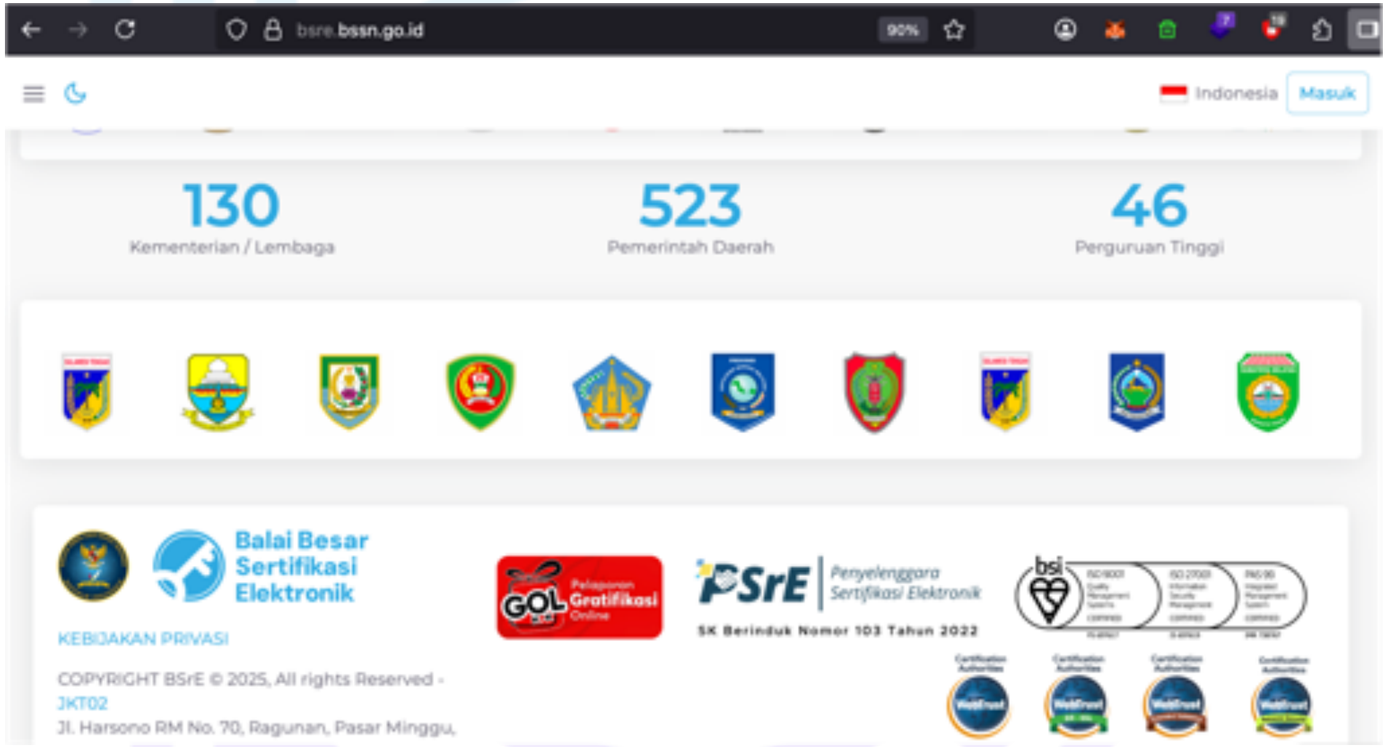
Apakah Penerapan Standar dan Regulasi Berhasil Menangani Isu-Isu Keamanan Terkini?

Presented by
Eko Yon Handri, S.ST, M.M., CISA, CC
Badan Siber dan Sandi Negara

Oktober 2025

APA KESAN PERTAMA ANDA?



CYBER ATTACKS

TINDAKAN oleh pihak jahat untuk mengeksploitasi kerentanan dalam sistem komputer, smart phone, jaringan, atau infrastruktur digital dengan cara merusak, mencuri data, mengganggu operasional, atau melakukan tindakan lain yang merugikan.

Malware (Malicious Software)

Virus, Trojans, Ransomware, Spyware, Adware, BotNet

Social Engineering

Mengambil alih dengan Kode OTP (One Time Password)

Injeksi SQL

Memasukkan kode berbahaya ke dalam basis data melalui SQL

E-mail Spam & Phishing

Mengelabui untuk mencuri data kartu kredit (CVC), password

Serangan DDoS

Membanjiri jaringan dan server dengan traffic, tujuan lag/lost

Domain Name

Typosquatting (plesetan), Cybersquatting (penyerobotan)

Man in the Middle (MITM)

Menyusup dalam komunikasi

Modus serangan dapat bervariasi tergantung pada situasi dan keadaan yang ditarget.

KASUS SERANGAN SIBER DI BERBAGAI DUNIA

1999 - NASA Cyber Attack
Seorang peretas berusia 15 tahun membobol sistem komputer NASA dan Pentagon, mencuri data sensitif dan menyebabkan gangguan selama 21 hari. Serangan ini menjadi peringatan dini tentang pentingnya keamanan siber, terutama bagi lembaga pemerintah.

2010 - Stuxnet Attack
Stuxnet adalah senjata siber canggih yang menargetkan program nuklir Iran. Dengan menginfeksi dan memanipulasi sistem kontrol industri, serangan ini menyebabkan kerusakan signifikan pada sentrifugal dan dengan kerugian biaya jutaan dolar.

2011 - PlayStation Network Attack
Peretas menyusup ke PlayStation Network Sony, mencuri informasi pribadi dari 77 juta akun pengguna dan menyebabkan pemadaman layanan selama 23 hari. Serangan ini mengakibatkan kerugian yang signifikan bagi Sony dan memicu tuntutan hukum dari para pengguna.

2014 - Yahoo Attack
Peretas yang disponsori oleh negara membobol Yahoo dan mencuri data dari sekitar 500 juta akun. Yahoo menunda pengungkapan pelanggaran tersebut, membuat pengguna rentan terhadap pencurian identitas dan serangan phishing.

2015 - Ukraine Power Grid Attack
Serangan siber ini menyebabkan pemadaman listrik di Ukraina bagian barat, termasuk sebagian besar Kyiv. Serangan ini dianggap sebagai serangan siber pertama yang berhasil yang menyebabkan pemadaman listrik pada jaringan nasional.

KASUS SERANGAN SIBER DI BERBAGAI DUNIA

2017 - WannaCry Ransomware
Serangan ransomware ini menginfeksi sekitar 230.000 komputer di lebih dari 150 negara, menyebabkan gangguan besar pada rumah sakit, bisnis, dan lembaga pemerintah. Serangan ini menyoroti bahaya ransomware dan pentingnya menambal kerentanan perangkat lunak.

2018 - Marriott Hotel Data Breach
formasi pribadi dari sekitar 500 juta tamu Marriott terekspos dalam pelanggaran data besar-besaran ini. Serangan ini terjadi selama beberapa tahun dan mengakibatkan kerugian finansial dan kerusakan reputasi Marriott.

2023 - MOVEit Software Attack
Kerentanan zero-day pada perangkat lunak transfer file MOVEit dieksploitasi oleh beberapa kelompok peretas, termasuk geng ransomware Cl0p. Serangan ini memengaruhi lebih dari 2.000 organisasi dan mengekspos data 60 juta orang, menjadikannya salah satu serangan siber terbesar dan paling merusak dalam sejarah.

2024 - Indonesia’s Data Center Attack
Pusat Data Nasional Sementara (PDNS) Indonesia mengalami serangan ransomware, mengganggu layanan publik dan berdampak pada lebih dari 200 lembaga pemerintah. Para peretas, menggunakan ransomware LockBit 3.0 Brain Chiper, mengenkripsi data dan meminta tebusan sebesar US$8 juta, tetapi akhirnya merilis kunci dekripsi secara gratis pada awal Juli.

2025 - Future cyber tttack
Serangan siber di masa depan diperkirakan akan menjadi semakin kompleks, memanfaatkan teknologi terdepan seperti kecerdasan buatan (AI) dan pembelajaran mesin untuk otomatisasi, penghindaran, dan serangan yang ditargetkan.

KASUS KEBOCORAN DATA DI INDONESIA (1)

38 MB data pengaduan KPAI [Okt 2021]

6 juta data pasien Rumah Sakit [Jan 2022]

1,3 juta data eHAC [Ags 2021]

2,3 juta data DPT 2014 [Mei 2020]

19 juta data BPJS Ketenagakerjaan [Mar 2023]

1,3 milyar data registrasi simcard [Sept 2022]

34 Juta data Passport [Jul 2023]

204,8 juta data DPT KPU [Dec 2023]

136 GB data Kemenko Perekonomian [Jun 2024]

kebocoran 6 juta data NPWP [Sep 2024]

OKT 2024
UU PDP DIJALANKAN

2020 | 2021 | 2022 | 2023 | 2024

272 Juta data BPJS Kesehatan [Mei 2021]

74 GB data Bank Indonesia [Jan 2022]

17 ribu data akun Ditjen Pajak [Mar 2022]

17 juta data pelanggan PLN [Ags 2022]

337 Juta data Disdukcapil [Jul 2023]

1.64 TB data dicuri dari situs Kemhan [Nov 2023]

186 Juta data KPU [Des 2023]

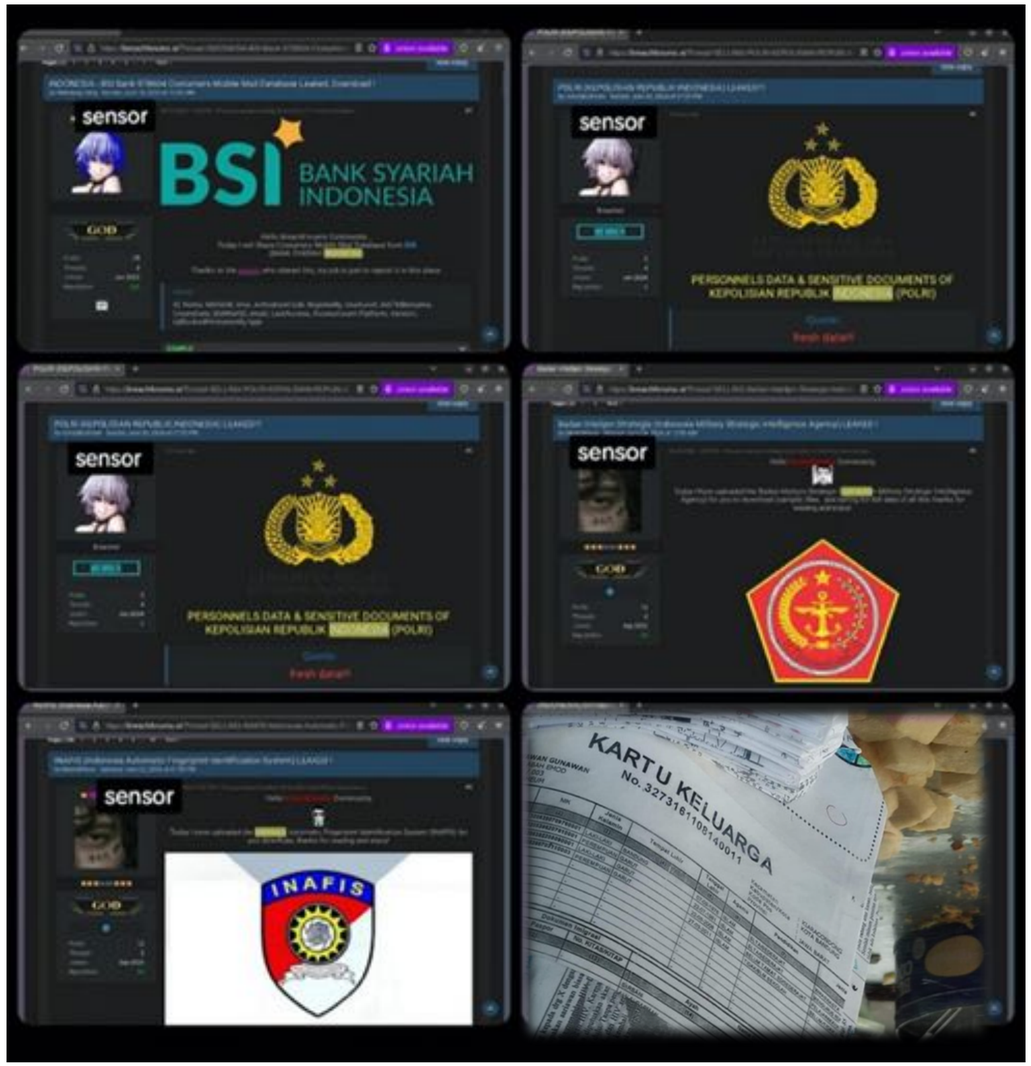
380 rb data pelanggan Biznet, 154 ribu pelanggan Biznet Gio [Mar 2024]

4,7 Juta Data ASN Diduga Bocor [Agustus 2024]

OKT 2022
UU PDP DISAHKAN

GOVERNMENT BUSINESS LAB
University of Indonesia

KASUS KEBOCORAN DATA DI INDONESIA (2)



Bjorka About Databases Contact

Databases Index

All databases owned by Bjorka that you can buy or download for free

FREE

341K Indonesian National Police Personnel Database

Bjorka • Sat Oct 04 2025

$10.000

6 MILION INDONESIA TAXPAYER IDENTIFICATION NUMBER (NPWP)

Bjorka • Fri Sep 13 2024

$5.000

217 MILLION SIAK DUKCAPIL MINISTRY OF HOME AFFAIRS OF INDONESIA

Bjorka • Thu Dec 28 2023

KERAWANAN FATAL YANG SELALU BERULANG

Bjorka About Databases Contact

Databases Index

Compressed	: 16 GB
Uncompressed	: 131 GB
Total Records	: 217,750,843
Breach Date	: Dec, 2023
Format	: CSV
Compromised Data	: NIK (ID CARD NO), Name, KK (Family Card No), Gender, DOB, Mother Maiden Name, Mother ID Card No, Father Name, Father ID CARD No, Address
Country	: Indonesia
File Sharing	: Private CDN
Price	: $5K

FREE

341K Indonesian National Police Personnel Database

Bjorka • Sat Oct 04 2025 • #indonesia

$5.000

217 MILLION SIAK DUKCAPIL MINISTRY OF HOME AFFAIRS OF INDONESIA

TAXPAYER IDENTIFICATION NUMBER (NPWP)

Bjorka • Fri Sep 13 2024

$5.000

217 MILLION SIAK DUKCAPIL MINISTRY OF HOME AFFAIRS OF INDONESIA

Bjorka • Thu Dec 28 2023

File Sharing : Private CDN
Price : FREE

SAMPLE

```
"PANGKAT","NAMA","TUGAS","HP","EMAIL"
"BRIPDA","A . MUHAMMAD YUSUF ","BANIT 23 UNITDALMAS SATSABHARA POLRES KENDARI POLDA
"AKP","A .IWAN TEJO SUNTONO ","PAUR YANUM SUBBAG UM BAG. KEMIN AKPOL LEMDIKPOL ",,
"BRIPKA","A A GD ALIT ARIAWAN ","BANIT 11 UNITLAKA SATLANTAS POLRES ENDE POLDA NTT
"BRIPKA","A A GD EDI PURNAMA ","BAMIN 1 SIWAS POLRES BANGLI POLDA BALI ","
"BRIGADIR","A A GEDE ADI PURNAMA, S.H. ","BANIT 4 UNIT 2 SUBDIT 2 DITRESNARKOBA POL
"AIPTU","A A GEDE JAYA ","BRIGADIR POLRES GIANYAR POLDA BALI(PENGUASAN PD BNNK GIAN
"BRIPDA","A A ISTRI ARISTYA DEVI ","BA POLDA KALTENG ","81936215629",
"AIPTU","A A KETUT ADI RAWA,S.H ","BHAYANGKARA OPERASIONAL PELAKSANA LANJUTAN BIDAN
"AKBP","A A KETUT AGUNG RUMASIA, S.H. ","PAMEN BAINTELKAM POLRI(PENGUASAN PD DIN)
"AKBP","A A KETUT AGUNG RUMASIA, S.H. ","PAMEN BAINTELKAM POLRI(PENGUASAN PD DIN)
```

DOWNLOAD

```
https://netleaks.net/idnpolice.zip
```

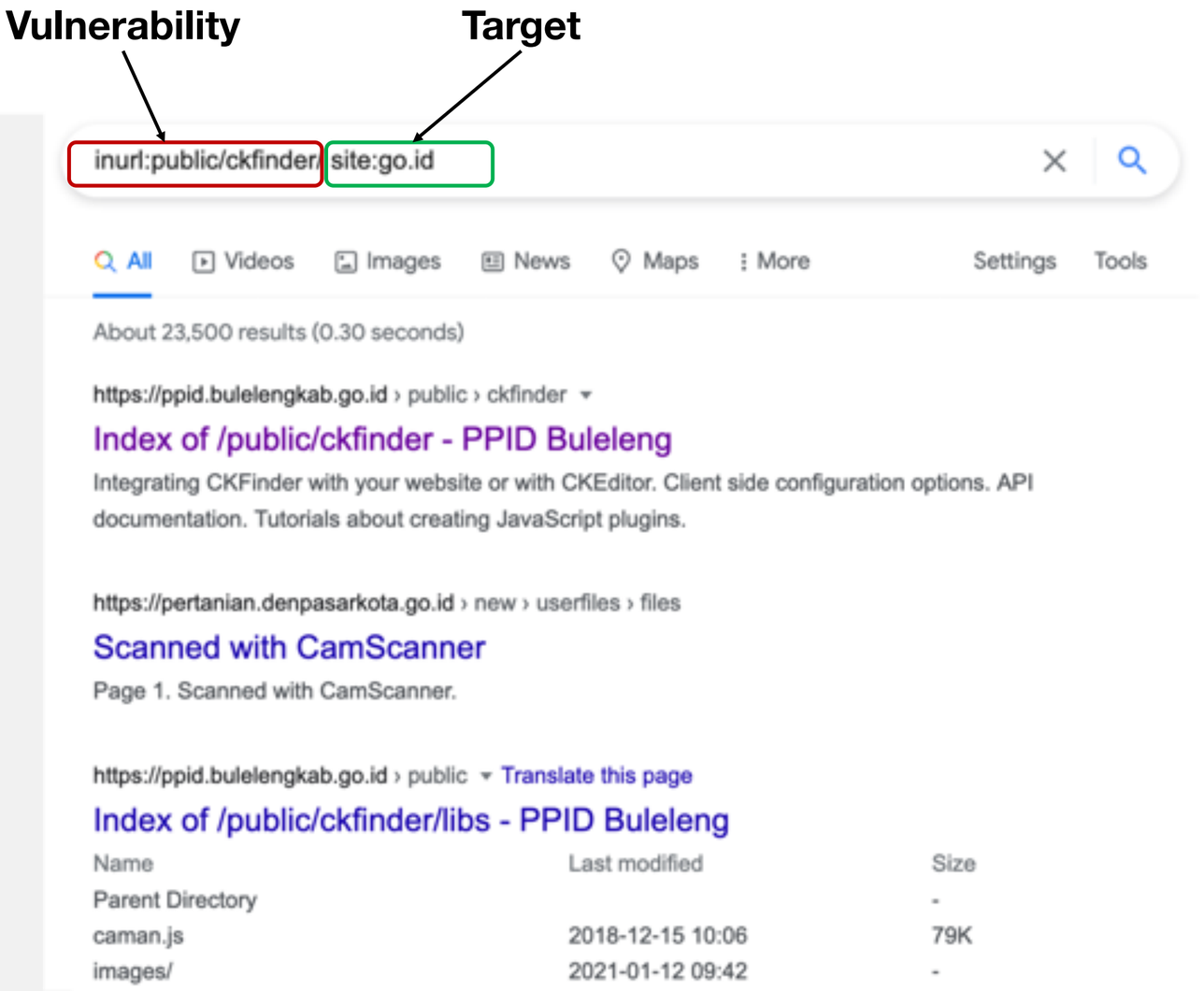
CLEAN SAMPLE

```
"NIK","NAMA_LGKP","JENIS_KLMN","TMPT_LHR","TGL_LHR","NO_AKTA_LHR","GOL_DRH","AGAM
"1101021712690001","USNIIAL. US","1","SUAK GERINGGENG","1969-12-17 00:00:00",NULL,
"1101021712720001","SYAURAWI","1","KP PAYA","1972-12-17 00:00:00",NULL,"4","1","72",
"1101021712800001","KHAIRIL AZMI","1","SIMPANG LHEE","1980-12-17 00:00:00",NULL,"1
"1101021712890001","SUHELMI","1","LADANG TUHA","1989-12-17 00:00:00",NULL,"13","1",
"1101021712920001","IRFANDI","1","KOTA FAJAR","1992-12-17 00:00:00",NULL,"3","1",
"1101021712930002","WIANNA FAJRINAL","1","LADANG TENGAH ","1993-12-17 00:00:00","
"1101021712950001","WAN NUR AMIN","1","TAPAKTUAN","1995-12-17 00:00:00",NULL,"13",
"1101021712980002","NURHAN FAUZI","1","LIMAU PURUT","1998-12-17 00:00:00",NULL,"13",
"1101021801000001","ZAINI","1","POLO IE I","2000-01-18 03:00:00","1101-LT-2408201
"1101021801040002","FADILAH GIOVANI DHOSAM","1","TAPAKTUAN","2004-01-18 00:00:00",
"1101021801050001","SATRIA FALDAN","1","KRUENG BATU","2005-01-18 02:00:00","1101-L
"1101021801050002","FATHURRAZI","1","PASIE KUALA BA'U","2005-01-18 00:00:00","1101
"1101021801070001","DAHRIAL","1","KRUENG BATU","2007-01-18 00:00:00","124/02/L/01
"1101021801080001","IHSAN KAMIL","1","PASIE KUALA BA'U","2008-01-18 02:00:00","110
"1101021801090001","IHAFIZH","1","SUAK GERINGGENG","2009-01-18 02:00:00","1101-L
"1101021801120001","AMALUL AMRI","1","KAMPUNG PAYA","2012-01-18 00:00:00","1101-LT
"1101021801130001","JAMALUL YAZIAN","1","ALURMAS","2013-01-18 00:00:00","1101-LT-1
"1101021801140001","MUHAMMAD FAZIL HUSEN","1","KOTAFAJAR","2014-01-18 01:00:00","1
"1101021801140002","FAJAR JASMANDI","1","ALUR NAS","2014-01-18 12:50:00","1101-LT-
"1101021801150001","AHMAD WILDAN","1","TAPAKTUAN","2015-01-18 00:00:00","1101-LT-1
"1101021801150001","M. SYARIF","1","KUDAI PADANG","1955-01-18 00:00:00",NULL,"13",
"1101021801740002","ADNAN","1","KAMPUNG TINGGI","1974-01-18 00:00:00",NULL,"13","1
"1101021801760004","TGK. SAIFUL B","1","POLO IE I","1976-01-18 00:00:00",NULL,"13"
```

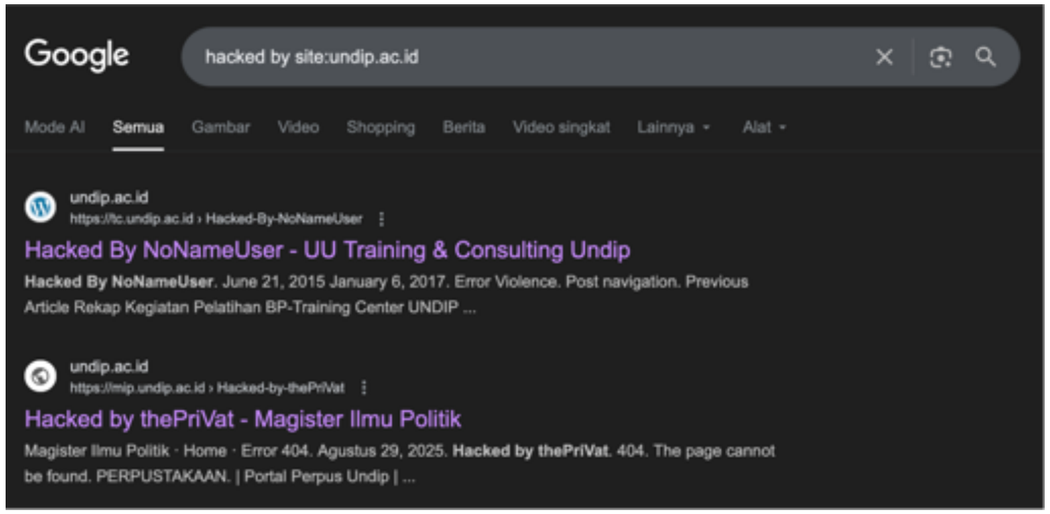
HACKING IN A MINUTE

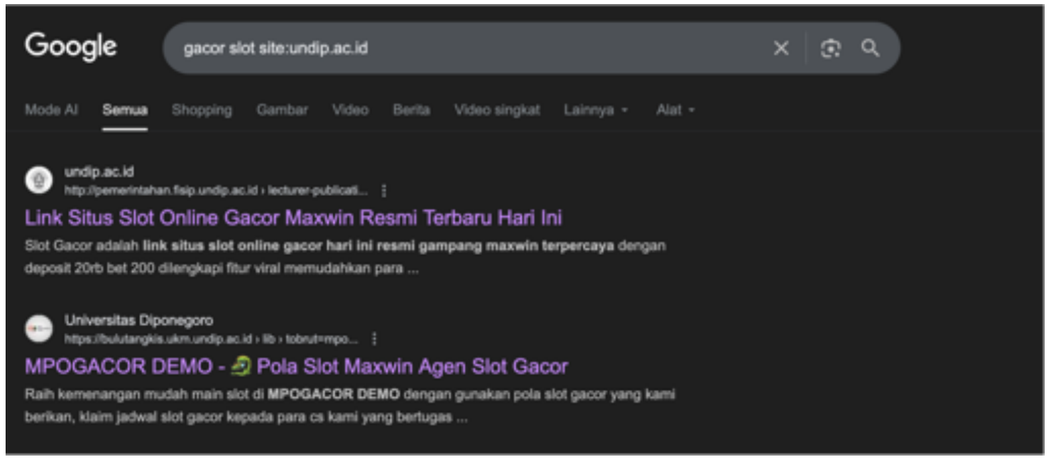
Google SQL Dorks

```
"index of" "siri"
"index of" "plugins/wp-rocket"
intitle:"index of" secrets.yml
intitle:"index of /" "*key.pem"
intitle:"index of" "admin/sql/"
intext:"index of /" "config.json"
index of .svn/text-base/index.php.svn-base
intitle:"index of" admin.tar
inurl:/servicedesk/customer/user/login
Dork: "Index of" "upload_image.php"
Dork: "index of" "Production.json"
index.of.?.frm
```



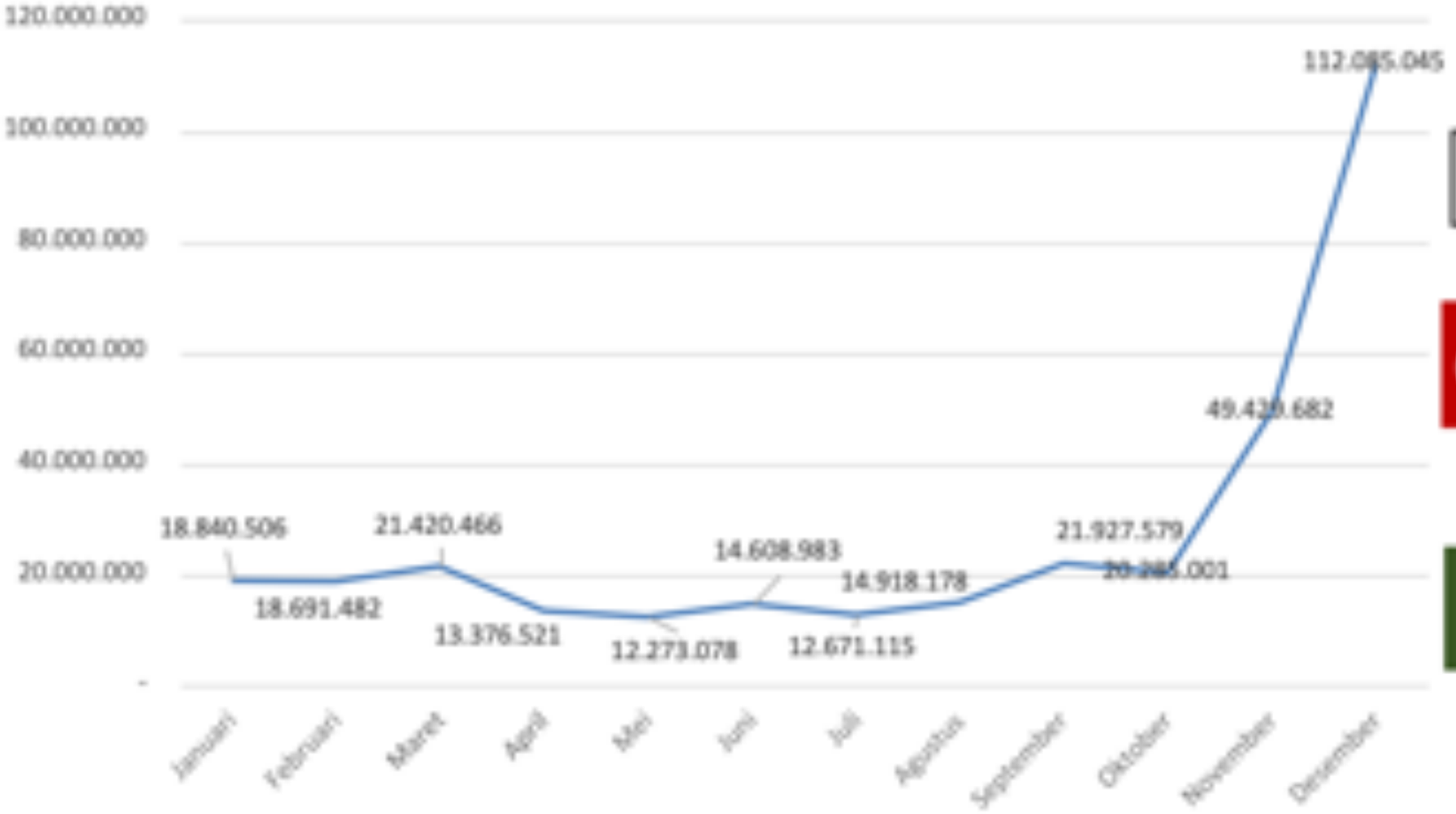
HACKING IN A MINUTE





ANCAMAN SIBER DI INDONESIA

ANOMALI TRAFIK INTERNET
Periode 1 Januari 2024 – 31 Desember 2024



330.527.636

ANOMALI TRAFIK

TOP #3 – JENIS ANOMALI TRAFIK

68,76%

223.978.545
MALWARE ACTIVITY

63.154.192
TROJAN ACTIVITY

19,11%

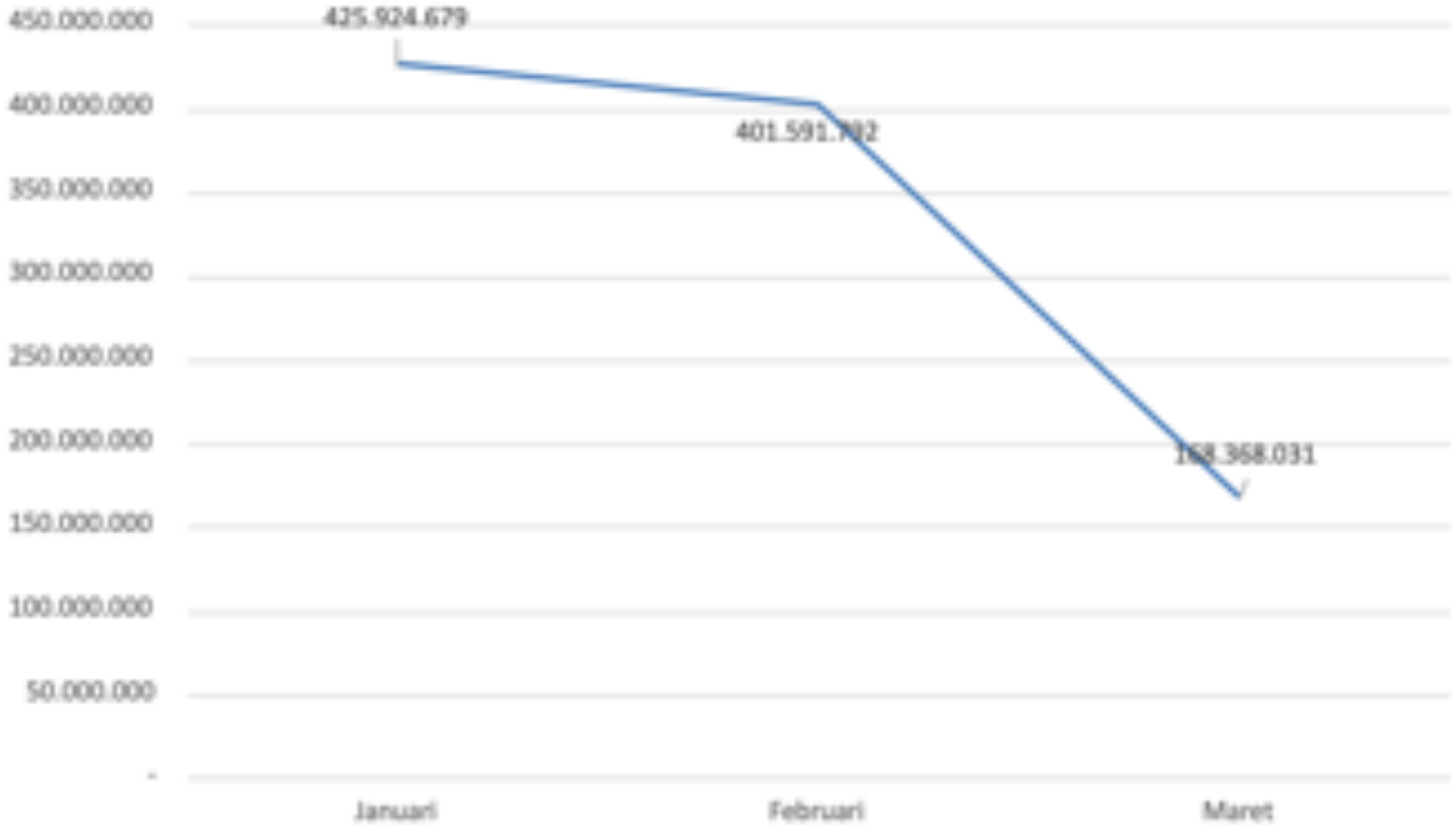
4,21%

13.915.451
UNAUTHORIZED ACCESS AND SYSTEM MISCONFIGURATION

Sumber : BSSN, 2024

ANCAMAN SIBER DI INDONESIA

ANOMALI TRAFIK INTERNET
Periode 1 Januari 2025 – 31 Maret 2025



995.902.462

ANOMALI TRAFIK

TOP #3 – JENIS ANOMALI TRAFIK

91,55% — 816.546.119 MALWARE ACTIVITY

6,19% — 63.783.577 UNAUTHORIZED ACCESS AND SYSTEM MISCONFIGURATION

0,76% — 7.603.420 EXPLOIT

Sumber : BSSN, 2025

SERANGAN SIBER SETIAP WAKTU

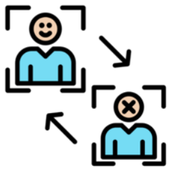
SERANGAN SIBER DI MASA DEPAN

- **Peningkatan Serangan Ransomware yang Lebih Canggih**
  Ransomware akan tetap menjadi ancaman utama, dengan taktik yang semakin canggih seperti *multi-extortion* dan layanan *ransomware-as-a-service (RaaS)*. Sasaran tidak hanya terbatas pada perusahaan besar, tetapi juga meluas ke usaha kecil dan menengah.

- **Serangan yang Lebih Tertarget dan Berbasis AI**
  Penyerang akan semakin memanfaatkan kecerdasan buatan (AI) untuk mengotomatisasi serangan, mengidentifikasi kerentanan, dan menghindari deteksi. Serangan akan disesuaikan secara spesifik terhadap korban, sehingga meningkatkan kemungkinan keberhasilan.

- **Peningkatan Serangan terhadap Infrastruktur Kritis**
  Infrastruktur penting seperti jaringan listrik, sistem transportasi, dan layanan kesehatan akan menjadi target utama serangan siber karena dampaknya yang signifikan terhadap masyarakat dan ekonomi.

- **Eksploitasi Kerentanan Perangkat IoT**
  Dengan meningkatnya penggunaan perangkat Internet of Things (IoT), penyerang akan memanfaatkan celah keamanan pada perangkat tersebut untuk memperoleh akses ke jaringan dan data.



- **Deepfake dan Disinformasi**
  Teknologi *deepfake* akan semakin canggih, memungkinkan penyerang membuat video dan audio palsu yang meyakinkan untuk menyebarkan disinformasi, memanipulasi opini publik, dan merusak reputasi.

SERANGAN SIBER DI MASA DEPAN

STRATEGI PENCEGAHAN DAN MITIGASI (1)

- **Keamanan Zero Trust**
  Menerapkan model keamanan *zero trust*, yang berarti tidak ada pengguna atau perangkat yang secara otomatis dipercaya, bahkan di dalam jaringan internal. Ini mencakup penggunaan autentikasi multi-faktor, segmentasi jaringan, dan kontrol akses yang ketat.
- **Pemantauan dan Deteksi Ancaman Lanjutan**
  Menggunakan teknologi keamanan terbaru seperti *User and Entity Behavior Analytics (UEBA)*, *machine learning*, dan intelijen ancaman untuk mendeteksi serta merespons ancaman secara proaktif.
- **Perencanaan dan Latihan Tanggap Insiden**
  Menyusun dan secara berkala menguji rencana tanggap insiden yang komprehensif untuk memastikan kesiapan menghadapi serangan siber.
- **Keamanan Rantai Pasokan**
  Memastikan bahwa vendor dan mitra bisnis juga menerapkan praktik keamanan siber yang kuat guna mengurangi risiko serangan melalui rantai pasokan.

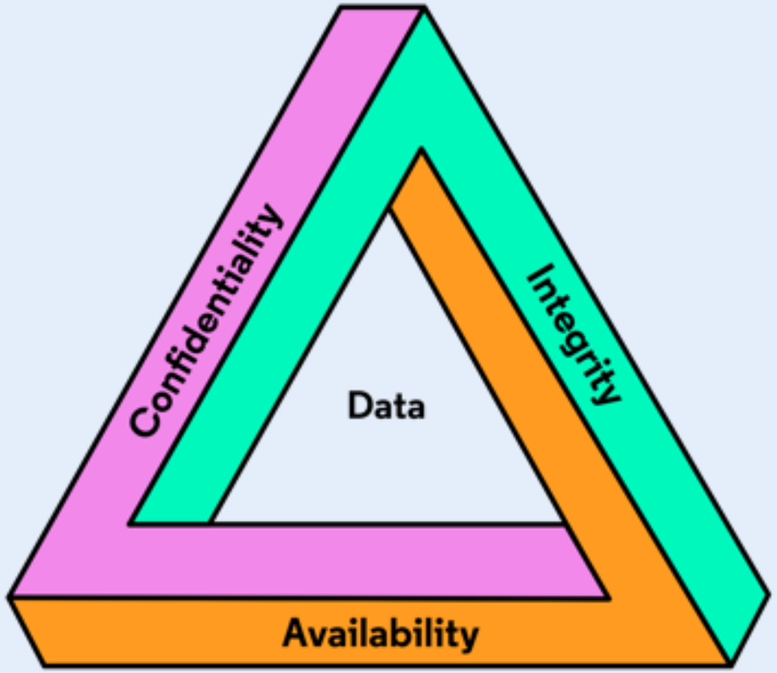
STRATEGI PENCEGAHAN DAN MITIGASI (2)

- **Pelatihan Kesadaran Keamanan Siber**
  Memberikan pelatihan berkelanjutan kepada personel tentang ancaman siber terkini, cara mengenalinya, serta pentingnya menerapkan praktik keamanan yang baik.
- **Kolaborasi dan Pertukaran Informasi**
  Berpartisipasi dalam inisiatif pertukaran informasi ancaman siber dengan organisasi lain dan pemerintah untuk meningkatkan kesadaran situasional dan memperkuat pertahanan kolektif.
- **Perlindungan Infrastruktur Kritis**
  Meningkatkan investasi dalam keamanan siber untuk melindungi infrastruktur penting, termasuk pembaruan perangkat lunak dan perangkat keras secara rutin, pemantauan ketat, dan sistem redundansi.
- **Regulasi dan Standar Keamanan**
  Mendorong pengembangan dan penerapan regulasi serta standar keamanan yang lebih ketat guna memastikan organisasi dan individu mengambil langkah-langkah yang diperlukan untuk melindungi diri dan data mereka.

CYBER SECURITY

SEKUMPULAN alat, kebijakan, konsep keamanan, langkah pengamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan, dan teknologi yang dapat digunakan untuk melindungi lingkungan siber serta aset organisasi dan pengguna. (ITU, Recommendation ITU-T X.1205)

Tujuan Utama Pelindungan di ruang siber



include authenticity and non-repudiation (ISO/IEC 27001:2022)

- Confidentiality/ Kerahasiaan
  - Menjamin bahwa sistem tidak dapat diakses atau terbuka bagi individu, entitas, atau proses yang tidak berwenang.
- Integrity/ Keutuhan
  - Menjaga keakuratan dan kelengkapan aset.
- Availability/ Ketersediaan
  - Memastikan bahwa sistem dapat diakses dan digunakan oleh entitas yang berwenang saat dibutuhkan.
- Authenticity/ Keaslian
  - Memastikan bahwa informasi, komunikasi, atau entitas benar-benar berasal dari sumber yang sah dan tepercaya.
- Non-repudiation/ Nir-Penyangkalan
  - Menjamin bahwa pengirim pesan tidak dapat menyangkal telah mengirimkan pesan tersebut, dan penerima tidak dapat menyangkal telah menerimanya, dengan menggunakan teknologi seperti *Public Key Infrastructure* (PKI).

REGULASI DI INDONESIA

UU Nomor 11 Tahun 2008 dan UU Nomo 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik

UU Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik

UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

Perpres Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik

Perpres Nomor 39 Tahun 2019 tentang Satu Data Indonesia

Perpres Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital

Perpres Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber

Peraturan BSSN Nomor 8 Tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik

Peraturan BSSN Nomor 4 Tahun 2021 tentang Manajemen Keamanan SPBE dan Standar Teknis dan Prosedur Keamaanan SPBE

Peraturan Badan Siber dan Sandi Negara Nomor 7 Tahun 2023 Tentang Identifikasi Infrastruktur Informasi Vital

Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 Tentang Pengelolaan Insiden Siber

Peraturan Badan Siber dan Sandi Negara Nomor 2 Tahun 2024 Tentang Manajemen Krisis Siber

SNI ISO/IEC 27001:2013 KE 27001:2022

ISO 27001:2013

Judul

Information technology — Security techniques — Information security management systems — Requirements

Kontrol

114 Kontrol dikelompokkan ke 14 Domain Kontrol

Annex A : Information Security Controls
(ISO 27002)

ISO 27001:2022

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

93 Kontrol dikelompokkan ke 4 Kategori/Tema

- 58 Kontrol tetap
- 24 kontrol digabung
- 11 kontrol baru

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains

5 Atribut

Membantu membuat pandangan yang berbeda sesuai tema kontrol sehingga dapat meningkatkan penilaian dan penanganan risiko

37 ORGANIZATIONAL CONTROL

5.1	Policies for information security
5.2	Information security roles and responsibilities
5.3	Segregation of duties
5.4	Management responsibilities
5.5	Contact with authorities..
5.6	Contact with special interest groups
5.7	Threat intelligence - New
5.8	Information security in project management
5.9	Inventory of information and other associated assets.
5.10	Acceptable use of information and other associated assets
5.11	Return of assets
5.12	Classification of information
5.13	Labelling of information
5.14	Information transfer
5.15	Access control
5.16	Identity management
5.17	Authentication information
5.18	Access rights
5.19	Information security in supplier relationships.
5.20	Addressing information security within supplier agreements
5.21	Managing information security in the ICT supply chain
5.22	Monitoring, review and change management of supplier services
5.23	Information security for use of cloud services - New
5.24	Information security incident management planning and preparation.
5.25	Assessment and decision on information security events
5.26	Response to information security incidents
5.27	Learning from information security incidents
5.28	Collection of evidence
5.29	Information security during disruption
5.30	ICT readiness for business continuity - New
5.31	Legal, statutory, regulatory and contractual requirements
5.32	Intellectual property rights
5.33	Protection of records
5.34	Privacy and protection of PII
5.35	Independent review of information security
5.36	Compliance with policies, rules and standards for information security
5.37	Documented operating procedures

8 PEOPLE CONTROL

6.1	6.2	6.3	6.4	6.5	6.6	6.7	6.8
Screening	Terms & condition	Information security awareness, education and training	Disciplinary process	Responsibilities after termination or change of employment	Confidentiality or non-disclosure agreements	Remote working	Information security event reporting

14 PHYSICAL CONTROL

7.1	Physical security perimeters
7.2	Physical entry
7.3	Securing offices, rooms and facilities
7.4	Physical security monitoring - New
7.5	Protecting against physical and environmental threats
7.6	Working in secure areas
7.7	Clear desk and clear screen
7.8	Equipment siting and protection

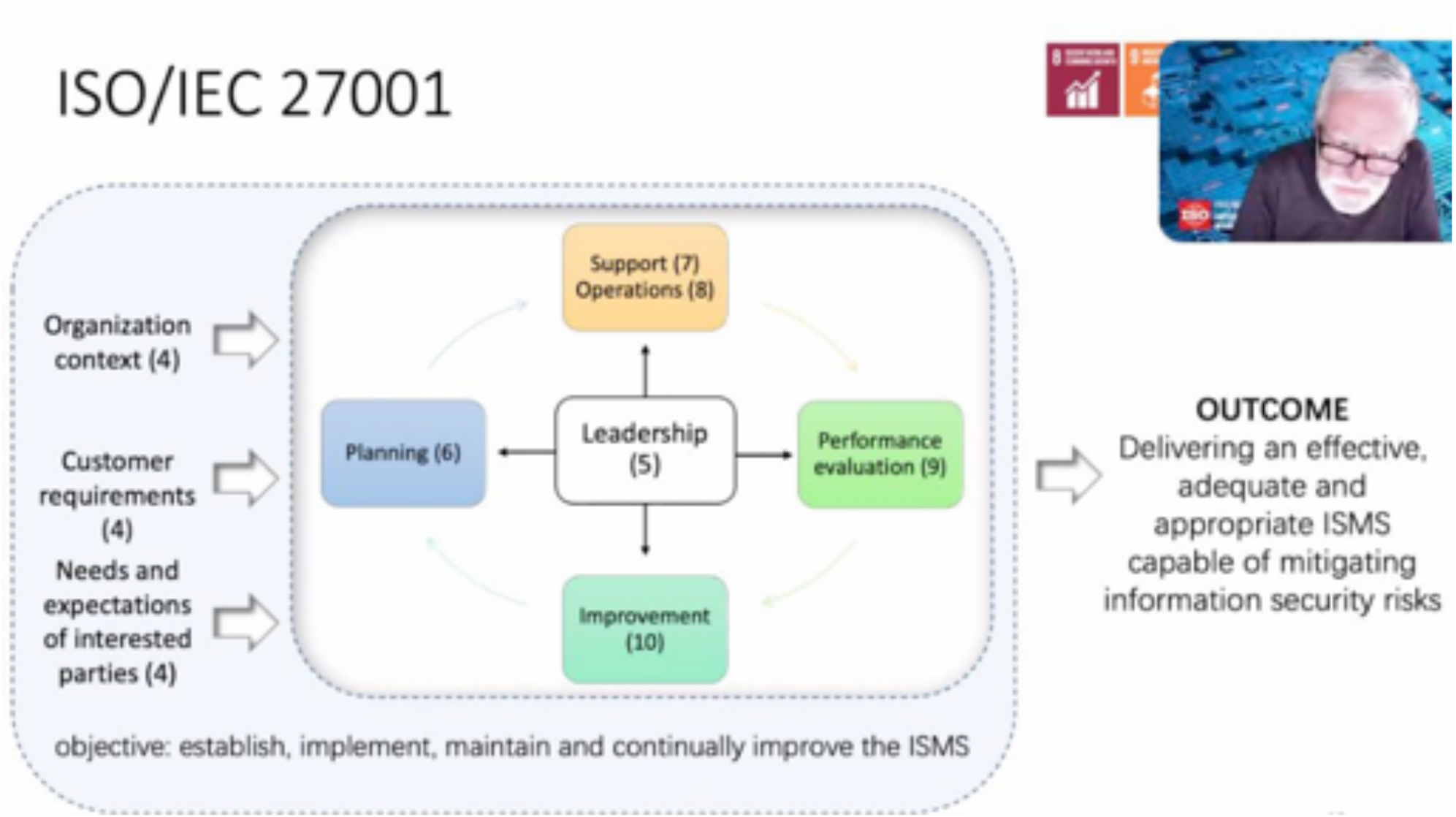
7.9	Security of assets off-premises
7.10	Storage media
7.11	Supporting utilities
7.12	Cabling security..
7.13	Equipment maintenance
7.14	Secure disposal or re-use of equipment.

34 TECHNOLOGY CONTROL

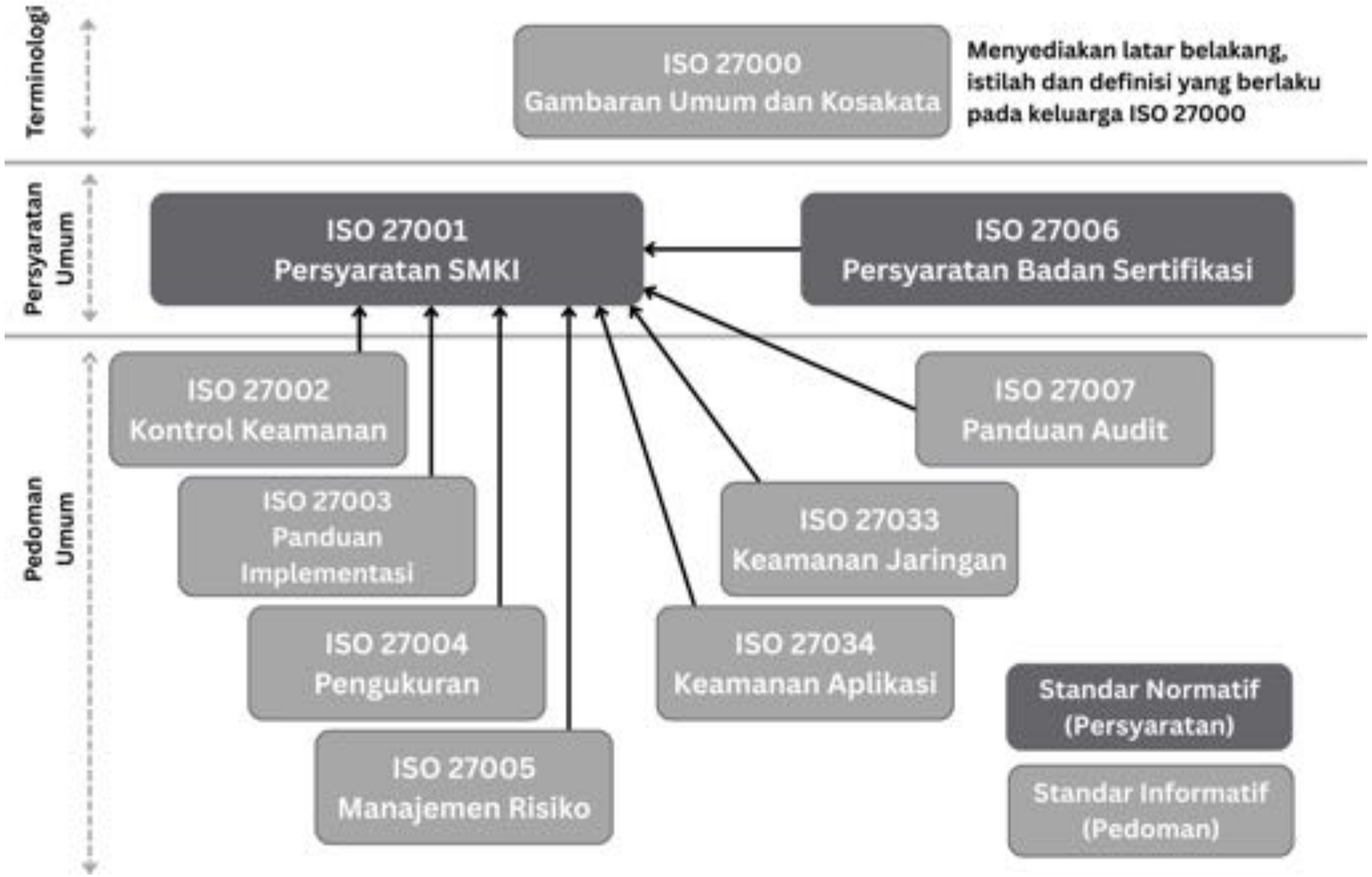
8.1	User endpoint devices
8.2	Privileged access rights
8.3	Information access restriction
8.4	Access to source code
8.5	Secure authentication
8.6	Capacity management
8.7	Protection against malware
8.8	Management of technical vulnerabilities
8.9	Configuration management - New
8.10	Information deletion - New
8.11	Data masking - New
8.12	Data leakage prevention – New
8.13	Information backup
8.14	Redundancy of information processing facilities
8.15	Logging
8.16	Monitoring activities - New
8.17	Clock synchronization
8.18	Use of privileged utility programs
8.19	Installation of software on operational systems
8.20	Networks security
8.21	Security of network services
8.22	Segregation of networks
8.23	Web filtering - New
8.24	Use of cryptography
8.25	Secure development life cycle
8.26	Application security requirements
8.27	Secure system architecture and engineering principles
8.28	Secure coding - New
8.29	Security testing in development and acceptance
8.30	Outsourced development
8.31	Separation of development, test and production environments
8.32	Change management
8.33	Test information
8.34	Protection of information systems during audit testing

11 NEW CONTROL

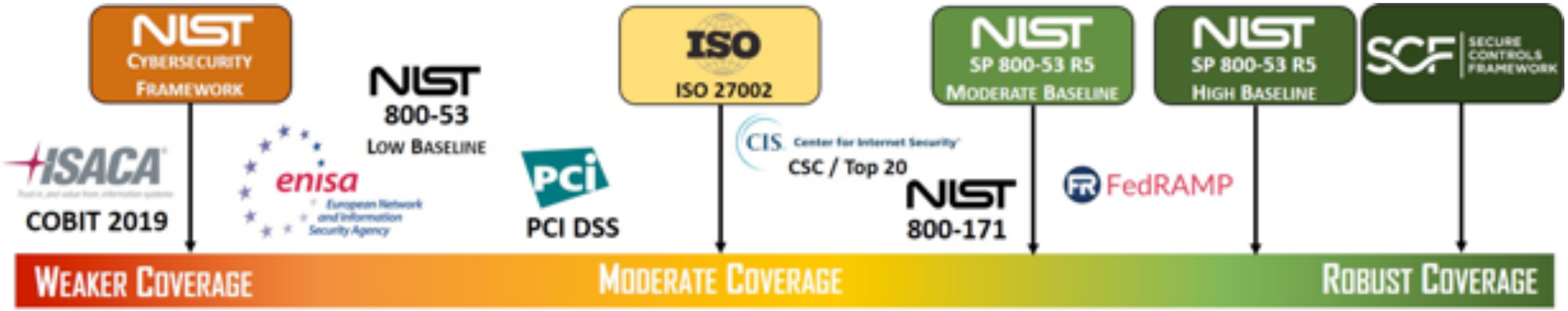
TUJUAN UTAMA SERTIFIKASI KEAMANAN



KERANGKA KERJA KEAMANAN SIBER ISO 27001 FAMILY

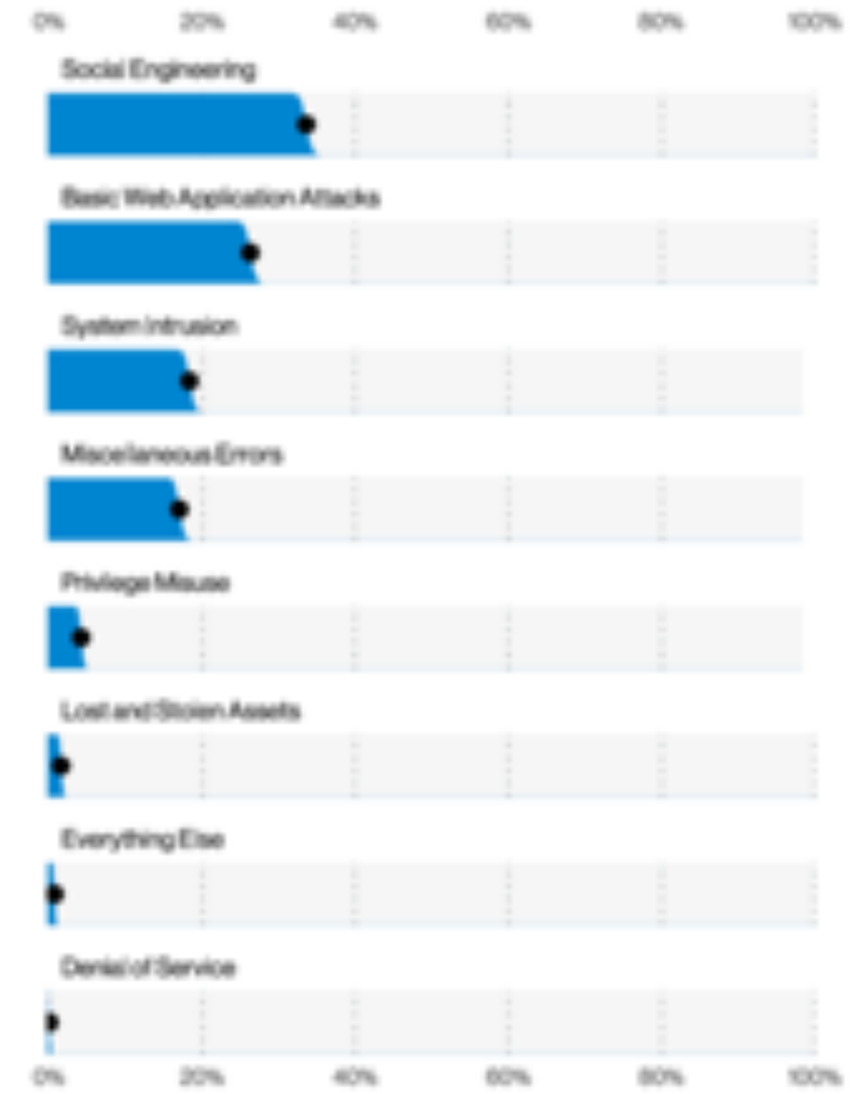


KERANGKA KERJA KEAMANAN SIBER



Kerangka kerja keamanan siber adalah suatu struktur yang dibutuhkan oleh organisasi agar terlindungi dari serangan siber dengan memberikan pedoman dalam proses implementasinya sehingga memenuhi persyaratan standar keamaanan

YOU ARE AS STRONG AS YOUR WEAKEST LINK



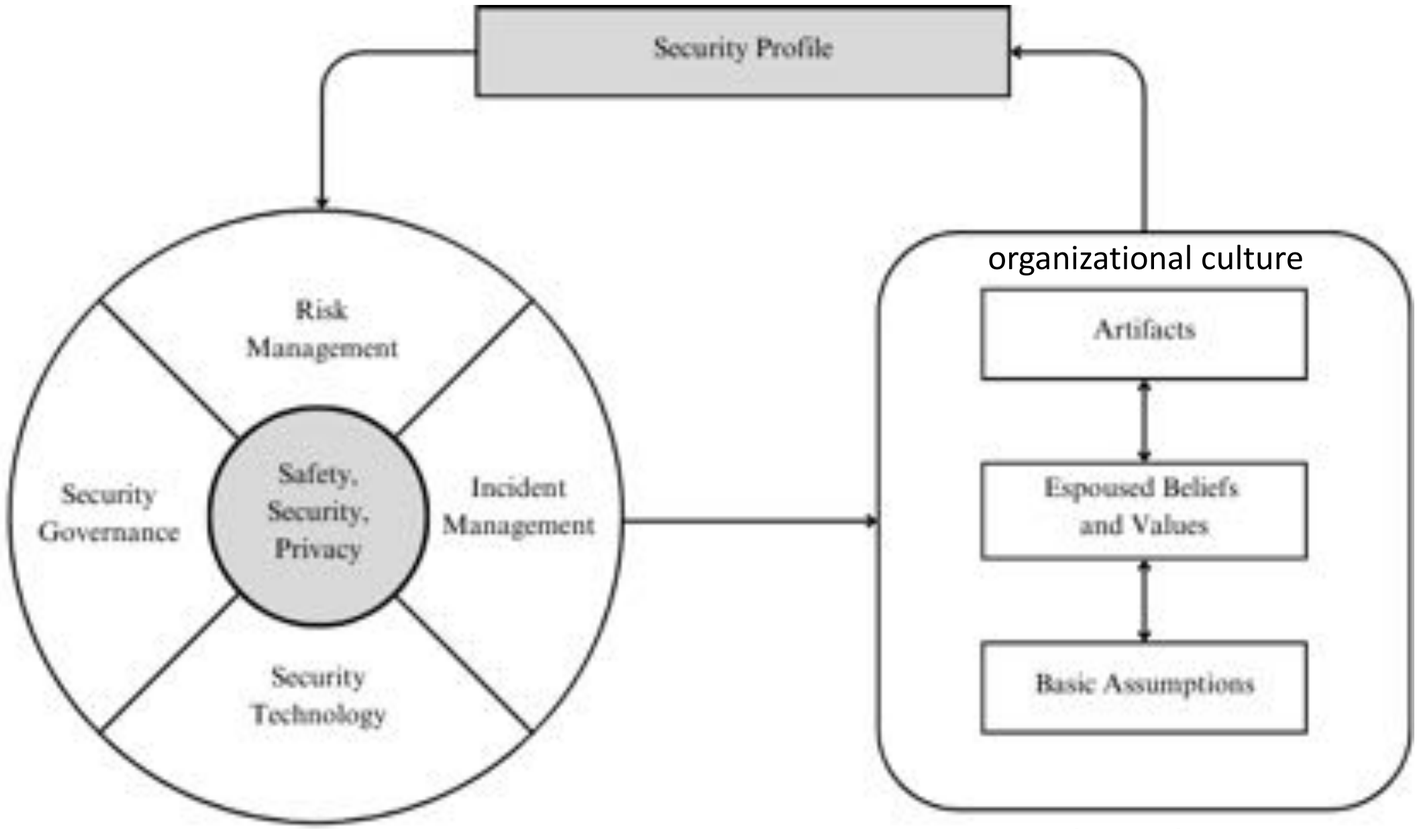
Social Engineering	• Memanfaatkan psikologi pengguna untuk memperoleh akses • 80% berasal dari pihak eksternal dengan metode phising
Basic Web Application Attack	• Serangan sederhana pada aplikasi web yang rentan • 3,3 Triliun percobaan akses login secara brute force attack
System Intrusion	• Serangan kompleks menggunakan malware dan teknik hacking • 99% metode ini digunakan untuk menyebarkan ransomware
	• aktifivitas yang tidak dikehendaki menyebabkan kerawanan • 52% karena miskonfigurasi sistem sehingga data personal dapat dicuri
	• Penyalahgunaan akses kontrol seperti administrator • 30% insiden ini dapat diketahui setelah beberapa bulan/tahun
	• Aset informasi hilang atau ditempatkan pada lokasi yang salah • Dapat disebabkan oleh perangkat yang dicuri
Deniel of Service	• Menyerang pada ketersediaan akses pada jaringan dan sistem • Serangan ini sulit diprediksi karena dilakukan secara terdistribusi
Everything Else	• Serangan lainnya • Contoh serangan adalah skimmer

95%

of Breaches are Caused by Human Error

Sumber : 2021 Data Breach Investigation Report (Verizon)

AGILE CYBERSECURITY FRAMEWORK



Metode *Agile* 1: DSDM

Metode *Agile* 2: FDD

Karakteristik

Art 1: Adaptif dan Modular
Menekankan pada adaptasi standar global terhadap budaya lokal dan komponen modular

Art 2 : Tangkas dan Terintegrasi
Menekankan pada kemampuan adaptasi implementasi keamanan siber dalam setiap perubahan dan terintegrasi dalam budaya organisasi

Art 3: Ketahanan dan Berorientasi Tujuan
Menekankan pada perbaikan berkelanjutan dalam mencapai tujuan organisasi yang berkembang

Source :
E. Y. Handri, D. Indra Sensuse, and A. Tarigan, “Developing an Agile Cybersecurity Framework With Organizational Culture Approach Using Q Methodology,” *IEEE Access*, vol. 12, pp. 108835–108850, 2024, doi: 10.1109/ACCESS.2024.3432160.

THANK YOU

yon.handri@bssn.go.id
eko.yon@ui.ac.id
https://frayas.web.id
https://www.youtube.com/@frademy

“There’s no silver bullet with cybersecurity, a layered defense is the only viable option”