

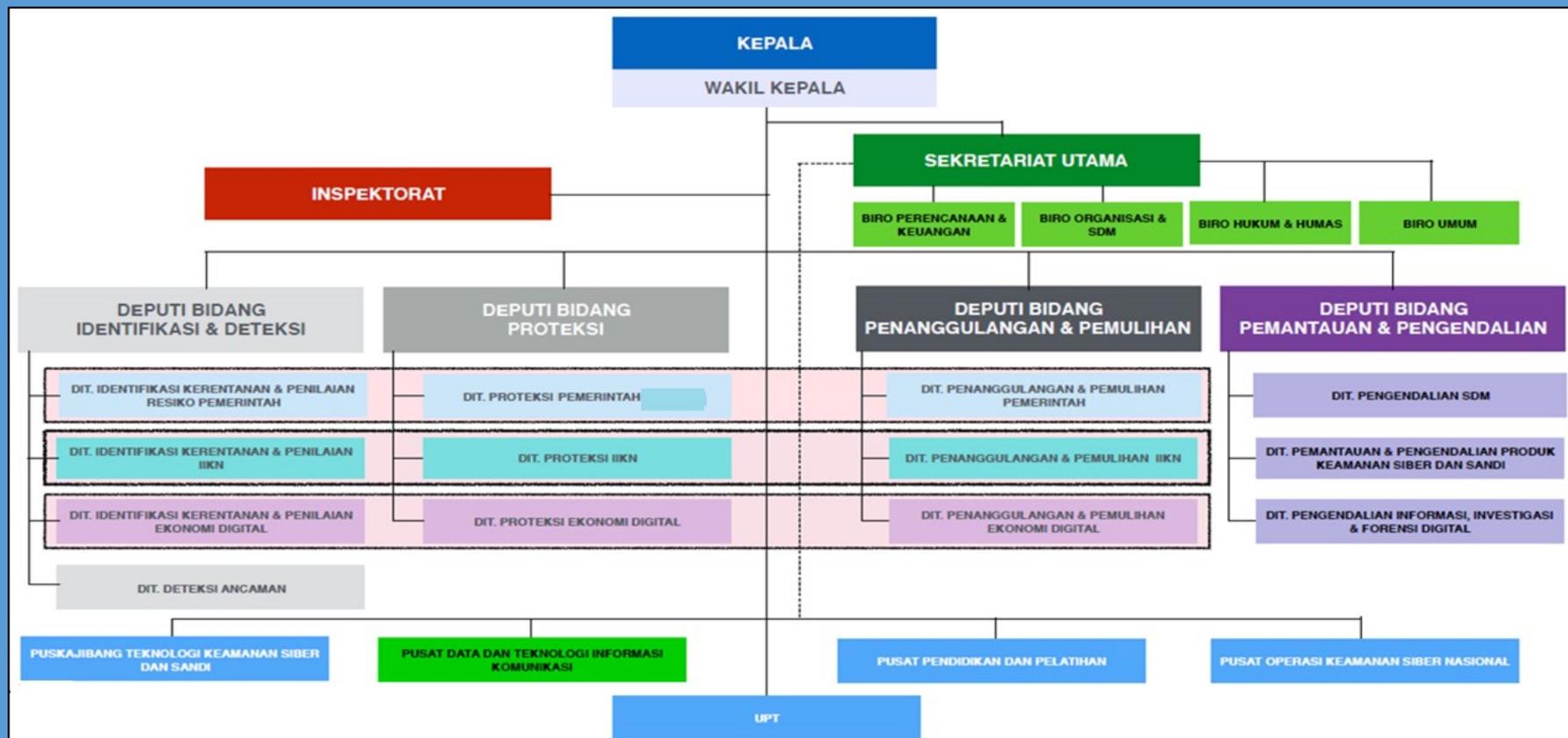


# Cyber Security Drill Test

Sriyanto, S.Sos., M.M.  
Kepala Sub Direktorat Penanggulangan dan Pemulihan Pemerintah Daerah Wilayah I  
Badan Siber dan Sandi Negara

<https://www.bssn.go.id>  
<https://govcsirt.bssn.go.id>

# SOTK BSSN



# Visi BSSN

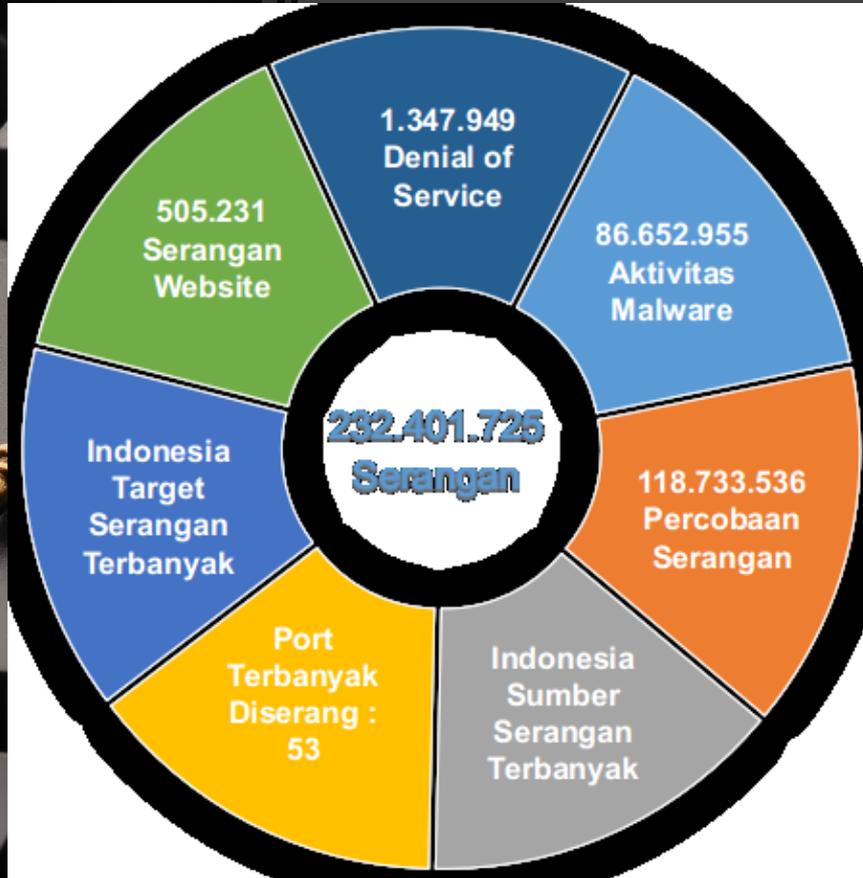


**Menjadi Institusi Terpercaya dalam Rangka Menjaga Keamanan Siber dan Sandi Negara dengan Menynergikan berbagai Pemangku Kepentingan Untuk Ikut Serta Mewujudkan Keamanan Nasional dan Meningkatkan Pertumbuhan Ekonomi Nasional**

# Misi BSSN

Membangun, mengoordinasikan, mengolaborasikan, dan mengoperasionalkan sistem identifikasi, deteksi, mitigasi, manajemen krisis, penanggulangan, dan pemulihan terhadap ancaman, insiden, dan/atau serangan siber dan Sandi.

# DATA SERANGAN SIBER 2018



- Indonesia menjadi Target Serangan dan Sumber Serangan Terbanyak
- Jumlah IP Indonesia yang terinfeksi botnet mencapai 15 Juta IP



## Insiden

Insiden adalah:  
Kejadian tak terduga yang menyebabkan gangguan operasi normal

### Insiden Keamanan

- Suatu kejadian pelanggaran terhadap kebijakan keamanan (security policy)
- Akses secara tidak sah terhadap sistem atau informasi
- Suatu peristiwa yang menghalangi/ mengganggu akses yang sah terhadap sistem atau informasi



# Mengapa perlu incident drill?

- drill memperbaiki incident response planning
- drill memperbaiki disaster recovery planning
- drill memperbaiki business continuity planning
- semua organisasi harus melakukan, hampir semua organisasi komersial sudah melakukan
- Beberapa industri tertentu, merupakan kewajiban



# Gov-CSIRT Indonesia



- Government – Computer Security Incident Response Team (CSIRT) Indonesia, disingkat Gov-CSIRT Indonesia merupakan CSIRT sektor Pemerintah Indonesia yang ditetapkan oleh Kepala Badan Siber dan Sandi Negara dalam Keputusan Kepala Badan Siber dan Sandi Negara Nomor 570 Tahun 2018 tanggal 20 Desember 2018.
- Bertanggungjawab sebagai ketua Gov-CSIRT Indonesia adalah Direktur Penanggulangan dan Pemulihan Pemerintah pada Deputy Bidang Penanggulangan dan Pemulihan BSSN.
- Anggota Tim dari Gov-CSIRT Indonesia adalah seluruh staf BSSN pada sektor pemerintah dan anggota CSIRT Instansi Pemerintah.



- membangun, mengoordinasikan, mengolaborasikan dan mengoperasionalkan sistem mitigasi, manajemen krisis, penanggulangan dan pemulihan terhadap insiden keamanan siber pada sektor pemerintah;
- membangun kerja sama dalam rangka penanggulangan dan pemulihan insiden keamanan siber pada sektor pemerintah;
- membangun kapasitas sumber daya penanggulangan dan pemulihan insiden keamanan siber pada sektor pemerintah;
- mendorong pembentukan CSIRT (Computer Security Incident Response Team) pada sektor pemerintah.



- Konstituen dari Gov-CSIRT Indonesia meliputi seluruh Pemerintah Daerah dan Pemerintah Pusat.
- Gov-CSIRT Indonesia memberikan layanan yang meliputi respon insiden dalam bentuk:
  - triase insiden;
  - koordinasi insiden; dan
  - resolusi insiden.
- Disertai dengan aktivitas proaktif dalam bentuk:
  - cyber security drill test;
  - workshop atau bimbingan teknis; dan
  - asistensi pembentukan CSIRT sektor pemerintah.



- Panduan Pelaporan Insiden
- Panduan Penanganan Insiden Web Defacement
- Panduan Penanganan Insiden Serangan DDoS
- Panduan Penanganan Insiden Serangan Phishing
- Panduan Penanganan Insiden Serangan SQL Injection
- Panduan Penanganan Insiden Malware



**BADAN SIBER  
DAN SANDI NEGARA**

# Tampilan Website Gov-CSIRT Indonesia

Berita Gov-CSIRT Indonesia



Berita Gov-CSIRT Indonesia

BSSN Susun Kebijakan Tata Kelola Penanggulangan dan Pemulihan Insiden Keamanan Siber Nasional



Berita Gov-CSIRT Indonesia

BSSN Lakukan Drill Test Penanggulangan Insiden Web Defacement Sektor Pemerintah



Berita Gov-CSIRT Indonesia

Forum Group Discussion Proteksi, Penanggulangan dan Pemulihan Insiden Siber Sektor Pemerintah

# 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 (021) 78833610  
Laporkan & Kirimkan bukti ke  
[bantuan70@bssn.go.id](mailto:bantuan70@bssn.go.id) atau  
[pusopskamsinas@bssn.go.id](mailto:pusopskamsinas@bssn.go.id)

## PUSAT KONTAK SIBER

Pusat Operasi Keamanan Siber Nasional **BSSN**



**BADAN SIBER  
DAN SANDI NEGARA**

**TERIMA KASIH**

---