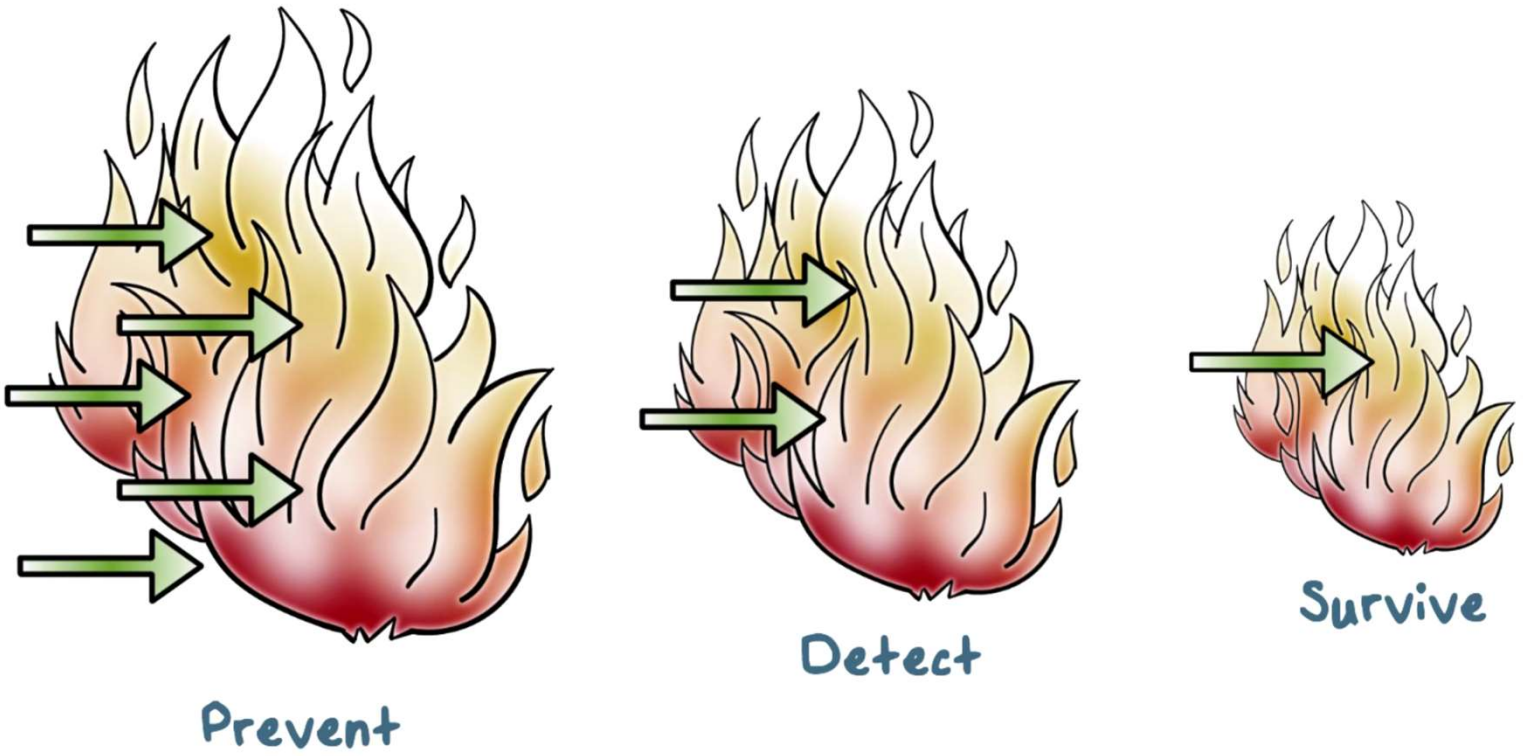
Intrusion Detection
Lesson Introduction

- Part of network defense-in-depth
- System architecture, algorithms, and deployment strategies of Intrusion detection
- Performance metrics
- Attacks on intrusion detection systems

Defense-in-Depth



Intrusion Examples

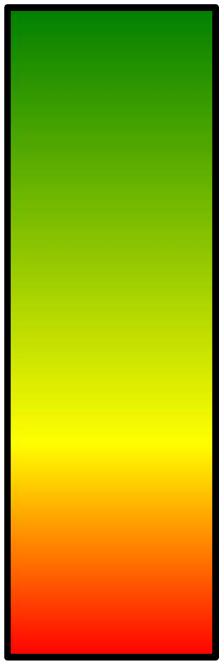
- Remote root compromise
- Web server defacement
- Guessing/cracking passwords
- Copying databases containing credit card numbers
- Viewing sensitive data without authorization
- Running a packet sniffer

- Distributing pirated software
- Using an unsecured modem to access internal network
- Impersonating an executive to get information
- Using an unattended workstation

Intrusion Detection Systems (IDS)

- Designed to Counter Threats:

Effective



Not effective

- Known, less sophisticated attacks
- Sophisticated targeted attacks
- New, Zero-day exploits

Intrusion Detection Systems (IDS)

Defense-In-Depth Strategies include:

- encryption
- detailed audit trails
- strong authentication and authorization controls
- active management of operating systems
- application security

ways of figuring out what's going on

Also known as a cyber "kill chain"

Almost all intrusion starts with some sort of reconnaissance

Intruder Behavior

Leave no trace that they were ever there

Done by setting up a back door. Some mechanism that allows you to come back easier than you did in the first time

I've got into the system, but I'm not happy just being a regular user. I want to be a super user, I want to get root access.

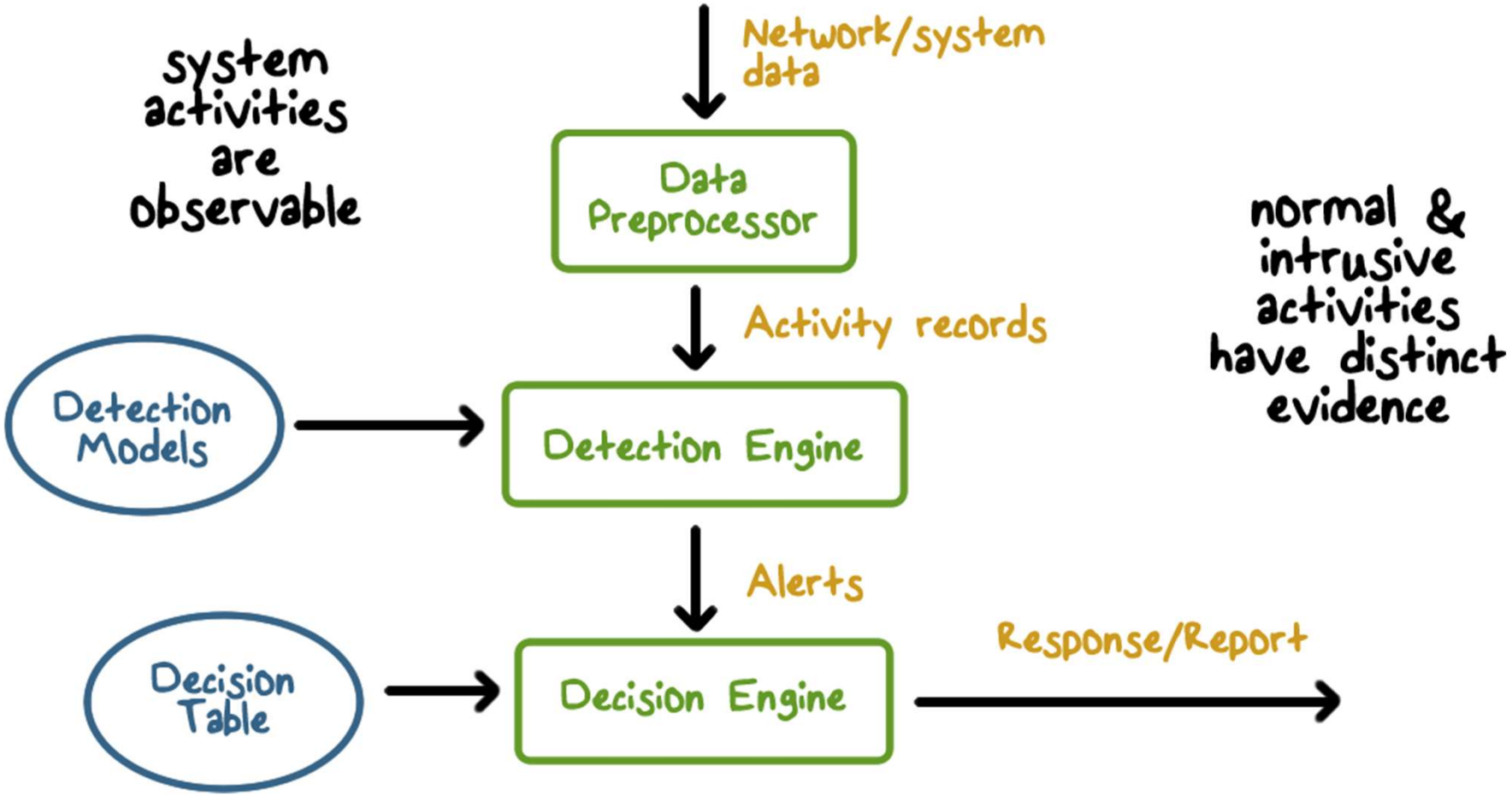
Elements of Intrusion Detection

- **Primary assumptions:**
  - System activities are observable
    We can tell what's going on.
  - Normal and intrusive activities have distinct evidence

Elements of Intrusion Detection

- **Components of intrusion detection systems:**
  - From an algorithmic perspective:
    - **Features** - capture intrusion evidences
    - **Models** - piece evidences together
  - From a system architecture perspective:
    - Audit data processor, knowledge base, decision engine, alarm generation and responses

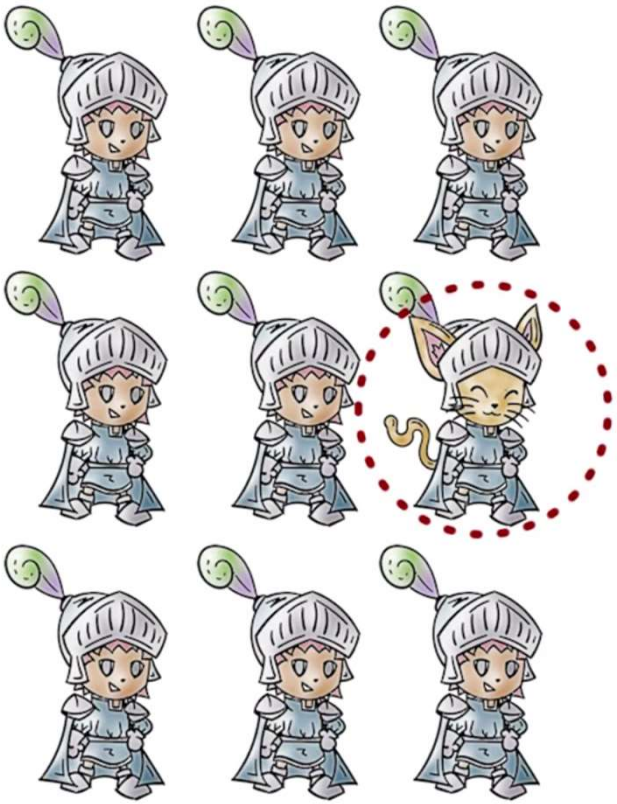
Components of Intrusion Detection Systems



Intrusion Detection Approaches

- **Modeling and analysis**
  - Misuse detection (a.k.a. signature-based)
  - Anomaly detection
- **Deployment**
  - Host-based
  - Network-based
- **Development and maintenance**
  - Hand-coding of “expert knowledge”
  - Learning based on data

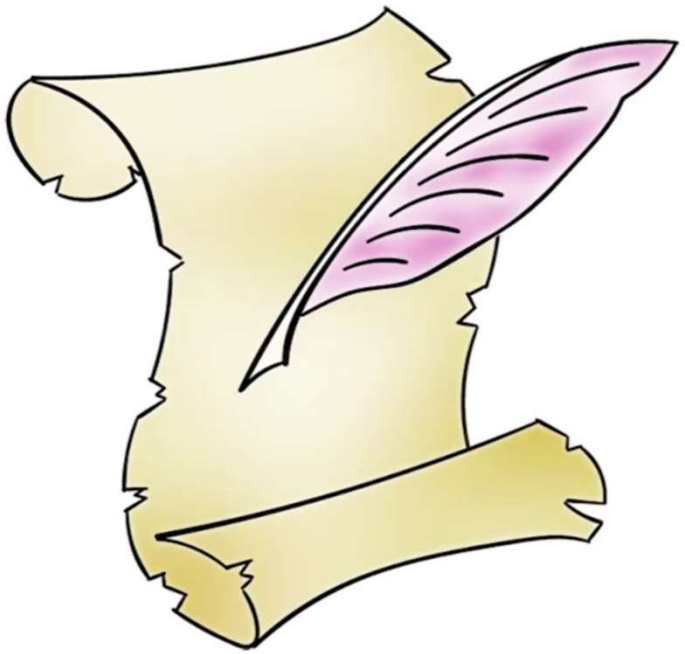
Analysis Approaches



Anomaly Detection:

- Involves the collection of data relating to the behavior of legitimate users over a period of time
- Current observed behavior is analyzed to determine whether this behavior is that of a legitimate user or that of an intruder

Analysis Approaches



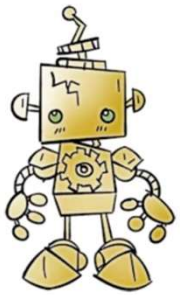
Misuse/ Signature Detection

- Uses a set of **known malicious data** patterns or attack rules that are **compared with current behavior**
- Also known as **misuse detection**
- **Can only identify known attacks** for which it has patterns or rules

A Variety of Classification Approaches

Statistical: Analysis of the observed behavior using univariate, multivariate, or time-series models of observed metrics.

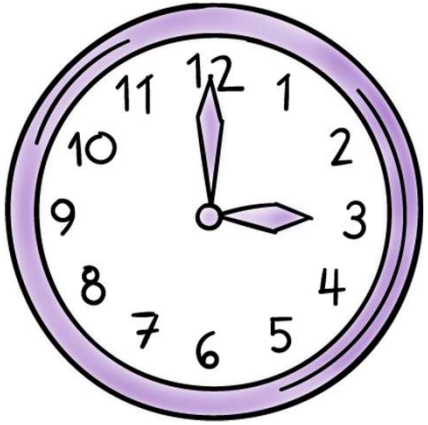
Knowledge Based: Approaches use an expert system that classifies observed behavior according to a set of rules that model legitimate behavior.



Machine Learning: Approaches automatically determine a suitable classification model from the training data using data mining techniques.

A Variety of Classification Approaches

Issues Affecting Performance:



- Efficiency

- Cost of Detection

Statistical Approaches

Characteristics:

- Use captured sensor data
- Multivariate models using time of and order of the event

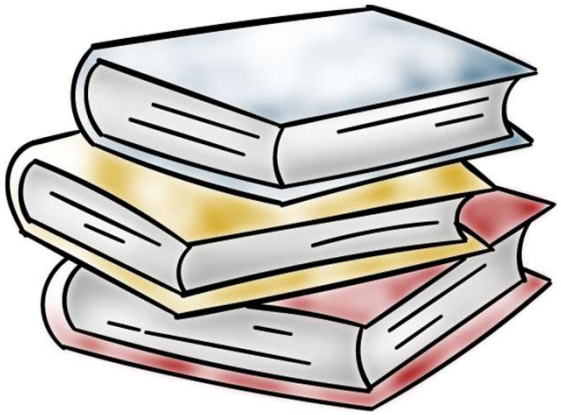
Advantages:

- their relative simplicity
- low computation cost
- lack of assumptions about expected behavior

Disadvantages:

- difficulty selecting suitable metrics
- not all behaviors can be modeled using these approaches.

Knowledge Based Approaches



- Developed during training to **characterize data into distinct classes**

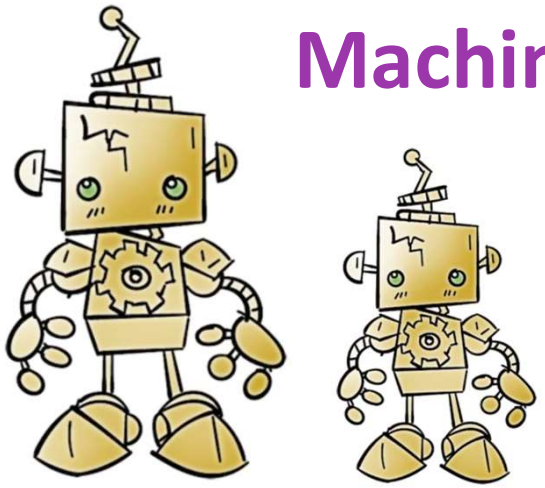
Advantages:

- Robust
- Flexible

Disadvantages:

- The difficulty and time required to develop knowledge from the data
- Human experts must assist with the process

Machine Learning Approaches



- Use **data mining techniques** to develop a model that can classify data as normal or anomalous

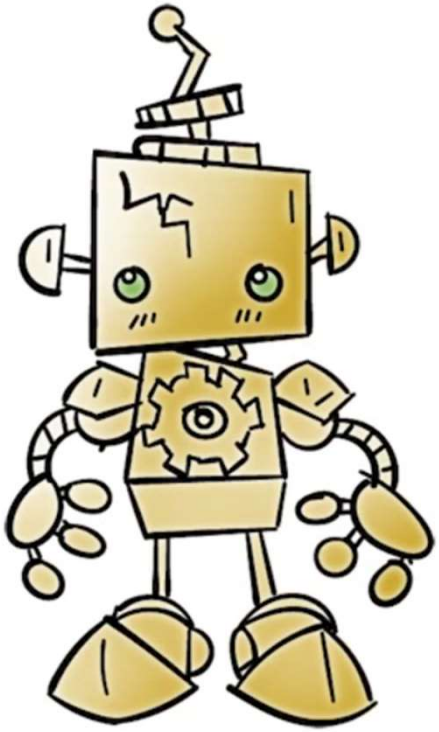
Advantages:

- Flexibility
- Adaptability
- Ability to capture interdependencies between observed metrics

Disadvantages:

- Dependency on assumptions about accepted behavior
- High false alarm rate
- High resource cost
- Significant time and computational resources

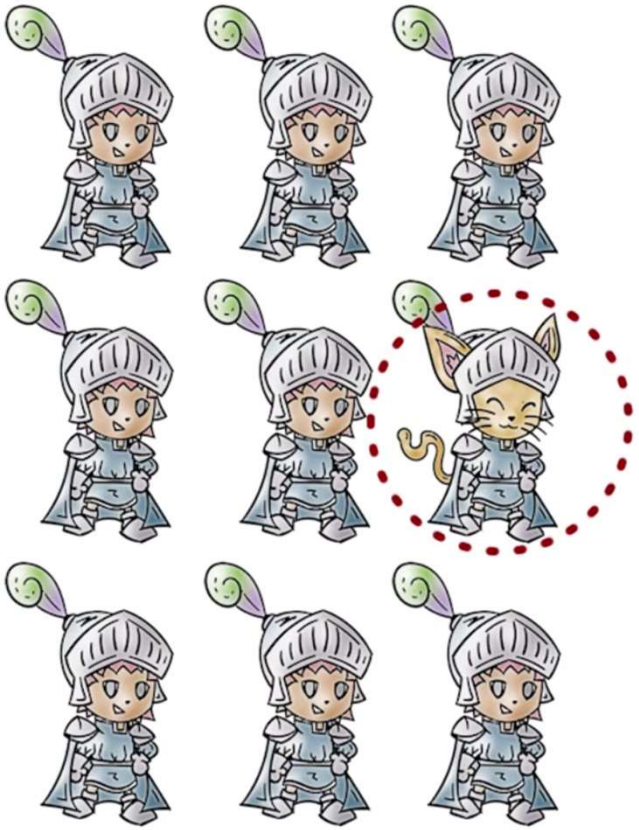
Machine Learning Intruder Detection Approaches



- Neural networks: Simulate human brain operation with neurons and synapse between them

- Clustering and outlier detection: Group the observed data into clusters then identify subsequent data as either belonging to a cluster or as an outlier.

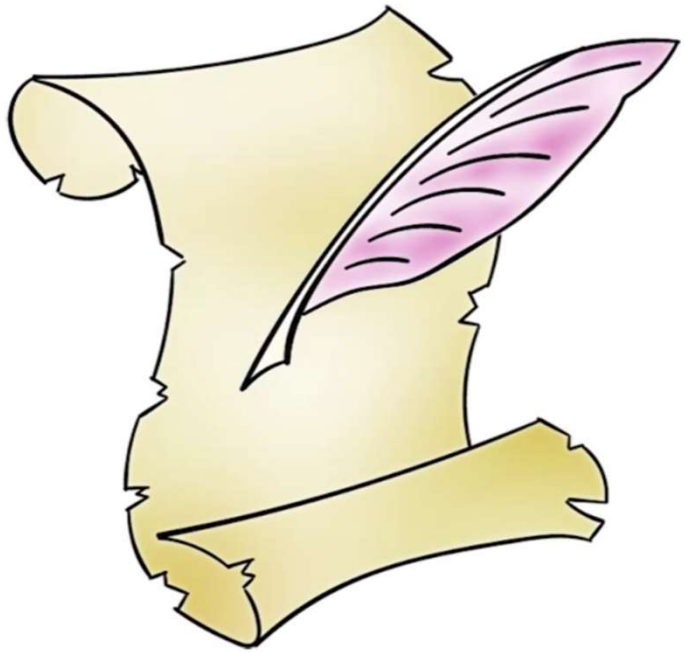
Limitations of Anomaly Detection



- They are generally trained on **legitimate data**

- This **limits the effectiveness** of some of the techniques discussed.

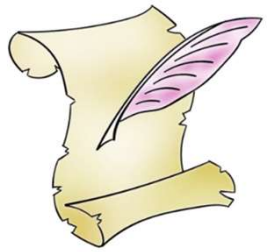
Misuse or Signature Detection



Detect intrusion by:

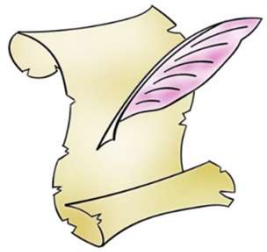
- observing events in the system
- applying a set of patterns or rules to the data
- determining if the is intrusive or normal

Signature Approaches



- **Match a large collection of known patterns** of malicious data against data stored on a system or in transit over a network
- The signatures need to be **large enough to minimize the false alarm rate**, while still detecting a sufficiently large fraction of malicious data
- **Widely used** in anti-virus products, network traffic scanning proxies, and in NIDS

Signature Approach
Advantages & Disadvantages



Advantages:

- Low cost in time and resource use
- Wide Acceptance

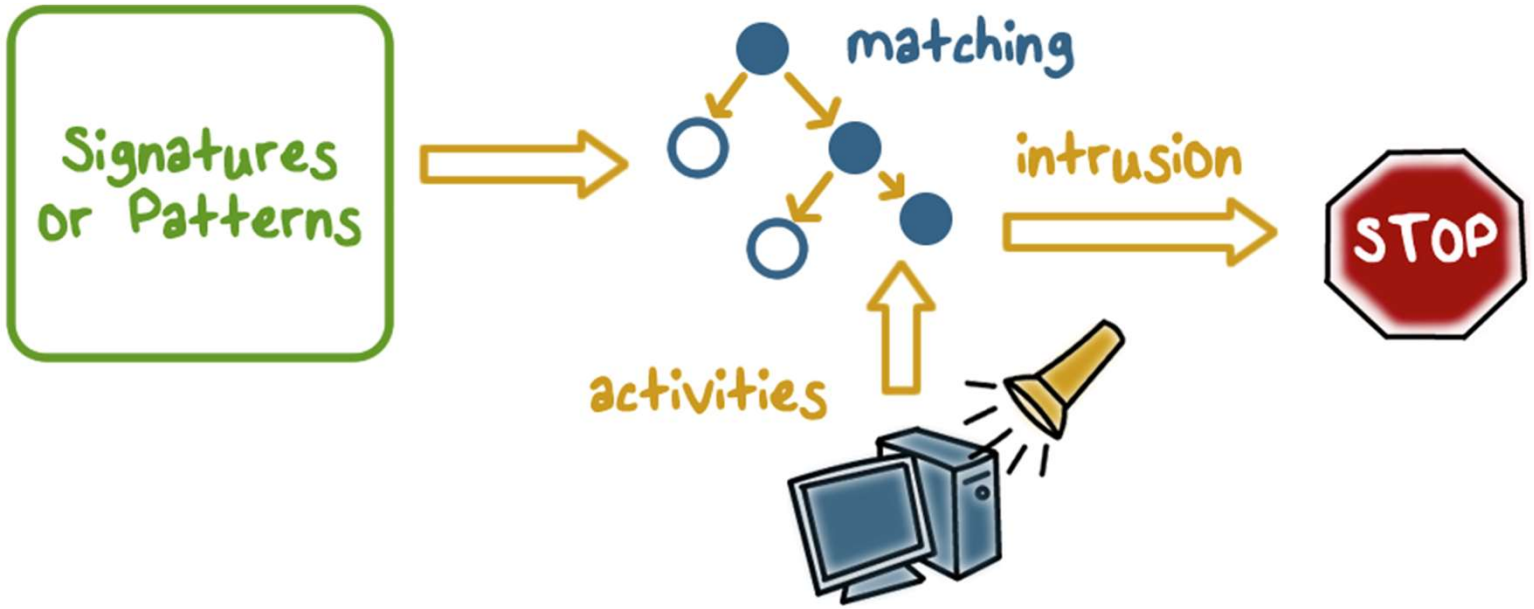
Disadvantages:

- Significant effort to identify and review new malware to create signatures
- inability to detect zero-day attacks

Rule-Based Detection

- Involves the **use of rules for identifying known penetrations** or penetrations that would exploit known weaknesses
- Rules can also be defined that **identify suspicious behavior**
- Typically rules used are **specific**
- **SNORT** is an example of a rule-based NIDS

Misuse Signature Intruder Detection



Example: if (src_ip == dst_ip && src_prt == dst_prt) then "land attack"

Hundreds of thousands of rules list. The application will loop over all the rules.

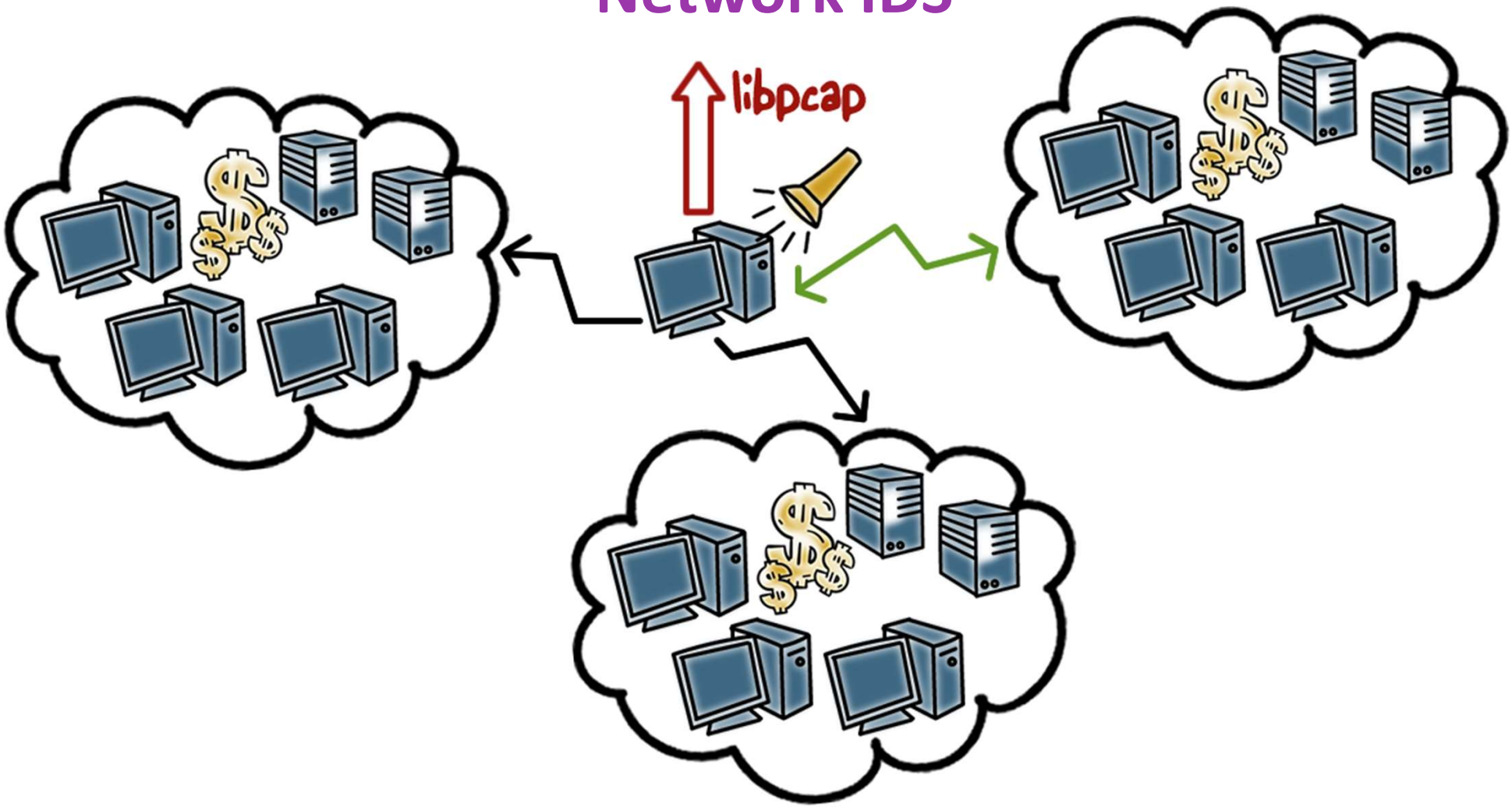
Can't detect new attacks

Monitoring Networks and Hosts

An IDS performs passive monitoring:

- It **records and analyzes data** about system and network activity
- If the IDS sends out an alert AND the response policy dictates intervention, then **activities are affected**

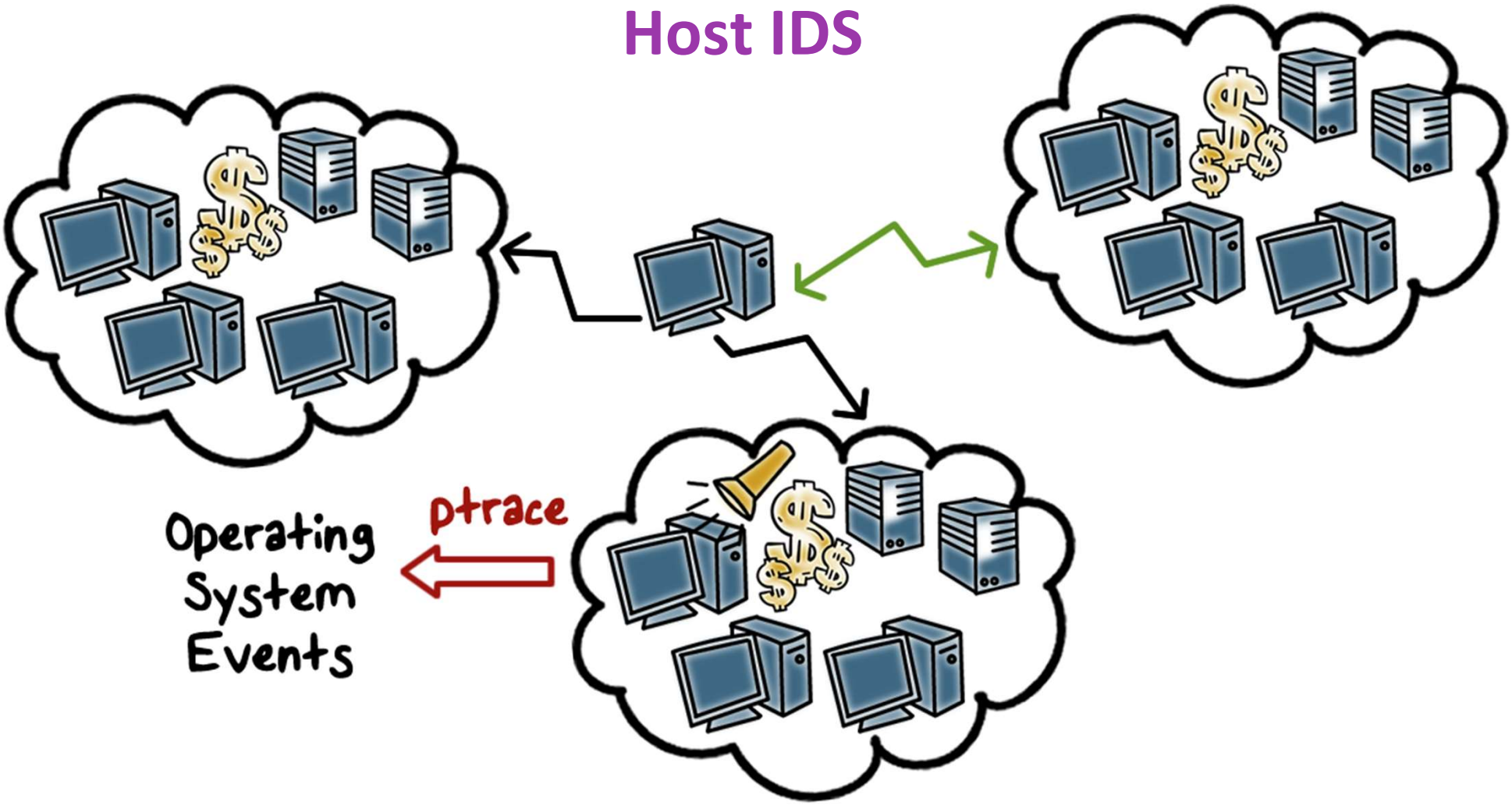
Network IDS



Network Based IDS (NIDS)

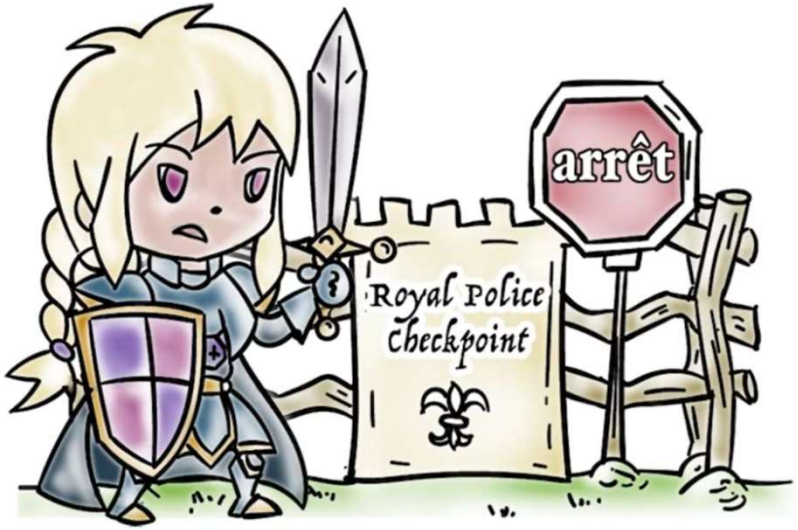
- **Monitors traffic at selected points** on a network in real or close to real time
- May examine network, transport, and/or application-level protocol activity
- **Comprised of a number of sensors**, one or more servers for NIDS management functions, and one or more management consoles for the human interface
- **Analysis of traffic patterns** may be done at the sensor, the management server or a combination of the two

Host IDS



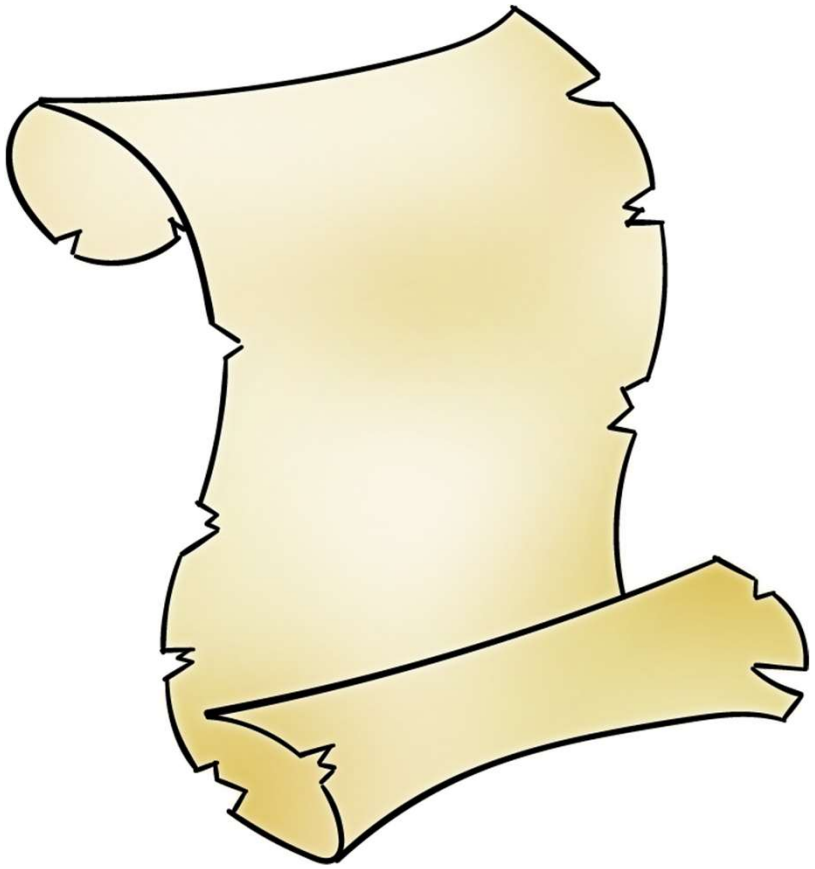
Inline Sensors

Can be achieved by:



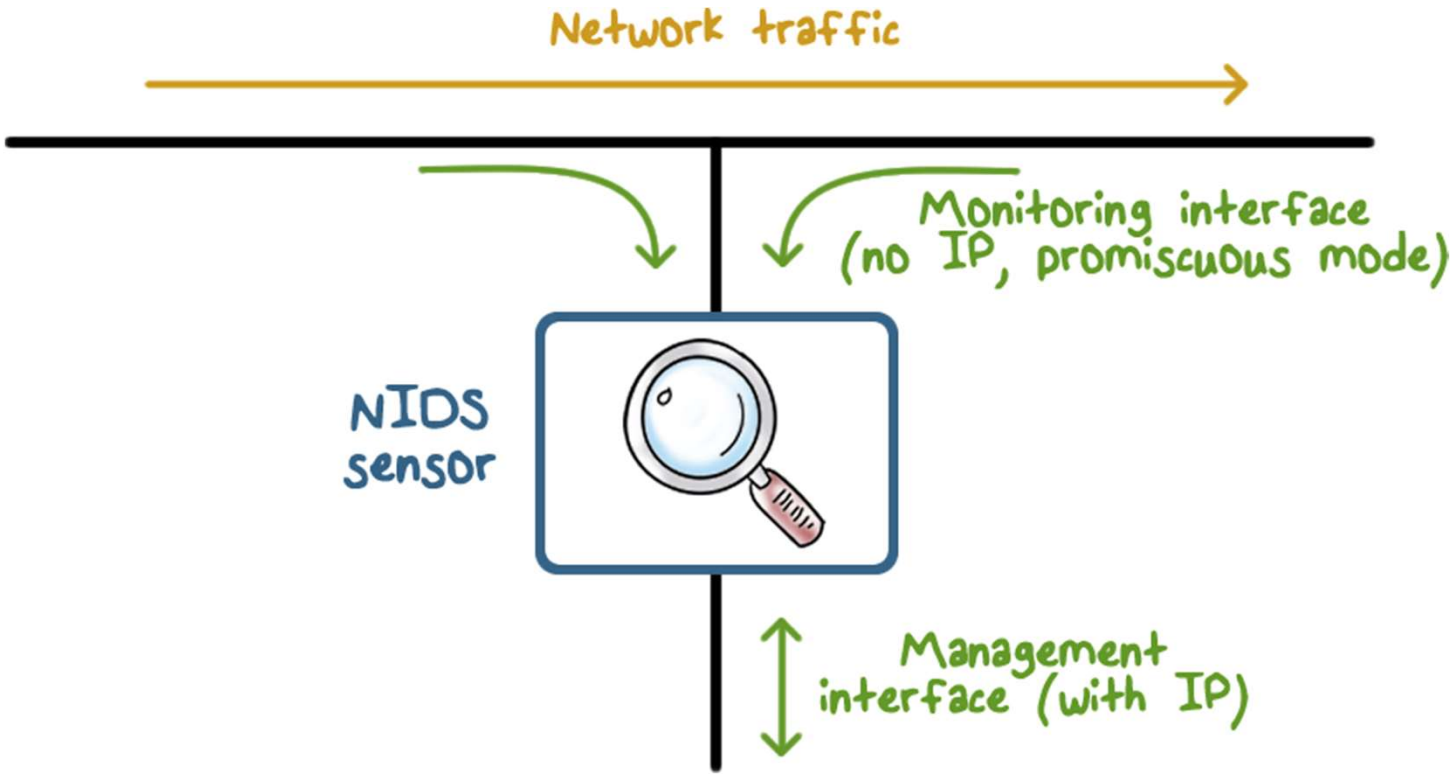
- **Combining NIDS sensor logic with a firewall or LAN switch**. This has the advantage of no additional hardware is needed
- Using a **stand-alone inline NIDS sensor**

Passive Sensors

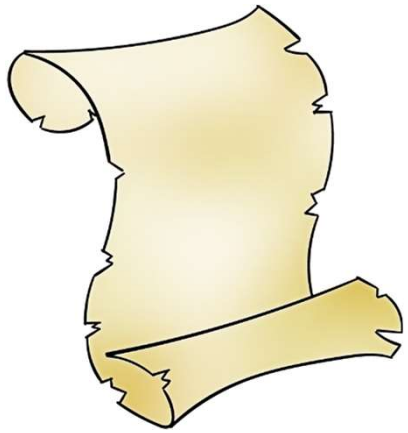


- A passive sensor **monitors a copy of network traffic**; the actual traffic does not pass through the device
- Passive sensors are more efficient

Passive Sensors

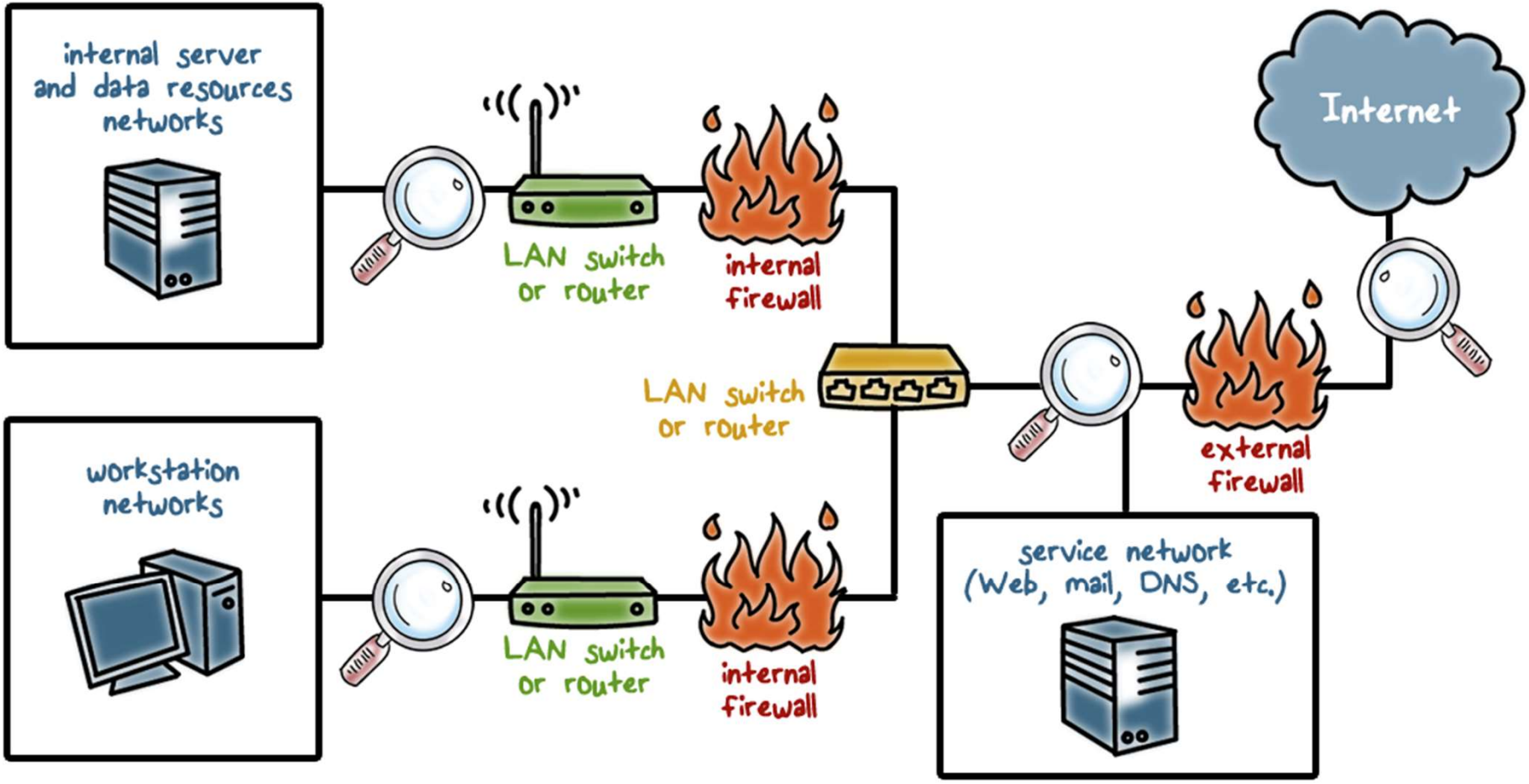


Firewall Versus Network IDS



- **Firewall**
  - Active filtering
  - Fail-close
- **Network IDS**
  - Passive monitoring
  - Fail-open

NIDS Sensor Deployment



Honeypots

Honeypots are **decoy systems designed to lure attackers** away from critical systems.

Honeypots are designed to:

- divert an attacker
- collect information about an attacker
- encourage an attacker to stay long enough for administrators to respond

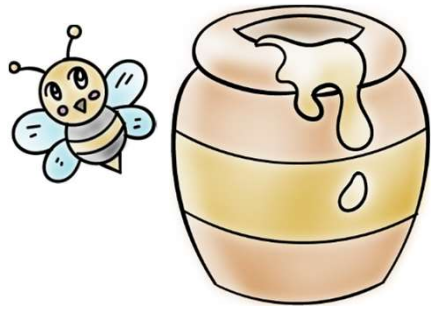
Honeypots

- Honeypots are filled with **fabricated information**
- **Any accesses** to a honeypot trigger monitors and event loggers
- An attack against a honeypot is made to **seem successful**

Honeypots

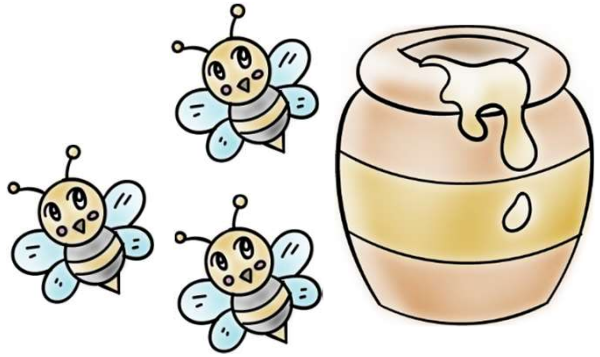
- A honeypot has **no production value**
- There is **no legitimate reason to access** a honeypot
- Any attempt to communicate with a honeypot is **most likely a probe, scan, or attack**
- If a honeypot **initiates outbound traffic**, the system is most likely compromised

Honeypot Classification



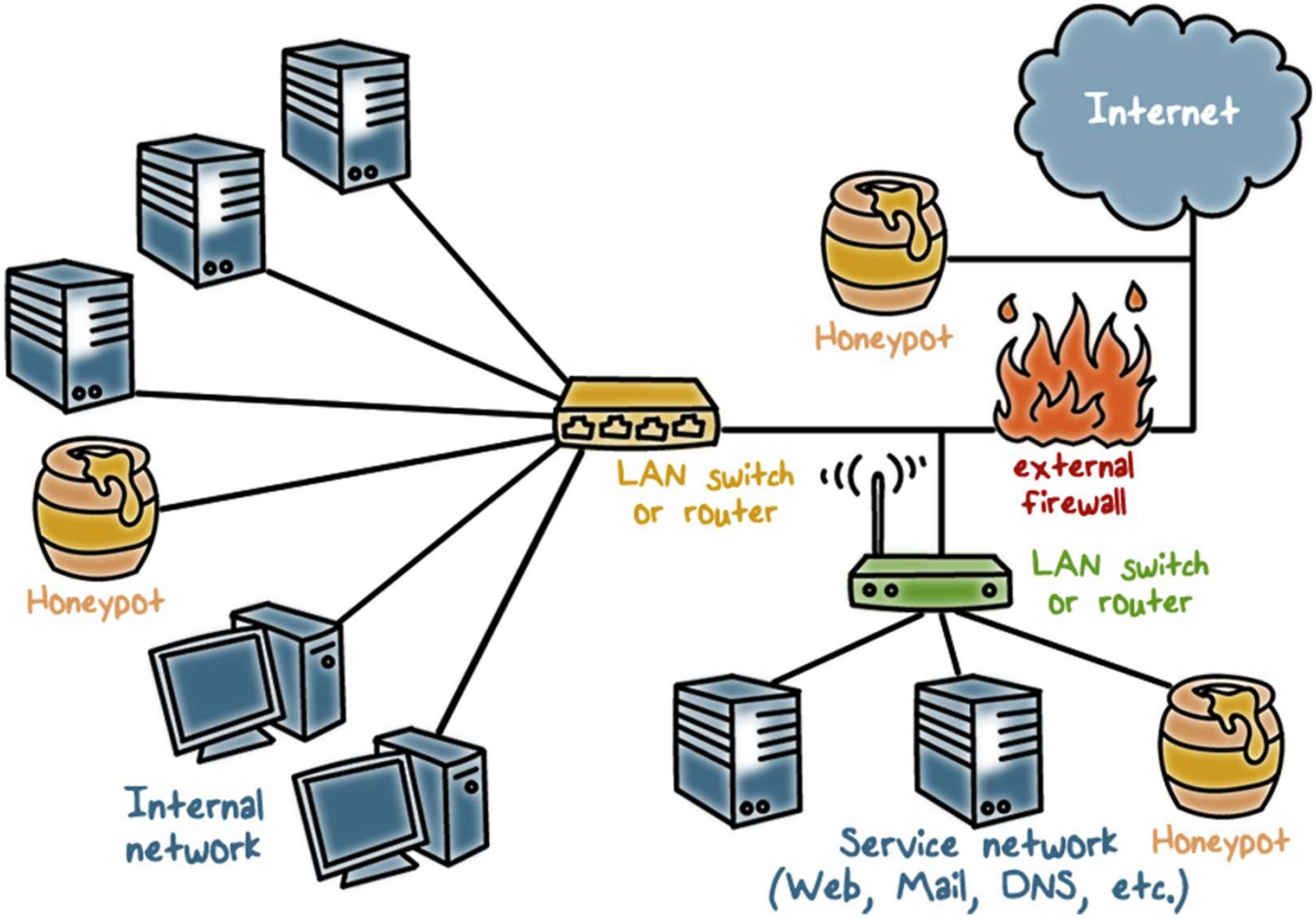
- **Low interaction honeypot:**
  - Emulates particular IT services or systems well enough to provide a realistic initial interaction, but **does not execute a full version** of those services or systems
  - Provides a **less realistic target**
  - Often **sufficient for use as a component** of a distributed IDS to warn of imminent attack

Honeypot Classification



- **High interaction honeypot**
  - A **real system, with a full operating system**, services and applications, which are instrumented and deployed where they can be accessed by attackers
  - **More realistic target** that may occupy an attacker for an extended period
  - However, it **requires significantly more resources**

Honeypot Deployment



Evaluating IDS

Detection rate or True Positive(TP) rate: given that there is an intrusion, how likely will the IDS correct output an alert.

False Negative Rate: FN = 1 - TP

Evaluating IDS

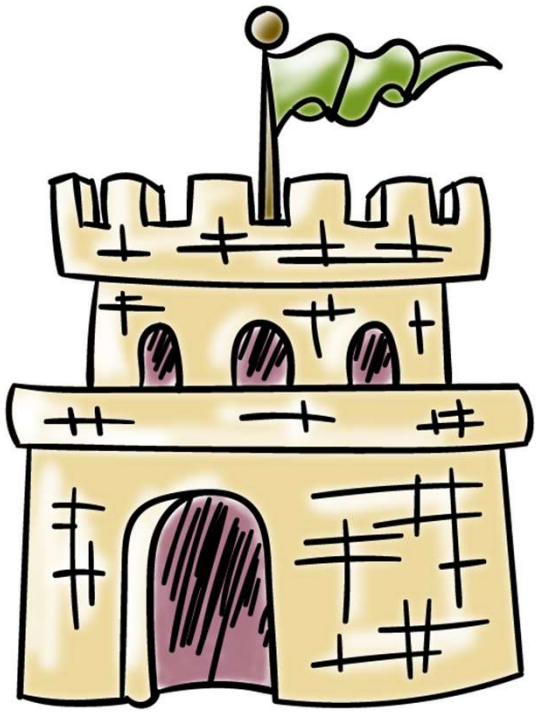
False alarm or False Positive (FP) rate: given that there is no intrusion, how likely is the IDS to falsely output an alert.

True Negative Rate: TN = 1 - FP

Evaluating IDS

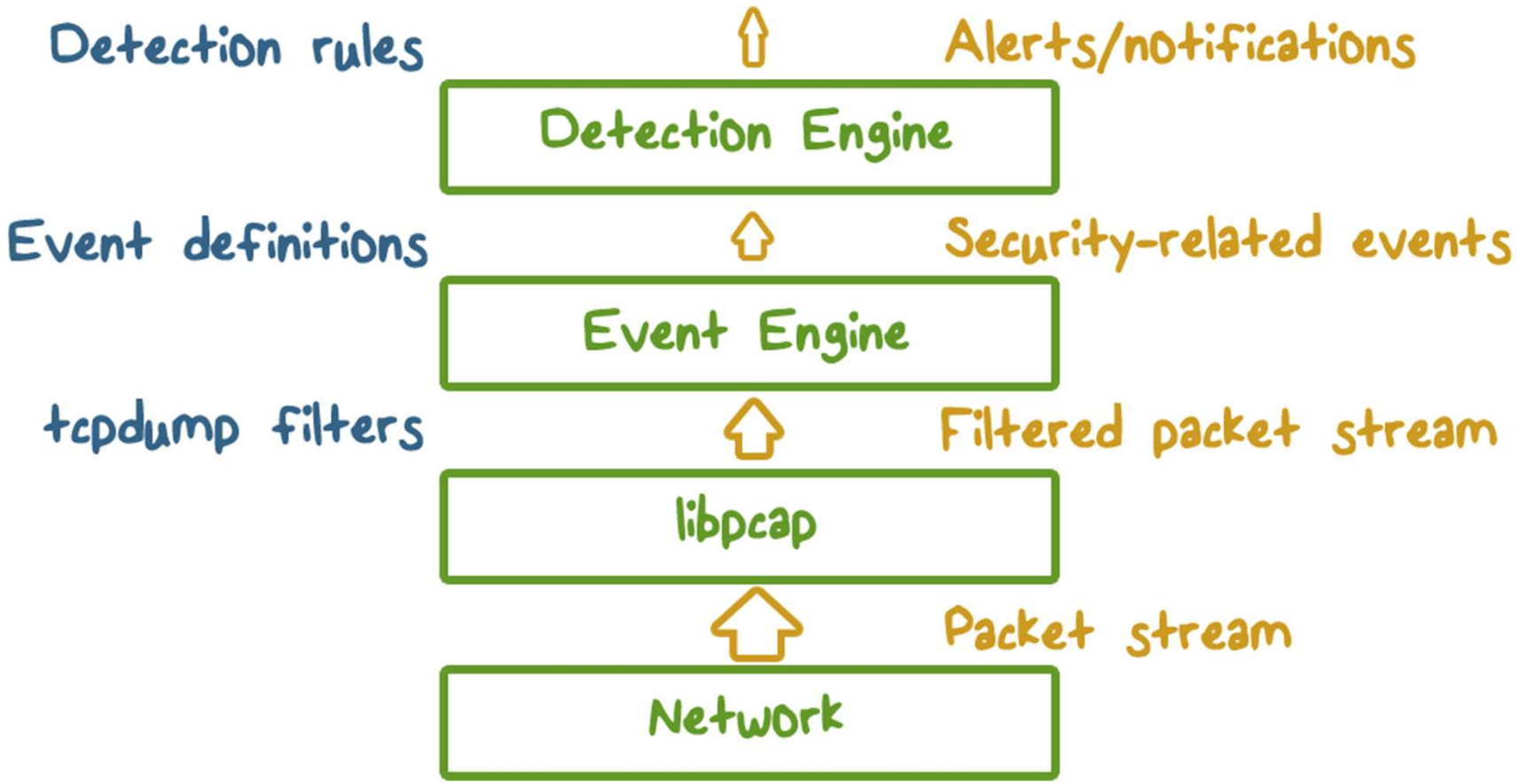
Bayesian detection rate: given that the IDS produces an alert, how likely is it that an intrusion actually occurs?

Architecture of Network IDS



- Packet data **volume can be huge**
- Base rate at the packet level **is typically low**
- Applying detection algorithms at this level **may result in a low bayesian detection rate**

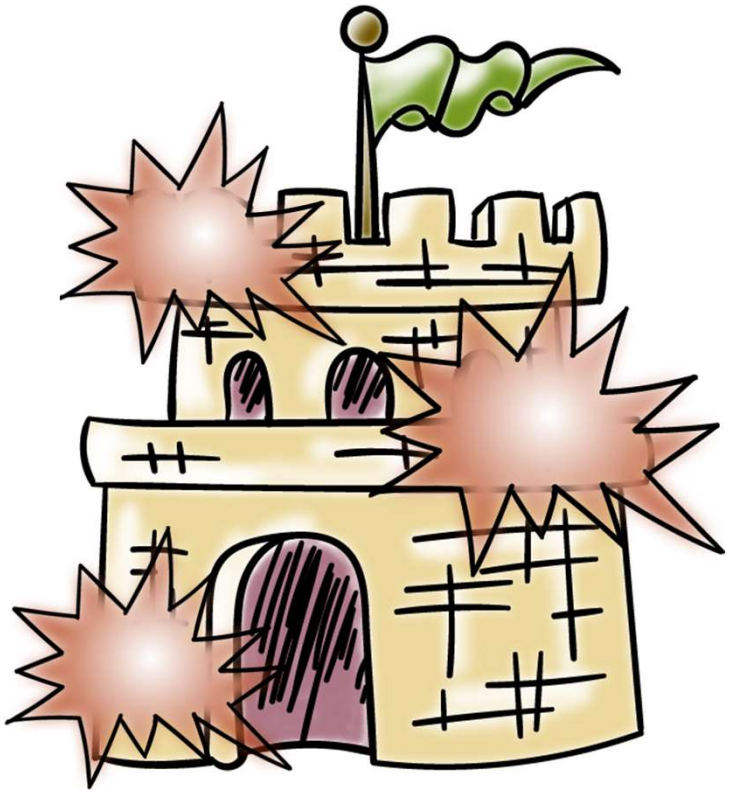
Architecture of Network IDS



Eluding Network IDS

- **What the IDS sees may not be what the end system gets**
  - **Ambiguities in protocols** lead different implementations in operating systems:
    - E.G. TTL, fragments

DoS Attacks on Network IDS



- **Resource exhaustion**
  - CPU resources
  - Memory
  - Network bandwidth
- **Abusing reactive IDS**
  - False positives
  - Nuisance attacks or “error” packets/connections

Intrusion Prevention Systems (IPS)

- Also known as **Intrusion Detection and Prevention System** (IDPS)
- Is an **extension of an IDS** that includes the capability to attempt to block or prevent detected malicious activity
- Can be host-based, network-based, or distributed/hybrid
- Can use **anomaly detection to identify behavior** that is not that of legitimate users, or signature/heuristic detection to identify known malicious behavior can block traffic as a firewall does, but makes use of the types of algorithms developed for IDSs to determine when to do so

making a system looks more secure and stronger, to discourage the attacker

Intrusion Detection
Lesson Summary

- Anomaly detection and misuse/signature detection
- Network IDS, IPS, and honeypots
- True positive, false positive, and the base-rate fallacy