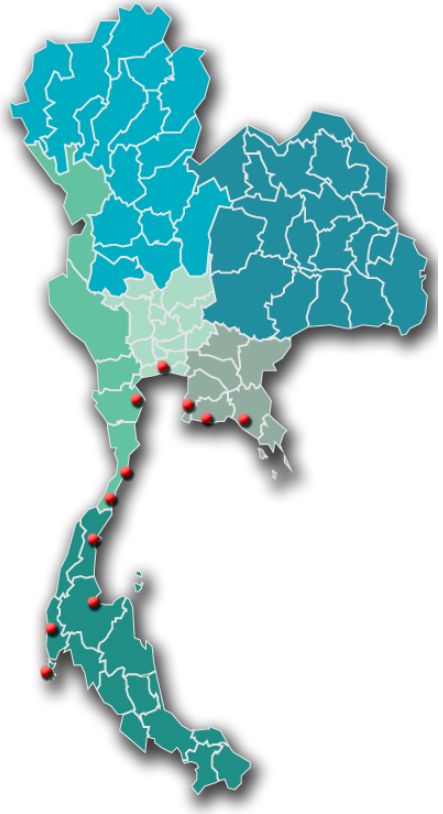
Scaling up security to the whole country

Martijn van der Heide, ThaiCERT Specialist

Electronic Transactions Development Agency (Public Organization)

FIRST™
Improving Security Together

Thailand



Country size:	513 km2
Population:	69 M
Internet users:	57 M
Facebook users:	46 M

Bangkok

Longest city name in the world.

The full ceremonial name reads as follows:

> กรุงเทพมหานคร อมรรัตนโกสินทร์ มหินทรายุธยา มหาดิลกภพ นพรัตนราชธานีบูรีรมย์ อุดมราชนิเวศน์มหาสถาน อมรพิมานอวตารสถิต สักกะทัตติยวิษณุกรรมประสิทธิ์
>
> Krungthepmahanakhon Amonrattanakosin Mahintharayutthaya Mahadilokphop Noppharatratchathaniburirom Udomratchaniwetmahasathan Amonphimanawatansathit Sakkathattiyawitsanukamprasit

It is composed of Pali and Sanskrit root words and translates as:

> City of angels, great city of immortals, magnificent city of the nine gems, seat of the king, city of royal palaces, home of gods incarnate, erected by Vishvakarman at Indra's behest.

How did I end up at ThaiCERT?

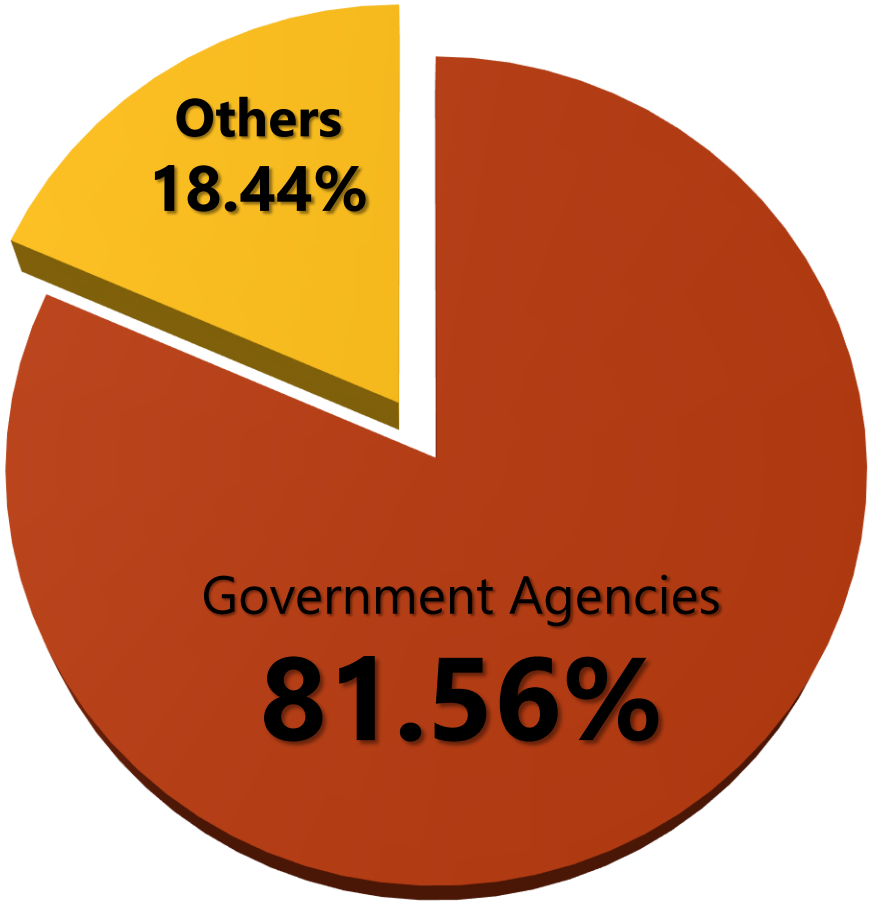
- 5 years ago, the FIRST Conference was held in Bangkok. ThaiCERT was the local host.
- At the last conference day, I met a lady.
- And married her.
- ThaiCERT kindly invited me to join their team.

So basically, I have been incredibly lucky!

Only CERT for the country: ThaiCERT

- Incident Response
  - Monitor and alert computer security incidents
  - Provide essential support and technical details
  - Research and develop tools and security guidelines
  - First team outside Europe to be TI Accredited
- Threat monitoring
- Member of APCERT Asia Pacific Computer Emergency Response Team and FIRST Improving Security Together
  - Cooperate with Thai organizations and overseas
- Incident Monitoring 24x7

Targets of web attacks in 2015

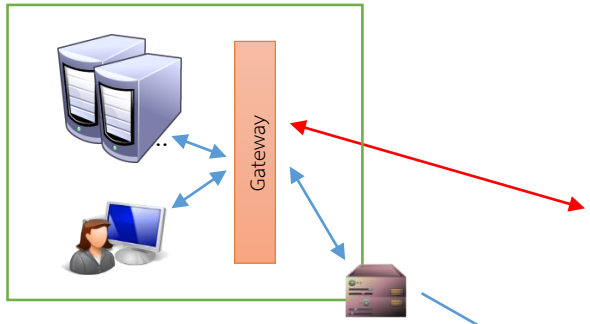


Observed trends

- Many repeated incidents
  - Back-ups are restored rather than underlying vulnerabilities patched.
  - Similar vulnerabilities throughout government IT.
- Lack of capacity and capabilities
  - Difficulties to find enough qualified staff (more than 250 agencies).
  - Security often not recognized as crucial.

→ Leverage scale: much more efficient to combine efforts into 1 solution

Agencies



Government Monitoring System (GMS)

1. Government Threat Monitoring System (GTM)
2. Government Website Protection (GWP)

ETDA/ThaiCERT

CyberSecurity Operations Center (CSOC)

DDoS Mitigation

WAF

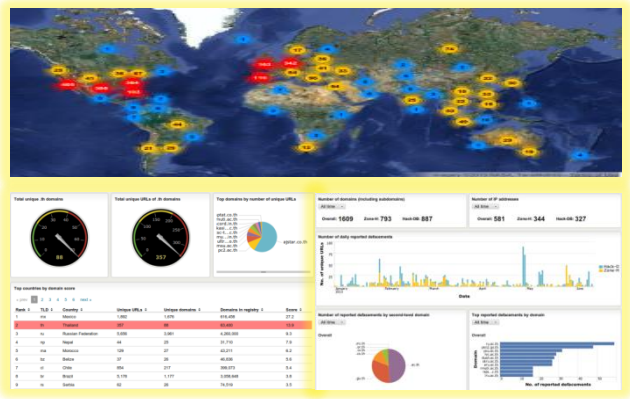
Threat watch

SIEM

Log collector

Malware Analysis
APT Detection
Forensics lab

Monitoring

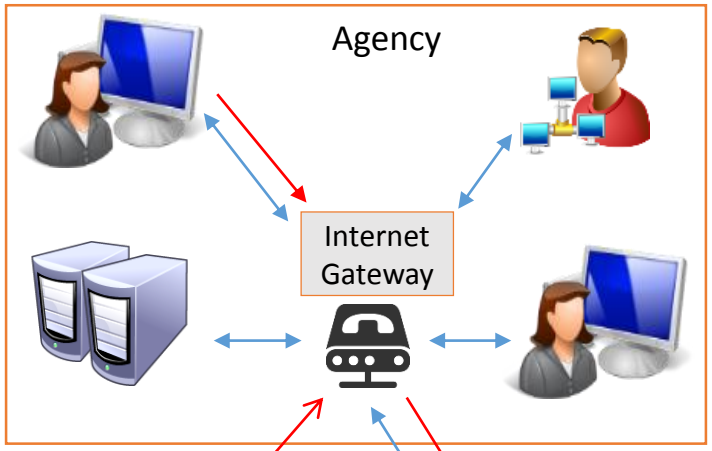


Post Incident Services

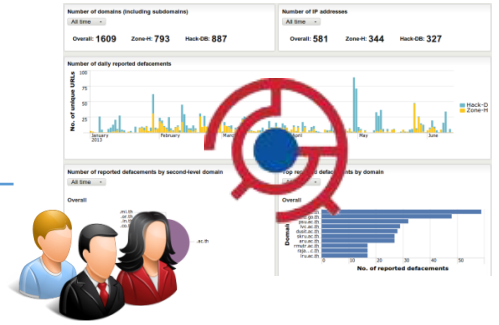
Incident Handling	Malware Analysis
Digital Forensics	Penetration Testing
Network Forensics	Awareness Training

Government Threat Monitoring

1 Collect log from agency's perimeter



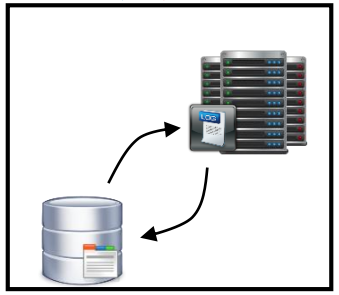
3 Send alert to agency including threat details and advisory



CyberSecurity Operations Center

2 Find suspicious traffic pattern

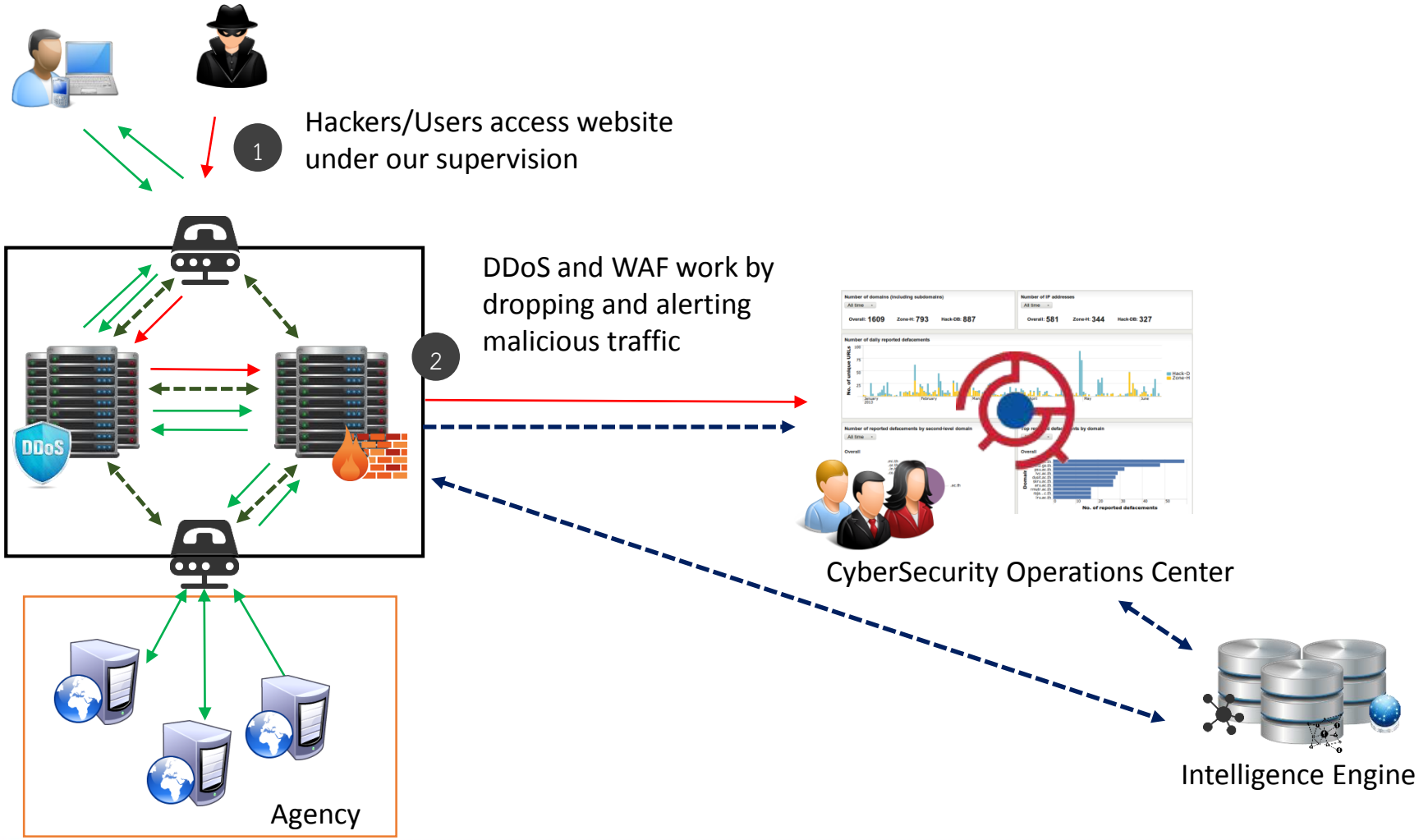
C&C



SIEM

Intelligence Engine

Government Website Protection

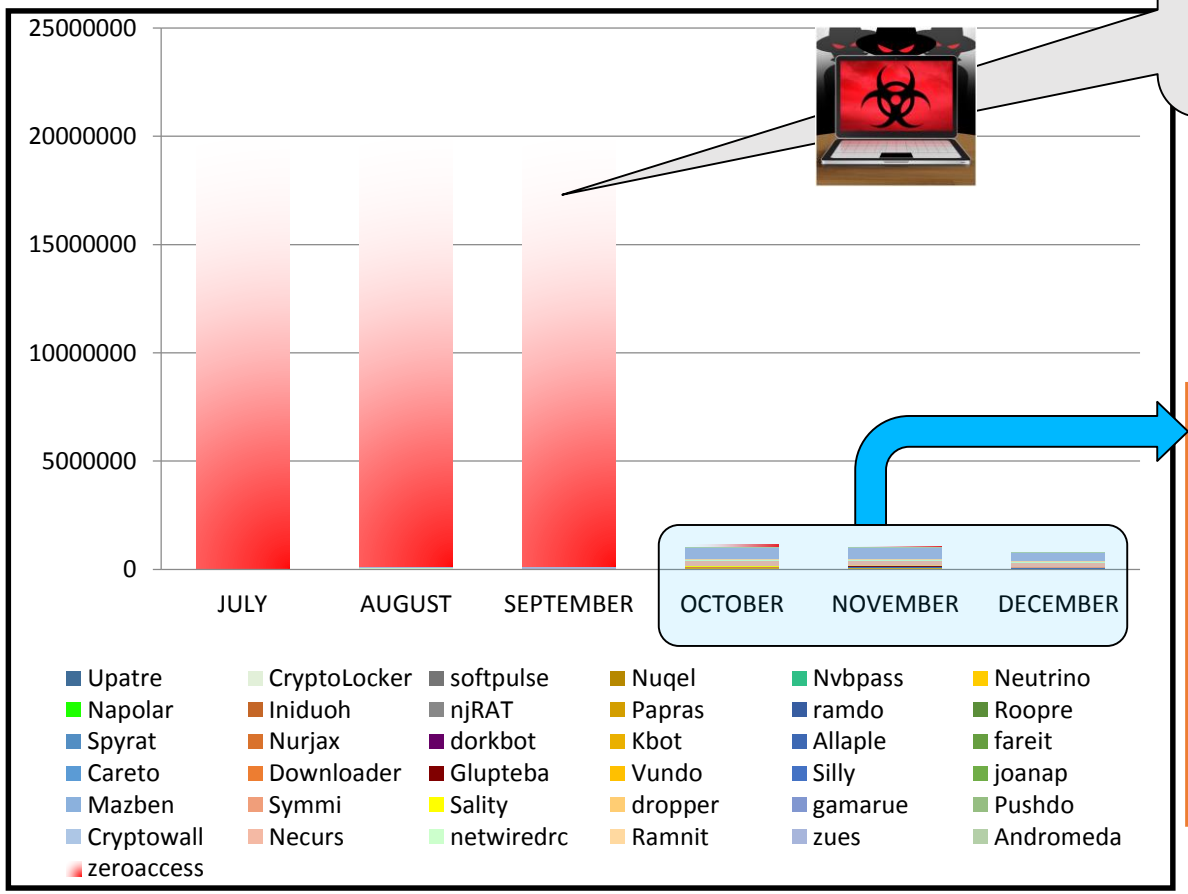


GMS drill twice per year

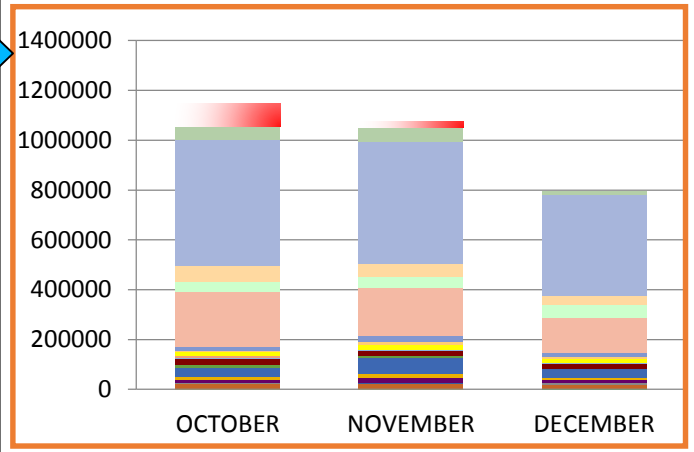
- Network forensics, DDoS attack response
- System forensics, finding point of entry, lateral movement, backdoors and other artifacts on hacked systems
- Log file analysis, correlating event alerts, reconstructing time-line

Getting results

Zeroaccess was the most seen infection family in 2015, after September 2016, the number of infection went down to 0.8 M records



Alert	Advisory
☑	☑



Other training

Malware Analysis Training

PHP/Java/Android Secure Coding

TRANSITS

Thailand CTF Competition

Going well, right?

We’re going too slowly!

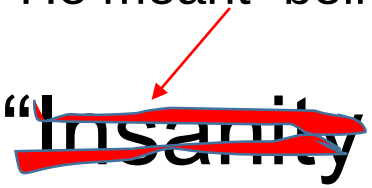
Trainings, especially hands-on classes, are for relatively small amounts of students per session.

We need tens of thousands of security staff

As this rate, that would take 25 years to accomplish. How can we step up the pace? National policy and public-private partnership.

Perseverance and stamina

He meant “being a CERT team”



“~~Insanity~~ is doing the same thing over and over again and expecting different results.”

“If at first you don't succeed, try, try again.”

“Never let a good crisis go to waste”

CII strategy

1. Defining clearly what CII (Critical Information Infrastructure) encompasses and establishing a formal list of CII in Thailand:
   - Critical government ministry/agency
   - Financial
   - ICT and telecommunications
   - Healthcare
   - Energy, water and utilities
   - Transportation and logistics
2. Comparing the strategies of other countries.

→ This leads to the CII strategy.

Table Top Exercises

Tactical exercise to discuss a theoretical (but plausible), high level scenario. TTXs give a relatively quick insight in the preparedness of an organization, or, in our case, entire sectors at a time.

- Thai Banking Sector
- Capital Market
- Healthcare Sector

New laws

All organizations in a CII are now required by law to implement security.

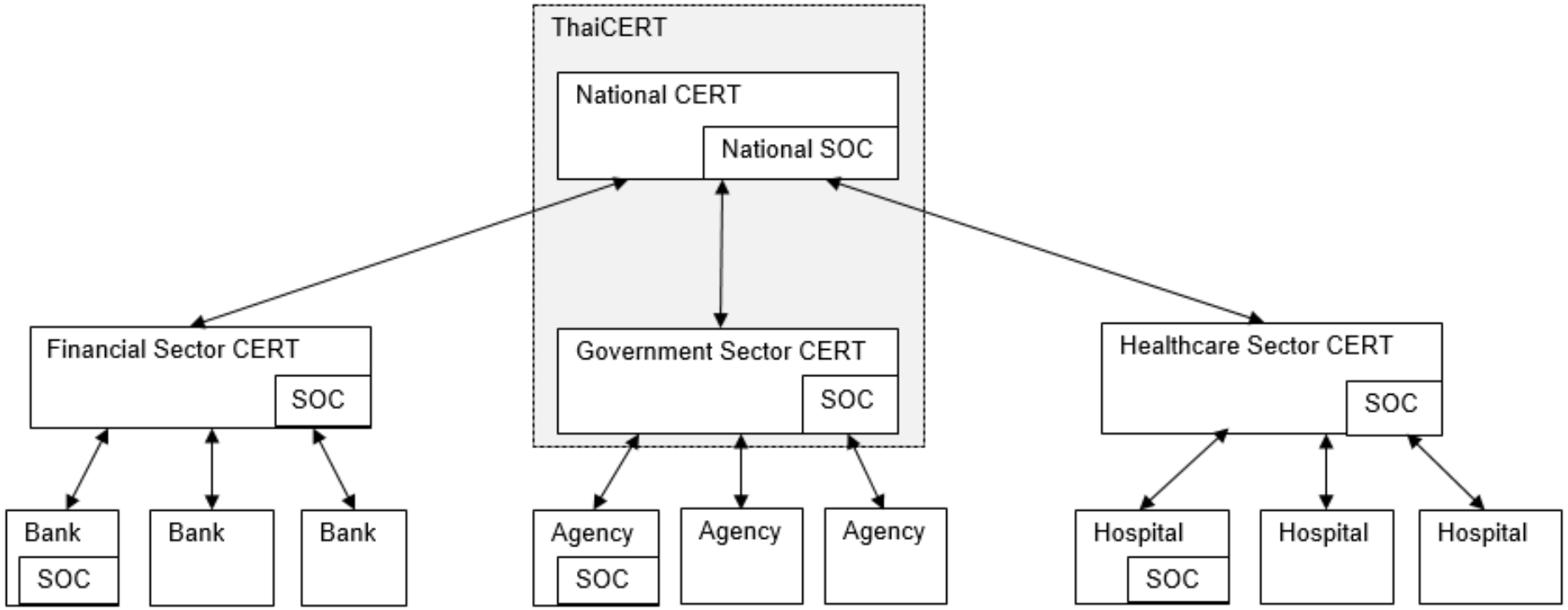
It is not yet entirely clear which standard(s) and minimal baselines are required for each sector, but this step has already been shown to be a good incentive.

- Budgets are being allocated.
- We receive requests for help.

New approach

Sector-based CERTs

Ultimate National Hierarchy



Sector-based CERTs

Allowing a better pace in implementing security in the individual organizations

- Where do we find enough staff?
- Getting the budget approved.

… while having some form of incident management and coordination in place already.

- Easier to staff 1 CERT than to staff all organizations in the sector at once.
- Getting more experience in the threats for this sector.
- As a sector, information sharing is a necessary service anyway.

First one is TB-CERT, recently became a FIRST member already.

New services

- Annual national security conference since 2017, called Thailand Cybersecurity Week (23-25 July).

- Daily human readable risk intelligence feed, weekly newsletter for executives and ministers.

[FYI] ThaiCERT Risk Intelligence 21 March 2018

Quick overview:

	Critical	Urgent	Important
Government/Law/Policy	0	0	5
Vulnerabilities	0	0	2
Malware	0	0	2
Breaches/Hacks/Leaks	0	0	3
General News	0	0	9

Government/Law/Policy

DHS Cyber Incident Response Teams Closer To Becoming Permanently Codified

"The House approved a bill on Monday that would make the Department of Homeland Security's cyber incident response

Abuse information exchange

There are many automated feeds from various sources, most of them free, several provided to national CERTs only.

We need a new, modern feed platform to properly handle these feeds.

- How do we get our actionable intelligence to the owners of the IP space?
- How can we leverage the knowledge learned from this intelligence?
- What are ISPs supposed to do?

There will be a BoF about this topic tomorrow right after the AGM.

Awareness starts at schools

Children today have much of their activities online from a very early age, either at school or at home.

- Start teaching them about security and safety of technology from elementary school onward, such as
  - Passwords, 2FA
  - Posting photos and identifiable information
  - Digital footprint
  - Cyberbullying
- We started in Bangkok, now train-the-trainer and spreading to other cities in the country.
- A joint venture with LINE Corporation.

Certifying 1,000 people per year

The target we received is to get 1,000 people certified per year.

For that, we have to train 5,000 people per year, 168 per week.

We team up with universities and organizations such as CMU, SANS and (ISC)2 to create a curriculum.

- First we will need to train the trainers to expand our training resources.
- Apart from the budget, the logistics and arrangement of enough training locations and facilities is a challenge.

ASEAN-Japan Cyber Capacity Building Center (AJCCBC)

https://www.etda.or.th/content/mdes-to-launch-ajccbc-this-june-in-preparation-for-cyber-attacks.html

The Ministry of Digital Economy and Society (MDES) of Thailand and Ministry of Internal Affairs and Communications (MIC) of Japan jointly announced the preparation for the establishment of ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) in Thailand. ETDA revealed 3 courses to prepare cybersecurity workforce in ASEAN for the rising threats of cyber-attacks. Officials are confident that after the launch in June, the Centre will play the key role in mitigating cybercrime in this region.

Cyber Security Agency

As ThaiCERT, part of an agency (ETDA) under the Ministry of Digital Economy & Society, we lack full visibility.

Also, our mandate is only advisory.

A new agency, provisionally named Cyber Security Agency (CSA), has been proposed to be set up, at a higher level in the government, with more funding and mandate. ThaiCERT should then integrally move into this new agency.

The proposal has been accepted by the cabinet.

Challenges

Language barriers

Thai is a very difficult language with 27 syllables, 44 consonants and 5 tones. I try, but may never learn.

- Sometimes consonants change if they are the last letter in a word.
  - The character for ‘L’ becomes an ‘N’.
  - Such language rules are often (incorrectly) applied to their English speaking, so we often hear of Googen, litten.
- Converting Thai characters to Latin is not done by transliteration, but substitution – did you know how to pronounce the name of our good King Bhumibol?
- The ‘R’ is generally not pronounced (although it should be).
  - So, “central” become “centan” when spoken. Takes getting used to.

Culture

Note: the following is much less true at management levels.

Thai are extremely polite, they will always say yes

- Can you do this extra task? Sure. Even when that is not possible.
- Trying to find out if you yourself understand how something is implemented is difficult, as they will not alert you of incorrect findings or interpretation.

There is no interaction during trainings and workshops.

- Difficult to gauge if the material is understood.

English is slowly being taught more, but many only speak Thai.

- Dual language training, but this halves the time you have.

Top-down vs. bottom-up

In Western countries there is a more direct communication between peers in different organizations, on each level.

- Techies among each other, managers talking to managers.
- Reporting incidents straight to the operator.

In Thailand (likely Asia in general), a strict top-down approach

- As ThaiCERT, we escalate incidents happening in Thailand to management level, so our managers can report an incident to their manager, where the process goes down again.

Same for technology. Convincing to use any technology always starts at the top. This requires a good technical understanding at management level.

Stretching to breaking point

Losing staff while getting extra workloads

- E.g. military draft or study abroad, unsuccessful in attracting new technical staff.

- Everything ad hoc, do work when you have a moment rather than planned.
- Temporarily suspended services due to lack of resources.
  - E.g. malware analysis and our daily short news articles.
- Teaming up with other teams. Thanks for all the help, guys!
- “Why is everything in English?”
  - Because I can’t write in Thai. ☹

I love Thailand

The previous may unintentionally have sounded negative.

I actually love this amazing country and team.

- Very kind and welcoming people.
- The team is like a family who help each other with everything.
- Ambitious targets every year, but those targets are generally met.

This is where I want to stay and help make a difference.