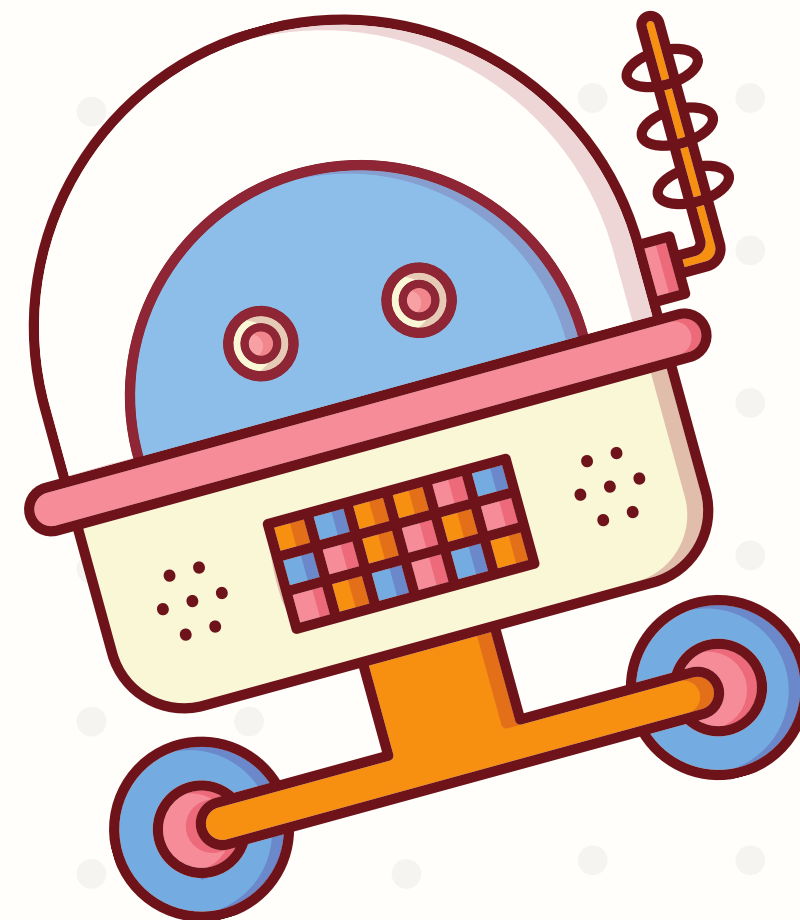
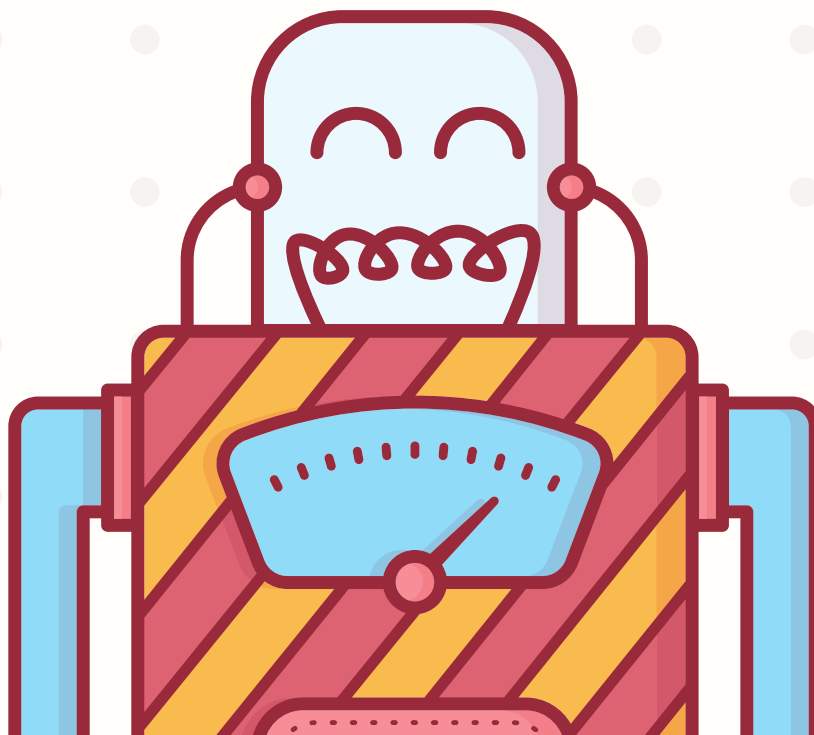
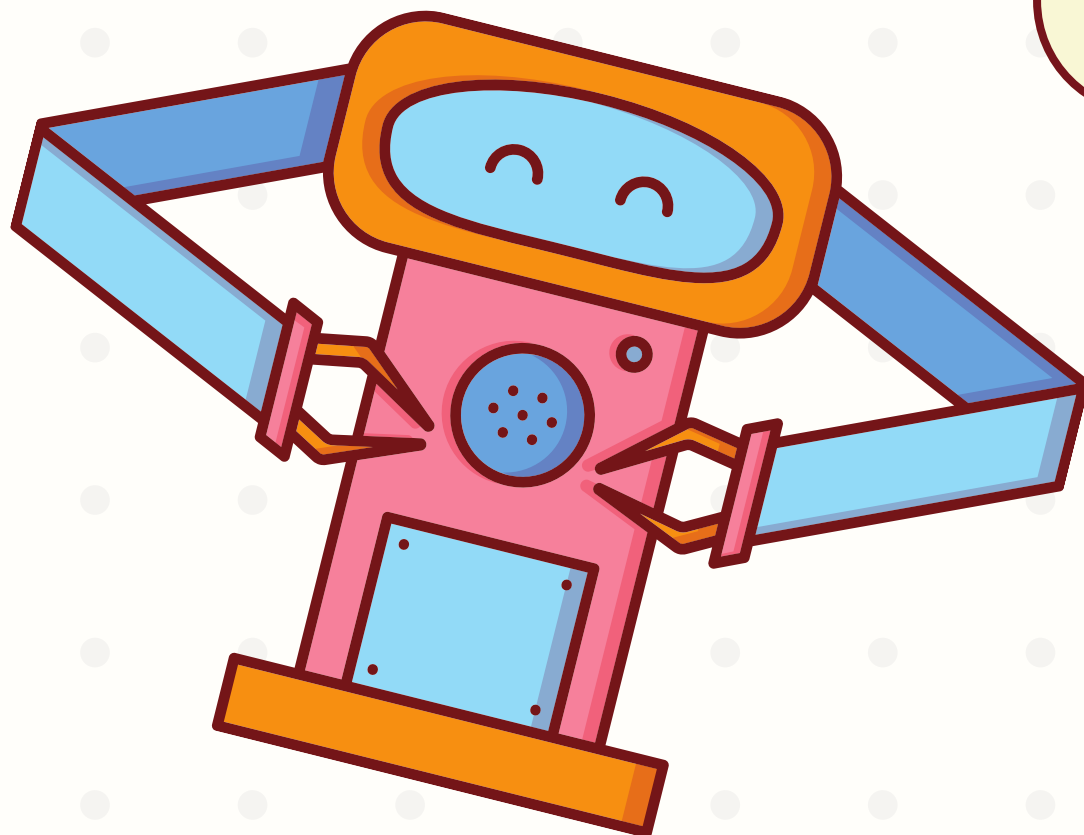


DISTRIBUTED OR HYBRID IPS

Keamanan Siber



ANGGOTA KELOMPOK

21102070 Muhammad Ilmi

21102110 Gilang Riyanto

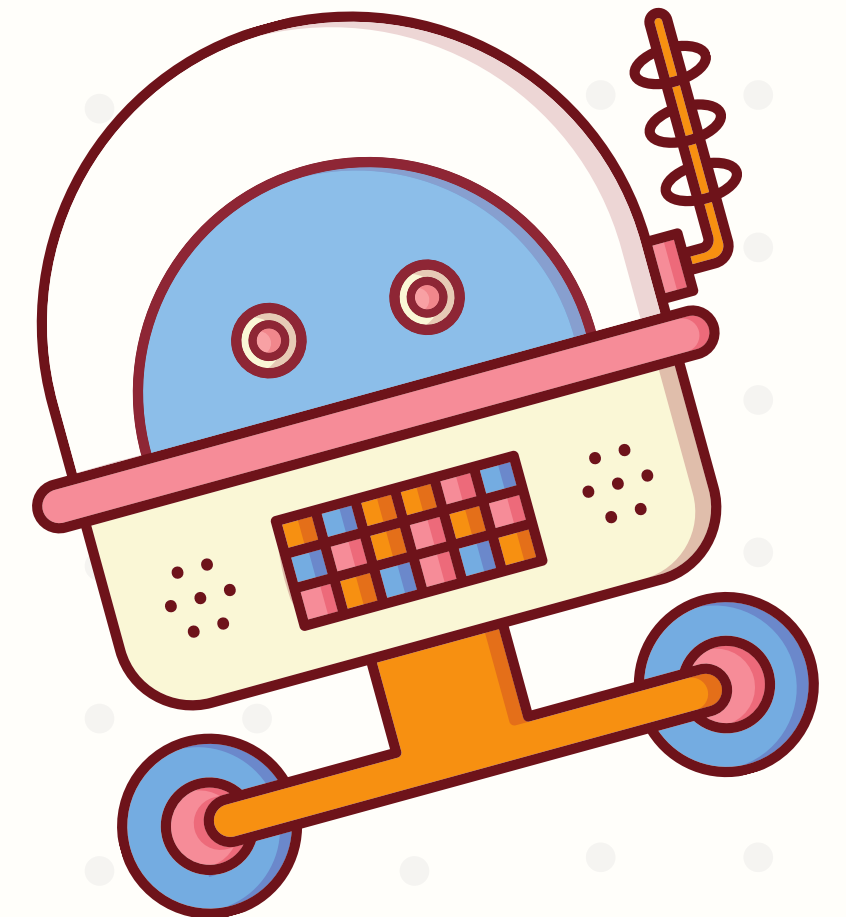
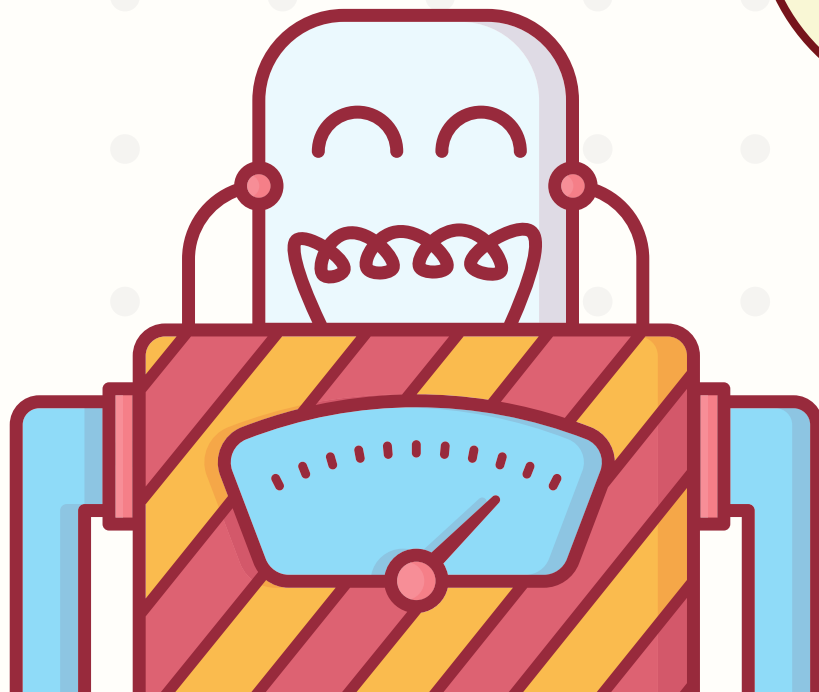
21102240 Sri Rejeki

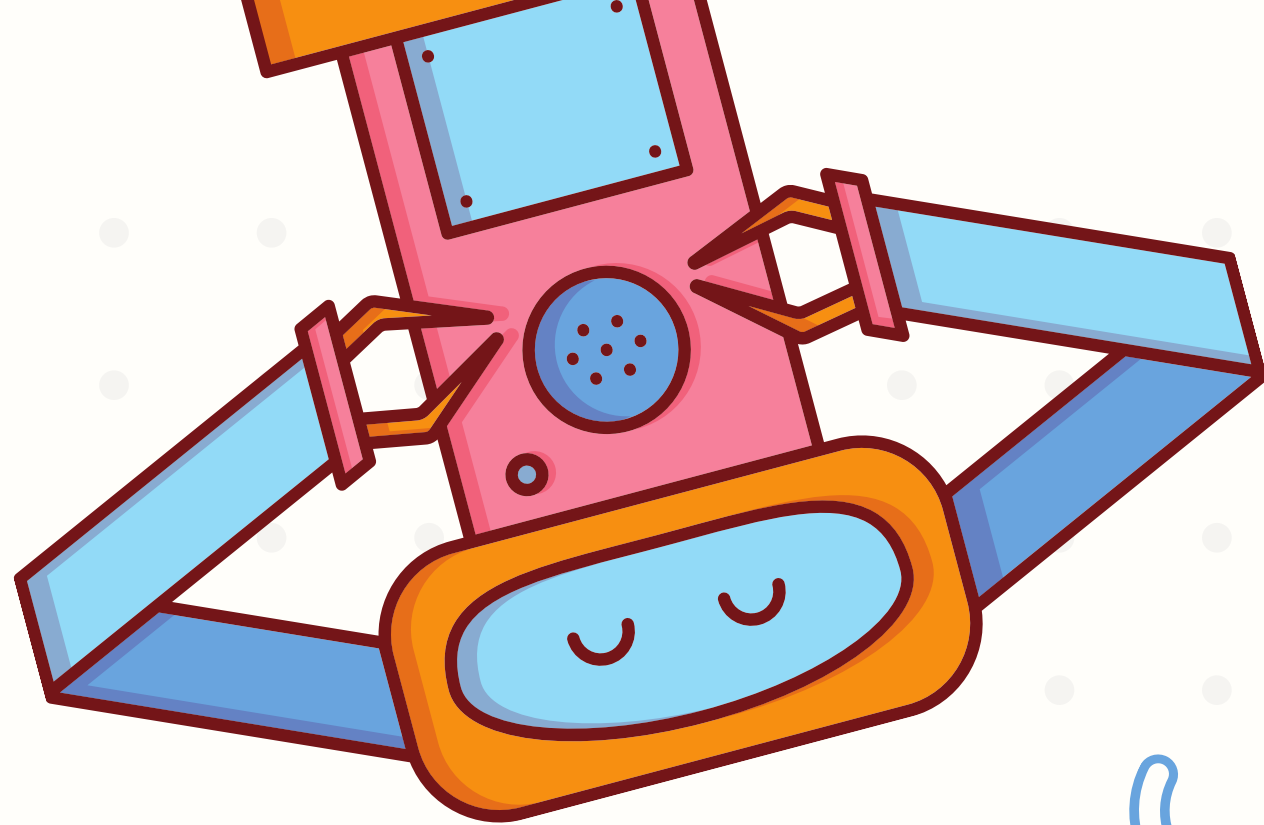
21102242 Amanda Dzunuri Elvira Yaniar

21102260 Ahmad Tri Fhatoni

21102279 Abdul Aziz

21102291 Agyl Restu Hermanto

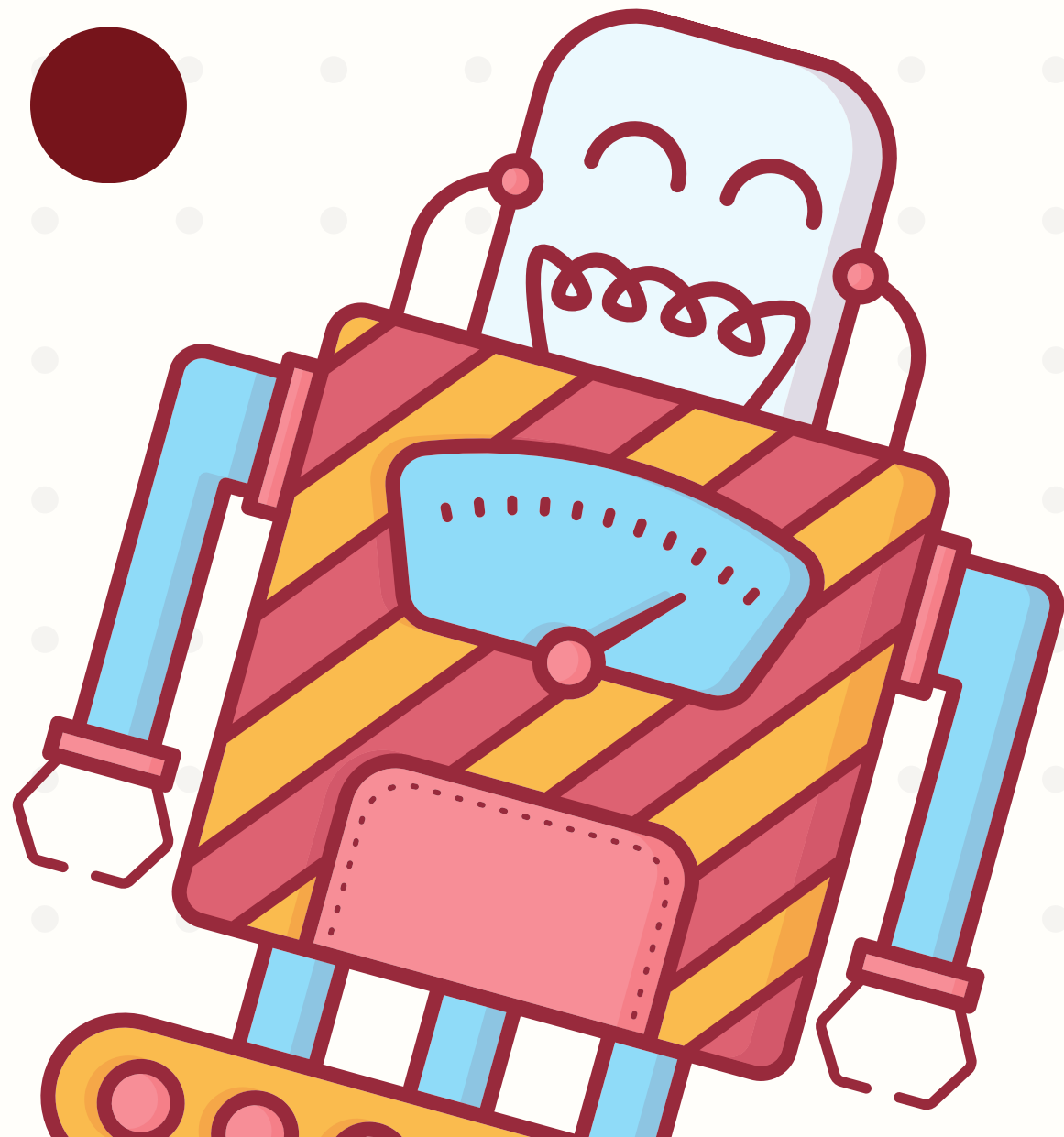




DEFINISI IPS

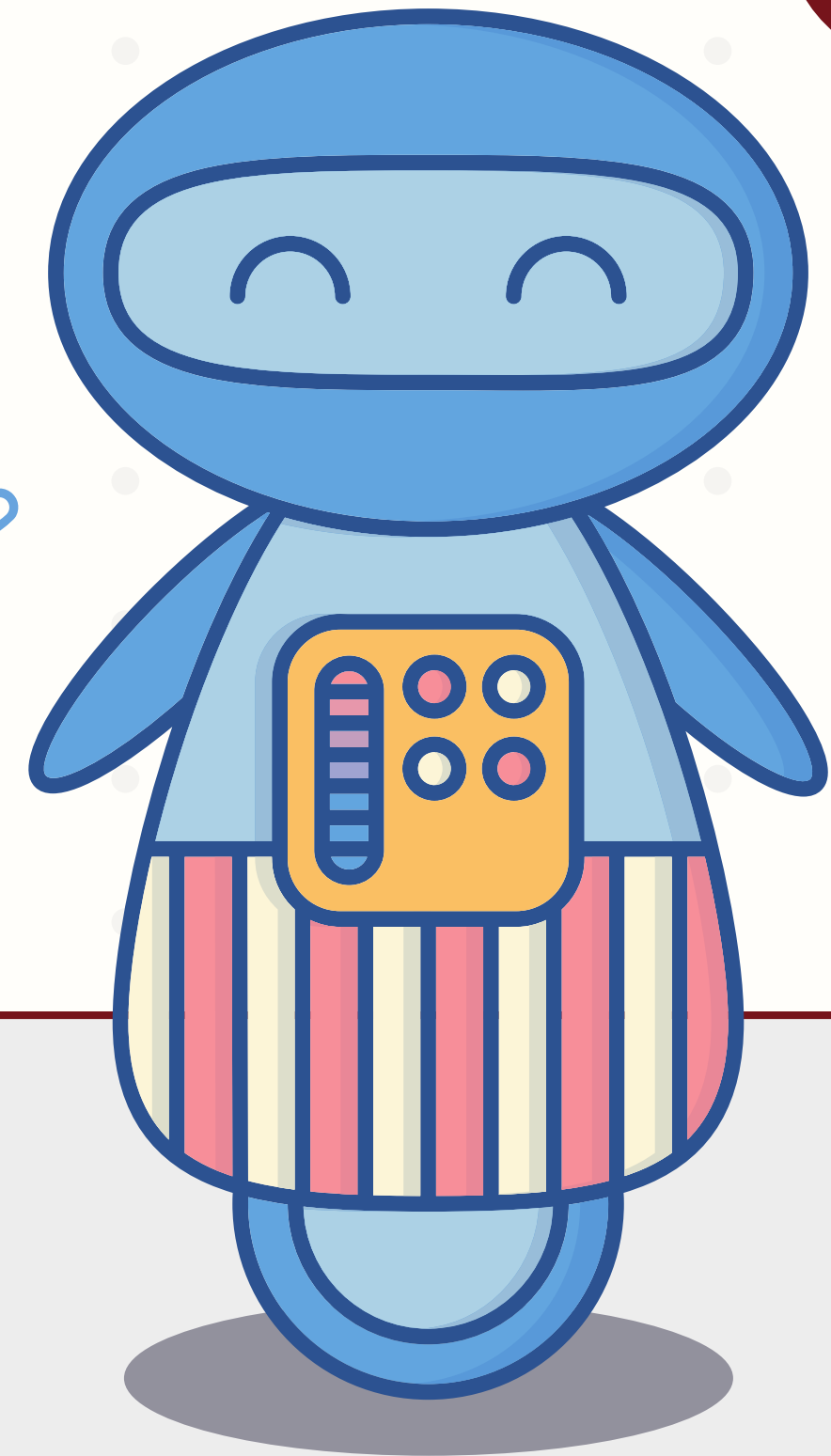
Intrusion Prevention System (IPS) adalah sistem yang dirancang untuk mendeteksi dan mencegah ancaman keamanan dalam jaringan.

Dengan meningkatnya serangan siber, IPS menjadi komponen penting dalam melindungi data dan infrastruktur TI.



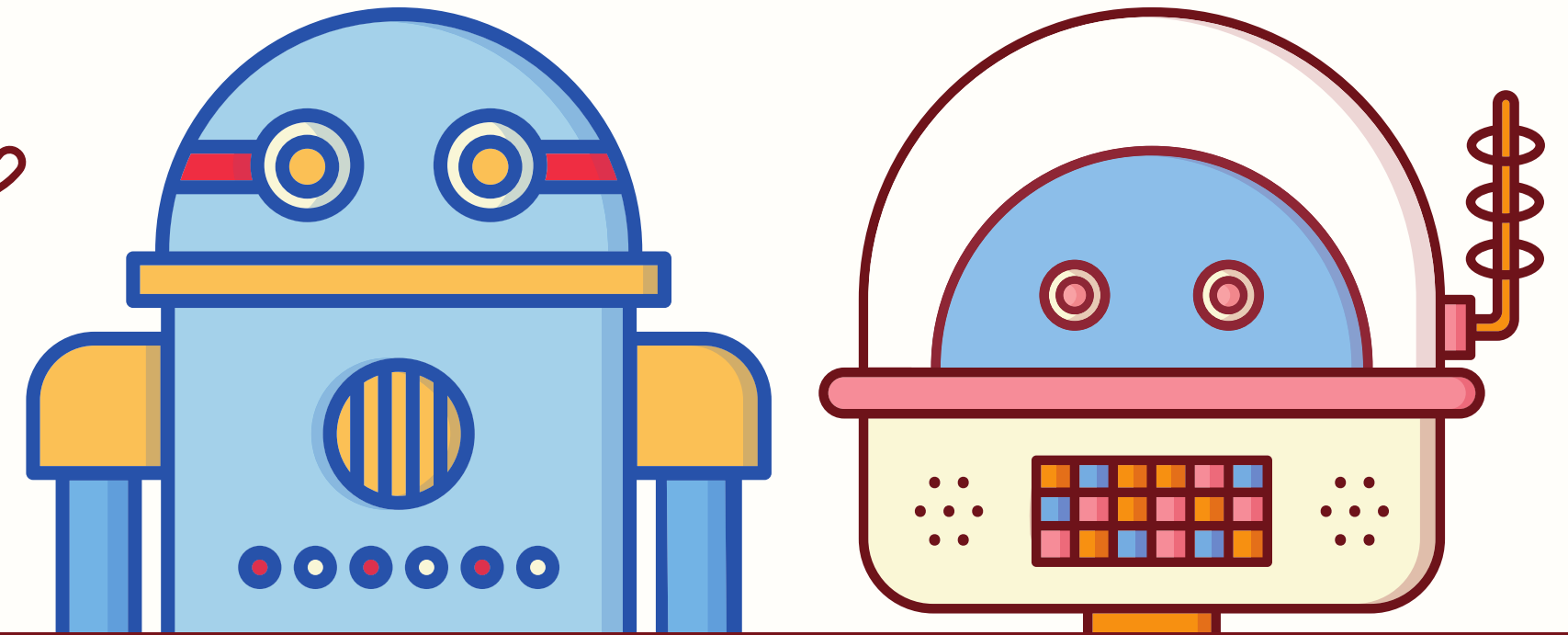
DISTRIBUTED INTRUSION PREVENTION SYSTEMS [DIPS]

Distributed IPS, solusi keamanan jaringan yang beroperasi di berbagai lokasi atau perangkat untuk mendeteksi dan mencegah intrusi. Sistem ini menggunakan arsitektur terdistribusi, memungkinkan deteksi ancaman secara real-time dan respons di berbagai segmen jaringan. Berbeda dengan IPS tradisional yang mungkin terpusat, sistem terdistribusi dapat menganalisis lalu lintas secara lokal di berbagai titik dalam jaringan, sehingga mengurangi latensi dan meningkatkan waktu respons.







LANJUTAN...

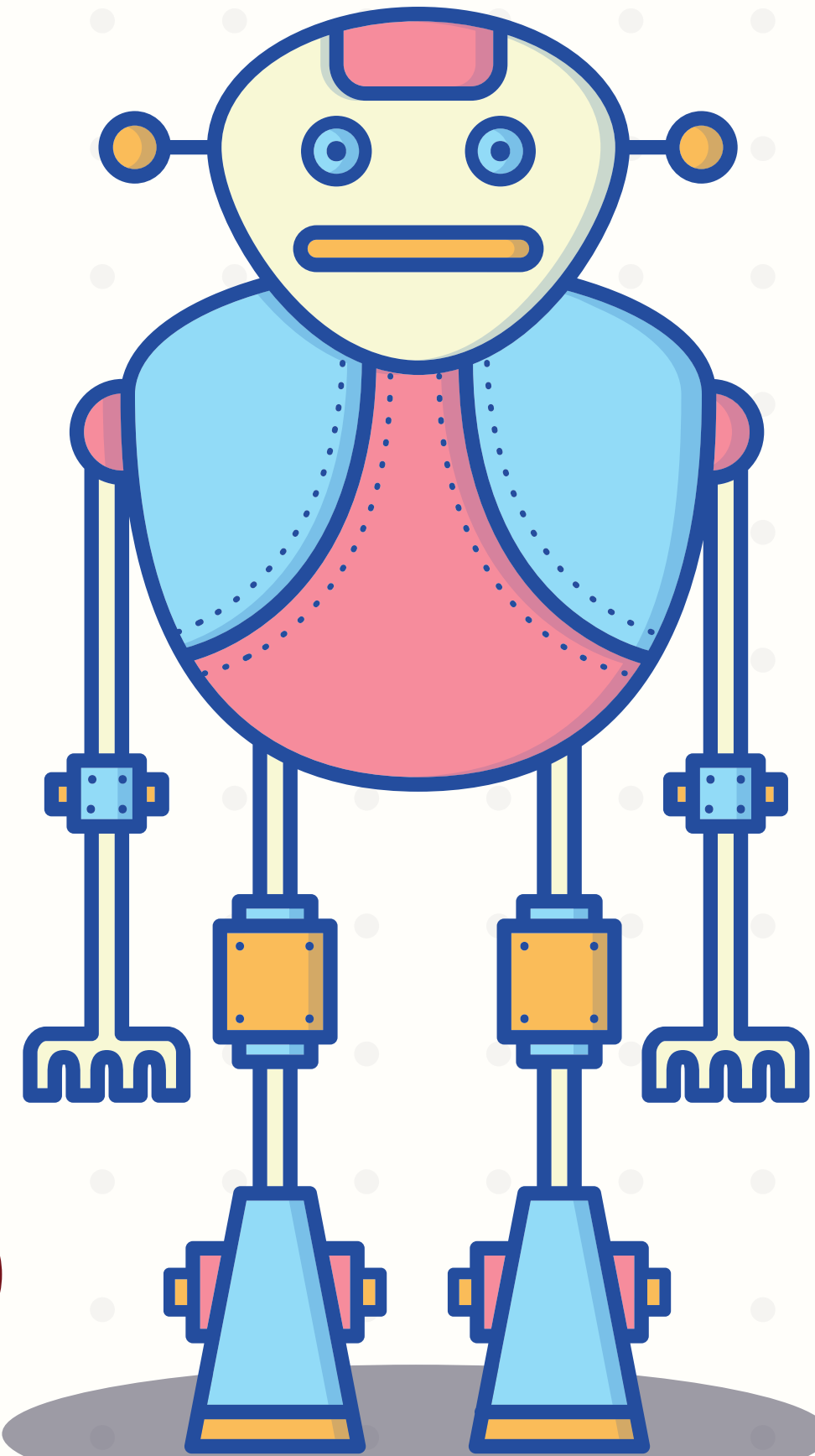


FITUR UTAMA DIPS

- 
- Deteksi Ancaman Real-Time: Memantau aktivitas mencurigakan di seluruh jaringan.
 - Respons Otomatis: Memblokir lalu lintas berbahaya secara otomatis.
 - Skalabilitas: Dapat berkembang seiring pertumbuhan organisasi tanpa konfigurasi ulang yang signifikan.

CONTOH IMPLEMENTASI DIPS

- 
- VMware NSX Distributed IDS/IPS: Mengintegrasikan fungsi IDS/IPS ke dalam setiap workload.
 - Memungkinkan deteksi ancaman di lalu lintas internal (east-west).
 - Mengurangi kompleksitas operasional dan meningkatkan cakupan keamanan tanpa titik buta



HYBRID INTRUSION PREVENTION SYSTEMS [HIPS]

HIPS menggabungkan metode deteksi berbasis tanda tangan dan anomali untuk meningkatkan akurasi deteksi ancaman.

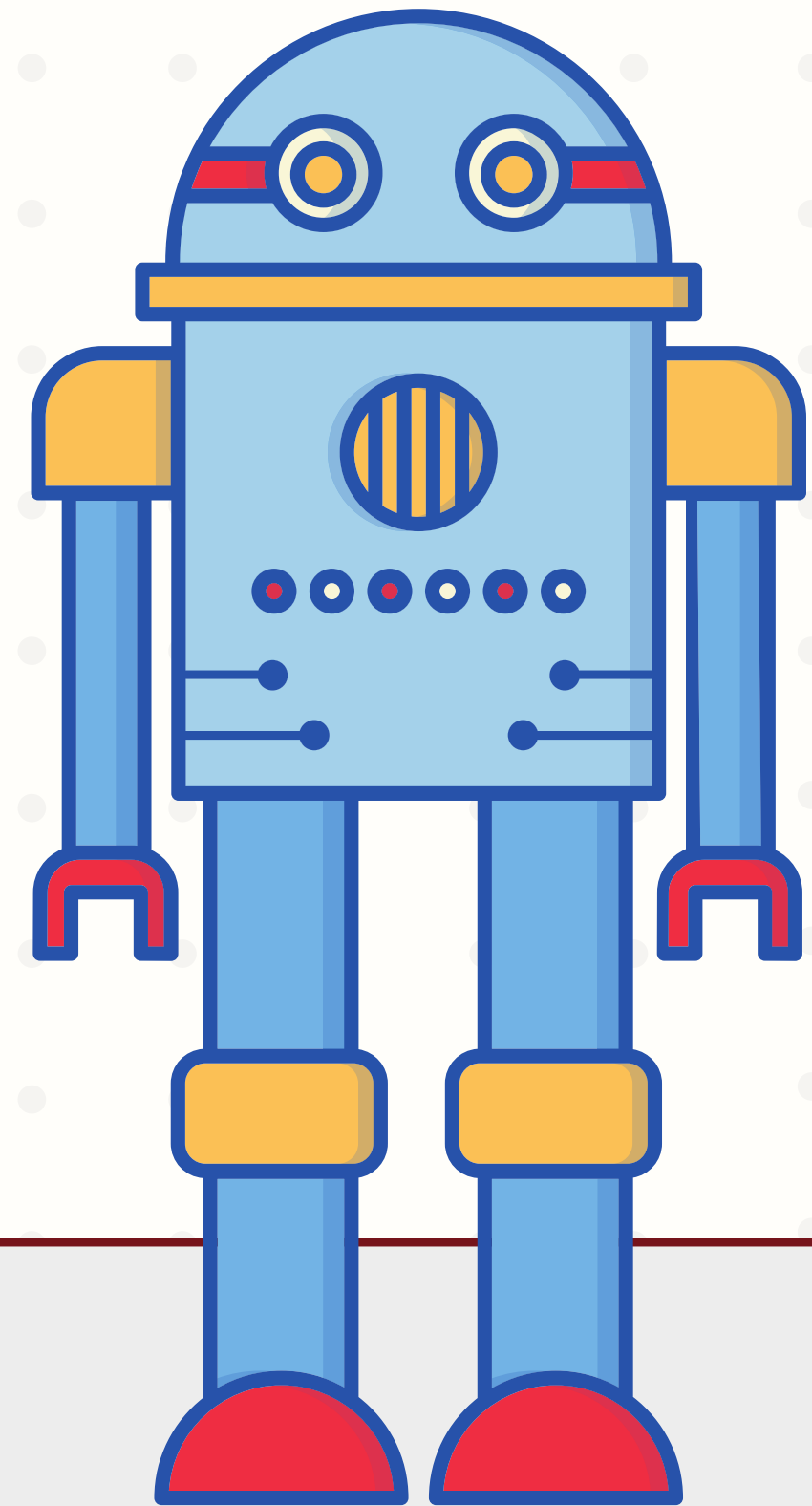
- Fungsi Utama: Mendeteksi ancaman yang dikenal dan tidak dikenal.
- Mengintegrasikan dengan solusi keamanan lainnya.

FITUR UTAMA HIPS

- Kemampuan Deteksi Komprehensif: Memanfaatkan kedua metode untuk meningkatkan akurasi.
- Integrasi dengan Solusi Keamanan Lainnya: Bekerja sama dengan firewall dan sistem SIEM.
- Fleksibilitas Penyebaran: Beroperasi di lingkungan cloud dan on-premise.

WAWASAN PENELITIAN HIPS

- Studi Kasus DDoS: Sistem deteksi intrusi hibrida yang dirancang untuk mendeteksi serangan DDoS menggunakan metode berbasis anomali dan tanda tangan
- Hasil menunjukkan bahwa sistem hibrida memberikan hasil yang lebih baik dibandingkan dengan sistem non-hibrida.





PENTINGNYA AKSESIBILITAS

01

Inklusivitas (Tidak semua orang dapat membeli perangkat mahal atau memiliki koneksi internet kencang. Menjadikan informasi mudah diakses berarti memperluas inklusi dan kesetaraan)

02

Pendidikan (Meningkatkan aksesibilitas informasi berarti meningkatkan akses ke peluang pendidikan dan memungkinkan lebih banyak orang menjadi lebih terdidik.)

03

Pengembangan Ekonomi (Dengan meningkatkan aksesibilitas informasi, kita dapat membuka peluang bisnis baru dan mendapatkan akses yang lebih mudah ke pasar global.)

MEMBANGUN KESEIMBANGAN ANTARA PRIVASI DAN AKSESIBILITAS

TRANSPARANSI

Kita harus transparan tentang informasi apa yang kita kumpulkan dan bagaimana kita akan menggunakannya.

INTERVENSI PENGGUNA

Pengguna harus dapat membuat perubahan atau menarik izin mereka kapan saja mereka mau.

OPT-IN

Pengguna harus memberikan izin sebelum data pribadi mereka digunakan.

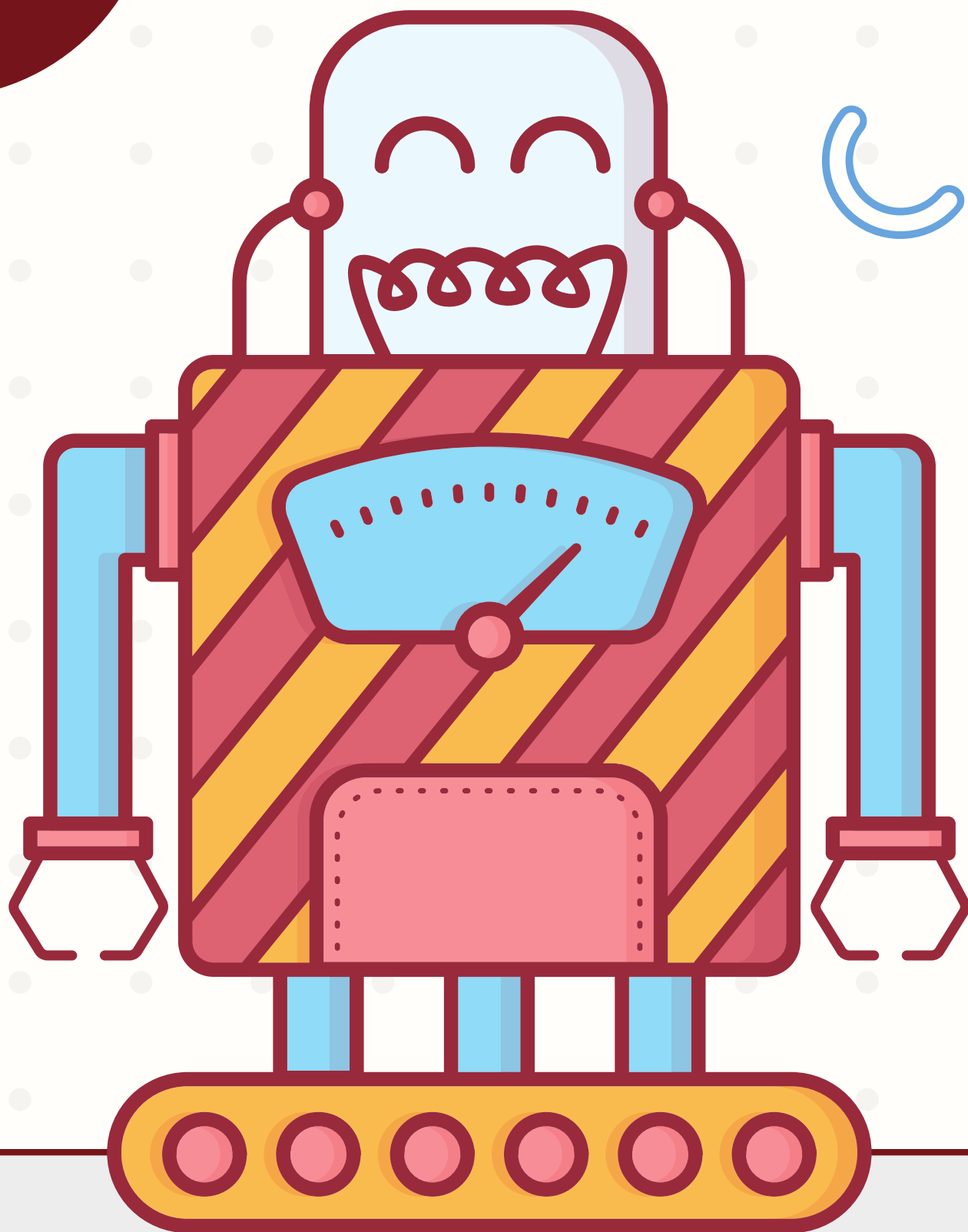
PERLINDUNGAN DATA

Data sensitif harus disimpan dengan aman dan tidak digunakan tanpa izin.

KESIMPULAN

DIPS dan HIPS memainkan peran penting dalam strategi keamanan siber modern.

Keduanya menawarkan perlindungan yang lebih baik melalui teknik deteksi canggih dan dapat mengakomodasi kompleksitas lingkungan TI hibrida.



REFERENSI

1. VMware NSX Distributed IDS/IPS. (n.d.). Diambil dari VMware.
2. Extreme Networks Intrusion Prevention System. (n.d.). Diambil dari Extreme Networks.
3. Özge, C., Büyükçorak, S., & Karabulut, K. G. (2016). Hybrid Intrusion Detection System for DDoS Attacks. Wiley Online Library. Diambil dari Wiley.
4. SAP IPS: Automated user management in hybrid landscapes. (n.d.). Diambil dari IBsolution.