KIWA TENGEN

MODUL KEAMANAN SIBER

Topik 4: Tanggap Insiden Siber

Subtopik 4.2: Tanda-Tanda Terjadinya Serangan Siber

Disusun oleh:
Ketut Ananda Dharmawati
NIM: 2215091035

Program Studi S1 Sistem Informasi
Jurusan Teknik Informatika
Fakultas Teknik dan Kejuruan
Universitas Pendidikan Ganesha

BERSAMA CORPU KIWA TENGEN,
KLUNGKUNG TANGGUH HADAPI SERANGAN SIBER

DINAS KOMUNIKASI DAN INFORMATIKA
KABUPATEN KLUNGKUNG
2025

KATA PENGANTAR

Puji syukur kita panjatkan ke hadirat Tuhan Yang Maha Esa, karena atas rahmat-Nya modul pembelajaran *"Keamanan Siber untuk ASN dan Masyarakat"* dapat disusun hingga membahas subtopik penting mengenai *Tanda-Tanda Terjadinya Serangan Siber*. Di tengah meningkatnya aktivitas digital di instansi pemerintahan dan masyarakat pada tahun 2025, serangan siber tidak lagi hanya menargetkan lembaga besar, tetapi juga individu dan perangkat pribadi. Kemampuan mengenali tanda-tanda awal serangan menjadi kunci dalam mencegah kerusakan yang lebih luas, baik terhadap sistem pemerintahan maupun data pribadi warga.

Melalui subtopik ini, diharapkan ASN dan masyarakat Kabupaten Klungkung mampu mengenali pola-pola serangan siber secara dini, mulai dari email mencurigakan, aktivitas jaringan yang tidak wajar, hingga munculnya notifikasi atau perubahan aneh pada sistem. Kesadaran dan respons cepat dari setiap pengguna menjadi bagian penting dari ketahanan siber daerah. Terima kasih kepada semua pihak yang telah berkontribusi dalam penyusunan subtopik ini. Semoga subtopik ini memberikan manfaat nyata dalam mendukung terwujudnya tata kelola pemerintahan dan kehidupan masyarakat yang lebih aman di era digital.

Kami menyadari bahwa modul ini masih memiliki keterbatasan dan belum sempurna. Oleh karena itu, kami sangat mengharapkan kritik dan saran yang membangun dari para pembaca demi penyempurnaan modul ajar ini di masa mendatang.

Klungkung, 2025

Penyusun

DAFTAR ISI

Tujuan Pembelajaran

Setelah mempelajari bagian ini, peserta (ASN maupun masyarakat) diharapkan mampu:

1. Memahami arti penting mengenali tanda-tanda dini serangan siber di lingkungan kerja dan pribadi.
2. Mengidentifikasi jenis-jenis serangan siber yang umum terjadi di Indonesia tahun 2025.
3. Mengetahui indikator teknis dan nonteknis dari aktivitas siber mencurigakan.
4. Membedakan antara gangguan teknis biasa dengan tanda-tanda serangan yang berpotensi berbahaya.
5. Membangun budaya kewaspadaan digital untuk mencegah dampak insiden siber di lingkungan pemerintahan dan masyarakat.

Sasaran Peserta

1. ASN: Agar mampu mengenali tanda-tanda dini serangan siber di lingkungan kerja, memahami potensi dampaknya terhadap sistem pemerintahan, serta dapat mengambil langkah cepat sesuai prosedur keamanan instansi. Dengan memahami ciri-ciri serangan seperti aktivitas mencurigakan pada jaringan, email palsu, atau perubahan sistem tanpa izin, ASN dapat menjadi garda terdepan dalam menjaga keutuhan data dan layanan publik.
2. Masyarakat: Agar lebih waspada terhadap gejala serangan siber di kehidupan sehari-hari, seperti pesan penipuan, aplikasi palsu, atau pencurian data pribadi. Dengan meningkatkan kesadaran dan kemampuan mengenali tanda-tanda serangan sejak dini, masyarakat dapat melindungi diri, keluarga, dan lingkungannya dari kerugian finansial maupun penyalahgunaan identitas digital.

A. Mengapa Penting Mengenali Serangan Siber Lebih Dini

Di era digital yang serba terhubung, serangan siber sering kali tidak langsung terlihat seperti kejahatan fisik. Ia datang diam-diam, tanpa suara, dan baru terasa ketika kerugian sudah terjadi. Mengetahui **tanda-tanda awal serangan** memberi kita kesempatan emas untuk mencegah kebocoran data, pencurian identitas, atau bahkan sabotase sistem pemerintahan.

Badan Siber dan Sandi Negara (BSSN, 2025) mencatat bahwa **lebih dari 72% insiden siber di Indonesia baru diketahui setelah 48 jam terjadinya serangan**, padahal deteksi dini dalam 6 jam pertama dapat mengurangi kerugian hingga 60%. Kesadaran adalah pertahanan pertama, bukan antivirus.

Coba bayangkan:

a. Komputer Anda tiba-tiba lambat padahal tidak sedang memproses data besar.
b. Muncul pop-up aneh di layar atau pesan “akses ditolak”.
c. Email Anda mengirim pesan sendiri tanpa Anda sadari.

Semua itu bukan hal sepele, bisa jadi pertanda bahwa ada pihak luar yang mencoba mengambil alih kendali.

B. Jenis dan Tanda-Tanda Umum Serangan Siber (Update 2025)

Serangan siber tidak selalu langsung terlihat seperti peretasan besar. Sering kali, tanda-tandanya kecil dan muncul perlahan, misalnya sistem tiba-tiba lambat, ada email aneh, atau file hilang tanpa sebab. Memahami tanda-tanda awal inilah yang membantu ASN maupun masyarakat mencegah dampak lebih besar.

1. Perubahan Sistem yang Tidak Wajar

Ciri-ciri ini paling sering terjadi di instansi maupun perangkat pribadi:

a. Komputer atau aplikasi pemerintah berjalan sangat lambat tanpa alasan jelas.
b. Muncul pesan error berulang padahal tidak ada perubahan sistem.
c. File, data, atau arsip dinas tiba-tiba hilang, rusak, atau berganti nama sendiri.
d. Adanya akun pengguna baru yang tidak pernah dibuat oleh admin resmi.

🔎 **Contoh nyata (2024):** CSIRT BSSN mencatat beberapa kasus di mana laptop ASN tiba-tiba mengirim data otomatis ke server luar negeri akibat malware tersembunyi di file laporan Excel.

2. Email atau Pesan Mencurigakan (Phishing Modern)

Serangan phishing kini semakin canggih, sering meniru gaya komunikasi pejabat atau rekan kerja. Tanda-tandanya:

a. Pengirim tampak resmi tapi alamat email sedikit berbeda (misal: @go.idn bukan @go.id).
b. Pesan mendesak, seperti "segera perbarui *password e-office* Anda."
c. Terdapat tautan (link) yang aneh atau tidak mengarah ke situs resmi.
d. Lampiran file dengan ekstensi tidak umum (.exe, .scr, .html).

📩 **Tips cepat:** Arahkan kursor ke link tanpa mengklik, jika alamat tujuan tidak sesuai domain resmi, jangan buka.

3. Aktivitas Login Asing atau Tidak Dikenal

Ada notifikasi login dari lokasi lain (misal: akun Anda masuk dari negara lain).

a. Sistem menolak login padahal password benar (tanda akun telah diubah pihak lain).
b. Riwayat login menunjukkan perangkat yang tidak pernah digunakan.

👥 **Langkah aman:** Segera ubah *password*, aktifkan *Two-Factor Authentication (2FA)*, dan laporkan ke unit keamanan siber instansi.

4. Perangkat Terasa Panas, Baterai Cepat Habis, atau Kuota Boros

Ini bisa jadi tanda perangkat disusupi *spyware* atau *cryptominer* yang bekerja diam-diam di latar belakang.

a. HP cepat panas meskipun tidak digunakan.
b. Kuota internet meningkat drastis tanpa aktivitas pengguna.
c. Terdapat aplikasi baru yang tidak pernah diunduh.

💡 Banyak masyarakat menganggap ini hanya masalah teknis, padahal bisa berarti

perangkat sedang digunakan untuk aktivitas ilegal (seperti *botnet* atau pencurian data).

5. Iklan Pop-Up, Situs Dialihkan, atau Browser Berperilaku Aneh

a. Muncul iklan otomatis walau tidak membuka situs.
b. Pencarian di Google selalu dialihkan ke situs lain.
c. Ekstensi atau *plugin* baru muncul tanpa persetujuan.

🧭 **Langkah aman:** Gunakan browser resmi dan perbarui secara berkala. Hindari mengunduh ekstensi dari sumber tidak jelas.

6. Tanda Spesifik di Lingkungan ASN

Serangan terhadap instansi pemerintah memiliki ciri berbeda dari pengguna umum:

a. Sistem internal tidak bisa diakses tiba-tiba (misal: SIAK, SIMPEG, e-Office).
b. Terdapat surat elektronik (SE) palsu yang meniru dokumen resmi pemerintah.
c. Server instansi mengirim data ke alamat IP luar negeri tanpa izin.
d. Aplikasi dinas memunculkan pesan "ransom" atau meminta pembayaran.

📊 **Tren 2025:** Menurut laporan BSSN (*State of Cybersecurity Indonesia 2025*), lebih dari **55% serangan terhadap pemerintah daerah** diawali dari email phishing internal dan penggunaan akun ASN yang diretas.

7. Tanda Serangan di Kalangan Masyarakat

a. Akun media sosial mengirim pesan otomatis ke semua kontak.
b. Dompet digital berkurang tanpa transaksi.
c. Muncul notifikasi "akun Anda digunakan di perangkat lain."
d. Nomor ponsel tiba-tiba tidak aktif (tanda SIM swap atau pencurian identitas).

⚠️ **Catatan:** Jika hal ini terjadi, segera **hubungi penyedia layanan digital**, ganti semua password terkait, dan laporkan ke **CSIRT Klungkung** atau **Aduan BSSN**.

C. Contoh Nyata Serangan Siber di Indonesia

Serangan siber di Indonesia semakin kompleks. Tidak hanya menargetkan lembaga pemerintah pusat, tetapi juga **pemerintah daerah**, **pelayanan publik**, bahkan

akun pribadi ASN. Berikut beberapa contoh nyata yang bisa menjadi pelajaran bagi kita semua:

1. Kasus Kebocoran Data Dukcapil (2023)

Pada pertengahan 2023, data kependudukan milik jutaan warga Indonesia dilaporkan beredar di forum gelap (*dark web*). Kebocoran ini diduga berasal dari integrasi sistem yang kurang aman antara aplikasi internal dan pihak ketiga.

🔍 **Pelajaran:**

a. Sistem pemerintah harus memiliki kontrol akses ketat dan audit keamanan rutin.
b. ASN wajib menjaga kerahasiaan akun dan tidak membagikan akses tanpa izin.

2. Serangan Ransomware pada Pemerintah Kabupaten (2024)

Beberapa sistem layanan publik di tingkat kabupaten lumpuh akibat ransomware. Data kepegawaian dan dokumen keuangan terkunci dengan pesan tebusan dalam mata uang kripto.

🧩 **Tanda Awal yang Terlewatkan:**

a. Server lambat beberapa hari sebelumnya.
b. File sistem berubah ekstensi menjadi ".locked".
c. Ada email masuk berisi "update keamanan terbaru", ternyata berisi malware.

💡 **Pelajaran:**

Penting bagi setiap instansi memiliki **backup rutin offline** dan SOP darurat ketika sistem terkena serangan.

3. Kasus Phishing Mengatasnamakan Instansi Pemerintah (2024)

Banyak ASN menerima email palsu dengan alamat hampir mirip domain resmi pemerintah, misalnya:

info@bssn-go.id (palsu) menggantikan info@bssn.go.id (asli). Isi pesan berisi tautan untuk "mengunduh surat tugas ASN digital".

📨 Setelah diklik, data login ASN langsung dicuri oleh pelaku.

🔎 **Pelajaran:**

a. Selalu periksa domain resmi (.go.id).
b. Jangan mengunduh atau mengklik lampiran tanpa verifikasi.
c. Laporkan segera ke **CSIRT** jika menemukan aktivitas mencurigakan.

4. Penipuan Digital dan Pengambilalihan Akun WhatsApp (2025)

Kasus ini marak di kalangan masyarakat umum. Pelaku mengaku sebagai petugas instansi dan meminta kode OTP. Begitu diberikan, akun langsung diambil alih dan digunakan untuk menipu kontak lain.

📱 **Pelajaran:**

a. OTP bersifat pribadi, tidak boleh diberikan kepada siapa pun.
b. Aktifkan fitur *verifikasi dua langkah (2FA)* di WhatsApp dan media sosial.
c. Edukasi keluarga agar lebih waspada terhadap pesan mendesak.

5. Serangan Siber pada Aplikasi Pelayanan Publik Daerah (2025)

Aplikasi berbasis web milik beberapa pemerintah daerah disusupi *SQL Injection*, menyebabkan data pengguna bocor. Modusnya: pelaku mengirim link survei palsu yang mengarahkan pengguna ke situs tiruan (*phishing mirror site*).

💻 **Pelajaran:**

a. Tim pengelola IT harus rutin melakukan *security assessment*.
b. ASN pengguna aplikasi wajib memastikan hanya mengakses dari domain resmi.

6. Kasus Deepfake dan Manipulasi Citra Pejabat Daerah (2025)

Kemunculan video palsu menggunakan teknologi *deepfake* menyerang reputasi pejabat publik daerah. Video disebar luas di media sosial dengan narasi menyesatkan.

🎯 **Pelajaran:**

a. Jangan langsung percaya atau membagikan konten digital tanpa verifikasi sumber.
b. ASN dan masyarakat harus memahami cara memeriksa keaslian konten (*fact-checking*).

c. Etika digital dan literasi media jadi bagian penting pertahanan sosial dari sisi non-teknis.

D. Langkah Cepat Mengenali dan Merespons Serangan

Serangan siber tidak selalu terlihat jelas. Terkadang hanya muncul dalam bentuk perubahan kecil yang sering diabaikan. Namun, langkah cepat di tahap awal dapat menyelamatkan sistem, data, bahkan reputasi instansi. Berikut panduan praktis yang perlu diterapkan:

🔍 **1. Amati Gejala Aneh pada Sistem atau Akun**

Beberapa tanda awal serangan sering tampak sepele:

a. Komputer menjadi lambat tanpa alasan jelas.
b. File tiba-tiba berubah nama atau tidak bisa dibuka.
c. Terdapat program asing yang tidak pernah diinstal.
d. Akun media sosial mengirim pesan tanpa sepengetahuan pemilik.
e. Ada *login* dari lokasi atau perangkat yang tidak dikenal.

🧩 **Langkah ASN & Masyarakat:**

Segera hentikan penggunaan perangkat, catat gejalanya, dan laporkan ke tim teknis atau CSIRT instansi.

⚠️ **2. Periksa Email dan Pesan yang Mencurigakan**

Serangan paling sering datang melalui pesan elektronik, baik email, WhatsApp, atau media sosial. Ciri khasnya:

a. Mengandung link atau lampiran dengan nada mendesak (“Akun Anda akan dinonaktifkan”, “Segera klik di sini”).
b. Menggunakan logo instansi tetapi domain tidak resmi.
c. Mengandung kesalahan ejaan atau tata bahasa aneh.

💡 **Langkah ASN & Masyarakat:**

a. Jangan klik tautan atau buka lampiran sebelum verifikasi.
b. Laporkan ke CSIRT atau ke admin keamanan TI instansi.

c. Hapus pesan setelah dilaporkan agar tidak tersebar ke rekan kerja.

🔒 **3. Perhatikan Perubahan Tak Biasa di Akun Pribadi**

Jika akun email, media sosial, atau sistem kerja meminta login ulang terus-menerus, itu bisa tanda ada percobaan *hacking*. Tanda lainnya:

a. Notifikasi login dari lokasi asing.
b. Pesan konfirmasi reset password padahal Anda tidak meminta.
c. Aktivitas aneh pada akun keuangan atau e-wallet.

🧠 **Langkah ASN & Masyarakat:**

Segera ubah password dari perangkat lain yang aman.

Aktifkan *two-factor authentication (2FA)*.

Jika tidak bisa masuk akun, laporkan ke penyedia layanan atau CSIRT.

🧯 **4. Putuskan Koneksi Internet Jika Ada Indikasi Serangan**

Langkah ini sering diabaikan, padahal sangat penting untuk mencegah penyebaran malware ke jaringan instansi.

🚫 **Langkah ASN:**

a. Cabut kabel LAN atau matikan Wi-Fi perangkat yang terinfeksi.
b. Jangan mencoba memperbaiki sendiri sebelum sistem diperiksa tim keamanan.

🚫 **Langkah Masyarakat:**

a. Jika laptop atau HP menunjukkan pop-up aneh, segera nonaktifkan koneksi data.
b. Jalankan pemindaian antivirus dari perangkat lain atau minta bantuan teknisi terpercaya.

🧩 **5. Laporkan Segera ke CSIRT atau Unit Keamanan Siber Instansi**

ASN wajib melaporkan indikasi serangan ke **CSIRT (Computer Security Incident Response Team)** di tingkat instansi atau daerah. Masyarakat dapat melaporkan melalui:

CSIRT Klungkung: https://csirtklungkung.klungkungkab.go.id

💡 Jangan takut melapor lebih awal, laporan dini sering kali menjadi kunci mencegah kerugian besar.

🛡️ **6. Gunakan Prinsip "Stop – Think – Verify"**

Prinsip sederhana tapi efektif:

Stop: hentikan tindakan saat muncul hal mencurigakan.

Think: pikirkan dampaknya sebelum mengklik, membalas, atau membagikan informasi.

Verify: pastikan sumber informasi dari domain atau akun resmi.

📌 Prinsip ini wajib diterapkan baik dalam pekerjaan ASN maupun aktivitas digital masyarakat umum.

E. Rekomendasi Tindakan ASN dan Masyarakat

Serangan siber tidak selalu datang dalam bentuk besar seperti peretasan sistem atau ransomware yang menakutkan. Sebagian besar justru dimulai dari **kelalaian kecil**, seperti mengabaikan email mencurigakan, lupa mengganti kata sandi, atau terlalu percaya pada pesan yang tampak "resmi". Tanda-tanda awal seperti **perangkat melambat, login mencurigakan, atau file yang berubah sendiri** sering kali menjadi sinyal bahaya yang muncul sebelum serangan besar terjadi.

Oleh karena itu, kemampuan **mendeteksi gejala awal dan bertindak cepat** adalah keterampilan dasar yang wajib dimiliki oleh setiap **ASN dan masyarakat digital tahun 2025**. Keamanan siber bukan hanya urusan teknis, tapi juga **tanggung jawab perilaku**. Dengan memahami tanda-tanda serangan dan menerapkan langkah tanggap dini, kita tidak hanya melindungi data pribadi, tapi juga menjaga kepercayaan publik terhadap sistem pemerintahan digital.

Rekomendasi untuk ASN

- **Bangun kebiasaan deteksi dini.** Perhatikan performa sistem kerja setiap hari, jangan abaikan notifikasi atau pesan peringatan sekecil apa pun.
- **Aktifkan sistem keamanan berlapis.** Gunakan *two-factor authentication* di semua aplikasi dinas dan email kerja.
- **Segera laporkan ke CSIRT instansi.** Jangan menunggu "masalah membesar" baru

melapor. Tindakan cepat sering kali menjadi pembeda antara insiden kecil dan bencana digital besar.

- **Ikuti pelatihan keamanan siber secara rutin.** ASN di Klungkung didorong untuk memperbarui literasi digital minimal dua kali setahun agar mampu menanggapi ancaman baru yang terus berkembang.

3. Rekomendasi untuk Masyarakat

- **Kenali tanda-tanda aneh di perangkat pribadi.** Jangan anggap remeh jika HP terasa panas, baterai cepat habis, atau akun mengirim pesan sendiri.
- **Lindungi identitas digital.** Jangan gunakan satu kata sandi untuk semua aplikasi, dan hindari login di perangkat umum.
- **Laporkan dengan bijak.** Jika menemukan aktivitas aneh atau akun palsu yang merugikan orang lain, laporkan melalui kanal resmi seperti **CSIRT Klungkung** atau **aduan.bssn.go.id**.
- **Bangun kesadaran keluarga.** Edukasi anggota keluarga, terutama anak dan orang tua, agar tidak mudah tertipu oleh tautan atau pesan berbahaya.

"Serangan siber bisa datang kapan saja,
tapi kesiapsiagaan digital adalah perisai terbaik."

Dengan memahami tanda-tanda awal dan mengambil tindakan cepat, setiap ASN dan masyarakat Klungkung menjadi bagian penting dari sistem pertahanan digital daerah. Kesadaran kolektif ini bukan hanya melindungi diri sendiri, tapi juga membangun **Klungkung yang Tangguh Digital: Aman, Cerdas, dan Berdaya** di tahun 2025.

Pertanyaan Reflektif

1. Saat perangkat kerja tiba-tiba melambat dan muncul notifikasi login dari lokasi asing, langkah apa yang paling tepat Anda lakukan sebagai ASN sebelum melapor ke tim teknis?
2. Banyak masyarakat menganggap pesan OTP yang dikirim ke ponsel mereka tidak berbahaya. Bagaimana Anda menjelaskan pentingnya menjaga kerahasiaan OTP agar tidak dimanfaatkan oleh pelaku kejahatan siber?
3. Ketika media sosial pribadi mulai mengunggah konten tanpa sepengetahuan Anda, bagaimana Anda menilai kemungkinan telah terjadi serangan, dan tindakan apa yang sebaiknya segera dilakukan?
4. Di lingkungan kerja, sering muncul email dengan judul mendesak seperti "Perbarui akun e-office Anda segera". Bagaimana Anda bisa membedakan mana pesan resmi dan mana yang berpotensi menjadi serangan siber terselubung?
5. Sebagai bagian dari masyarakat digital Klungkung, bagaimana Anda dapat berkontribusi membangun budaya deteksi dini insiden siber di lingkungan kerja atau komunitas Anda?
6. Seorang rekan ASN tidak sadar bahwa laptop dinasnya menampilkan aktivitas aneh, namun tetap digunakan untuk pekerjaan harian. Bagaimana Anda akan menasihatinya agar bertindak cepat tanpa menimbulkan kepanikan?
7. Jika akun layanan publik daerah tiba-tiba memposting informasi mencurigakan, bagaimana Anda menilai situasi tersebut dan menentukan langkah koordinasi dengan pihak yang berwenang?

DAFTAR PUSTAKA

Alasmary, W., Alenezi, M., & Alghamdi, H. (2024). *Early detection of cyber-attacks using hybrid machine learning models*. Computers & Security, 142**,** 103962. https://doi.org/10.1016/j.cose.2024.103962

Alshamrani, A., Alharkan, I., & Alghazzawi, D. (2023). *Detecting suspicious system behavior in enterprise networks using anomaly-based monitoring*. IEEE Access, 11**,** 121094–121109. https://doi.org/10.1109/ACCESS.2023.3334507

Badan Siber dan Sandi Negara (BSSN). (2024). *Laporan Tahunan Keamanan Siber Indonesia 2024*. Jakarta: BSSN. Retrieved from https://bssn.go.id

Chen, L., & Wang, J. (2023). *Indicators of compromise: A comprehensive approach for early-stage cyber incident detection*. Journal of Information Security and Applications, 76, 103503. https://doi.org/10.1016/j.jisa.2023.103503

European Union Agency for Cybersecurity (ENISA). (2024). *Threat Landscape 2024: Key insights and emerging cyber threats*. Luxembourg: ENISA. https://www.enisa.europa.eu/publications

Ghosh, D., & Lee, S. (2023). *Phishing and ransomware attack indicators in public sector networks*. Government Information Quarterly, 40(4), 101934. https://doi.org/10.1016/j.giq.2023.101934

Liu, X., Zhang, Y., & Zhao, L. (2024). *A behavioral approach to detecting cyber intrusions in real-time government systems*. Computers & Electrical Engineering, 113**,** 109020. https://doi.org/10.1016/j.compeleceng.2024.109020

Moustafa, N., & Slay, J. (2024). *Cyber threat intelligence for proactive incident detection in smart cities*. Future Generation Computer Systems, 150**,** 238–249. https://doi.org/10.1016/j.future.2024.01.013

Sari, A. P., & Wicaksono, B. (2023). *Analisis deteksi dini insiden siber menggunakan metode hybrid intrusion detection system pada lembaga pemerintahan di Indonesia*. Jurnal Keamanan Siber Nasional, **5**(2), 44–56.

https://doi.org/10.52389/jksn.v5i2.118

Verizon. (2024). *Data Breach Investigations Report 2024*. New York: Verizon Enterprise Solutions. Retrieved from https://www.verizon.com/business/resources/reports/dbir/

Wulandari, D., & Prasetyo, R. (2025). *Pemanfaatan sistem monitoring otomatis untuk mendeteksi anomali keamanan pada instansi pemerintah daerah*. Jurnal Sistem Informasi dan Keamanan Digital, 6(1), 27–38. https://doi.org/10.31219/osf.io/x7r4b