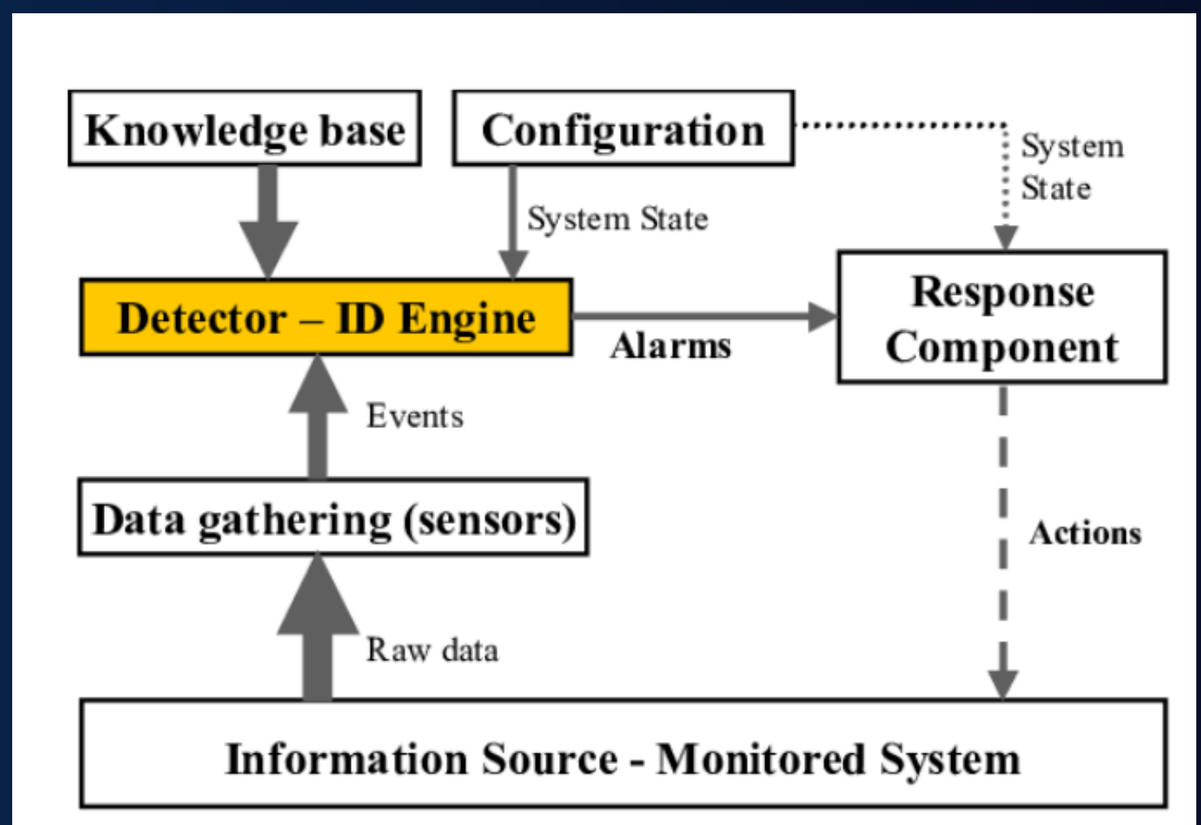
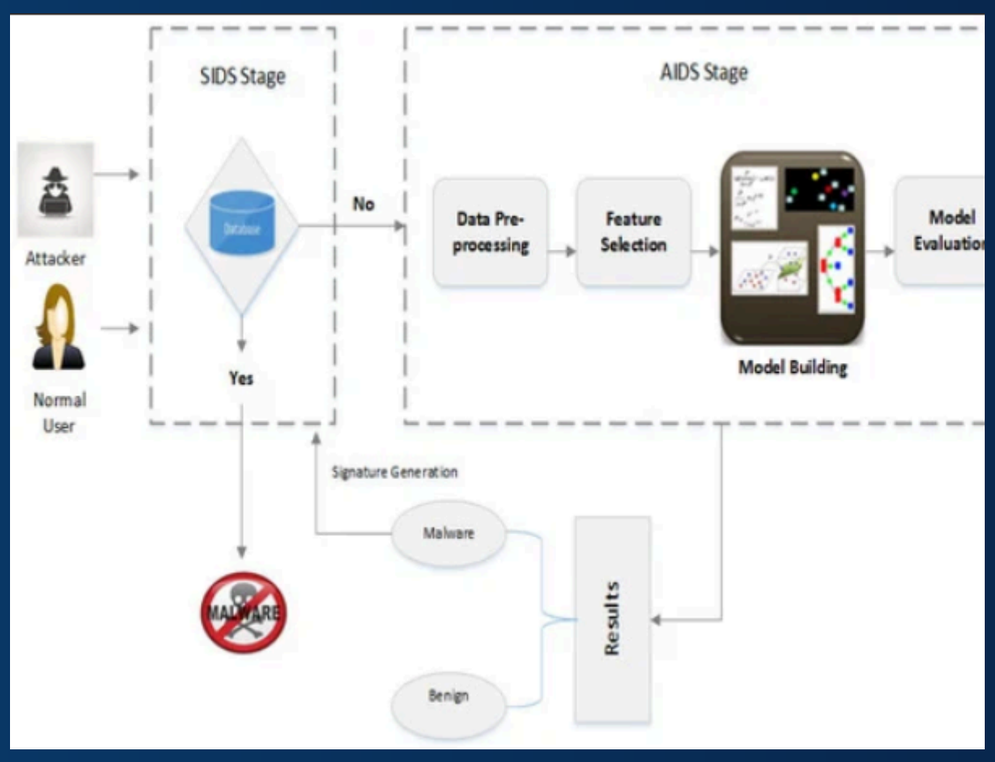
Securing the Digital Frontier: IDS & IPS

Introduction

- Intrusion Detection System (IDS)
- Monitors network traffic for suspicious activities and alerts when a potential threat is detected.
- Intrusion Prevention System (IPS)
- Not only detects but also prevents attacks by taking immediate action, such as blocking traffic or quarantining files.





How They Work

- IDS:
  - Analyzes network packets and system activities.
  - Alerts administrators of potential threats.
  - Example: A magnifying glass icon symbolizing detection and analysis.
- IPS:
  - Actively monitors and controls network traffic.
  - Blocks malicious activities in real-time.
  - Example: A shield with a checkmark representing protection and prevention.

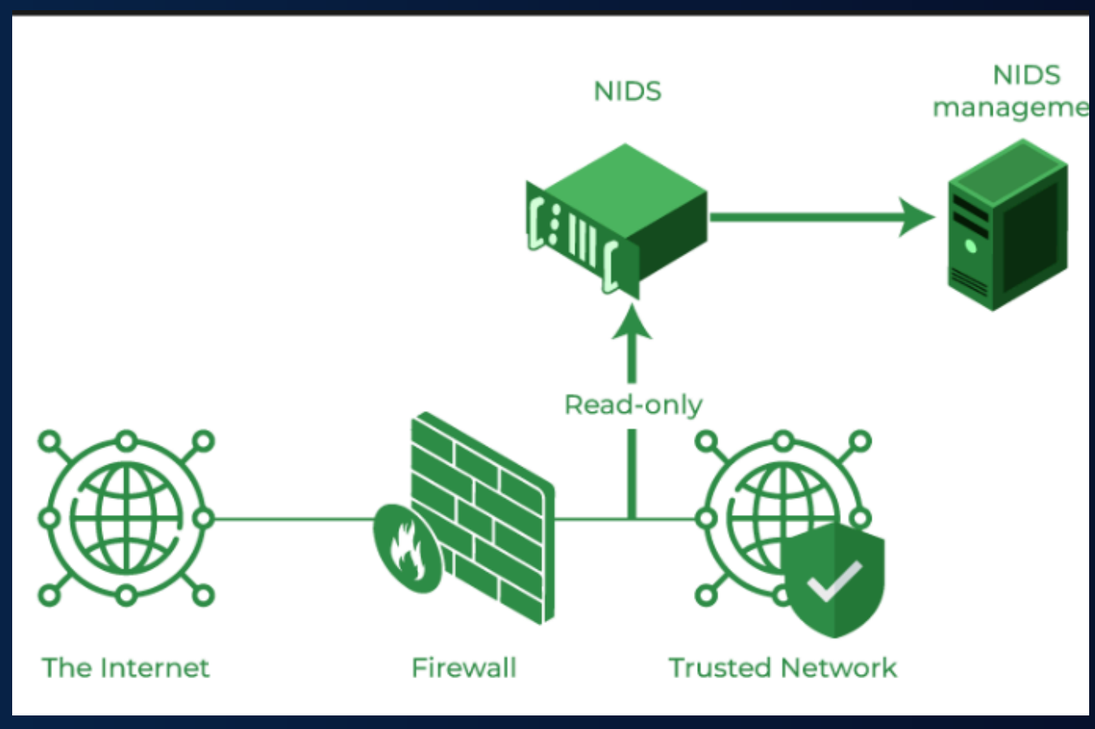
Key Differences and Similarities:

- IDS: Passive monitoring, focuses on detection.
- IPS: Active prevention, can block threats.

Common Types
IDS:

Network-based (NIDS): Monitors traffic on the network.
Example: A server icon.
Host-based (HIDS): Monitors activities on individual devices.
Example: A laptop icon.
IPS:

Network-based (NIPS): Acts at the network level to prevent intrusions.
Example: A server with a shield icon.
Wireless (WIPS): Specifically targets wireless networks.
Example: A Wi-Fi icon with a shield.
Host-based (HIPS): Protects individual hosts from attacks.
Example: A computer icon with a shield.



Deep Salunkhe
21102A0014