Intrusion Detection Systems and Supporting Tools

Ian Welch

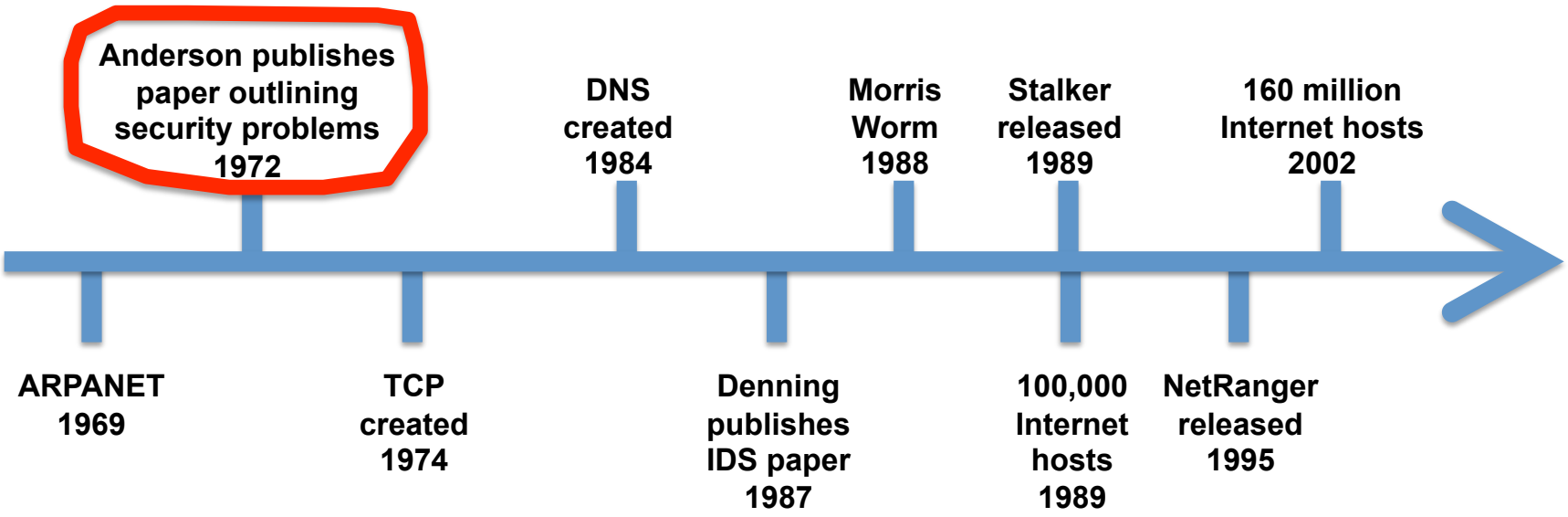
NWEN 405

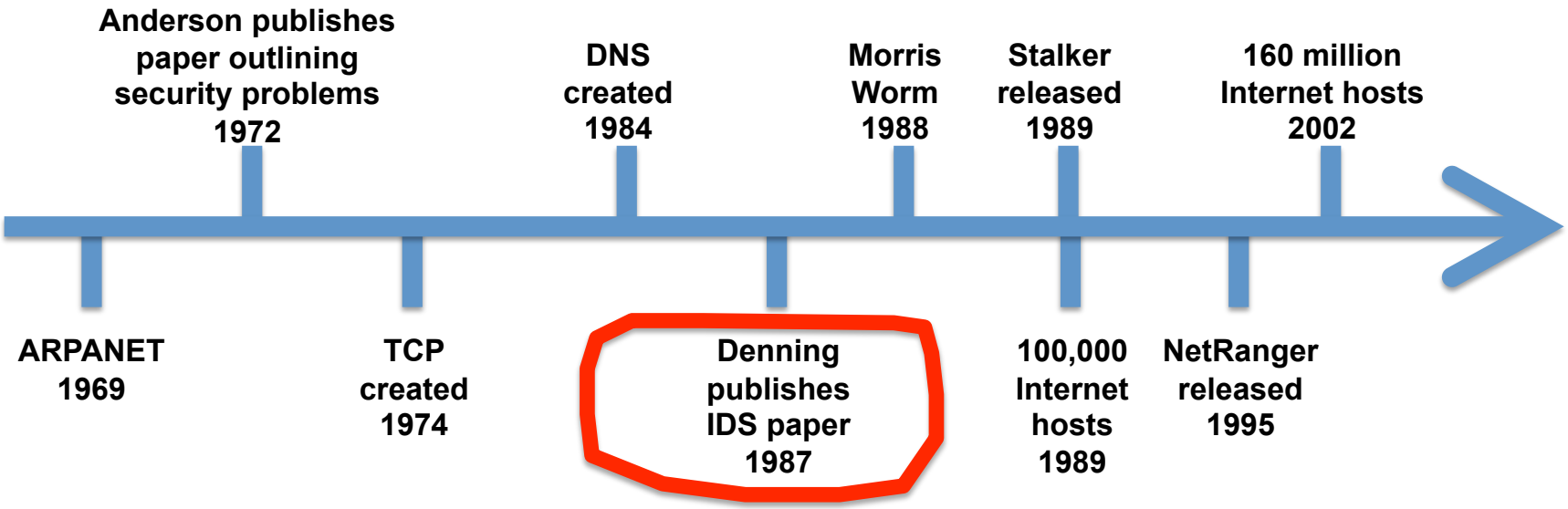
Week 12

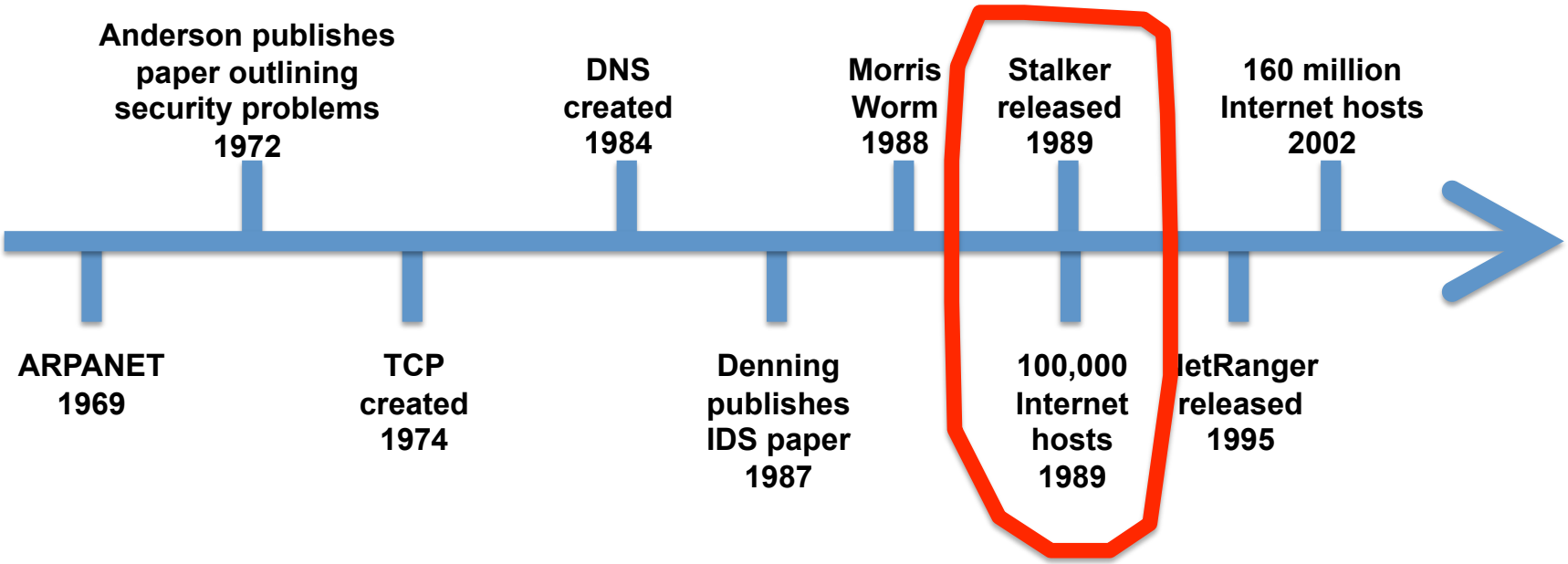
IDS CONCEPTS

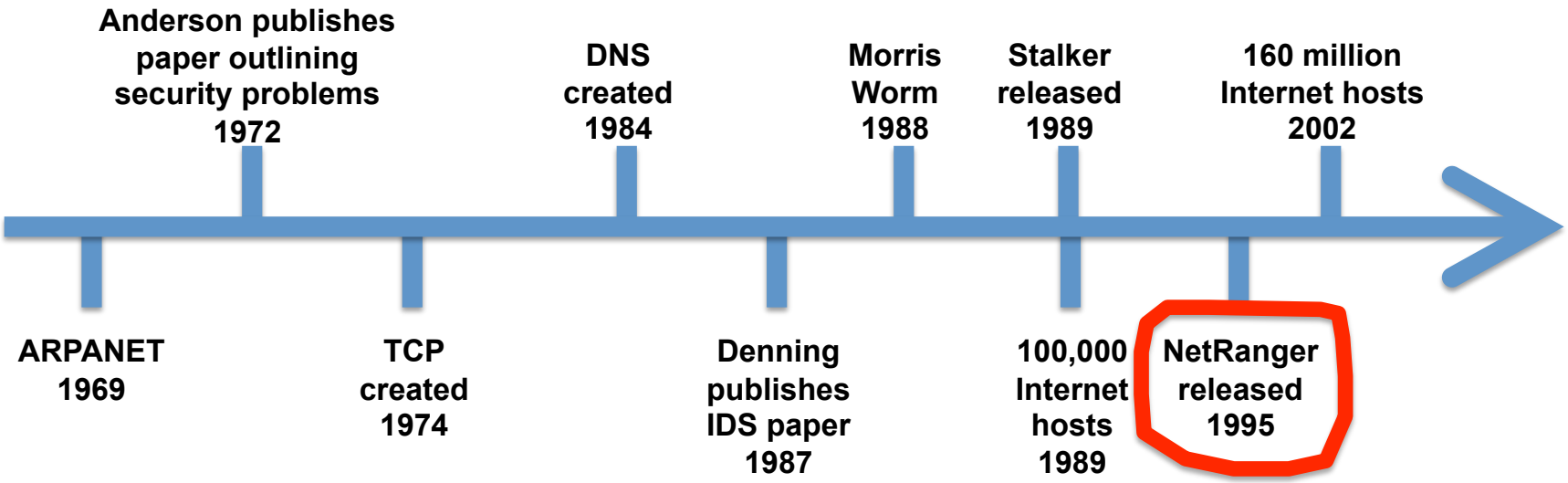
Firewalls.

Intrusion detection systems.


Anderson publishes paper outlining security problems 1972
DNS created 1984
Morris Worm 1988
Stalker released 1989
160 million Internet hosts 2002
ARPANET 1969
TCP created 1974
Denning publishes IDS paper 1987
100,000 Internet hosts 1989
NetRanger released 1995


Anderson publishes paper outlining security problems 1972
DNS created 1984
Morris Worm 1988
Stalker released 1989
160 million Internet hosts 2002
ARPANET 1969
TCP created 1974
Denning publishes IDS paper 1987
100,000 Internet hosts 1989
NetRanger released 1995


Anderson publishes paper outlining security problems 1972
DNS created 1984
Morris Worm 1988
Stalker released 1989
160 million Internet hosts 2002
ARPANET 1969
TCP created 1974
Denning publishes IDS paper 1987
100,000 Internet hosts 1989
letRanger released 1995


Anderson publishes paper outlining security problems 1972
DNS created 1984
Morris Worm 1988
Stalker released 1989
160 million Internet hosts 2002
ARPANET 1969
TCP created 1974
Denning publishes IDS paper 1987
100,000 Internet hosts 1989
NetRanger released 1995

What is an Intrusion?

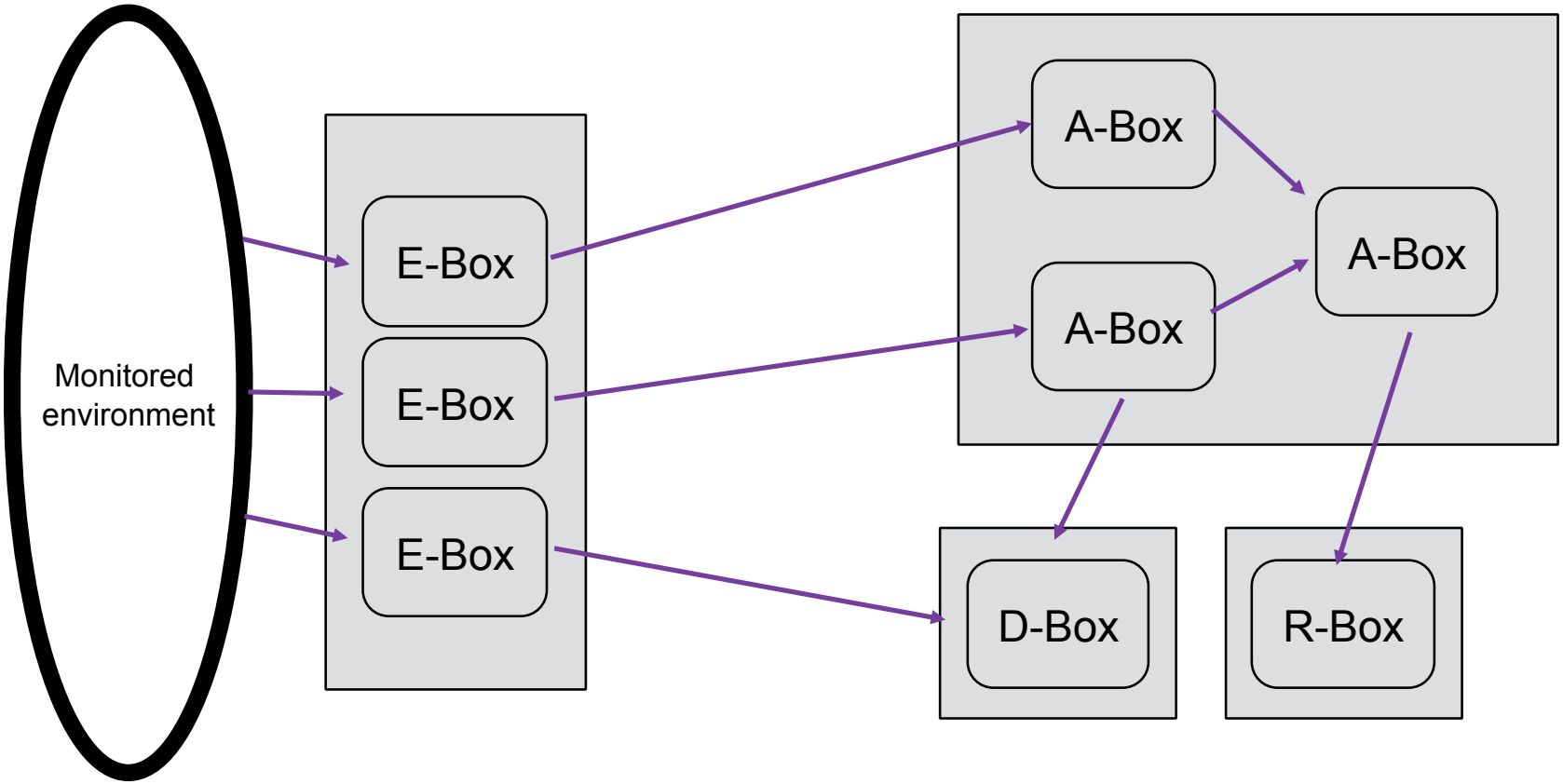
Can happen at any layer of the stack.

Attack. Sequence of related actions by a malicious adversary that results in occurrence of security threats to target computer or network.

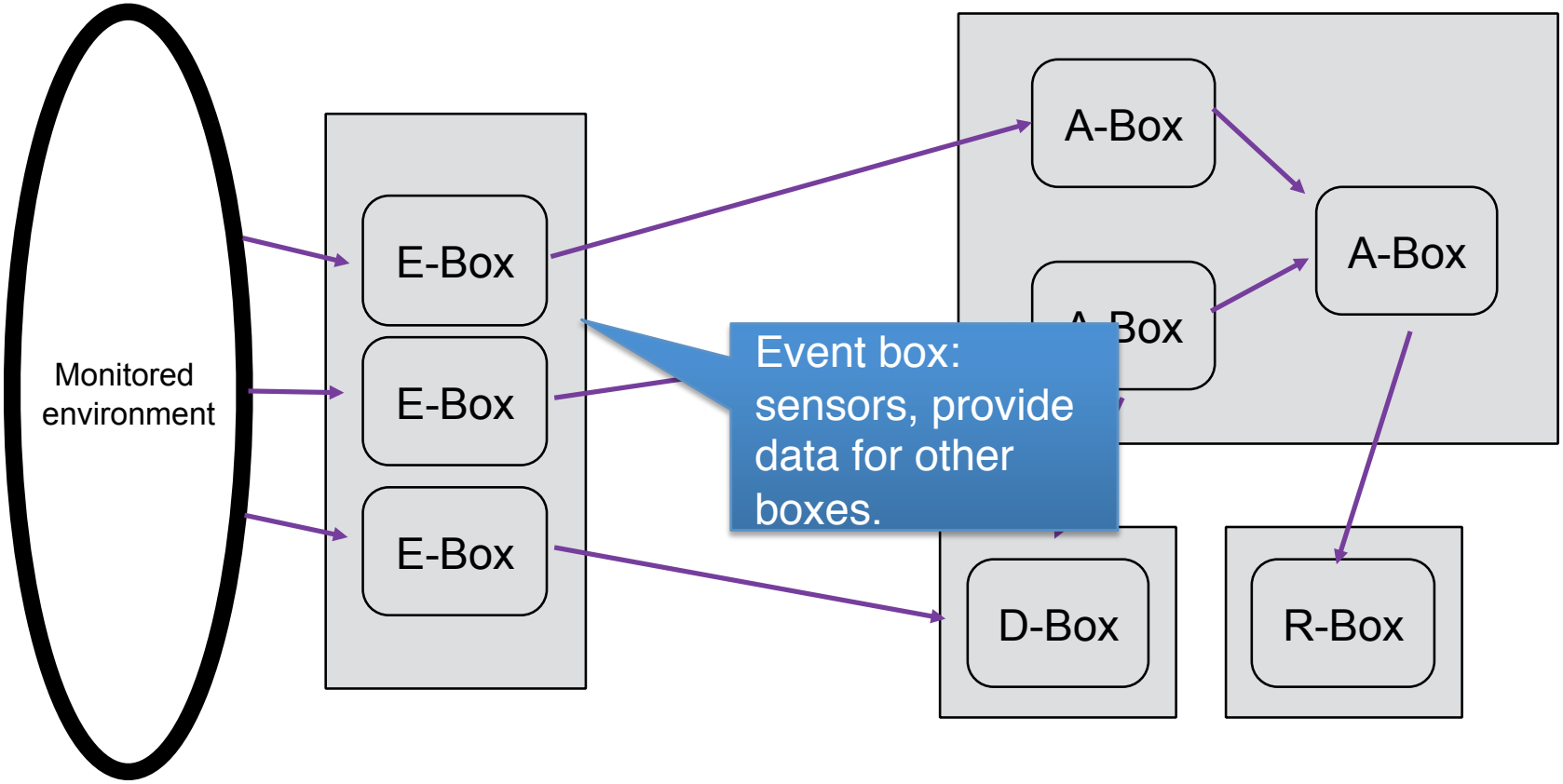
Misuse. Actions that are allowed by the system but violate organisational policies.

Arrived at by monitoring sequences of **system events** at host or network level.

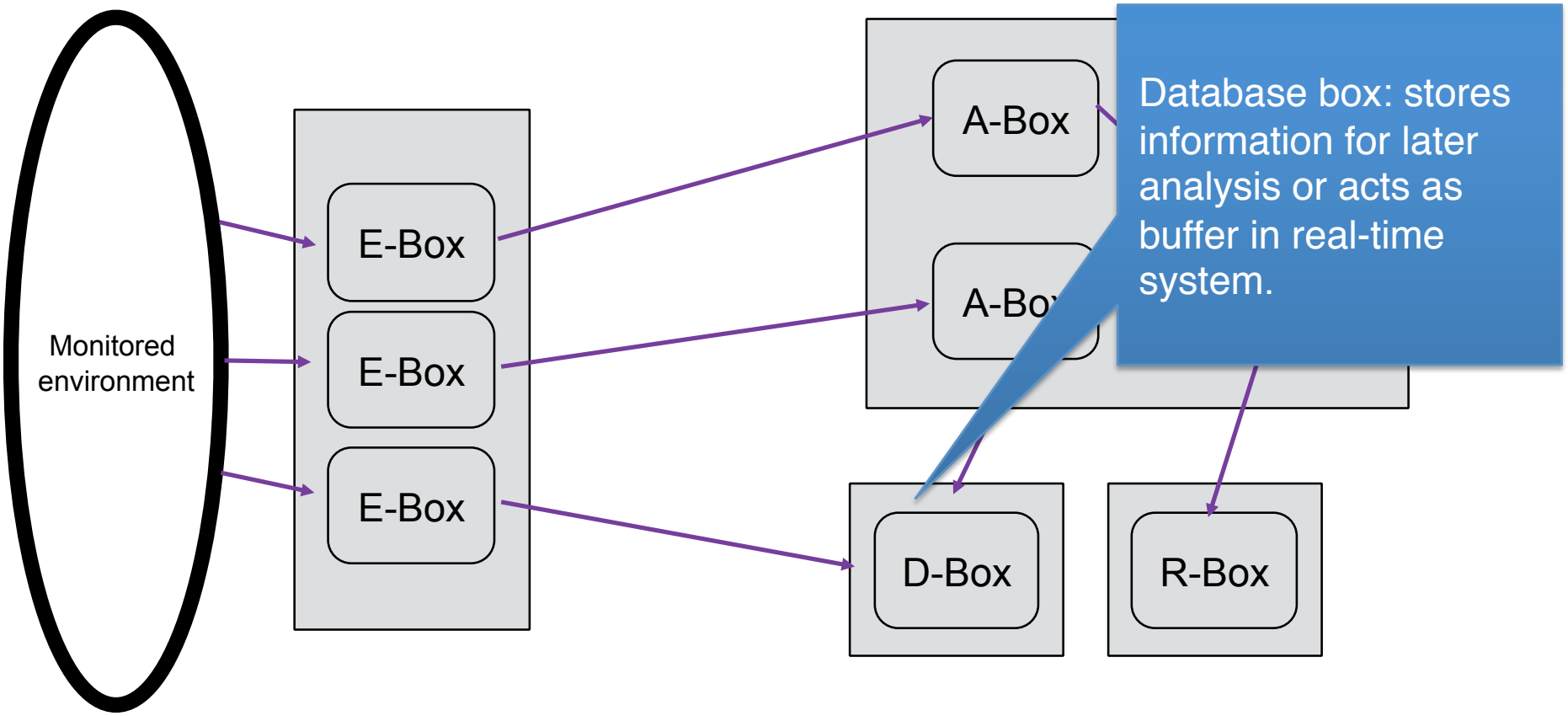
Common Intrusion Detection Framework (1999)



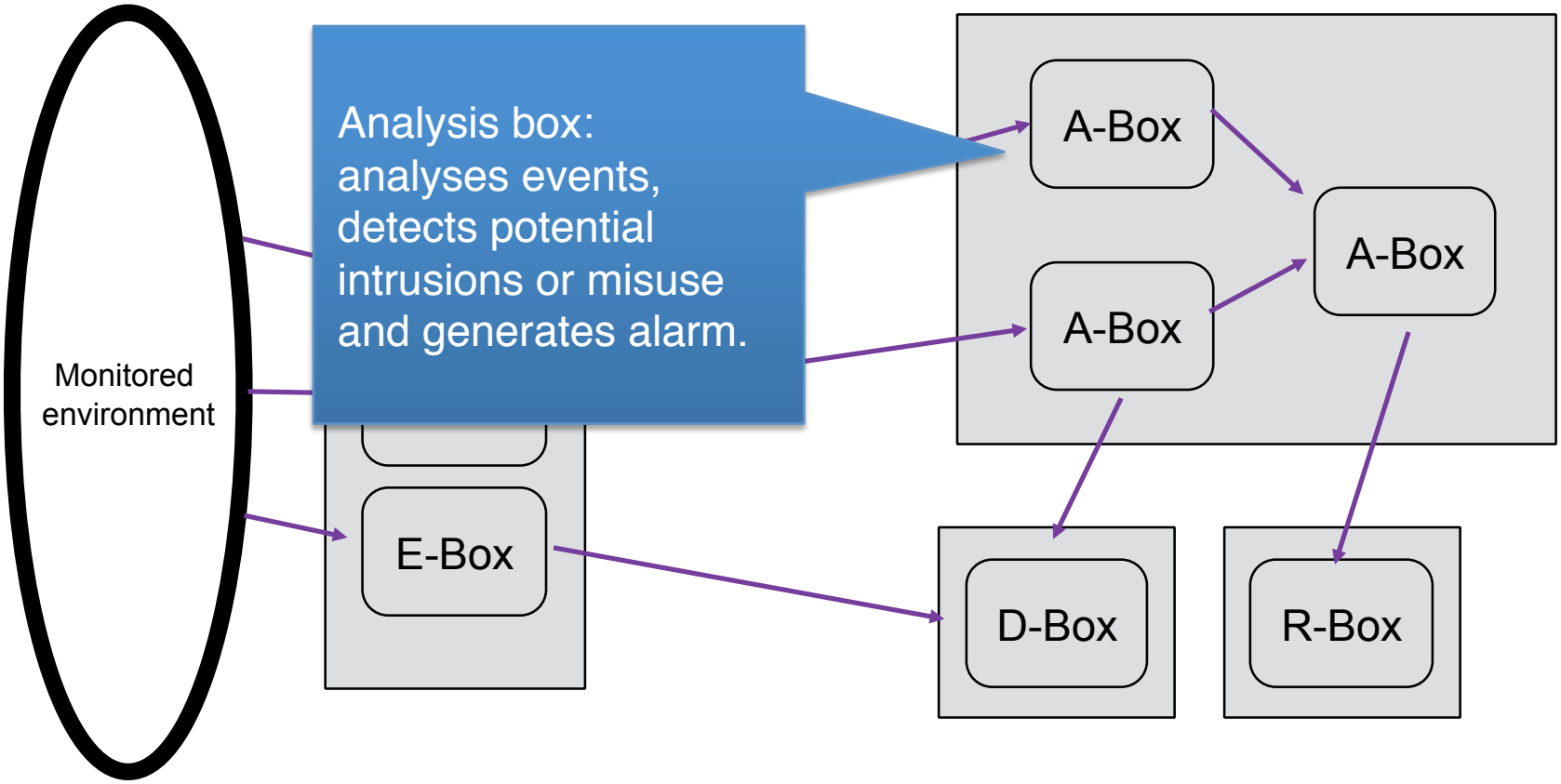
Common Intrusion Detection Framework (1999)



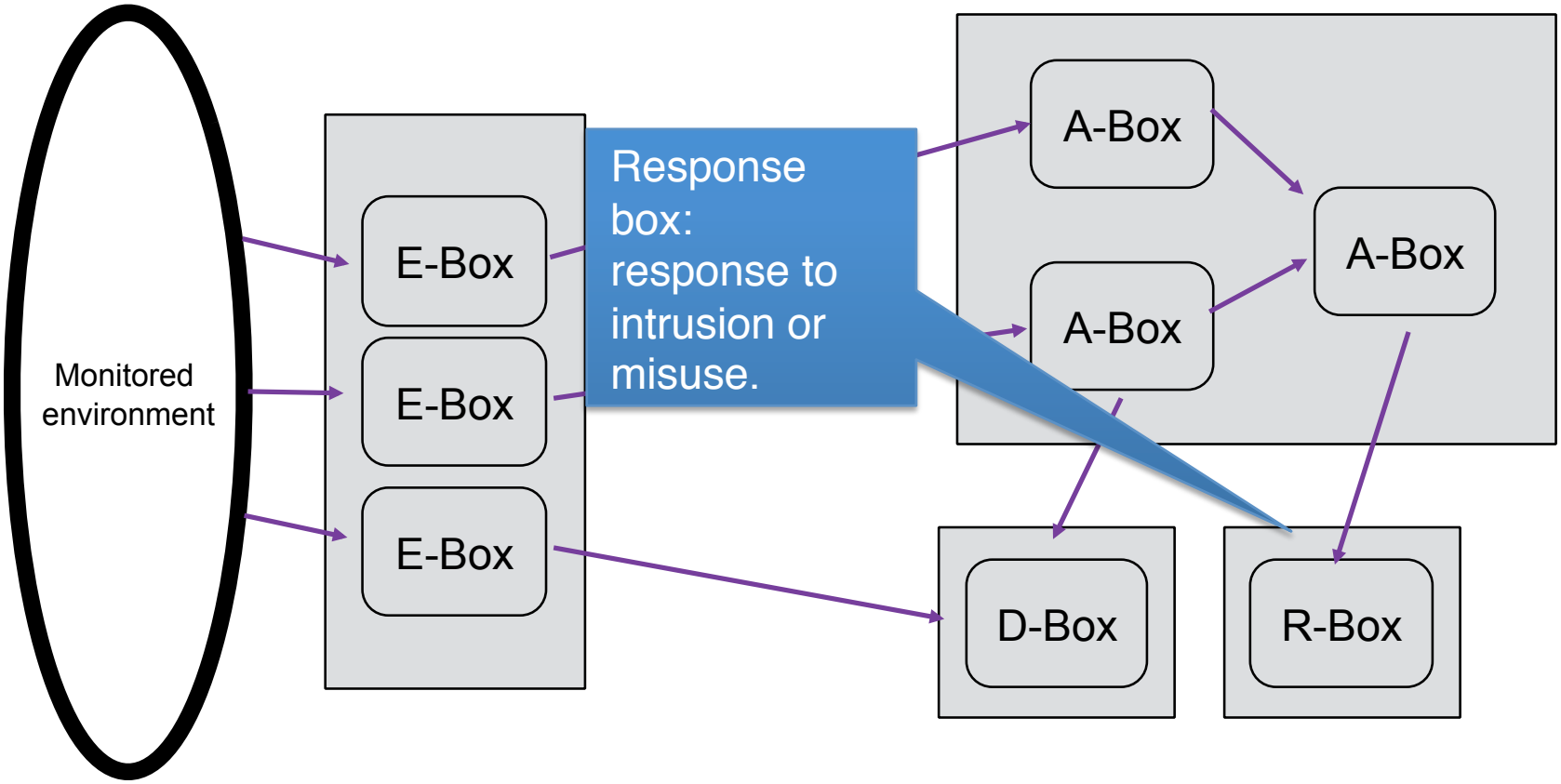
Common Intrusion Detection Framework (1999)



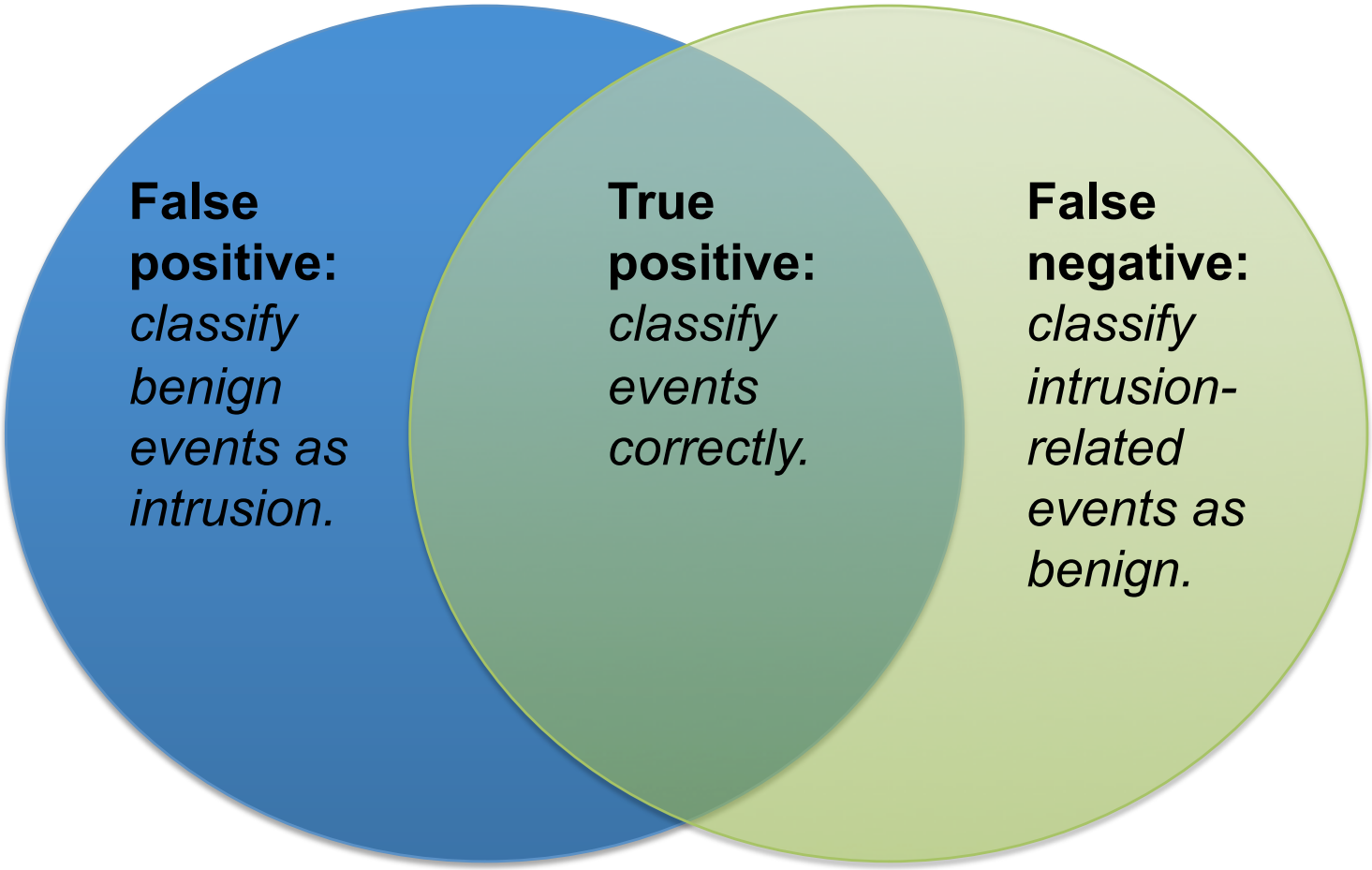
Common Intrusion Detection Framework (1999)



Common Intrusion Detection Framework (1999)

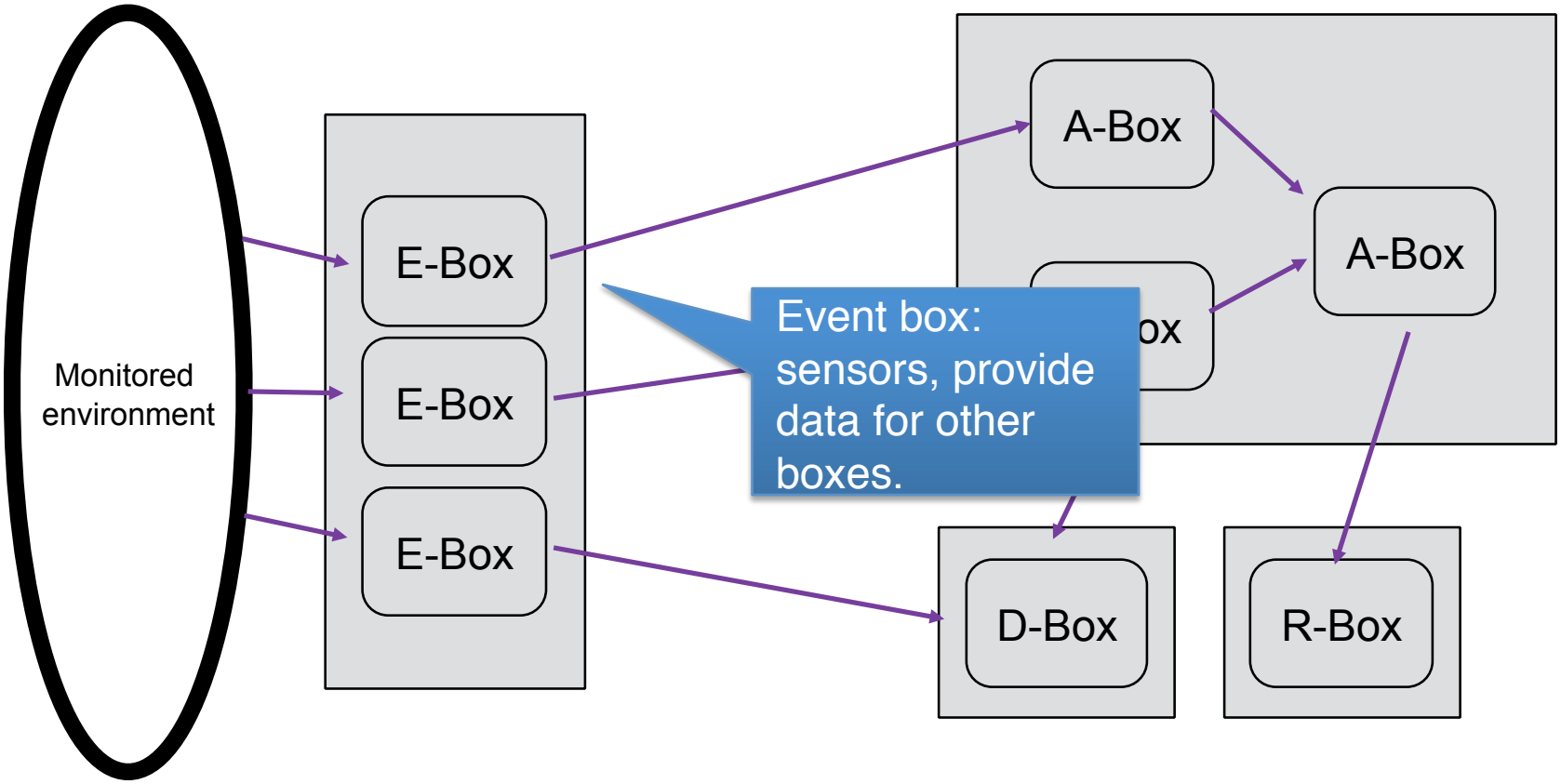


Classification Accuracy



IDS TYPES

Common Intrusion Detection Framework (1999)



Host Based IDS (HIDS)

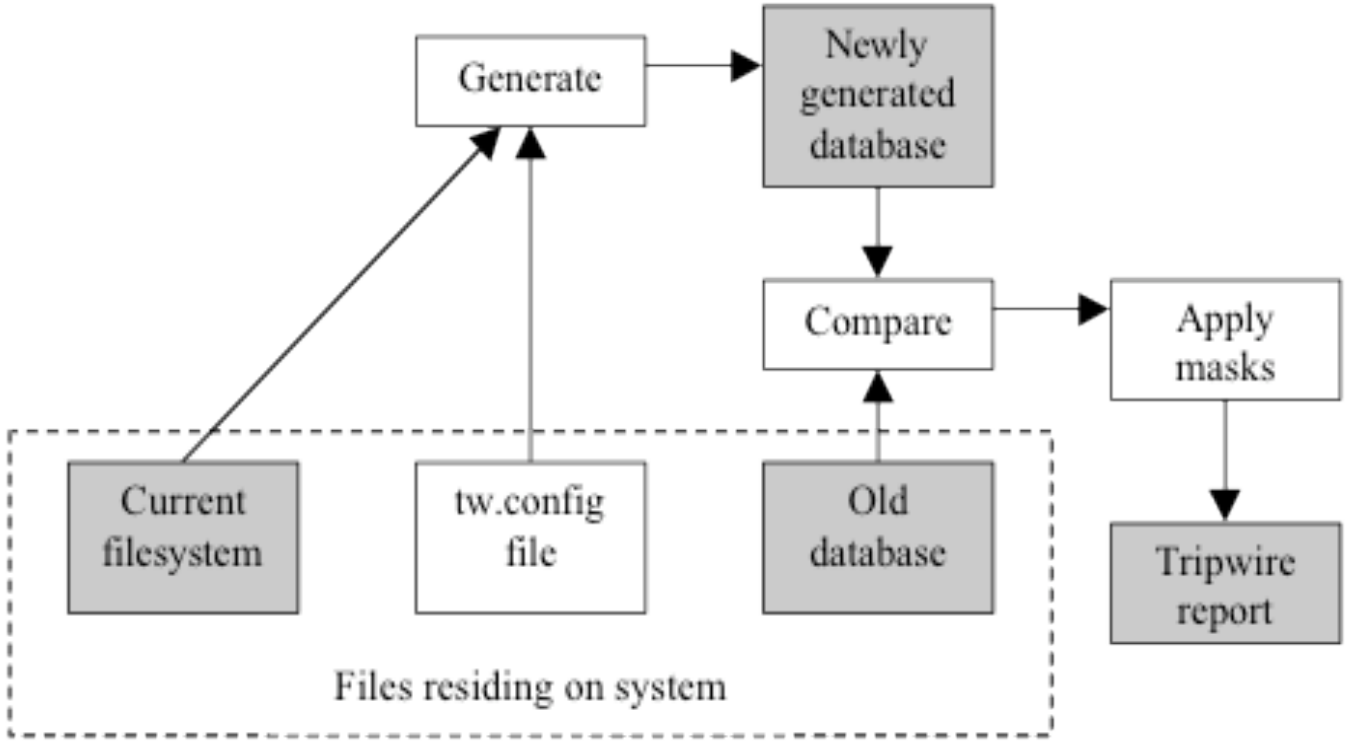
E-box is integrated into the host.

Operating system or application-level.

Highly localised view of activity but allows operating system/ application specific attacks/ misuse to be detected.

Major types: file-integrity and behavioural.

File-Integrity monitoring



Structure of the Tripwire system

Behaviour monitoring

BlackIce

Host-based IDS for Windows and carries out extensive port analysis

Four levels: Paranoid, Nervous, Cautious, Trusting

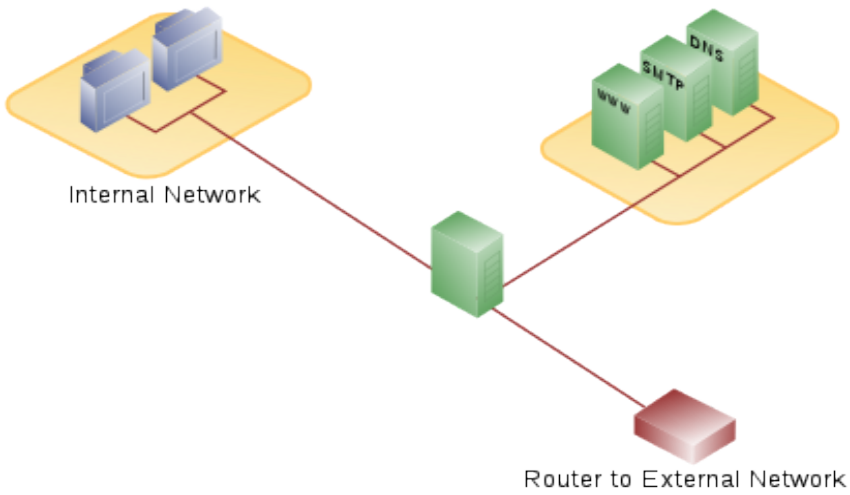
Detects known attacks.

Real time network usage graph

Links to full protocol stack

www.networkice.com

Network Based IDS (NIDS)



E-box monitors network traffic.

Operating system agnostic.

Sensor placement crucial to ability to detect attacks.

Performance an issue if on backbone.

Won't affect performance of hosts, doesn't require installation on hosts simplifying deployment.

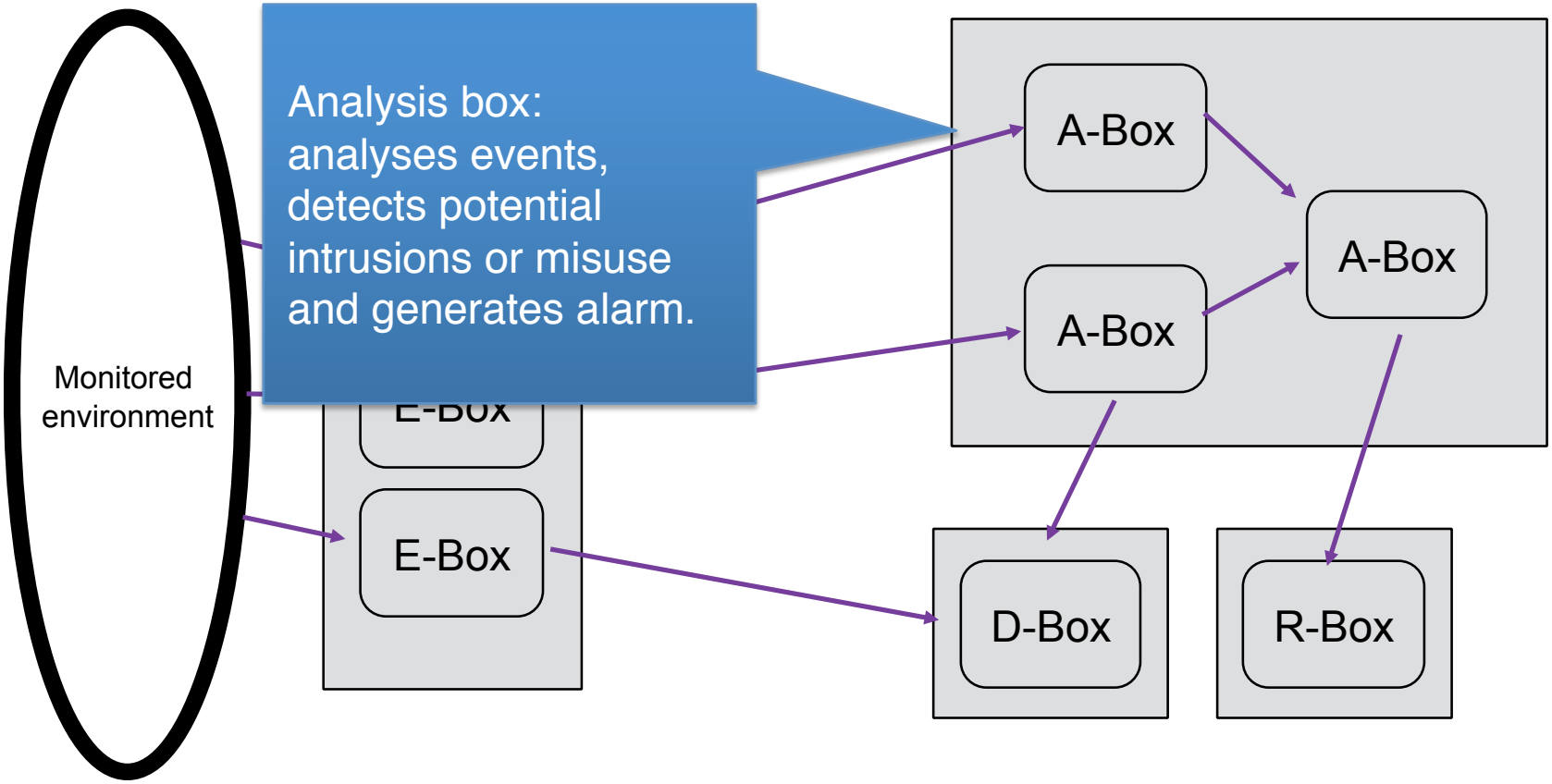
Example: SNORT

Lightweight IDS system capable of performing real-time traffic analysis and packet logging
Snort has three primary uses. It can be used as:

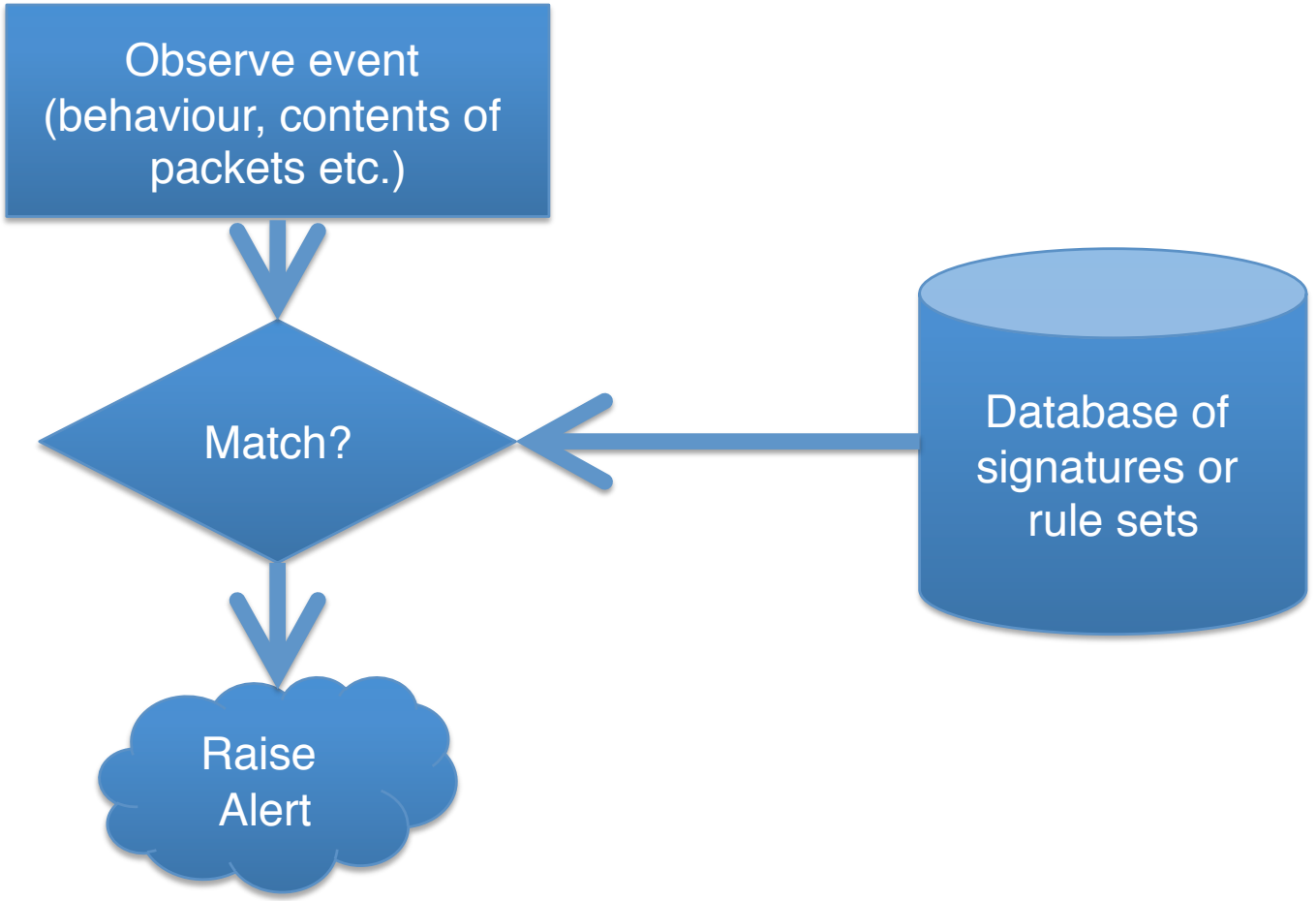
1. a packet sniffer like tcpdump
2. a packet logger (useful for network traffic debugging, etc)
3. a full network intrusion detection system

DETECTION MODELS

Common Intrusion Detection Framework (1999)



Misuse or Signature-Detection



Signature-Detection: Rules

NIDS-style rules

Unique signature byte sequence

Protocol to examine (such as TCP, UDP, ICMP)

IP port requested

IP addresses to inspect (destination and source)

Action to take (such as allow, deny alert, log, disconnect).

HIDS-style rules

Unique signature byte sequence

Files to examine.

Action to take (such as delete, quarantine, alert).

Signature-Detection: SNORT

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 139
  flow:to_server,established
content:"|eb2f 5feb 4a5e 89fb 893e 89f2|"
msg:"EXPLOIT x86 linux samba overflow"
reference:bugtraq,1816
reference:cve,CVE-1999-0811
classtype:attempted-admin
```

Signature-Detection: Advantages/Disadvantages


False negatives are low.

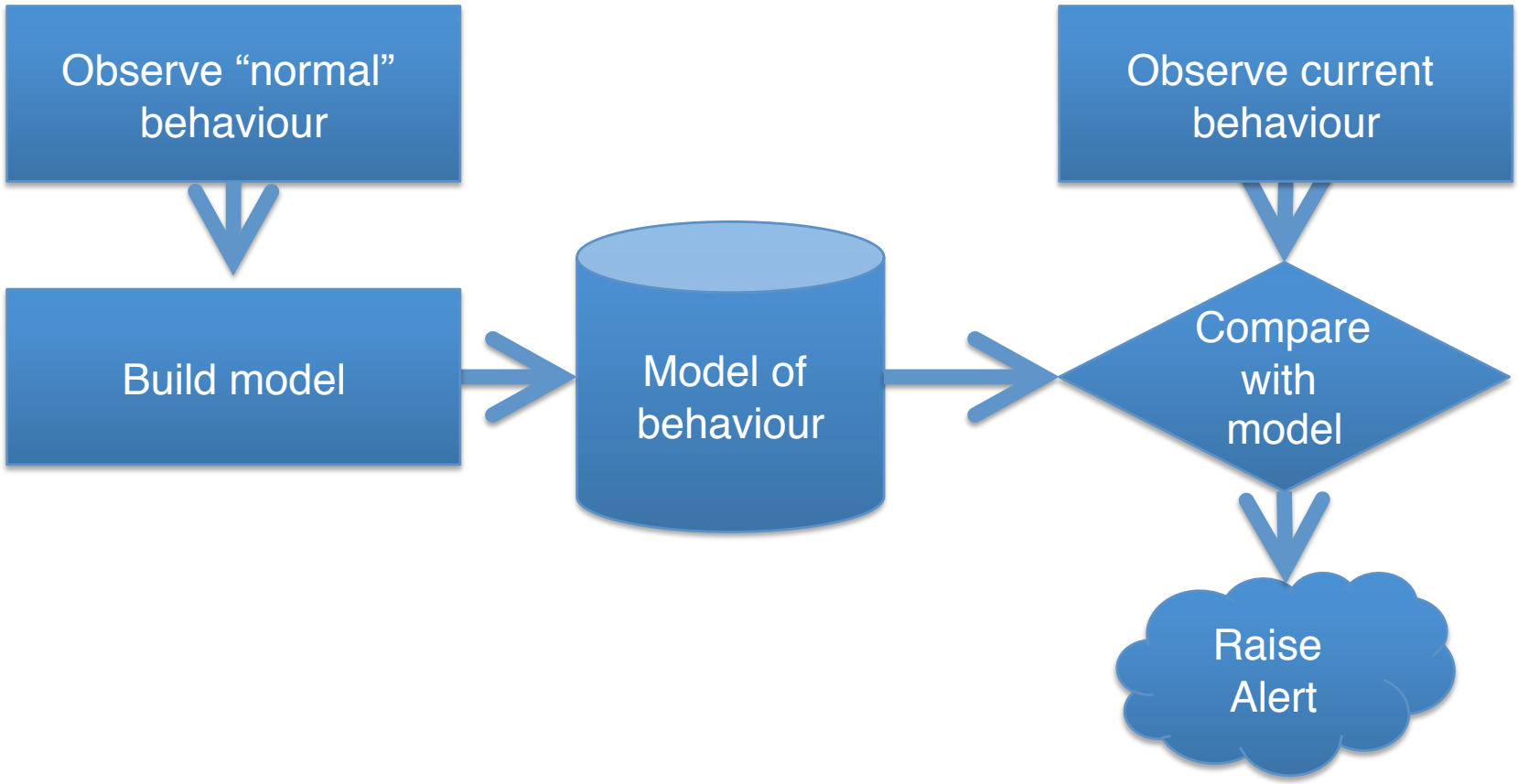

Able to specify the nature of the attack.


Polymorphic attacks/viruses are a problem.


Performance degrades as signature database grows.


Zero-day attacks are a problem.

Anomaly Detection



Anomaly-Detection: Events

Unusual account activity.

Excessive file and object accesses.

High CPU utilization.

Unusual pattern of commands issued at terminal.

High number of sessions.

Unusual traffic volumes or protocol types.

Unusual process activity.

Anomaly-Detection: Advantages/Disadvantages

Can deal with unknown attacks because focuses on effect of attack rather than characteristics of attack itself.

Difficulty of defining what is “normal” behaviour leading to high false positives.

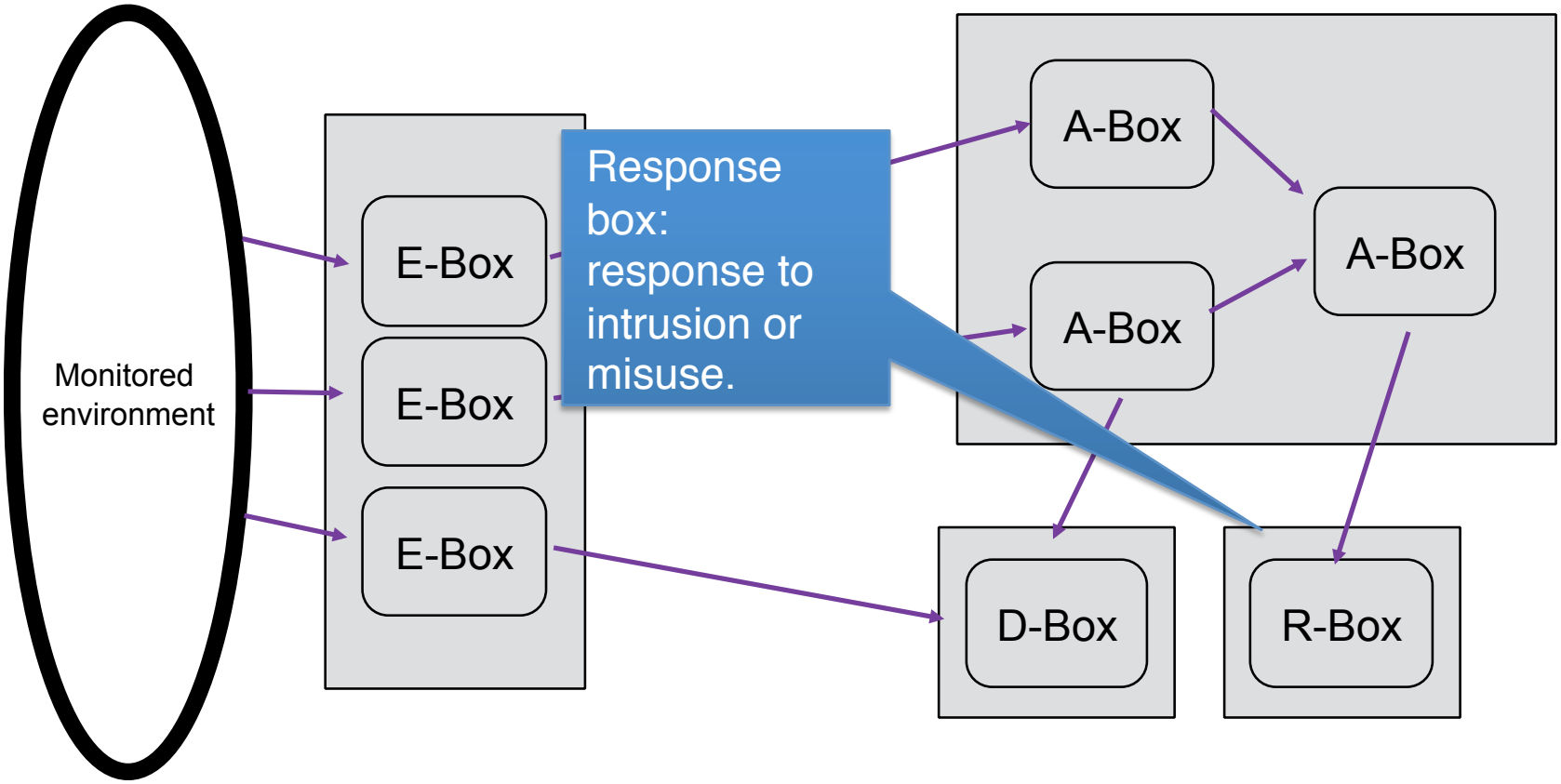
Hackers who understand the model can deliberately change their behaviour to avoid detection.

Anomaly Detection: Self Non-Self Discrimination

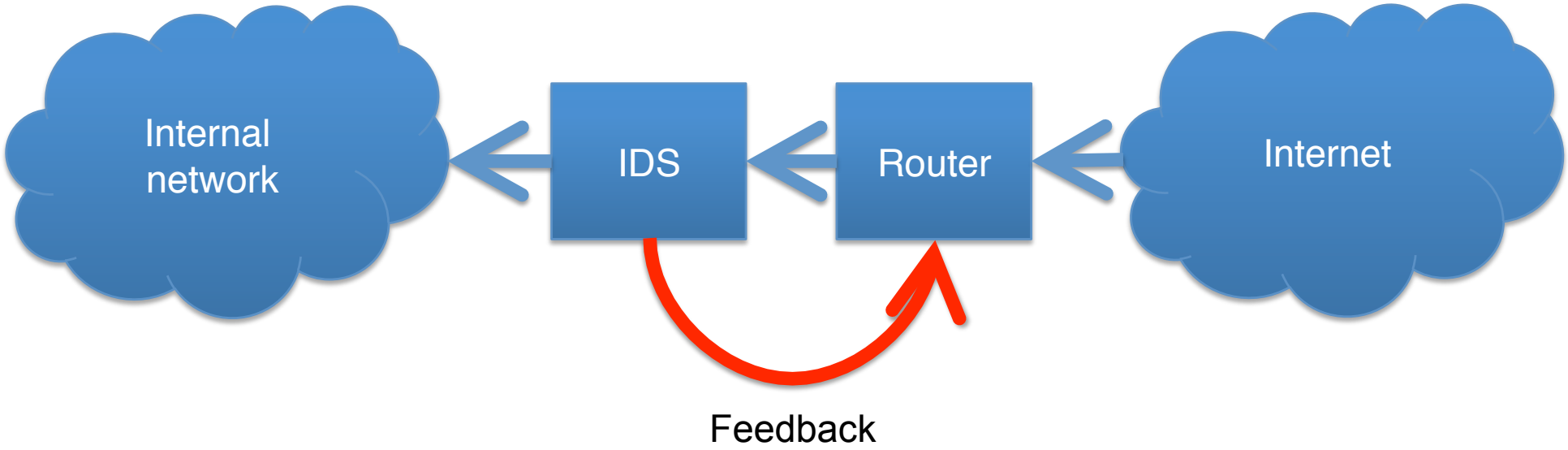
```
[larre@galadriel homeostasis]$ strace ./hello
execve("./hello", ["./hello"], [/* 35 vars */]) = 0
uname(sys="Linux", node="galadriel", ...) = 0
brk(0)                                  = 0x8049674
open("/etc/ld.so.preload", O_RDONLY)    = -1 ENOENT (No such file or directory)
open("/etc/ld.so.cache", O_RDONLY)      = 3
fstat64(3, st_mode=S_IFREG|0644, st_size=107844, ...) = 0
old_mmap(NULL, 107844, PROT_READ, MAP_PRIVATE, 3, 0) = 0x40017000
close(3)                                = 0
open("/lib/i686/libc.so.6", O_RDONLY)   = 3
read(3, "77ELF 06"..., 1024) = 1024
fstat64(3, st_mode=S_IFREG|0755, st_size=5772268, ...) = 0
old_mmap(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x40032000
old_mmap(NULL, 1290088, PROT_READ|PROT_EXEC, MAP_PRIVATE, 3, 0) = 0x40033000
mprotect(0x40165000, 36712, PROT_NONE)  = 0
old_mmap(0x40165000, 20480, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED, 3,
0x131000) = 0x40165000
old_mmap(0x4016a000, 16232, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_ANONYMOUS,
-1, 0) = 0x4016a000
close(3)                                = 0
munmap(0x40017000, 107844)              = 0
write(1, "hello, world!", 14hello, world!)         = 14
_exit(0)                                = ?
[larre@galadriel homeostasis]$
```

INTRUSION PREVENTION SYSTEMS

Common Intrusion Detection Framework (1999)



IPS Concept



Advantages/Disadvantages

Can mitigate effect of an ongoing attack rather than deal with the aftermath.

Efficiency, how long does it take to react?

Can attackers turn the IPS to create a denial-of-service by tricking it into false positive?

Evading IDS

Overwhelm IDS with false positives (denial-of-service).

Create operator fatigue by generating false positives.

Exploit understanding of structure of IDS to defeat attacks.

Targeting IDS component vulerabilities (buffer overflow etc.).

SUPPORTING TECHNOLOGIES

Network Mappers

Commercial and free tools available - Cheops and nmap

Carry out - DNS zone transfers, address/port scanning, host requests, promiscuous monitoring

nmap sends variety of packets with illegal flags, ICMP echos, fragmented packets etc to hosts and analysing responses

Eg recognise Linux with kernels older than 2.0.35 by using packet with SYN and illegal flags set

Security Scanners

Network mapping tools (nmap) allow verification of system

Network Security Scanners test and report system security

Sample tools:

SATAN/SAINT/SANTA

Metasploit

Snort, ShieldsUP!, LeakTest (probe for vulnerabilities)

Host-based - search for mis-configurations and dangerous settings, unusual privileges etc

Network-based - checks host security policies, dangerous or unnecessary services

Honeypots Systems

Current IDS methodologies have shortcomings:

- problem recognising novel attacks
- occurrence of false positives
- reporting of attacks of no interest

Honeytrap system – simulated or real system that exists for sole purpose of being attacked!

Looks and behaves like real system

Must not be launching pad

Must gather valuable information on attacker