IDS

- intrusion detection system
- passive monitoring solution for detecting cyber security threats/ breaches.
- IDS designed to aid in mitigating damage caused by hacking.
- IDS generates an alert
  - notifies security personnel to investigate the incident and take remediative action.

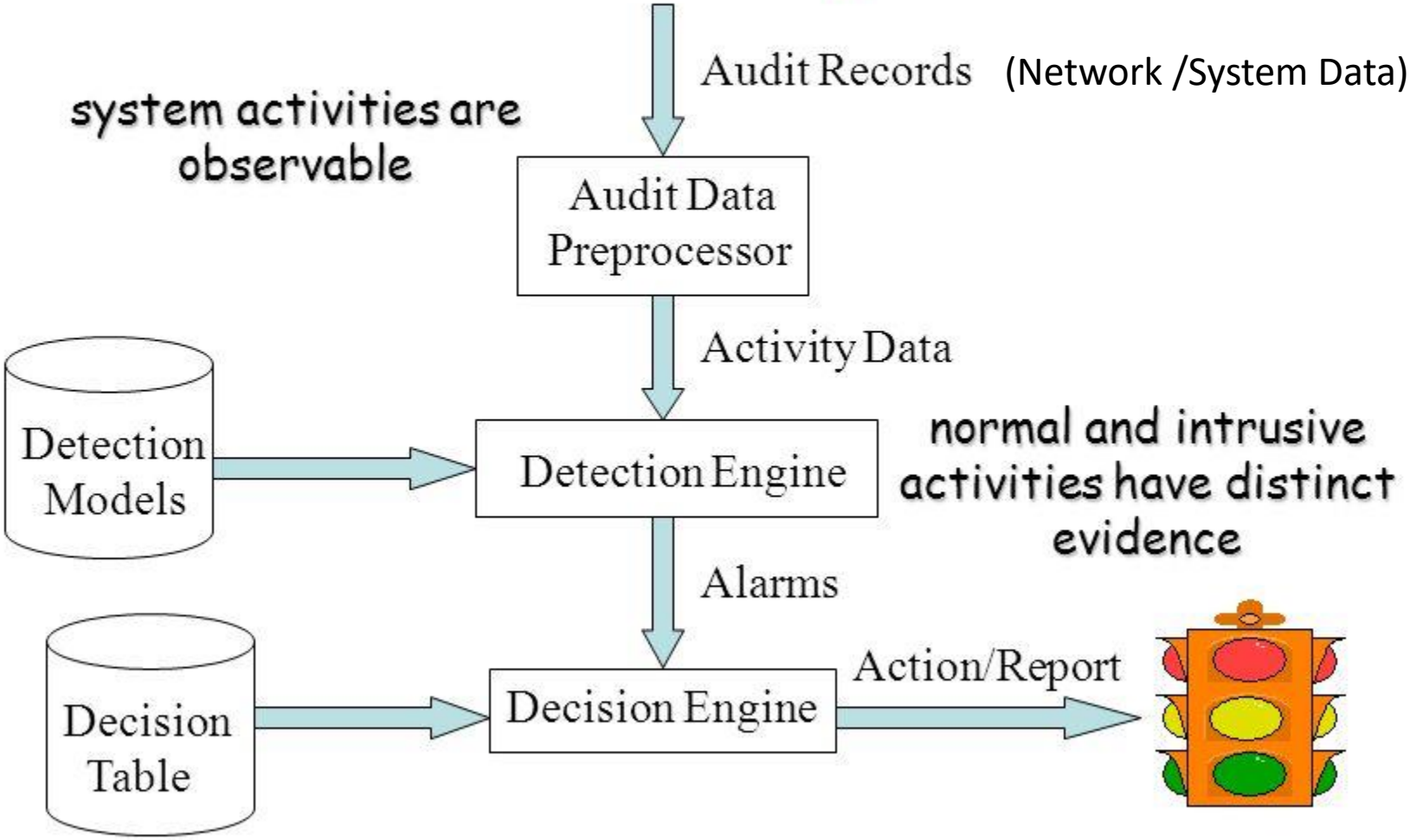
IDS

- Basic intent behind IDS: spot something suspicious on NW/system and sound alarm.
- May look for data bits that indicate questionable activity or monitor system logs.
- **Events that sound alarm** – may not be an intrusion; any abnormal activity may trigger, depending on configuration.

IDS

- All IDS have three things in common:
- **Sensors:**
  - collect traffic and user activity data and sends to analyzer.
- **Analyzer:**
  - Looks for suspicious activity.
- **Administrator Interface:**
  - If analyzer detects suspicious activity, sends an alert to the Admin Interface.

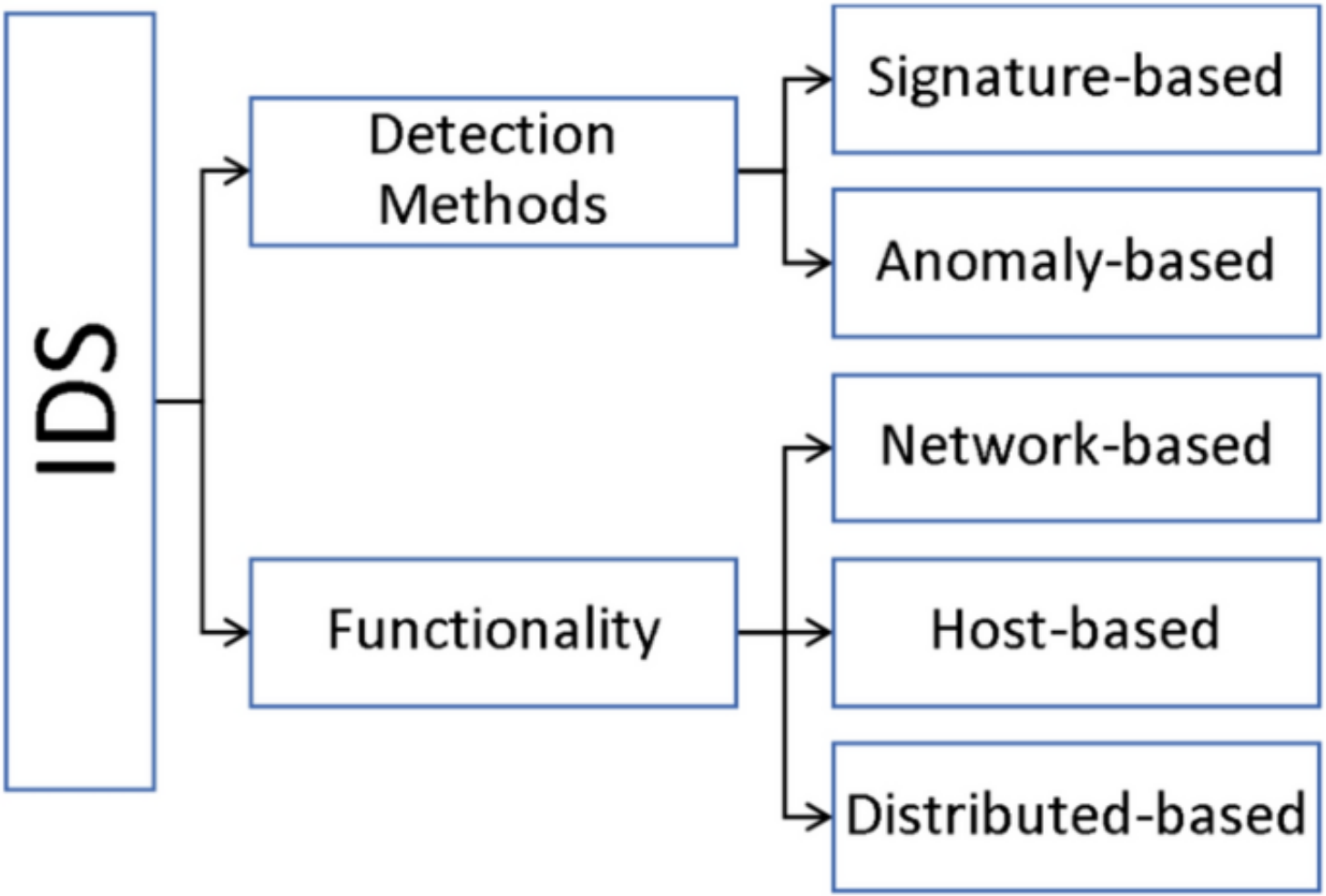
Components of Intrusion Detection System



HIDS

- can be configured for:
  - Watch for attacks
  - Parse audit logs
  - Terminate a connection
  - Alert an admin as attacks are happening
  - Protect system files
  - Expose a hacker's techniques
  - Throw up vulnerabilities that need to be addressed
  - Possibly help to track down hackers

IDS Classification



Classification of HIDS

- The major classifications are
  - Active Vs passive IDS,
  - Network Intrusion detection systems (NIDS) Vs
  - Host Intrusion detection systems (HIDS)
  - Knowledge-based (Signature-based) IDS Vs behavior-based (Anomaly-based) IDS

Active and passive IDS

- An active Intrusion Detection Systems (IDS) is also known as Intrusion Detection and Prevention System (IDPS).
- IDPS is configured to automatically block suspected attacks without any intervention required by an operator.
- IDPS has the advantage of providing real-time corrective action in response to an attack.
- **A passive IDS** is a system that's configured to only monitor and analyze network traffic activity and alert an operator to potential vulnerabilities and attacks.
- A passive IDS is not capable of performing any protective or corrective functions on its own.

Classification

- Based on Where to deployed/Functionality :
  - Host based Intrusion Detection Systems (HIDS)
  - Network Intrusion Detection Systems (NIDS),

Classification of HIDS

- Host based Intrusion Detection Systems (HIDS)
  - monitors the host's network traffic, running processes, logs, etc., or
  - Installed on individual workstations/ servers
  - Watches for abnormal activity NIDs understands and monitors NW traffic, HIDS monitors the computer only on which it is installed.
  - Generally, HIDS installed on critical servers only due to administrative overheads.

Classification

- Network Intrusion Detection Systems (NIDS),
  - identify threats to the entire network.
  - Uses sensors to monitor all NW traffic
  - Cannot see the activities within the computer itself.

Types of HIDS/NIDS

- **Based on how they identify potential threats/ Detection Methods**
- Signature based
  - uses a library of signatures of known threats to identify them.
    - Pattern matching
    - Stateful matching
- Anomaly based
  - builds a model of “normal” behavior of the protected system and reports on any deviations.
    - Statistical anomaly based
    - Protocol anomaly based
    - Traffic anomaly based
- Rule based

IDS

- Classified based upon
  - A signature-based IDS
  - An anomaly-based IDS
- A hybrid system uses both methods to identify potential threats.

Knowledge or Signature based IDS

- Knowledge is gained by sensors about how specific attacks are carried out.
- Each identified attack has a signature
- Eg of a signature:
  - A pkt having the same source and destination address (LandAttack)
  - A TCP header of a pkt in which all values are set to 1s (xmasattack).
  - Once these type of attack discovered, vendors wrote signatures that looks specially for pkts with same source and destination addresses or with TCP headers flag set to all 1s.

Knowledge or Signature based IDS

- Most popular IDS today.
- Effectiveness depends on regularly updating signature database.
- May not be able to uncover new types of attacks.

State based IDS

- **State transition:** Every change that an OS experiences (user log on, opening of applications, user data input, etc), is a state transition.
- Generally happens continuously in any system.
- So again, what is a state ?
  - A snapshot of an OS's values in volatile and non-volatile memory locations.
- In a state based IDS:
  - Initial state is the state prior to attack execution.
  - Compromised state is the state after successful penetration.
- The IDS has rules as to which state transitions should trigger alarm.

State based IDS

- An example of State based IDS
  - A remote user connects to a system
  - Sends data to an applications(data exceeds alloted buffer for this empty variable).
  - The data is executed and overwrites the buffer and possibly other memory segments.
  - A malicious code executes.
- State based IDS looks for activity between initial and compromised state and sends alert if any state transition sequence matches its preconfigured rules.
- Requires frequent signature updates.

Statistical Anomaly based IDS

- A behavior based system (also called heuristic IDS).
- Does not use a signature database.
- Initially put in a learning mode wherein the IDS learns the `normal'NW activities.
- The longer it is in learning mode, more accurate profile of anormal state is built up.
- After a profile is built, all future activities are compared to this`normal' profile.
- If an activity exceeds a predefined `normal' threshold, the alert is triggered.

Statistical Anomaly based IDS

- **Benefits**
  - Can react to 0 day attacks
  - Also capable of detecting the low and slow attacks
- **Problems**
  - May provide overwhelming number of false positives.
  - If an attacker discovers an IDS on a NW, will try to detect type so that he can circumvent it.
  - With a behavior based IDS, attacker will try to integrate activities in the `normal' NW usage.
  - If an attack was underway when the IDS was in learning mode,an attack will never be detected.
  - Sends generic alerts compared to specific alerts thrown up by signature based IDS.

Statistical Anomaly based IDS

- **Strength of this IDS** lies in determining actual thresholds of normal activity.
- **Once an attack is identified**, the IDS can:
  - Send an alert to the admin's console.
  - Send an email to a preconfigured address.
  - Kill the connection of the detected attack
  - Reconfigure a router/firewall to stop any further similar attacks.