CSIRT Dalam Keamanan Siber Di Indonesia

Dr. Pratama Persadha
Chairman Lembaga Riset Keamanan Siber CISSReC

Kejahatan Siber
Meningkat Selama Pendemi

Tercatat oleh BSSN sepanjang Januari 2021 sampai dengan Agustus tercatat ada 888.711.736 serangan siber, yang berarti **hampir 2x lipat dibanding tahun 2020**

Marketplace Indonesia masih jadi **sasaran** empuk peretas, selain itu peretas juga menyasar lembaga negara yang memegang data pribadi masyarakat. **BPS** sangat rawan menjadi target peretasan karena mengumpulkan dan mengolah data nasional.

BPS mempunyai fungsi strategis yang membuatnya menjadi incaran peretas, baik untuk dicuri maupun dimanipulasi datanya.

- Menyediakan kebutuhan data bagi pemerintah dan masyarakat. Data ini didapatkan dari sensus atau survey yang dilakukan sendiri dan juga dari departemen atau lembaga pemerintahan lainnya sebagai data sekunder
- Membantu kegiatan statistik di departemen, lembaga pemerintah atau institusi lainnya, dalam membangun sistem perstatistikan nasional.
- Mengembangkan dan mempromosikan standar teknik dan metodologi statistik, dan menyediakan pelayanan pada bidang pendidikan dan pelatihan statistik.
- Membangun kerjasama dengan institusi internasional dan negara lain untuk kepentingan perkembangan statistik Indonesia.

Perlu Penguatan Pengaman Siber

1. **Dari Sisi SDM**
2. **Infrastruktur & Teknologi**
3. Dan yang paling penting **CSIRT di tiap lembaga**

Pekerjaan Rumah Ruang Siber Indonesia

Regulasi

- KUHP, UU ITE, UU PDP, UU KKS
- Aturan Server
- Kewajiban riset

Riset

Riset kampus, negara dan swasta, penyiapan SDM serta kurikulum edukasi siber dini.

Industri Siber Tanah Air

Kemandirian aplikasi lokal dan penyerapan produk aplikasi lokal oleh negara.

Ego Sektoral

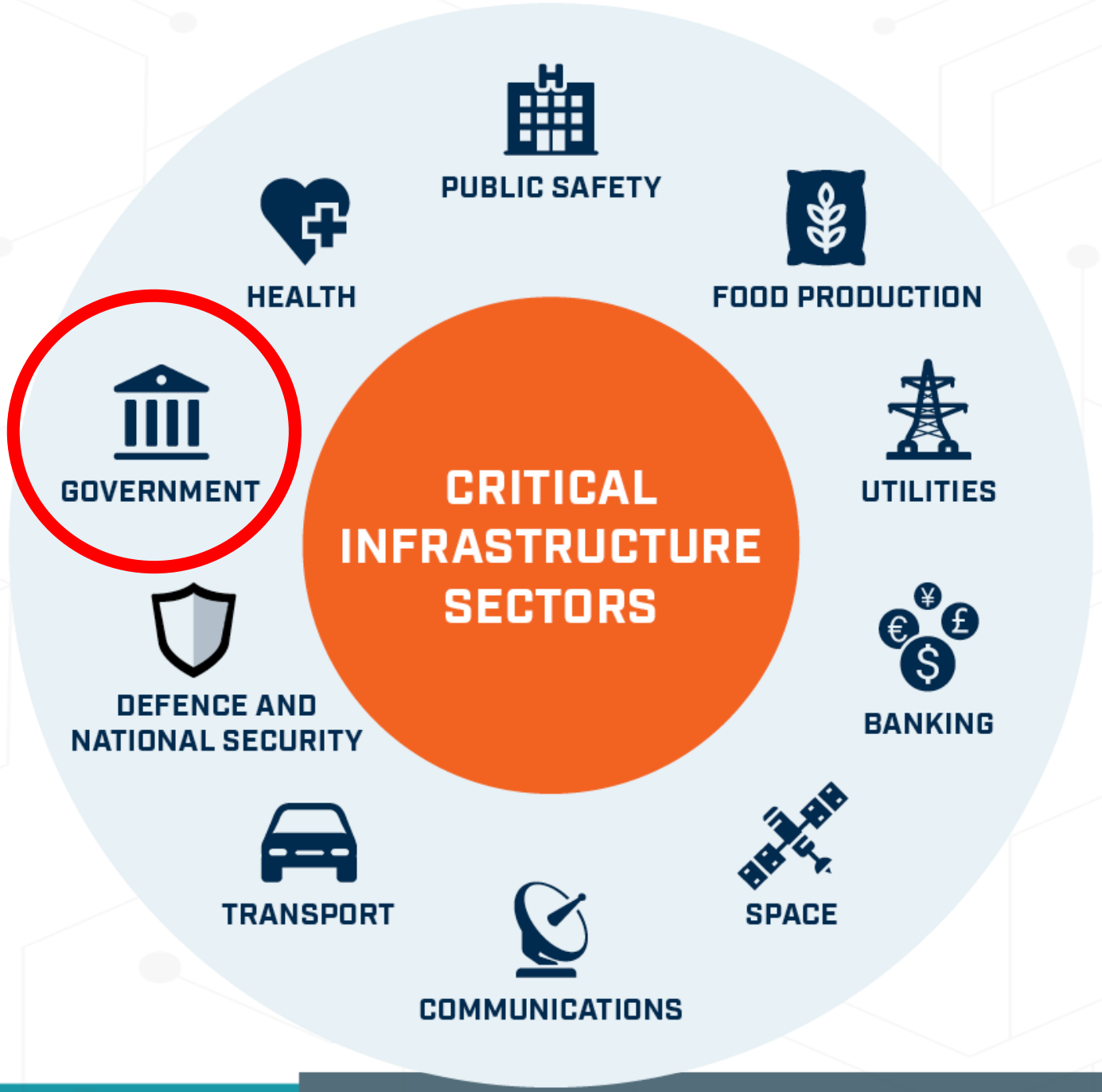
- Industri Siber

INFRASTRUKTUR KRITIS,

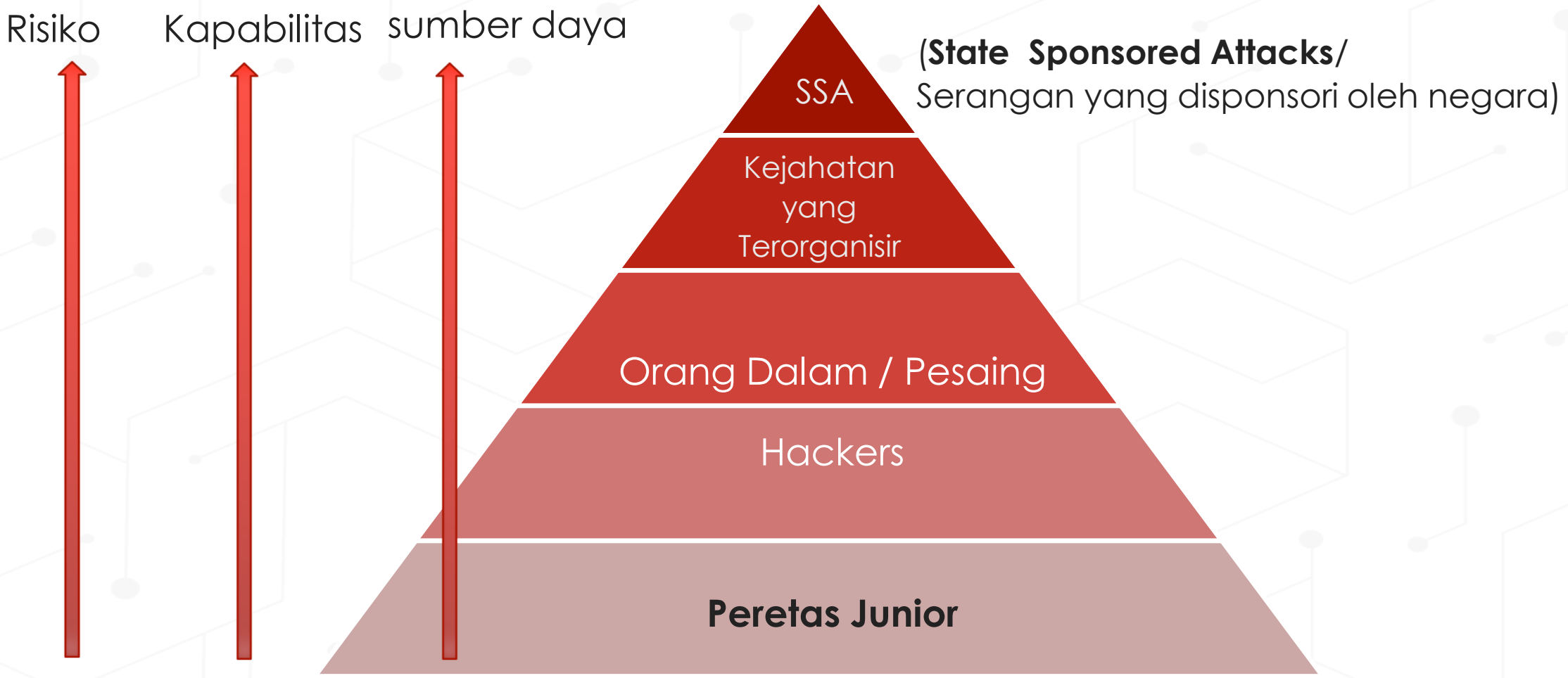
Ancaman serangan siber pada pemerintahan baik institusi negara maupun swasta jelas besar.

Upaya manipulasi dan serangan harus direspon dengan kewaspadaan menyeluruh.

Keberhasilan serangan dan manipulasi pada sistem akan meningkatkan ketidakpercayaan publik kepada negara

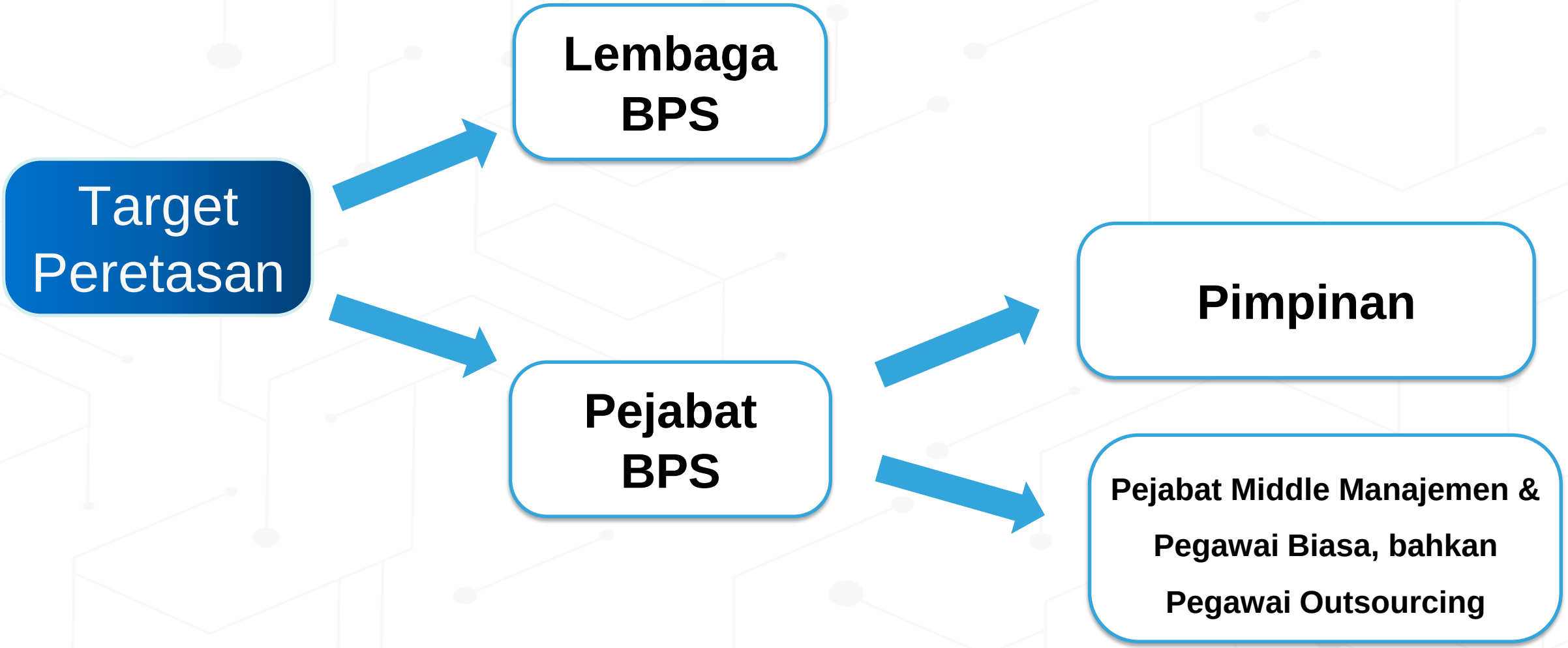


PIRAMIDA ANCAMAN SIBER



(**State Sponsored Attacks**/
Serangan yang disponsori oleh negara)

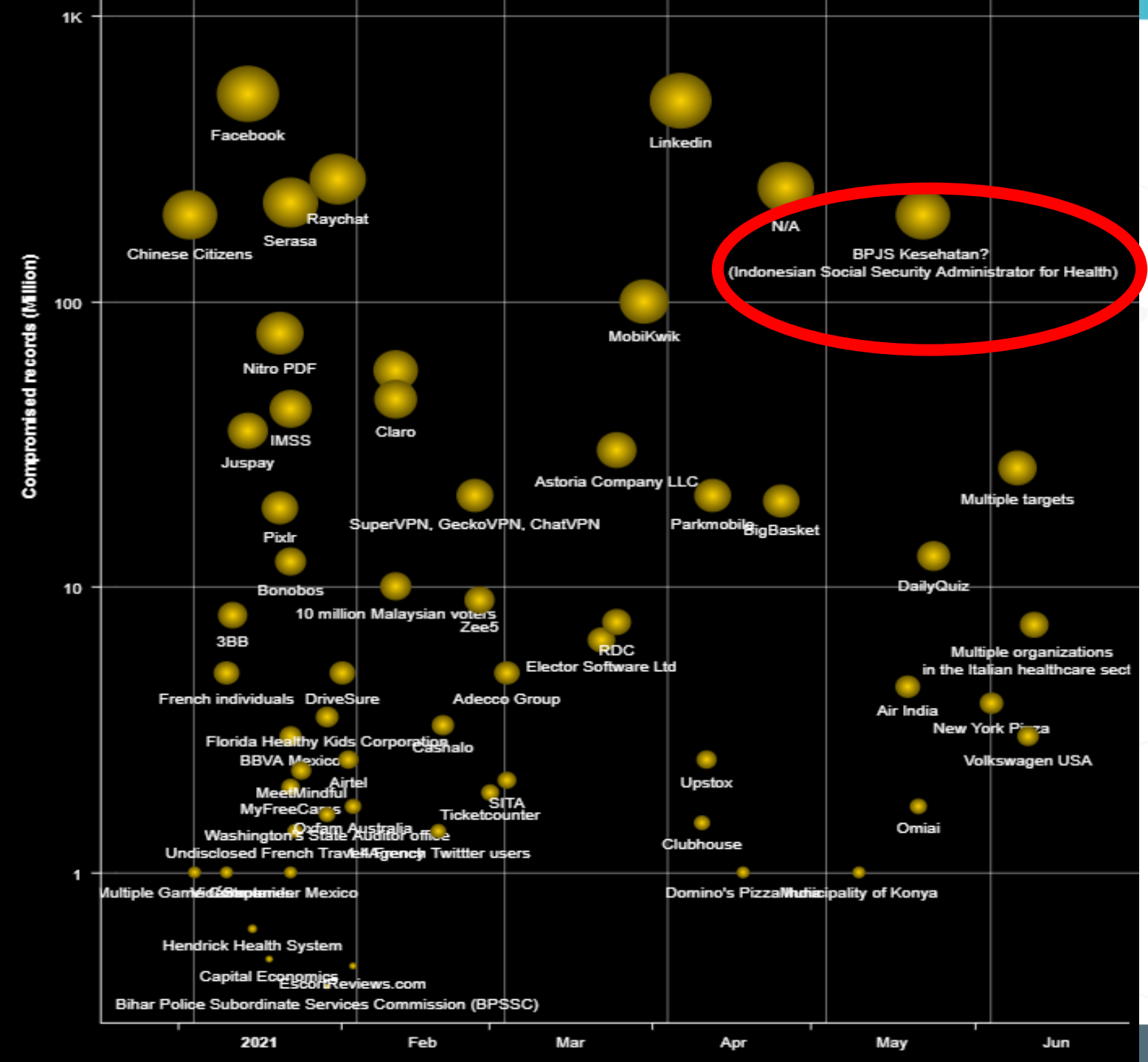
Target Peretasan di BPS



MENGAMANKAN DIRI SENDIRI.

Ancaman di dunia siber sangat banyak, dari ancaman peretasan sampai pada hoaks. Ancaman teknis seperti virus dan malware memang menyeramkan, padahal hoaks berakibat lebih destruktif.

BERBAGAI KASUS KEBOCORAN DATA DAN PERETASAN K/L NEGARA DI INDONESIA



Kasus Kebocoran 279 Juta Data BPJS Merupakan Salah Satu Pencurian Data Terbesar Di Dunia Sepanjang Tahun 2021

*hackmageddon

Peretasan Website Pemerintah

Sepanjang Desember 2020 hingga Agustus 2021, setidaknya terjadi 33.748 kali peretasan pada domain resmi pemerintah, baik pusat maupun daerah. Sistem keamanan yang relatif lemah membuat situs web pemerintah, baik pusat maupun daerah, menjadi sasaran empuk para peretas.

Kominfo Buka Suara Soal Kebocoran 2,3 Juta Data Penduduk di KPU

Fira Nursyabani - Jumat, 22 Mei 2020 | 13:58 WIB

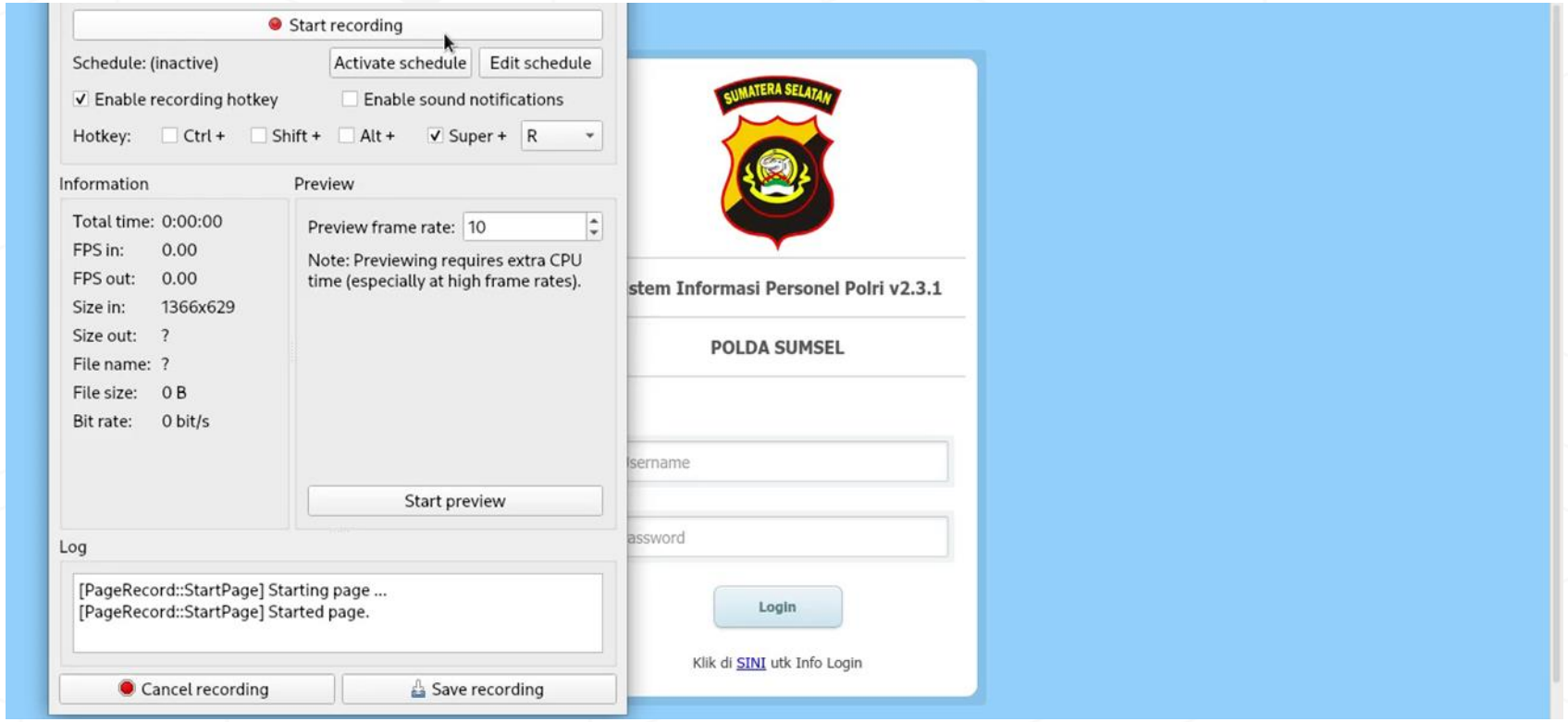
DAFTAR PEMILIH TETAP
Pemilihan Umum Anggota DPR, DPD, DPRD Provinsi dan DPRD Kabupaten/Kota
Tahun 2014

Peretas atau hacker mengklaim telah membobol 2,3 juta data warga Indonesia dari Komisi Pemilihan Umum (KPU). Peretas menyebutkan bahwa data tersebut tampaknya merupakan data tahun 2013. Tidak hanya itu, peretas juga mengklaim akan membocorkan 200 juta data lainnya.

Serangan Ransomware Pertamina

Geng peretas *ransomware*, RansomEXX, mengklaim meretas perusahaan negara minyak dan gas bumi Pertamina dan membocorkan data yang dicurinya ke *dark web*.

Tangkapan Layar Video Peretasan Database Polri



Polisi bahkan keluarganya, dalam bahaya. Data anggota Kepolisian Negara Republik Indonesia hasil peretasan dapat dibeli kelompok kriminal dan disalahgunakan untuk menyasar polisi. Server (peladen) basis data anggota Polri telah diretas, karena pelaku yang mengklaim telah melakukan peretasan mengunggah video cara meretas sistem kepolisian.

Data e-HAC

Aplikasi Covid-19, Indonesia Health Alert Card (eHAC), tak sengaja mengekspose lebih dari satu juta orang. Kebocoran data massal itu diungkap oleh vpnMentor.

Basis data milik dua juta nasabah BRI life bocor. Informasi yang bocor berupa pin polis asuransi Secure Hash Algorithm 1 (SHA-1), manfaat yang diterima nasabah, lama menjadi klien, dan lainnya.

Setidaknya ada 463 ribu dokumen yang diduga bocor. Isinya berupa foto Kartu Tanda Penduduk (KTP), Kartu Keluarga (KK), foto buku rekening, akta kelahiran, akta kematian, bukti transfer, foto hasil lab hingga keterangan penyakit.

Berkaca dari Dugaan Peretasan BIN dan 10 Kementerian oleh Hacker Tiongkok

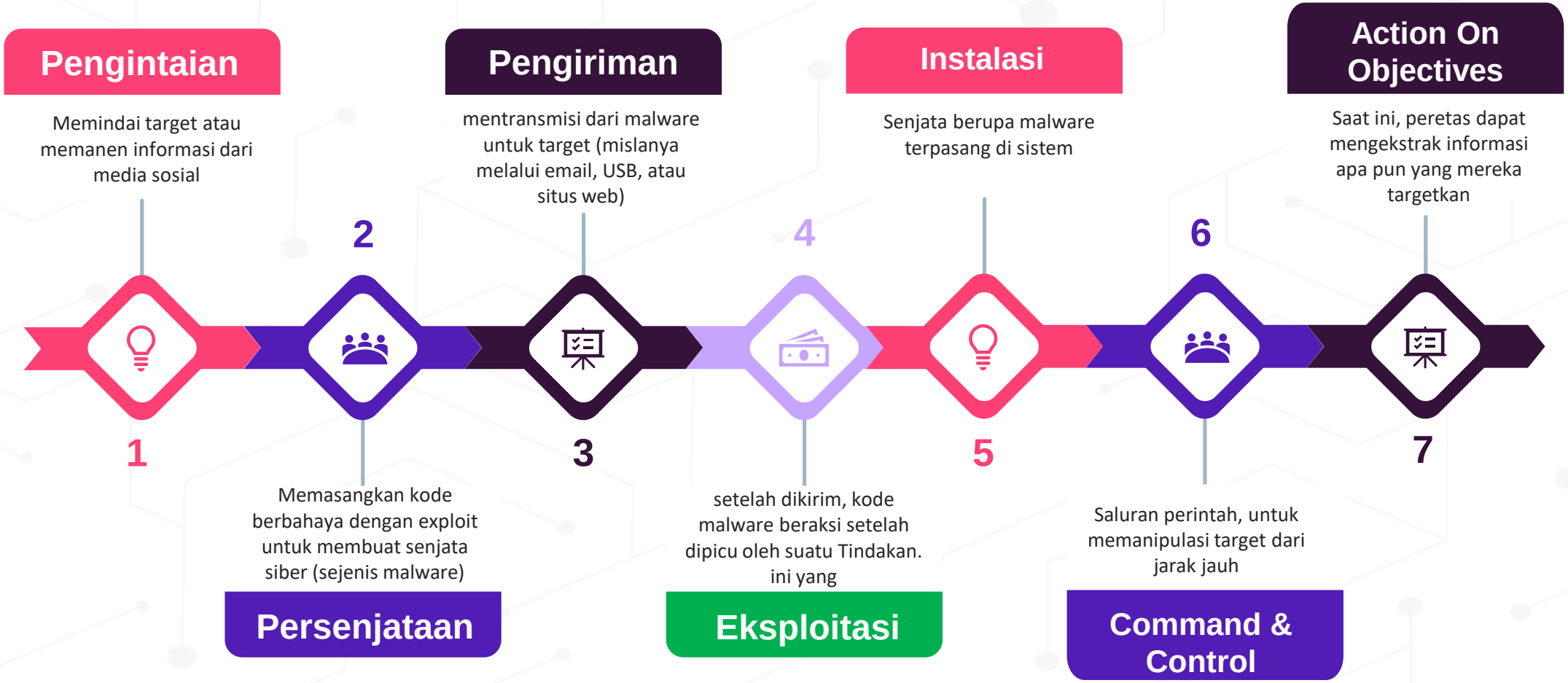
Iskandar

12 Sep 2021, 16:27 WIB

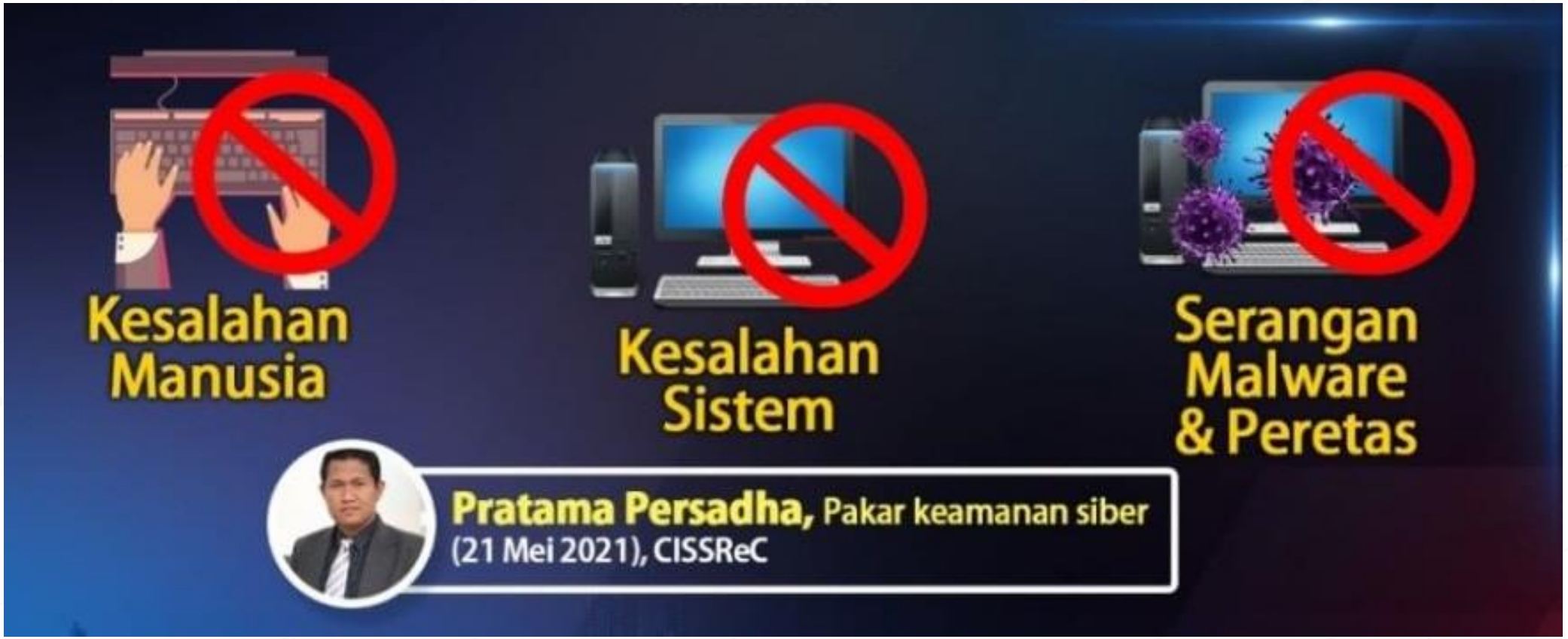
Share 12

Insikt Group melaporkan adanya **peretasan di 10 kementerian dan lembaga negara di Indonesia** (salah satunya Badan Intelijen Negara/BIN), yang mana pelakunya disebut sebagai Mustang Panda (*hacker* asal Tiongkok) menggunakan *private ransomware* bernama Thanos.

7 TAHAPAN SERANGAN SIBER


Pengintaian
Memindai target atau memanen informasi dari media sosial
1
2
Memasangkan kode berbahaya dengan exploit untuk membuat senjata siber (sejenis malware)
Persenjataan
Pengiriman
mentransmisi dari malware untuk target (mislanya melalui email, USB, atau situs web)
3
4
setelah dikirim, kode malware beraksi setelah dipicu oleh suatu Tindakan. ini yang
Eksploitasi
Instalasi
Senjata berupa malware terpasang di sistem
5
6
Saluran perintah, untuk memanipulasi target dari jarak jauh
Command & Control
Action On Objectives
Saat ini, peretas dapat mengekstrak informasi apa pun yang mereka targetkan
7

Penyebab Kebocoran Data



Dampak Dari Kebocoran Informasi Bagi Negara

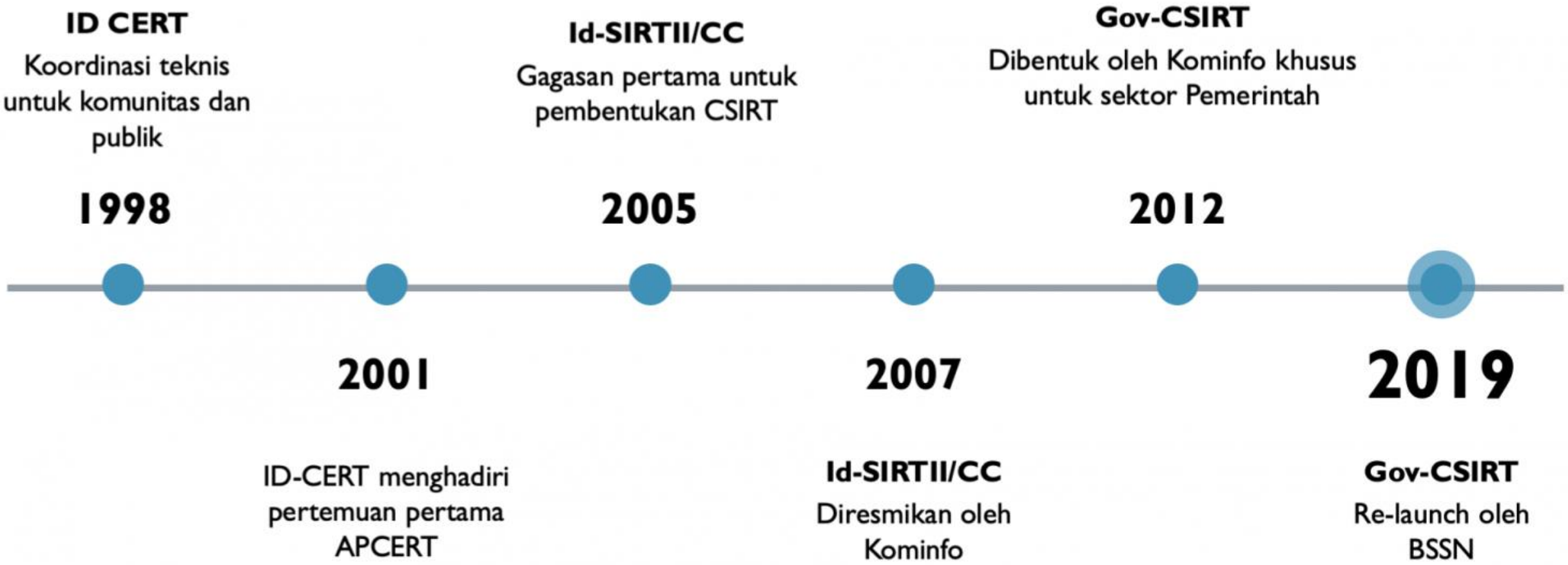
- *Reputation loss*
- *Financial loss*
- *Intellectual property loss*
- *Legislative Breaches leading to legal actions (Cyber Law)*
- *Loss of public confidence*
- *Service interruption costs*

CSIRT SEBAGAI SOLUSI

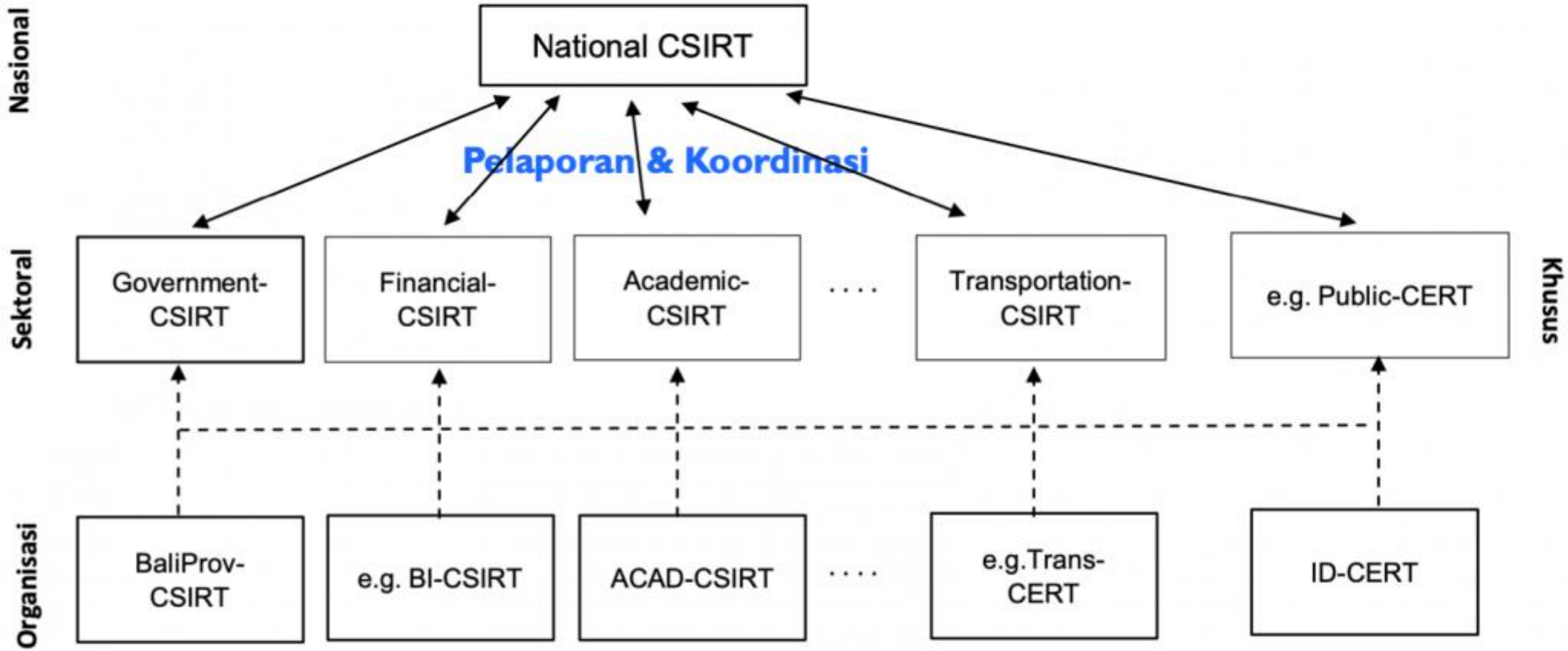
Pengertian CSIRT (Computer Security Incident Response Team)

- Sebuah organisasi atau tim yang bertanggungjawab untuk menerima, meninjau dan menanggapi laporan dan aktivitas insiden keamanan siber.
- Tim ini dibentuk dengan tujuan untuk melakukan penyelidikan komprehensif dan melindungi sistem atau data atas insiden keamanan siber yang terjadi pada organisasi.

Perjalanan CSIRT di Indonesia



Koordinasi CSIRT dalam Lingkup Nasional



Alasan Pendirian CSIRT

- Infrastruktur keamanan yang terbaikpun tidak dapat menjamin serangan tidak akan terjadi.
- Bila insiden terjadi, maka institusi bergerak cepat untuk merespon secara efektif dengan meminimalisasi kerusakan dan mengurangi biaya recovery.
- Untuk melindungi kejadian-kejadian yang tidak diinginkan di masa depan dengan mengatur strategi keamanan, berbagi informasi untuk update pengetahuan dan berkolaborasi dengan CSIRT yang lain.
- Fokus kepada pencegahan kerentanan keamanan, melakukan mitigasi dan memastikan pemenuhan/pencapaian regulasi dan kebijakan keamanan institusi.

Mengapa butuh CSIRT?

Saat insiden siber terjadi dan menyebar, maka perlu tindakan segera seperti :

- Secara efektif mendeteksi dan mengidentifiaksi segala macam aktivitas.
- Melakukan mitigasi dan merespons secara strategis.
- Membangun saluran komunikasi yang dapat dipercaya.
- Memberikan peringatan dini kepada masyarakat dan Kementerian/Lembaga tentang dampak yang akan dan sudah terjadi.
- Memberitahu pihak yang berkepentingan tentang masalah yang potensial di komunitas keamanan dan internet.
- Berkoordinasi dalam meresponse insiden.
- Berbagi data dan informasi tentang segala aktivitas dan melakukan korespondensi untuk response segala solusi kepada Kementerian/Lembaga terkait.
- Melacak dan memonitor informasi untuk menentukan tren dan strategi jangka panjang.

Fungsi CSIRT

- **DEFENSE** – melindungi infrastruktur kritis
- **MONITORING** – menganalisis anomaly dengan berbagai pola terdefinisi dan pola tak terdefinisi. (disebut sebagai vulnerability database).
- **INTERCEPTING** – mengumpulkan kontek spesifik atau disebut targeted content.
- **SURVEILLANCE** –mengamati dan menganalisis aktivitas yang dicurigai dan informasi yang berubah dalam sistem.
- **MITIGATING** – mengendalikan kerusakan dan menjaga ketersediaan serta kemampuan layanan tersebut.
- **REMEDIATION** – membuat solusi untuk mencegah kegiatan yang berulang-ulang dan mempengaruhi sistem.
- **OFFENSIVE** – pencegahan/perlawanan dengan menyerang balik seperti Cyber Army dan kemampuan untuk menembus sistem keamanan.

SERVICE AREAS

INFORMATION SECURITY INCIDENT MANAGEMENT

- Information Security Incident Report Acceptance
- **Information Security Incident Analysis**
- **Artifact and Forensic Evidence Analysis**
- Mitigation and recovery
- **Information Security Incident Coordination**
- Crisis management Support

VULNERABILITY MANAGEMENT

- Vulnerability Discovery/Research
- Vulnerability Report intake
- Vulnerability Analysis
- **Vulnerability Coordination**
- Vulnerability Disclosure
- Vulnerability Response

SITUATIONAL AWARENESS

- Data Acquisition
- Analysis and Synthesis
- Communication

KNOWLEDGE TRANSFER

- **Awareness Building**
- Training and Education
- Exercises
- Technical and Policy Advisory

INFORMATION SECURITY EVENT MANAGEMENT

- Monitoring and Detection
- Event Analysis

Alur Dari Siklus Tanggap Insiden

6 Langkah Tanggap Insiden

- **Persiapan (Preparation)**

Pada tahap persiapan, diharuskan untuk meninjau dan menyusun kebijakan keamanan dasar yang menginformasikan rencana respons insiden.

- **Identifikasi (Identification)**

Tim harus dapat secara efektif mendeteksi keanehan dari sistem normal dalam dan mengidentifikasi apakah keanehan tersebut mewakili insiden keamanan yang terjadi saat ini.

- **Penahan-an (Containment)**

Setelah tim mengidentifikasi insiden keamanan, tujuan langsungnya adalah menahan insiden tersebut dan mencegah terjadinya kerusakan lebih lanjut.

- **Pemberantasan (Eradication)**

Tim harus mengidentifikasi akar penyebab serangan, penghapusan malware atau ancaman, dan mencegah serangan serupa di masa mendatang.

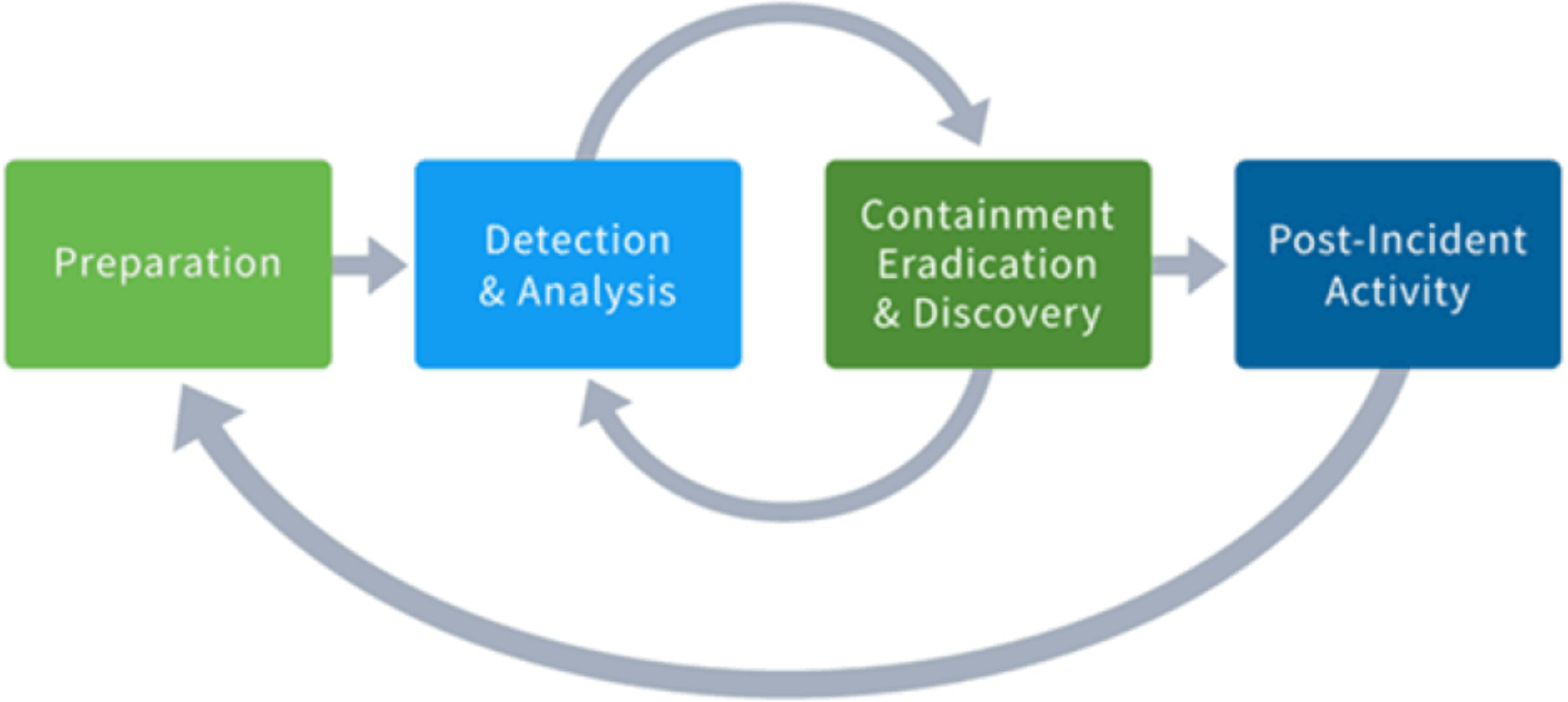
- **Pemulihan (Recovery)**

Tim membawa sistem yang terdampak untuk kembali online, dan mengecek ulang untuk memastikan insiden lain tidak terjadi.

- **Evaluasi (Lessons Learned)**

Dengan mempelajari insiden yang terjadi untuk mencegah kejadia terulang. Termasuk menambal kerentanan server, atau meluncurkan teknologi yang lebih baik. Juga memperbaiki kelemahan atau kerentanan keamanan yang ditemukan.

Alur rekomendasi untuk merespons insiden keamanan siber



Contoh Alur Kasus Kebocoran eHAC Kemenkes

1. **22 Juli 2021**, VPN Mentor pihak yang mempublikasi informasi tersebut pada awalnya mengirimkan informasi tentang kebocoran data aplikasi e-HAC milik Kementerian Kesehatan ke Indonesia Computer Emergency Response Team (CERT.ID), namun tidak mendapat respon.

2. **23 Agustus 2021** pukul 06.00 WIB, VPNMentor kembali mengirimkan laporan tersebut melalui email ke ID-SIRTII (Indonesia Security Incident Response Team On Internet Infrastructure) dan bantuan70@bssn.go.id.

3. Laporan yang dikirim VPNMentor kemudian direspon oleh Tim Tanggap Insiden BSSN pada 23 Agustus 2021 pukul 08.39 WIB, setelah memverifikasi informasinya.

4. Pada hari yang sama (23 Agustus 2021), tim BSSN langsung berkoordinasi dengan pihak Kementerian Kesehatan untuk menindaklanjuti laporan ini.

5. **24 Agustus 2021**, Tim BSSN melakukan verifikasi dan mengkonfirmasi kembali ke pihak Kementerian Kesehatan melalui laporan dengan Nomor 021/TI/SDE.824.1/N/2021.

6. **25 Agustus 2021**, Tim Kementerian Kesehatan menindaklanjuti laporan itu dengan mengatasi celah keamanan pada aplikasi e-HAC. Tim BSSN mengkonfirmasi hal ini kepada pihak Kementerian Kesehatan pada 25 Agustus 2021 pukul 15.31 WIB.

Kesalahan Respon Pada Kasus eHAC Kemenkes

- Kemenkes tidak responsif saat diberi laporan
- Baru pada saat laporan masuk BSSN, langsung ada pergerakan
- Dan itupun setelah 2 hari, yang seharusnya hanya beberapa jam saja

TERIMAKASIH