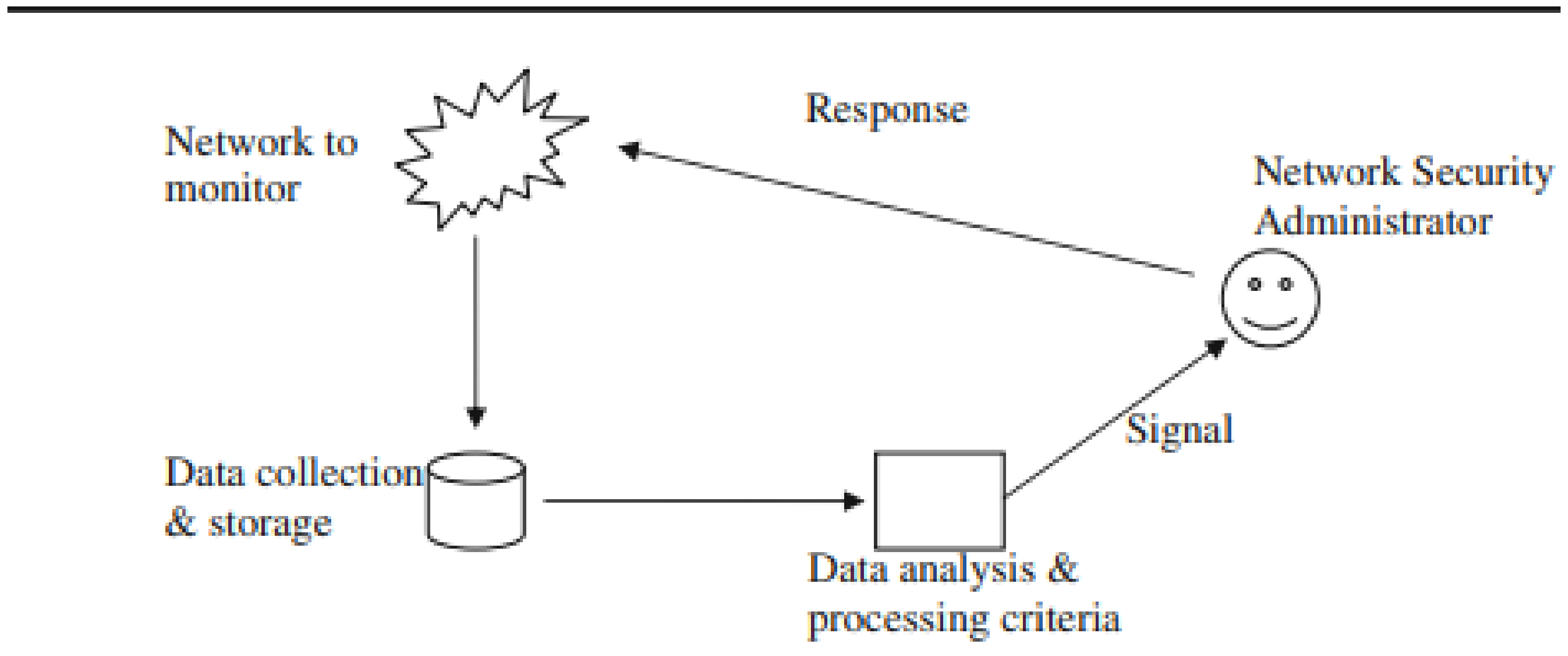
Intrusion Detection Systems (IDS)

Introduction to IDS

monitor network traffic for suspicious activity and generate alerts when such activity is discovered

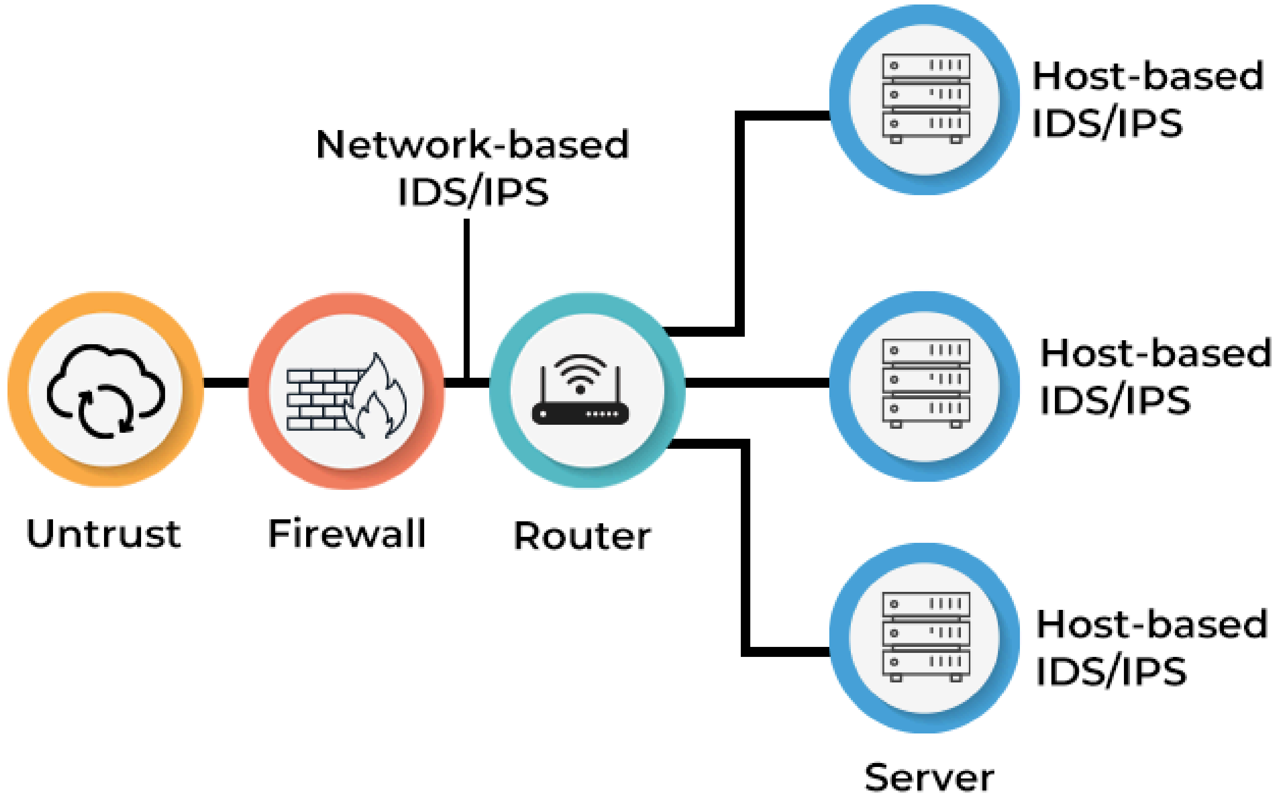

Network to monitor
Response
Network Security Administrator
Signal
Data collection & storage
Data analysis & processing criteria

Common components for IDS

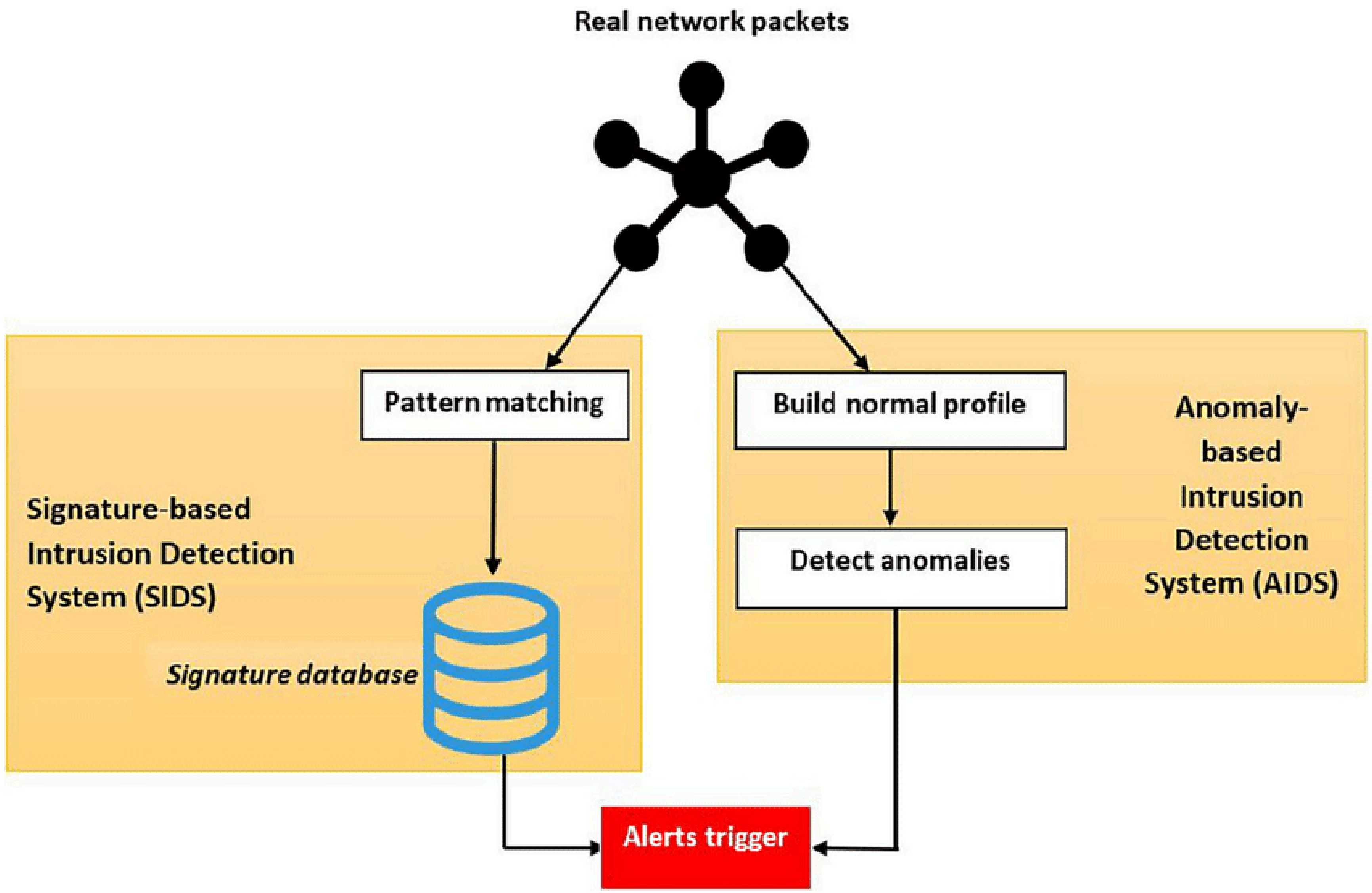
- *Network to monitor:* observes network traffic
- *Data collection & storage:* collects network traffic data and logs it for further analysis.
- *Data Analysis & Processing Criteria:* contains the whole functionality to find the suspicious behavior of attack traffic
- *Signal:* output of IDS which is sent to the Network Security Administrator

Types of IDS

Based on Deployment Method



Based on Detection Method



Emerging Technologies in IDS

- AI & ML Integration:

Enhance threat detection through pattern recognition and predictive analytics.

- Behavioral Analysis:

Identify deviations from normal behavior to detect zero-day exploits and APTs.

- SIEM Integration:

Consolidate security events for better threat correlation and response.

- Cloud-based Solutions:

Offer scalable and flexible IDS tailored for cloud environments.

- Deception Technology:

Deploy decoys and traps to mislead attackers and gather intelligence.

AI based IDS

Reference

[1] S. A. Aljawarneh, “SIDSs vs. AIDSs detection main phases,” ResearchGate, 2021. [Online]. Available: https://www.researchgate.net/publication/349921614.

[2] H. Badgujar, “What is IDS (Intrusion Detection System)? How it works?,” Medium, 2023. [Online]. Available: https://medium.com/@hrushikeshbadgujar/what-is-ids-intrusion-detection-system-how-it-works-732d81a13fb5.

[3] “DS/IPS on an Enterprise Network”, ZD Brightspot, 2022. [Online]. Available: https://zd-brightspot.s3.us-east-1.amazonaws.com/wp-content/uploads/2022/03/21120032/59-1.png.

[4] E. Kavas, "Strengthening Network Security: Evolution and Future of IDS & IPS," LinkedIn, Available: https://www.linkedin.com/pulse/strengthening-network-security-evolution-future-ids-ips-erkan-kavas-17tlf.

[5] N. Sharma, A. Gupta, A. Jain, and R. C. Jain, “Artificial Intelligence Based Intrusion Detection Techniques - A Review,” 2014. Available: ResearchGate.