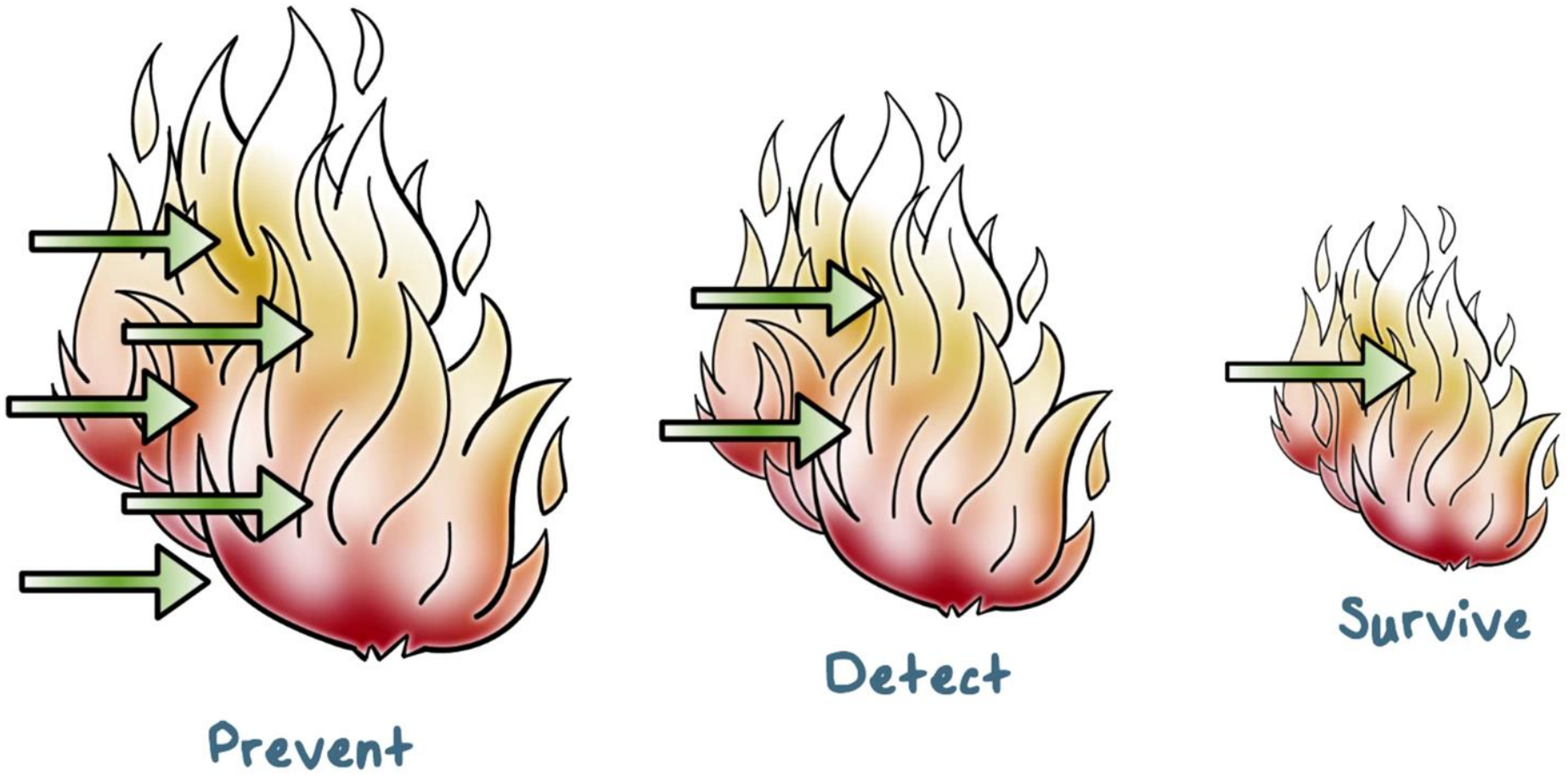
Intrusion Detection

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
- Running a packet sniffer
- Web server defacement
- Distributing pirated software
- Guessing/cracking passwords
- Using an unsecured modem to access internal network
- Copying databases containing credit card numbers

- Impersonating an executive to get information
- Viewing sensitive data without authorization
- Using an unattended workstation

Intrusion Detection Quiz

Select the characteristic that best describes each network security system.

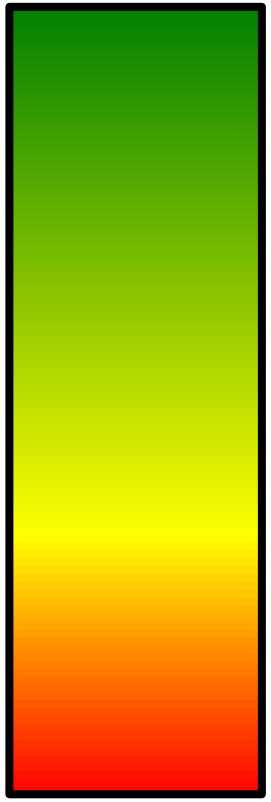
Type (F) for Firewalls or (I) for IDS:

- ☐ tries to stop intrusion from happening
- ☐ tries to evaluate an intrusion after it has happened
- ☐ watches for intrusions that start within the system
- ☐ limits access between networks to prevent intrusion

Intrusion Detection Systems (IDS)

- Designed to Counter Threats:

Effective

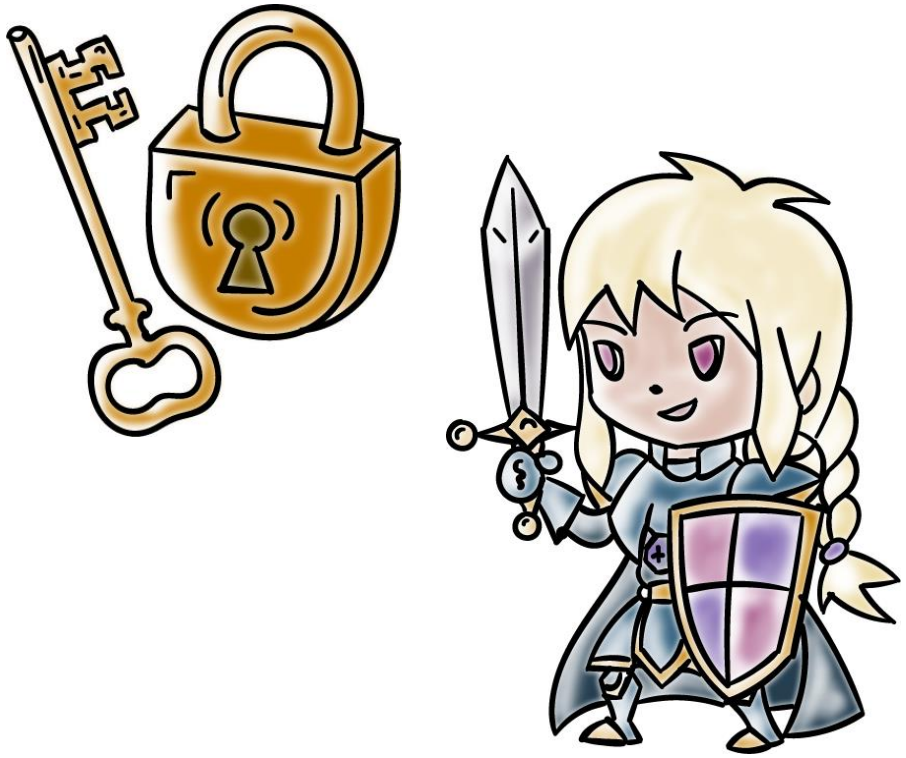


Not effective

- 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

Intruder Behavior

Intruder Quiz

Type True (T) or False (F) for each statement:

- ☐ An intruder can also be referred to as a hacker or cracker.
- ☐ Activists are either individuals or members of an organized crime group with a goal of financial reward.
- ☐ Running a packet sniffer on a workstation to capture usernames and passwords is an example of intrusion.
- ☐ Those who hack into computers do so for the thrill of it or for status.
- ☐ Intruders typically use steps from a common attack methodology.

Types of Backdoors Quiz

Choose the description that best fits each type of backdoor:

- ☐ Compiler Backdoors
- ☐ Object Code Backdoors
- ☐ Asymmetric Backdoors

A. This backdoor is hard to detect because it modifies machine code.

B. This backdoor can only be used by the person who created it, even if it is discovered by others.

C. This backdoor inserts backdoors into other programs during compilation.

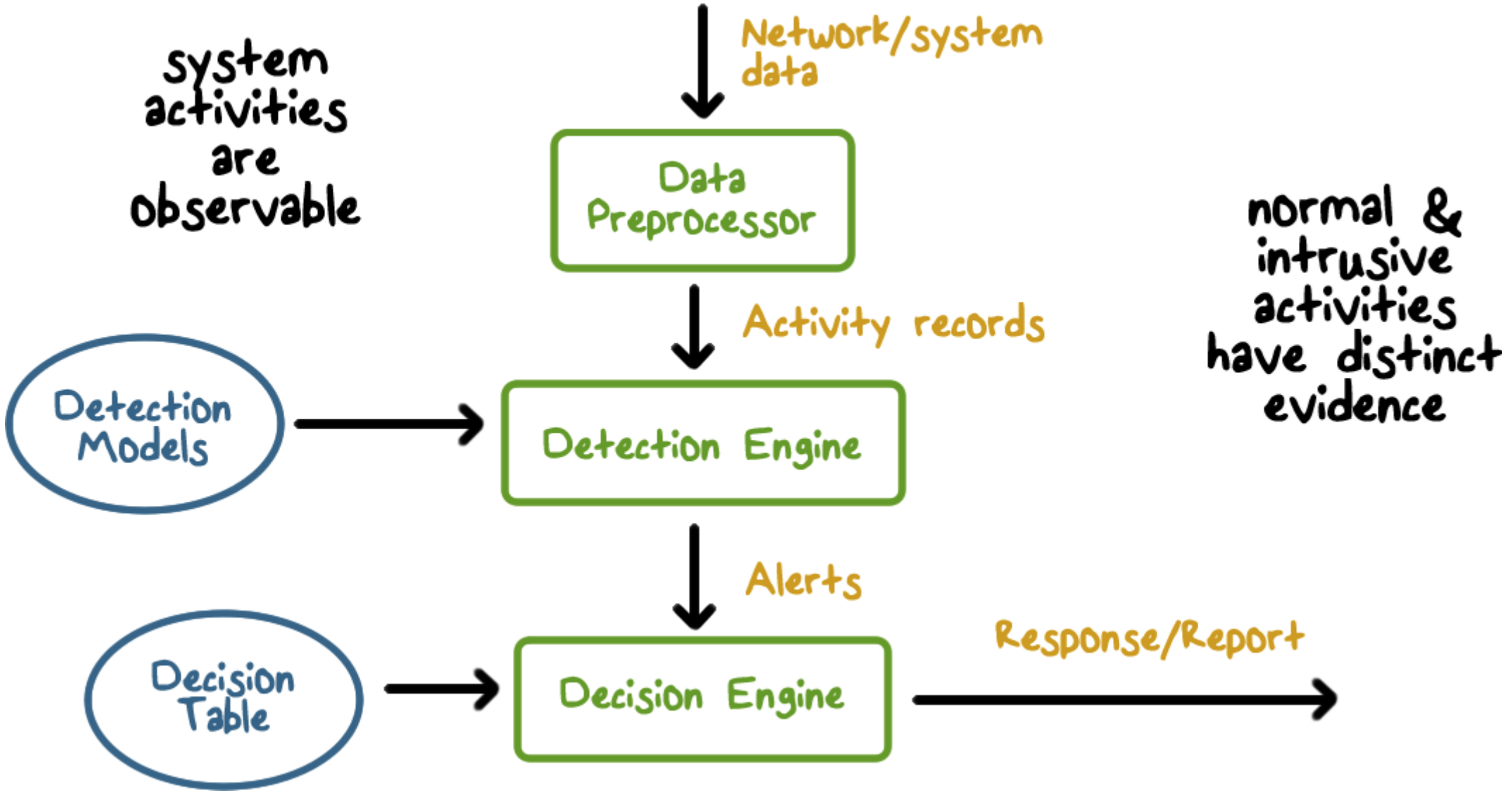
Elements of Intrusion Detection

- **Primary assumptions:**
  - System activities are observable
  - 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

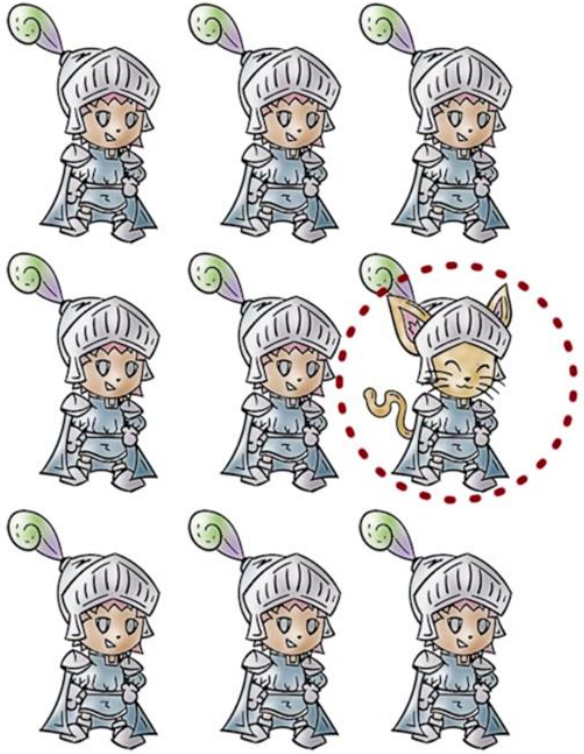
Components of Intrusion Detection Systems



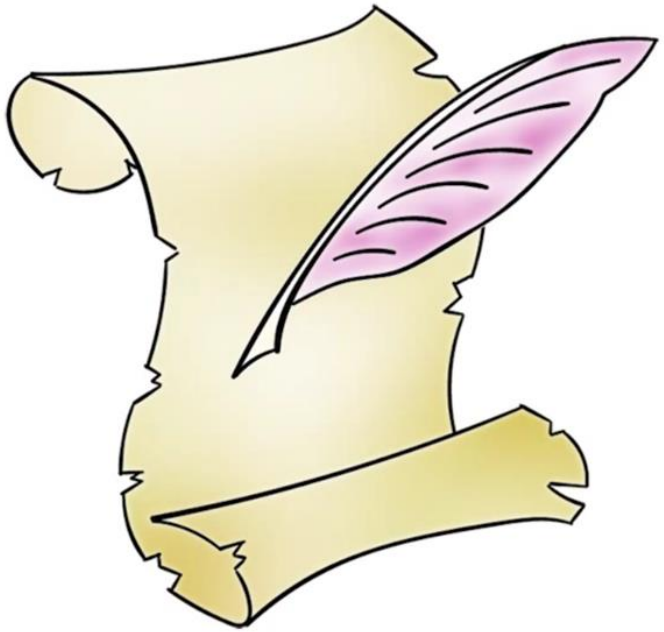
Intrusion Detection Approaches

- **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

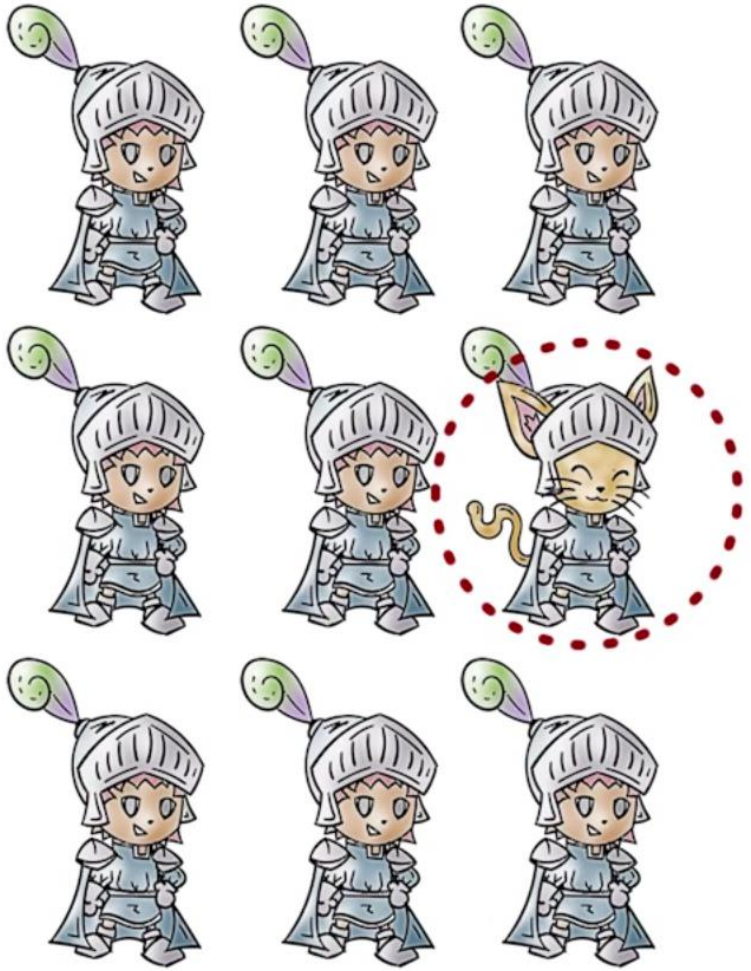


- Anomaly Detection



- Misuse/ Signature Detection

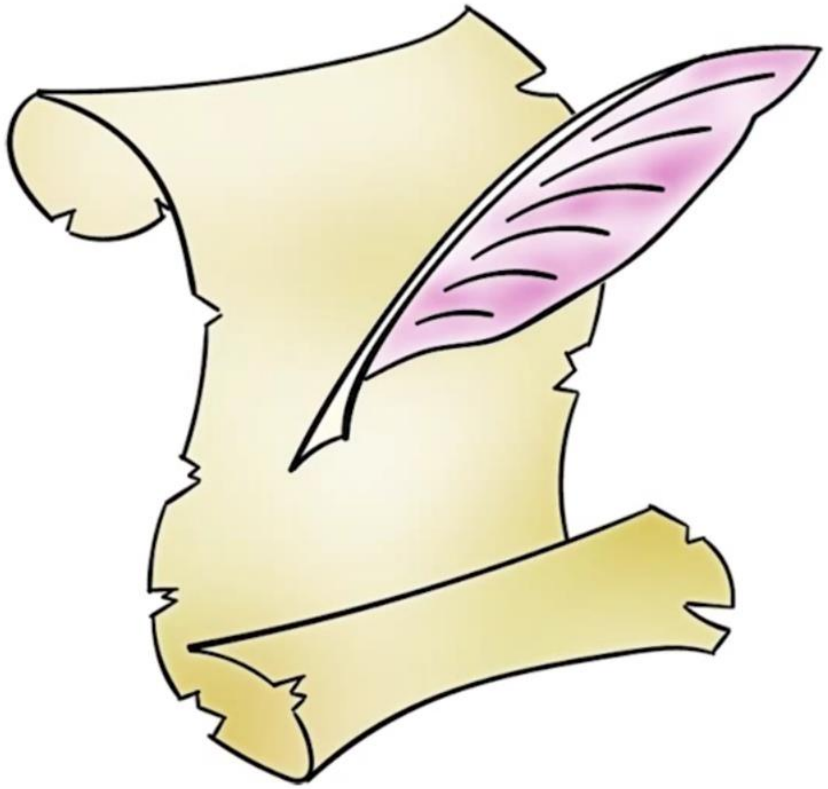
Analysis Approaches



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

Anomaly Detection Quiz

Check all answers that are true regarding Anomaly detection systems:

- ☐ The longer the system is in use, the more it learns about network activity.
- ☐ If malicious activity looks like normal traffic to the system, it will not detect an attack.
- ☐ False positives can become a problem, normal usage can be mistaken for an attack.

Signature Detection Quiz

Check all answers that are true regarding

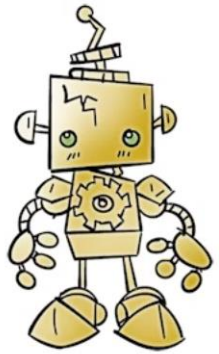
Signature Based detection:

- ☐ New threats can be detected immediately.
- ☐ When a new virus is identified, it must be added to the signature databases
- ☐ Can only detect an intrusion attempt if it matches a pattern that is in the database

A Variety of Classification Approaches

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

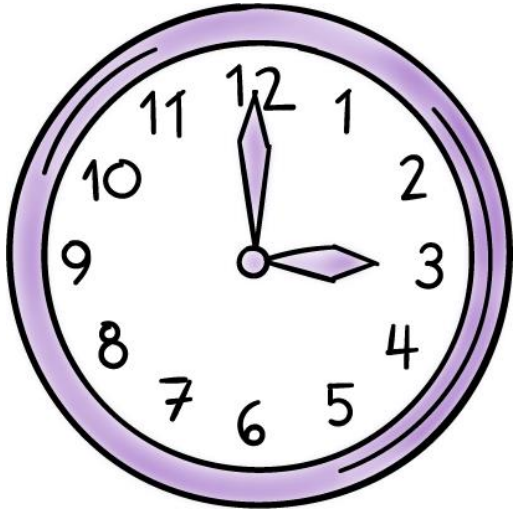
Knowledge Based: Approaches use an expert system that classifies observed behavior according to a set of rules that model legitimate behavior.



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

Anomaly Quiz

Which of the following **could be considered an anomaly** to typical network traffic?

- ☐ A IP address
- ☐ A port address
- ☐ Packet length
- ☐ Flag setting

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

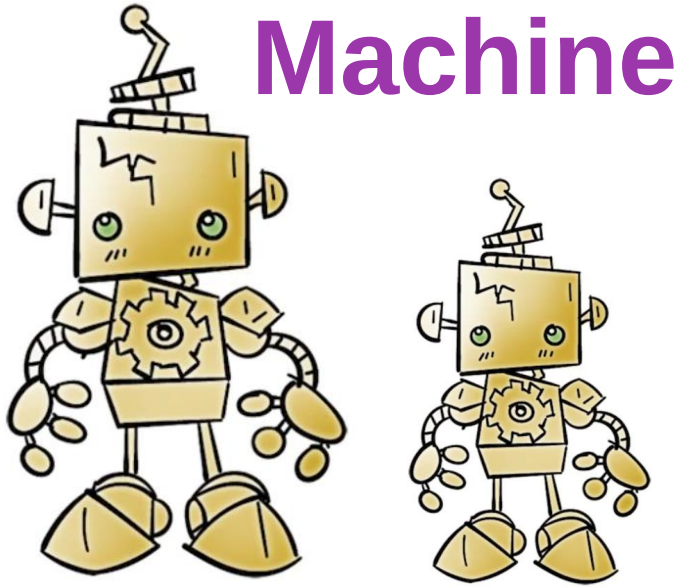
Statistical & Knowledge Based Approaches Quiz

Which of these characteristics describes the **statistical approach** and which describe a **knowledge based** approach? **Write S or K in the box:**

☐ Any action that does not fit the normal behavior profile is considered an attack.

☐ Any action that is not classified as normal is considered to be an attack.

Machine Learning Approaches



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

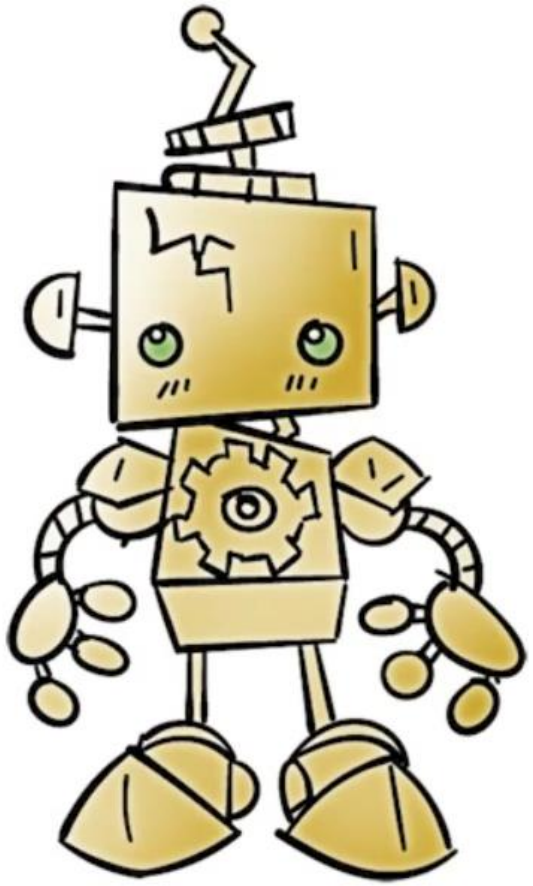
Advantages:

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

Disadvantages:

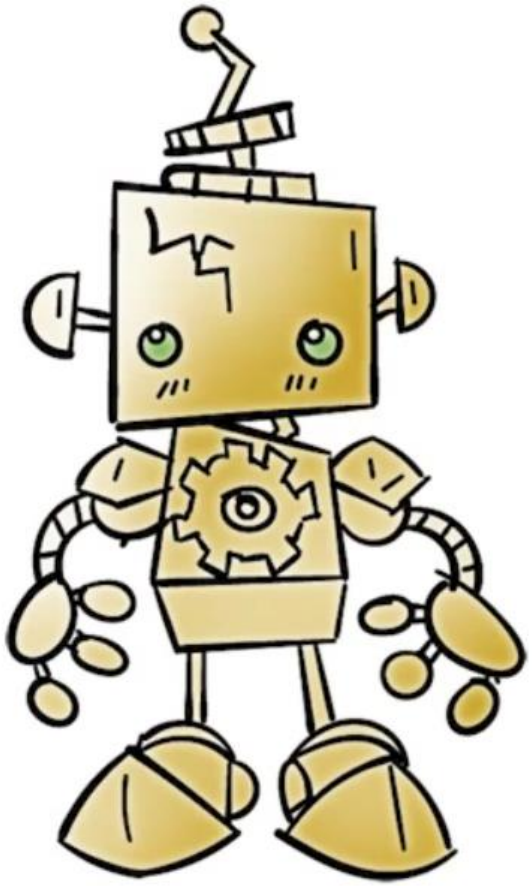
- Dependency on assumptions about accepted behavior
- High false alarm rate
- High resource cost
- Significant time and computational resources

Machine Learning Intruder Detection Approaches



- Bayesian networks: Encode probabilistic relationships among observed metrics.
- Markov models: Develop a model with sets of states

Machine Learning Intruder Detection Approaches

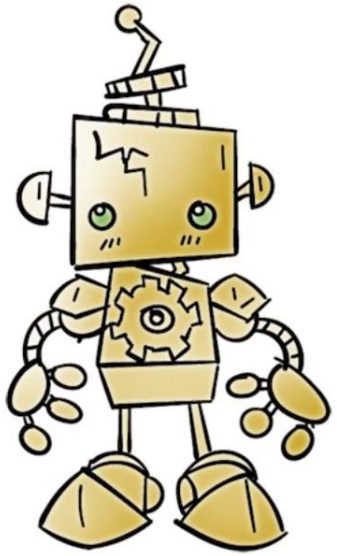


- Neural networks: Simulate human brain operation with neurons and synapse between them

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

Machine Learning Quiz

Which description best describes the Machine Learning **approach for Intruder Detection**:

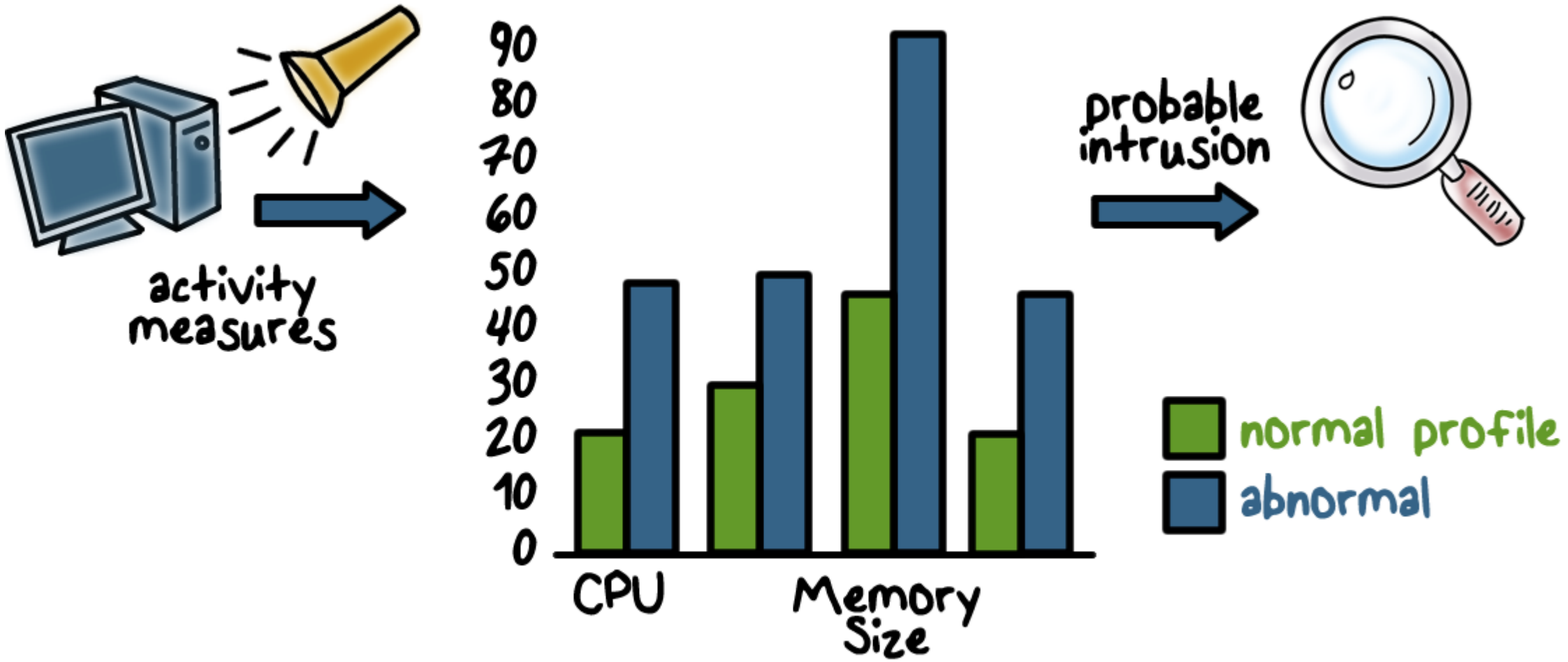


- ☐ detects new and novel attacks
- ☐ detects attacks similar to past attacks

Limitations of Anomaly Detection

- They are generally trained on **legitimate data**
- This **limits the effectiveness** of some of the techniques discussed.

Anomaly Detection Example



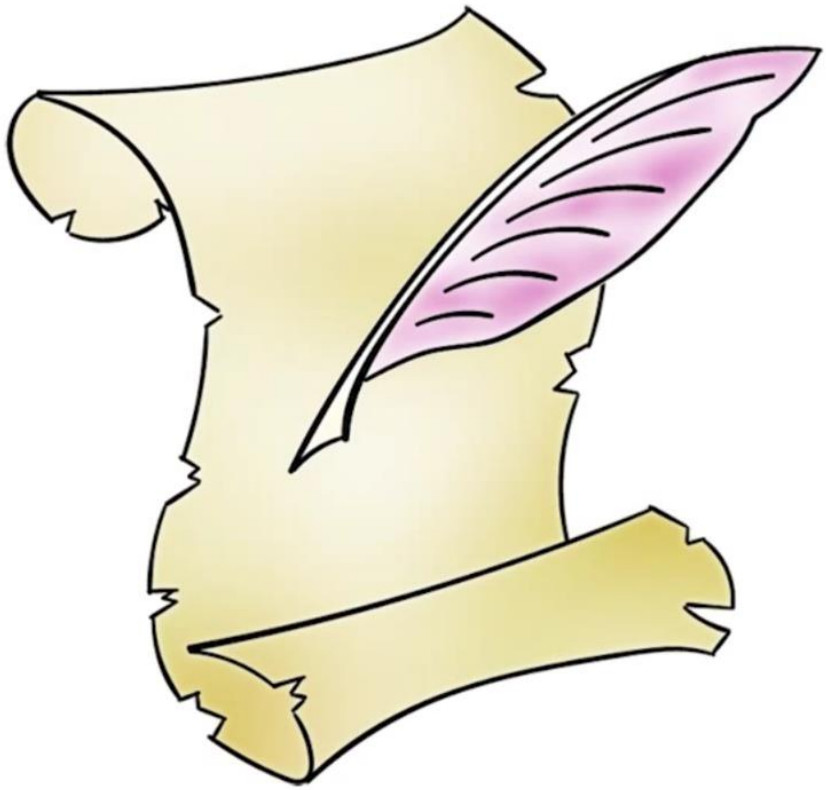
Relatively high false positive rate - anomalies can just be new normal activities.

Anomalous Behavior Quiz

One of the weaknesses of anomalous intruder detection is that a system must learn what is normal behavior. While it is learning this, the network is vulnerable to attack. What can be done to mitigate this weakness?

Write your answer in the textbox:

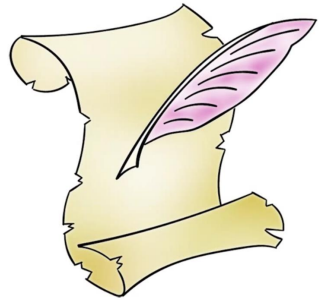
Misuse or Signature Detection



Detect intrusion by:

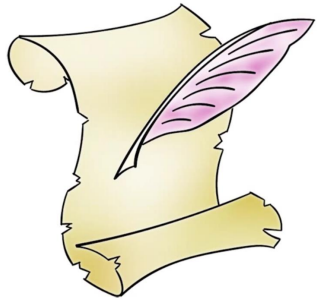
- observing events in the system
- applying a set of patterns or rules to the data
- determining if the is intrusive or normal

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

Zero Day Market Place Quiz

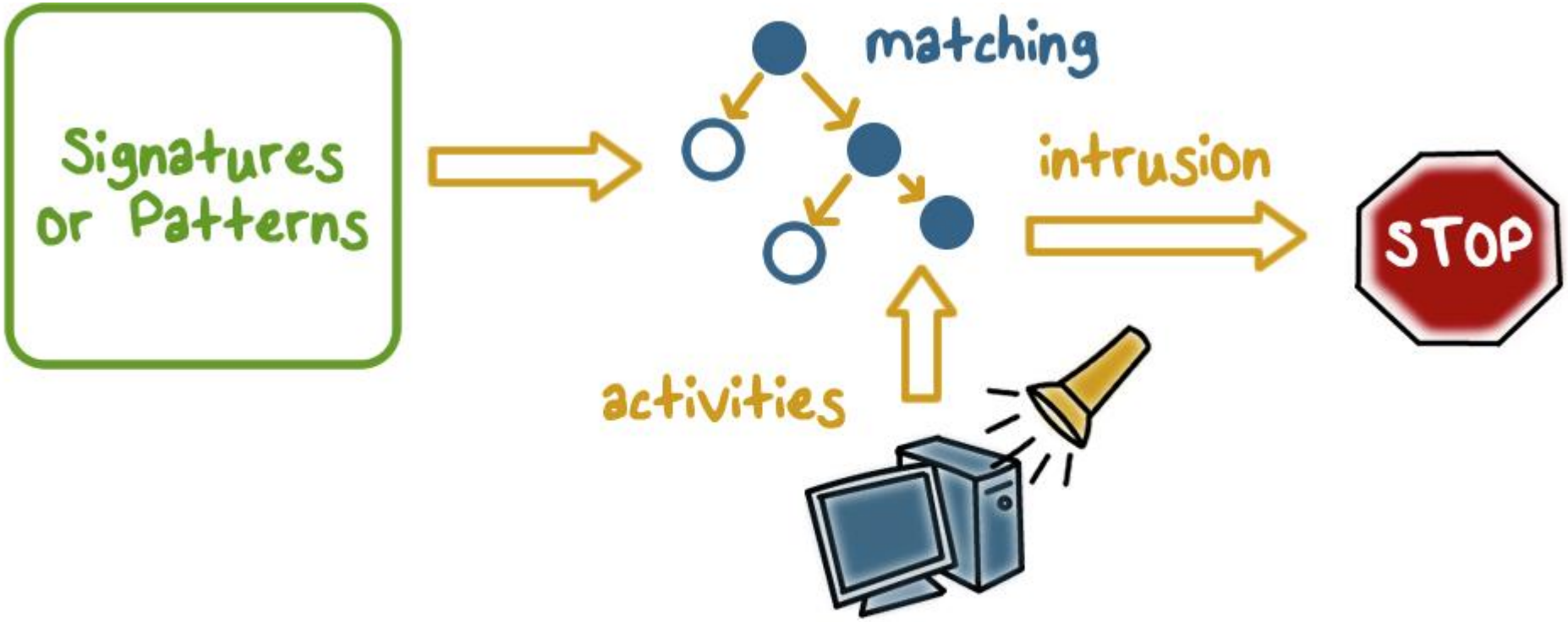
In the thriving zero day attack marketplace hackers sell information on software vulnerabilities. **Can you guess some of the buyers**?

- [ ] Apple
- [ ] Google
- [ ] Microsoft
- [ ] U.S. Government

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”

Can’t detect new attacks

Attacks Quiz

Write the name of each attack next to it's definition. The choices are **Scanning Attack (S), DOS(D)**, and **Penetration Attack(P)**.

☐ an attacker sends various kinds of packets to probe a system or network for vulnerability that can be exploited

☐ attempts to slow down or completely shut down a target so as to disrupt the service for legitimate users

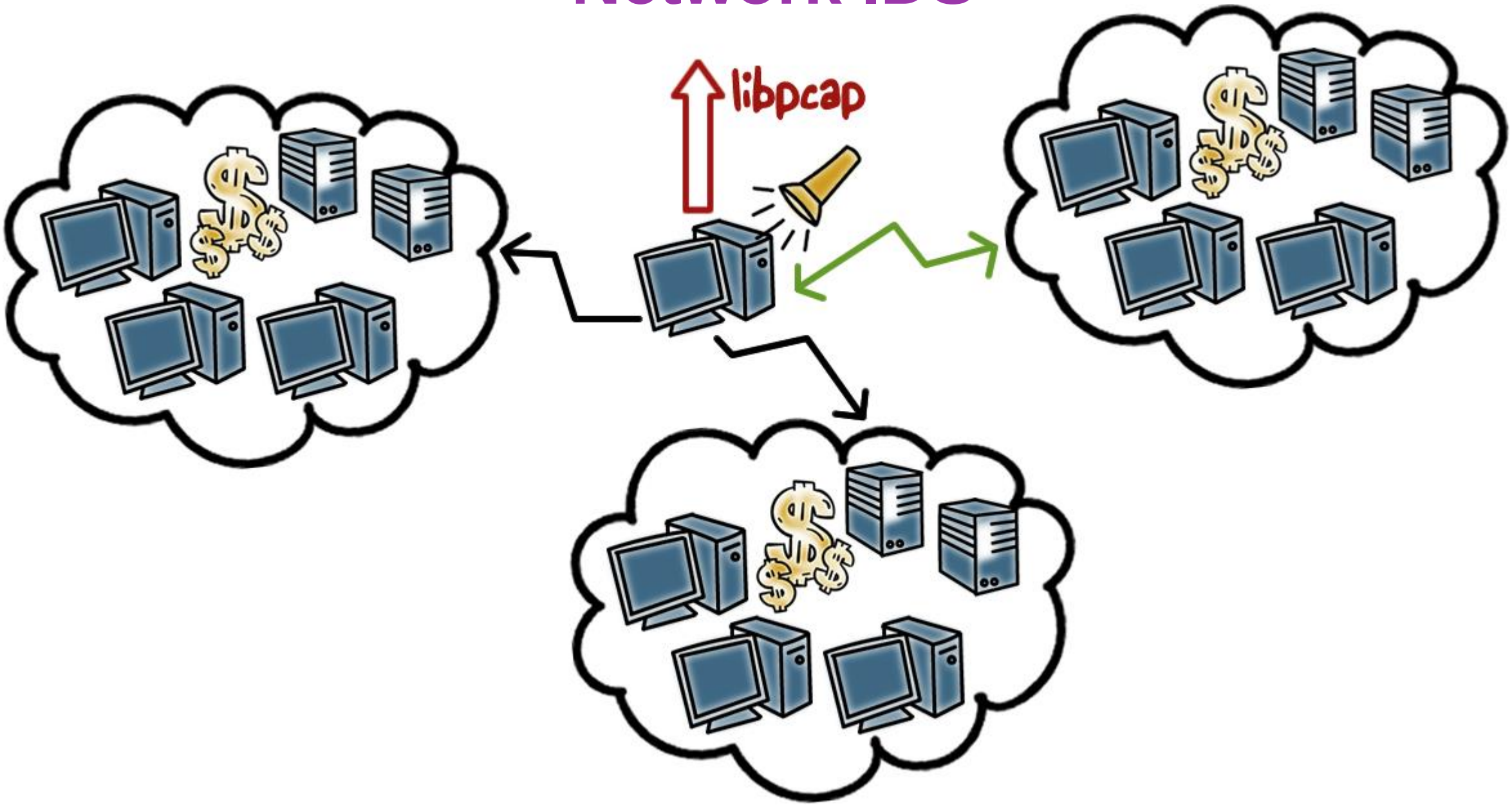
☐ an attacker gains an unauthorized control of a system

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**

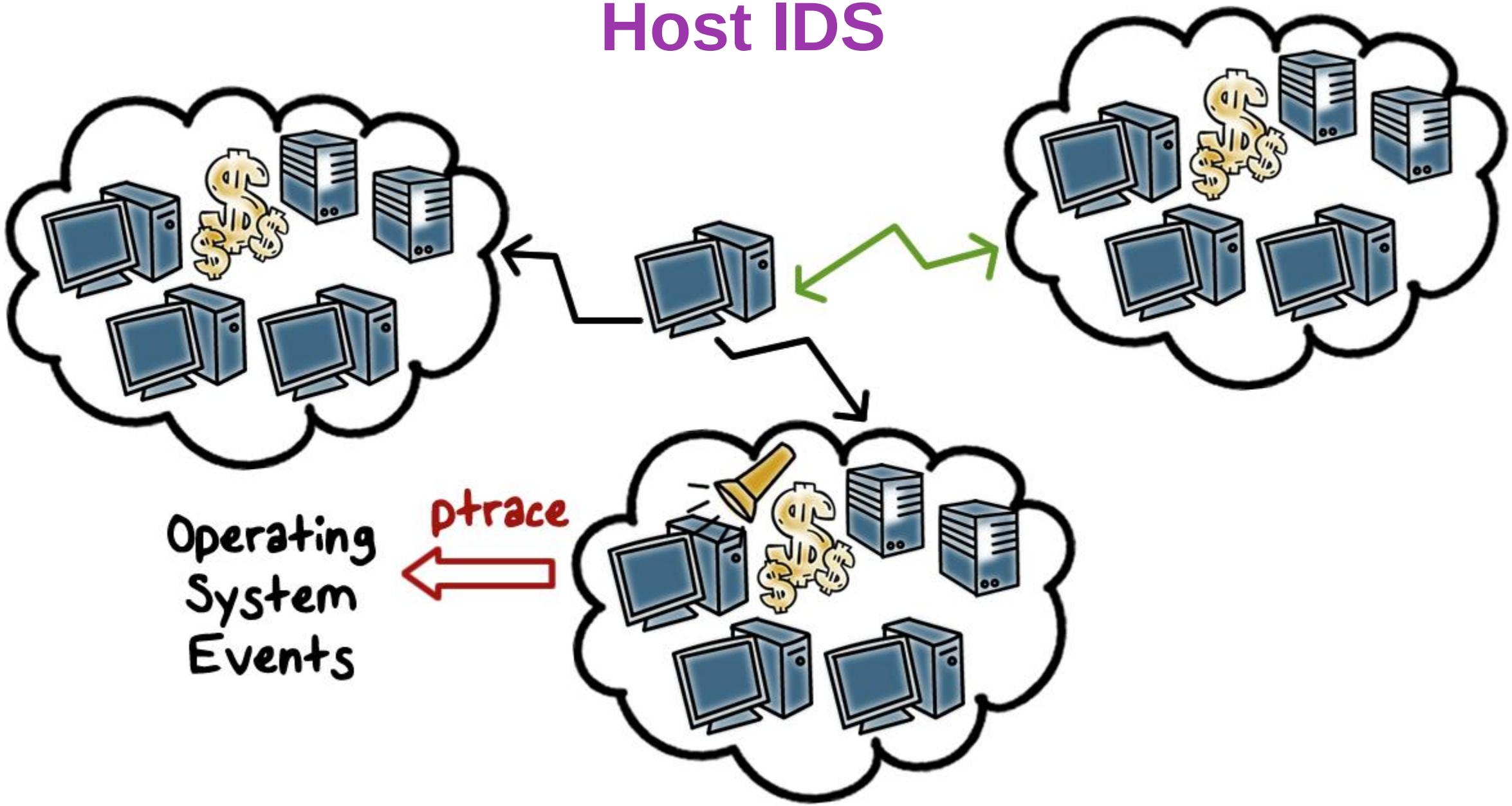
Network IDS



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

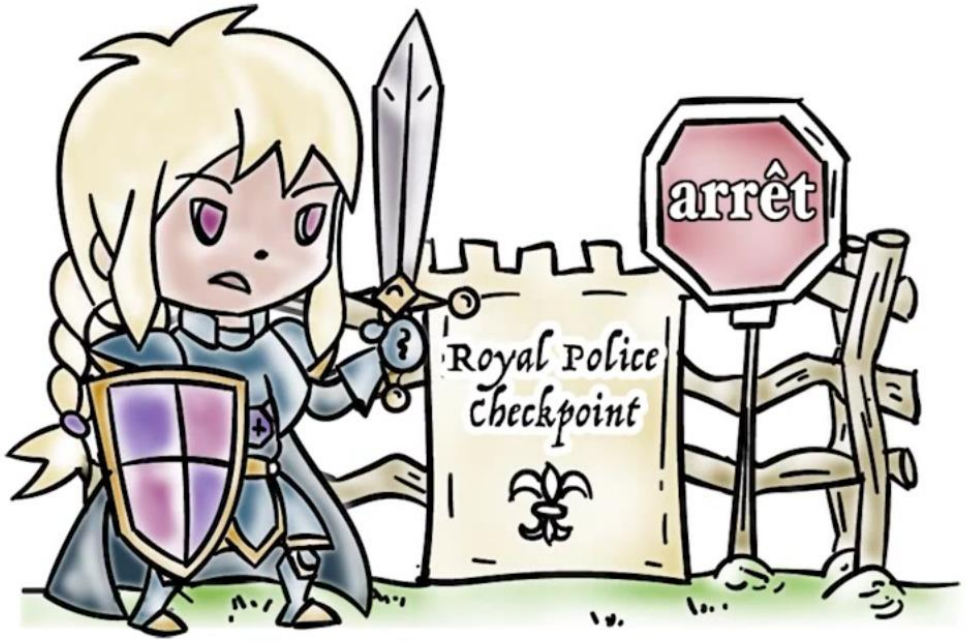


NIDS QUIZ

Can you think of a way to reduce the impact of excessive reporting on a system's administrator?

Write your answer in the textbox:

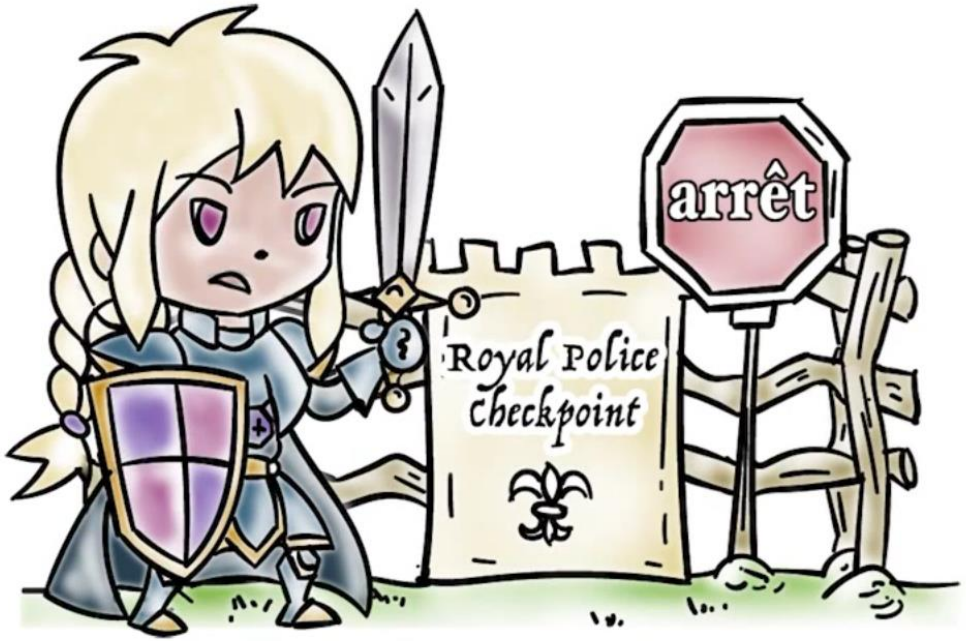
Inline Sensors



- Used to block an attack when one is detected, **performing both intrusion detection and prevention functions**
- An inline sensor is inserted into a network segment so that the **traffic that it is monitoring must pass through the sensor**.

Inline Sensors

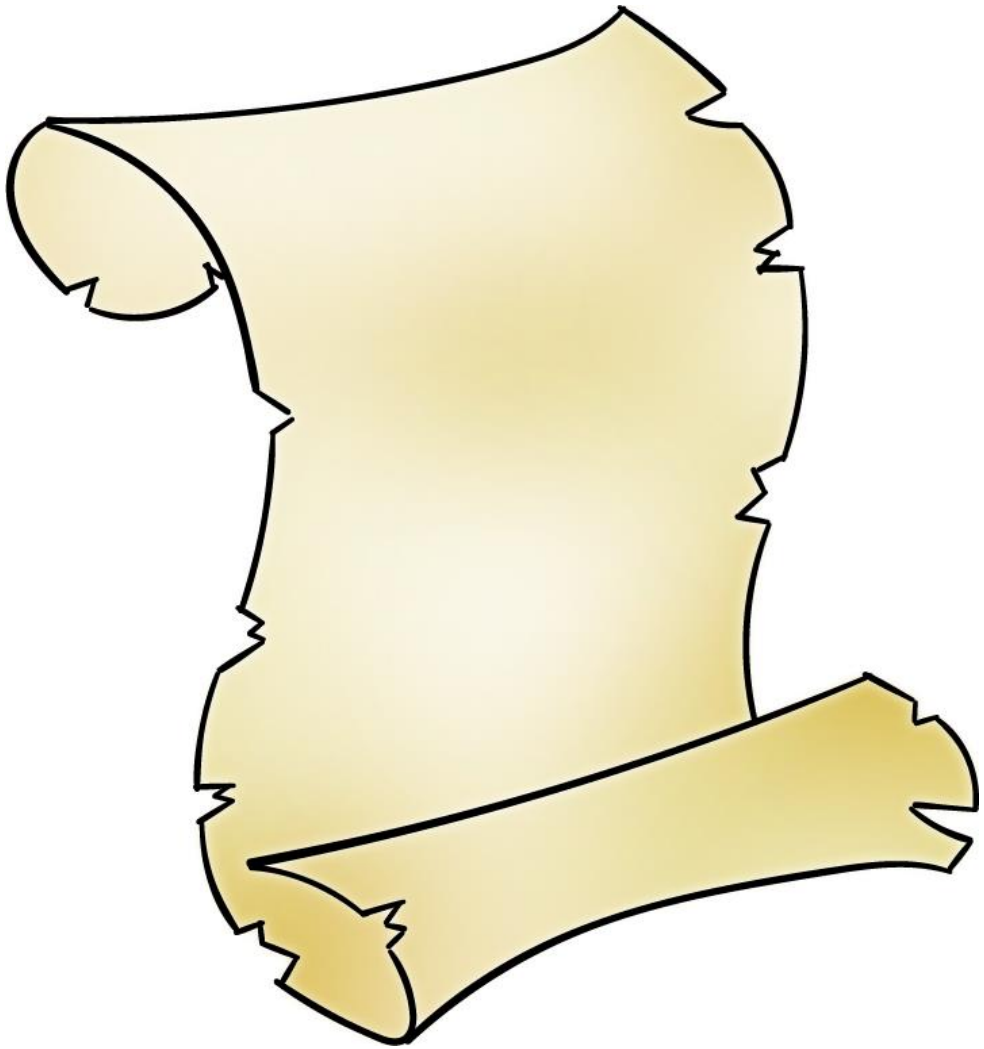
Can be achieved by:



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

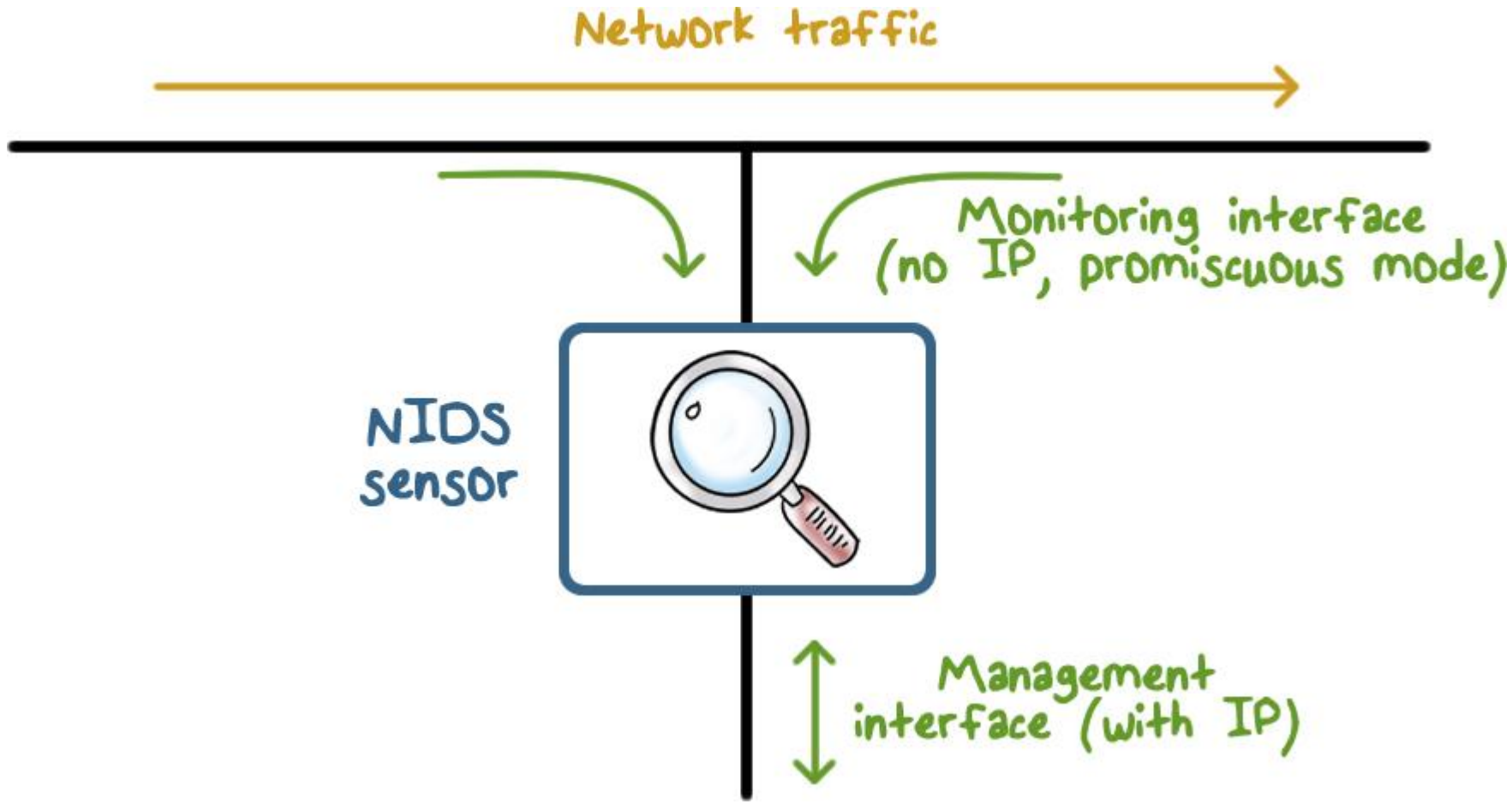
- Using a **stand-alone inline NIDS sensor**

Passive Sensors

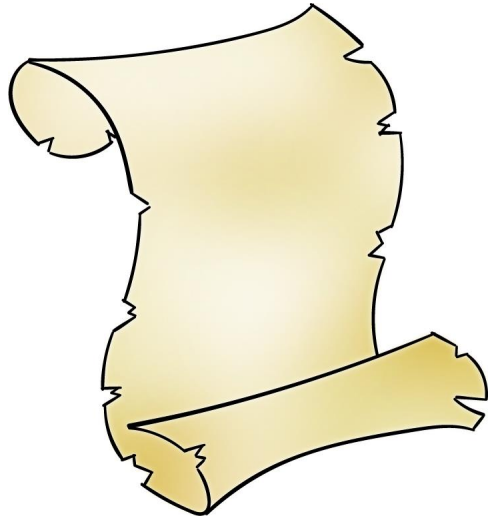


- A passive sensor **monitors a copy of network traffic**; the actual traffic does not pass through the device
- Passive sensors are more efficient

Passive Sensors



Firewall Versus Network IDS



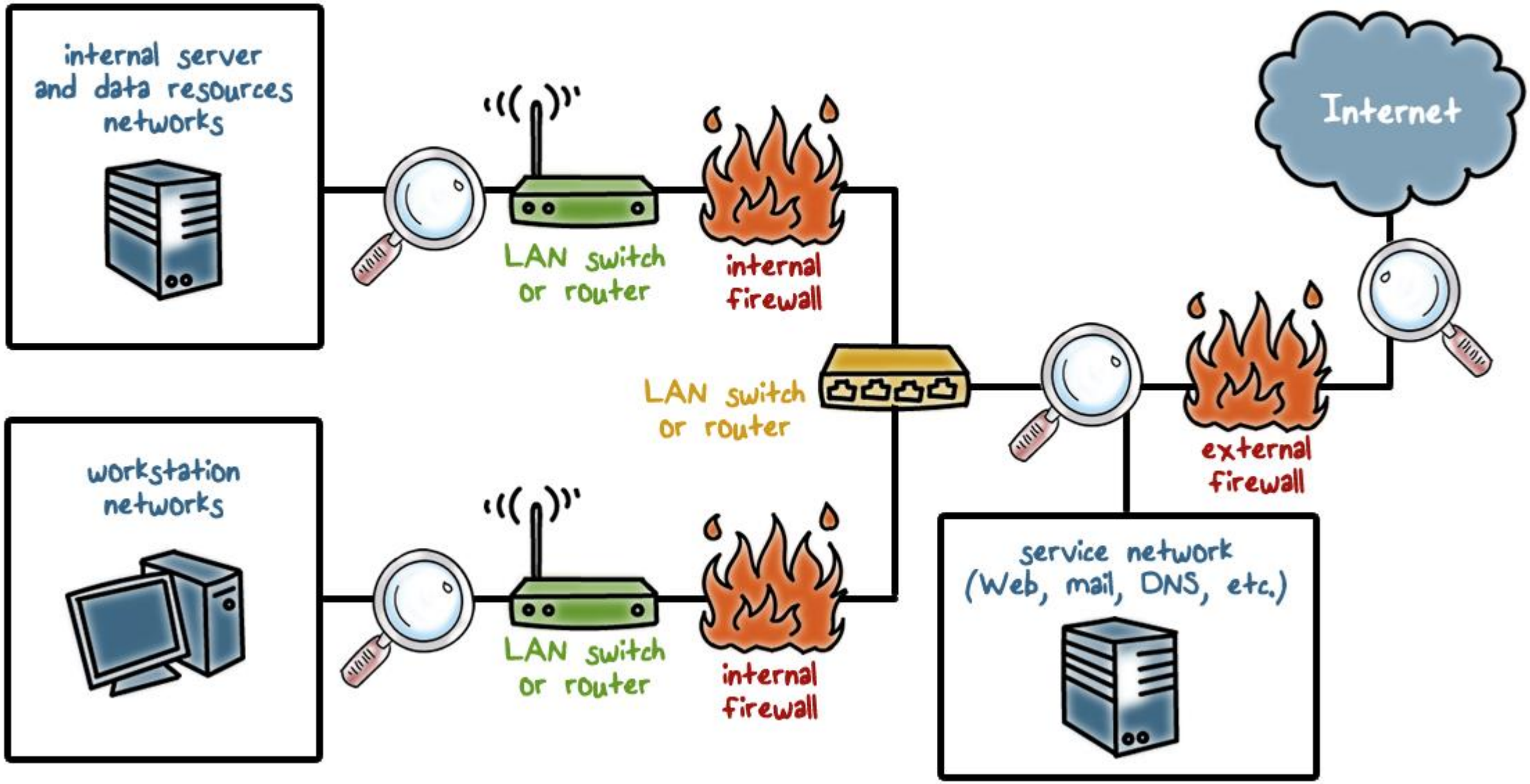
- **Firewall**
  - Active filtering
  - Fail-close
- **Network IDS**
  - Passive monitoring
  - Fail-open

IDS Quiz

Put a **(T) for True** next to each true statement and a **(F) for False** next to each false statement.

- ☐ Intrusion detection is based on the assumption that the behavior of the intruder differs from that of a legitimate user in ways that can be quantified.
- ☐ The primary purpose of an IDS is to detect intrusions, log suspicious events, and send alerts.
- ☐ Signature-based approaches attempt to define normal, or expected, behavior, whereas anomaly approaches attempt to define proper behavior.
- ☐ An network IDS sensor monitors a copy of network traffic; the actual traffic does not pass through the device.
- ☐ Network-based intrusion detection makes use of signature detection and anomaly detection.

NIDS Sensor Deployment



NIDS Sensor Deployment Quiz

When using sensors which of the following is considered good practice? Check all the **true** statements:

- ☐ Set the IDS level to the highest sensitivity to detect every attack
- ☐ Monitor both outbound and inbound traffic
- ☐ Use a shared network resource to gather NIDS data
- ☐ NIDS sensors are turnkey solutions, system administrators can interpret alerts.

SNORT

- Open source
- Highly configurable
- Lightweight IDS

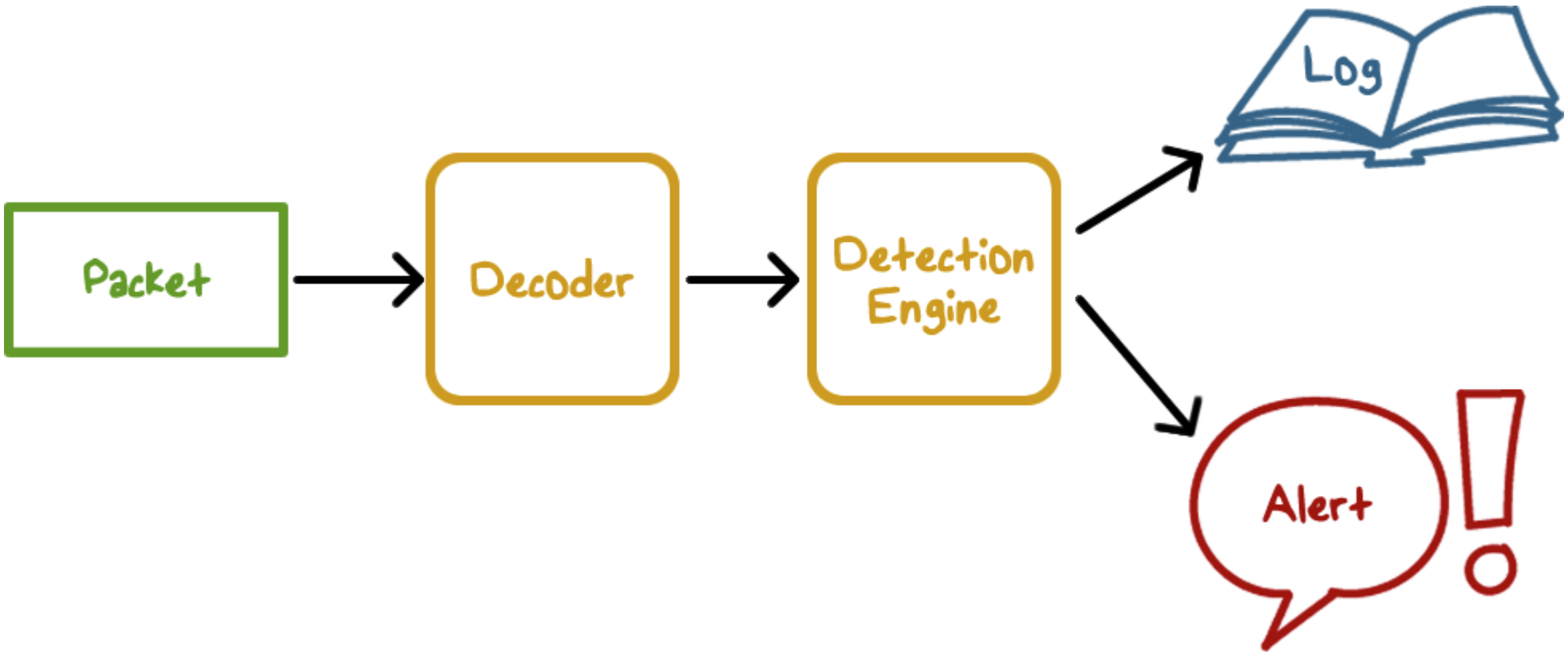
SNORT

- Characteristics:
  - Easily deployed on most nodes
  - Efficient operation
  - Easily configured by system administrators

- Performs real-time packet capture
- Detects a variety of attacks and probes

SNORT

Consists of Four Logical Components



SNORT Configuration

Configured as passive

- Monitors traffic
- Is not in the main transmission path
- Is not an inline sensor

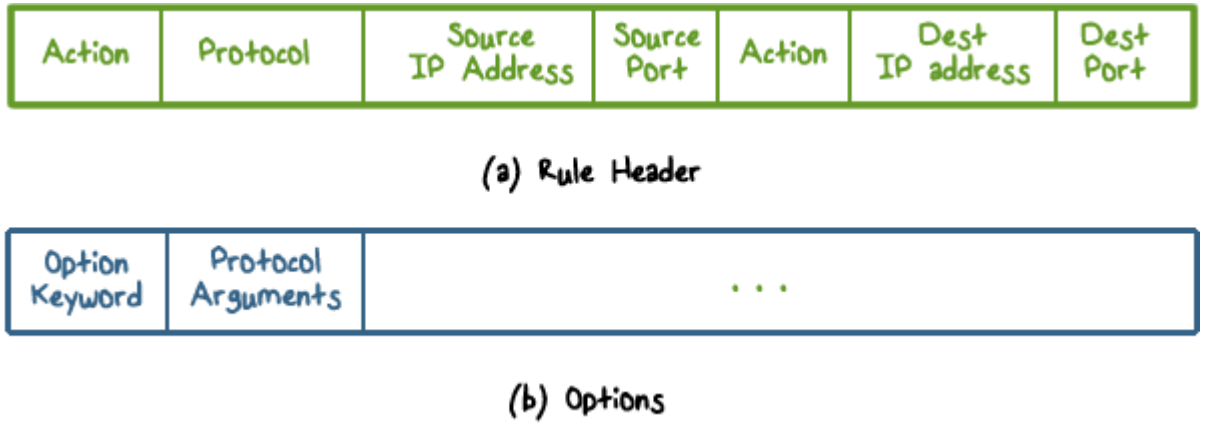
Configured as Intrusion Detection

Snort Rules

(a) Rule Header

(b) Options

Snort Rule Options



- **Meta-data**: provides information about the rule but do not have any effect during detection

- **Payload:** look for data inside the packet
- **Non-payload**: Look for non-payload data
- **Post-detection**: rule-specific triggers that happen after a rule has matched a packet

Snort Rule Actions

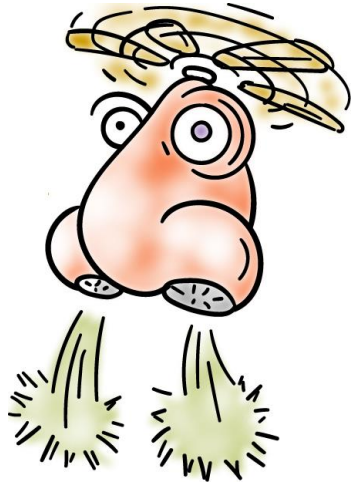
Action	Description	Inline Mode Only
alert	Generate an alert using the selected alert method, and then log the packet.	
log	Log the packet.	
pass	Ignore the packet.	
activate	Alert and then turn on another dynamic rule.	
dynamic	Remain idle until activated by an activate rule, then act as a log rule.	
drop	Make iptables drop the packet and log the packet.	X
reject	Make iptables drop the packet, log it, and then send a TCP reset if the protocol is TCP or an ICMP port unreachable message if the protocol is UDP.	X
sdrop	Make iptables drop the packet but does not log it.	X

Snort Rule Actions

(a) Rule Header

(b) Options

Snort Rule Example:

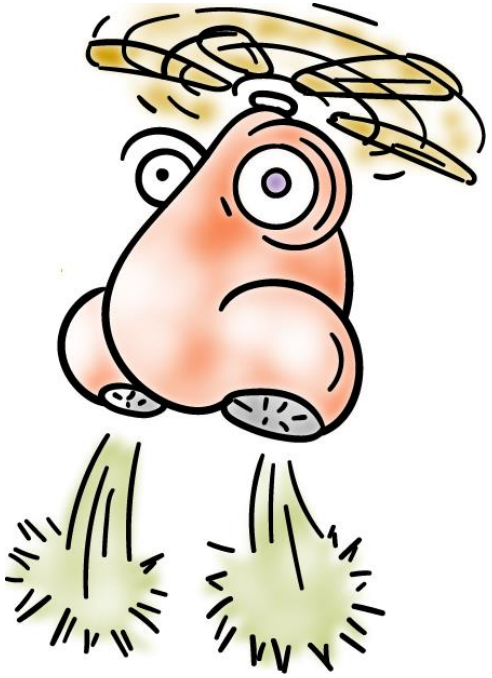


alert tcp any any -> 192.168.1.0/24 25

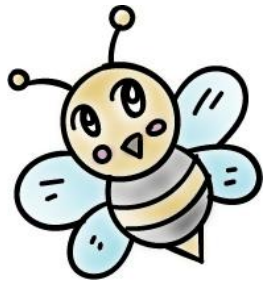
(content: “mail from: root”; msg: “root users attempts to send an email”;)

SNORT Quiz

Check all those **who can write rules** for SNORT:



- ☐ Users of SNORT
- ☐ The SNORT Community
- ☐ Talos Security Intelligence and Research Team

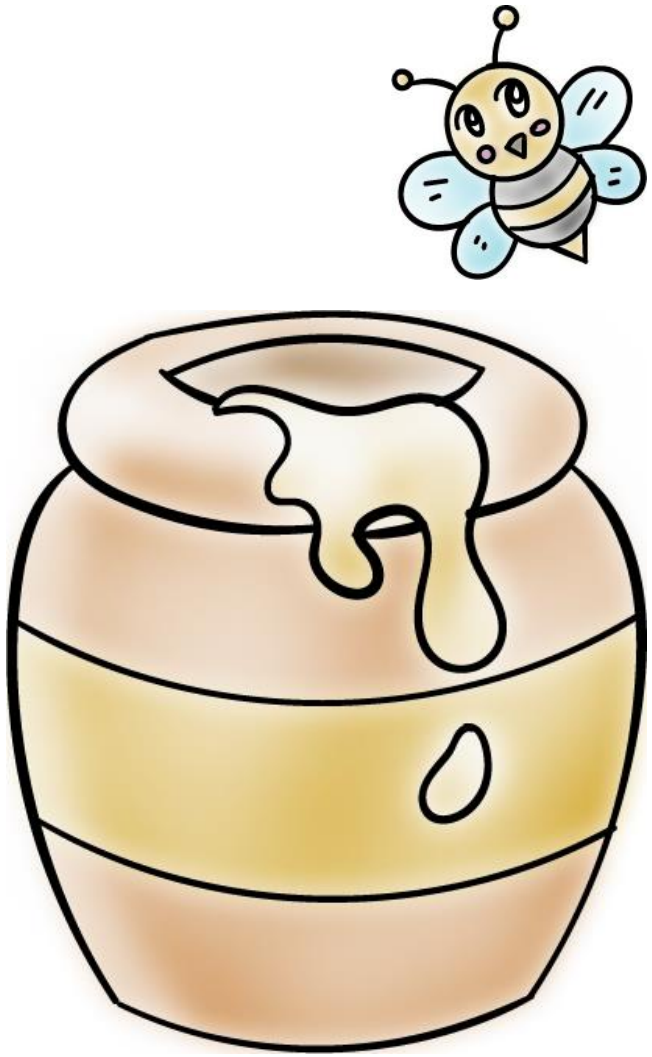


Honeypots

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



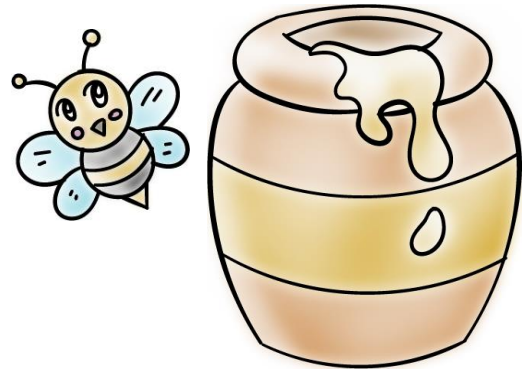
Honeypots

- 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

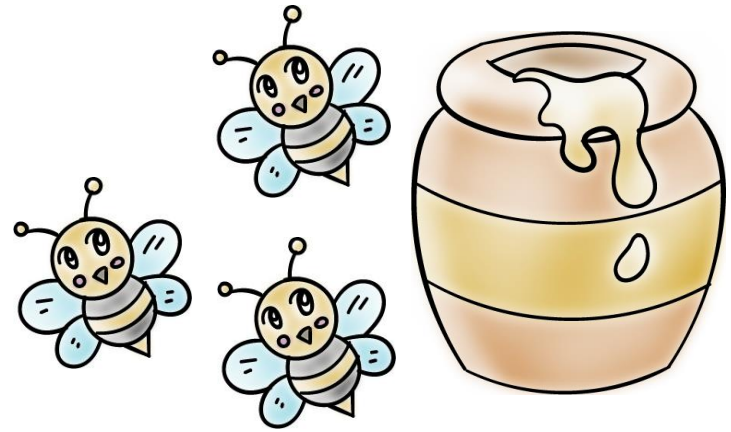
- A honeypot has **no production value**
- There is **no legitimate reason to access** a honeypot
- Any attempt to communicate with a honeypot is **most likely a probe, scan, or attack**
- If a honeypot **initiates outbound traffic**, the system is most likely compromised

Honeypot Classification



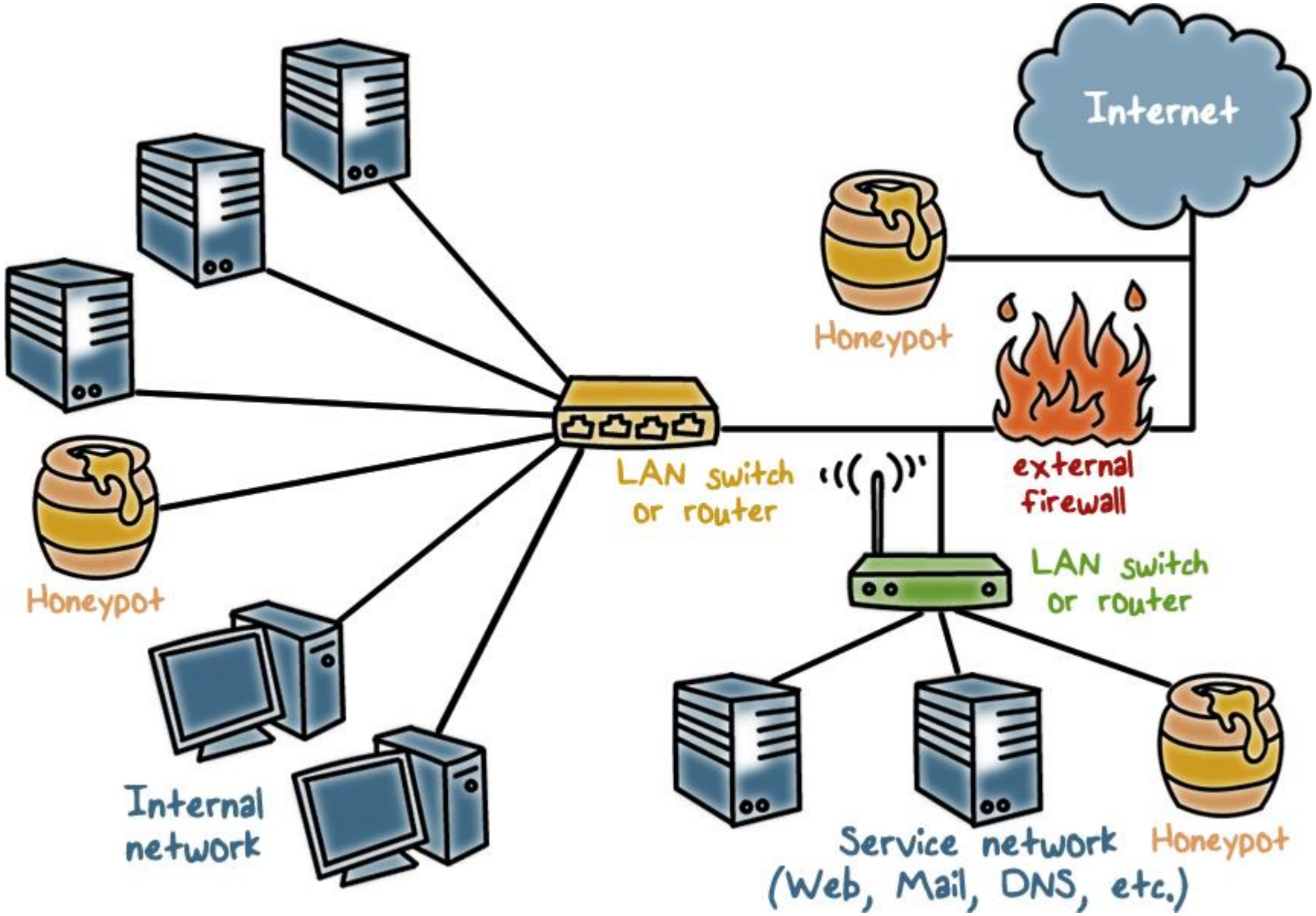
- **Low interaction honeypot:**
  - Emulates particular IT services or systems well enough to provide a realistic initial interaction, but **does not execute a full version** of those services or systems
  - Provides a **less realistic target**
  - Often **sufficient for use as a component** of a distributed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



Honeypot Quiz

Put **True (T)** next to each true statement and **False (F)** next to each false statement.

- ☐ A common location for a NIDS sensor is just inside the external firewall
- ☐ A Honeypot can be a workstation that a users uses for work
- ☐ There is no benefit of deploying a NIDS or Honeypot outside of the external firewall

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?

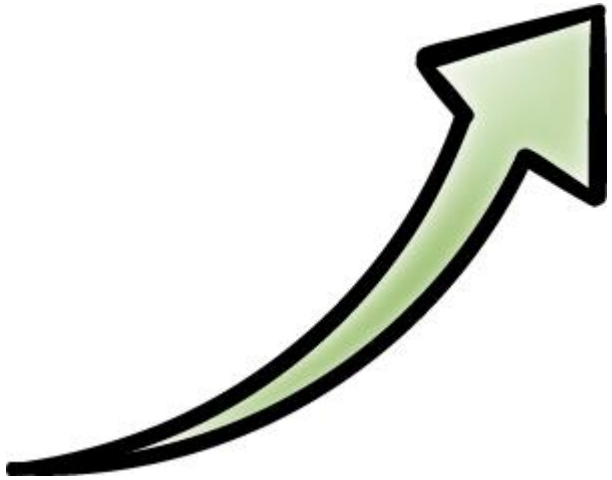
Evaluating IDS

Algorithm

- Alarm/positive: A; Intrusion: I
- Detection (true positive) rate: P(A|I)
  - False negative rate P(¬A|I)
- False alarm rate: P(A|¬I)
  - True negative rate P(¬A|¬I)
- Bayesian detection rate: P(I|A)

Evaluating IDS

System should be:



- Scalable

- Resilient to attacks

Bayesian Detection Rate

$$P(I \mid A) = \frac{P(I)P(A \mid I)}{P(I)P(A \mid I) + P(\neg I)P(A \mid \neg I)}$$

P(I) is prior probability of attacks: this is the probability of intrusion evidences in the data.

Bayesian Detection Rate

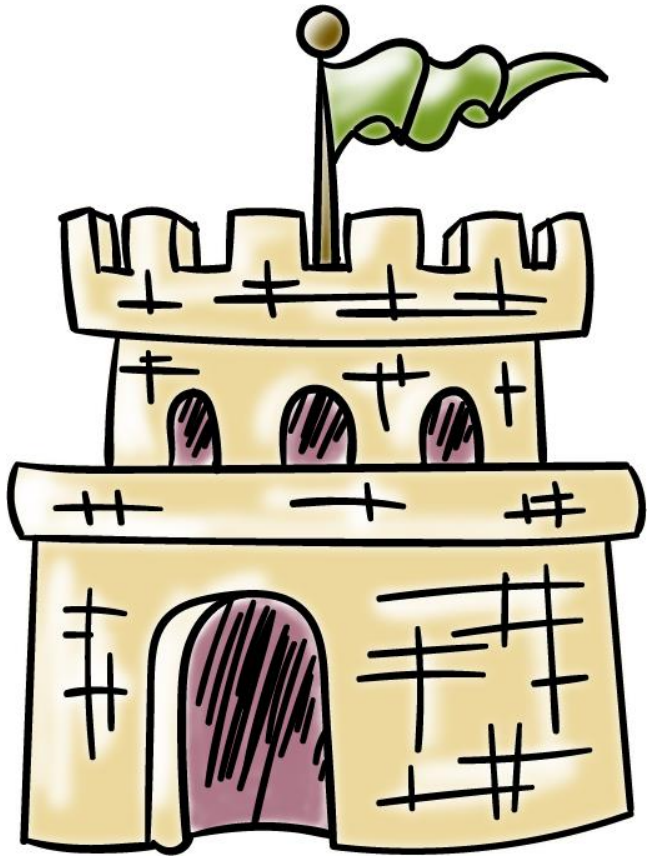
- **P(I) is base rate:** prior probability of attacks
- **Base-rate fallacy**
  - Even if false alarm rate $P(A|\neg I)$ is very low, Bayesian detection rate $P(I|A)$ is still low if base-rate $P(I)$ is low
  - E.g. if $P(A|I) = 1$, $P(A|\neg I) = 10^{-5}$, $P(I) = 2\times10^{-5}$, $P(I|A) =$ 66%

Bayesian Detection Rate

When the IDS produces an alert, the probability that an intrusion has actually occurred is low.

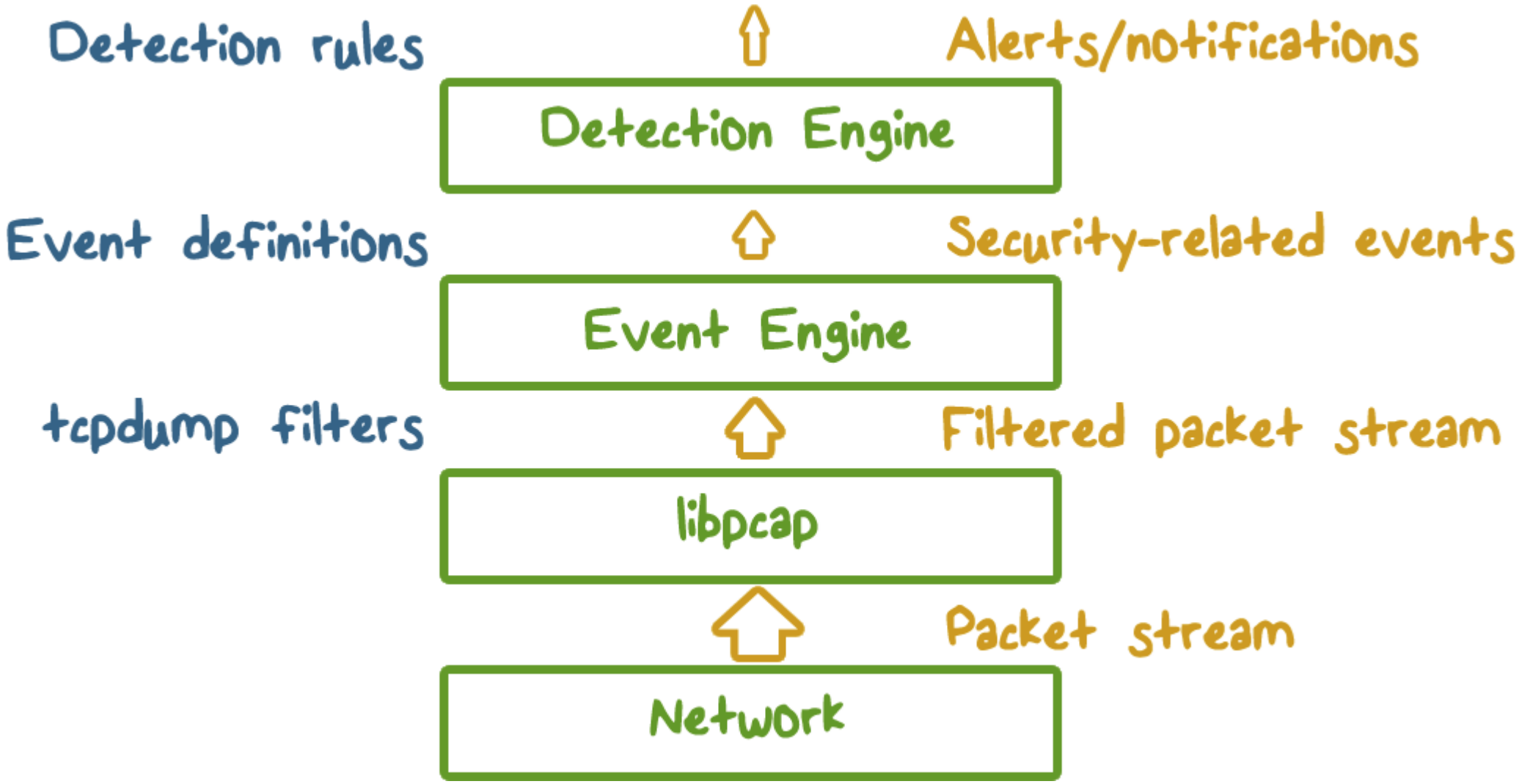
- **Implications to IDS**
  - Design algorithms to reduce false alarm rate
  - Deploy IDS to appropriate point/layer with sufficiently high base rate
  - Multiple independent detection models

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



IDS Quiz

Check any item that is true. **To improve detection performance**, an IDS should:

- ☐ Reduce false alarm rate while detecting as many intrusions as possible
- ☐ Apply detection models at all unfiltered packet data directly
- ☐ Apply detection models at processed event data that has higher base rate

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

Insertion Attack

End-Host sees:

A T T A C K

IDS sees:

A T X T A C K

Attacker's data stream:

T X T C A A K

Examples:
bad checksum,
TTL.

Evasion Attack

End-Host sees:

A T T A C K

IDS sees:

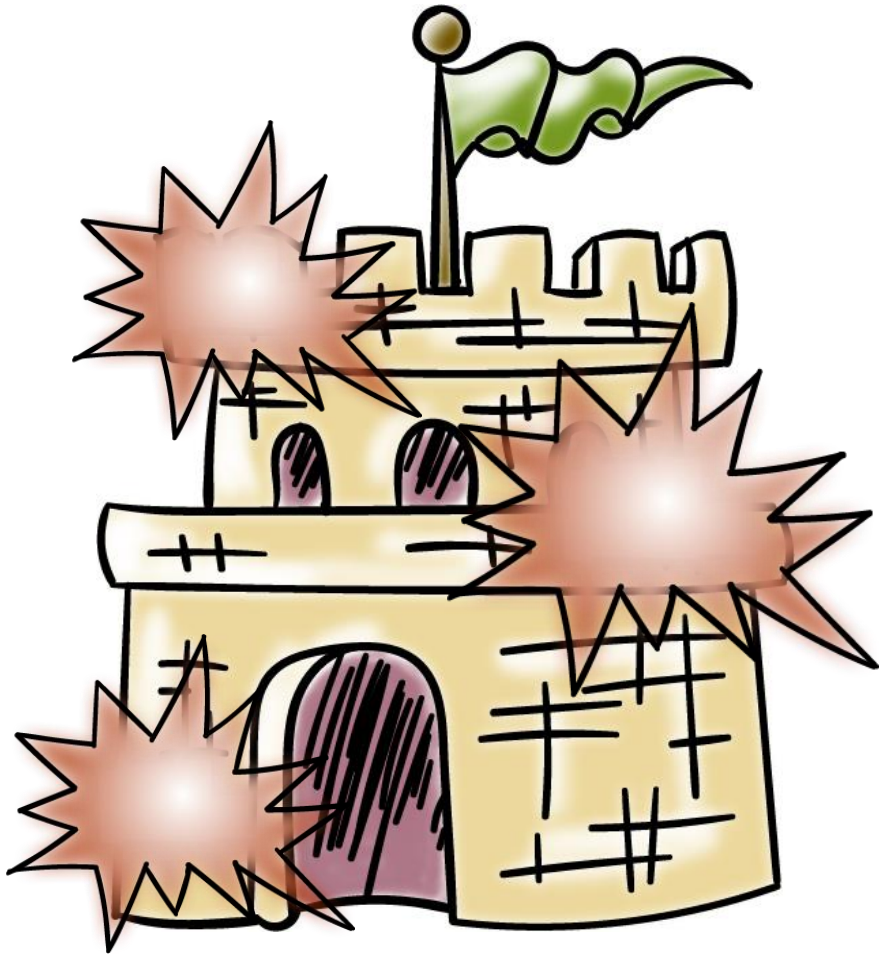
A T T C K

Attacker's data stream:

T T C A A K

Example:
fragmentation
overlap

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

IDS Attack Quiz

Check any item that is true. **To defeat an IDS, attackers can**:

- ☐ Send a huge amount of traffic
- ☐ Embed attack in packets what cause non-uniform processing by different operating systems, e.g., bad checksum, overlapping fragments
- ☐ Send traffic that purposely matches detection rules
- ☐ Send a packet that would trigger a buffer-overload in the IDS code

Intrusion Detection

Lesson Summary

- Anomaly detection and misuse/signature detection
- Network IDS, IPS, and honeypots
- True positive, false positive, and the base-rate fallacy
- Insertion, evasion, and DoS attacks on IDS