Nama : **Muh. Rifky**

Nim **220205600005**

Prodi : **D4-Teknik Elektronika**

Kampus : **Universitas Negeri Makassar**

Soal

1. Buatlah laporan terkait issue problem, dampak dan solusi yang diberikan oleh instansi/organisasi tersebut dalam common cyber threat pada phising, social engineering (sosial media), password attack, device threat.Masing-masing 1, berikan sumber pada masing-masing issue.Issue bersifat internasional Max 2 halaman

Jawab:

1. **Pihsing**
   - **a. Issue**
     - Pada September **25 Agustus, 2025** Check Point melaporkan kampanye phishing global yang memanfaatkan invitasi Google Classroom palsu untuk menyampaikan email phishing kepada lebih dari 13.500 organisasi melalui ~115.000 email. Serangan ini sulit terdeteksi karena memanfaatkan infrastruktur cloud resmi
   - **b. Dampak**
     - banyak email berbahaya tetap masuk ke inbox utama pengguna tanpa ditandai sebagai ancaman.
     - Ribuan guru, mahasiswa, karyawan, dan staf pemerintah berisiko membuka link phishing karena mereka terbiasa menerima undangan semacam itu.
     - Risiko pencurian kredensial, penyusupan malware, dan pelanggaran data.
   - **c. Solusi yang Diberikan**
     - Penerapan pendidikan dan pelatihan user secara kontinu.
     - Penggunaan AI-powered detection tools untuk mendeteksi ancaman konten.
     - Peningkatan pemantauan keamanan aplikasi cloud secara terus-menerus.
   - **d. Link issue**
     - https://blog.checkpoint.com/email-security/phishing-in-the-classroom-115000-emails-exploit-google-classroom-to-target-13500-organizations/
2. **Social Engineering melalui Media Sosial**
   - **a. Issue**
     - Melaporkan dari cio healthcare Indonesia Serangan Siber Global Melonjak 75% di Q3 sejak **02 Nov, 2024**
   - **b. Dampak**
     - Tingkat ancaman meningkat drastis dari sisi volume dan frekuensi, memaksa organisasi memperkuat pertahanan.
     - Segmen tertentu seperti pendidikan dan sosial sangat rentan, karena tingginya serangan per minggu yang dapat mengganggu operasional dan keamanan data..
     - Industri seperti manufaktur (30%), kesehatan (13%), dan ritel/grosir (10%) menjadi target utama ransomware

c. **Solusi**
   - mplementasi sandboxing, alat anti-ransomware, dan teknologi intelijen keamanan
   - Verifikasi identitas yang ketat untuk setiap pengguna dan perangkat.
   - Patch sistem secara berkala dan gunakan proteksi berlapis seperti firewall dan endpoint protection.

d. **Link issue**
   - https://ciohealthcare.or.id/berita/serangan-siber-global-melonjak-di-2024

3. **Password Attack**

a. **Issue**
   - Menurut laporan Gitnux (**April 29, 2025**), sebagian besar serangan dimulai dari kelemahan kata sandi

b. **Dampak**
   - 81% pelanggaran data melibatkan serangan berbasis brute-force atau kredensial yang dicuri.
   - 91% serangan dunia maya dimulai lewat email phishing, sering kali untuk mencuri kredensial.

c. **Solusi**
   - Adopsi autentikasi multi-faktor (MFA) secara luas.
   - Pelatihan kesadaran keamanan untuk mengenali phishing terkait kredensial.
   - Pemantauan perilaku login untuk mendeteksi anomali seperti login dari lokasi atau perangkat tidak biasa.

d. **Link issue**
   - https://gitnux.org/social-engineering-attacks-statistics/

4. **Device Threat**

a. **Issue**
   - TSA telah mengeluarkan peringatan mendesak **Juni 22, 2025** tentang penjahat yang menggunakan port pengisian daya USB palsu, honeypot Wi-Fi gratis untuk mencuri identitas Anda menjelang liburan musim panas

b. **Dampak**
   - Infeksi Malware, Pencurian Data, Kompromi Kredensial dan Gangguan Operasional Organisasi

c. **Solusi**
   - Gunakan charger & adaptor milik sendiri, sambungkan ke colokan listrik, bukan ke port USB publik.
   - Gunakan USB data blocker (charge-only cable) agar tidak ada transfer data.
   - Bawa power bank pribadi untuk menghindari ketergantungan pada port publik.
   - Update sistem operasi & aplikasi secara rutin untuk menutup celah keamanan.
   - Organisasi membuat kebijakan keamanan perangkat mobile, termasuk pelatihan bagi karyawan untuk waspada terhadap device threat.

d. **Link issue**
   - https://www.techradar.com/pro/security/the-us-transportation-security-administration-issues-an-urgent-warning-about-criminals-using-fake-usb-charging-ports-free-wi-fi-honeypots-to-steal-your-identity-ahead-of-summer-holidays?utm_source=chatgpt.com