Jum’at, 3 Juni 2022

PAPARAN
TIM TANGGAP INSIDEN SIBER / SUB-CSIRT
KEMENTERIAN PERTAHANAN

PUSAT PERTAHANAN SIBER
BADAN INSTALASI STRATEGIS PERTAHANAN
KEMENTERIAN PERTAHANAN RI

AGENDA PEMBAHASAN :

A. CSIRT KEMHAN
B. KEGIATAN DGN BSSN → *COMMUNICATION CHECK*
C. *CALL CENTER*
D. RENCANA LATIHAN SATUAN

LATAR BELAKANG PELAKSANAAN CSIRT

1. Pemanfaatan teknologi informasi dan komunikasi maupun teknologi internet dapat menyebabkan kerawanan dan ancaman siber yang meliputi aspek kerahasiaan, keutuhan, ketersediaan, nir-sangkal, otentisitas, akuntabilitas dan keandalan layanan, sehingga dibutuhkan penyediaan pelayanan publik yang cepat, andal, dan aman;

2. Semakin maraknya serangan siber terhadap infrastruktur pemerintahan, pelayanan publik sudah seharusnya institusi pemerintahan memiliki sistem keamanan yang dapat meminimalisir kejahatan siber dan merespon bila ada serangan siber.

PENYELENGGARA SISTEM ELEKTRONIK

- Penyelenggara sistem elektronik wajib menyediakan sistem pengamanan yang mencakup prosedur dan sistem pencegahan, penanggulangan dan pemulihan terhadap ancaman dan serangan yang menimbulkan gangguan, kegagalan, dan kerugian
- Untuk menjamin sistem elektronik dapat beroperasi secara terus menerus, maka diperlukan kemampuan untuk melakukan penanggulangan insiden dan/atau pemulihan insiden

TUJUAN INCIDENT HANDLING

01 Memastikan bahwa insiden terjadi atau tidak terjadi

02 Melakukan pengumpulan informasi yang akurat

03 Melakukan pengambilan dan penanganan bukti-bukti

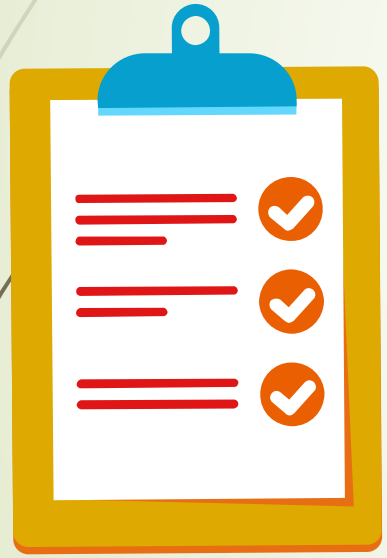
04 Menjaga agar kegiatan berada dalam kerangka hukum

05 Meminimalkan gangguan terhadap operasi dan jaringan

06 Membuat laporan yang akurat beserta rekomendasinya

BAGAIMANA BILA ADA INCIDENT

Laporan incident



Laporan Incident dari Internal

Laporan Incident dari External

Koordinasi Kolaborasi

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

- Secara Efektif mendeteksi dan mengidentifikasi segala macam aktivitas
- Melakukan mitigasi dan merespons secara strategis
- Membangun saluran komunikasi yang dapat dipercaya
- Memberikan peringatan dini kepada satker kemhan dan konstituen tentang dampak yang akan dan sudah terjadi

Saat Insiden Siber terjadi dan menyebar, maka perlu tindakan segera seperti:

- Memberitahu pihak lain tentang masalah-masalah yang potensial di komunitas keamanan dan internet.
- Berkoordinasi dalam meresponse masalah
- Berbagi data dan informasi tentang segala aktivitas dan melakukan korespondensi untuk response segala solusi kepada konstituen
- Melacak dan memonitor untuk menentukan tren dan strategi jangka panjang

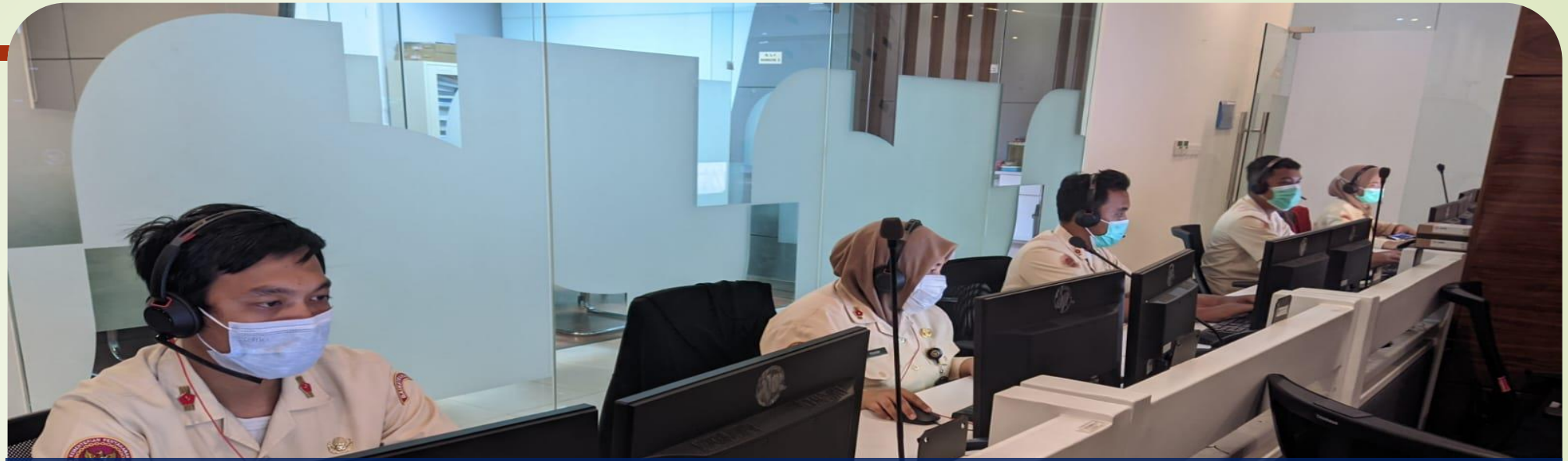
COMMUNICATION CHECK
CSIRT KEMHAN - BSSN

Tanggal 23 Maret 2022, Materi pmbahasan, Format Pelaporan Kronologi, Format Pelaporan Insiden & *Platform* u/ berbagi informasi (*Discord*, Palapa, *Slack*).

Pada 24 Maret 2022, Materi Pmbahasan, mlakukan simulasi akuisisi data m'gunakan aplikasi FTK imager & analisa hasil data imaging dari FTK imager m'gunakan aplikasi/sistem ELK.

COMMUNICATION CHECK
CSIRT KEMHAN - BSSN

- Tanggal 20 April 2022, Materi P’mbahasan, dimana GOV-CSIRT memastikan CSIRT Pemerintah Daerah ataupun Pusat dapat berkirim dan mengirim pesan e-mail melalui email dinas yang terenkripsi dengan PGP key sesuai dengan standar RFC 2350.
- Tanggal 21 April 2022, Workshop Teknik, m’lakukan akuisisi data serta m’lakukan dokumentasi *chain of custody* , seperti : Merk server yang diakuisisi, Nomor seri, kapasitas, foto, dan informasi lainnya.



CALL CENTER CSIRT
Kementerian Pertahanan

PUSAT PERTAHANAN SIBER
BADAN INSTALASI STRATEGIS PERTAHANAN
KEMENTERIAN PERTAHANAN RI

KEGIATAN CALL CENTER CSIRT KEMHAN

MENERIMA PENGADUAN BILA TERJADI INSIDEN SIBER DI LINGKUNGAN KEMENTERIAN PERTAHANAN

ALUR ADUAN INSIDEN SIBER

Segera laporkan !!!
Apabila anda menemukan insiden siber

Terjadi
Insiden siber

Kumpulkan bukti insiden berupa
Foto / screenshot insiden / log file
Yang ditemukan

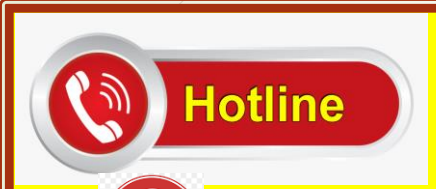
Aduan segera
Kami tangani

Hubungi **Hotline 021-29770001**
dan Media Sosial
Laporkan & Kirimkan bukti ke
csirt@kemhan.go.id

LAYANAN CALL CENTER
CSIRT KEMHAN

BADAN SIBER DAN SANDI NEGARA

LAYANAN CALL CENTER CSIRT KEMHAN



Line1 : 021-29770001

Line2 : 021-80600200

MEDIA SOSIAL

Email	:	Cs.csirt@kemhan.go.id
Facebook	:	CSIRT Kemhan
Twitter	:	@CsirtKemhan
Instagram	:	csirt.kemhan

JENIS INSIDEN YANG DILAYANI :

- ✓ **Laporan Insiden Keamanan Siber**
- ✓ **Laporan Kerentanan (*Vulnerability Disclosure*)**
- ✓ **Laporan *Phising***
- ✓ **Laporan Indikator Serangan**
- ✓ **Laporan *Malware***

RENCANA LATIHAN DALAM SATUAN

- Rencana kedepan bahwa Pushansiber akan lakukan Latihan Dalam Satuan dengan adanya Serangan Siber.
- Datin Satker sebagai Sub CSIRT nantinya juga akan dilibatkan.

TERIMA KASIH