BADAN SIBER DAN SANDI NEGARA

Bocor Tanpa Sadar

Bagaimana Hacker Mencuri Data Digital

Sashimi #1 Kota Magelang

10 Agustus 2026 | Magelang

Reikal Taupaani, S.Tr.TP, M.T
Sandiman Muda - Direktorat KSS Pemerintah Daerah

BADAN SIBER DAN SANDI NEGARA

Pernahkah Anda "disapa" oleh Hacker?

SETNEG RI <setneg.ri@register-now.co>
To REIKAL TAUPAANI
Reply To setneg <setneg@register-now.co>

This message contains external images. Click to load
Always display images from register-now.co or setneg.ri@register-now.co

Selamat Pagi Bapak/Ibu REIKAL TAUPAANI,

Ayo...! Jangan Lewatkan

Pendaftaran Awal Undangan

Upacara Peringatan Detik-Detik Proklamasi dan
Upacara Penurunan Bendera Sang Merah Putih

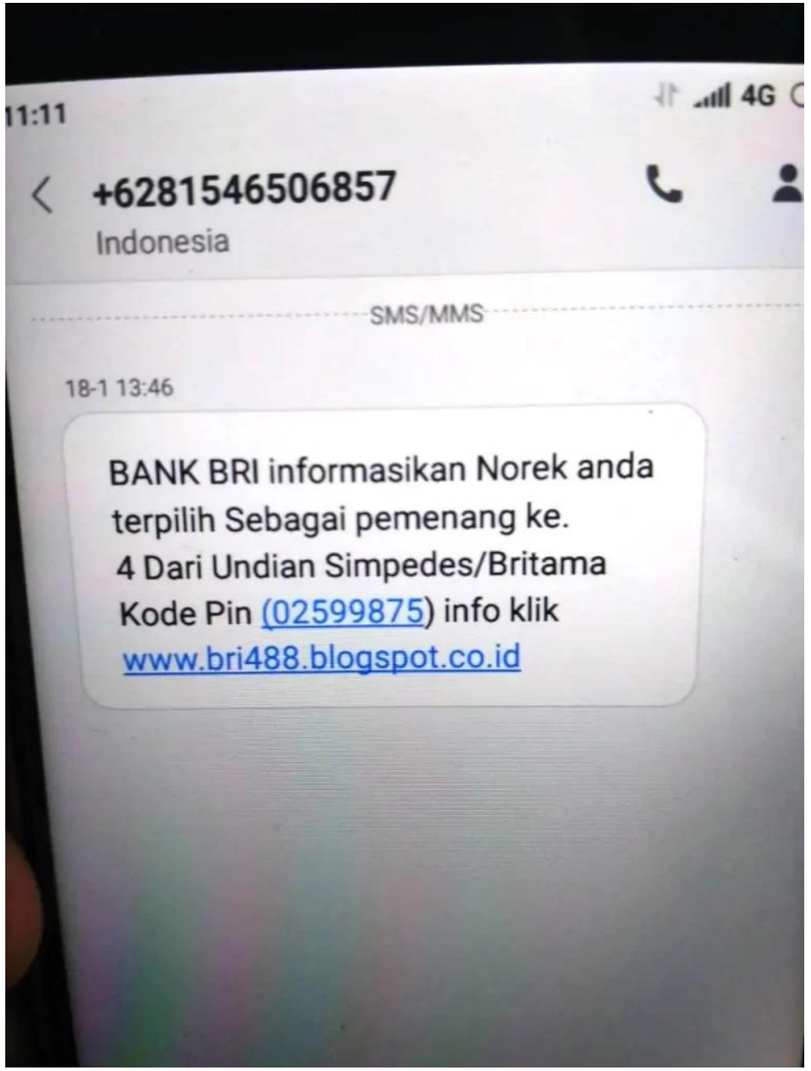
☐ Senin, 17 Agustus 2026

☐ Istana Merdeka, Jakarta

Siapkan diri Anda,

Daftar Melalui:

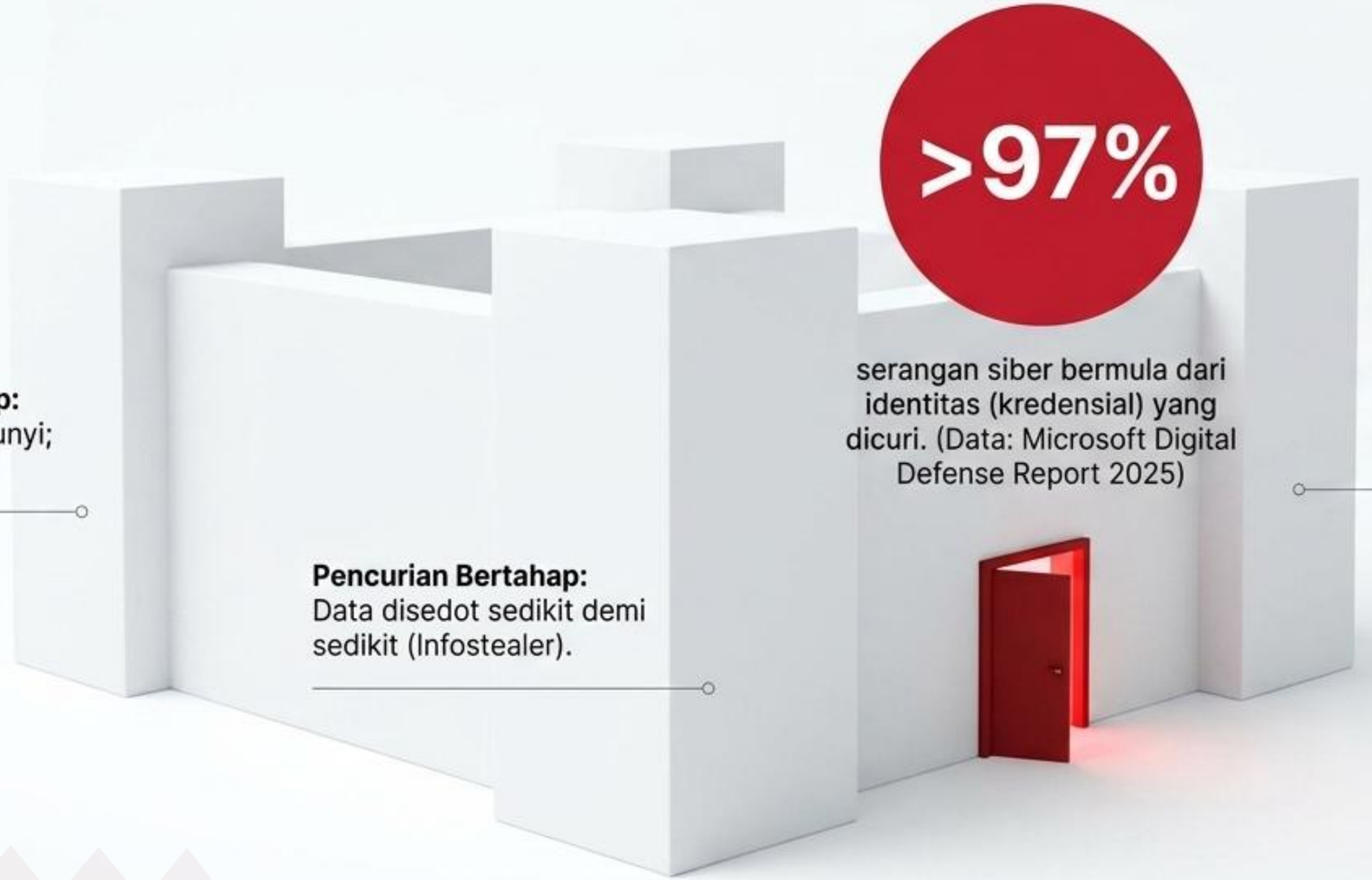
https://pandang.istanapresiden.go.id



Mengapa Kebocoran Terjadi Tanpa Disadari?

Bekerja dalam Senyap: Tidak ada alarm berbunyi; sistem terasa normal.

Pencurian Bertahap: Data disedot sedikit demi sedikit (Infostealer).



serangan siber bermula dari identitas (kredensial) yang dicuri. (Data: Microsoft Digital Defense Report 2025)

Bukan Merusak, Tapi Menyamar: Hacker menggunakan kunci Anda sendiri.

Mitos vs Realita Serangan Siber

MITOS

Hacker membobol sistem pertahanan komputer (Firewall) dengan paksa.

Membutuhkan keahlian teknis tingkat tinggi.

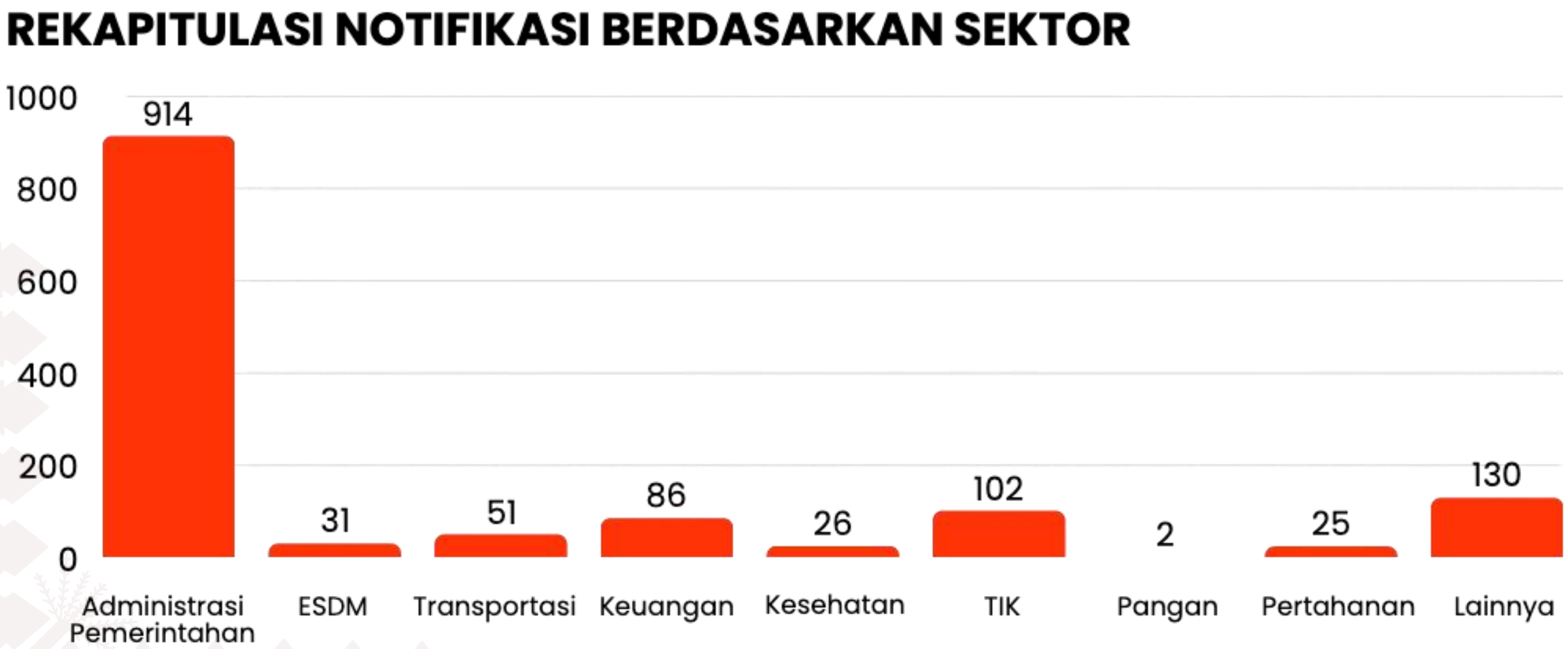
REALITA

Hacker memanipulasi manusia (Social Engineering).

Mereka membujuk Anda untuk menyerahkan kunci aksesnya.

“Penyerang tidak lagi mendobrak masuk; mereka sekadar *login*.”

Aset Digital Pemerintah menjadi "Lahan" Hacker

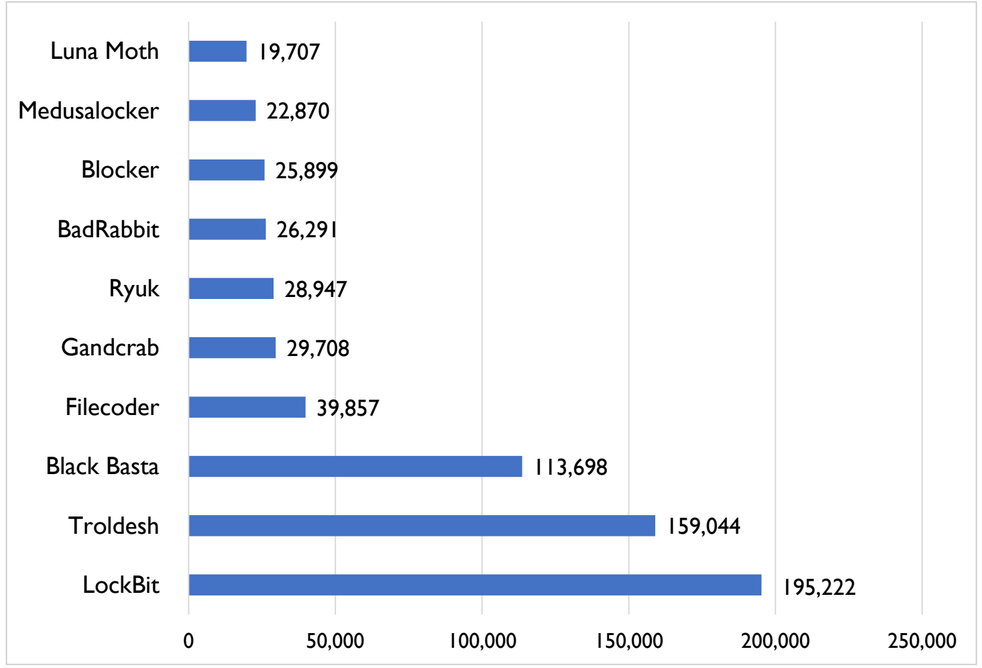


Banyaknya serangan yang terjadi "dibalik layar"

> Periode 1 Januari – 16 Mei 2026

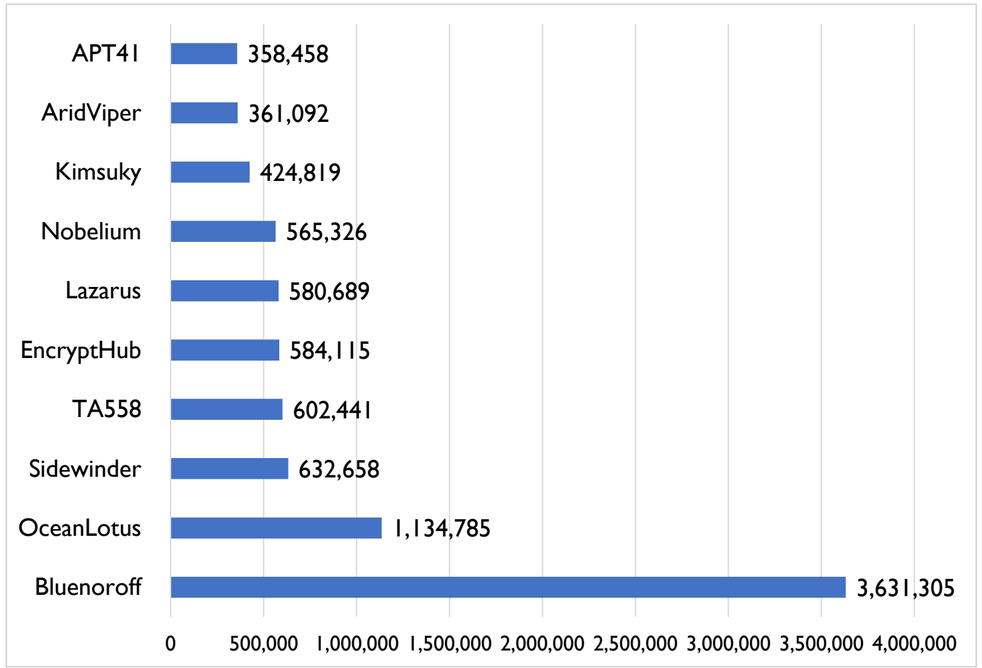
Ransomware

1.159.993
Anomali Trafik Berjenis Ransomware



Advanced Persistent Threat

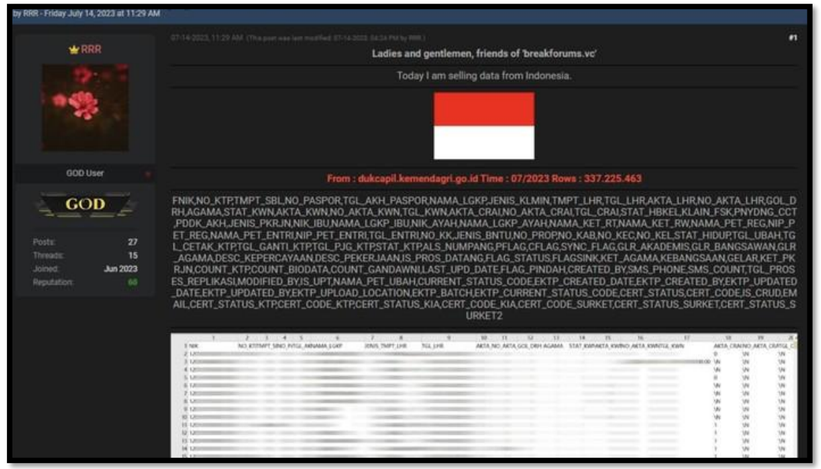
13.701.689
Anomali Trafik Berjenis APT



Maraknya Isu Kebocoran Data dan Keamanan Siber – Data Pribadi Bocor

Dampak: potensi penyalahgunaan untuk pinjaman online ilegal, penipuan, dsb.

Kasus ini menekankan pentingnya UU Perlindungan Data Pribadi (UU 27/2022).



Studi Kasus: Satu Klik Menuju Bencana

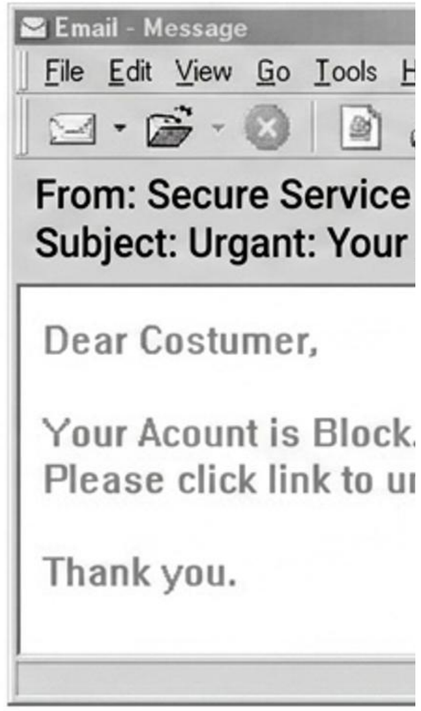
1. Pancingan Emosi: Terima pesan mendesak (contoh: "Paket gagal dikirim, cek resi di sini").

2. Penyerahan Akses: Klik tautan & login ke situs web palsu. (Kredensial dicuri tanpa sadar).

3. Penguasaan Sistem: Akun dikuasai secara senyap, data pribadi/perusahaan disedot.

AI Mengubah Permainan Manipulasi

2020 P



Tata bahasa buruk & t

Mudah dideteksi denga

Permohonan Penilaian IKASSANSI

BNPB <bnpb@uscis-gov.site>
To REIKAL TAUPAANI
Reply To bnpb <bnpb@uscis-gov.site>

08/03/2026, 2:14 PM

BADAN NASIONAL PENANGANAN BENCANA
REPUBLIK INDONESIA
Gedung Graha BNPB, Jalan Pramuka Kav. 38, Jakarta Timur 13120

Yth. Bapak/Ibu Pegawai,

Dalam rangka meningkatkan tingkat kematangan tata kelola keamanan siber dan persandian serta mendukung terwujudnya penyelenggaraan Pemerintah Digital yang aman, andal, dan berkesinambungan di lingkungan Badan Nasional Penanganan Bencana (BNPB), bersama ini kami mengajukan permohonan agar BNPB dapat mengikuti **Penilaian IKASSANDI Tahun 2026**.

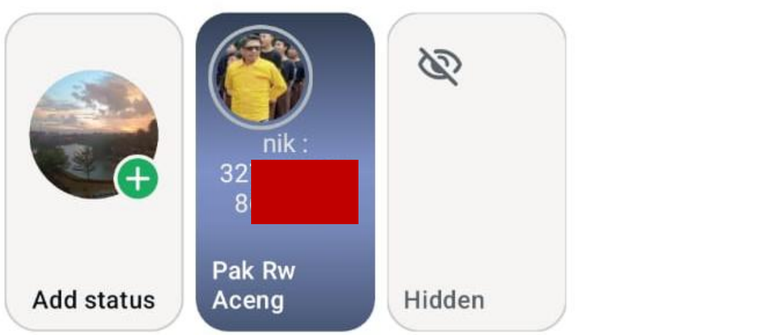
Melalui pelaksanaan penilaian tersebut, kami berharap memperoleh evaluasi yang komprehensif terhadap implementasi tata kelola keamanan siber dan persandian, sekaligus mendapatkan rekomendasi perbaikan sebagai dasar peningkatan kapasitas organisasi dalam melindungi aset informasi, sistem elektronik, dan layanan digital yang mendukung pelaksanaan tugas dan fungsi BNPB.

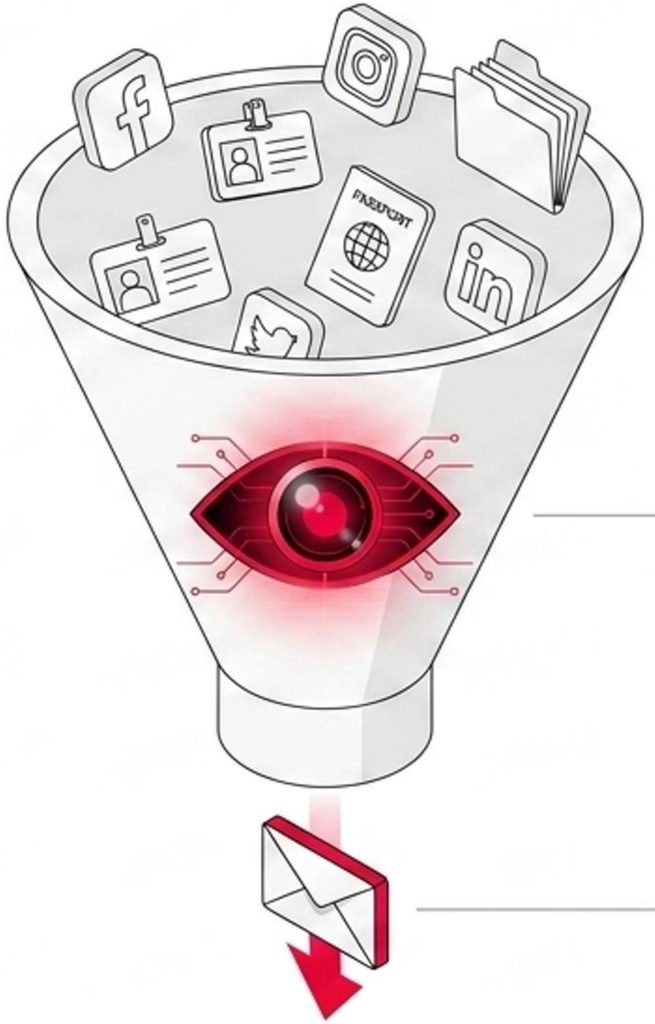
Sebagai bentuk kesiapan pelaksanaan penilaian, BNPB berkomitmen untuk:

Phishing

- **Tata Bahasa Sempurna**: AI merancang teks Bahasa Indonesia yang sangat natural dan kontekstual.
- **Voice Cloning**: Meniru suara atasan Anda melalui telepon dalam hitungan detik.
- **Deepfake Executive**: Video call palsu yang hampir tidak dapat dibedakan dari aslinya.

Jejak Digital Anda Adalah Senjata Mereka (OSINT)



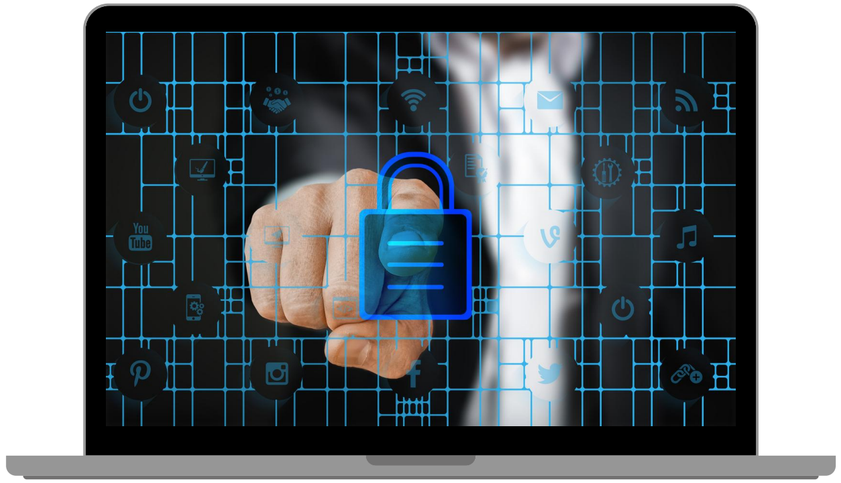


Input: Unggahan liburan, update proyek kantor, struktur organisasi.

Proses: AI memindai dan merangkai data profil Anda dalam hitungan detik.

Output: Serangan Spear-Phishing yang terasa sangat personal, akrab, dan relevan.

“Mereka tahu rutinitas Anda sebelum mereka menyapa Anda.”



Bagaimana Langkah Konkrit Meningkatkan Keamanan Informasi?

Langkah Konkrit #1 – Inventarisasi Aset dan Analisis Risiko

1. Kenapa Penting?

- **Aset yang tidak terinventarisasi tidak dapat dikelola, dilindungi, maupun dipulihkan saat terjadi insiden**. (Case Defacement BSSN)
- Hampir seluruh kerangka kerja keamanan siber diawali dengan identifikasi aset dan risiko. Cybersecurity Framework, Zero Trust Architecture Implementation etc.
- Identifikasi Aset → Analisis Risiko → Penentuan Prioritas → Pengamanan

2. Yang Perlu Dilakukan

✅ Menyusun tata kelola (kebijakan, SOP, dan penanggung jawab) **Manajemen Risiko**

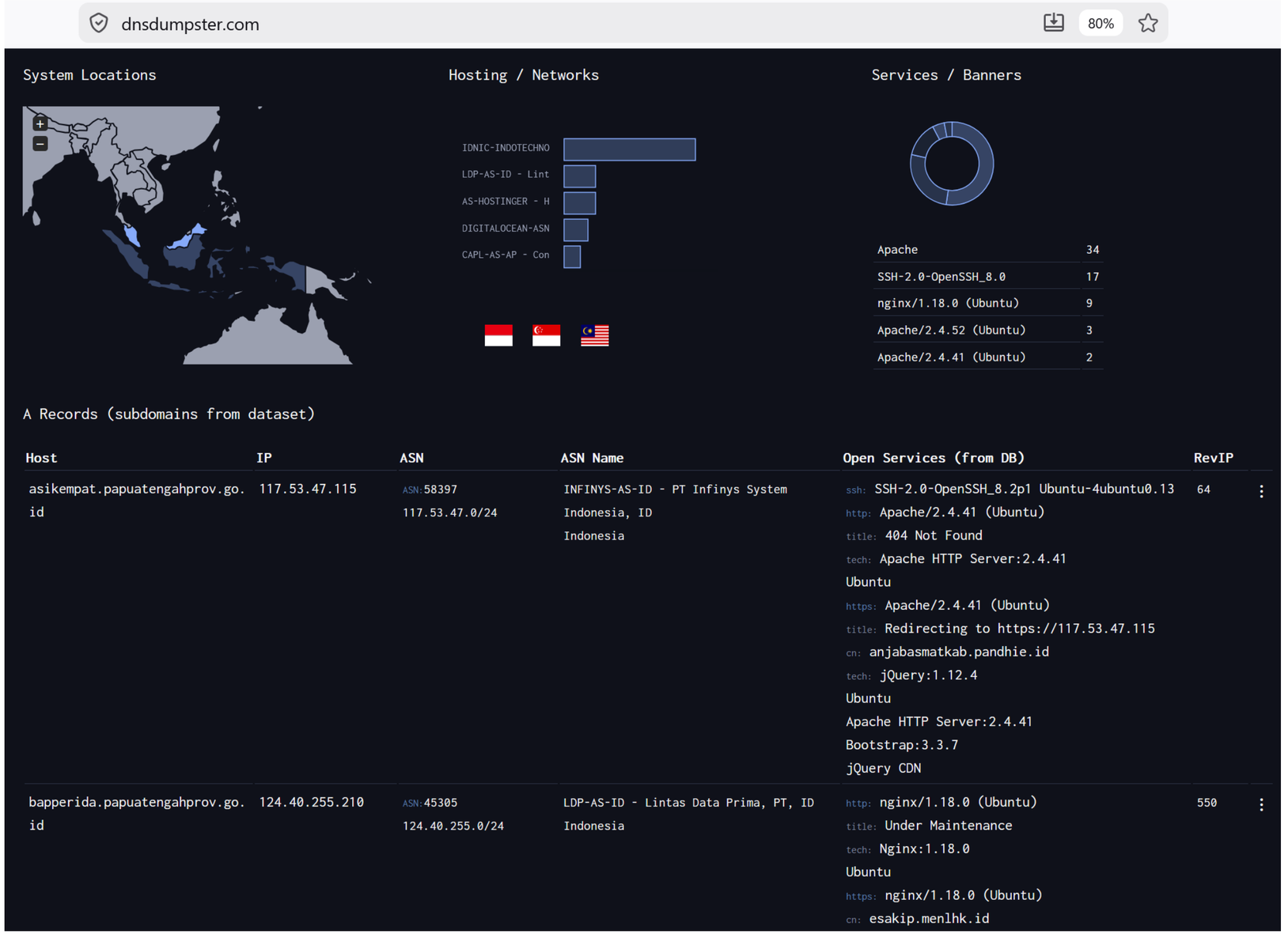
✅ Membangun **register aset** sebagai living document yang selalu diperbarui

✅ Melakukan **analisis risiko** terhadap aset yang telah teridentifikasi

Langkah Konkrit #1 – Inventarisasi Aset dan Analisis Risiko

Tools sederhana untuk identifikasi asset aplikasi yang terekspos ke internet: DNSDumpster

https://dnsdumpster.com



Langkah Konkrit #1 – Inventarisasi Aset dan Analisis Risiko

Langkah Teknis juga didasari dengan NSPK untuk memperoleh nilai optimal

>>Sumber: https://kominfo.paserkab.go.id

URAIAN PROSEDUR

NO	URAIAN KEGIATAN	PELAKSANAAN		MUTU BAKU		
		Kabid TKI	Tim Monitoring	Kelengkapan	Waktu	Output
1.	Menugaskan Tim Pengelola untuk melaksanakan monitoring jaringan intra di lingkungan Pemerintah Kabupaten Paser.			Perintah Lisan / Tertulis	10 Menit	Perintah / Tugas
2.	Melaksanakan monitoring jaringan intra dan melaporkan kepada Kepala Bidang Teknologi Komunikasi dan Informatika (TKI)			Komputer (PC/Laptop), Printer, Internet	180 Menit	Laporan Hasil Monitoring
3.	Menerima laporan dari Tim Pengelola dan menyetujui		Ya / Tidak	Hasil Laporan	15 Menit	Disposisi
4.	Telah melaksanakan monitoring jaringan intra			Persetujuan Hasil Laporan	15 Menit	Arsip

BADAN SIBER DAN SANDI NEGARA

Langkah Konkrit #2 – Susun, terapkan dan evaluasi Kebijakan SMKI

1. Kenapa Penting?

- Teknologi keamanan yang baik tidak akan efektif tanpa aturan dan tata kelola yang jelas.
- Kebijakan SMKI menjadi dasar bagi organisasi untuk menentukan:
  - Apa yang harus dilindungi.
  - Siapa yang bertanggung jawab.
  - **Bagaimana pengamanan diterapkan.**
  - **Bagaimana keberhasilannya diukur.**

2. Yang Perlu Dilakukan

✅ Menyusun kebijakan dan prosedur keamanan informasi
✅ Menetapkan peran dan tanggung jawab
✅ Menerapkan kebijakan secara konsisten
✅ Melakukan evaluasi dan perbaikan secara berkala

3. Contoh Penerapannya

Mekanisme Backup Data
Mekanisme Penggunaan Password
Mekanisme Multi-Factor Authentication (MFA)
Mekanisme Penanganan Insiden Siber

Langkah Konkrit #2 – Susun, terapkan dan evaluasi Kebijakan SMKI

1. Kenapa Backup Penting?

- 60% organisasi yang terkena ransomware gagal pulih karena tidak punya backup yang benar (Sophos 2023).
- **Banyak OPD daerah masih simpan data hanya di 1 server/1 PC, rawan hilang karena serangan atau kerusakan hardware**
- Kasus nyata dan sering: beberapa OPD di Indonesia harus mematikan layanan dan kembali ke sistem manual karena ransomware → backup tidak tersedia/teruji

Susun SOP Backup dan implementasikan

2. Prinsip Backup yang Benar (3-2-1 Rule)

- 3 salinan data: 1 data asli + 2 backup.
- 2 media **BERBEDA**: misalnya harddisk eksternal & cloud.
- 1 salinan offsite/offline: misalnya disimpan di lokasi berbeda atau media tidak selalu terhubung internet (air-gap).

3. Jenis Backup (disesuaikan)

- Full backup: semua data disalin.
- Incremental/Differential backup: hanya perubahan terbaru.
- Cloud backup: lebih fleksibel, tapi harus hati-hati soal regulasi (jangan taruh data rahasia negara di cloud publik luar negeri).

Langkah Konkrit #2 – Susun, terapkan dan evaluasi Kebijakan SMKI

SOP dilengkapi dengan form/laporan sebagai bukti pelaksanaan

>>Sumber: https://kominfo.paserkab.go.id

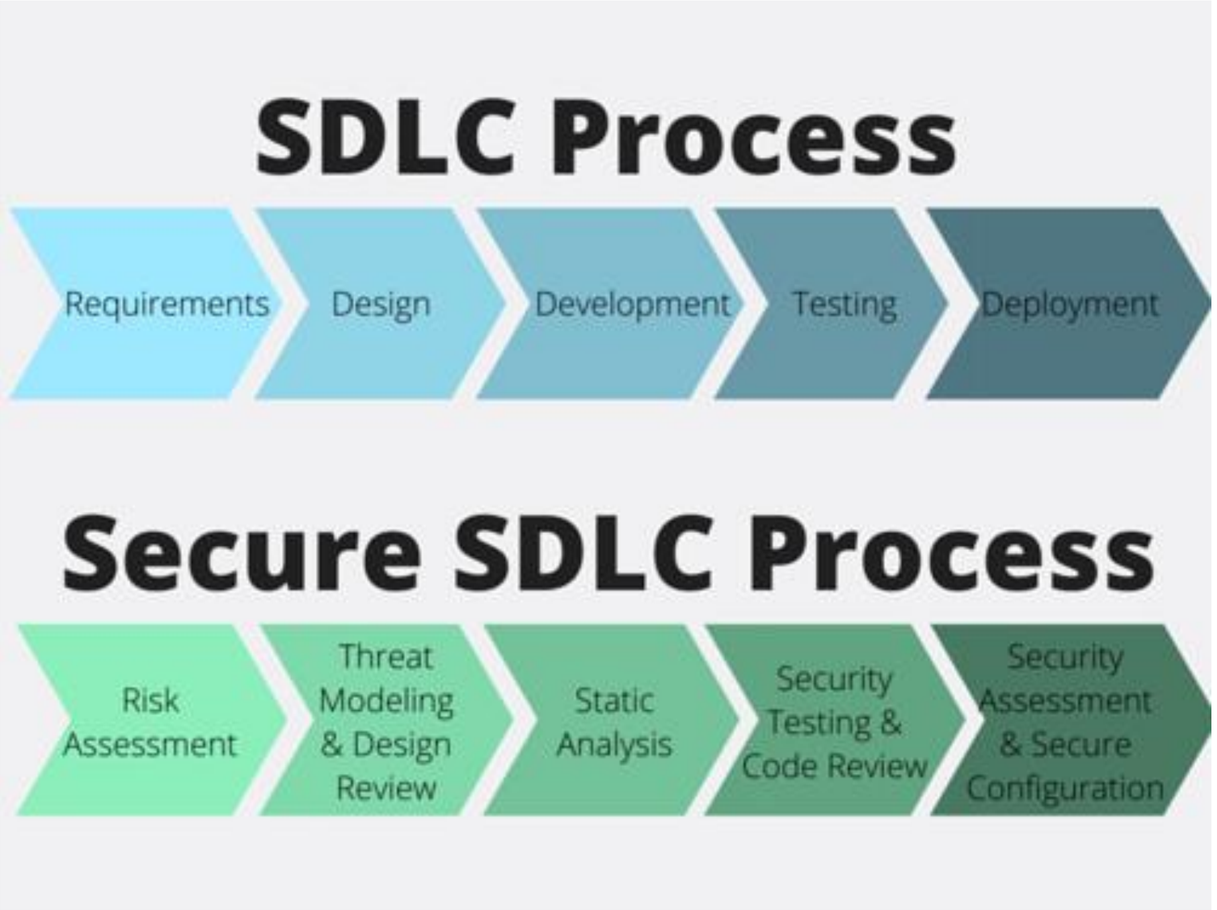
No. Dokumen :
Revisi :

SOP BACK UP DAN RESTORE

NO	URAIAN KEGIATAN	PELAKSANA		Mutu Baku			Keterangan
		Pengelola Pusat Data	Admin	Perlengkapan	Waktu	Output	
1	Melakukan Backup Sesuai dengan jadwal	Mulai		- Komputer kerja			
2	Memastikan proses backup berhasil dilakukan						
3	Memberi nama file sesuai dengan ketentuan			- Formuiis pencatatan backup			
4	Mengamankan hasil backup						
5	Mengisi form pelaksanaan backup			- Formulir pencatatan backup	30 menit		

Langkah Konkrit #2 – Susun, terapkan dan evaluasi Kebijakan SMKI

Terapkan Secure SDLC dan Software Requirements Specification (SRS) sesuai PBSSN No 4 2021



Langkah Konkrit #2 – Susun, terapkan dan evaluasi Kebijakan SMKI

Terapkan Secure SDLC dan Software Requirements Specification (SRS)

>>Sumber:
https://dpmptsp.bantulkab.go.id
https://kominfo.slemankab.go.id

Gambar 8 Konsep Arsitektur Entitas Web Service

E. Aspek Keamanan

Untuk menjamin keamanan aplikasi, data dan informasi dilakukan beberapa metoda pengamanan dengan menggunakan perangkat keras dan perangkat lunak, yaitu sebagai berikut.

- Untuk memenuhi aspek *Authentication*, setiap pengguna memiliki identitas *(user id)* dan kata kunci *(password)* tertentu yang *unique* dengan otoritas yang berbeda-beda secara bertingkat sesuai dengan tugas dan tanggung jawabnya. *User* id dan password tersebut harus dimasukan setiap kali mulai menjalankan aplikasi. Jika terjadi kesalahan penulisan password dalam jumlah/batas tertentu, misalkan 3 (tiga) kali salah menuliskan pasword, maka akses dari userid pengguna yang bersangkutan akan diblokir (*locked-out*) sementara untuk kurun waktu tertentu, misalnya 15 (lima belas) menit. Setelah waktu *locked-out* terlewati, pengguna baru dapat mencoba untuk mengakses sistem.
- Untuk memenuhi aspek *Access Control*, setiap pemakai[illegible]s akses terhadap aplikasi, data & informasi sesuai dengan kewenangannya.
- Untuk memenuhi aspek *Confidentiality*, proses pertukaran data antar fungsi dan elemen, dilakukan secara tersandi *(encrypt/decrypt)* sehingga data akan tidak terbaca jika data tersebut disadap ditengah jalan oleh orang yang tidak berkepentingan. Data password pun akan akan disimpan di database dalam kondisi terenkripsi.
- Untuk memenuhi aspek *Non Repudiation*, setiap perubahan data akan dilakukan pencatatan *user* id, tanggal dan waktu perubahan data tersebut secara otomatis oleh aplikasi. Hasil pencatatan ini hanya dapat dilihat oleh pihak manajemen sehingga jika

BAGAN ALUR PENGEMBANGAN APLIKASI

No.	Uraian Prosedur	Pelaksana						Mutu Baku			Keterangan
		System Analyst	Web-Mobile Programmer	Kepala Seksi Aplikasi dan Integrasi Sistem Informasi	Staff seksi aplikasi dan Integrasi Sistem Informasi	Instansi Pemilik Sistem	Bidang Layanan e-Gov dan Persandian	Kelengkapan	Waktu	Output	
	Identifikasi kebutuhan Aplikasi Baru							Dokumen Identifikasi kebutuhan	120 menit	Dokumen Identifikasi kebutuhan	
	Pembuatan spesifikasi kebutuhan							Dokumen Spesifikasi kebutuhan	120 menit	Dokumen Spesifikasi kebutuhan	
	Pertemuan review spesifikasi kebutuhan							Dokumen Permintaan Modifikasi kebutuhan	120 menit	Dokumen Permintaan Modifikasi kebutuhan	
	Penunjukan System Programmer.							Surat Perintah Tugas	45 menit	Surat Perintah Tugas	
	Pembuatan rencana implementasi dan jadwal pelaksanaan, dan kebutuhan usulan programmer							Dokumen rencana implementasi dan jadwal, dan usulan kebutuhan programmer	2 hari	Dokumen rencana implementasi dan jadwal, dan usulan kebutuhan programmer	
	Penunjukan Programmer							Surat Perintah Tugas	45 menit	Surat Perintah Tugas	
	Pembuatan Data Flow Diagram, Entity Relation Diagram							Dokumen DFD, ERD	3 hari	Dokumen DFD, ERD	
	Pembuatan Dokumen Awal User Acceptance Test							Dokumen Awal User Acceptance Test	3 hari	Dokumen Awal User Acceptance Test	
	Pembuatan Prototype System.							Prototype System	90 hari	Prototype System	

+ Uji Penetrasi sebelum Publish

BADAN SIBER DAN SANDI NEGARA

Langkah Konkrit #2 – Susun, terapkan dan evaluasi Kebijakan SMKI

Fakta Penting

- 80% insiden data breach terjadi karena password lemah atau dicuri (Verizon DBIR 2023).
- **Password populer di Indonesia masih “123456”, “password”, “bismillah” atau tanggal lahir.**
- Serangan credential stuffing dan brute force adalah ancaman umum ke akun OPD.

Prinsip Password Kuat

- Panjang ≥ 8 karakter.
- Kombinasi huruf besar, kecil, angka, simbol.
- Jangan pakai data pribadi (NIK, tanggal lahir, nama anak).
- Gunakan passphrase: contoh → “SatePadang!2024Enak”.
- **Simpan di password manager jika memungkinkan.**

Aturan Tambahan (Best Practice BSSN & NIST SP 800-63B)

- **Ganti password hanya jika ada indikasi kompromi (bukan sekadar 3 bulan sekali).**
- Gunakan Multi-Factor Authentication (MFA).
- Jangan pakai password yang sama di banyak aplikasi.

Persyaratan Keamanan pada seluruh Aplikasi

Langkah Konkrit #2 – Susun, terapkan dan evaluasi Kebijakan SMKI

01

Apa itu Multi-Factor Authentication (MFA)?

- MFA = kombinasi 2 atau lebih faktor autentikasi:

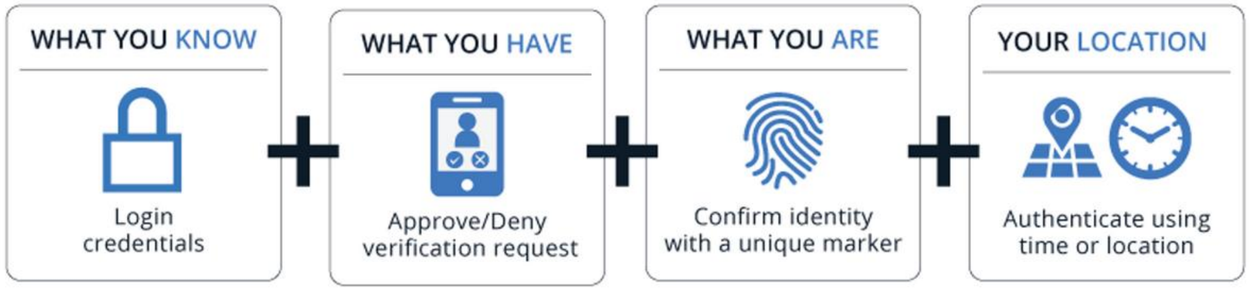
1. Sesuatu yang kita tahu → password/PIN.
2. **Sesuatu yang kita punya → HP/OTP/token.**
3. Sesuatu yang kita adalah → biometrik (sidik jari, wajah).

- Contoh: login email dengan password + kode OTP SMS/Google Authenticator.

02

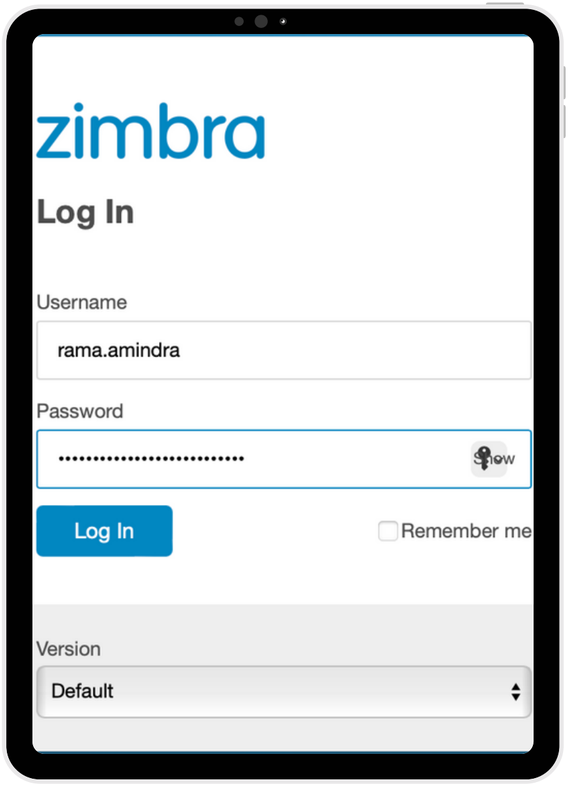
Kenapa Penting?

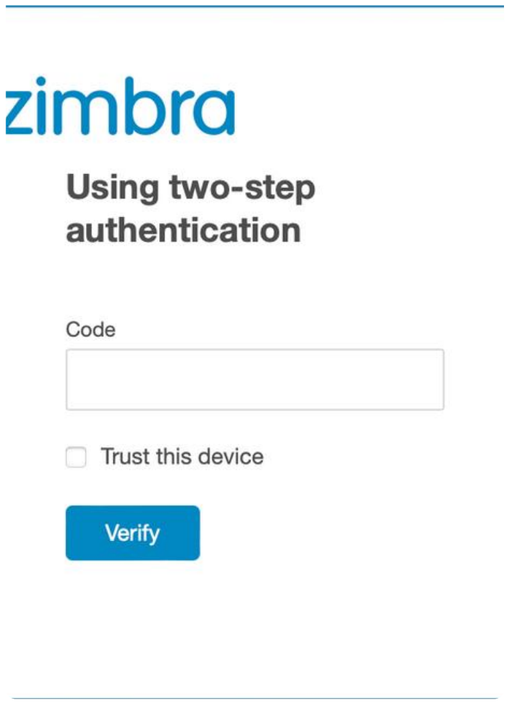
- Password bisa dicuri lewat phishing, malware, keylogger, data breach.
- **MFA memutus rantai: walaupun password bocor, hacker tetap tidak bisa login tanpa faktor kedua.**
- BSSN (2023): banyak **serangan ke akun admin OPD berhasil karena tidak ada MFA aktif.**
- NIST SP 800-63B juga merekomendasikan MFA sebagai standar autentikasi modern.

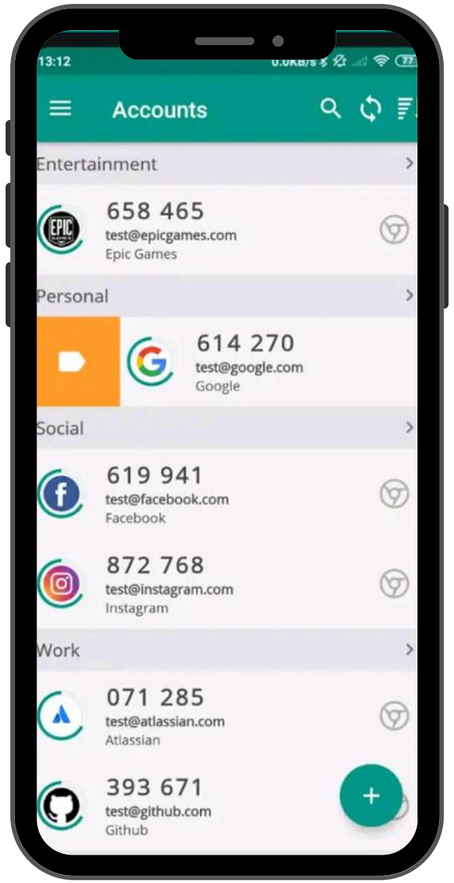


MFA sebagai salah satu kontrol teknis tanpa "biaya"

Langkah Konkrit #2 – Susun, terapkan dan evaluasi Kebijakan SMKI

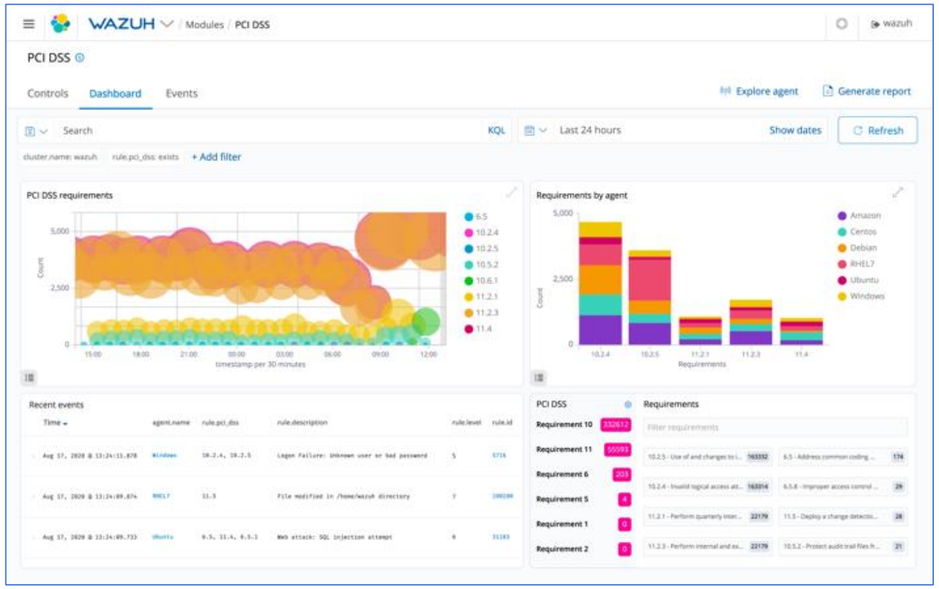




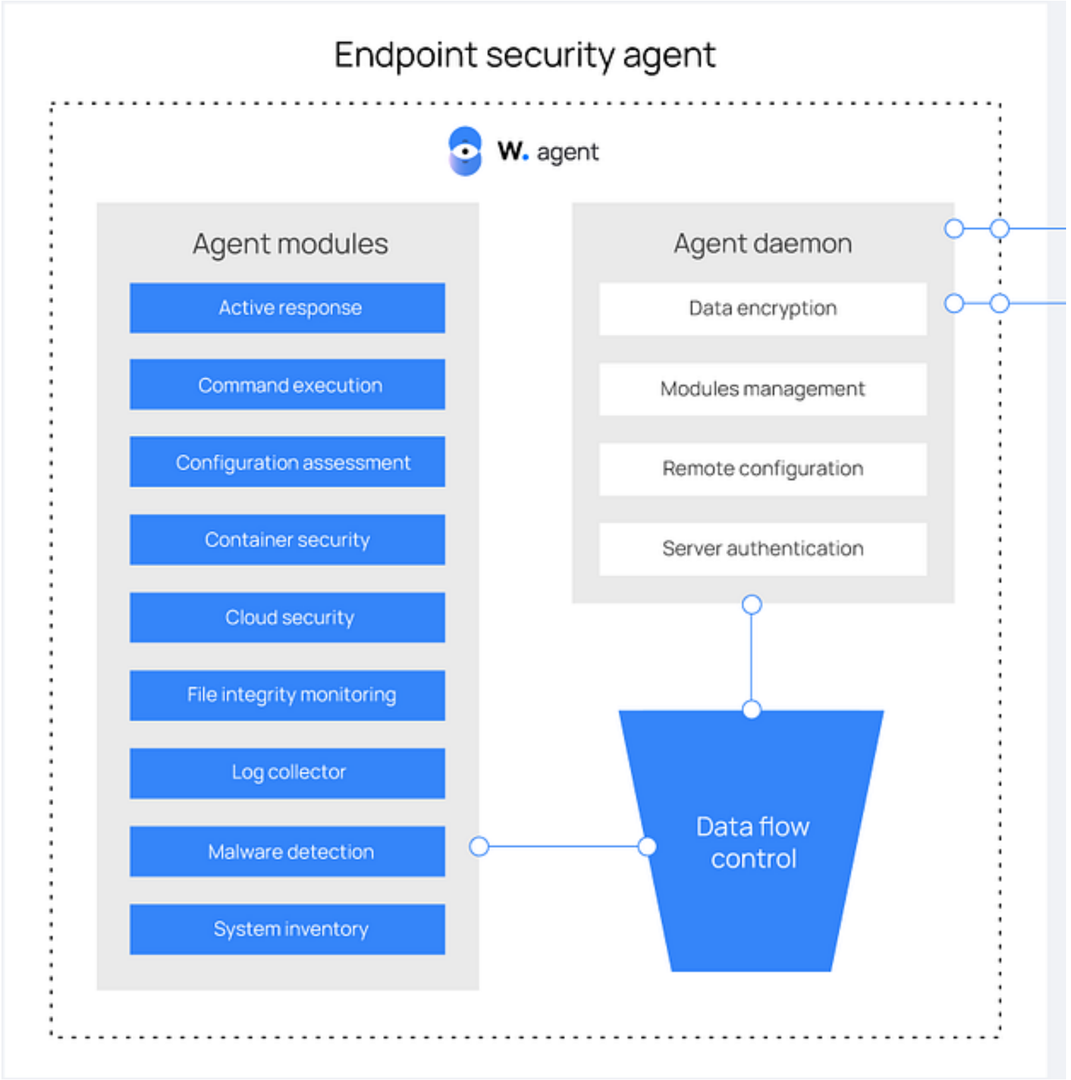


MFA sebagai salah satu kontrol teknis tanpa "biaya"

Langkah Konkrit #2 – Susun, terapkan dan evaluasi Kebijakan SMKI



Optimalkan perangkat keamanan TTIS untuk laporan monitoring



BADAN SIBER DAN SANDI NEGARA

Langkah Konkrit #3 – Budayakan Cyber Hygiene untuk setiap pegawai daerah

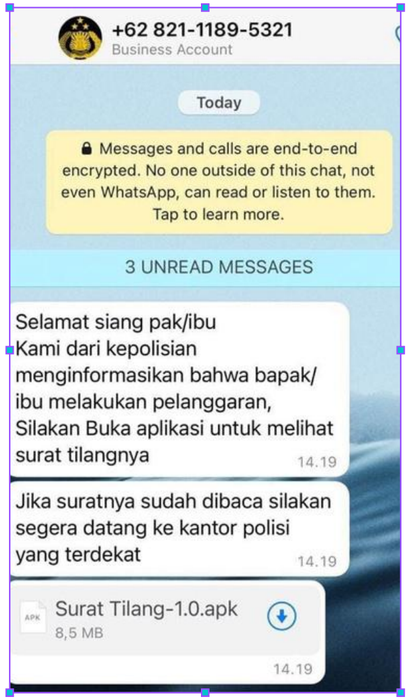
1. Kenapa Cyber Hygiene Penting?

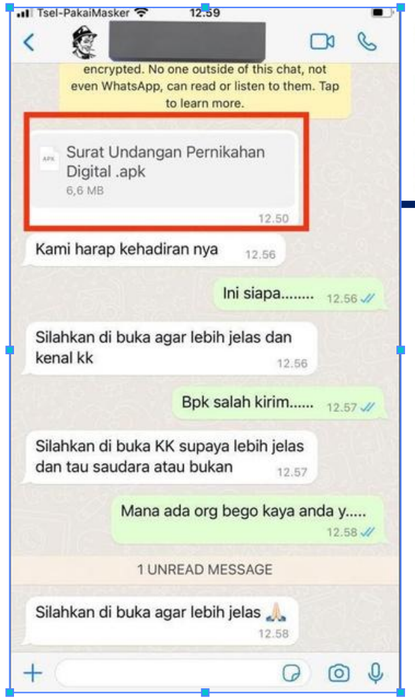
- 95% insiden keamanan berasal dari human error (IBM Cyber Security Report 2022).
- **Kasus phishing dan social engineering di pemerintah daerah meningkat (laporan BSSN 2024).**
- Contoh nyata: banyak akun email ASN dibobol karena klik tautan berbahaya.

2. Komponen Cyber Hygiene

- **Sadar phishing: jangan asal klik link/attachment. Sediakan Phising Campaign.**
- Selenggarakan Sosialisasi Sadar Keamanan untuk pegawai.
- Selalu update aplikasi & antivirus di perangkat kerja.
- Say no to crack

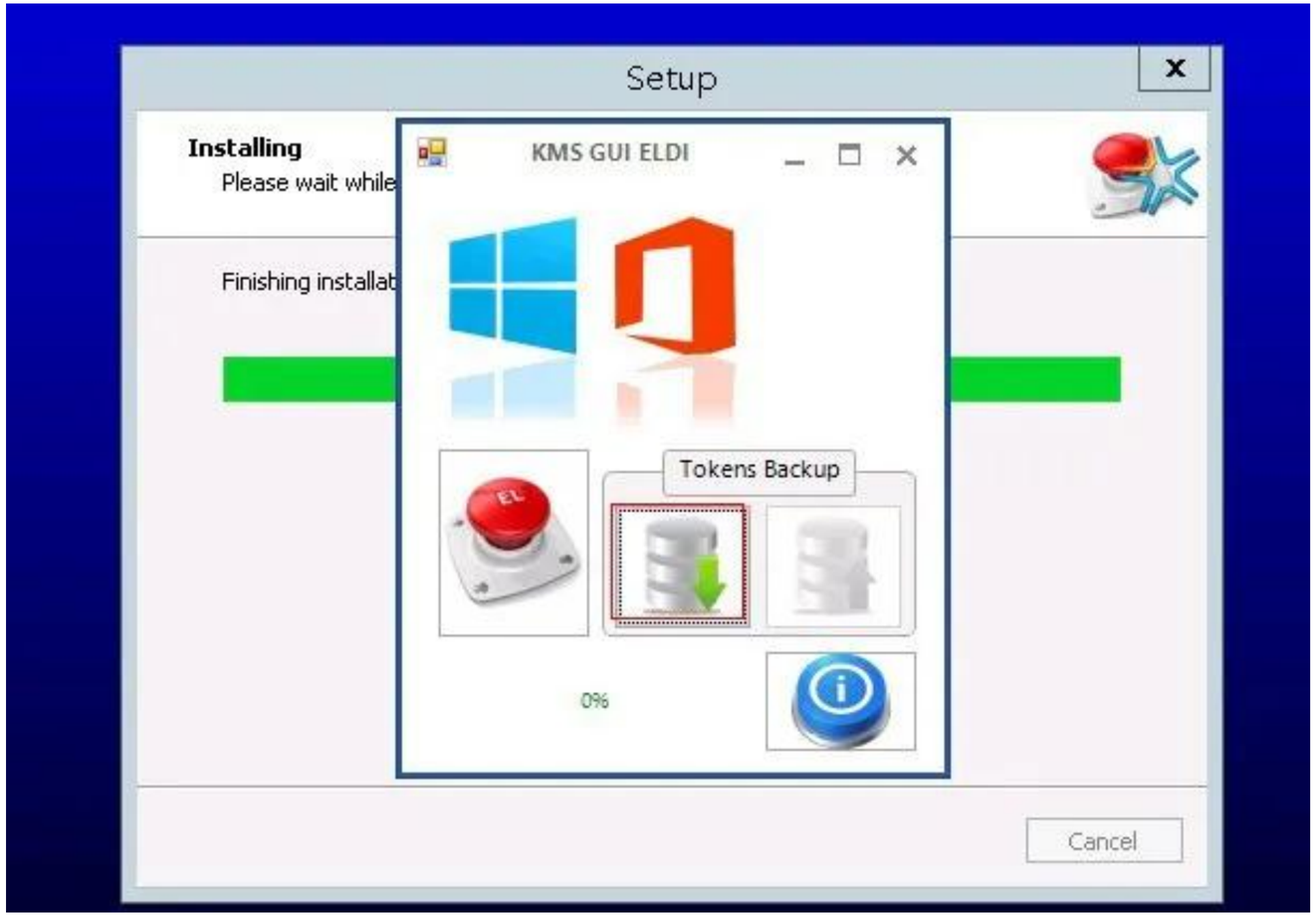
Langkah Konkrit #3 – Budayakan Cyber Hygiene untuk setiap pegawai daerah





Langkah Konkrit #3 – Budayakan Cyber Hygiene untuk setiap pegawai daerah

Menggunakan Crack/bajakan = Memberikan pintu masuk bagi hacker



PccrackBox WINDOWS MAC MULTIMEDIA DOWNLOADER SOFTWARE DMCA

Adobe Photoshop CC 22.4.3 Crack With Keygen [2021 Latest]

July 26, 2021 by zoro — 2 Comments

CRACK + ZIP FILE

Contents [hide]

1 Adobe Photoshop CC 2021 Crack + Keys Full Version For (Mac/Windows)
1.1 Download Adobe Photoshop CC 2021 Keygen + Torrent 100% Free Latest
1.2 Features of Adobe Photoshop CC Cracked
1.3 Adobe Photoshop CC Serial Key (2021)
1.4 Photoshop CC 2021 Latest Cracked Features
1.5 What's Better Than the Previous Release?
1.6 Adobe Photoshop CC 22.4.3.317 Serial Number July-2021
1.7 Procedure for Crack?

Adobe Photoshop CC 2021 Crack + Keys Full Version For (Mac/Windows)

Adobe Photoshop CC 2021 v22.4.3.317 Crack is the world's no#1 photo editing program for Windows and Mac users. This application is very popular in the world due to its outstanding efficiency. The

/* */

Search this website

RECENT POSTS

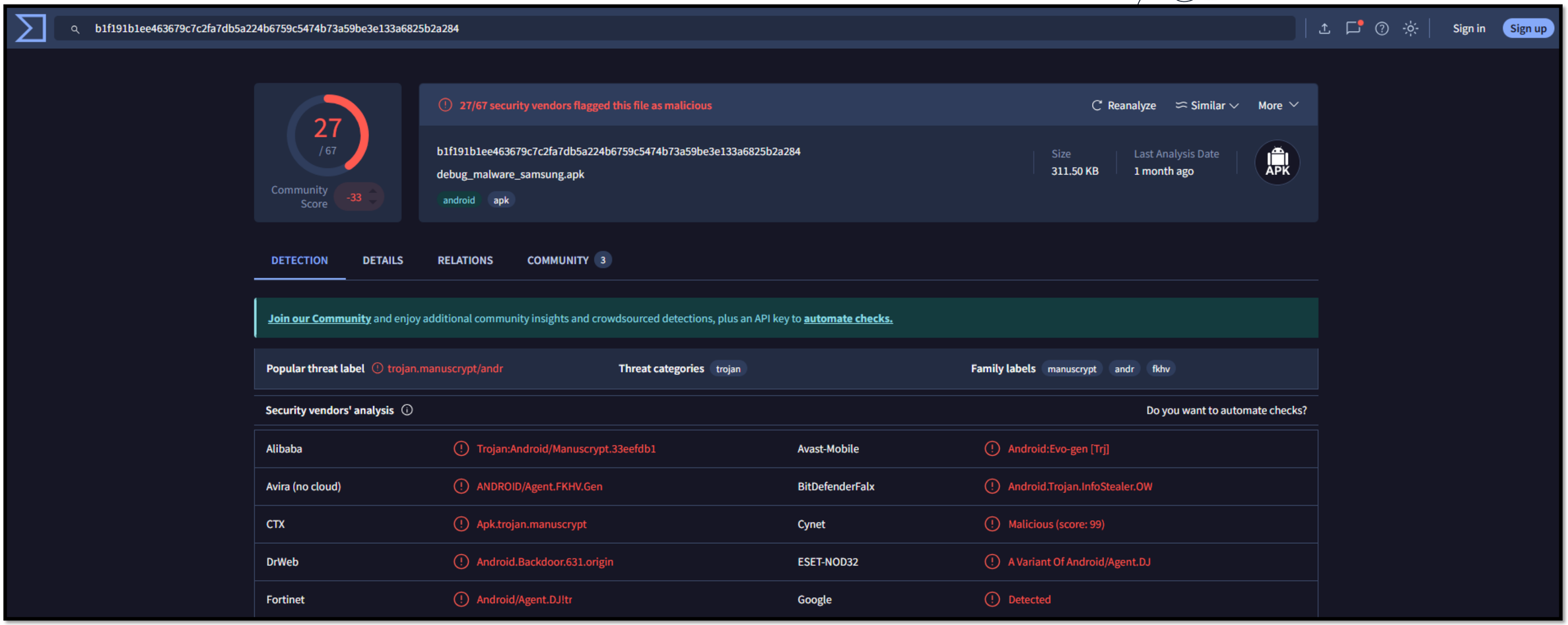
AnyDVD HD 8.5.6.0 Crack With Keygen (2021)
Express Burn 10.20 Crack + Registration Code (2021)
K7 Total Security 16.0.0521 Crack + Activation Key 2021
Emsisoft Anti-Malware 2021 Crack with License Key (Latest)
Logic Pro X 10.6.3 Crack With Torrent [Latest 2021]

BADAN SIBER DAN SANDI NEGARA

Langkah Konkrit #3 – Budayakan Cyber Hygiene untuk setiap pegawai daerah

Tools untuk memeriksa file apakah berbahaya atau berisi malware: VirusTotal

https://www.virustotal.com



BADAN SIBER DAN SANDI NEGARA

Langkah Konkrit #4 – Berkolaborasi dalam Menangani Insiden Siber

1

Deteksi di OPD

OPD menemukan indikasi insiden (website error, login janggal, data hilang, email phishing, alert aneh).

2

Pelaporan Cepat ke CSIRT Organisasi

OPD melaporkan lewat kanal resmi (email, hotline, form pelaporan, dsb).

3

Tindakan Awal OPD

- Jaga bukti (jangan hapus log/file).
- Isolasi perangkat terdampak bila memungkinkan.

4

Tindak Lanjut oleh CSIRT

- CSIRT menerima laporan → analisis → menentukan level eskalasi.
- Jika insiden besar, bisa diteruskan ke BSSN atau CSIRT sektoral terkait.

5

Komunikasi Balik ke OPD

- CSIRT memberikan update status & rekomendasi.
- OPD mendukung pemulihan layanan.

Langkah Konkrit #4 – Berkolaborasi dalam Menangani Insiden Siber

Peran CSIRT Organisasi (Contoh: CSIRT Kota Magelang)

Menjadi Pusat Koordinasi Insiden

- Menerima laporan insiden dari OPD
- Menentukan tingkat keparahan & prioritas

Melakukan Analisis Teknis

- Investigasi penyebab insiden
- Mengidentifikasi dampak & potensi penyebaran

Mengendalikan & Memulihkan Sistem

- Membantu containment (mencegah meluas)
- Mendukung eradikasi malware & recovery layanan

Memberikan Rekomendasi Pencegahan

- Menyusun lesson learned setelah insiden
- Memberi advis keamanan ke OPD (patch, awareness, SOP)

Menjadi Jembatan ke BSSN/CSIRT Lain

- Eskalasi insiden besar ke level nasional
- Berkolaborasi lintas sektor jika perlu

BADAN SIBER DAN SANDI NEGARA

Langkah Konkrit #4 – Berkolaborasi dalam Menangani Insiden Siber

Peran OPD

Menjadi Mata & Telinga Awal

- OPD adalah pihak pertama yang tahu ada gangguan di aplikasi/sistemnya.
- Peran: mendeteksi gejala insiden (website error, data hilang, login mencurigakan).

Melaporkan Segera ke CSIRT

- Jangan diam atau mencoba perbaiki sendiri tanpa koordinasi.
- Gunakan kanal resmi pelaporan CSIRT Organisasi.

Menjaga Bukti Insiden

- Jangan hapus log atau jejak insiden.
- Biarkan CSIRT melakukan analisis forensik.

Mendukung Respons & Pemulihan

- Menyediakan akses/sumber daya yang diperlukan CSIRT.
- Bekerjasama dalam mengembalikan layanan.

Membangun Budaya Aman di OPD

- Edukasi pegawai soal phishing, password kuat, dan pelaporan insiden.
- Menjadi garda depan pencegahan.

BADAN SIBER DAN SANDI NEGARA

Langkah Konkrit #4 – Berkolaborasi dalam Menangani Insiden Siber

CISRT tidak bisa jalan sendiri

01

- CSIRT ada di Diskominfo, tapi serangan bisa terjadi di aplikasi atau sistem yang dikelola OPD.
- Artinya, OPD adalah garda terdepan deteksi awal.

OPD juga tidak bisa sendirian

02

- Kalau sistem kena serangan, OPD tidak punya semua kemampuan teknis untuk investigasi & recovery.
- Harus segera eskalasi ke CSIRT

Kolaborasi itu kunci

03

- OPD = mata & telinga (deteksi, lapor, jaga bukti).
- CSIRT = otak & tangan teknis (analisis, containment, pemulihan).
- Bersama → serangan bisa cepat ditangani, dampak bisa diminimalkan.

04

**“CSIRT butuh OPD, OPD butuh CSIRT.
Hanya dengan kolaborasi, layanan publik bisa tetap berjalan aman.”**

“Kechilafan Satu Orang Sahaja
Cukup Sudah Menyebabkan Keruntuhan Negara”

Mayjen TNI (Purn) dr. Roebiono Kertopati
(1914 - 1984)
Bapak Persandian Republik Indonesia

Survey Layanan
D32 BSSN

https://s.id/LayananD32