INTRODUCTION TO INTRUSION DETECTION SYSTEM

MODULE 1

CONTENTS

INTRUDERS

- A significant security problem for networked system is unwanted trespass by users or software.

1)User trespass: Unauthorized login to a machine, acquisition of privileges or performance of actions beyond those that have been authorized.

2) Software trespass: Form of a virus, worm or Trojan Horse.

Classes of Intruders

- There are three classes of Intruders:
  - **Masquerader-** An individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account.
  - **Misfeasor-** A legitimate user who accesses data, programs or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges.
  - **Clandestine User-** An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection.

Examples of Intrusion

- Remote root compromise
- Web server defacement
- Guessing / cracking passwords
- Copying viewing sensitive data/databases
- Running a packet sniffer
- Distributing pirated software
- Using an unsecured modem to access net
- Impersonating a user to reset password
- Using an unattended workstation

IDS Principles

- Assume intruder behavior differs from legitimate users
- Expect overlap as shown
- Observe deviations from past history
- Problems of:
- False Positives
- False Negatives
- Must Compromise

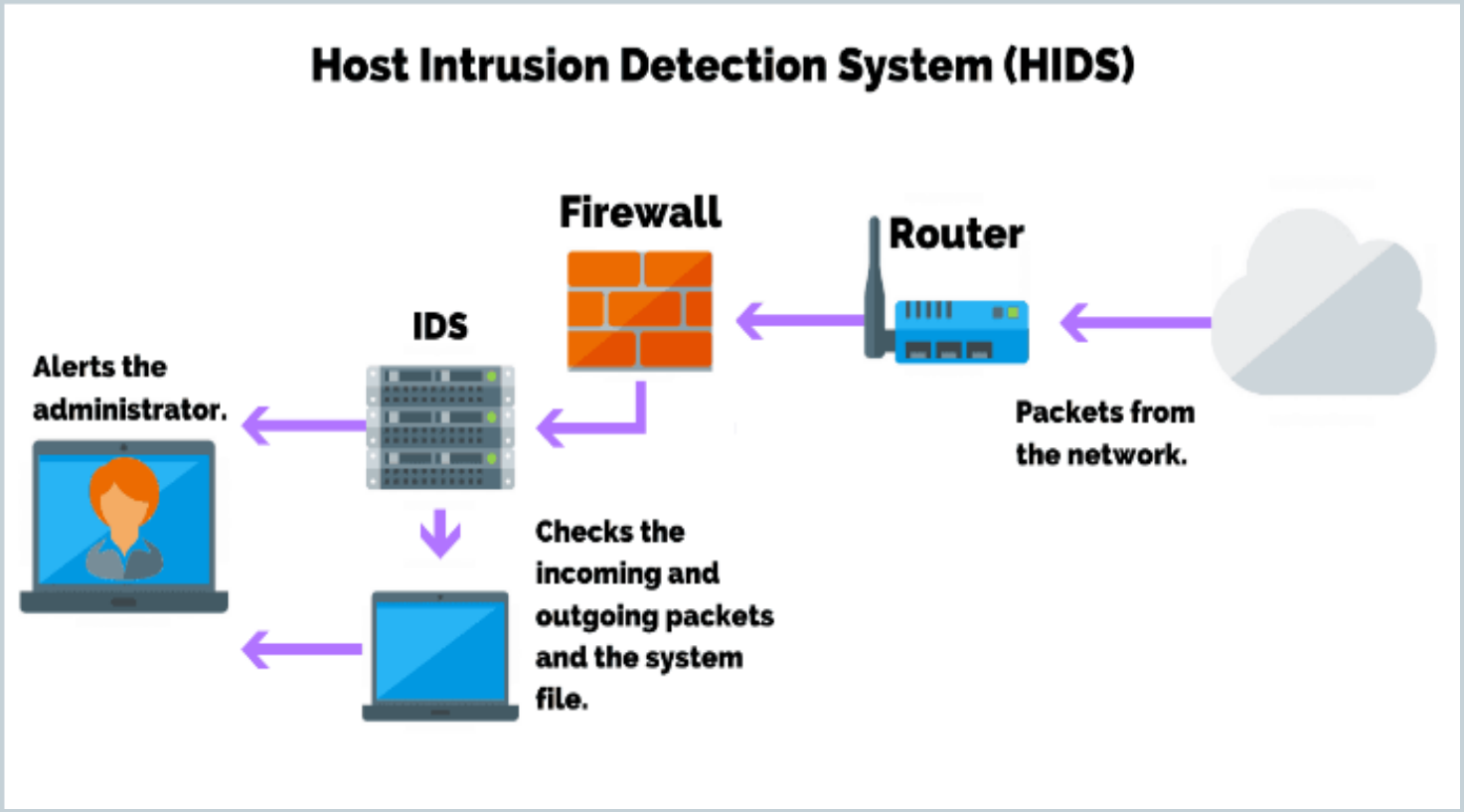
IDS Requirements

- Run continually
- Be fault tolerant
- Resist subversion
- Impose a minimal overhead on system
- Configured according to system security policies
- Adapt to changes in system and users
- Scale to monitor large number of systems
- Provide graceful degradation of service
- Allow dynamic configuration

Host-Based IDS

- Specialized software to monitor system activity to detect suspicious behavior
- Primary purpose is to detect intrusions, log suspicious events and send alerts.
- Can detect both internal and external intrusions
- Two approaches, often used in combination:
- Anomaly detection – Defines normal/expected behavior
- Threshold Detection
- Profile Based
- Signature detection – Defines proper behavior

How HIDS work??



Anomaly Detection

- Threshold Detection
  - Checks excessive event occurrences over time
  - Alone a crude and ineffective intruder detector
  - Must determine both thresholds and time travels
- Profile based
  - Characterize past behavior of users/groups
  - Then detect significant deviations
  - Based on analysis of audit records

Signature Detection

- Observe events on system and applying a set of rules to decide if intruder
- Approaches:
  - Rule-based anomaly detection
- Analyze historical audit records for expected behavior, then match with current behavior
  - Rule-based penetration identification
- Rules identify known penetrations/weaknesses
- Often by analyzing attack scripts from Internet
- Supplemented with rules from security experts

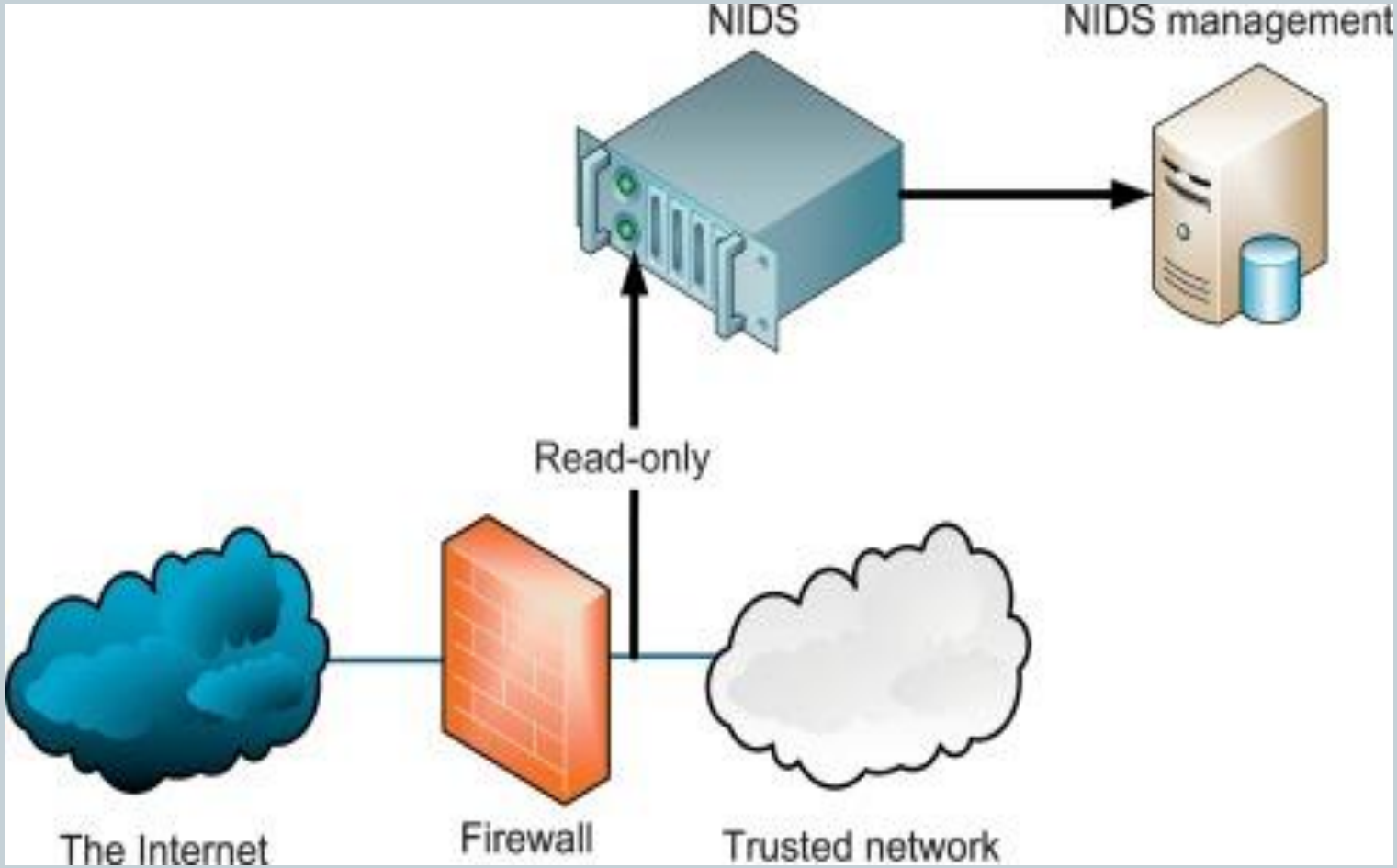
- There are many threats that can be eliminated with the help of a host-based IDS:

- **Malicious Attacks-** Such as unauthorized authentication attacks, HIDS detects the attack and sends it for analysis.
- **Asymmetric Routing-** When data packets traveling through the network take a particular route to their destination and take a different route back, it is called asymmetric routing. This mechanism allows the attackers to perform a DDOS attack. HIDS helps determine such routes

- **Buffer Overflow Attacks-** This kind of attack attempts to infiltrate segments of memory in the device on which the host-based IDS is installed.
- **Scanning Attacks-** Scanning attacks involve sending data to the network to collect data about the network, traffic, ports, and hosts. HIDS will help minimize these attacks using advanced features such as a web application firewall to protect the data within the system.

Network-Based IDS

- Network-based IDS (NIDS)
  - Monitor traffic at selected points on a network
  - In real time to detect intrusion patterns
  - May examine network, transport and/or application level protocol activity directed towards systems
- Comprises a number of sensors
  - Inline (possibly as part of other net device)
  - Passive (monitors copy of traffic)


NIDS
NIDS management
Read-only
The Internet
Firewall
Trusted network

NIDS Sensor Deployment

- Inline sensor
- Inserted into a network segment so that the traffic it is monitoring must pass through the sensor
- Passive sensor
- Monitors a copy of network traffic

NIDS- Intrusion Detection Techniques

- Signature Detection
  - At application, transport, network layers; unexpected application services, policy violations
- Anomaly Detection
  - Of Denial of Service Attacks
- When potential violation detected sensor sends an alert and log information
  - Used by analysis module to refine intrusion detection parameters and algorithms
  - By security admin to improve protection

Anomaly based Methodology Architecture

- Anomaly based methodology works by comparing observed activity against a baseline profile.
- The baseline profile is the learned normal behaviour of the monitored system and is developed during the learning period were the IDPS learns the environment and develops a normal profile of the monitored system.

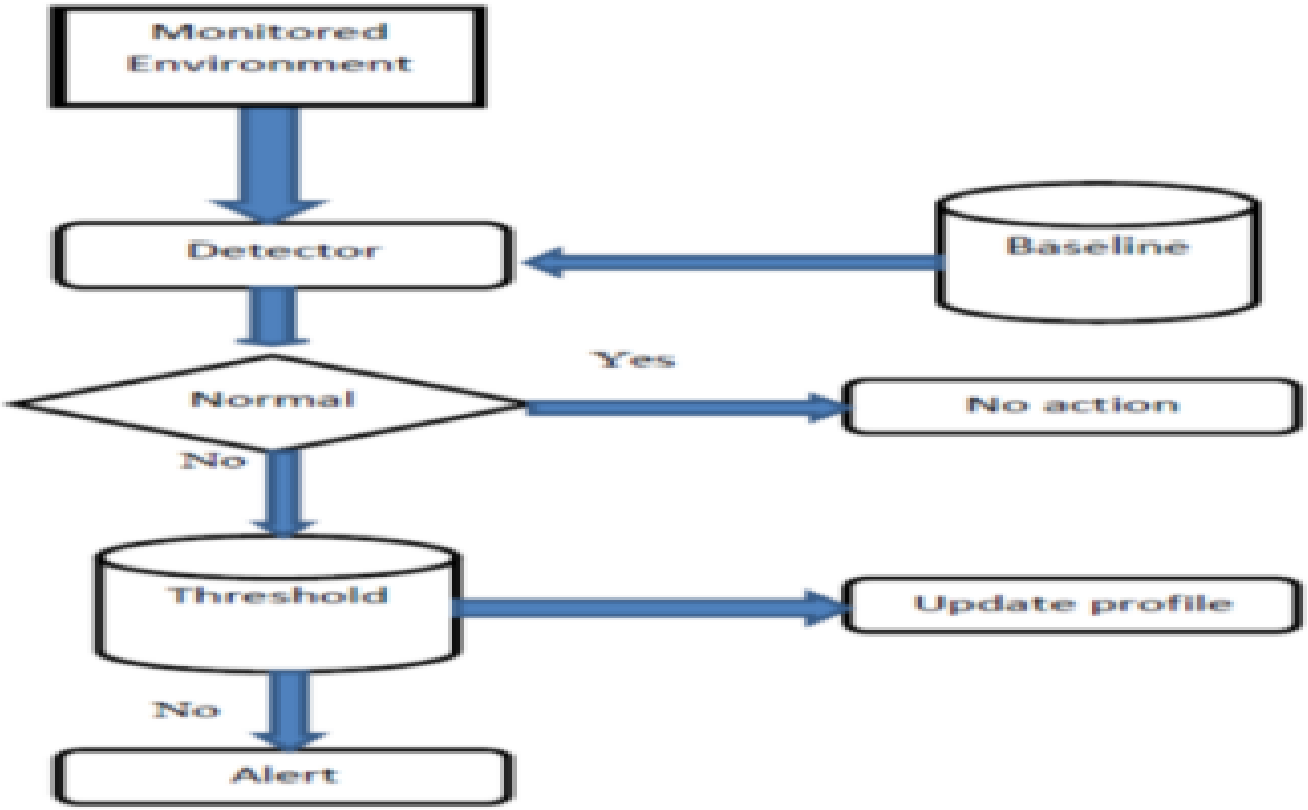
- Uses three general techniques for detecting anomalies:-

1) Statistical Anomaly Detection- The threshold or profile must be tuned according to the requirements and behaviour of the environment being monitored for the systems to be effective.
2) Knowledge/data-mining- Monitor searches for anomalies and this process places a very high overheard on the system
3) Machine learning based- Works by analyzing the system calls

CONTT..

- The monitored environment is monitored by the detector that examines the observed events against the baseline profile.
- If the observed events match the baseline, no action is taken, but if it does not match the baseline profile and it is within the acceptable threshold range then the profile is updated.
- If the observed events do not match the baseline profile and falls outside the threshold range they are marked as an anomaly and alert is issued.

Anomaly based Methodology Architecture

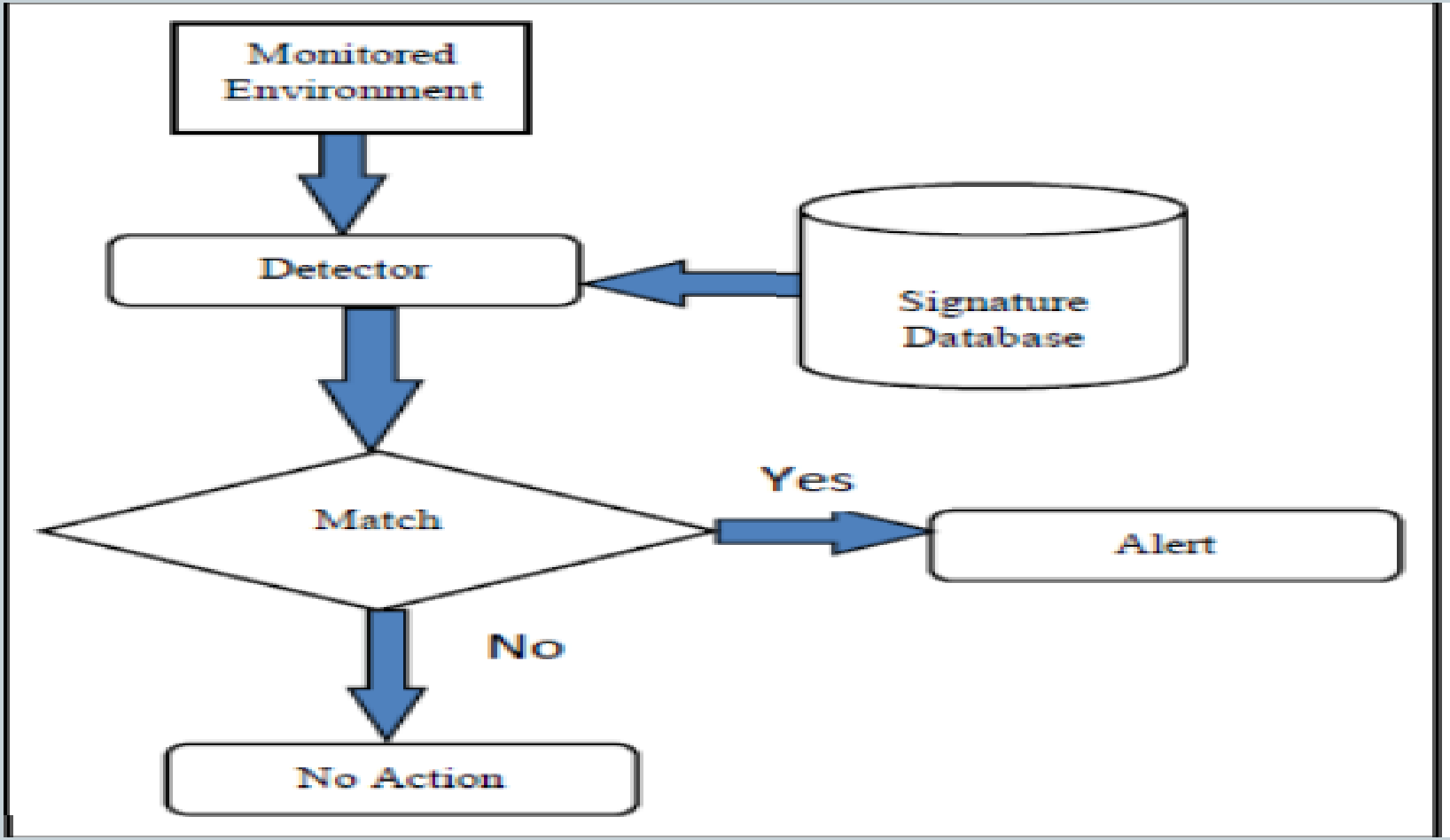


Signature based Methodology Architecture

- Signature based methodology works by comparing observed signatures to the signatures on file. This file can be database or a list of known attack signatures.
- The signature based IDPS has little overhead since it does not inspect every activity or network traffic on the monitored environment. Instead it only searches for known signatures in the database or file.
- Easy to deploy as no need to learn the environment.

- **Signature based methodology is very effective against know attacks/violations but it cannot detect new attacks until it is updated with new signatures**
- **Signature based IDPS are easy to evade since they are based on known attacks and are depended on new signatures to be applied before they can detect new attacks**
- **Signature based detection systems can be easily bypassed by attackers who modify known attacks and target systems that have not been updated with new signatures that detect the modification.**
- **Requires significant resources to keep up with the potential infinite number of modifications to known threats.**
- **Simpler to modify and improve since its performance is mainly based on the signatures or rules deployed.**

Signature based Methodology Architecture



CONTT…

- This architecture uses the detector to find and compare activity signatures found in the monitored environment to the known signatures in the signature database. If a match is found, an alert is issued and there is no match the detector does nothing.

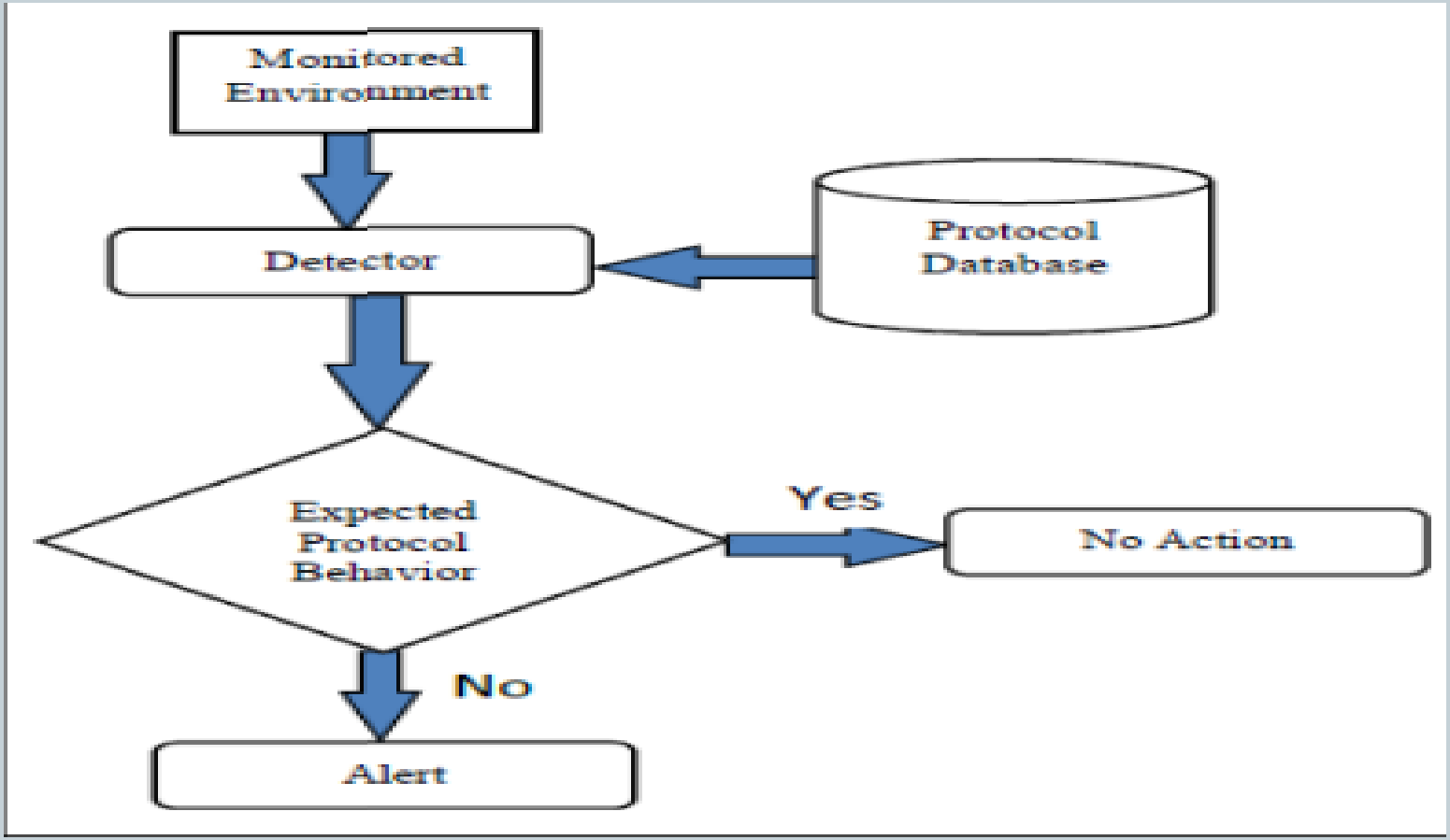
Stateful Protocol Analysis based Methodology Architecture

- The Stateful protocol analysis methodology works by comparing established profiles of how protocols should behave against the observed behaviour.
- Stateful protocol analysis has a deep understanding of how the protocols and applications should interact/work. This deep understanding/analysis places a very high overhead on the systems.

CONTT..

- This architecture is identical to that of the signature based methodology with one exception, instead of the signature database the Stateful protocol analysis has database of acceptable protocol behaviour.

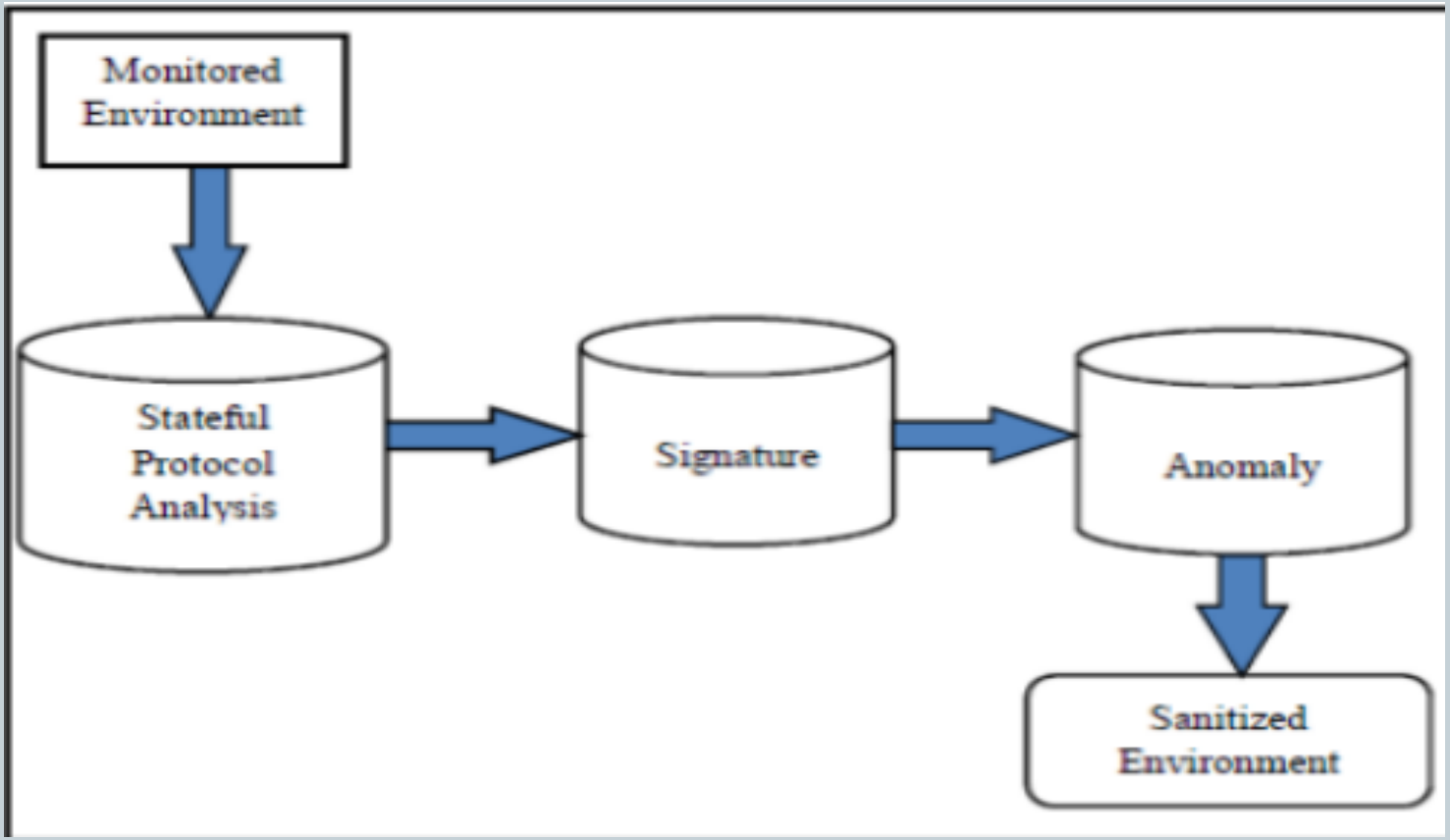
Stateful Protocol Analysis based Methodology Architecture



Hybrid based Methodology Architecture

- The hybrid based methodology works by combining two or more of the other methodologies.
- Prelude is one of the first hybrid IDS that offered a **framework** based on the Intrusion Detection Message Exchange Format (IDMEF) that allows different **sensors to communicate**.
- A general over view of a hybrid based methodology is shown in Figure. **Three other methodologies** are combined. The monitored environment is **analyzed by first methodology** and passed to the next and then the last one. This produces a better system.

Hybrid based Methodology Architecture



Parameters	Anomaly	Signature	Stateful Protocol Analysis	Hybrid
Resistance to Evasion	Medium	Low	Low	High
High accuracy rate	Medium	Medium	Medium	High
Scalability	Medium	High	High	Medium
Easy to Configure	No	Yes	Yes	No
Overhead on Monitored System	Medium	Low	Low	Medium
Maintenance	Low	Medium	Medium	Medium
Performance	Medium	High	High	Medium
Protection against New attacks	High	Low	Medium	High
Easy to Use	Medium	Low	Low	Low

TYPES OF THREATS

There are two types of threats:-

- **Internal Threat-** Refers to risk of somebody from inside the company who can exploit a system to cause damage or steal data.
- **External Threat-** Any potential danger or risk that originates from outside an organization.


WHAT ARE INTERNAL THREATS?
Network Security Threats
Human Threats
Physical Security Threats
Software Threats
Legal Threats
Communication Security Threats
Other Threats
Social & Economic Threats

INTERNAL THREAT

- As employees of any organization have the privilege of accessing **physical equipment and documents**, without appropriate security measures they can **purposely cause damage**. Eg- Yahoo email leaks, Company was subject to the largest data breach on record.
- Accidental data loss and data breach are quite common. **Around 95% of security breaches happen due to human errors.**
- The common example we see is the people leaving their **laptops accidentally in train and buses while travelling**, or accidentally **deleting data** from a folder, or spilling a drink on devices**.**

CONTT..

- An organization's **servers are left unlocked** in a room, there are high chances anybody could walk into the room and **steal crucial information**.
- Even ordinary employees of the organization can also exploit the vulnerabilities accidentally by viewing anything on a **malicious website**. They may **unintentionally download a virus** and cause harm to the entire network**.**


External Suppliers
Poor Defence
Outdated Software
WHAT ARE EXTERNAL THREATS?
Cyber Attack
Exploitation
Social Engineering

EXTERNAL THREAT

- External attacks are harder to deal with than internal threats **because you have no control over people outside your organization.**
- Its better to understand the **intensity of attacks**, organizations need to know the **entry points from where these attacks can take place.**
- Some software is less harmful while some have the potential to destroy a network. The common examples include **spyware, adware, ransomware, worms, Rootkits, and Trojans.**

CONTT..

- Outsiders can launch an attack through hacking.
- Lack of knowledge regarding **cyber-attacks and unsafe practices can lead to cybercrimes.** Social engineering is the **biggest example where bank frauds and identity frauds happen**.
- A phishing email is a common form where a **bot or a person sends an email pretending to be in an authoritative position** in any **organization asking for confidential data.**

CONTT..

- Considering both **internal and external threats**, we realize that **both are devastating for any organization.** However, it depends on the industry and intention behind carrying out an attack.
- External threats are **equally dangerous** and are often a priority when **data security is concerned**.
- Most outsider attacks attempt to manipulate data and take advantage of a **company's structure, resources, employees, and information**. Thus, organizations need to inspect the network perimeters.
- We can prevent any attack that could stem from the inside by following strict policies and security measures.

How to protect company from threats?

- Consider a risk-based approach by addressing each problem individually. This way, we will know the priorities and reach an informed decision that can be cost-effective and gives you the best results.
- Make sure to **restrict the sharing of passwords** and other credentials through any means whether **emails, messages, Skype, or any communication channel as a part of cyber security measures**.
- Always remove **ex-employees data access rights** and eliminate **any data access controls after keeping a backup file of the data.**

CONTT..

- Consider automating everything by implementing **automation programs** that include **filtering, detecting, and sending alerts based on keywords to check** for any unusual activities. However, don't completely rely on **automation; instead, use a mix of both. Traditional methods that include background checks of employees and pre-employment screening are also important.**
- Recommended to conduct **risk assessments, insider threat analysis, and ensure proper implementation of security management practices.**