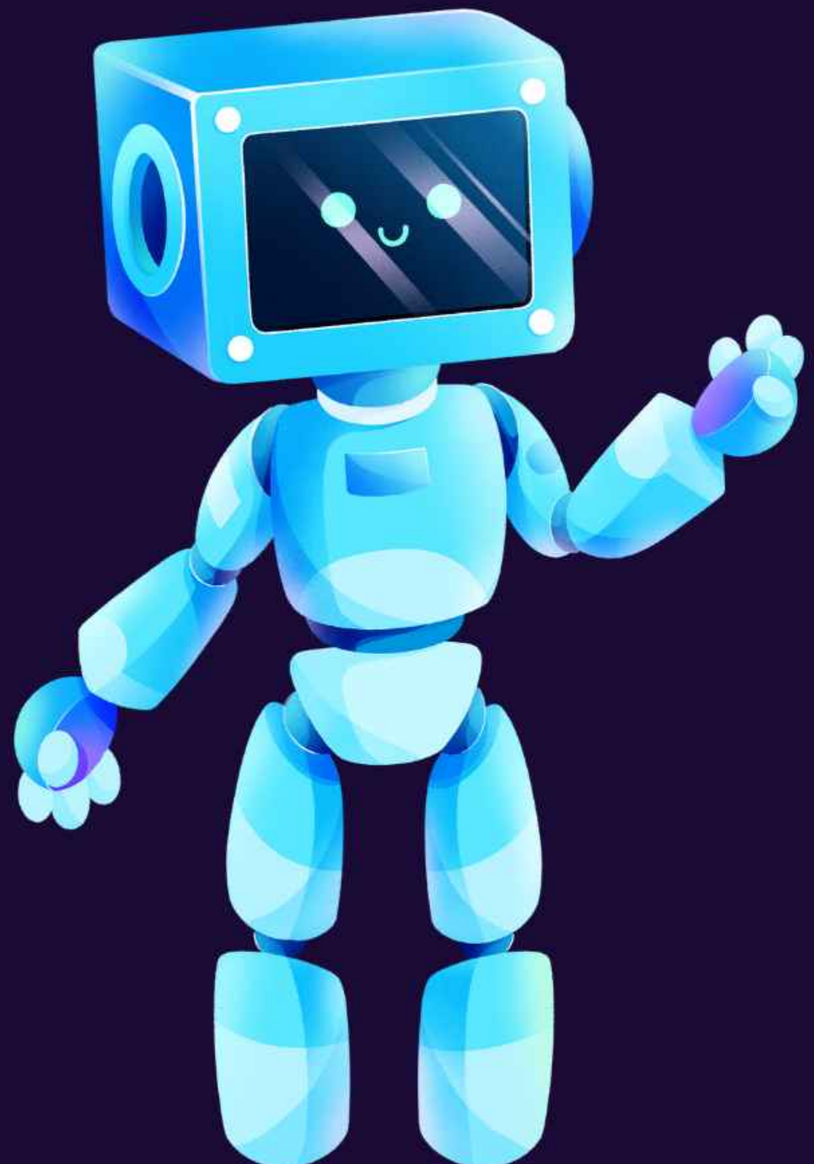
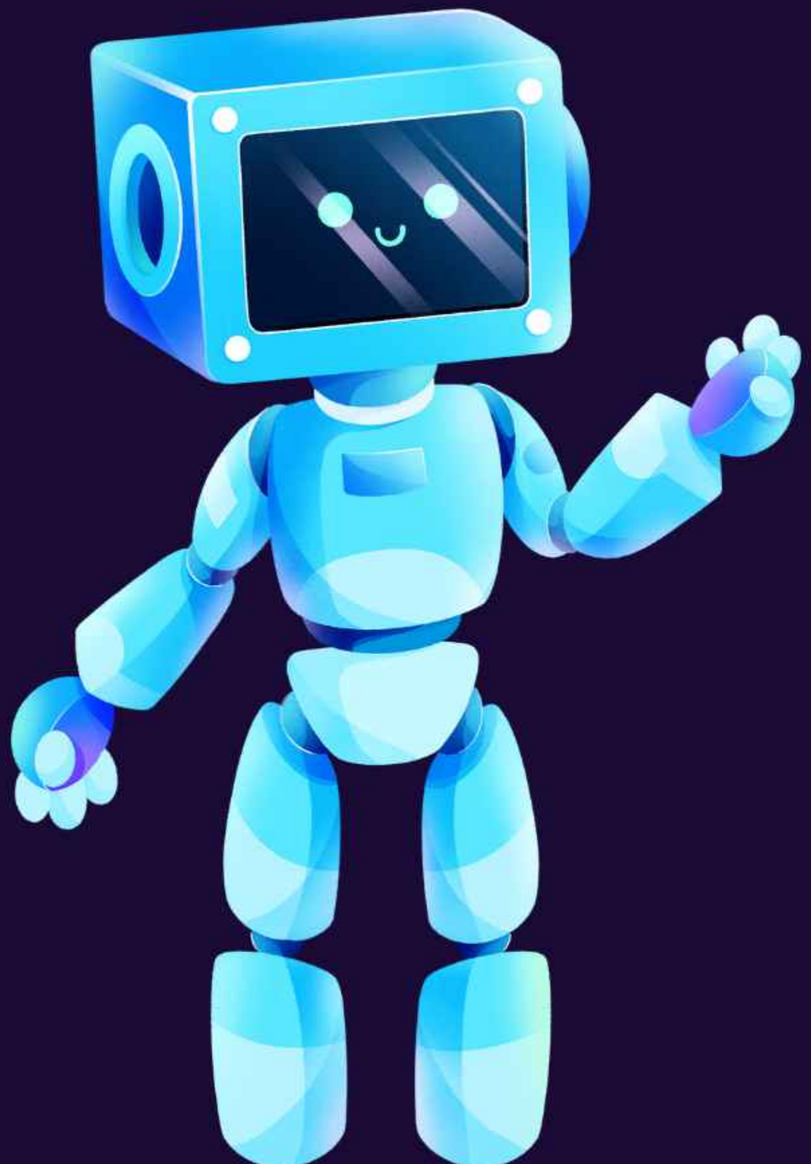


SISTEM PROTEKSI

Protokol Keamanan Sistem Operasi

Kelompok 5



ANGGOTA

1. Ratu Naurah Calista (H1D023004)
2. Nadzare Kafah Alfatiha (H1D023014)
3. Diyah G putri (H1D023022)
4. Khaila Salsa Marfa Bilqis (H1D023030)
5. Nisa Izzatul Ummah (H1D023034)
6. Mufthie Alie (H1D023042)
7. Putranto Surya Wijanarko (H1D023048)

Hak Akses (Access Rights) ?

Hak akses (access rights) adalah izin atau hak istimewa yang diberikan kepada pengguna, program, atau workstation untuk membuat, mengubah, menghapus, atau melihat data dan file dalam sebuah sistem, sebagaimana ditetapkan oleh aturan yang dibuat oleh pemilik data dan sesuai kebijakan keamanan informasi

Komponen utama Hak Akses (Access Rights)

- Identifikasi Pengguna (User Identification)
  Setiap pengguna dalam sistem operasi memiliki identitas unik yang di gunakan seperti sebuah akun dengan **nama pengguna (username) dan password.**

- **Otorisasi (Authorization)**
  Adalah proses yang menentukan hak akses yang dimiliki oleh pengguna terhadap sumber daya tertentu, Hak akses didefinisikan dalam bentuk peran (roles) atau izin (permissions), Contoh izin membaca (read), menulis (write), dan menjalankan (execute).

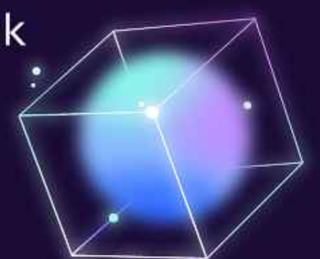
- **Manajemen Hak Akses (Access Control Management)**
  Sistem operasi menyediakan mekanisme untuk mengelola dan mengatur hak akses pengguna.

Komponen utama Hak Akses (Access Rights)

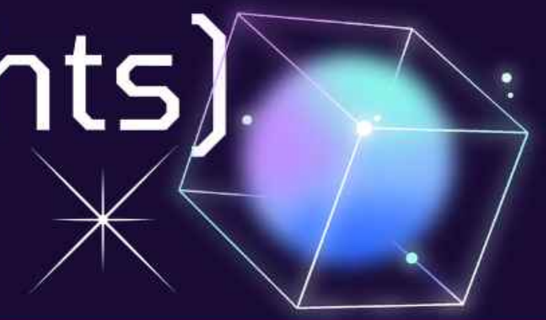
- **Pemeriksaan Hak Akses (Access Checking):**
  sistem operasi melakukan pemeriksaan hak akses untuk memverifikasi apakah pengguna memiliki izin yang cukup.

- Pelacakan Log (Logging)
  Log ini dapat digunakan untuk audit, penelusuran kegiatan yang mencurigakan, atau pemecahan masalah keamanan.

- Pemisahan (islation)
  Bertujuan untuk memisahkan akses pengguna untuk mencegah pengguna yang tidak berwenang dari mengakses atau merusak sumber daya milik pengguna lain.



Hak Akses (Access Rights) Di Sistem Operasi



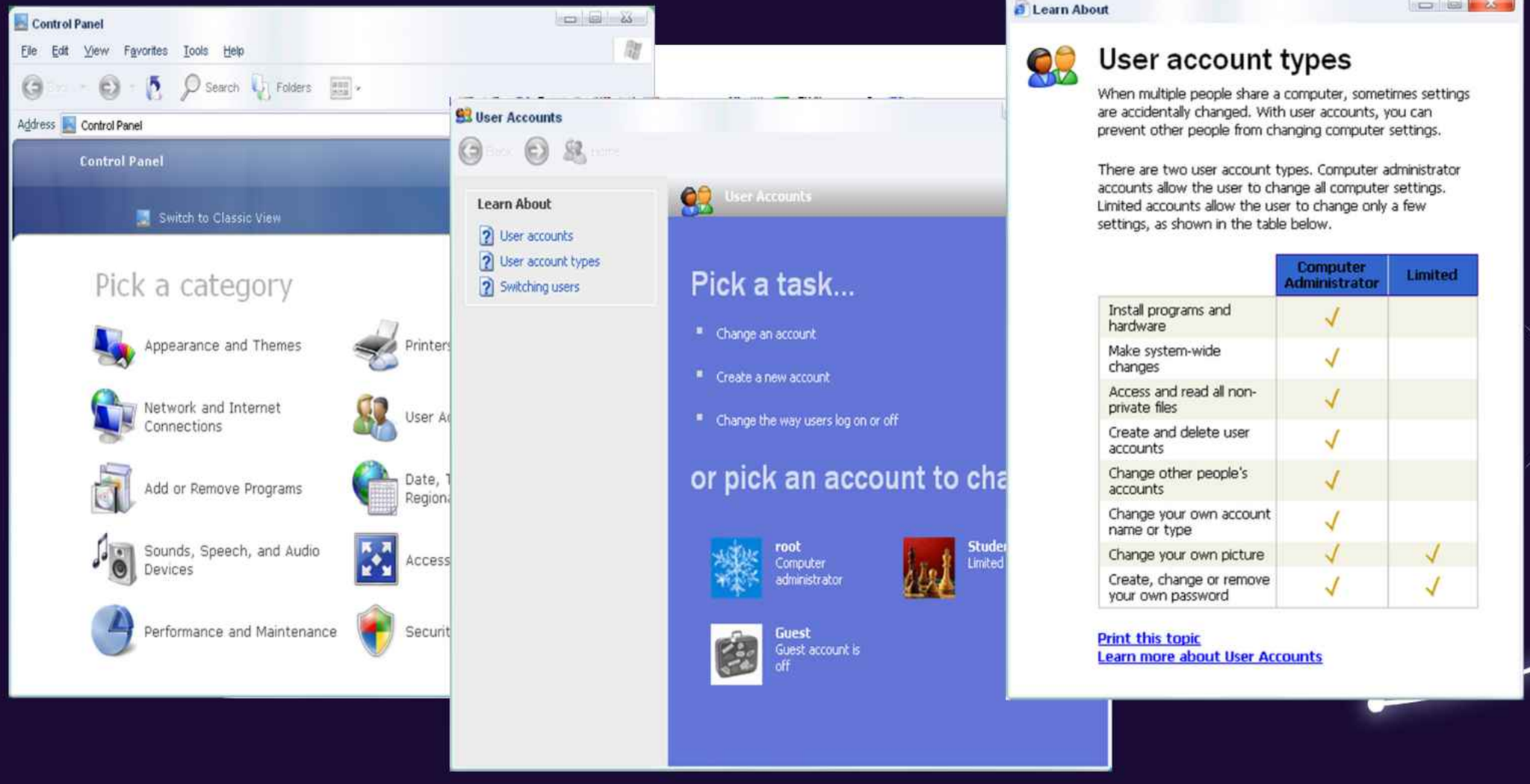
Hak Akses pada Linux

Pada Linux, hak akses terhadap suatu file merupakan fasilitas keamanan yang berarti bahwa setiap file memiliki informasi tentang siapa yang dapat mengakses, mengubah, atau menghapusnya. Hak akses ini dapat dikontrol dengan menggunakan password, serta dengan mengelompokkan user menjadi Owner/User, Group, dan Other

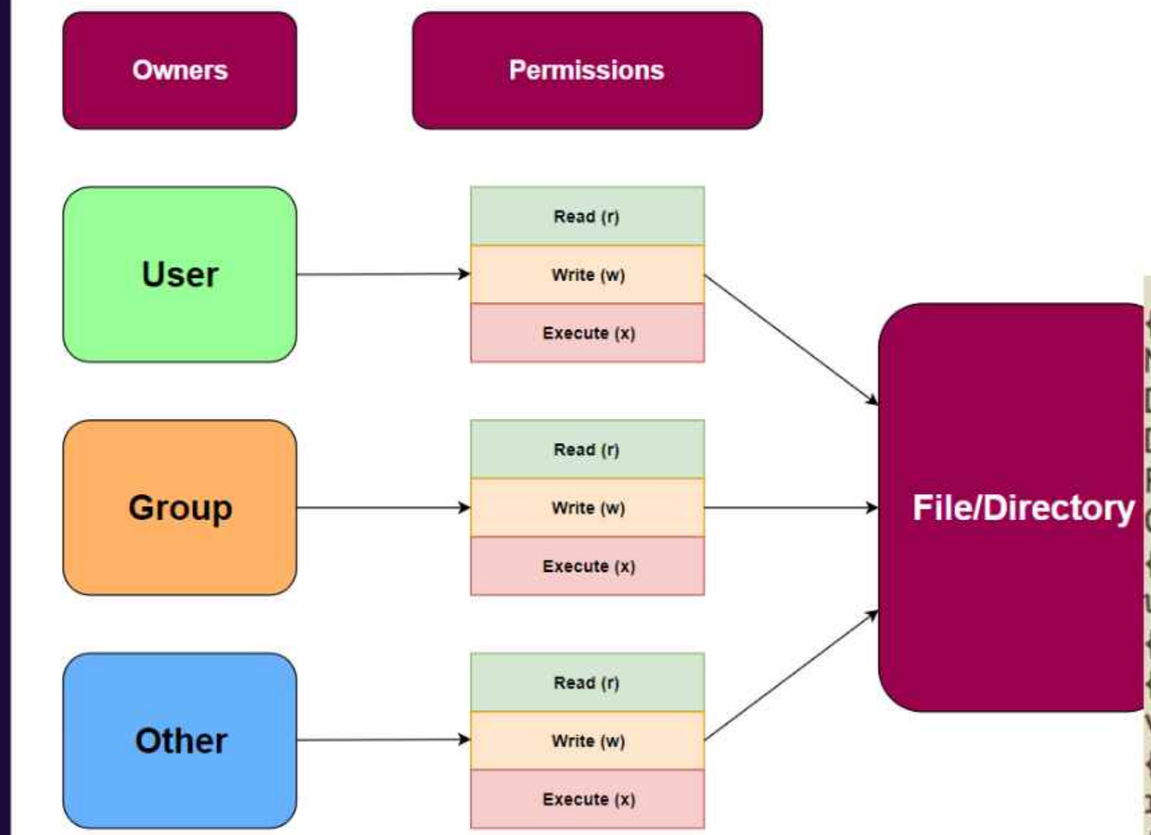
Hak Akses pada Windows

Pada Windows, hak akses yang valid untuk objek proses mencakup hak akses standar dan beberapa hak akses khusus proses. Hak akses standar meliputi HAPUS, READ_CONTROL, SINKRONKAN, WRITE_DAC, dan WRITE_OWNER.

Windows


Control Panel
File Edit View Favorites Tools Help
Search Folders
Address Control Panel
Control Panel
Switch to Classic View
Pick a category
Appearance and Themes
Network and Internet Connections
Add or Remove Programs
Sounds, Speech, and Audio Devices
Performance and Maintenance
User Accounts
Learn About
User accounts
User account types
Switching users
Pick a task...
Change an account
Create a new account
Change the way users log on or off
or pick an account to cha
root
Computer administrator
Guest
Guest account is off
Learn About
User account types
When multiple people share a computer, sometimes settings are accidentally changed. With user accounts, you can prevent other people from changing computer settings.
There are two user account types. Computer administrator accounts allow the user to change all computer settings. Limited accounts allow the user to change only a few settings, as shown in the table below.
Computer Administrator
Limited
Install programs and hardware
Make system-wide changes
Access and read all non-private files
Create and delete user accounts
Change other people's accounts
Change your own account name or type
Change your own picture
Create, change or remove your own password
Print this topic
Learn more about User Accounts

Linux




```
{cyberciti.biz}~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 12.04.4 LTS
Release:        12.04
Codename:       precise
{cyberciti.biz}~$ id
uid=1000(vivek) gid=1000(vivek) groups=1000(vivek)
{cyberciti.biz}~$
{cyberciti.biz}~$ groups
vivek
{cyberciti.biz}~$ id -Gn root
root
{cyberciti.biz}~$ groups root
root : root
{cyberciti.biz}~$ id -Gn vivek
vivek
{cyberciti.biz}~$ id -gn vivek
```

Kontrol Akses (Access Control)?

Kontrol Akses (Access Control) adalah mekanisme yang digunakan dalam sistem proteksi untuk mengatur akses pengguna terhadap sumber daya sistem, seperti file, direktori, atau perangkat keras. Tujuan utamanya adalah untuk memastikan bahwa hanya pengguna yang diotorisasi yang dapat mengakses sumber daya tersebut, serta untuk mempertahankan kerahasiaan, integritas, dan ketersediaan informasi.

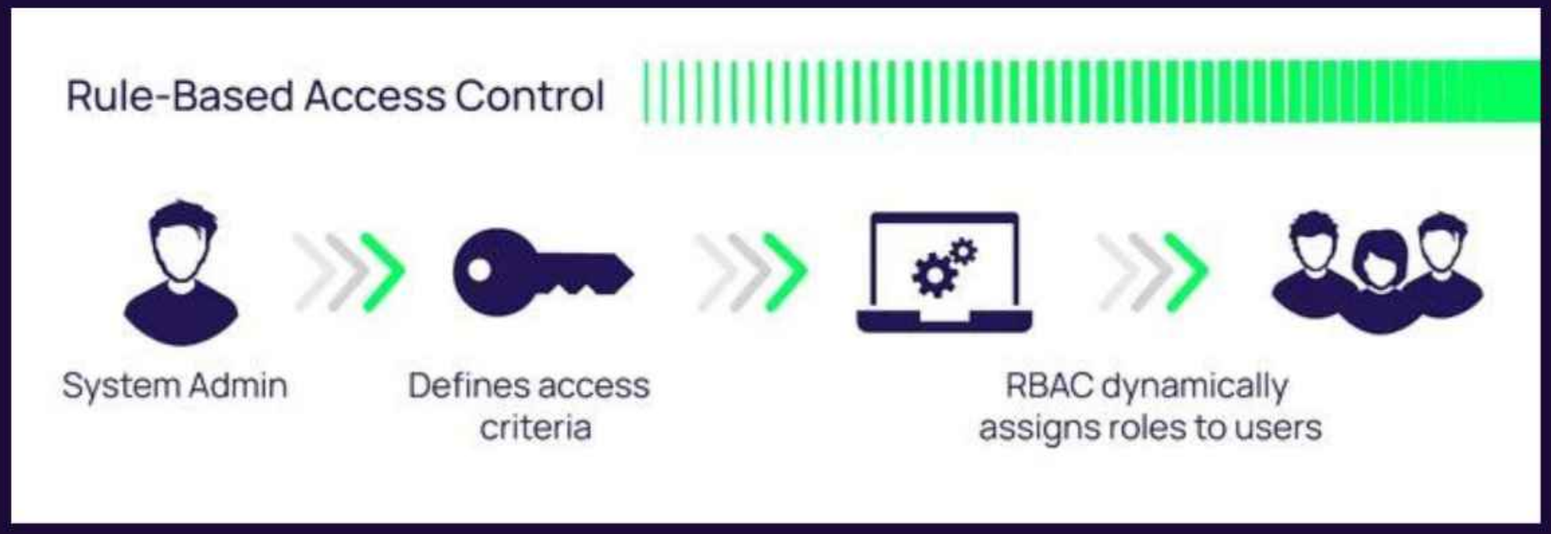
Jenis Kontrol Akses

KONTROL AKSES BERBASIS PERAN (ROLE-BASED ACCESS CONTROL - RBAC)	KONTROL AKSES BERBASIS ATURAN (RULE-BASED ACCESS CONTROL)	KONTROL AKSES BERBASIS KEBUTUHAN (NEED-TO-KNOW)
Dalam RBAC, akses terhadap sumber daya ditentukan berdasarkan peran atau posisi pengguna dalam organisasi	Kontrol Akses Berbasis Aturan menggunakan seperangkat aturan atau kebijakan untuk mengatur akses pengguna terhadap sumber daya	Prinsip ini mengatur akses berdasarkan kebutuhan pengguna terhadap informasi tertentu.

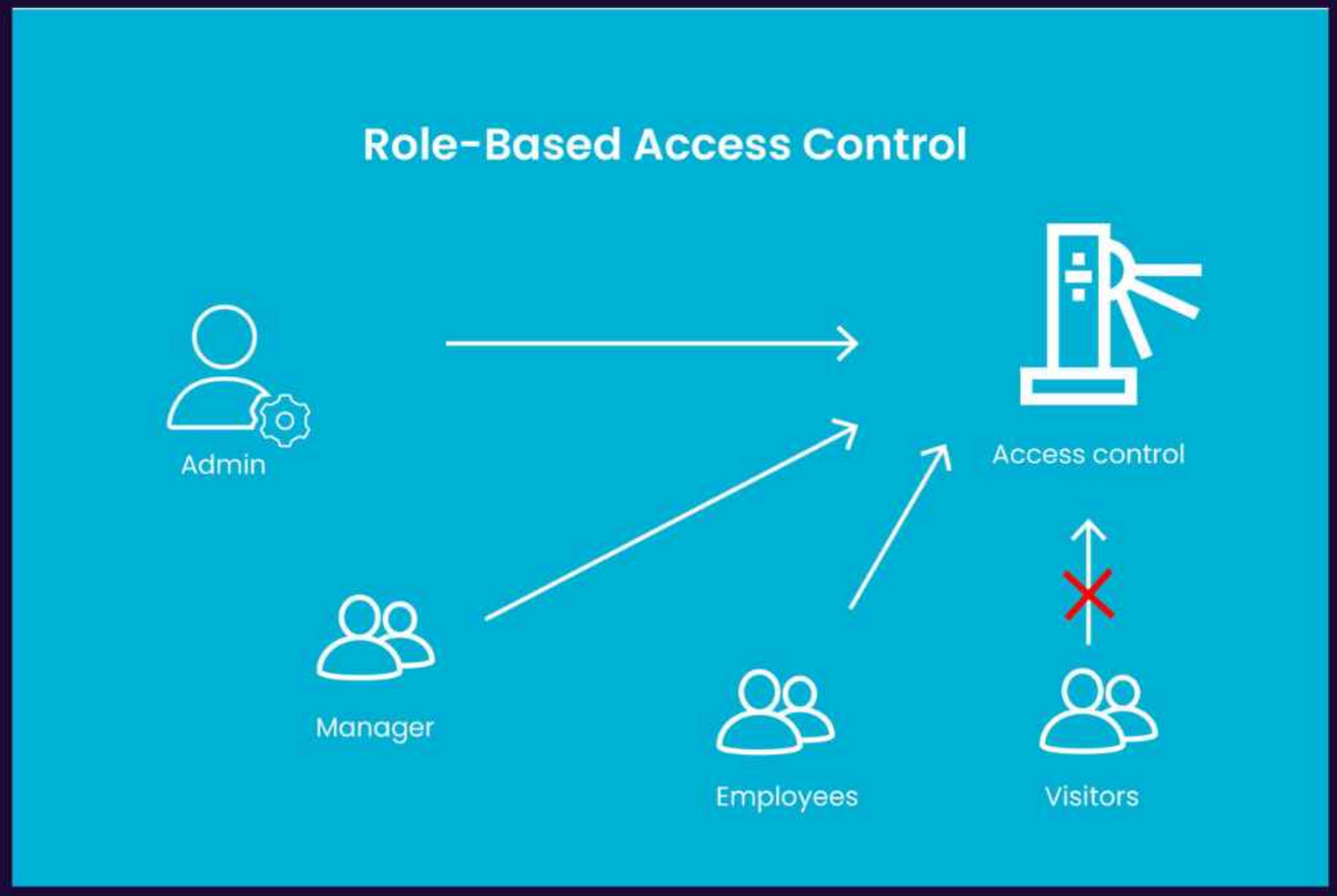
Jenis Kontrol Akses

DAC (DISCRETIONARY ACCESS CONTROL)	KONTROL AKSES BERBASIS LABEL (LABEL-BASED ACCESS CONTROL)	MAC (MANDATORY ACCESS CONTROL)
pengguna memiliki kendali atas objek yang mereka miliki, termasuk siapa yang memiliki akses ke objek tersebut. Pemilik objek dapat menentukan izin akses individu untuk pengguna lain.	Dalam label-based access control, setiap sumber daya dan pengguna memiliki label keamanan yang menentukan tingkat akses yang diizinkan. Hanya pengguna dengan label keamanan yang sesuai atau lebih tinggi yang diizinkan untuk mengakses sumber daya tersebut.	MAC memberikan atau menolak akses ke objek sumber daya berdasarkan tingkat keamanan informasi pengguna atau perangkat

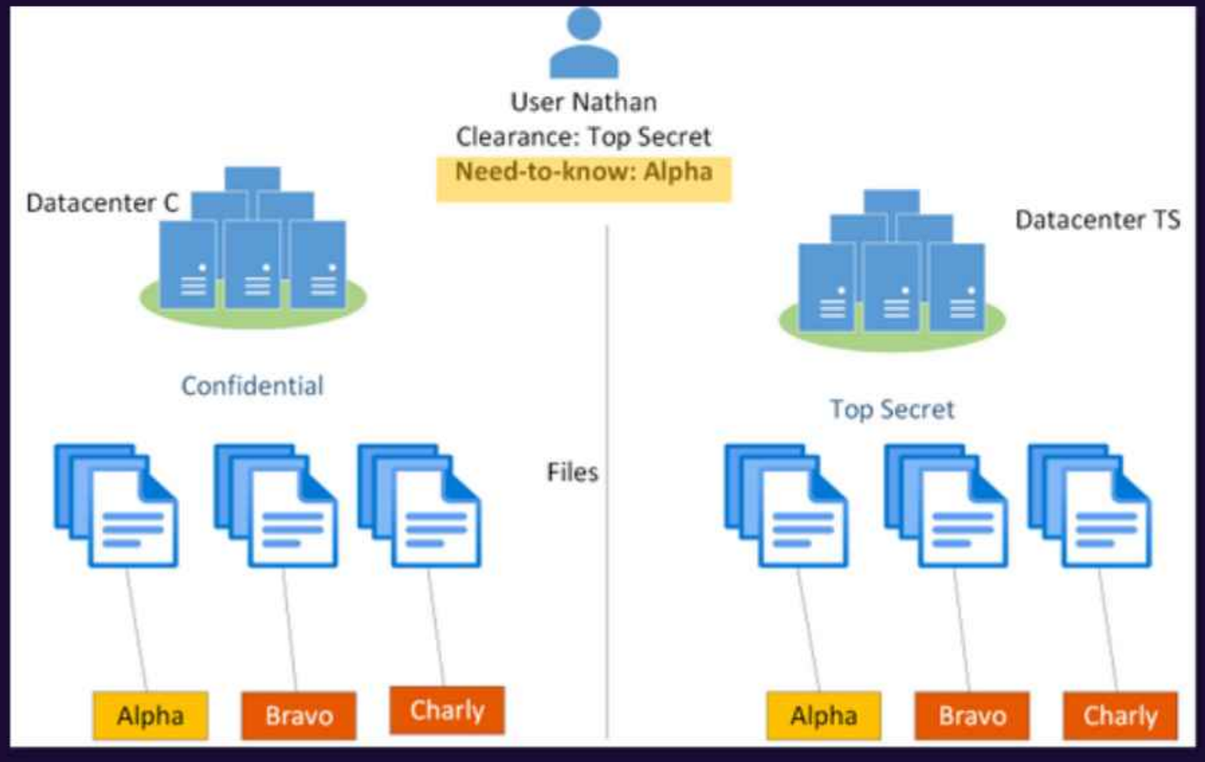
RBAC (Rule-Based)



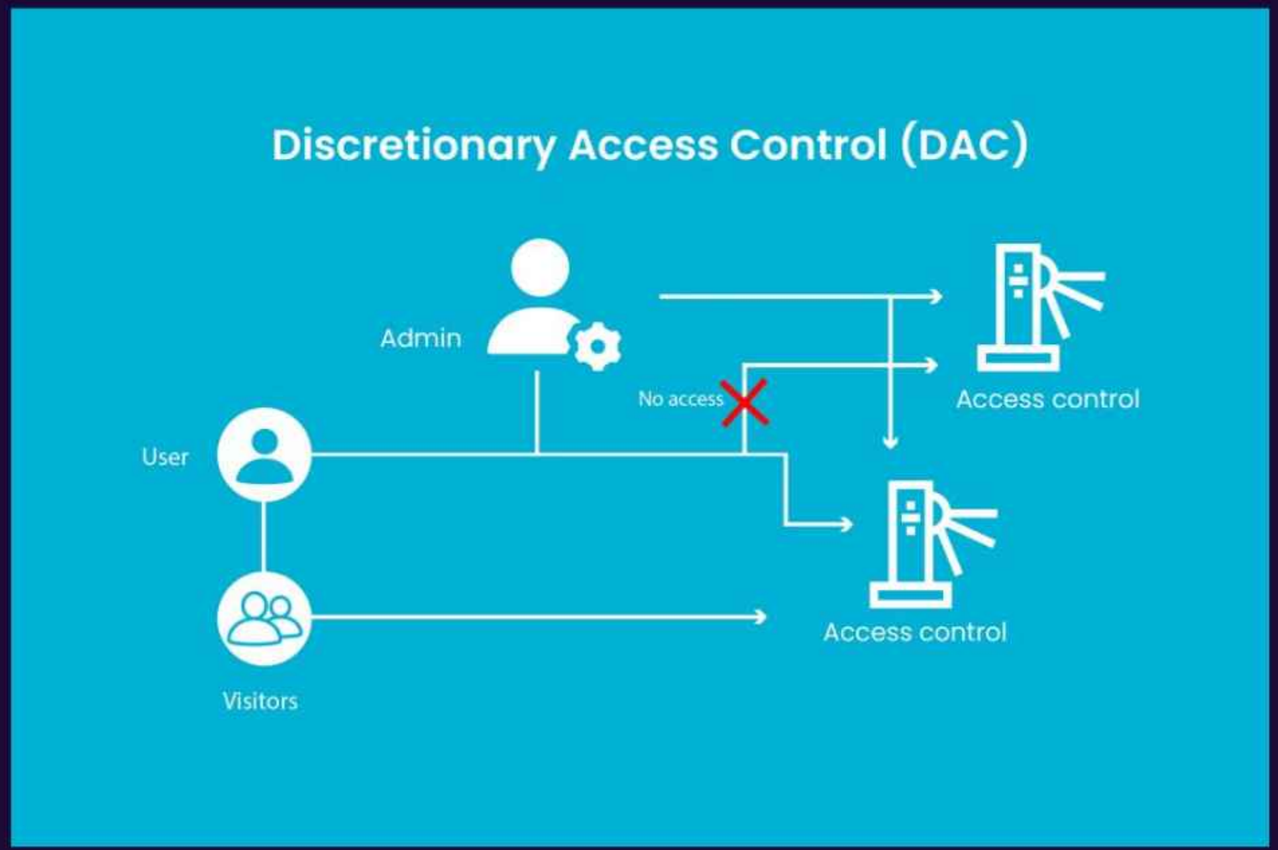
RBAC (Role-Based)



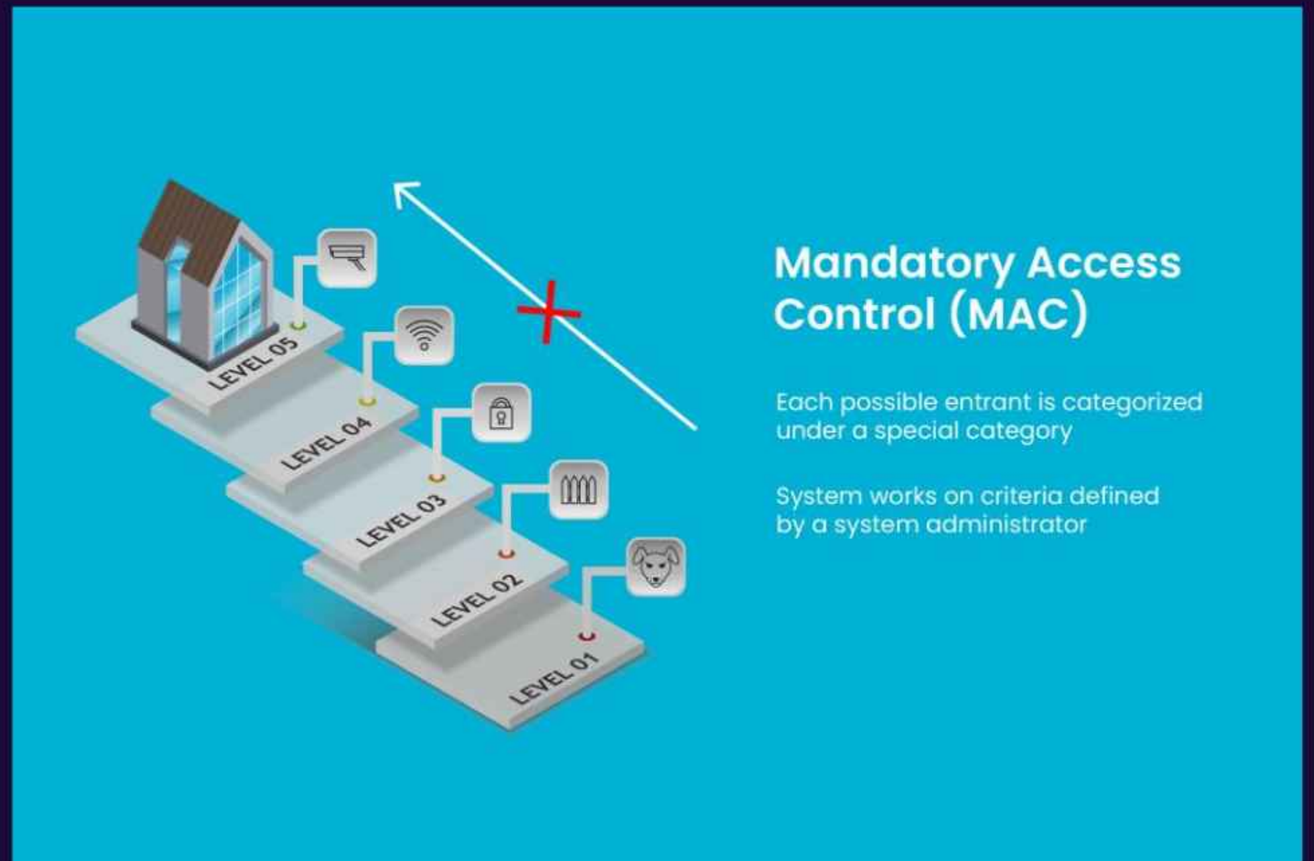
Need-To-Know


User Nathan
Clearance: Top Secret
Need-to-know: Alpha
Datacenter C
Datacenter TS
Confidential
Top Secret
Files
Alpha
Bravo
Charly
Alpha
Bravo
Charly

DAC


Discretionary Access Control (DAC)
Admin
No access
Access control
User
Access control
Visitors

MAC


LEVEL 05
LEVEL 04
LEVEL 03
LEVEL 02
LEVEL 01
Mandatory Access Control (MAC)
Each possible entrant is categorized under a special category
System works on criteria defined by a system administrator

Isolasi Proses?

Isolasi proses dalam sistem operasi mengacu pada strategi yang digunakan untuk memastikan bahwa proses-proses yang berjalan secara bersamaan tidak dapat mengganggu atau mempengaruhi proses lain secara tidak langsung. Isolasi proses ini dilakukan dengan cara membagi sumber daya sistem, seperti memori dan CPU, menjadi bagian-bagian yang terisolasi dan tidak dapat diakses secara langsung oleh proses lain. Dengan demikian, setiap proses dapat berjalan secara independen dan tidak dapat mengganggu proses lain, memastikan stabilitas dan keamanan sistem operasi.

Implementasi Isolasi Proses

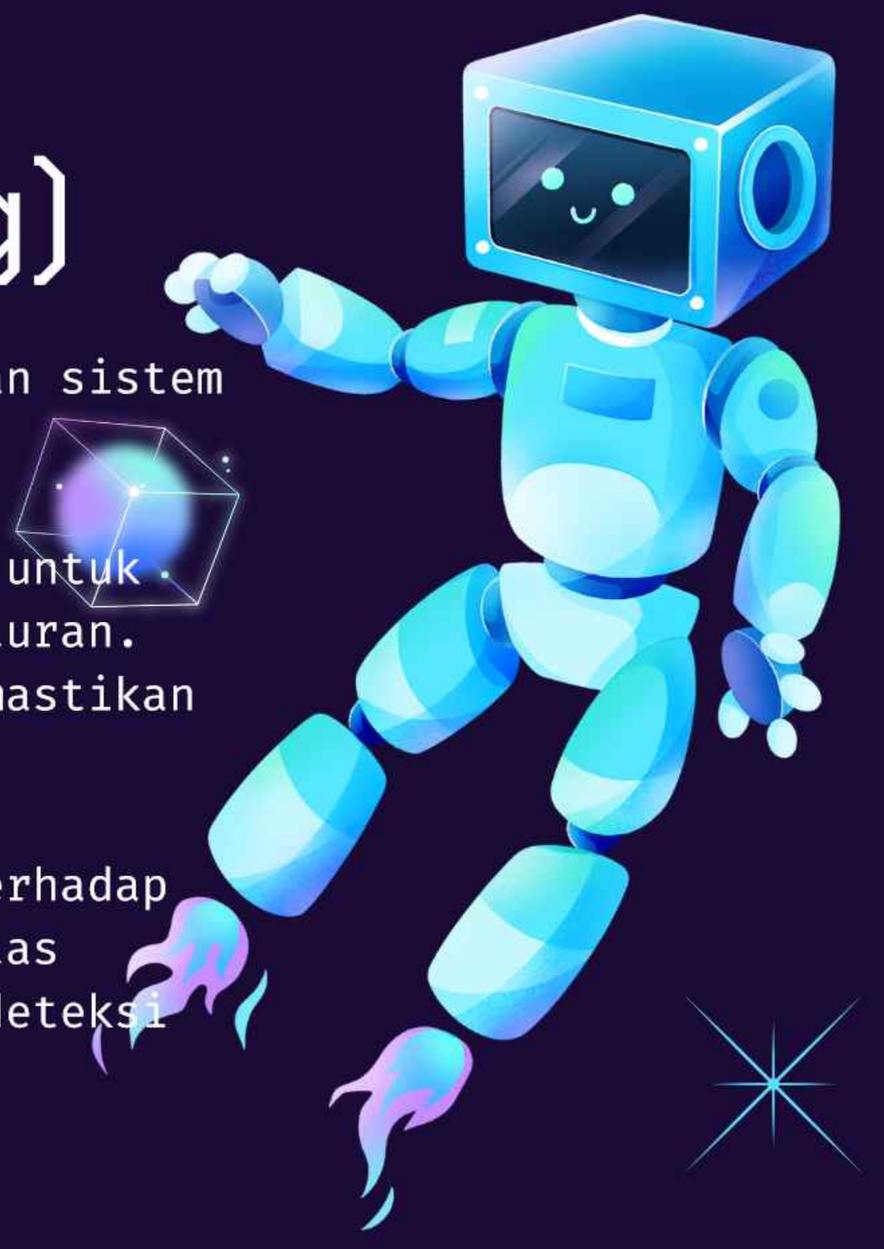
Ruang Alamat Virtual: Mekanisme ini membagi memori sistem menjadi bagian-bagian yang terisolasi dan tidak dapat diakses secara langsung oleh proses lain.	**Kontrol Hak Akses:** Kontrol hak akses memastikan bahwa hanya kode yang sah dan memiliki hak akses yang sesuai dapat mengakses sumber daya sistem.	**Pemisahan Memori:** Pemisahan memori memungkinkan setiap proses memiliki bagian memori yang terisolasi dan tidak dapat diakses secara langsung oleh proses lain.

Pemantauan (Monitoring)

Audit dan pemantauan adalah proses penting dalam keamanan sistem operasi.

- Audit: Ini melibatkan pemeriksaan dan evaluasi sistem untuk memastikan kepatuhan terhadap standar keamanan dan peraturan. Tujuannya adalah mengidentifikasi celah keamanan dan memastikan kepatuhan dengan kebijakan yang ditetapkan.

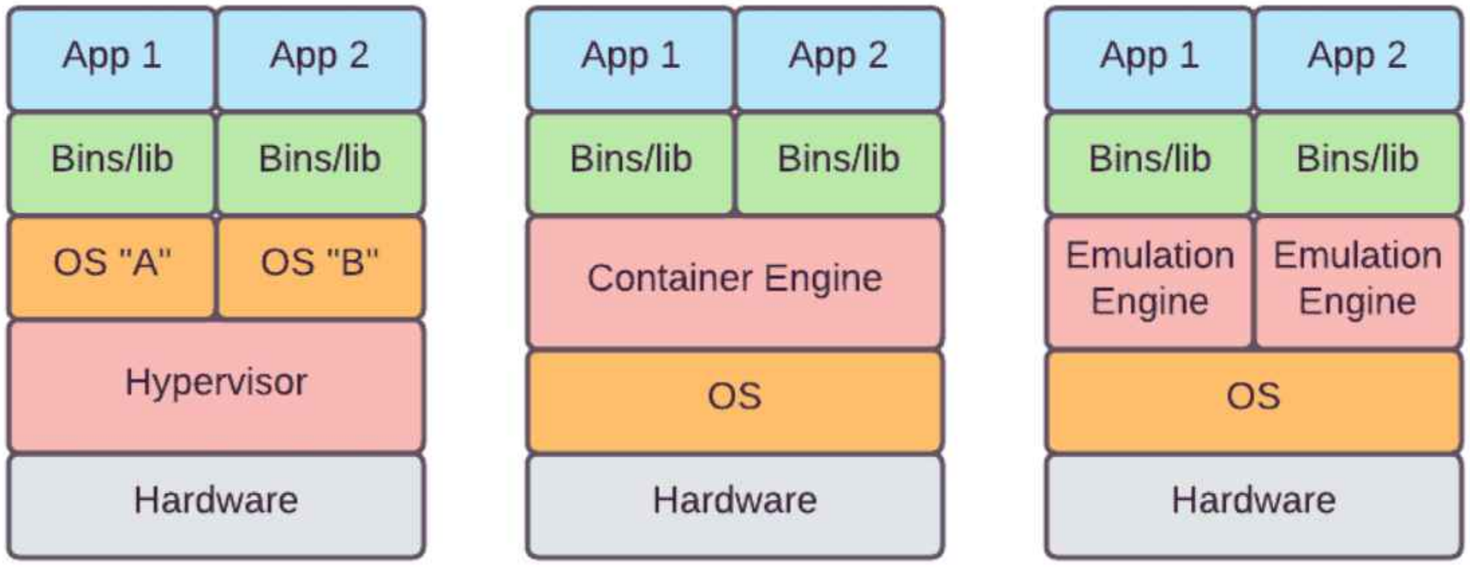
- Pemantauan: Ini melibatkan pengawasan terus-menerus terhadap sistem, jaringan, atau aplikasi untuk mendeteksi aktivitas mencurigakan atau masalah kinerja. Tujuannya adalah mendeteksi ancaman keamanan dan merespons dengan cepat.



Sandboxing?

Sebuah mekanisme keamanan yang mengisolasi sebuah program, mempersempit akses dan izin untuk mengakses sumber daya sistem. Mirip seperti kontainer yang memisahkan satu barang dari dunia luar (aplikasi ke sistem) di mana program berjalan tetapi dengan akses dan izin seperlunya dan sekecil mungkin.

Jenis Sandboxing



Keamanan Jaringan?

Merupakan proteksi infrastuktur bagian jaringan dari akses yang tidak diinginkan, penyalahgunaan, bahkan pencurian. Memiliki peran terhadap pembuatan infrastruktur jaringan yang aman untuk perangkat, aplikasi, pengguna, dan aplikasi pekerja (work apps) yang memenuhi standar keamanan.

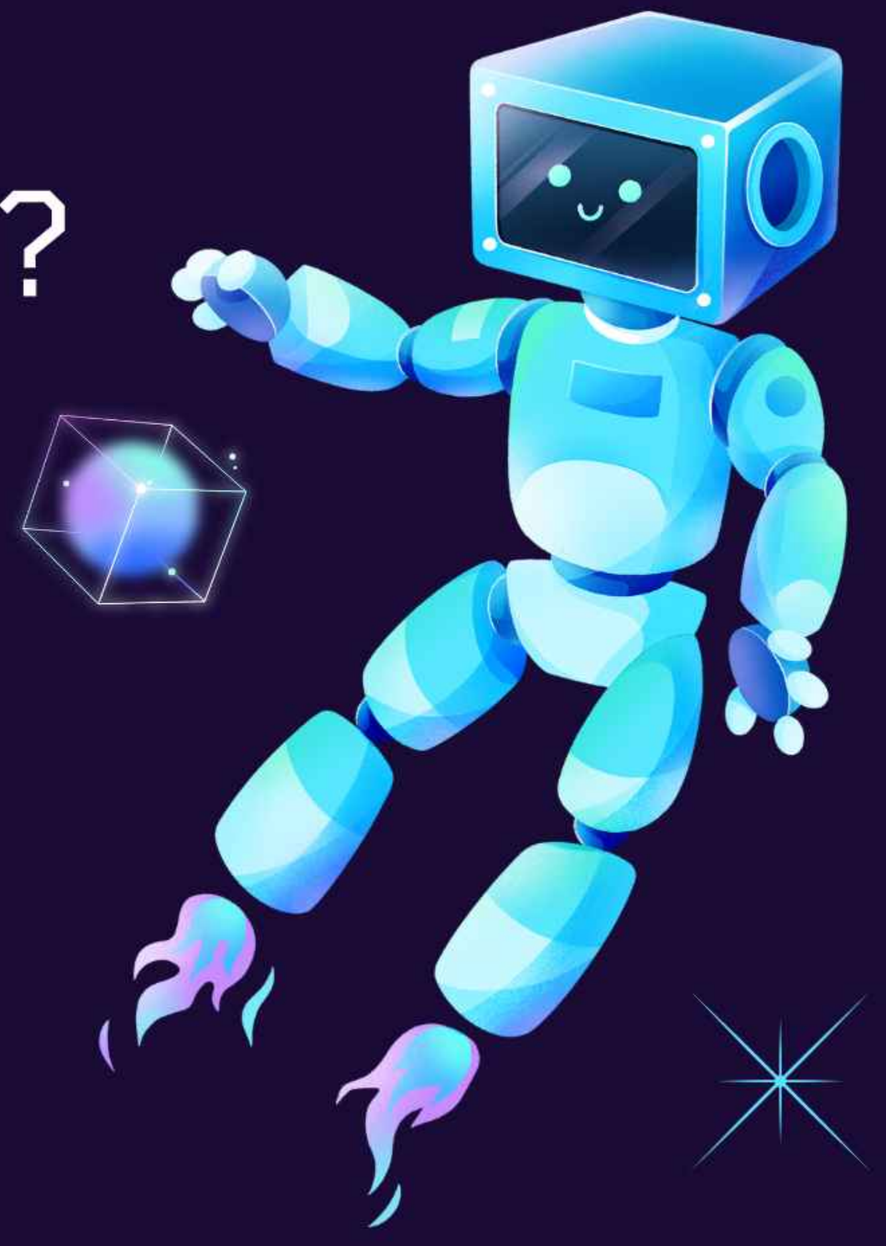
Pengamanan Jaringan

FIREWALL	INTRUSION DETECTION	AUTHENTICATION
Firewall adalah sebuah perangkat atau sistem software yang digunakan untuk membatasi akses ke jaringan. Firewall dapat diatur untuk hanya mengizinkan maupun memblokir traffic yang diinginkan	Intrusion Detection System adalah sistem keamanan komputer yang dirancang untuk mendeteksi aktivitas tidak sah atau mencurigakan pada sebuah perangkat.	Authentication memastikan bahwa hanya pengguna yang sah yang dapat mengakses jaringan atau data. Ini dapat dilakukan dengan menggunakan kata sandi atau metode lainnya seperti file authentikasi

Enkripsi dan Dekripsi ?

Encryption atau enkripsi adalah proses untuk membuat suatu susunan acak dari teks yang dapat dibaca oleh manusia (human-readable plaintext) menjadi teks yang tidak dapat dibaca oleh manusia hanya dimengerti oleh sistem saja Teks hasil dari enkripsi disebut dengan “ciphertext”

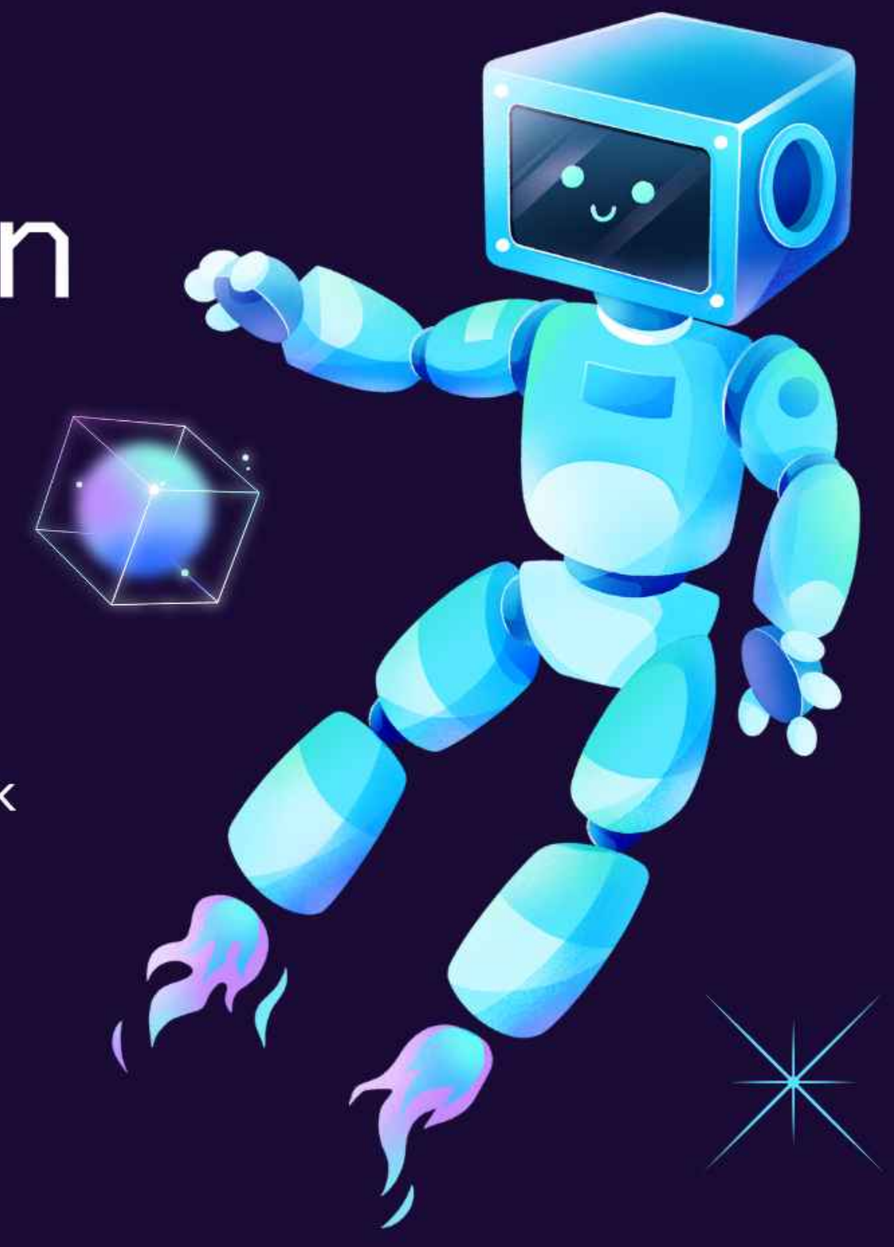
Dekripsi adalah proses mengonversi ciphertext kembali ke teks biasa.



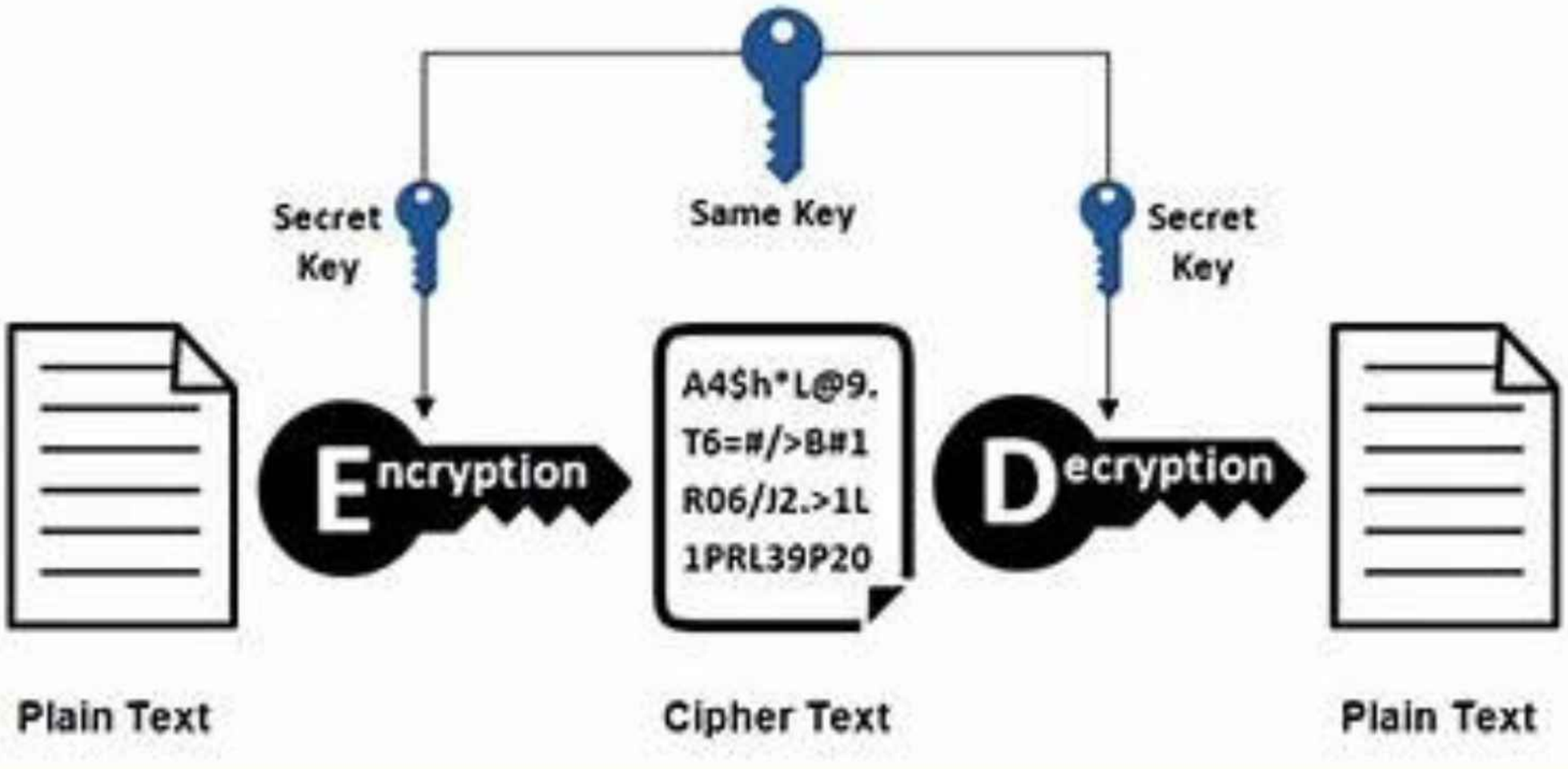
Jenis-jenis enkripsi

Symmetric encryption

Enkripsi simetrik ini memiliki nama lain yaitu secret key encryption. Jenis ini hanya menggunakan satu buah kunci atau key sehingga pengirim dan penerima informasi memiliki kunci yang identik. Jadi pengirim atau sistem harus memberikan kuncinya kepada siapa saja yang berhak mendekripsikan pesan atau informasi. Contoh algoritma yang sering digunakan oleh enkripsi simetrik ini adalah Caesar, Blowfish, dan Advanced Encryption Standard atau AES.

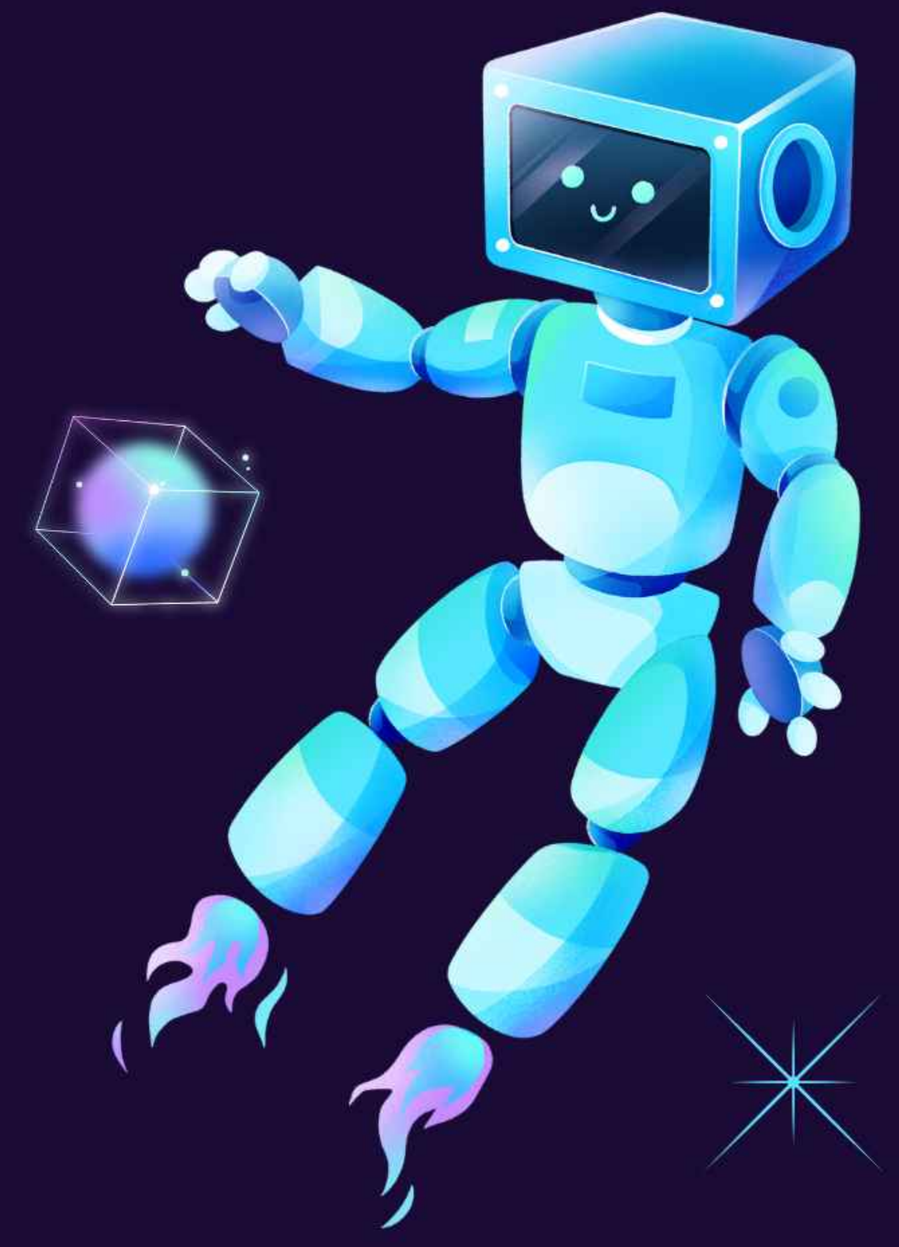


Symmetric Encryption

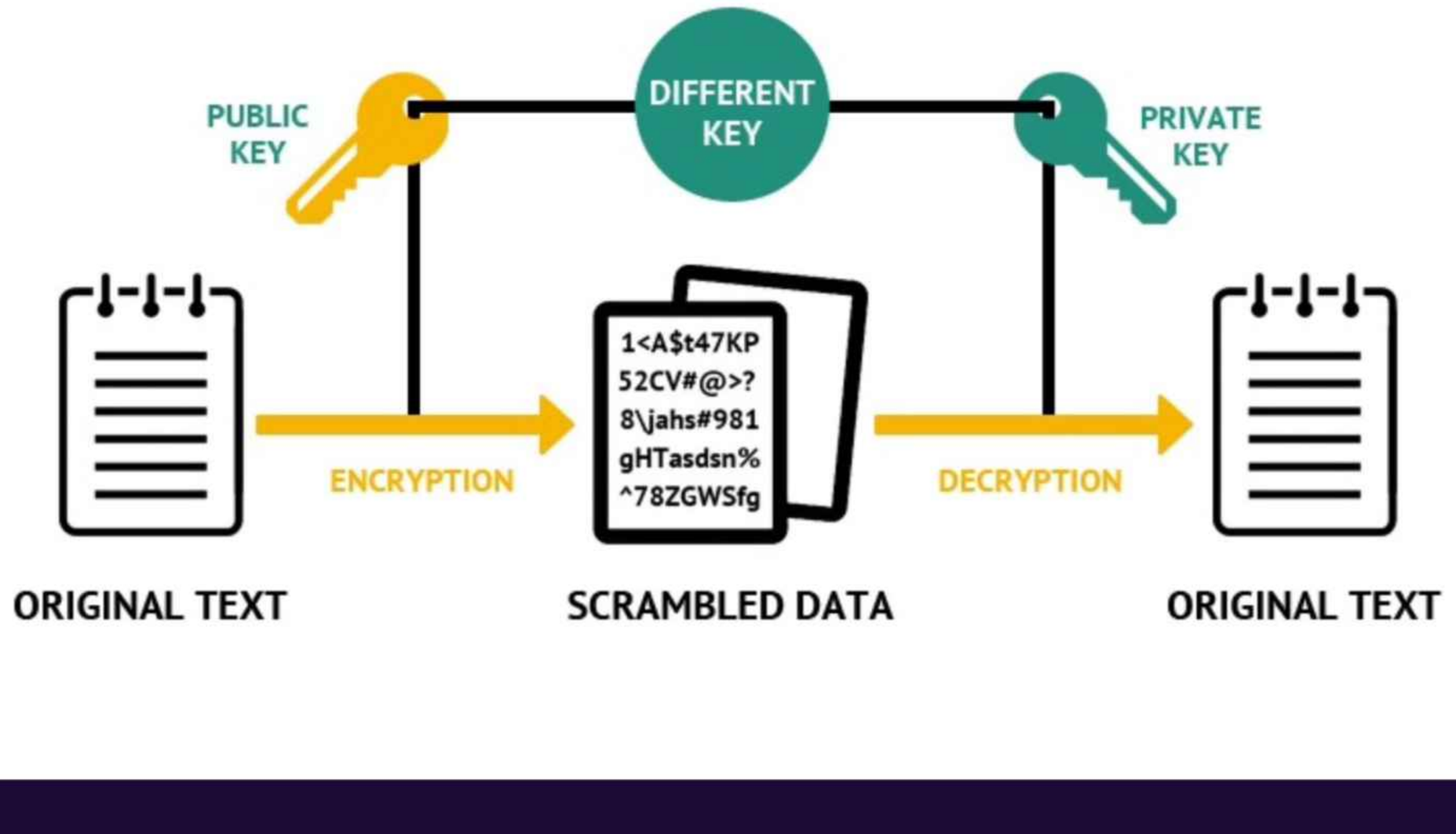


Asymmetric encryption

Asymmetric encryption
Jenis enkripsi asimetrik ini memiliki nama lain yaitu public key encryption. Berbeda dari jenis simetrik, jenis ini menggunakan dua buah kunci atau key yang berbeda tetapi saling berhubungan. Key itu biasanya disebut dengan public key dan private key.

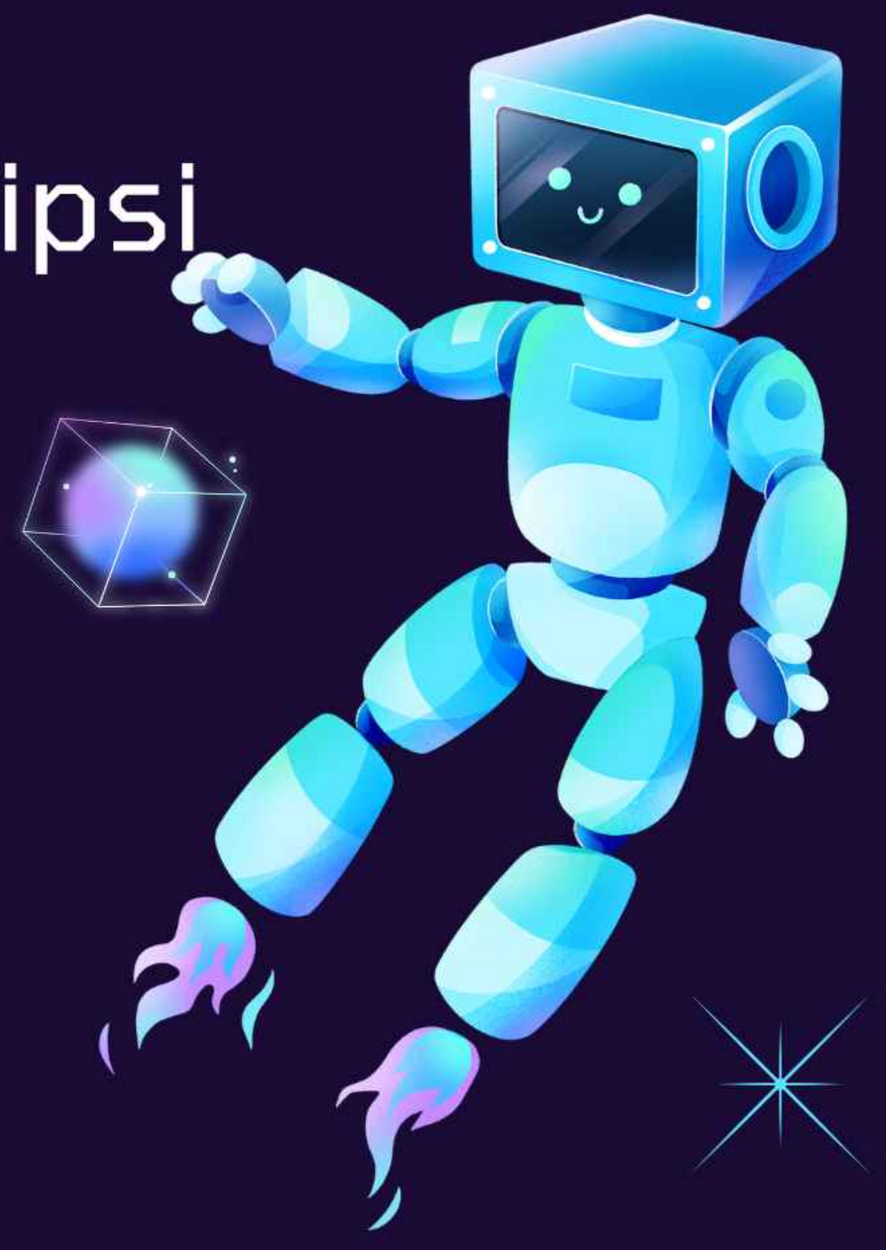


Asymmetric Encryption



Fungsi dan Manfaat enkripsi

- Menjamin kerahasiaan data
- Melindungi saluran percakapan (Aplikasi chat dan email yang Anda miliki)
- Memberikan perlindungan pada keuangan Anda yang disimpan secara digital
- Dapat digunakan sebagai digital signature



Patch Management?

Apa itu Patch Management?
Patch Management adalah proses yang melibatkan identifikasi, pengujian, dan penerapan pembaruan perangkat lunak, termasuk pembaruan keamanan yang dirilis oleh penyedia perangkat lunak untuk mengatasi kerentanan yang ditemukan.

Mengapa Patch Management Penting?

Patch Management penting karena melindungi sistem dari eksploitasi kerentanan yang bisa dimanfaatkan oleh penyerang. Dengan menginstal pembaruan perangkat lunak, perusahaan dapat mencegah kebocoran data sensitif dan memastikan kelancaran operasi bisnis.

Manfaat Patch Management

Praktik Patch Management membantu organisasi untuk menjaga sistem mereka tetap aman dari serangan malware dan ancaman keamanan lainnya. Dengan mengelola pembaruan perangkat lunak secara efektif, perusahaan dapat mengurangi risiko keamanan dan meningkatkan keandalan sistem mereka.

Key Management

Manajemen kunci berperan penting dalam mempertahankan keamanan data dengan kunci enkripsi yang menjadi dasar untuk melindungi data sensitif, sehingga tanpanya, upaya keamanan data bisa menjadi tidak efektif.

01	02	03	04	05
Membuat kunci enkripsi yang kuat dan unik untuk setiap kebutuhan sistem.	Menyimpan kunci secara aman menggunakan teknik kriptografi tambahan atau hardware keamanan.	Distribusi/mengirimkan kunci hanya kepada pihak berwenang secara terenkripsi.	Rotasi kunci dengan memperbarui kunci secara berkala untuk mengurangi risiko kompromi keamanan.	Memastikan akses hanya kepada pengguna yang diotorisasi.

Fungsi Utama Manajemen Kunci

01

Backup secara teratur untuk mencegah kehilangan data dan pemulihan ketika terjadi kehilangan atau kerusakan.

02

Pencabutan dan penghancuran untuk mengatasi kunci yang telah terancam kerahasiaannya (dikompromikan).

Tindakan Penting Dalam Manajemen Kunci

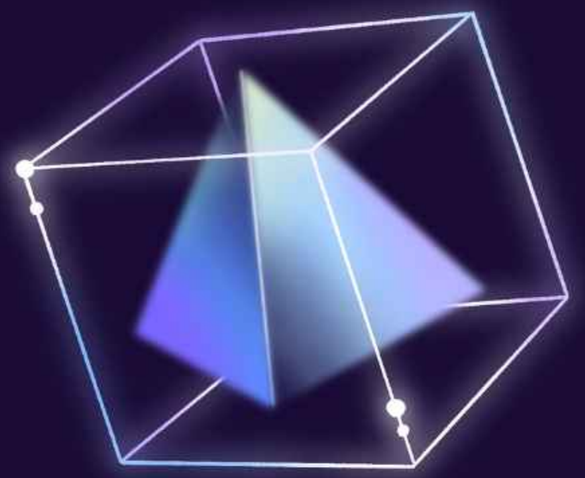
01

Kebijakan keamanan untuk mengatur penggunaan dan akses kunci.

02

Pemisahan tugas untuk mengurangi risiko kebocoran data karena satu individu atau entitas tidak memiliki kontrol penuh atas semua aspek manajemen kunci.

Penerapan Kebijakan Manajemen Kunci



Terima Kasih!