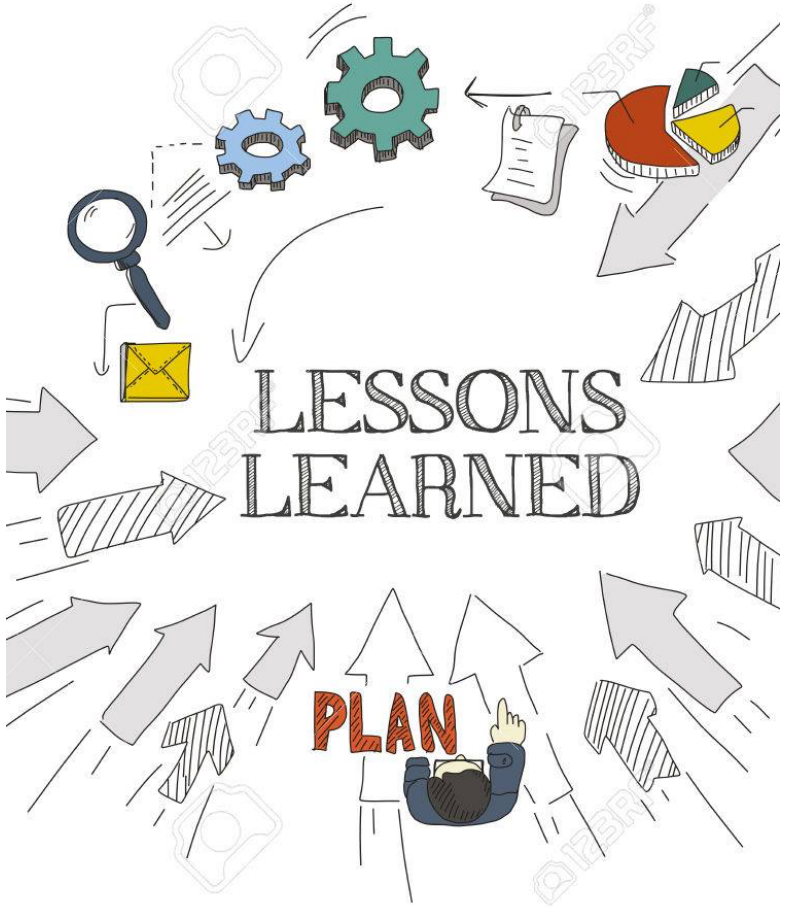
- Attacker send email with macro-enabled document as attachment to certain/targeted employee. ***DAY 1 : 1.10 pm.***

- Some of the victims opened/ executed the macro-enabled document. ***DAY 1 : 3.42 pm.***
- Attacker gained access to the victim's computer and send malicious codes from C2. ***3.44 pm.***
- Attacker installed persistence mechanism. ***4.30 pm.***

- Remotely control the victim machine from C2. ***DAY 2 : 9.20 am.***
- Lateral movement between internal networks. ***10.05 am.***
- Asset discovery. ***12.07 pm.***
- Data exfiltration. ***16.35 pm.***

LESSONS LEARNED

- Identify the exercise measures to be tested first (the processes that need testing, the people involved in those processes, then build the exercise around these critical factors, i.e. defining exercise type, scenario, etc).
- The exercise participants should be involved in the planning phase, in order to ensure that the exercise addresses the issues that they consider most important, and that the scenario is as realistic as possible.
- Provide training or briefing for participants at the start of the exercise. The participants will need to understand the general conditions, the rules of the exercise, and the roles of the monitors. They may also require some training, if special tools will be used to simulate their duties.
- Consider how you will measure success of the exercise. For example, surveys of participants before and after the exercise to measure importance of certain issues, or a survey at the end to evaluate the effectiveness of the exercise.



THANK YOU FOR YOUR ATTENTION!

ANY QUESTIONS?