

Evolusi Ancaman Siber

dan

Dampak di Industri Keuangan



Largest Companies by Marketcap

Rank	Name	Market Cap	Price	Today	Price (30 days)	Country
1	 Apple AAPL	\$ 3.674 T	\$244.60 ▲ 1.27%	▲ 1.27%		USA
2	 NVIDIA NVDA	\$ 3.400 T	\$138.85 ▲ 2.63%	▲ 2.63%		USA
3	 Microsoft MSFT	\$ 3.036 T	\$408.43 ▼ 0.51%	▼ 0.51%		USA
4	 Amazon AMZN	\$ 2.423 T	\$228.68 ▼ 0.73%	▼ 0.73%		USA
5	 Alphabet (Google) GOOG	\$ 2.266 T	\$186.87 ▼ 0.54%	▼ 0.54%		USA
6	 Meta Platforms (Facebook) META	\$ 1.866 T	\$736.67 ▲ 1.11%	▲ 1.11%		USA
7	 Saudi Aramco 2222.SR	\$ 1.781 T	\$7.37 ▼ 0.18%	▼ 0.18%		S. Arabia
8	 Tesla TSLA	\$ 1.144 T	\$355.84 ▼ 0.03%	▼ 0.03%		USA
9	 Broadcom AVGO	\$ 1.092 T	\$233.04 ▼ 1.17%	▼ 1.17%		USA
10	 TSMC TSM	\$ 1.057 T	\$203.90 ▲ 1.03%	▲ 1.03%		Taiwan

A conceptual image showing several offshore oil rigs in the ocean. Instead of traditional drilling equipment, the rigs are topped with logos of major technology companies: Amazon, Microsoft, Google, Facebook, and Tesla. Cranes are visible on the rigs, and streams of binary code (0s and 1s) are being pumped out into the sky, suggesting a flow of data. The text 'Data is The New Oil' is written in a large, white, serif font across the middle of the image, with '→ Internet' below it in a similar font, underlined.

Data is The New Oil

→ Internet





Murahin harga KUOTA INTERNET, bang

Dear, kami [redacted]

Lu jadi operator kagak usah mahal-mahal. Talk!

Pegimane bangsa Indonesia mau maju kalo internet aja mahal

Makan aja susah, apalagi beli kuota internet. Mon [redacted]

harga kuota internet, Nyet! Kagak usah pake dibagi-bagi 2G/

kagak butuh HOOQ, VIU, iming-iming kuota music ame vider

Gue cuma butuh KUOTA INTERNET. TITIK.

*Apa bedanya dirampok
dengan diretas*

Kehilangan data sensitif karena
diretas selain menderita
kerugian finansial juga
menderita kerugian reputasi dan
orang lain ikut menderita

Internet

Merevolusi bisnis

Murah, tersebar

Siapapun bisa mengakses

Bisa di sadap

... apa solusinya ?

Tantangan Verifikasi Digital

Dasarnya :

- Tidak ada Tatap Muka langsung.
- “Siapa saja” asalkan dapat melewati tahap verifikasi identitas dianggap sah sebagai pemilik identitas / akun.

Masalahnya :

Internet adalah jalan umum dan siapapun dapat mengakses jalan itu karena siapapun dapat terhubung ke internet.

Tidak mudah memastikan keabsahan identitas pengakses internet karena anonimitas dan sifat internet yang sangat terbuka. Padahal hal ini merupakan suatu keharusan dalam menjalankan verifikasi yang aman.

Verifikasi Digital dan Ancamannya

Password
→ Keylogger,
Rootkit (malware)

TFA
→ Two Factor
Authentication

Malware Lumma

Memalsukan
Captcha

Mencuri
kredensial
browser

Mengincar
add on kripto

Two factor authentication



SMS



Google Authenticator /
Authy



Token

Mengapa SMS OTP populer ?

Mudah dan Nyaman

Jangkauan Luas

Murah

Implementasi mudah

Mengapa TFA SMS kurang aman ?

Melibatkan banyak pihak

Tidak terenkripsi

SMS menggunakan SS7

Terikat ke Kartu SIM

Salah Siapa kalau SMS OTP Bocor ?



NASABAH ?



BANK ?

Solusi (user)

Amankan kartu SIM dgn PIN.

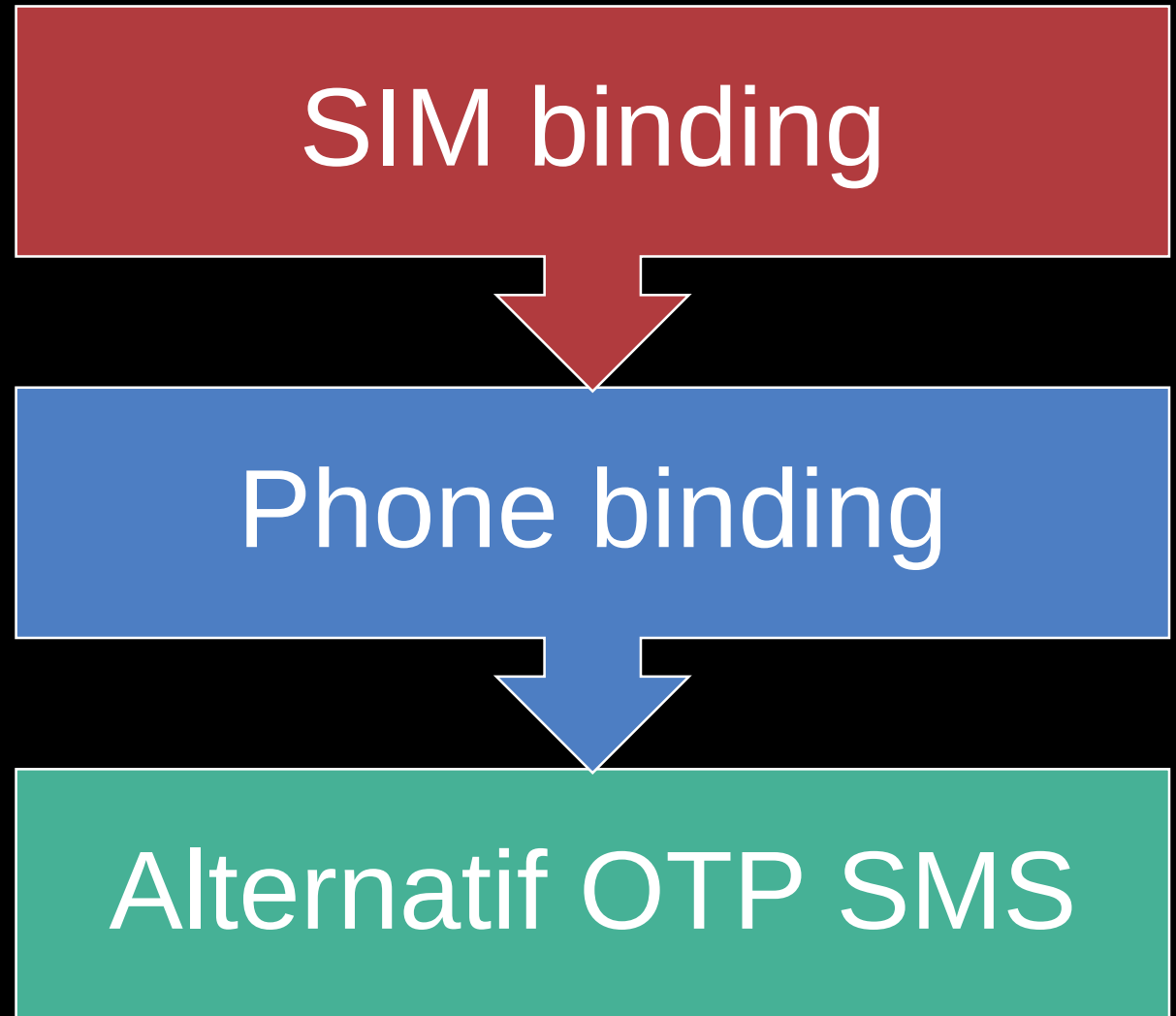


Waspada SMS Forwarding /
Phishing



Kunci perangkat dgn baik.

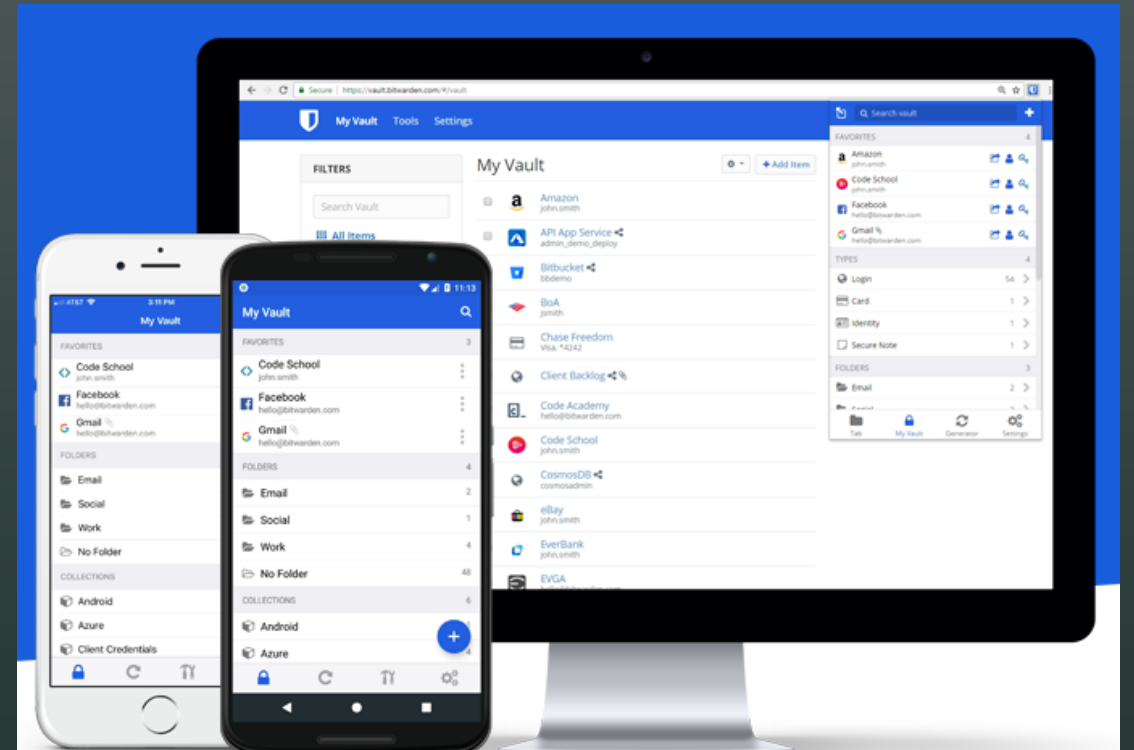
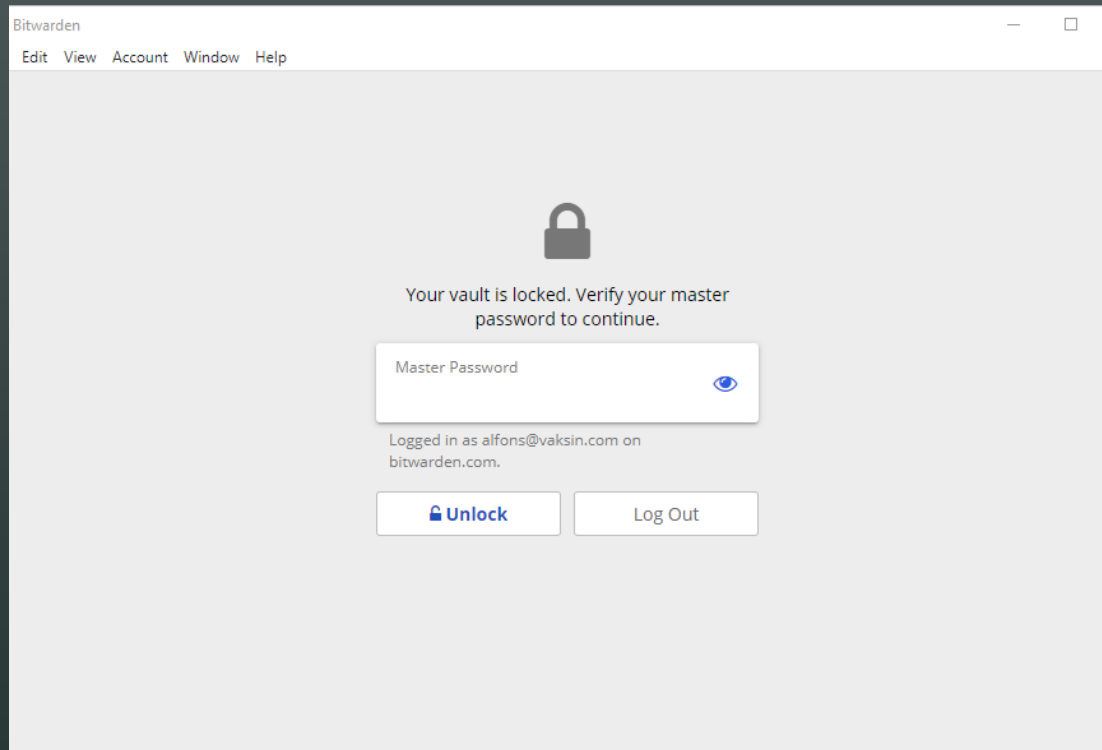
Solusi (bank)





@alfonstan

*Call paman
onetime*



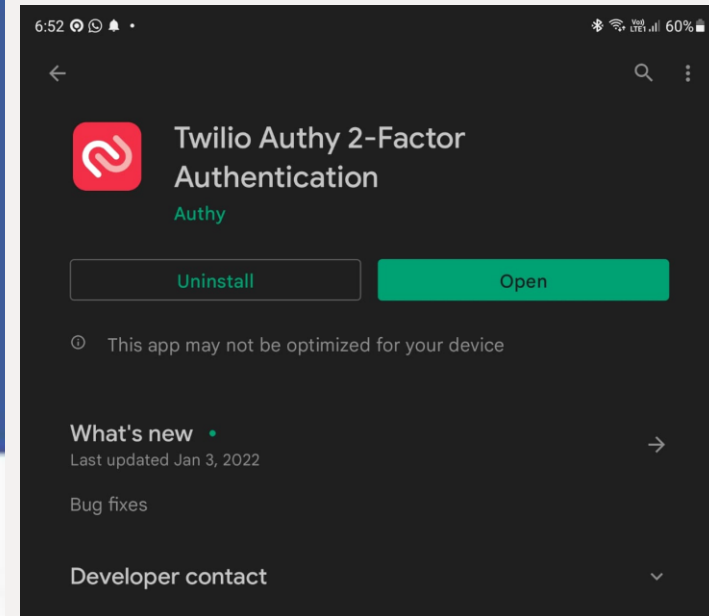
bitWarden

@alfonstan



 Blocking

Authy





Search

DQL

Last 24 hours

Show dates

Refresh

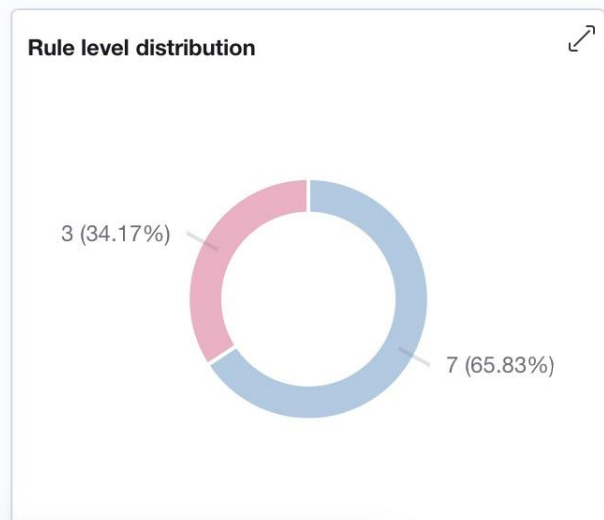
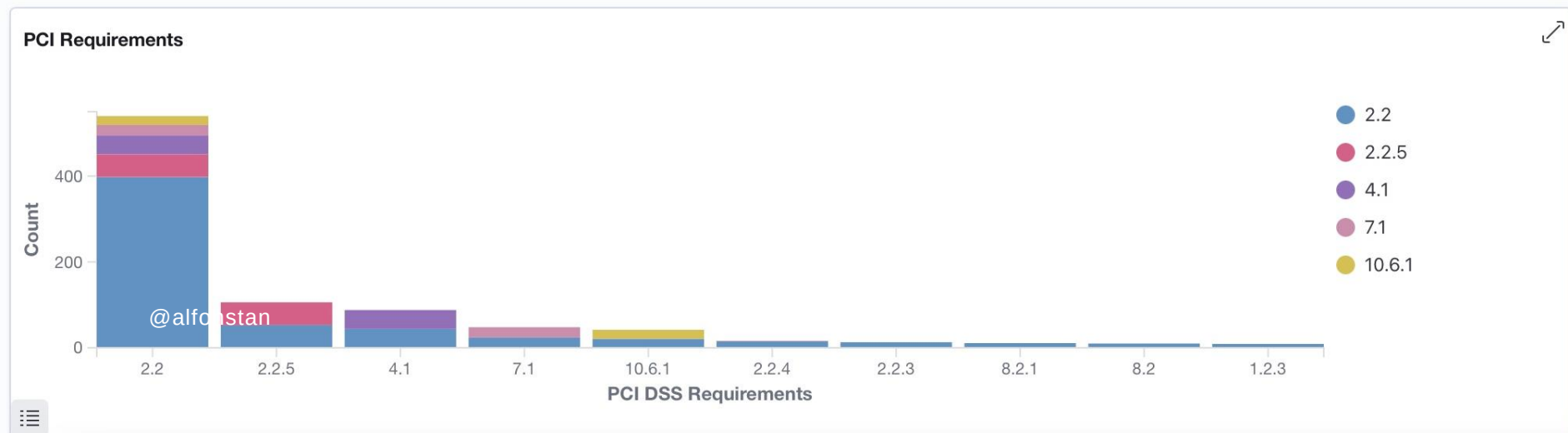
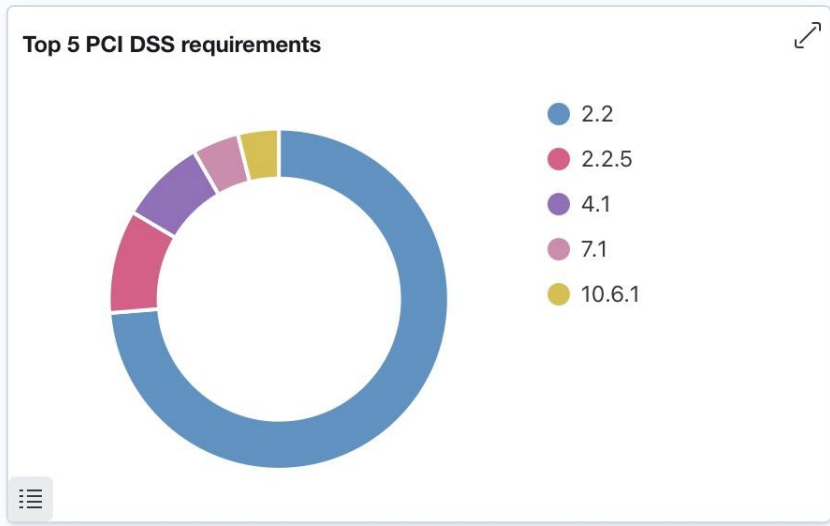
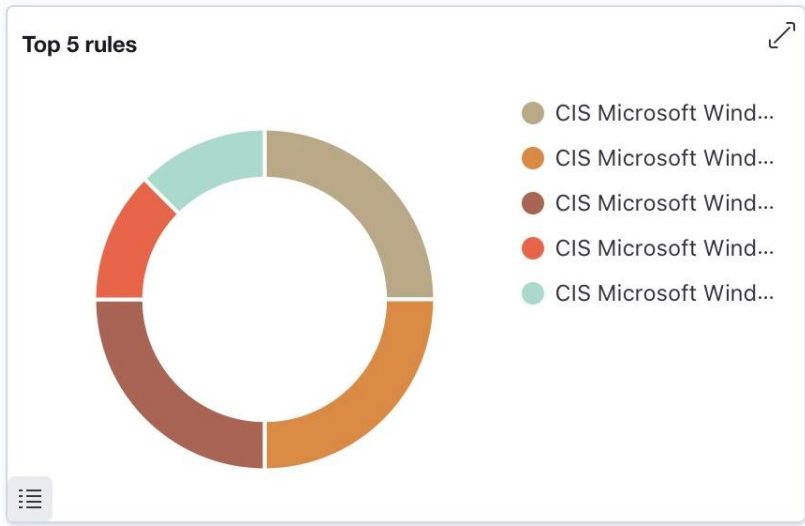
manager.name: ip-172-31-65-197

rule.pci_dss: exists

agent.id: 004

rule.pci_dss: 2.2

+ Add filter



W.

PCI DSSWGM-Cikini

DashboardControlsEvents

WGM-Cikini

Search

DQL

Last 24 hours

Show dates

manager.name: ip-172-31-65-197

rule.pci_dss: exists

agent.id: 004

+ Add filter

PCI DSS

Requirement 2427

Requirement 10159

Requirement 444

Requirement 810

Requirement 65

Requirement 11

Requirement 111

Requirement 50

@alfonstan

Requirements

View details of 2.2

2.2 - Develop configuration standards for all system components. Assume that these standards address all known security vulnerabilities and are consistent with industry accepted system hardening standards (CIS, ISO, NIST).

2.2 - Develop configuration standards for all system components. Assume that these standards address all known security vulnerabilities and are consistent with industry accepted system hardening standards (CIS, ISO, NIST).	10.2.5 - Use of and changes to ...	4.1 - Use strong cryptography a...	10.6.1 - Review the following at l...
2.2.4 - Configure sy	additional sec...	6.2 - Ensure that all system com...	8.1.8 - If a session has been idle...
8.2.4 - Change user	on, stopping, ...	8.1.2 - Control addition, deletion...	10.4 - Using time-synchronizati...
1.3.4 - Do not allow unauthorize...	2.2.2 - Enable only necessary s...	6.5.8 - Improper access control ...	11.4 - Use intrusion detection an.
1.1.1 - A formal process for appr...	1.4 - Install personal firewall soft...	5.1 - Deploy anti-virus software ...	5.2 - Ensure that all anti-virus m...
6.5 - Address common coding v...	6.5.1 - Injection flaws, particularl...	6.5.2 - Buffer overflows	6.5.5 - Improper error handling
6.5.7 - Cross-site scripting (XSS)	6.5.10 - Broken authentication a...	6.6 - For public-facing web appl...	8.1.4 - Remove/disable inactive ...
8.1.5 - Manage IDs used by thir...	8.1.6 - Limit repeated access att...	8.5.1 - Additional requirement fo...	8.7 - All access to any data'
10.1 - Implement audit trails to li...	10.2.1 - All individual user acces...	10.2.2 - All actions taken by any ...	10.2.4 - Invalid logical acce...

Bank di Indonesia hadapi tantangan lebih berat

Bank di Indonesiamenghadapi tantangan yang lebih besar dibandingkan negara lain di Asean karena data kependudukannya sudah bocor.



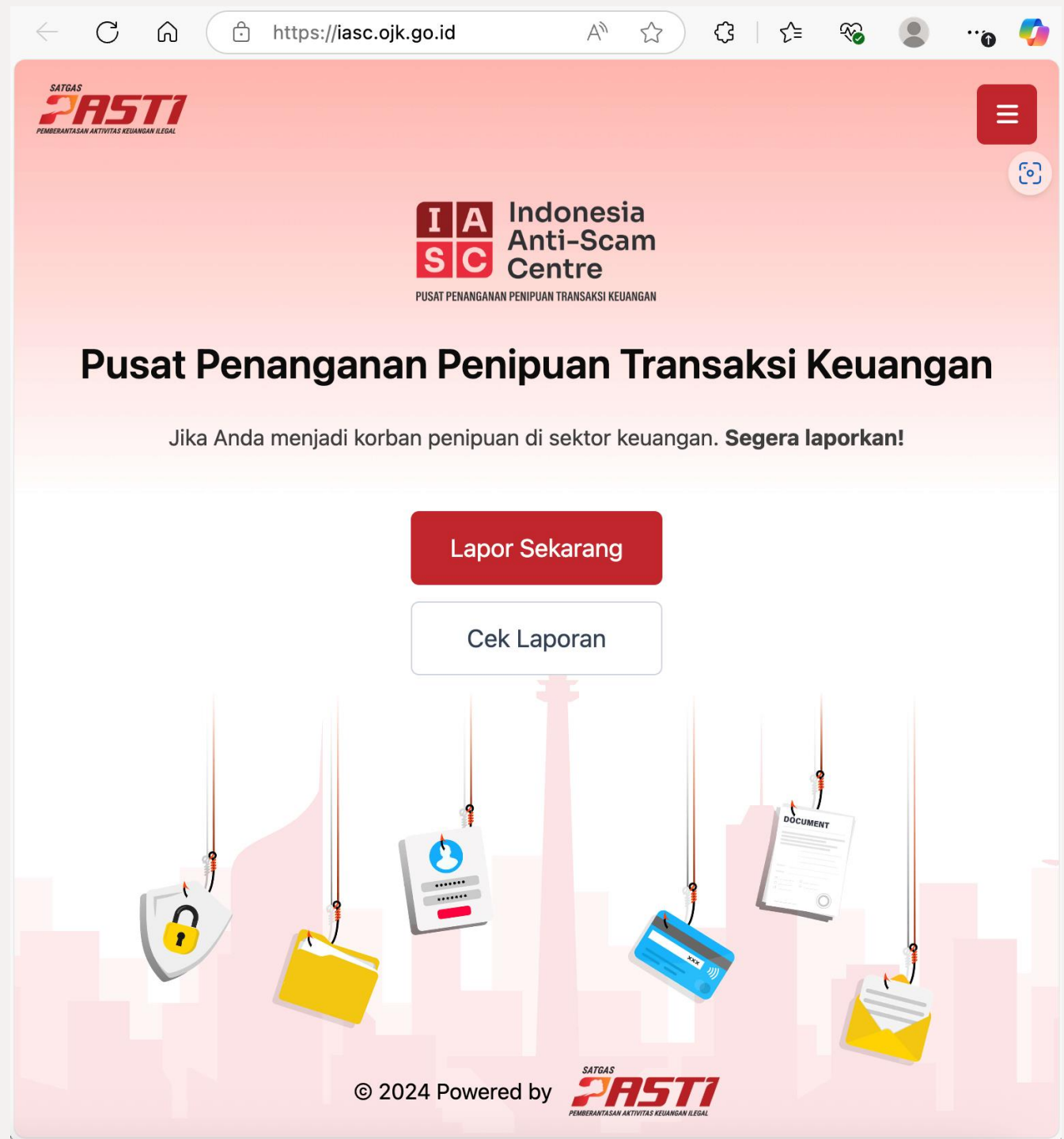
Ibarat biasa nyetir di Indonesia, kalua nyetir di Malaysia atau Singapura, soal skill sih ngga usah khawatir. Cuma soal disiplin itu perlu belajar banyak.



Promosi iPhone

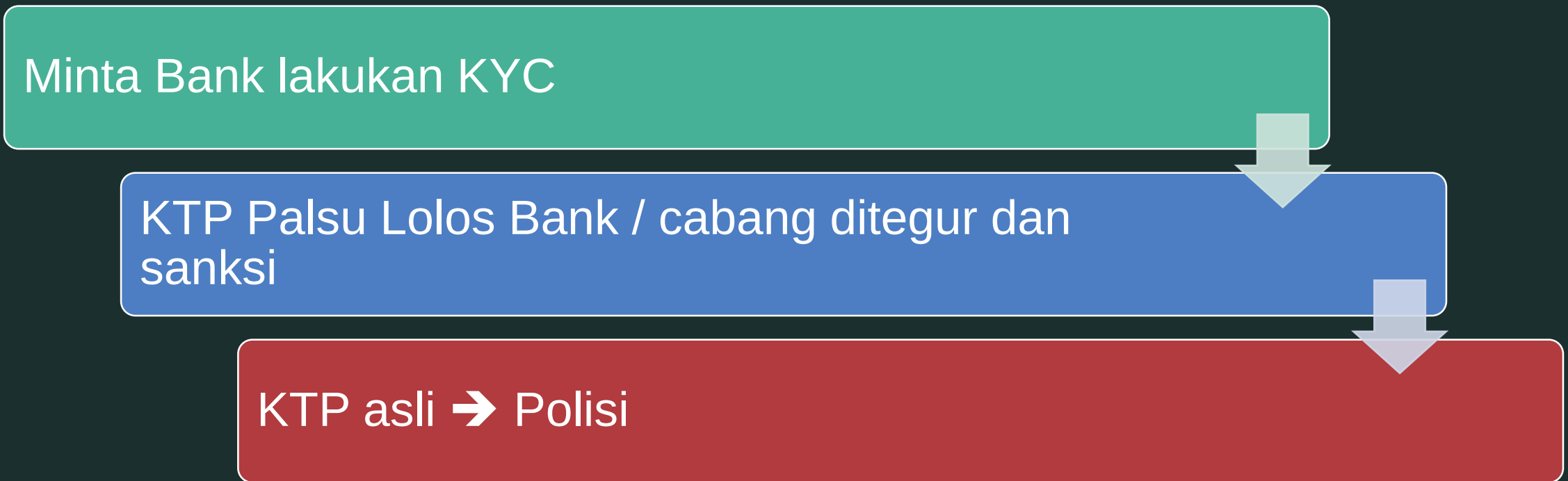
IASC

@alfonstan



Tindakan Kuratif

Minta Bank lakukan KYC



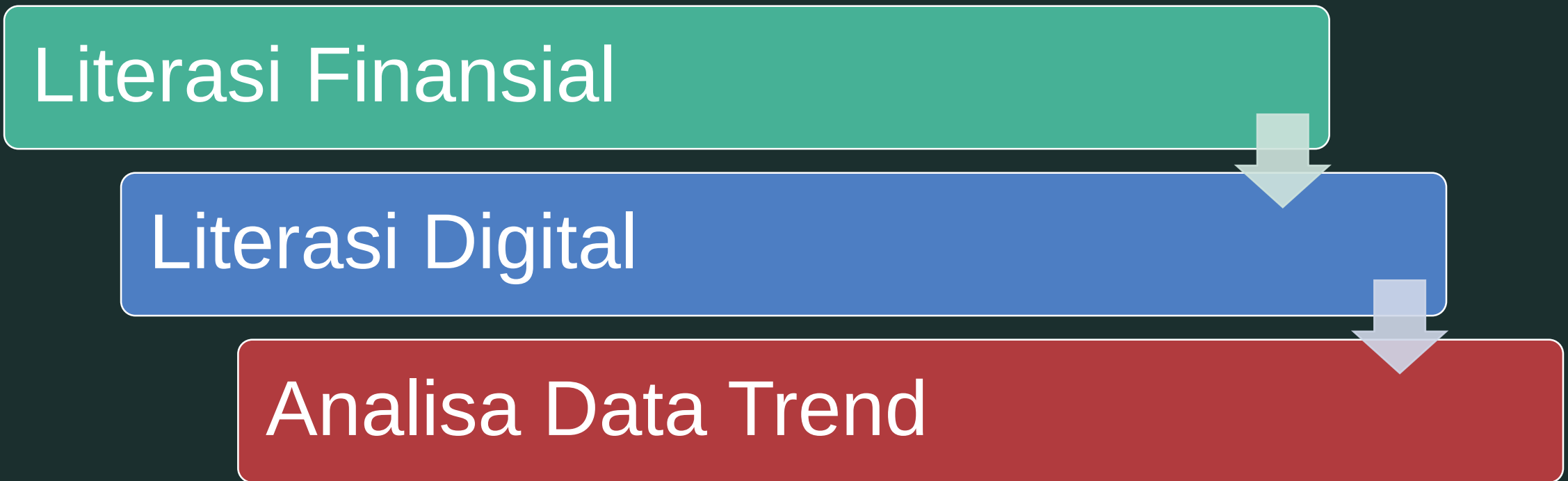
```
graph TD; A[Minta Bank lakukan KYC] --> B[KTP Palsu Lolos Bank / cabang ditegur dan sanksi]; B --> C[KTP asli → Polisi];
```

KTP Palsu Lolos Bank / cabang ditegur dan sanksi

KTP asli → Polisi

Tindakan Preventif

Literasi Finansial



```
graph TD; A[Literasi Finansial] --> B[Literasi Digital]; B --> C[Analisa Data Trend];
```

Literasi Digital

Analisa Data Trend