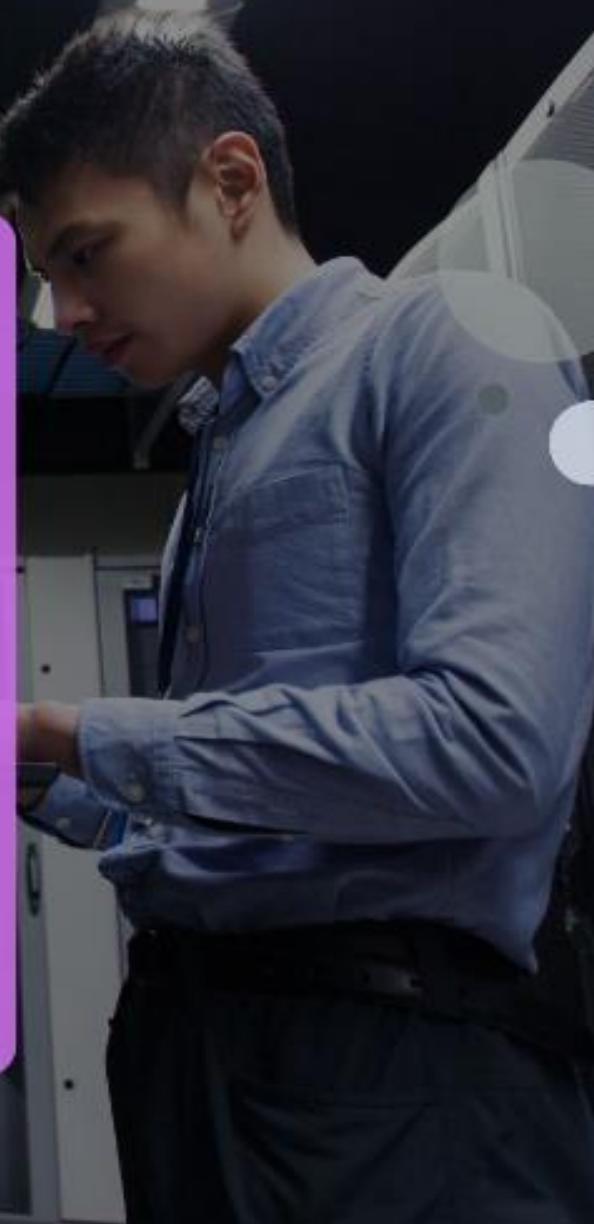


Webinar Inixindo Jogja

Meningkatkan Keamanan Pusat Data: Melindungi Aset Digital di Era Ancaman Siber yang Semakin Canggih



Andrian The

andrian@inixindojogja.co.id

Instruktur Inixindo Jogja bidang:

- IT Governance / Management
- Cyber Security
- Secure Software Design
- Secure Software Development
- Certified Information Systems Auditor

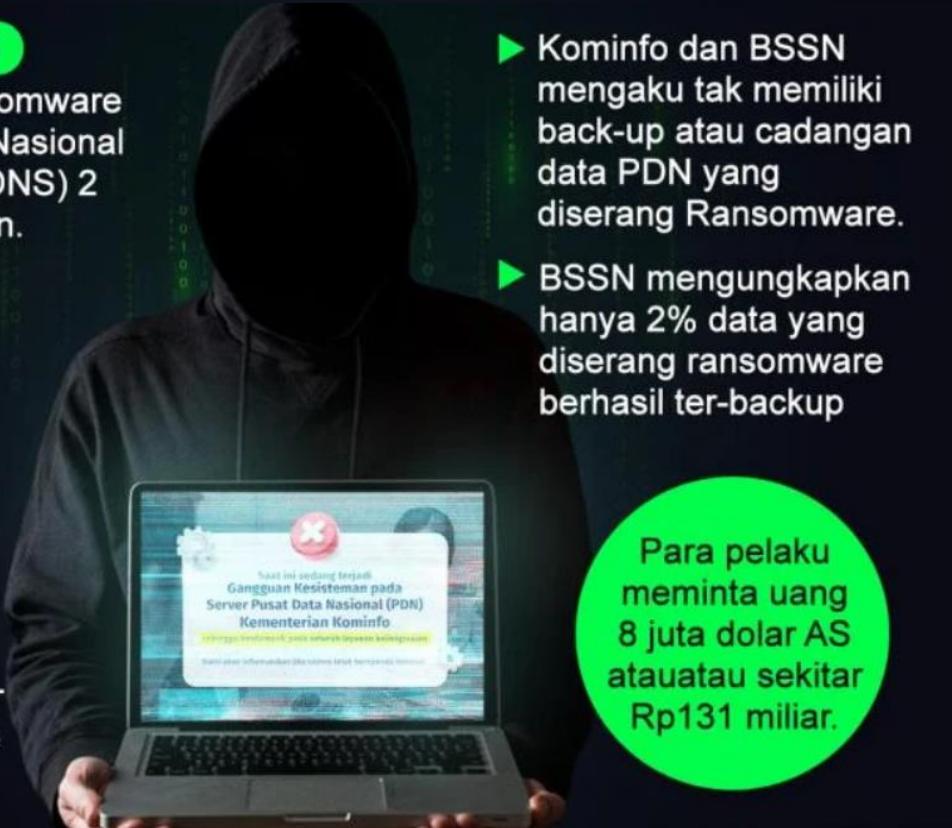


PDNS 2 Diserang Ransomware

28 JUNI 2024

Serangan ransomware di Pusat Data Nasional Sementara (PDNS) 2 menjadi sorotan.

Ransomware adalah jenis perangkat perusak yang mencegah pengguna mengakses sistem, baik dengan mengunci layar sistem atau file pengguna.



SUMBER iNews.id • NASKAH Dini Listiyani • INFOGRAFIS Johan

FAKTA-FAKTA BRAIN CIPHER: HACKER YANG BOBOL PDNS 2 DI SURABAYA

1. Serangan yang Menghebohkan

Pada 20 Juni 2024, Brain Cipher melumpuhkan PDNS 2 dengan ransomware, mengunci data dari 282 institusi dan mengganggu layanan e-KTP, SIKDIS, dan SIM Nasional.

2. Modus Operandi

Brain Cipher menggunakan ransomware untuk menyerang dengan manfaatkan kerentanan di Windows Defender, memungkinkan mereka mengakses dan mengenkripsi data di PDNS 2.

INFOGRAFIK: FIAN/PRMN, TEKS: MITHA PARADILLA RAYADI/PRMN

RANSOMWARE BRAIN CIPHER KASIH KEY PDNS GRATIS

brain cipher

infokab
More important than money, only honor.

We want to make a public statement.

This Wednesday, we'll give you the keys for free. We hope that our attack made it clear to you how important it is to finance the industry and recruit qualified specialists.

Our attack did not carry a political context, only a pentest with post payment.

Citizens of Indonesia, we apologize for the fact that it affected everyone.

We also ask for public gratitude and confirmation that we have consciously and independently made such a decision.

If the government representation, considers it wrong to thank the hacker. You can do it privately at the post office.

p.s.

We leave a monero wallet for donations, we hope that by Wednesday we will get something. (And we repeat again: we will give the keys absolutely free of charge and on our own initiative.)

42mSIK7EWq4TSKXu6FkDiPQwsnk3uNBhMwN71SrZuuJtk6TPpAACSLLeAofaYuKvhqz
2RcCNVeHWPtzjQXYIRs79gLfPH

p.s.s.

On Wednesday, we will prove that we keep our word.

Hacker Iba, Brain Cipher Bakal Kasih Kunci Pemulihan Sistem PDNS Secara Gratis

Foto: X @stealthmole_int

PERETASAN PADA PDNS 2 YANG DIKELOLA TELKOMSIGMA TELAH BERLANGSUNG SELAMA 12 HARI



"Kami membuka donasi dalam bentuk monero. Kami harap pada Rabu (2/7/2024) akan berbuat sesuatu. Kami ulangi, kami akan memberikan key sepenuhnya dan (keputusan) ini murni inisiatif kami," tulis terduga Brain Cipher Ransomware, dikutip dari postingan perusahaan intelijen siber, Fusion Intelligence Center StelathMole di X (Twitter)

Efek lumpuhnya pusat data, sebanyak database

282

institusi pemerintah pusat dan daerah, kementerian lembaga mengalami gagal akses via cloud

Kementerian Komunikasi dan Informatika (Kominfo) belum memberi pernyataan terkait hal ini. Direktur Jenderal Aplikasi Informatika (Aptika) Semuel Abrijani Pangerapan belum merespons permintaan atas komentar

Kelompok ini berharap peretasan PDNS tersebut mendorong pendanaan dan SDM yang lebih layak di sektor teknologi ini

INDICATOR OF COMPROMISE BRAIN CIPHER RANSOMWARE

RILIS : 27 JUNI 2024

No	Indicator Of Compromise	Hash	File	Path
1.	c60a0b99729eb6d95c2d9f8b76b9714411a3a751	SHA1	Win_old.exe	C:\User\itadmin\music\
2.	9c5698924d4d1881efaf88651a304cb3	MD5	Win_old.exe	C:\User\itadmin\music\
3.	935c0b39837319fd4571aa800b67d997b79c3198	SHA1	Win.exe	Any Path
4.	448f1796fe8de02194b21c0715e0a5f6	MD5	Win.exe	Any Path

13.	131.253.33.203	IPv4
14.	184.25.191.235	IPv4
15.	20.99.133.109	IPv4
16.	20.99.186.246	IPv4
17.	204.79.197.203	IPv4

- Reverse Engineering Ransomware Brain Cipher penyerang PDN:
<https://blog.compactbyte.com/2024/07/01/reverse-engineering-ransomware-brain-cipher-penyerang-pdn/>
- Reverse Engineering Dekriptor Babuk untuk PDN:
<https://blog.compactbyte.com/2024/07/03/reverse-engineering-dekriptor-babuk-untuk-pdn/>



Josua M Sinambela

DFIR Team BSSN found LockBit in Windows (use Salsa20 Algoritma), we identified from Win_old.exe and Win.exe, your d_esxi decryptor use only for hypervisor ESXI (



brain.support@cyberfear.com

to me ▾

We do not see the need for this. The esxi tool is enough to decrypt the entire network.

Ancaman Utama Pusat Data Saat Ini



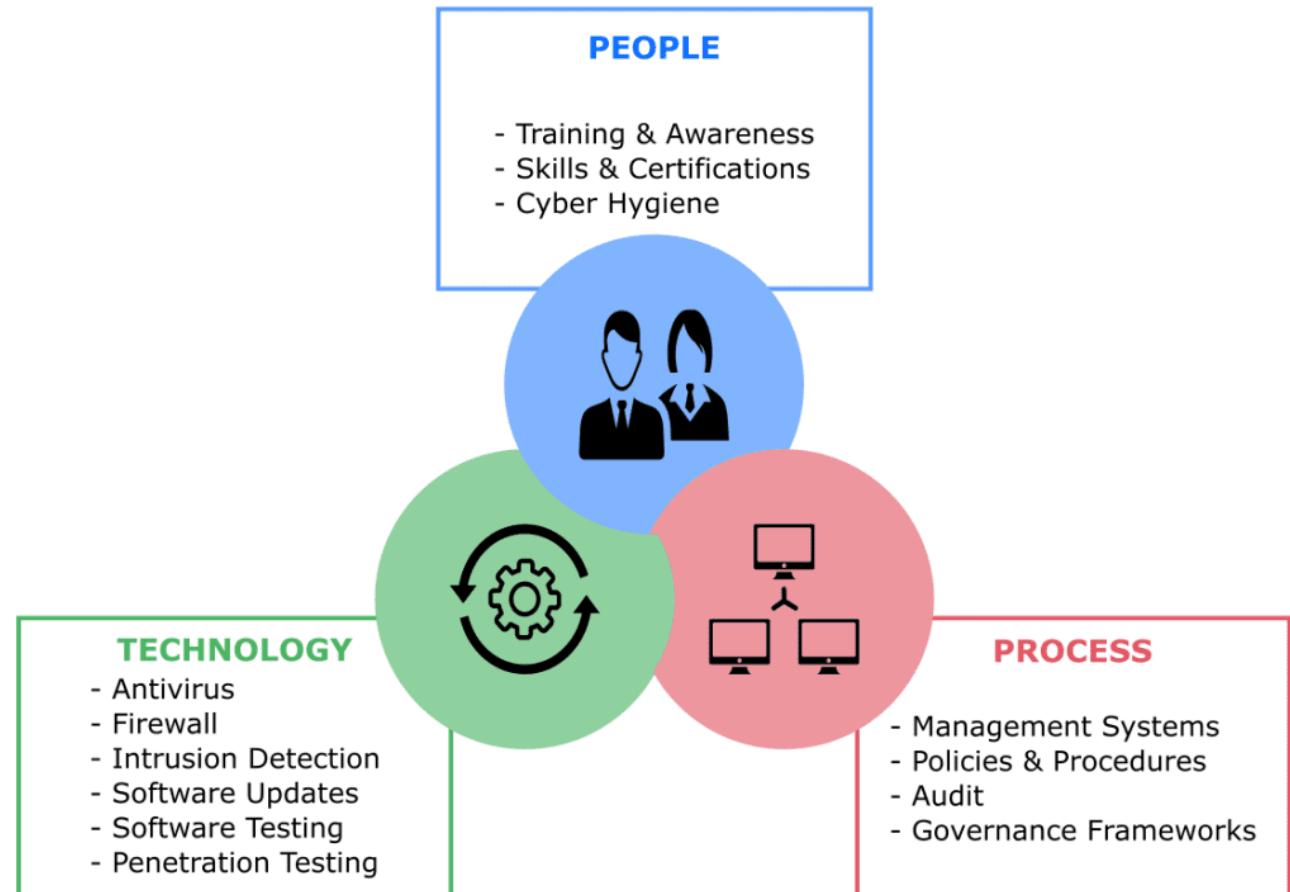
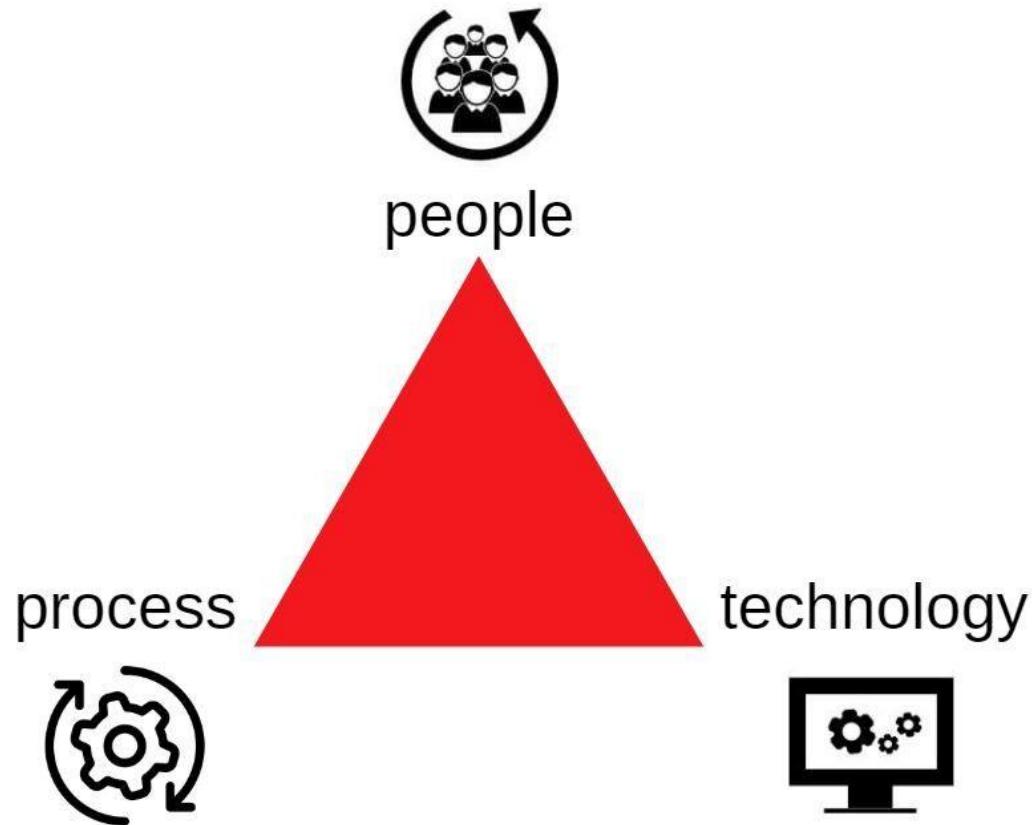
- 1. Unauthorized Intruders :**
Pelanggaran keamanan fisik
- 2. DDoS :**
Distributed Denial of Service
- 3. Ransomware :**
Data dienkripsi dan meminta tebusan untuk dekripsi
- 4. Malware at Scale :**
Malware yang menyerang DCIM
- 5. SSL-induced Blind Spot :**
SSL untuk infiltrasi & eksfiltrasi data

Prioritas Utama Keamanan Pusat Data

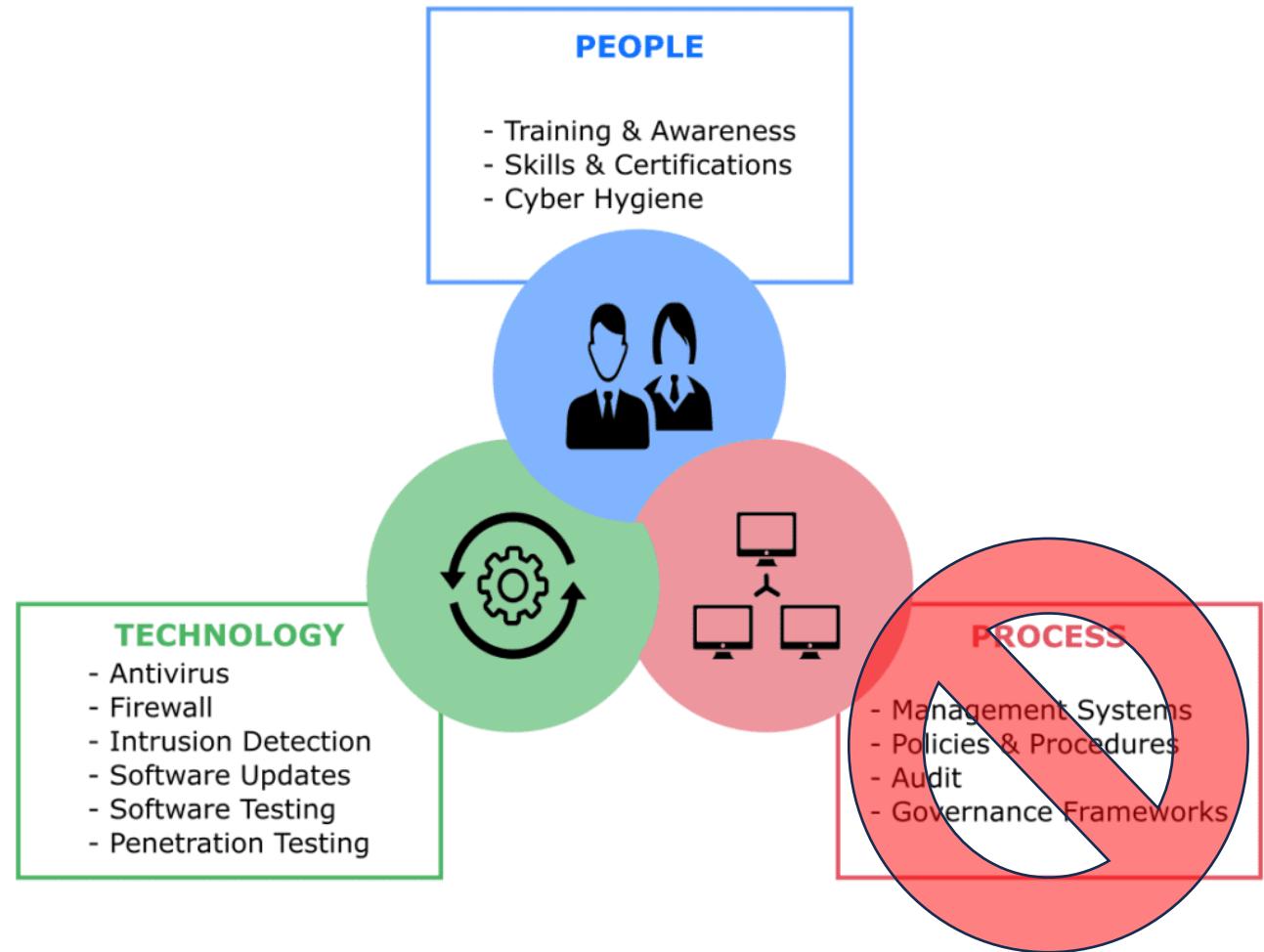
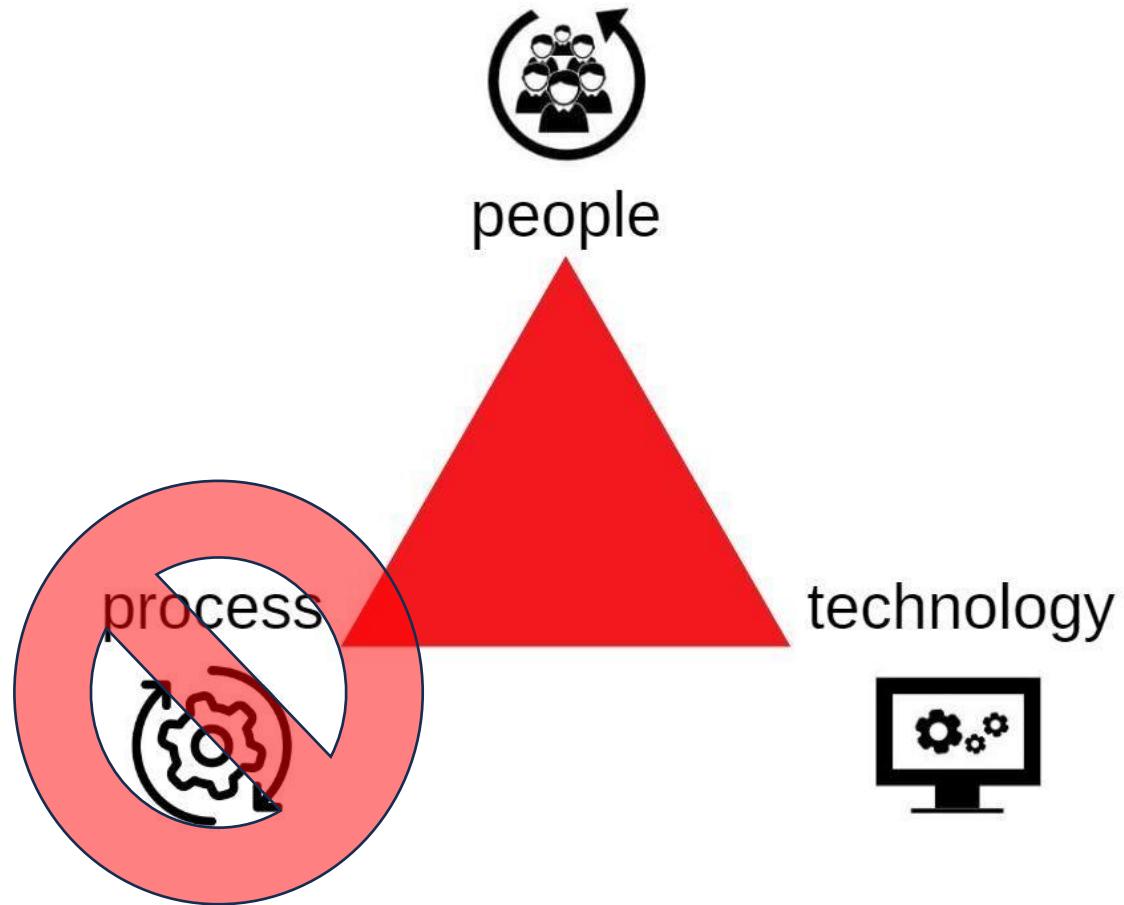


- 1. Advanced Physical Security Measures**
- 2. Network Segmentation**
- 3. Security Information & Event Management**
- 4. ML & AI enabled Cyber Defense**
- 5. Zero Trust Network Access**
- 6. Tools to Address Specific Threats:**
Misalnya : FWaaS, XDR, dan RPaaS
- 7. Anti Phishing Tools & Employee Education**
- 8. Secure By Design & Secure By Default**
- 9. Robust Audits & Compliance**

Apa yang Dibutuhkan untuk Keamanan Pusat Data?



Mana yang Gagal di PDNS 2?



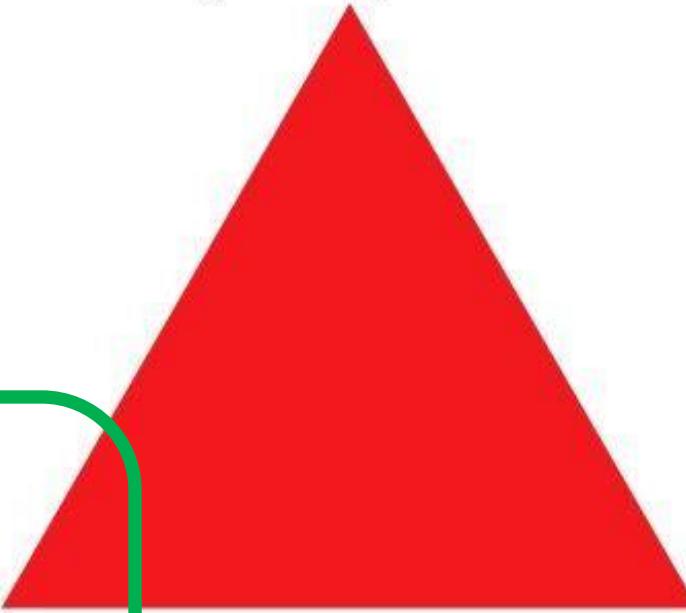
A man in a dark suit and white shirt stands from behind, looking towards a road sign. The sign has two arrows pointing in opposite directions. The top arrow points up and is labeled 'NOT TO DO'. The bottom arrow points right and is labeled 'TO DO'. A large red circle highlights the 'TO DO' sign. To the right of the man, a large red arrow points to the right. The background is a gradient from red on the left to blue on the right.

APA YANG
PERLU
DILAKUKAN?

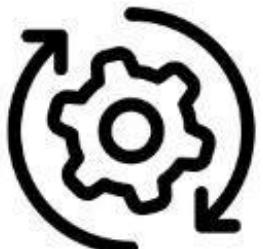
DIMULAI DARI
MANA?



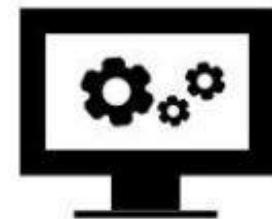
people



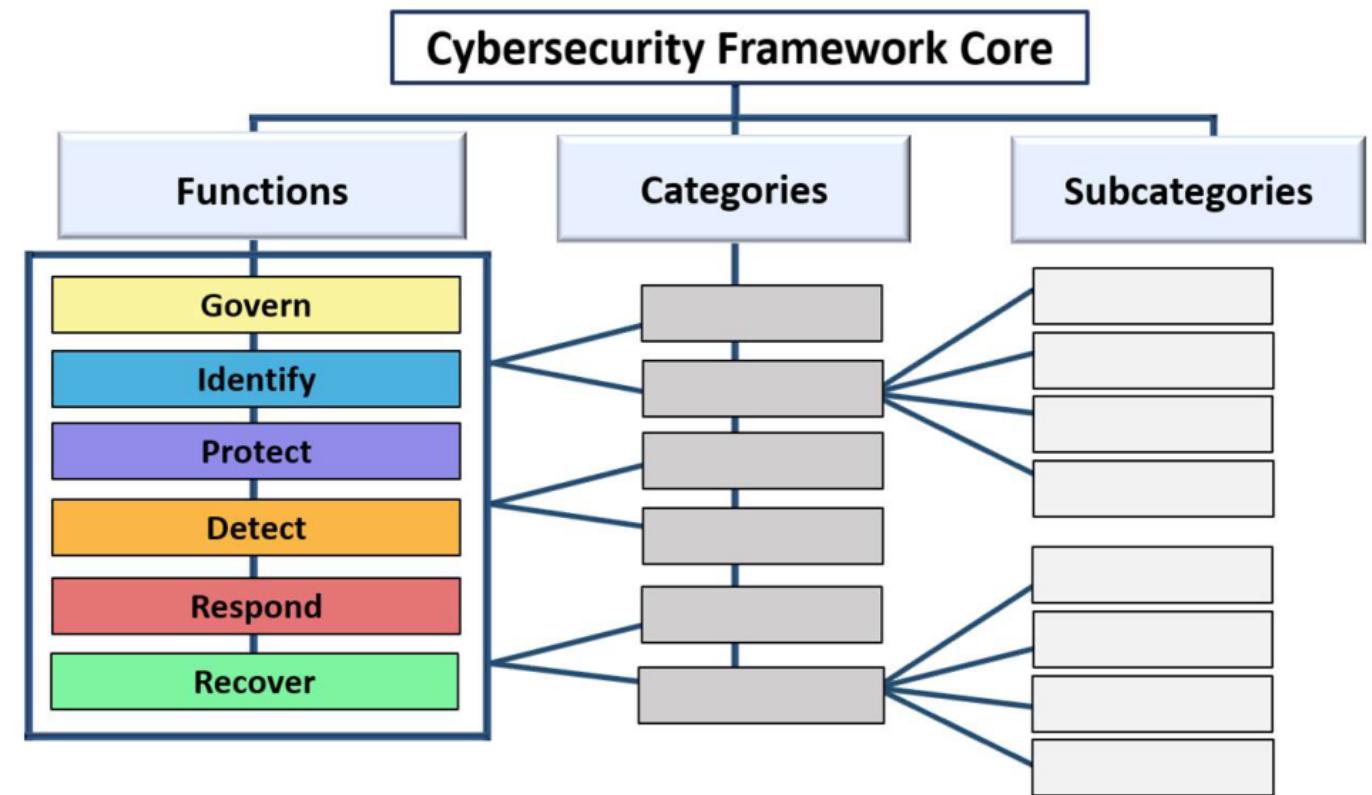
process



technology



The NIST Cybersecurity Framework (CSF) 2.0



The NIST Cybersecurity Framework (CSF) 2.0



Function	Category	Category Identifier
<u>Govern (GV)</u>	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
<u>Identify (ID)</u>	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
<u>Protect (PR)</u>	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
<u>Detect (DE)</u>	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
<u>Respond (RS)</u>	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
<u>Recover (RC)</u>	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

Implementasi NIST CSF 2.0



Target

Goals

- Core outcome description
- Informative References
- Implementation Examples

Create and Use Organizational Profiles



Current

Improvements

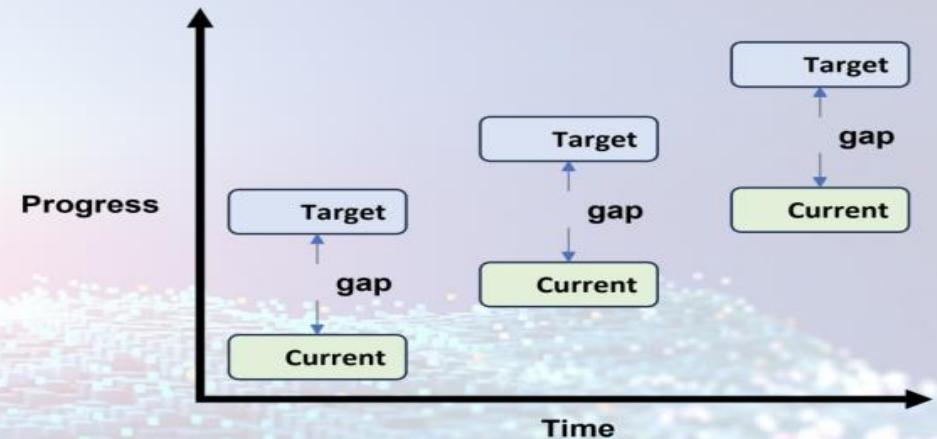
- action
- priority
- owner
- deadline
- resources

Current

Practices

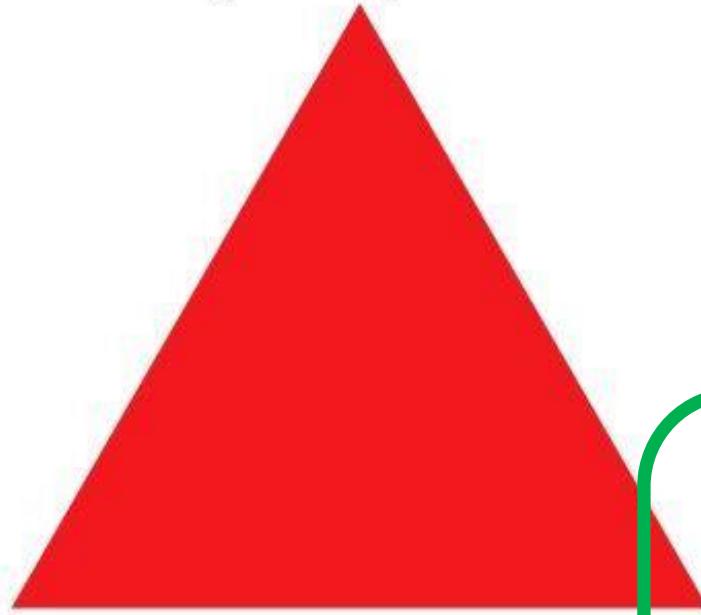
- people
- process
- technology

Drive Progress Over Time





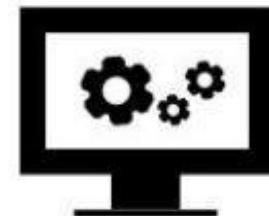
people



process



technology



The CIS Critical Security Controls v8

- 01 Inventory and Control of Enterprise Assets
- 02 Inventory and Control of Software Assets
- 03 Data Protection
- 04 Secure Configuration of Enterprise Assets and Software
- 05 Account Management
- 06 Access Control Management
- 07 Continuous Vulnerability Management
- 08 Audit Log Management
- 09 Email and Web Browser Protection

- 10 Malware Defenses
- 11 Data Recovery
- 12 Network Infrastructure Management
- 13 Network Monitoring and Defense
- 14 Security Awareness and Skills Training
- 15 Service Provider Management
- 16 Applications Software Security
- 17 Incident Response Management
- 18 Penetration Testing

3 Implementation Groups for CIS Controls



The number of Safeguards an enterprise is expected to implement increases based on which group the enterprise falls into.

153

TOTAL SAFEGUARDS

IG3

IG3 assists enterprises with IT security experts to secure sensitive and confidential data. IG3 aims to prevent and/or lessen the impact of sophisticated attacks.

23

SAFEGUARDS

IG2

IG2 assists enterprises managing IT infrastructure of multiple departments with differing risk profiles. IG2 aims to help enterprises cope with increased operational complexity.

74

SAFEGUARDS

IG1

IG1 is the definition of essential cyber hygiene and represents a minimum standard of information security for all enterprises. IG1 assists enterprises with limited cybersecurity expertise thwart general, non-targeted attacks.

56

SAFEGUARDS



Top 5 Attacks

IG1 CIS Safeguards

All CIS Safeguards

Malware

77%

94%

Ransomware

78%

92%

Web Application Hacking

86%

98%

Insider Privilege and Misuse

86%

90%

Targeted Intrusions

83%

95%

associated with malware, ransomware, and other top cyber threats.



Center
for Internet
Security®



CIS Controls



MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

Establishing Essential Cyber Hygiene

<https://www.cisecurity.org/controls/v8>

CIS Critical Security Controls

**Mappings to Safeguards to National Institute
of Standards and Technology (NIST)
Cybersecurity Framework (CSF)**

Version 2



Pemetaan
NIST CSF 2.0
dengan
CIS CSC v8

<https://www.cisecurity.org/controls/v8>

Organizational Profile Scope : Ransomware



- 1. NIST IR 8374 Ransomware Risk Management: A Cybersecurity Framework Profile**
Profil untuk memitigasi risiko Ransomware
- 2. Cyber Risk Institute (CRI) Profile version 2.0**
Pemetaan Profil Ransomware ke NIST CSF 2.0
- 3. CIS Controls v8 Mapping to CSF 2.0**
Pemetaan ke CIS Controls v8
- 4. Establishing Essential Cyber Hygiene**
Tools & Resources untuk CIS Controls v8

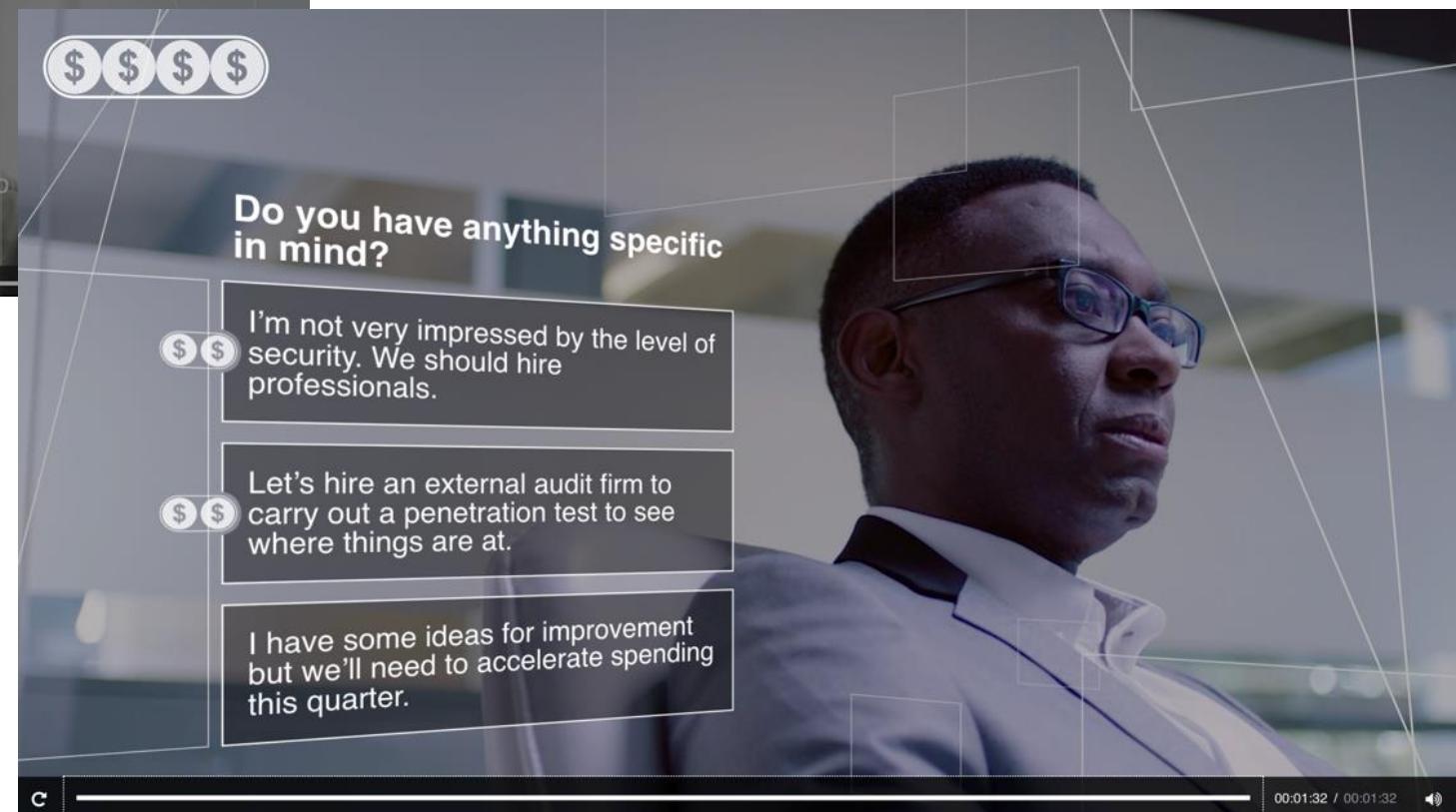
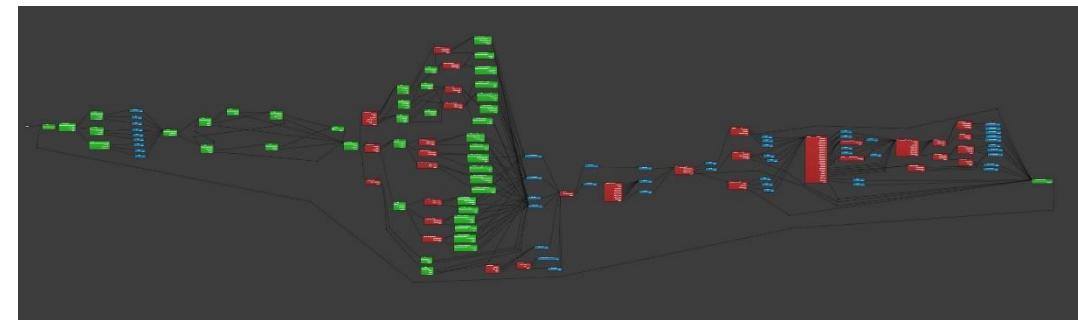
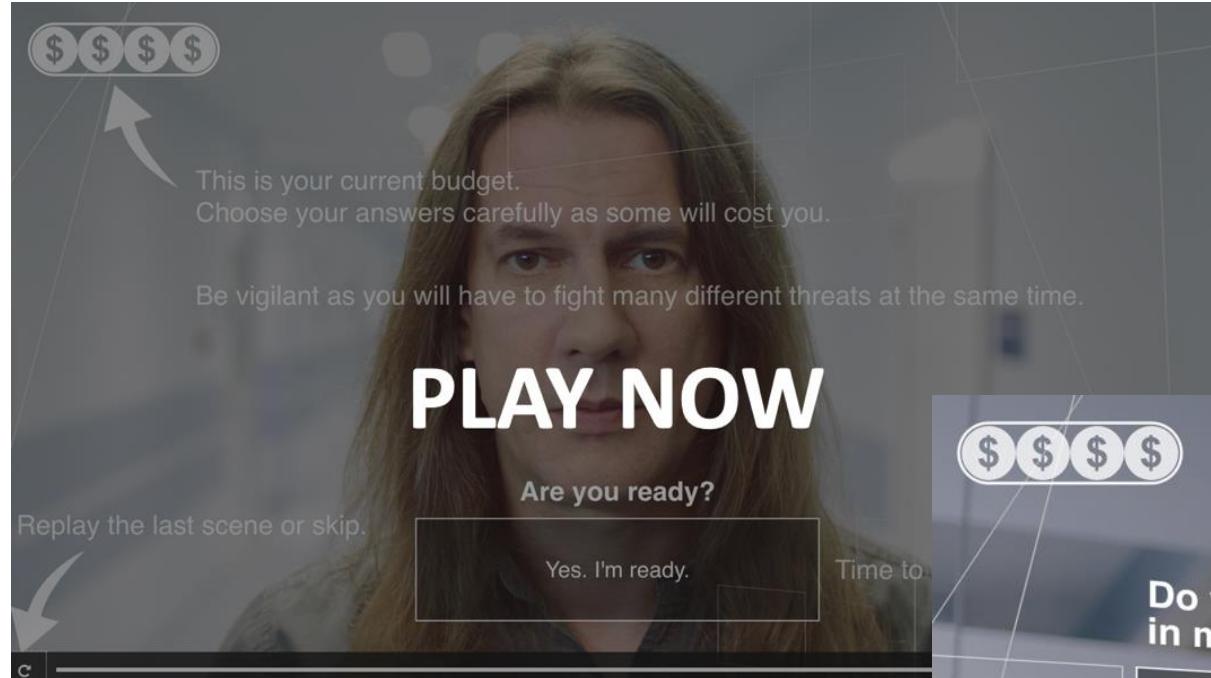


WILL YOUR
DECISIONS
HELP SAVE LIVES?

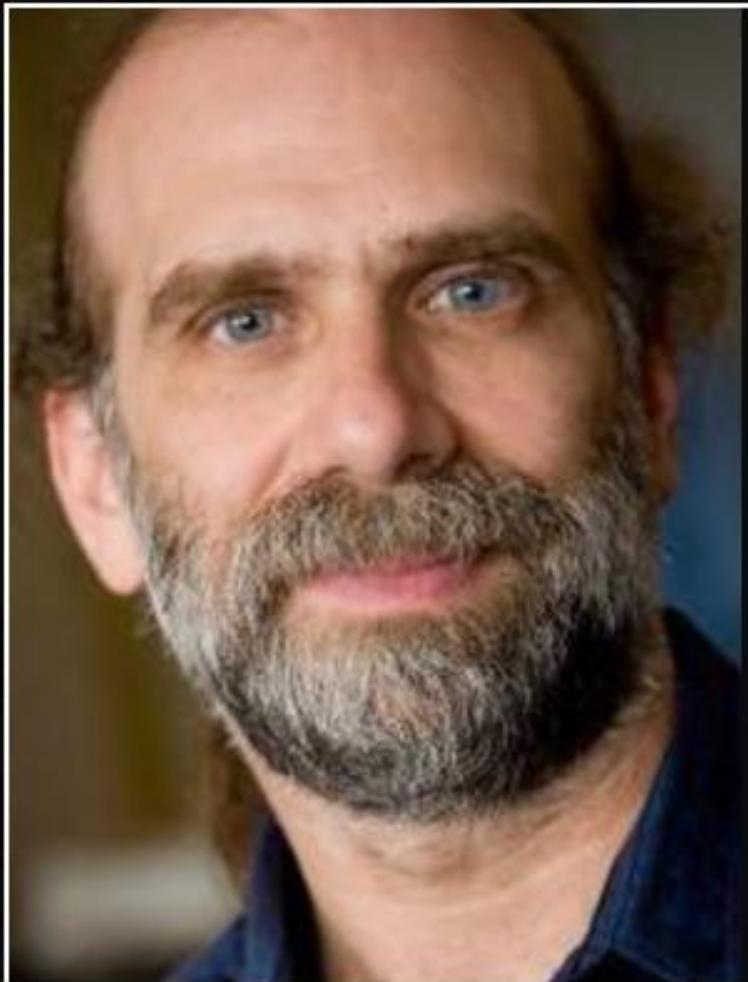
DATA CENTER ATTACK: THE GAME

CLICK TO PLAY





<https://resources.trendmicro.com/datacenter-attack.html>



If you think technology can solve
your security problems, then you
don't understand the problems and
you don't understand the
technology.

— *Bruce Schneier* —

AZ QUOTES