



***Pengarahan  
Bimbingan Teknis Kesiapsiagaan Teknis Insiden  
Keamanan Siber pada CSIRT Sektor Pemerintah Daerah***

*Direktorat Keamanan Siber dan Sandi Pemerintah Daerah  
Surabaya, 23-25 Mei 2023*

# DASAR KEGIATAN

- Peraturan Presiden Republik Indonesia Nomor 18 Tahun 2020 tentang Rencana Pembangunan Jangka Menengah Nasional Tahun 2020-2024;
- Peraturan Presiden Republik Indonesia Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital;
- Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2020 tentang Tim Tanggap Insiden Siber;
- Program Kerja Direktorat Keamanan Siber dan Sandi Pemerintah Daerah Tahun Anggaran 2023;
- Surat Undangan Direktur Keamanan Siber dan Sandi Pemerintah Daerah Nomor 1553/BSSN/D3/PS.02.02/03/2023 tanggal 7 Maret 2023 perihal Undangan Bimbingan Teknis Kesiapsiagaan Teknis Insiden Keamanan Siber pada *Computer Security Incident Response Team (CSIRT)* Sektor Pemerintah Daerah;

# KEGIATAN PENINGKATAN KAPASITAS SDM



**Cyber Security Exercise Technical** adalah kegiatan simulasi teknis dalam menangani insiden keamanan di dunia teknologi informasi (*Incident Response*)

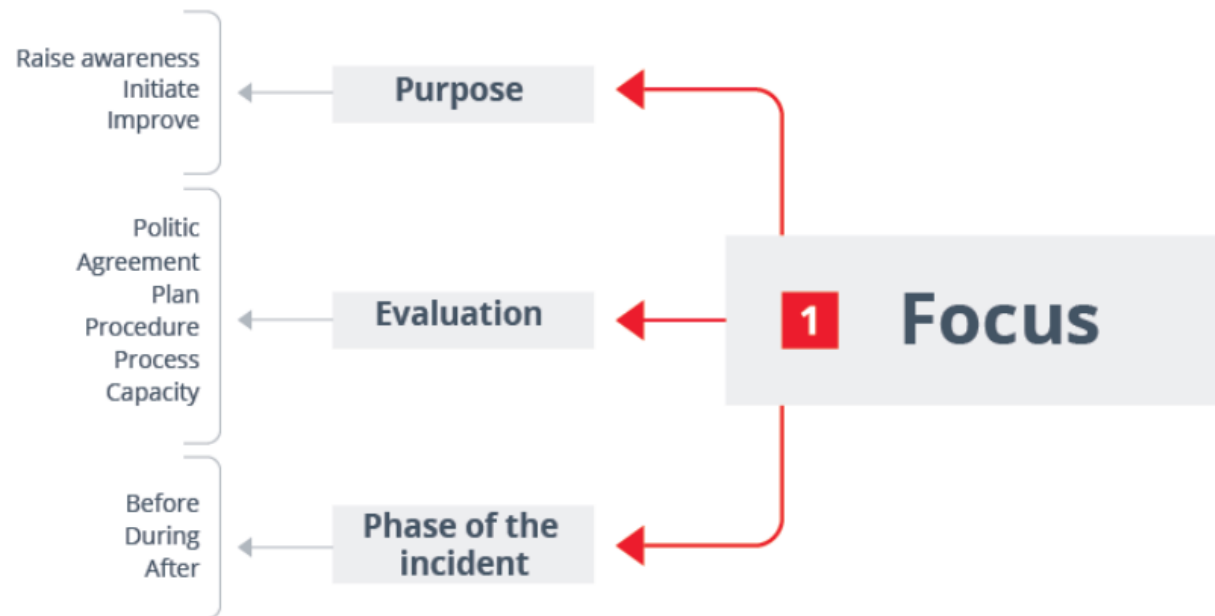
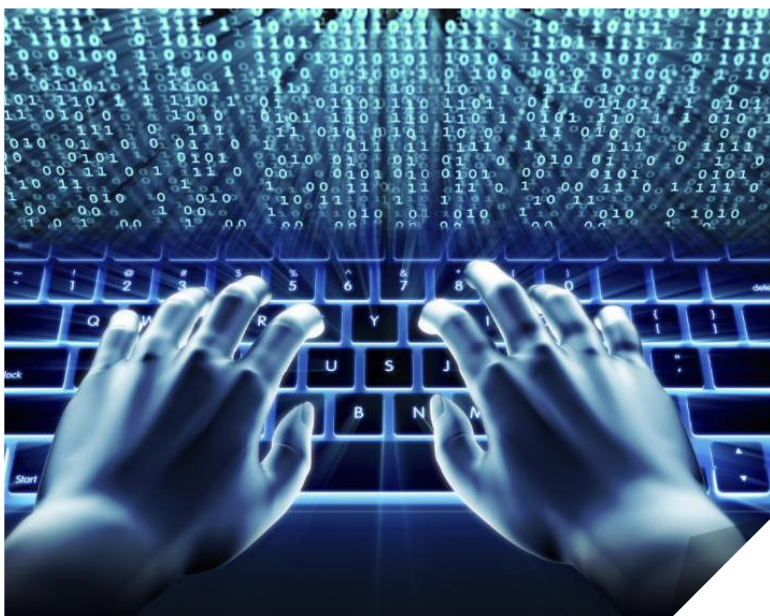
## ■ Tujuan

- Membangun fungsi koordinasi bersama dengan stakeholder sektor pemerintah terkait penanganan insiden keamanan siber.
- Sebagai sarana peningkatan wawasan bagi stakeholder sektor pemerintah dalam rangka penanganan insiden keamanan siber.

## ■ Sasaran

- Melakukan pengujian pada prosedur penanganan insiden keamanan siber yang dimiliki
- Meningkatkan kesadaran akan adanya ancaman siber
- Meningkatkan koordinasi dalam hal berbagi informasi penanganan insiden keamanan siber

# CYBER SECURITY EXERCISE TECHNICAL



## Model

Jenis ini digunakan sebagai latihan pertama yang dilakukan dalam suatu organisasi, untuk secara bertahap meningkatkan kompleksitas.

Model cyber exercise ini mencakup berbagai jenis, seperti: Seminar, Workshop, Technical, Table Top, dan Games.

Jenis-jenis ini digunakan untuk memvalidasi rencana, kebijakan, perjanjian dan prosedur, yang telah dikonsolidasikan sebelumnya pada Discussion Based. Model ini memungkinkan untuk memperjelas peran dan tanggung jawab, mengimplementasikan rencana dan prosedur, dan meningkatkan kinerja individu maupun kolektif. Model ini mencakup berbagai jenis, seperti: Hybrid Exercise & Full-scale Cyber Exercise.

# SKENARIO EXERCISE



## Cyber Exercise Technical

Pada kegiatan ini, akan diberikan sebuah artefak atau bukti insiden sebagai bahan untuk melakukan identifikasi dan analisa insiden tersebut. Setiap peserta akan diberikan sebuah Injeksi yang di dalamnya terdapat pertanyaan yang harus dijawab oleh seluruh peserta.

Setiap injeksi merupakan gambaran dari tahapan-tahapan tim Penanganan Insiden dalam melakukan penanganan insiden keamanan siber sampai dengan proses dokumentasi dan pelaporan penanganan insiden.

**Skenario-nya adalah Penanganan Insiden Siber Hijacking Situs Judi Online**

# SKENARIO EXERCISE



## **Ketua Tim**

---

Berperan sebagai penanggungjawab dan koordinator Tim Penanganan Insiden serta merangkap *Point of Contact*

## ***Point of Contact***

---

Berperan sebagai pusat koordinasi antara pelapor dan tim teknis penanganan insiden.

## ***Incident Handler***

---

Berperan sebagai tim teknis penanganan insiden yang melakukan investigasi bukti insiden

# PESERTA KEGIATAN

## 27 Pemerintah Provinsi dan 42 Kabupaten/Kota

1. Prov Sumatera Utara
2. Provinsi Kepulauan Riau
3. Provinsi Riau
4. Provinsi Sumatera Barat
5. Provinsi Jambi
6. Provinsi Sumatera Selatan
7. Provinsi Kepulauan Bangka Belitung
8. Provinsi Lampung
9. Provinsi DKI Jakarta
10. Provinsi Banten
11. Provinsi Jawa Barat
12. Provinsi Jawa Tengah
13. Provinsi Jawa Timur
14. Provinsi Bali
15. Provinsi Kalimantan Utara
16. Provinsi Kalimantan Barat
17. Provinsi Kalimantan Tengah
18. Provinsi Kalimantan Timur
19. Provinsi Kalimantan Selatan
20. Provinsi Gorontalo
21. Provinsi Sulawesi Utara
22. Provinsi Sulawesi Tengah
23. Provinsi Sulawesi Selatan
24. Provinsi Sulawesi Tenggara
25. Provinsi Maluku
26. Provinsi Maluku Utara
27. Provinsi Sulawesi Barat

# PESERTA KEGIATAN

## 27 Pemerintah Provinsi dan 42 Kabupaten/Kota

- |                   |                       |                   |                    |
|-------------------|-----------------------|-------------------|--------------------|
| 1. Kota Palembang | 12. Kota Cilegon      | 23. Kab Karawang  | 33. Kab Semarang   |
| 2. Kota Tangerang | 13. Kota Surakarta    | 24. Kab Mojokerto | 34. Kab Bandung    |
| 3. Kota Mojokerto | 14. Kota Bekasi       | 25. Kab Klaten    | 35. Kab Belitung   |
| 4. Kota Blitar    | 15. Kota Probolinggo  | 26. Kab Demak     | 36. Kab Pasuruan   |
| 5. Kota Kediri    | 16. Kab Kebumen       | 27. Kab Tangerang | 37. Kab Pamekasan  |
| 6. Kota Salatiga  | 17. Kab Banyumas      | 28. Kab Bogor     | 38. Kab Purworejo  |
| 7. Kota Batu      | 18. Kab Batang        | 29. Kab Subang    | 39. Kab Banyuwangi |
| 8. Kota Surabaya  | 19. Kab Madiun        | 30. Kab Gresik    | 40. Kab Sumedang   |
| 9. Kota Cirebon   | 20. Kab Trenggalek    | 31. Kab Badung    | 41. Kab Muba       |
| 10. Kota Denpasar | 21. Kab Solok Selatan | 32. Kab Bondowoso | 42. Kota Malang    |
| 11. Kota Semarang | 22. Kab Sukoharjo     |                   |                    |





# SUSUNAN ACARA

## 1<sup>st</sup> Day

1.	10.00 - 14.00	- Registrasi Peserta - Makan Siang
2.	14.00 - 15.00	Pembukaan Kegiatan : - Pembukaan - Menyanyikan Lagu Indonesia Raya - Do'a - Sambutan Ketua Panitia - Sambutan Provinsi Jawa Timur - Sambutan Walikota Surabaya - Sambutan Deputi III BSSN - Foto Bersama
3.	15.00 - 15.45	Coffe Break
4.	15.45 - 17.00	- Pengarahan Bimtek - Prosedur Penanganan Insiden Siber
5.	17.00 - 19.00	Istirahat + Check in Peserta
6.	19.00 - 21.00	Instalasi dan Konfigurasi Environment Bimtek

## 2<sup>nd</sup> Day

1.	06.00 - 08.00	Makan Pagi
2.	08.00 - 09.00	Registrasi Peserta
3.	09.00 - 12.00	Sesi Bimtek I - Praktik Penanganan Insiden Case : Identifikasi dan Analisa Insiden - Pengenalan Tools Penanganan Insiden

4.	12.00 - 13.30	Ishoma
5.	13.30 - 15.30	Sesi Bimtek II : - Praktik Penanganan Insiden Case : Containment, Eradication & Recovery
7.	15.30 - 16.00	Coffe Break
8.	16.00 - 17.00	Sesi Bimtek III: - Pembuatan Laporan Penanganan Insiden
9.	17.00 - 19.00	Istirahat
10.	19.00 - 21.00	Sesi Exercise - Exercise

## 3<sup>rd</sup> Day

1.	06.00 - 08.00	Makan Pagi
2.	08.00 - 09.00	Registrasi Peserta
3.	09.00 - 11.00	Sesi Evaluasi Bimtek : - Survey Kepuasan - Update Narahubung CSIRT
4.	11.00 - 11.30	Penutupan Kegiatan
5.	11.30 - 12.00	Check Out Peserta

# LINK BIMTEK KESIAPSIAGAAN TEKNIS INSIDEN KEAMANAN SIBER PADA CSIRT SEKTOR PEMERINTAH DAERAH

<https://s.id/csirt23>



  
**BIMTEK KESIAPSIAGAAN CSIRT**  
23-25 Mei 2023  
Novotel Samator, Surabaya

- Registrasi Peserta
- Materi Bimtek
- Tools Pendukung Bimtek
- Survey Layanan & Update Narahubung CSIRT
- Sertifikat Peserta (Coming Soon)



TERIMA KASIH