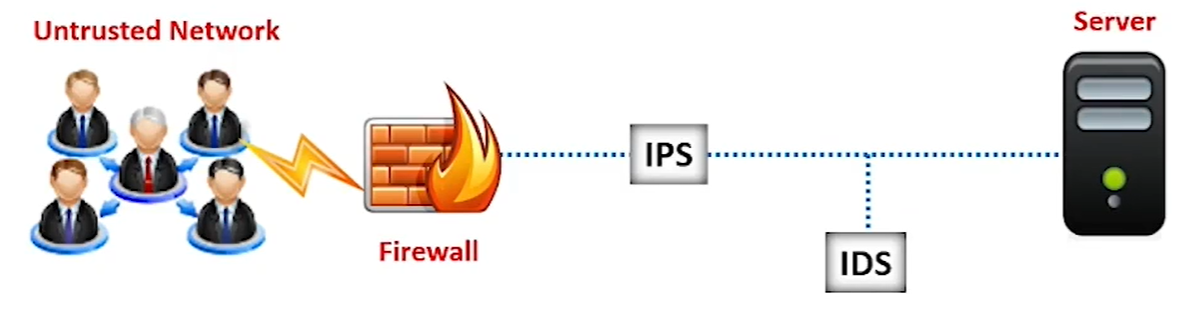
# Intrusion detection &Prevention System(IDS/IPS)

* Inspects all inbound, outbound network traffic for suspicious patterns that might indicate a n/w or system security breach
* If found, the IDS will alert the admin about the suspicious activities
* IDS Checks the network traffic for signatures the match known intrusion patterns and triggers an alarm when match is found





## IDS Role in N/w defense:

* It will be behind the firewall
* It works from inside the network unlike firewall which oly looks outside intrusions
* Inspects all traffic, looking for heuristics & pattern that match for intrusions

# Intrusion Detection by IDS

1. Signature Recognition/ misuse detection

* Tries to identify events that indicate an abuse of system or network resource

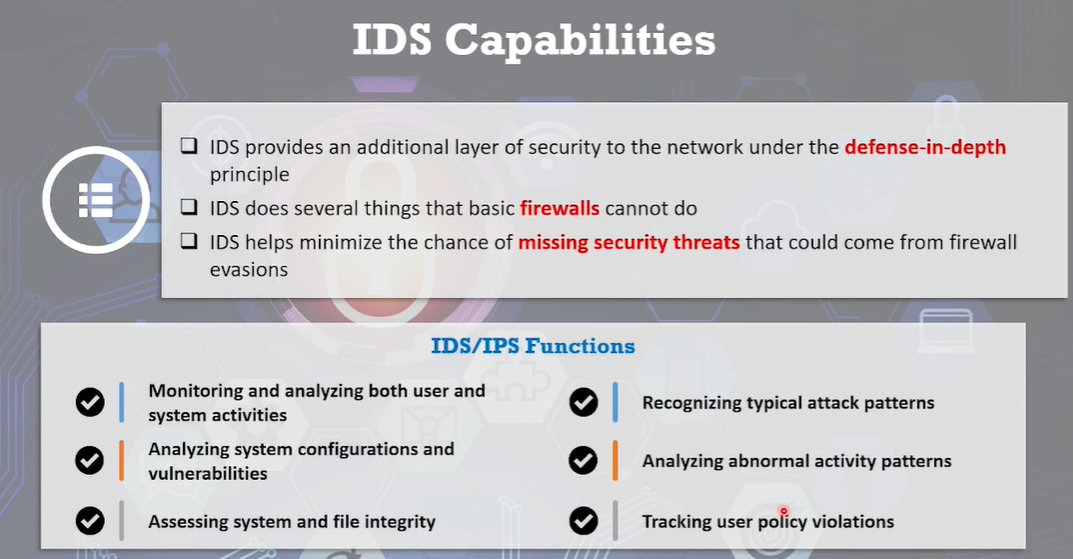
1. Anomaly Detection (General &

* Detects intrusion based on fixed behavioral characteristics of users and components in a computer system

1. Protocol Anomaly Detection

* Models are built to explore anomalies in the way in which vendors deploy TCP/IP specification

# IDS capabilities



# IDS/IPS Limitations:

Can’t replace

* N/w logging systems
* Vulnerability assessment tools
* Antivirus products
* Cryptographic systems

# IDS/IPS security concerns

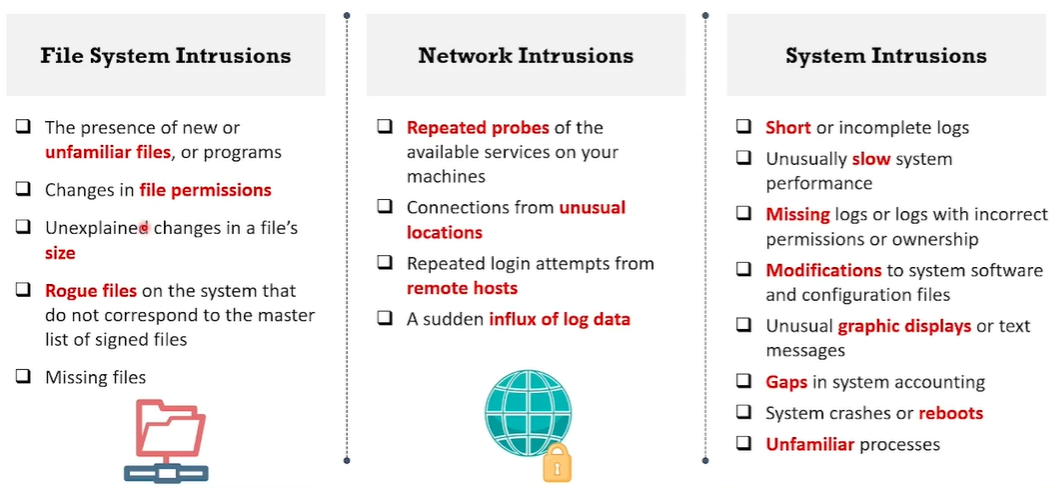
Deployment should be done carefully

Planning preparation prototyping testing specialized training

# Mistakes in configuring:



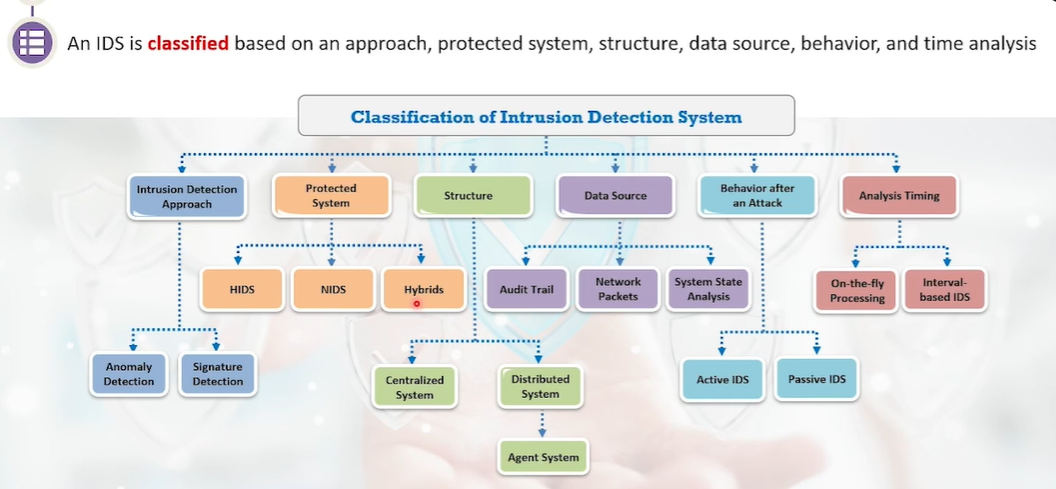
# 3 types of Intrusion indicators



HIDS – Host-based intrusion Detection System

NIDS- Network based

# IDS Classification:



## Approach Based IDS – uses string comparison

* Monitors data packets in the network and compares them to pre-configured n/w attack patterns (Signatures)

|  |  |
| --- | --- |
| Pros | Cons |
| Detects attacks with min. fake alarms | Only detects known threats  The database must be updated with new signatures |
| Quickly identify the use of specific tool or technique | It utilizes tightly defined signatures that prevent it from detecting common variants of the attacks |
| It assists admins to quickly track any potential security issues and initiate accident handling procedures |  |

### Anomaly Based Detection

* Alarms for anomalous activities are generated by evaluating n/w patterns
* Like what sort of bandwidth used, protocols used, ports and devices connected to each other
* IDS monitors typical activity for particular time interval and **builds statistics** for network traffic
* Ex: Normal internet band usage, failed login attempts, processor utilization levels etc

|  |  |
| --- | --- |
| Pros | Cons |
| Identifies abnormal behavior in the network and Detects the symptoms of attacks without any clear details | The chances of generating false alarms is high due to unpredictable behavior of users and networks |
| Information acquired by anomaly detectors is further used to define signatures for misuse detectors | The need to create extensive set of system events in order to characterize normal behavior patterns |

## EXAMPLES TO UNDERSTAND

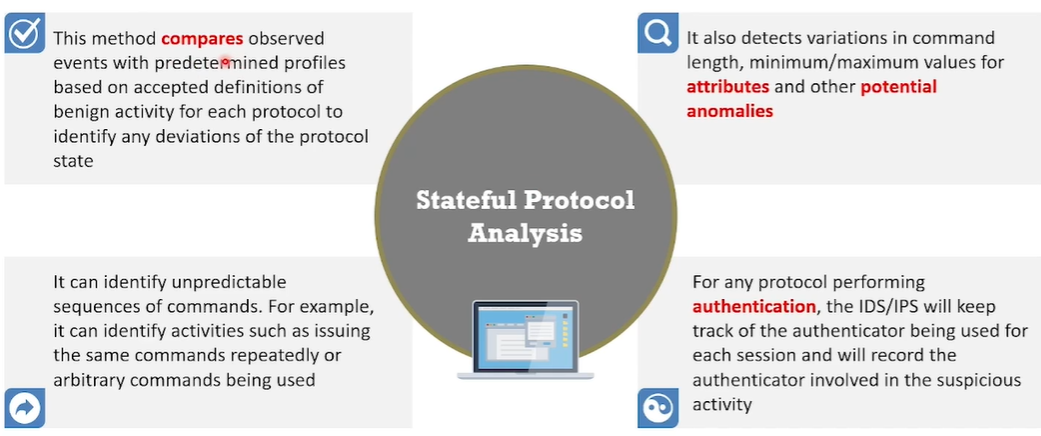
**Signature-Based Detection (Approach-Based)**

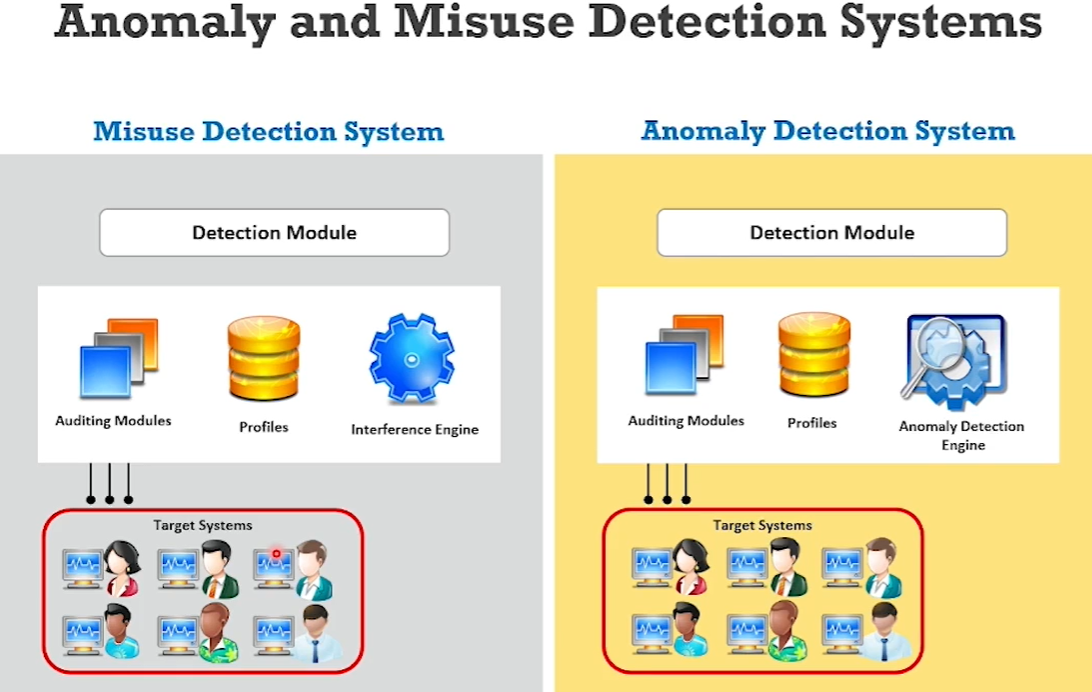
* **Imagine a bouncer at a club:** The bouncer has a list of known troublemakers (known threats) with descriptions (signatures). Anyone matching a description gets denied entry (blocked).
* **How it works:**
  + Relies on pre-defined patterns or signatures of malicious activity (malware code, exploit attempts).
  + These signatures come from known threats and constantly updated databases.
  + Network traffic is scanned for these signatures.
* **Best Example:** Imagine a company receives an email with a specific attachment known to be malicious (based on its file hash or code). A signature-based IDS would identify this email and block it because the attachment matches a known malicious signature.

**Anomaly-Based Detection**

* **Imagine a parent monitoring their child's behaviour:** The parent knows the child's usual activities (normal network traffic patterns). Any significant deviation from the norm raises suspicion.
* **How it works:**
  + Learns the normal behaviour of the network (traffic patterns, user activity).
  + Monitors for deviations from this baseline and flags them as anomalies.
  + Often uses machine learning algorithms to identify patterns in network traffic.
* **Best Example:** Imagine a user account that typically logs in during business hours from a specific location suddenly starts logging in from a different country at night. Anomaly-based detection would flag this as suspicious because it deviates from the user's normal behavior.

## Stateful Protocol analysis:





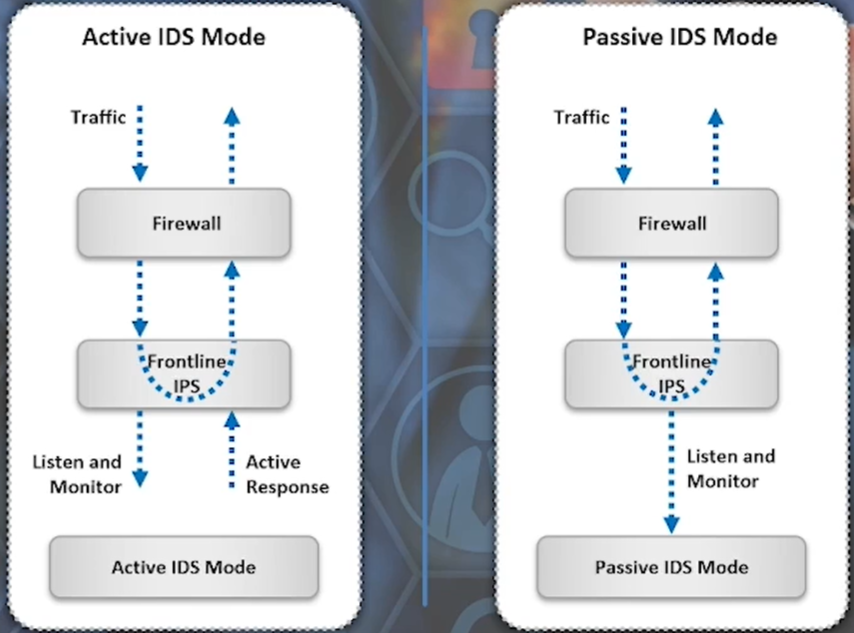
## Behavior-based IDS:

* Based on how it reacts to potential intrusion
* Based on behavior after an attack it functions on 2 modes

1. Active IDS : Detects & responds to detect intrusions

Like blocks IP address or Port

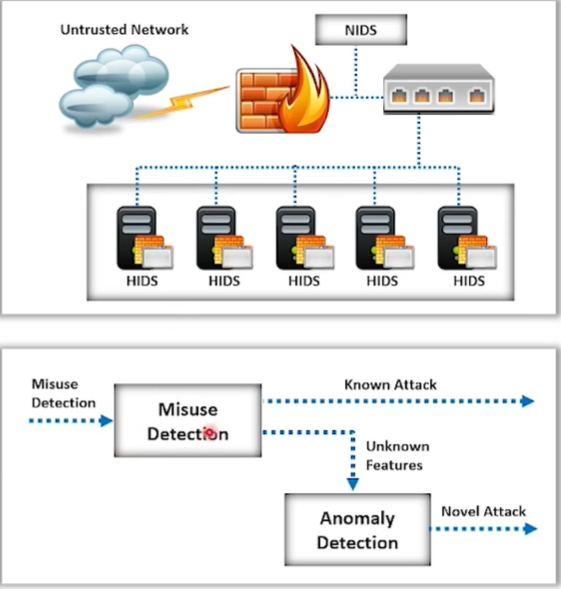
1. Passive IDS : Only detects intrusions



## Protection based IDS:

* Based on system/ network it offers protection to

1. Hybrid IDS has advantages of both low false-positive rate of NIDS and the anomaly based detection of a HUDS to detect unknown attacks



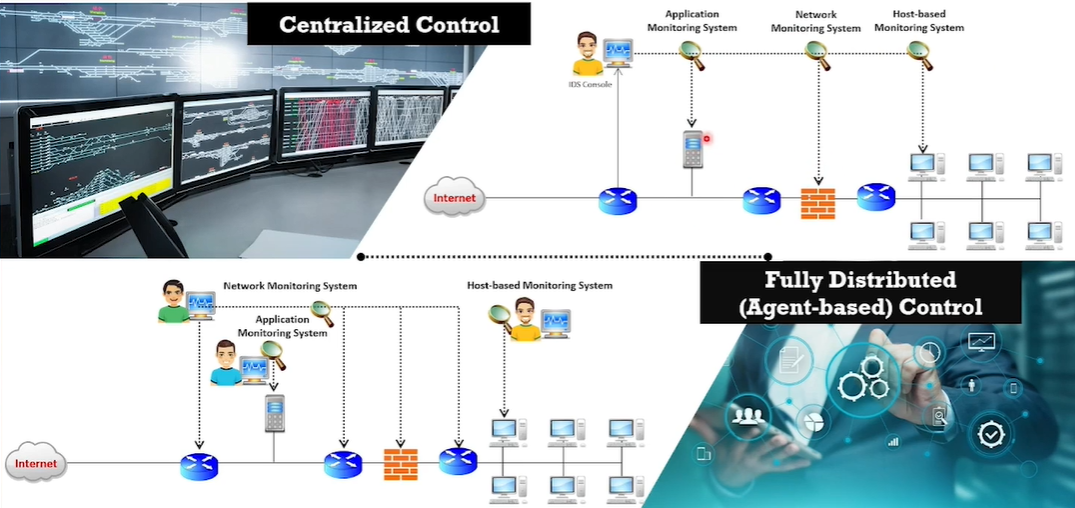
## Structure based IDS:

1. **Centralized IDS**: All data shipped to central location for analysis

Independent of the no.of hosts that are monitored

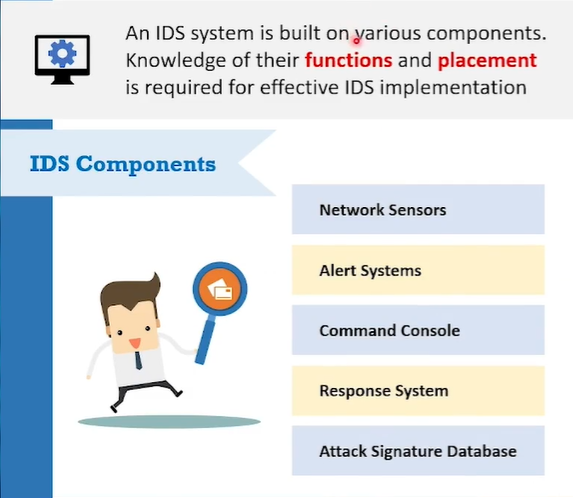
1. **Distributed IDS**; Several IDS are deployed over a large n/w and

each IDS communicates with each other for traffic analysis



## Source data analysis based IDS:

# IDS Components



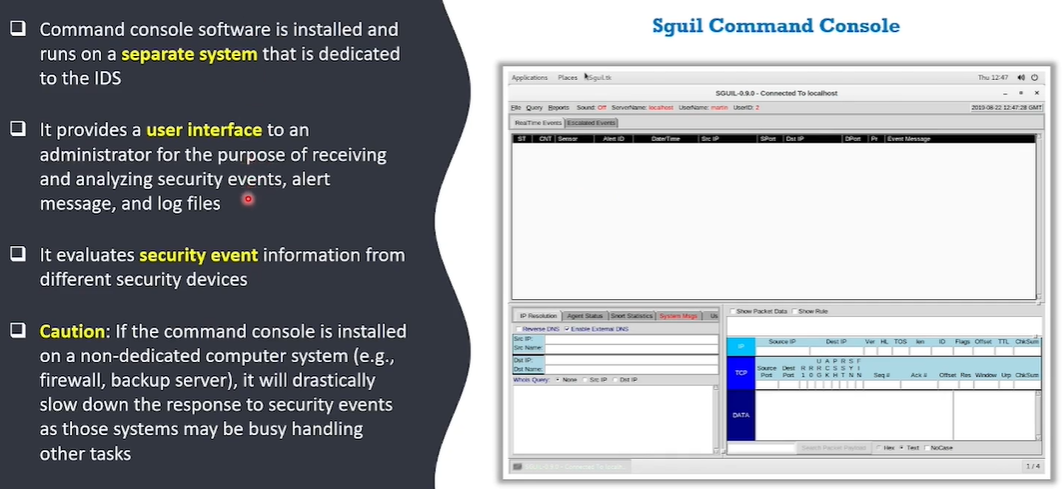
## Network sensors- are hardware & software components that monitor n/w traffic & trigger alarms if any abnormal activity is detected

Sensors should be placed & located at common entry points in a network  
 Internet gateways VPN devices

In b/w LAN connections Either side of firewall (In some cases infront too)

Remote access servers used to receive dial-up connections

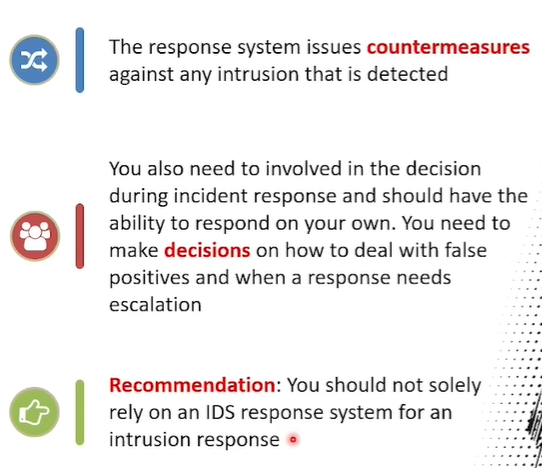
## Command Console



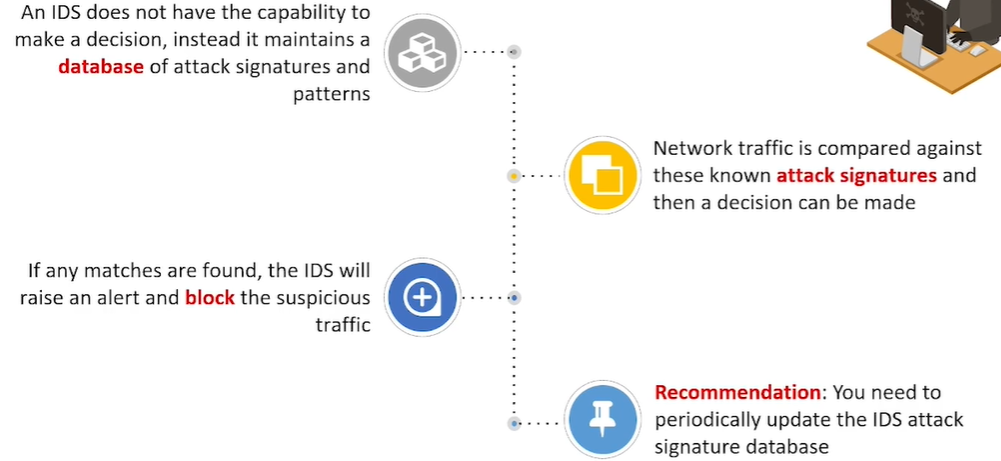
## Alert Systems



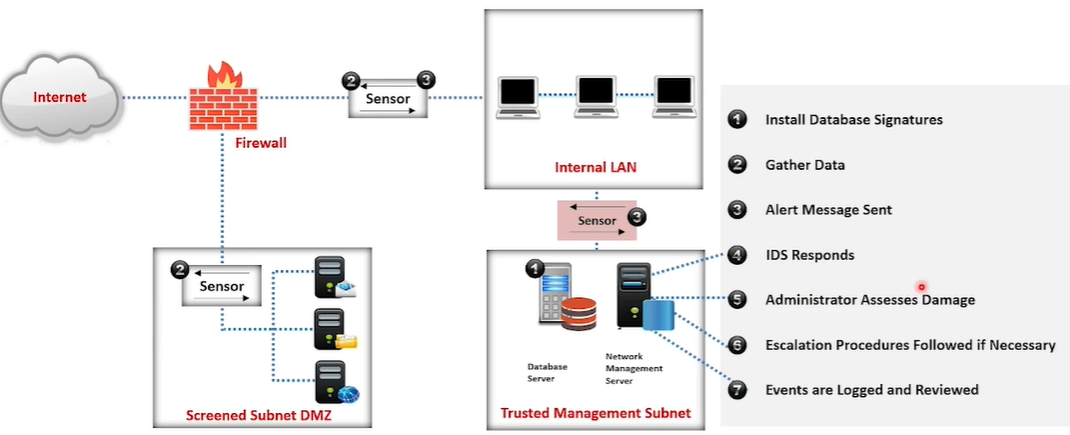
## Response system



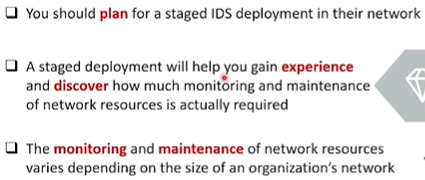
## Attack signature Database



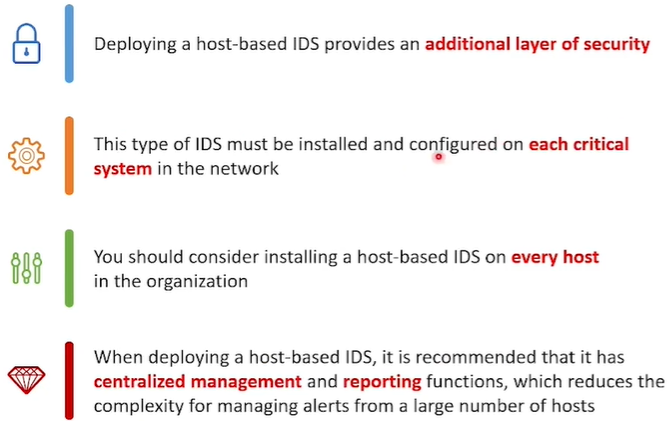
# Collaboration of IDS Components in intrusion Detection



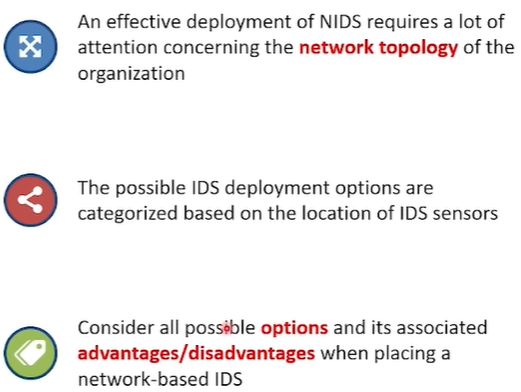
# Deployment of Network & HIDS

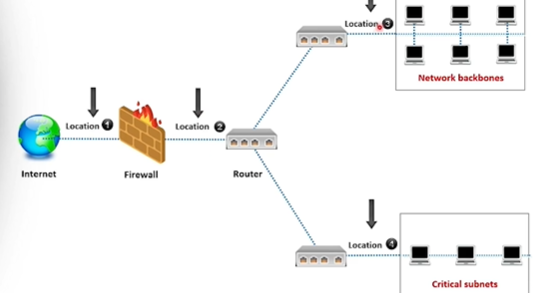


## Deploying HIDS

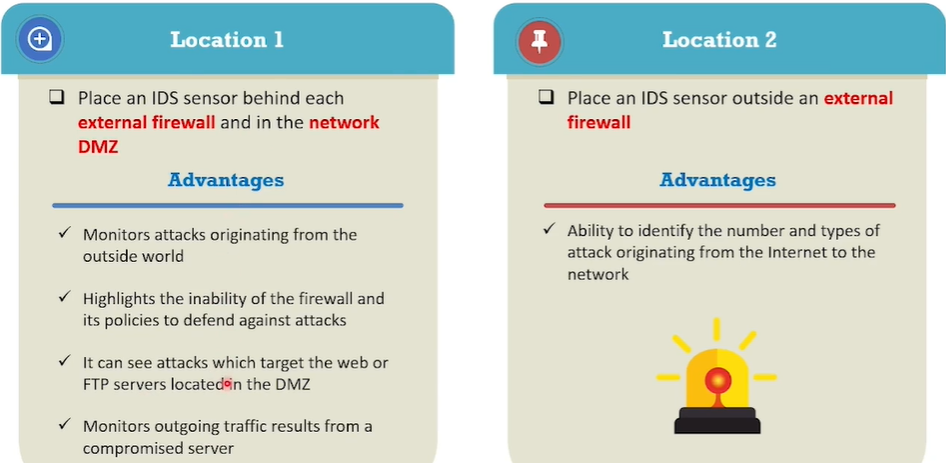


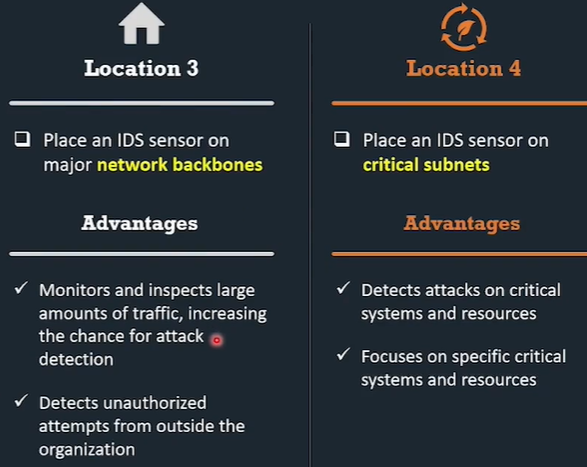
# Deploying NIDS





## Locations

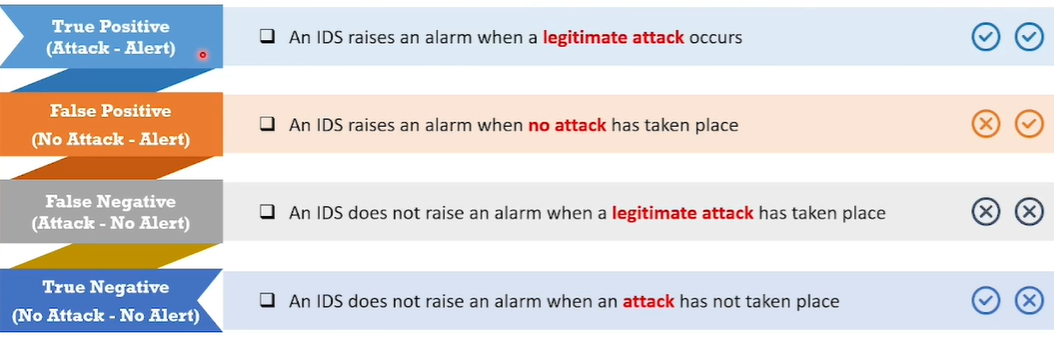




# IDS Alert:

* Alert is a graduated event, which notifies that a particular event has reached a specified threshold & needs proper action by a responsible party
* It send the notification, saying something is wrong & requires immediate attention & monitoring

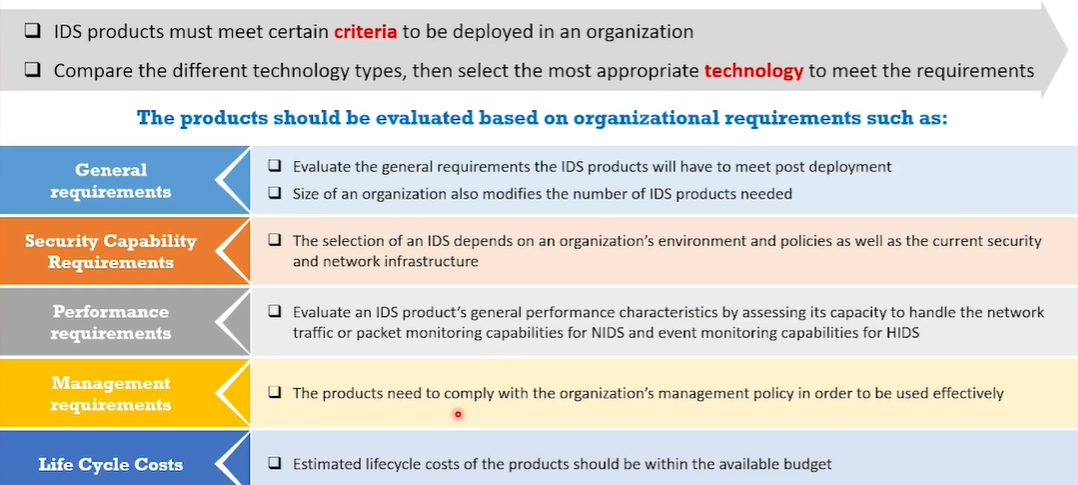
## Types:



## Characteristics of Good IDS solutions

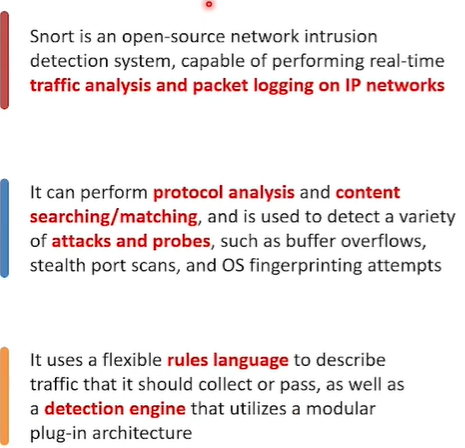
 Automation

# Selection of appropriate IDS/IPS Solutions

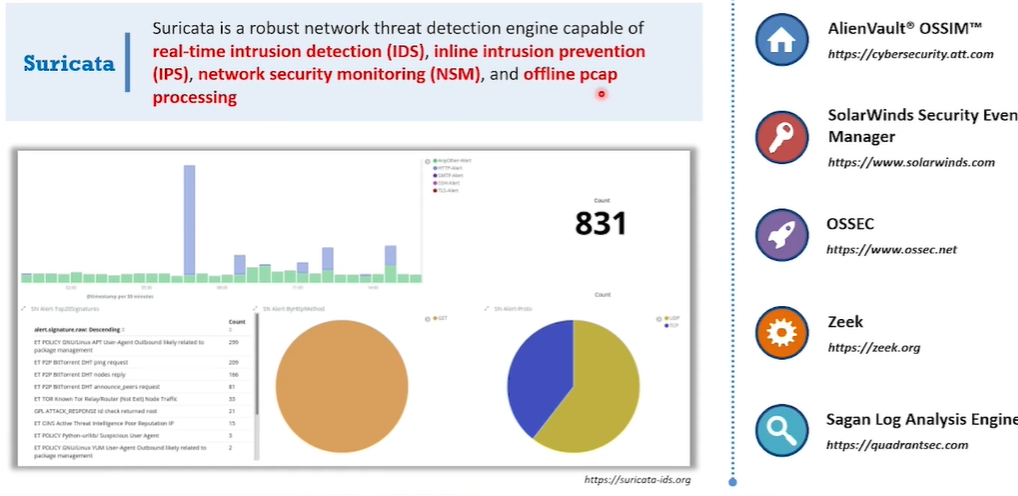


# Intrustion detection tools

## with snort: snort is an opensource



## With suricata & others:



|  |  |  |
| --- | --- | --- |
| Detection Method | Pros | Cons |
| Signature-Based | * Highly accurate for known threats | * Fast and efficient detection * Can't detect new or zero-day attacks (attacks with no known signature) * Reliant on keeping signature databases up-to-date |
| Anomaly-Based | * Can detect new and unknown threats | * More adaptable to changing network environments * Can generate false positives (flagging normal activity as suspicious) * Requires initial training period to establish a baseline * May be computationally expensive |