

# URGENSI PEMBENTUKAN CSIRT

*Rudi Lumanto PhD*

BSSN-Launching JatengProv-CSIRT  
7-Oktober-2020

# Ruang Siber Saat ini

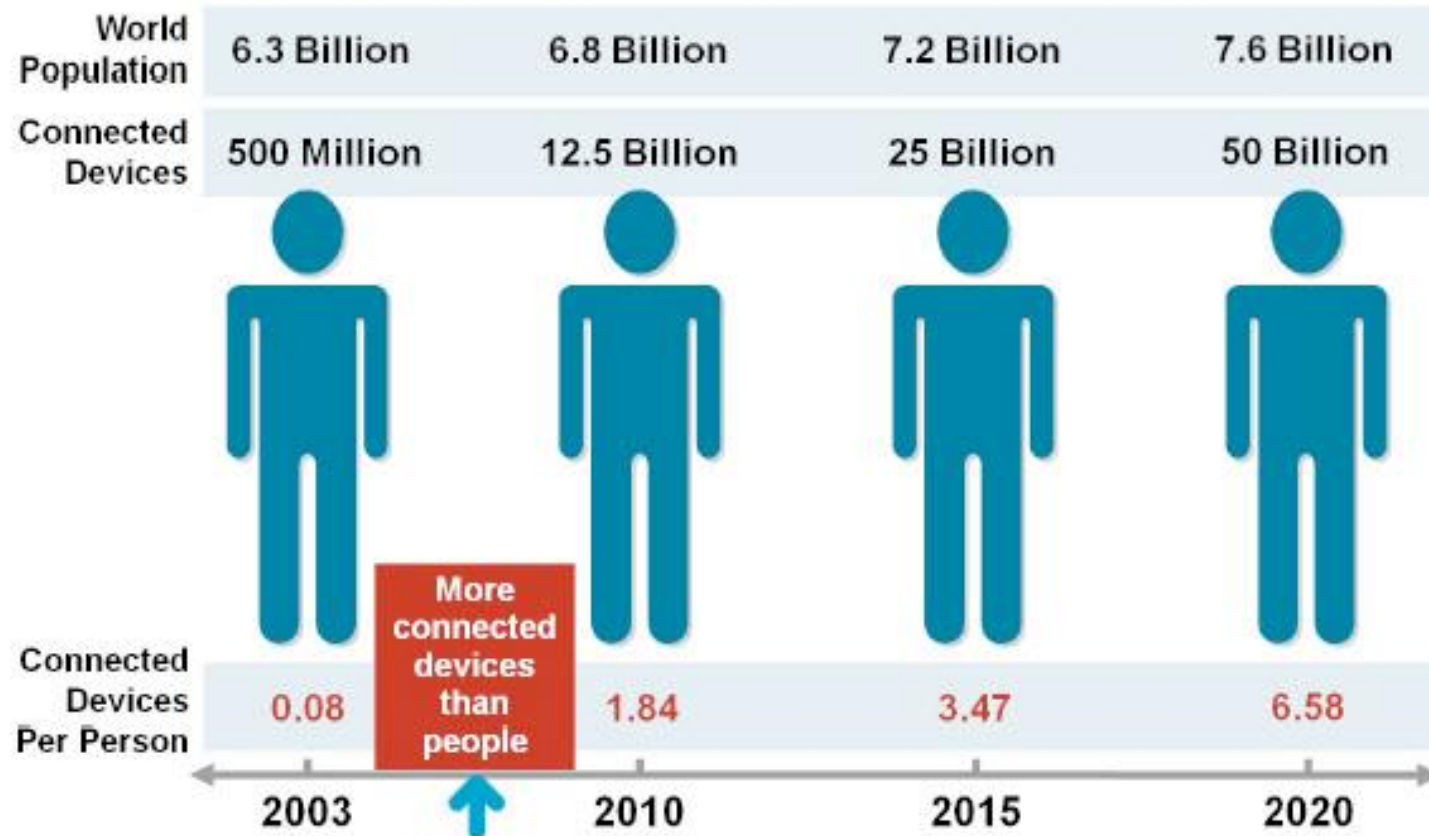
- TOP 10 COUNTRIES WTH HIGHEST NUMBER OF INTERNET USERS – 2020Q1

#	Country or Region	Internet Users 2020 Q1	Internet Users 2000 Q4	Population, 2020 Est.	Population 2000 Est.	Internet Growth 2000 - 2020
1	<a href="#">China</a>	854,000,000	22,500,000	1,439,062,022	1,283,198,970	3,796 %
2	<a href="#">India</a>	560,000,000	5,000,000	1,368,737,513	1,053,050,912	11,200 %
3	<a href="#">United States</a>	313,322,868	95,354,000	331,002,651	281,982,778	328 %
4	<a href="#">Indonesia</a>	171,260,000	2,000,000	273,523,615	211,540,429	8,560 %
5	<a href="#">Brazil</a>	149,057,635	5,000,000	212,392,717	175,287,587	2,980 %
6	<a href="#">Nigeria</a>	126,078,999	200,000	206,139,589	123,486,615	63,000 %
7	<a href="#">Japan</a>	118,626,672	47,080,000	126,854,745	127,533,934	252 %
8	<a href="#">Russia</a>	116,353,942	3,100,000	145,934,462	146,396,514	3,751 %
9	<a href="#">Bangladesh</a>	94,199,000	100,000	164,689,383	131,581,243	94,199 %
10	<a href="#">Mexico</a>	88,000,000	2,712,400	132,328,035	2,712,400	3,144 %

Source : Statistica

# Ruang Siber Saat ini

Figure 1. The Internet of Things Was "Born" Between 2008 and 2009



Source: Cisco IBSG, April 2011

► IMPLEMENTASI IOT 2020

## Asiote Targetkan 200 Juta Sensor

Bisnis, JAKARTA — Asosiasi Internet of Things Indonesia (Asiote) akan melakukan aksi jemput bola ke seluruh sektor industri untuk mencapai target implementasi 200 juta sensor internet of things (IoT) dengan average revenue per user (ARPU) mencapai US\$2 miliar oleh seluruh sektor industri pada 2020.

### HEMAT BIAYA

Berdasarkan laporan Global System for Mobile Communications Association (GSMA), badan usaha mampu menghemat biaya sebesar 4%–5% dengan pemanfaatan IoT yang masih minim. Dengan pengimplementasian yang masif serta tepat sasaran, badan-badan usaha diyakini dapat melakukan penghematan yang lebih signifikan.

### Adopsi & Target Adopsi Sensor

- Adopsi sensor IoT 2019
  - Perangkat 150 juta sensor
  - ARPU US\$1,5 miliar
- Target Adopsi sensor IoT 2020
  - Perangkat 200 juta sensor
  - ARPU US\$2,0 miliar



*Hermaul Fauzan*  
hermaul@pikiran.com

Ketua Umum Asosiasi IoT Indonesia Teguh Prasetya mengatakan angka pengadopsian sensor IoT yang telah direalisasikan di Indonesia pada tahun ini mencapai 150 juta perangkat atau dengan ARPU setara US\$1,5 miliar. "Tahun depan, asosiasi siap menjemput bola ke seluruh industri sebagai akselerasi pengadopsian IoT. Kami akan go to seluruh industri dengan membuat solusi dan kemudian kami dorong penetrasinya," ujar Teguh kepada *Ratus*, Jumat (20/12). Upaya tersebut, salah satunya dilakukan dengan dilaksanakannya program strategis seperti IoT Goes to BUMN, di mana pihak asosiasi bekerja sama dengan salah satu lembaga pemerintah, Kementerian Komunikasi dan Informatika (Kemenkominfo). Melalui program tersebut, kedua

Pada tahun ini pengadopsian teknologi IoT di Indonesia masih dihadapkan pada kendala fundamental, seperti regulasi yang masih baru, serta soal kesiapan sumber daya manusia (SDM). Namun, optimisme Teguh cukup realistis. Pasalnya, bekerja sama dengan lembaga pemerintah, pihak asosiasi telah menyelesaikan Standar Kompetensi Keahlian Nasional Bidang IoT. Tidak hanya itu, pelaku industri IoT juga telah menemukan mitra sehingga seluruh fondasi dapat dikatakan beres. Selain itu, dengan diselesaikannya Standar Kompetensi Keahlian Nasional Bidang IoT, maka pengadopsian materi mengenai IoT ke dalam kurikulum pendidikan, baik itu pendidikan vokasi maupun formal menjadi mudah. "Kita berharap tahun depan banyak sertifikasi-sertifikasi IoT yang bisa dikeluarkan oleh Asosiasi IoT bekerja sama dengan Lembaga Sertifikasi Profesi (LSP)," kata Teguh. Dengan persiapan yang dilakukan, pihak asosiasi pun optimis target

Rp444 triliun dan 400 juta sensor bisa terwujud di Tanah Air.

EDUKASI BADAN USAHA  
Sementara itu, Direktur Jendral Sumber Daya dan Perangkat Pos dan Informatika (SDPPPI) Kemenkominfo Ismail mengatakan pelaku industri dan seluruh pemangku kepentingan di industri IoT perlu mengedukasi pasar badan usaha.

"Dengan rampungnya low power wide area (LPWA) pada 2019, maka tahun depan pelaku industri IoT perlu melakukan blumakan ke badan-badan usaha," ujarnya.

Pemanfaatan IoT, ujar Ismail, berpotensi memberikan peluang penghematan yang besar bagi badan-badan usaha.

Berdasarkan Laporan Global System for Mobile Communications Association (GSMA), badan usaha mampu menghemat biaya sebesar 4%–5% dengan pemanfaatan IoT yang masih minim. Dengan pengimplementasian yang masif serta tepat sasaran, maka badan usaha diyakini dapat melakukan penghematan yang lebih signifikan. Namun demikian, monetisasi masih menjadi isu dalam pengimplementasian IoT. Survei GSMA mengungkapkan 45% badan usaha yang menjadi responden masih melihat biaya implementasi sebagai kendala, dan 22% lainnya menyebut return of investment (ROI) yang belum jelas. ■

► Adopsi teknologi IoT di Indonesia masih dihadapkan pada kendala fundamental.  
► IoT berpotensi membuka peluang penghematan besar bagi badan usaha.

Bisnis Indonesia, 27-12-2019

# Apa yang terjadi di ruang siber ?



- Konektivitas semakin tinggi
- Aset penting semakin terhubung ke luar
- Setiap koneksi dijalankan aplikasi yg memiliki kerentanan (vuln)
- Inovasi di underground
- Kurangnya kemampuan pertahanan siber
- Info tehnik serangan berserakan
- Tingkat anonimity yang semakin tinggi

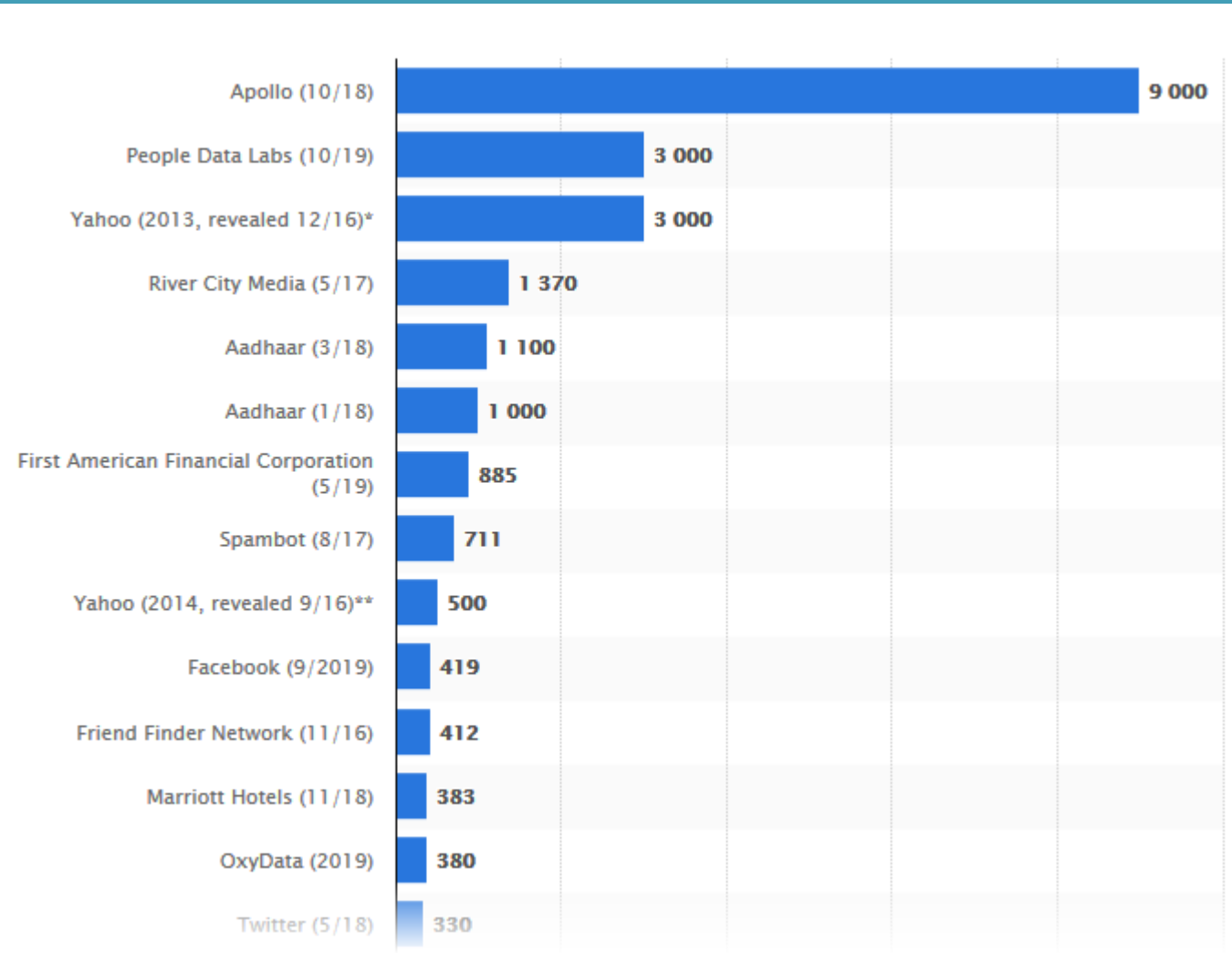
**Kita dikelilingi dengan ancaman, Insiden siber terjadi setiap saat, !**



# Apa yang terjadi di ruang siber ?



Number of compromised data records in selected data breaches as of April 2020 (in millions)



# DATA BREACH di INDONESIA

**Under the Breach** @underthebreach · May 2  
Actor leaked the database of Tokopedia - a large Indonesian technology company specializing in e-commerce. (@tokopedia)

- Hack occurred in March 2020 and affects 15,000,000 users though the hacker said there are many more.
- Database contains emails, password hashes, names

Exclusive - Tokopedia, 15 million users

ip_email	user_pwd	status	full_name	sex	birth_date	location	msisdn	me
li.com	1	1	Linda					
me	1	1	[CHARACTER_NOT_ALLOWED]	1	1997-01-05			
li.com	1	1	Luci		1996-01-07			
com	1	1	Janni				6285719678685	
1	1	1	Oka		2002-06-29			6287868837705
li.com	1	1	Komang		1998-07-28			
li@yahoo.com	1	1	Hismawan					
li.com	1	1	Ihsan					628383131
1	1	1	M Samsul		1999-09-21			628966111
1	1	1	Aris		1987-02-09			628222121
li.com	1	1	Frans					628229801
li.com	1	1	Indra					628229721
1	1	1	Hahardis					628593823799
li.com	1	1	Diana					628592131
1	1	1	Nandallitha					628135751
1	1	1	Endang		1984-04-19			628138241
com	1	1	Muhlis					
com	1	1	Edi					628572021226
me	1	1	Wido					
li.com	1	1	Ardy					628575621
1	1	1	masdiah					
me	1	1	seva					
100.co.id	1	1	Osi					628132271
1	1	1	ABDI					628968783567
com	1	1	Awalia					
li.com	1	1	Indra					628155651
1	1	1	ChairulFajri					6282154800014
1	1	1	NaniFah					6282137164434
1	1	1	hanydita					628532465564811
1	1	1	Dadan					6281383475921
li.com	1	1	Smyet1011va8@gmail.com					021ve85
1	1	1	Bizal					

### Tokopedia 91M

Contact: XMPP: shinyhunters@xmpp.jp Twitter: @sh\_corp

Sold by **ShinyHunters** - 0 sold since May 03, 2020 **Vendor Level 1** **Trust level 1**

Unlimited items available for auto-dispatch

Product Class	Features	Origin Country	Features
Quantity Left	Digital	Ships to	World Wide
Ends In	Unlimited	Payment	World Wide Escrow
	Never		

default - 1 day - USD + 0.00

Purchase price: **USD 5,000.00**

Qty: 1 **Buy Now** **Buy Now** **Queue**

0.561030 BTC / 77.990953 XMR

Description Feedback Refund policy

### Tokopedia 91M

Contact:  
XMPP: shinyhunters@xmpp.jp  
Twitter: @sh\_corp

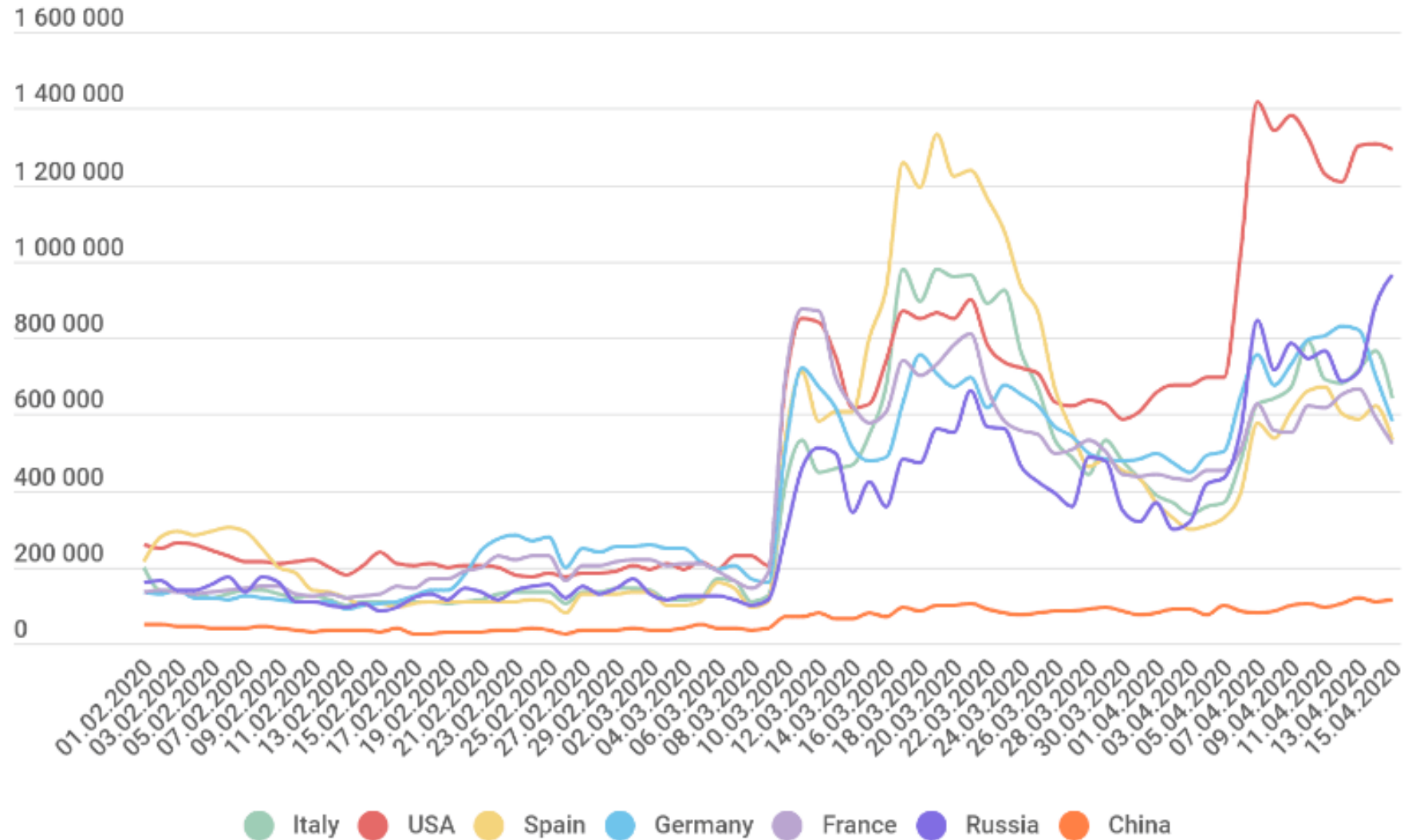
Shinyhunters Dump Hacked Data Tokopedia Breach Data Hack Hacked Million Millions Dumped Db Database

Userbase Password Combo Md5 Salted Passwords

Terdapat lebih dari 500 email address pemerintahan dan 450 bank email address !!

# BAHKAN SAAT PANDEMI

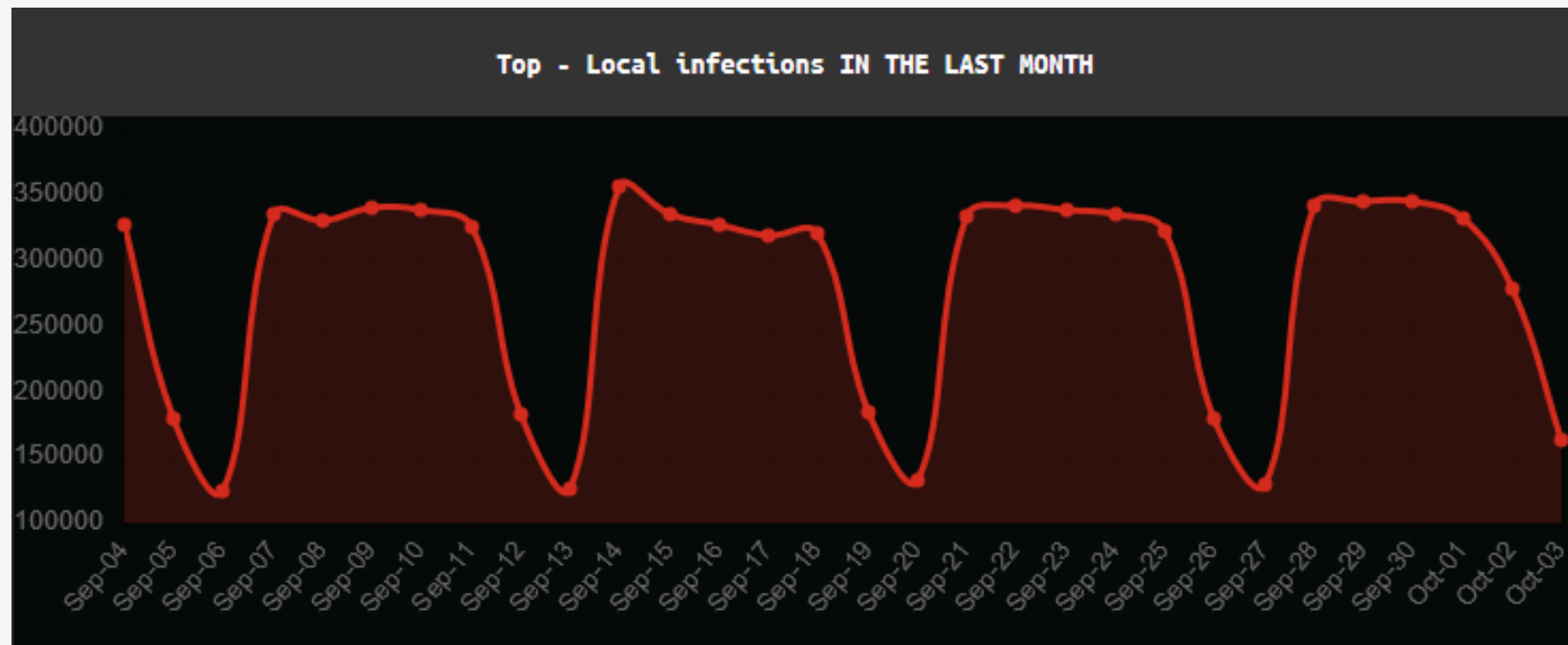
RDP attacks has been rocketed across almost the entire planet. By the end of last march it reached million per day. (Karpesky)



# Number of Infected Host in Indonesia last month

(4 Sep - 3 Okt 2020)

Source : Kaspersky



Top - Local infections IN THE LAST MONTH

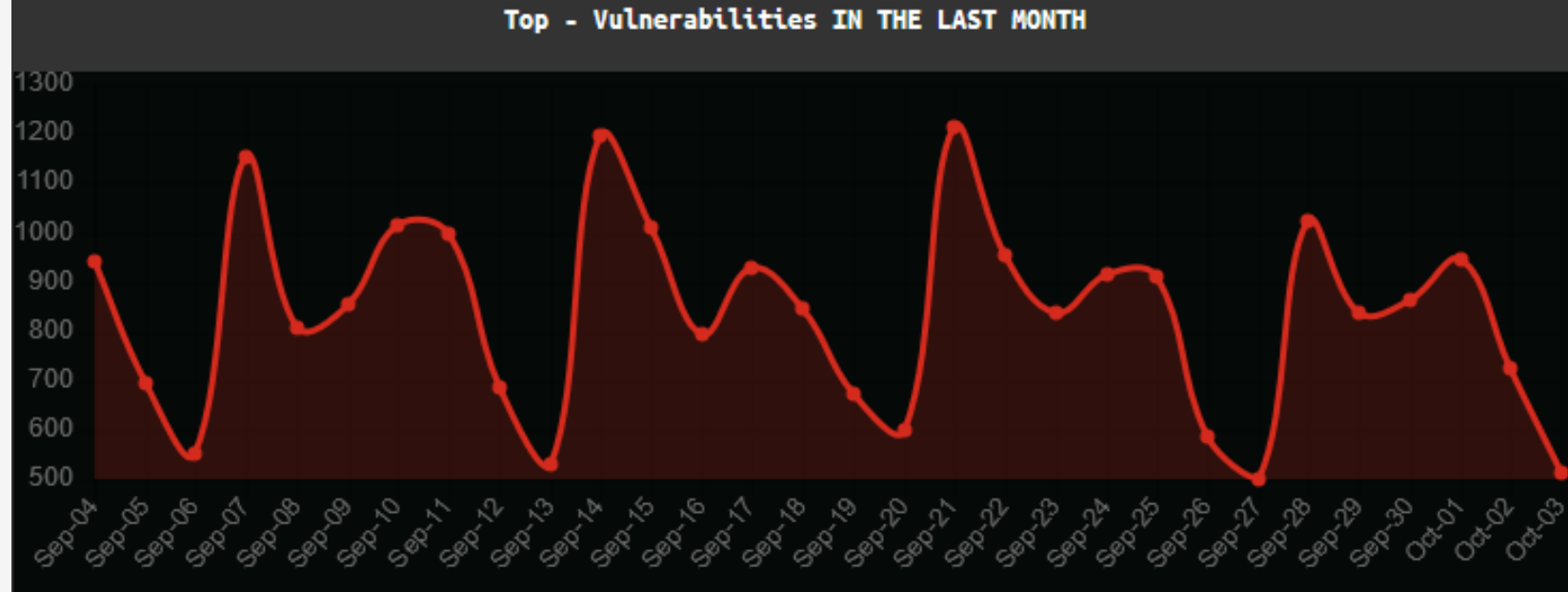
1	DangerousObject.Multi.Generic	10.08%
2	HackTool.Win32.KMSAuto.gen	5.87%
3	Trojan.Win32.Agentb.bqyr	4.73%
4	Backdoor.Win32.Zepfod.yy	4.45%
5	Virus.Win32.Pioneer.cz	3.81%
6	HackTool.MSIL.KMSAuto.dh	3.78%
7	HackTool.MSIL.HackKMS.a	3.17%
8	Virus.Win32.Renamer.j	3.08%
9	HackTool.Win64.HackKMS.b	2.83%
10	Trojan.Win32.AutoRun.gen	2.57%



# Number of Vulnerabilities Indonesia last month

(4 Sep - 3 Okt 2020)

Source : Kaspersky



Top - Vulnerabilities IN THE LAST MONTH

1	Exploit.Win32.CVE-2019-1184.a	23.92%
2	Exploit.Win32.ShadowBrokers.ae	13.95%
3	Exploit.Win32.MS17-010.shc	10.63%
4	Exploit.Win64.ShadowBrokers.d	5.59%
5	Exploit.Win32.ShadowBrokers.z	5.53%
6	Exploit.Win64.ShadowBrokers.c	5.52%
7	Exploit.Win32.ShadowBrokers.ad	5.31%
8	Exploit.Win32.ShadowBrokers.ab	5.27%
9	Exploit.Win32.ShadowBrokers.aa	5.25%
10	Exploit.Win32.CVE-2015-1701.gen	4.18%

# PETA ANCAMAN BOTNET SELURUH DUNIA

## LIVE BOTNET THREATS WORLDWIDE

The IP address locations of servers used to control computers infected with malware

● Locations with the most intense bot activity ● Command & Control botnet servers

20:22:03

Oct 5, 2020

Number of active bots in the last 24 hrs

1,166,757



Last 24 hrs hourly activity

Source :



# PETA ANCAMAN BOTNET SELURUH DUNIA

TOP 10 WORST BOTNET COUNTRIES ▲		
1	Egypt	1905067
2	China	1572739
3	India	1513422
4	United States of America	999211
5	Viet Nam	735782
6	Iran (Islamic Republic of)	513953
7	United Kingdom of Great Britain and Northern Ireland	446257
8	Brazil	424372
9	Indonesia	349214
10	Thailand	336389

TOP 10 WORST BOTNET ISPS ▲		
1	tedata.net	1865599
2	chinanet.cn.net	858878
3	vnnic.net.vn	705069
4	airtel.in	571562
5	cnc-noc.net	427820
6	rr.com	284554
7	zvi.ru	213520
8	hathway.net	197693
9	telkom.co.id	183372
10	ptcl.net.pk	147304

Data from the Spamhaus Project

source



# Threat follow asset Attack follow vulnerabilities

$$\text{TOTAL RISK} = T * V * A$$

The screenshot shows a Google search results page. At the top, the Google logo is visible on the left, and a search bar with a red background is on the right. Below the search bar, navigation links for 'All', 'Videos', 'News', 'Images', 'Maps', and 'More' are present, along with 'Settings' and 'Tools' on the far right. The search results are organized into several sections, each with a breadcrumb trail, a title, and a 'Translate this page' link. The first section is for 'disperindag.jatengprov.go.id > upliddir', with the title 'Index of /v2/upliddir/ktp - disperindag prov jateng'. It lists several image files with their parent directory, file names, and sizes. The second section is for 'disperindag.jatengprov.go.id > content', with the title 'Index of /content/files - disperindag prov jateng', listing PDF and DOC files. The third section is for 'pusdataru.jatengprov.go.id > dokumen', with the title 'Index of /dokumen/RTRW-Prov/14-Kab-Sukoharjo', listing a directory of files. The fourth section is for 'sijoli.jatengprov.go.id > download-cisco-ios-index', with the title 'Download cisco ios index - Sijoli', providing a link to a download page. The fifth section is for 'sijoli.jatengprov.go.id > google-dorks-list', with the title 'Google dorks list - Sijoli', providing a link to a dorks list. The sixth section is for 'sijoli.jatengprov.go.id > ...', with the title 'B374k upload file - Sijoli', providing a link to a file upload page. At the bottom, there is an 'Images for intitle: index of site:jatengprov.go.id' section showing a grid of image thumbnails, including official IDs and organizational charts.



# PHISHING SITES di Domain Jatengprov ? =12,800

The image shows a Google search interface. The search bar contains the word "Semua". Below the search bar, there are navigation tabs for "Semua", "Gambar", "Maps", "Berita", "Video", and "Lainnya". The search results show approximately 12,800 results in 0.28 seconds. The first result is a link to "カーペット 激安 通販 サンゲツのロールカーペット! 半額以下" from the domain "bpbj.jatengprov.go.id". The search results are repeated for several different product listings, all from the same domain. To the right of the search results is a grid of product images, including kitchen stickers, carpets, dining tables, makeup cases, and strollers, all with captions and links to the same domain.

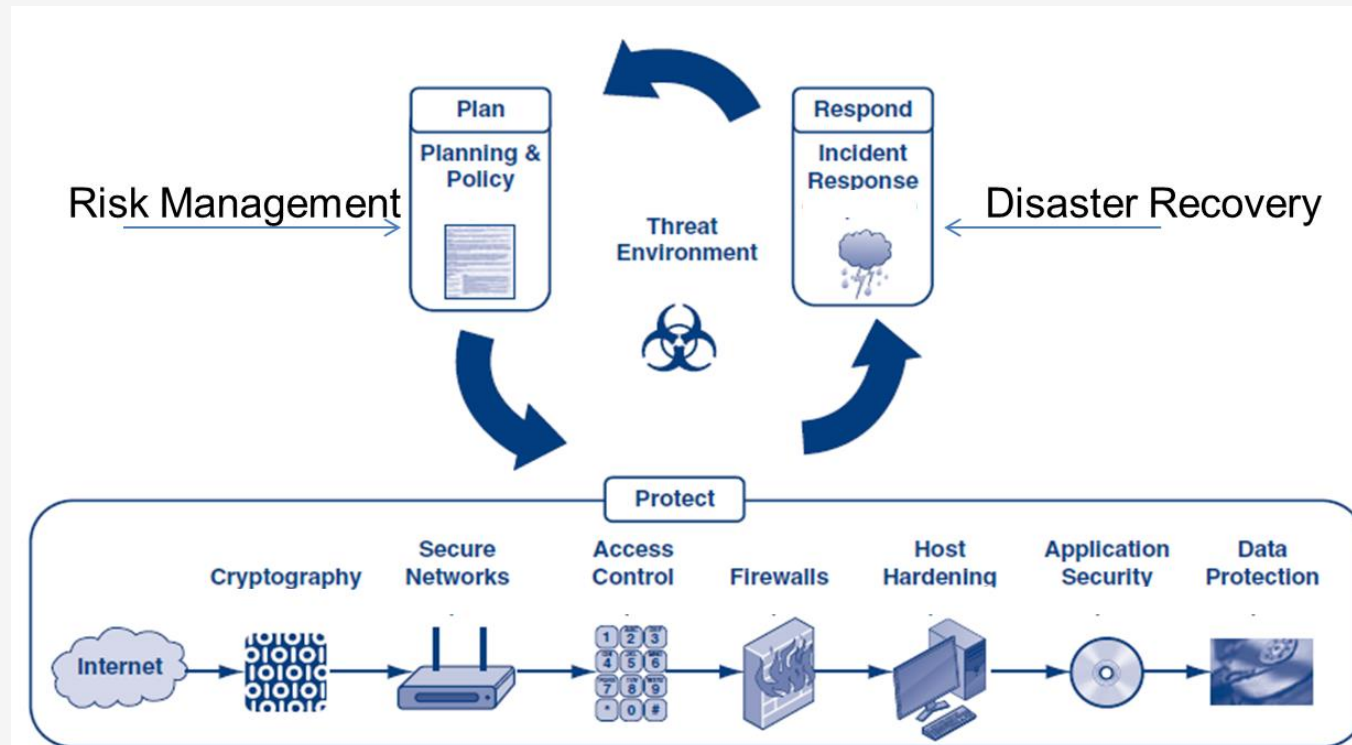
# **CSIRT=CERT=CIRT=IRT perlu !**

- 1. KARENA ANCAMAN SUDAH DIDEPAN PINTU,  
TINGGAL MENUNGGU WAKTU**

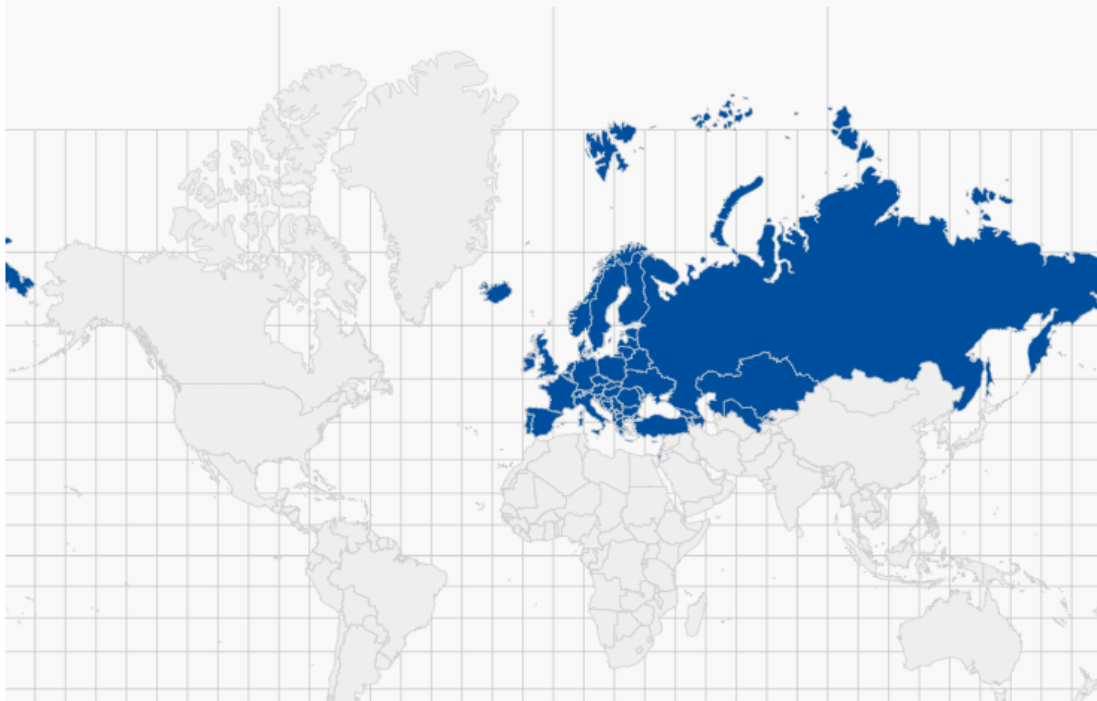
# CSIRT=CERT=CIRT=IRT perlu !

## 2. SEBAGAI SALAH SATU KOMPONEN PENTING STRATEGI KEAMANAN SIBER YANG KOMPREHENSIV

Comprehensive security management process  
“Plan-Protect-Respond Cycle”



# CSIRT=CERT=CIRT=IRT perlu !



**HAMPIR SEMUA NEGARA Di EROPA**  
sudah memiliki CSIRT, bahkan banyak yang  
lebih dari satu ( misal di Spanyol: 54 team, Perancis 40 team dsb)

Constituency Types



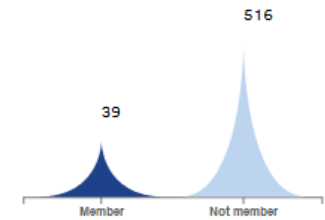
Operators of Essential Services



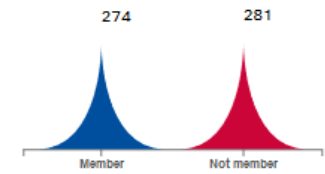
+

+

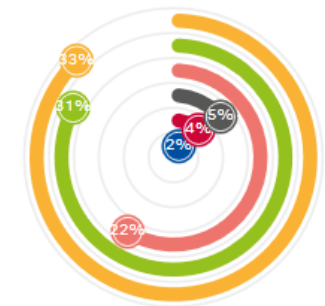
CSIRTs Network



FIRST



Trusted Introducer



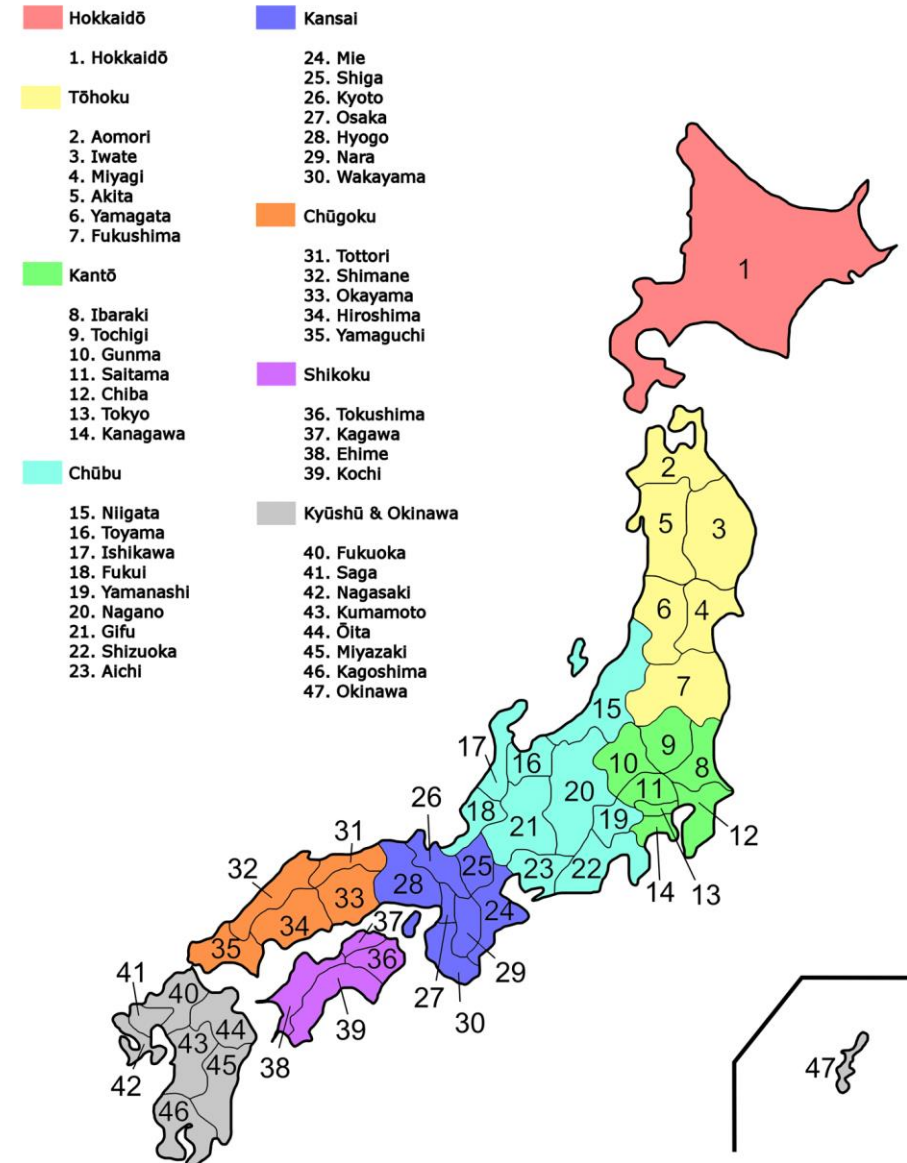
- Re-Listing Pending
- Certified
- Other
- Not listed
- Accredited
- Listed



**CSIRT=CERT=CIRT=IRT perlu !**

**Jepang 47 Propinsi,  
Jumlah CSIRTs saat ini  
404 team**

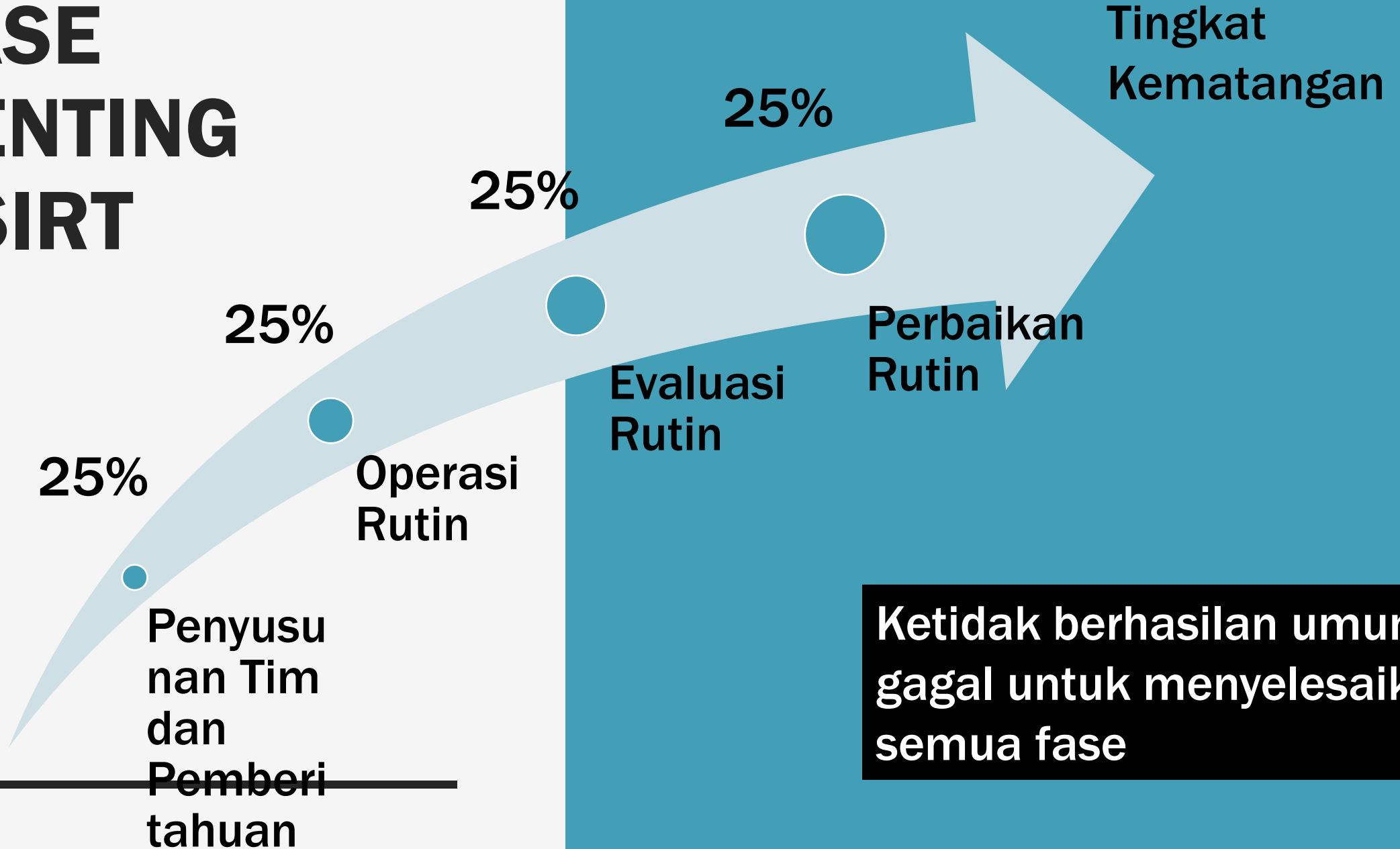
## Regions and Prefectures of Japan



# **CSIRT=CERT=CIRT=IRT perlu !**

**3. KARENA DENGAN ADANYA CSIRT, MAKA INSIDEN DAPAT DITANGANI LEBIH SISTEMATIS DAN PENANGANAN YG TEPAT DAPAT DIAMBIL. INI AKAN MEMBANTU ORGANISASI MEMPERKECIL KERUGIAN, KEBOCORAN DATA DAN MEMPERPENDEK LAYANAN YANG TERHENTI**

# FASE PENTING CSIRT



# **Faktor Sukses menjadi CSIRT yang efektif**

- **Selalu update dgn Threat Intelligence**
- **Banyak Latihan dan Drill (Train like you fight, Fight like you train)**
- **CSIRT metric**
- **Increasing maturity level**





**Last**  
But Not  
**Least**

**Those who prepare most  
for incidents  
will survive and stay safer**

---

# THANK YOU

23



**more information:**

**Email:  
rudi@csirt.id**