inixindo bandung

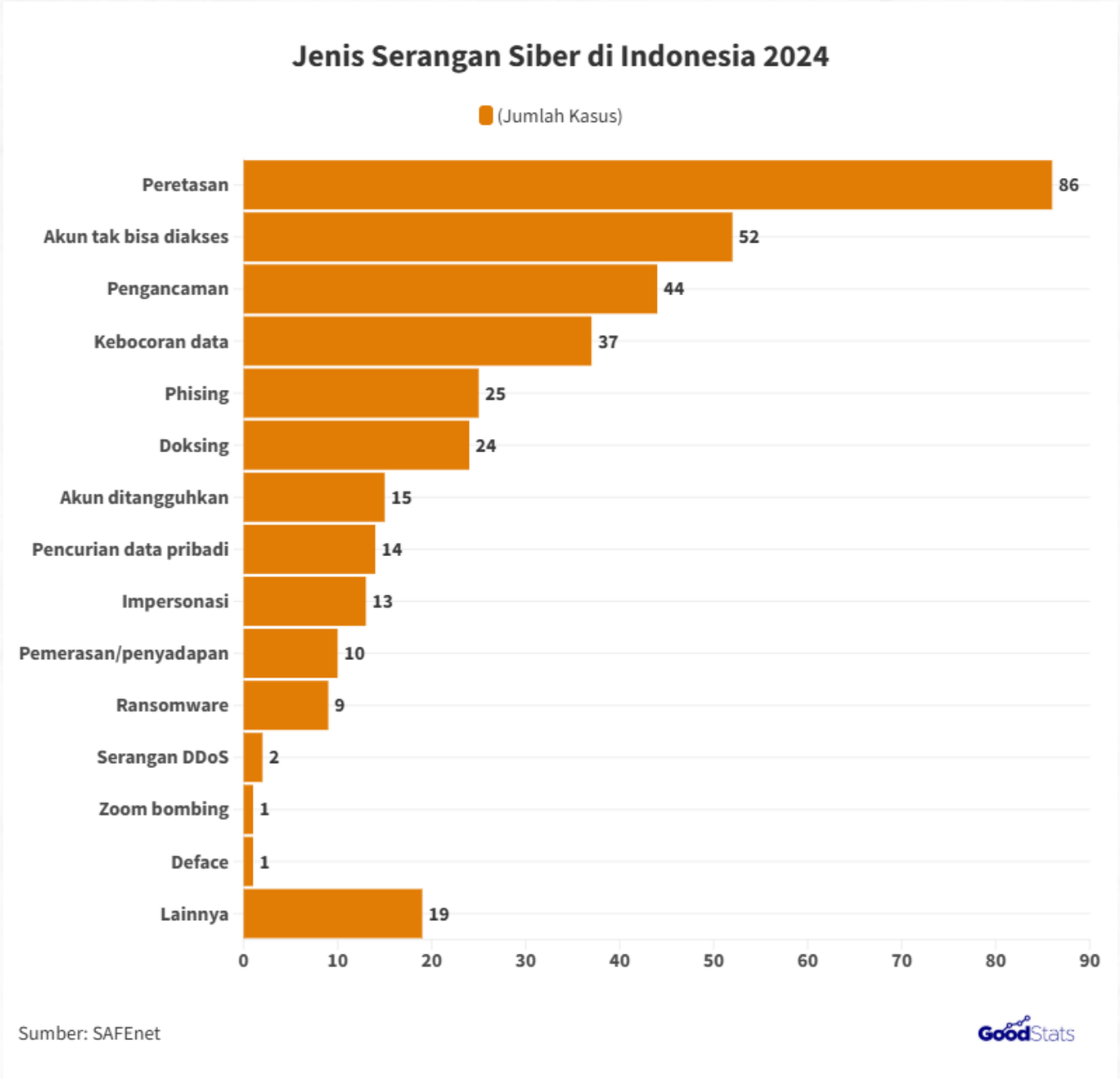
Cybersecurity

Ancaman Dunia Digital

Outline materi

1. Tipe ancaman *Cybersecurity*
2. Sumber ancaman
3. Kerentanan Di Dunia *Cybersecurity*
4. *Cyber Warfare*

Tipe Ancaman *Cybersecurity*


Jenis Serangan Siber di Indonesia 2024
(Jumlah Kasus)
Peretasan 86
Akun tak bisa diakses 52
Pengancaman 44
Kebocoran data 37
Phising 25
Doksing 24
Akun ditangguhkan 15
Pencurian data pribadi 14
Impersonasi 13
Pemerasan/penyadapan 10
Ransomware 9
Serangan DDoS 2
Zoom bombing 1
Deface 1
Lainnya 19
0 10 20 30 40 50 60 70 80 90
Sumber: SAFEnet
GoodStats

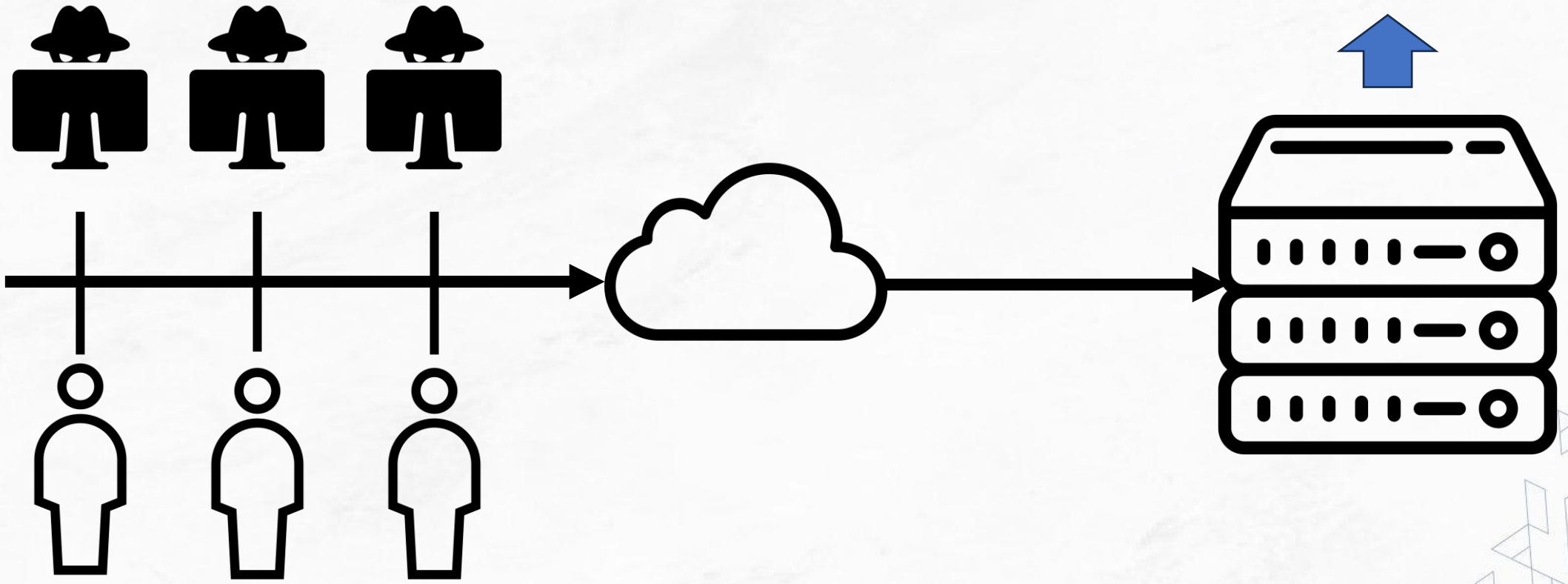
Social Engineering

1. Email
2. SMS
3. Whatapps
4. Telegram
5. Website
6. DLL

Malware (Malicious Software)

- Virus
- Trojan
- Worm
- Crypter
- Ransomware

Denial-of-Service (DoS)

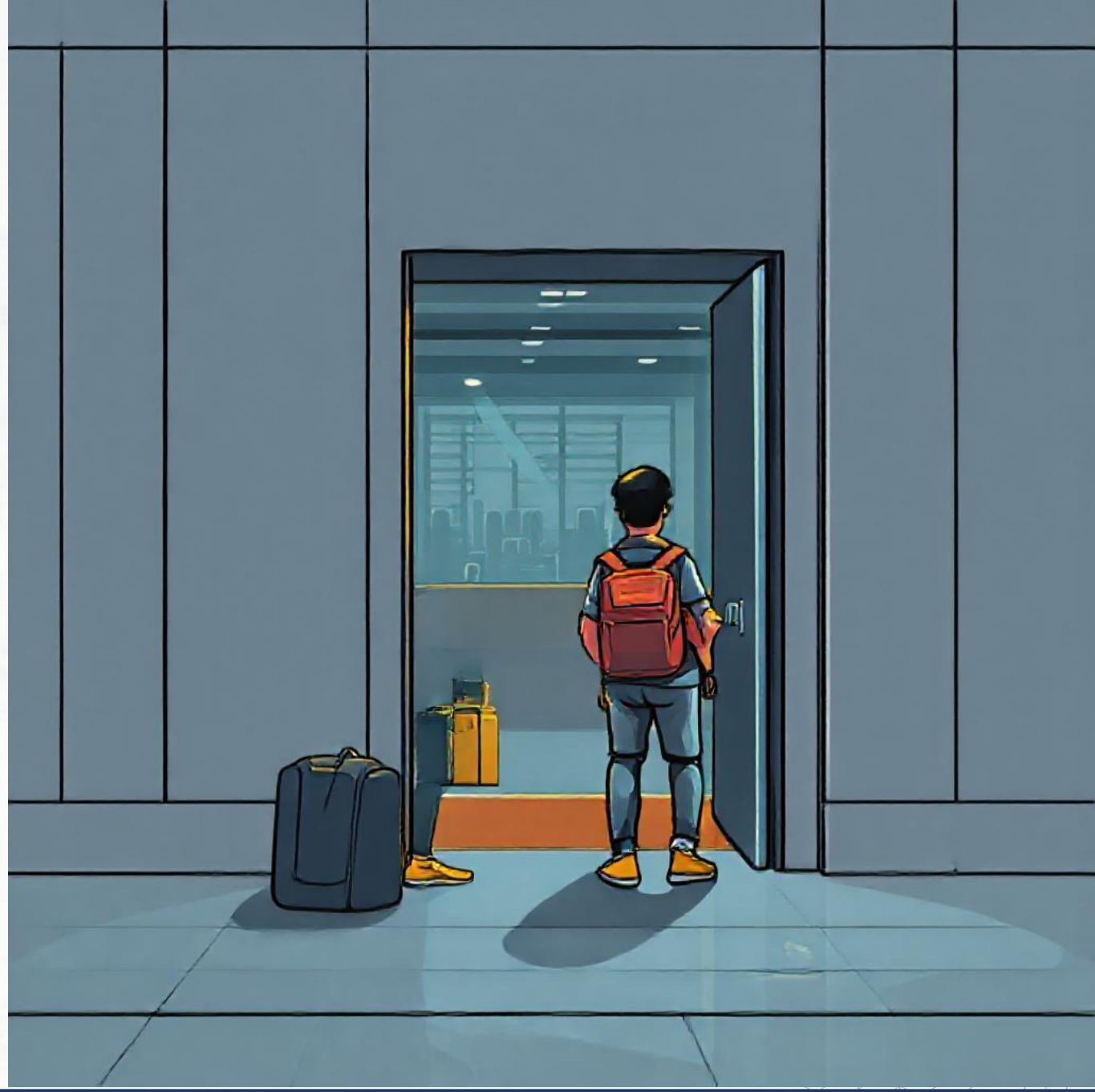


Web Application Attack

- Sql Injection
- Cross-site Scripting (XSS)
- Cross-site Reqeust Forgery
- Remote Code Execution (RCE)

Physical Attack

1. Eavesdropping
2. Tailgating
3. Piggybacking



Sumber Ancaman

Suber ancaman

- Bencana Alam
- Insiden yang tidak disengaja
- Insiden yang disengaja

Bencana Alam

- Kebakaran
- Banjir
- Pemadaman Listrik
- Gempa
- Angin topan
- Badai
- Longsor
- DSB

Insiden yang tidak di sengaja

1. Team yang tidak mengikuti SOP
2. Karyawan yang tidak memiliki awareness
3. Karyawan yang melanggar aturan

Insiden disengaja

1. Internal
   - Karyawan yang dipecat
   - Karyawan yang memiliki rasa dendam
   - Vendor
2. External
   - Hackers
   - Terorris
   - Mata-Mata Perusahaan pesaing

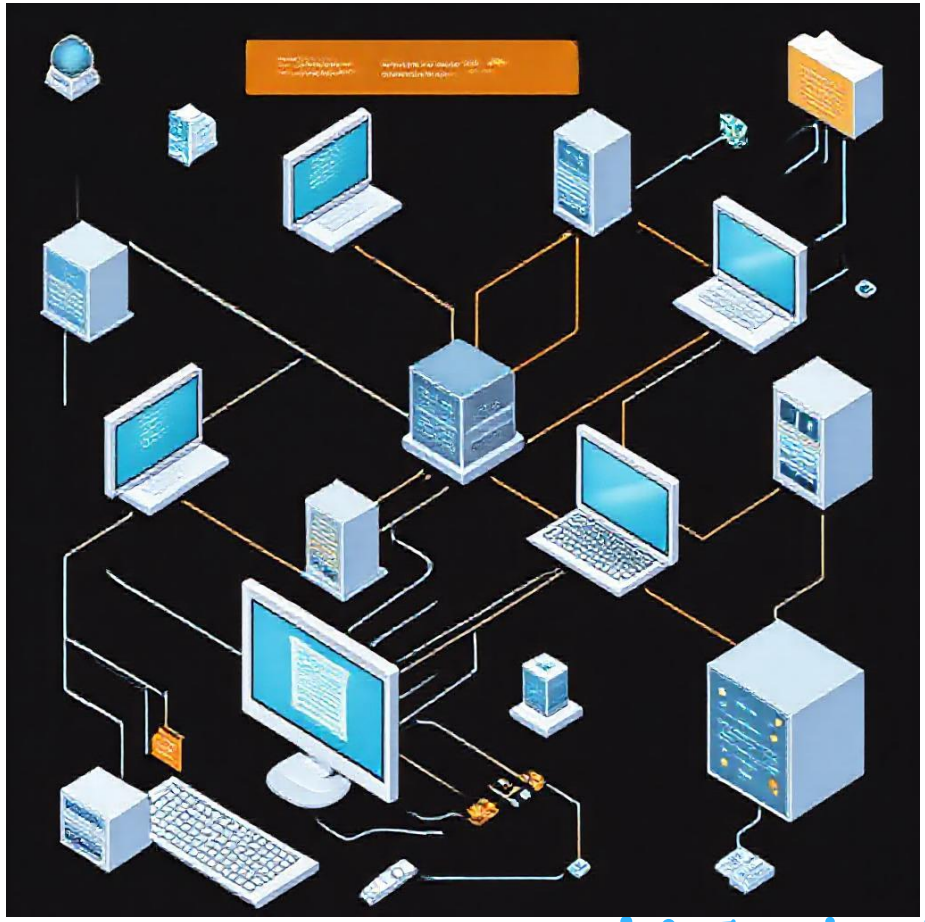
Kerentanan di Dunia *Cybersecurity*

Common Vulnerability

- *Hardware* atau *Software Misconfiguration*
- Desain yang tidak aman dari jaringan atau Aplikasi
- Penggunaan teknologi yang rentan/jadul
- Karyawan yang bodo amat

Jaringan

- Aplikasi
- Operating system (OS)
- Protokol



Aplikasi

- SQL injection
- XSS
- Command Injection
- IDOR
- CSRF
- Etc

Operating system (OS)

- CVE
- CWE
- CVSS
- NVD

Protokol

- SMB
- FTP
- HTTP
- dsbV

Cyber Warfare

Information Warfare

- Defensive Warfare
  - semua strategi dan tindakan yang dirancang untuk mempertahankan diri dari serangan terhadap aset TIK
- Offensive Warfare
  - perang informasi yang melibatkan serangan terhadap aset TIK

Cyber threat Intelligence (CTI)

Tujuan Utama CTI

1. **Mendeteksi ancaman lebih awal** sebelum menjadi serangan nyata.
2. **Mengidentifikasi pelaku ancaman** (aktor, teknik, tujuan).
3. **Mengurangi risiko serangan** dengan tindakan preventif.
4. **Membantu pengambilan keputusan** dalam keamanan siber.
5. **Memberikan konteks pada peringatan teknis** seperti log, IOC, dll.

Cyber Threat Intelligence

Jenis	Kegunaan	Contoh
Stategic	Untuk manajemen/pengambil kebijakan	Laporan tren serangan global, target negara
Operational	Untuk tim operasional keamanan	Info actor APT, taktik kampanye aktor
Tactical	Untuk tim SOC	Teknik serangan, malware behavior
Tachnical	Untuk mesin/system	IOC: IP address, hash file, domain, url anomali