Системи за откриване на заплахи (IDS) и за предпазване от заплахи (IPS)

проф. д-р инж. Венета Алексиева

Основни моменти

- Системи за откриване на заплахи (IDS)
  - Архитектура,
  - Предимства, недостатъци
- Системи за предпазване от заплахи (IPS)
  - Архитектура,
  - Предимства, недостатъци

Системи за откриване на заплахи

- Не може да се предотвратят всички атаки към системата.
- Винаги ще има пропуски, нови атаки и нови атакуващи.
- Търсят се начини за защита:
  - Повечето единични защити могат да се провалят.
  - Затова се прилага защита в дълбочина – на няколко слоя:
    - 1 слой - системи за откриване на проникване (IDS)
    - 2 слой – системи за защита от проникване (IPS)

IDS , IPS и IDPS

- Системата за откриване на проникване (IDS) е софтуер, който автоматизира процеса на откриване на проникване. Заплахата е разпозната, но е достигнала до целта.
- Системата за предотвратяване на проникванията (IPS) е софтуер, който разполага с всички възможности на система за откриване на проникване, но може да се опита да спре евентуални инциденти.
- Системата за откриване и предотвратяване на проникванията (IDPS) = IDS+IPS

Допускания

- Действията в компютърните системи са наблюдаеми.
- И нормалната работа, и заплахите имат определена последователност от събития, която може да бъде проследена.

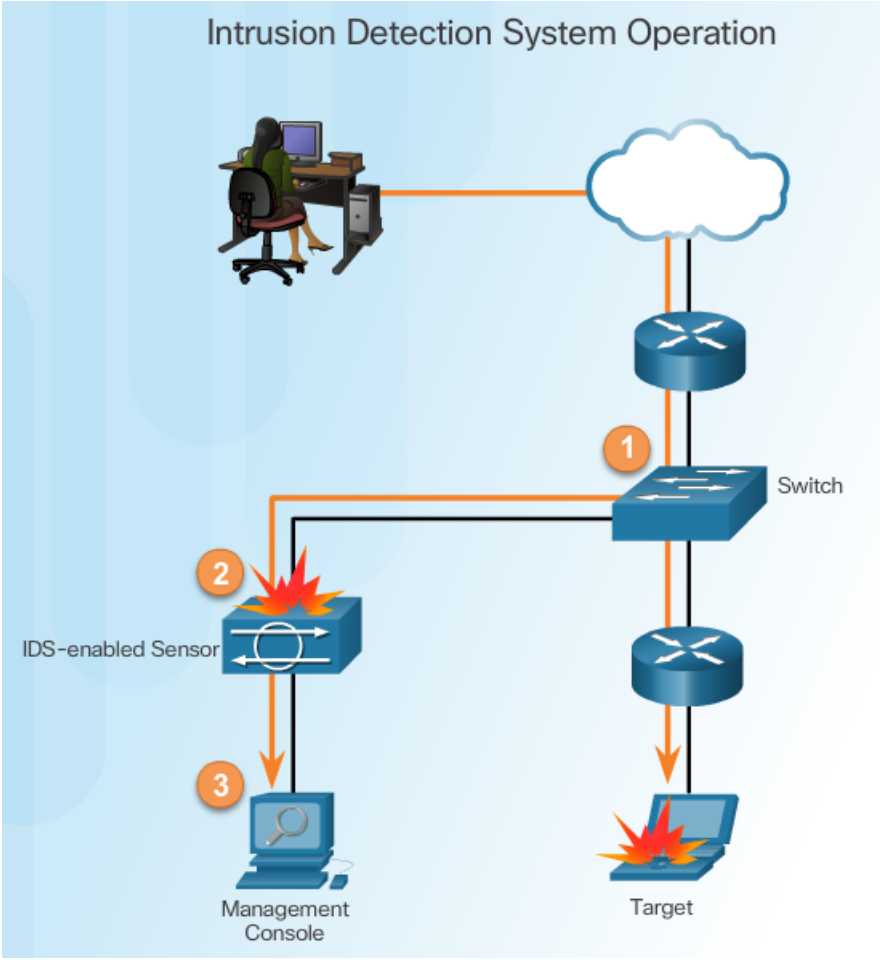
Наблюдение на системата

- Наблюдават се събитията, настъпващи в компютърна система или мрежа.
- Анализират се признаци на възможни инциденти, които са нарушения или непосредствена заплаха от нарушение на правилата за компютърна сигурност.
- Инцидентите са **злонамерени**, породени от:
  - Зловреден софтуер (червеи, шпионски софтуер…),
  - Неупълномощен достъп до системите от Интернет
  - Злоупотреба с привилегии на упълномощени потребители
  - Опити за получаване на допълнителни привилегии
- Инцидентите са и **случайни**:
  - Човек може да сгреши адреса на компютъра и случайно се опитва да се свърже с различна система без разрешение.

Наблюдение на атаките

Предимства на IDS:

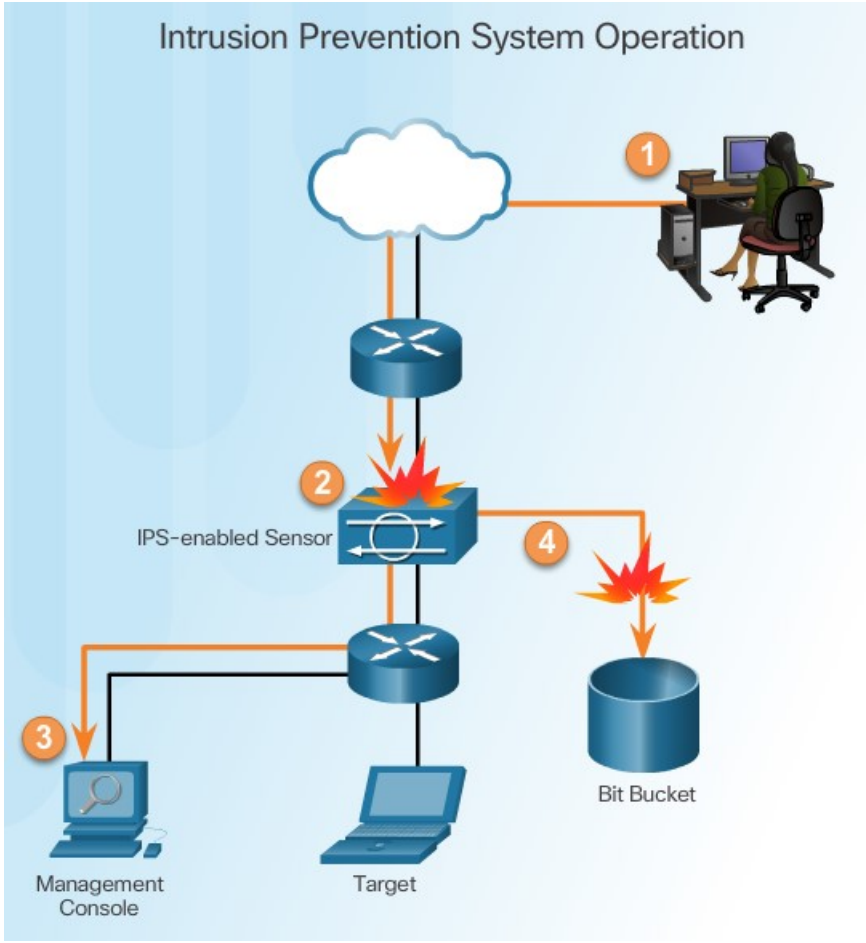
- Работят пасивно.
- Изискват трафика да бъде дублиран (mirror) през системата, за да бъде анализиран.
- Мрежовият трафик не преминава през IDS освен ако не е дублиран (mirror).



Откриване и спиране на атаките

Предимства на IPS:

- Изпълняват се в режим инлайн.
- Наблюдават трафик на слой 3 и слой 4.
- Могат да спрат един пакет от атаката да не достигне целта.
- Реагират веднага и не позволяват на всеки злонамерен трафик да премине.



Прилики между IDS и IPS

- Разработени са като сензори.
- Използват сигнатури за откриване на шаблони на злоупотреби в мрежовия трафик.
- Могат да откриват шаблон в единичен пакет или в група пакети.

Предимства на IDS и IPS

IDS	IPS
Няма въздействие върху мрежата, т.к. няма времезадръжка при преминаване на пакетите.	Спира пакетите на атаката.
Няма въздействие върху мрежата, ако има прекъсване на сензора.	Могат да се използват техники за нормализация на данновия поток.
Няма въздействие върху мрежата, ако има претоварване на сензора.	Наблюдават мрежови събития от ниско ниво.
	Не са видими в мрежата.
	Независими от ОС
	Евтини

Недостатъци на IDS и IPS

IDS	IPS
Ответното действие не може да спре атаката.	Проблеми със сензора може да се отразят на мрежовия трафик.
Изисква се правилна настройка за ответни действия.	Претоварване на сензора може да се отрази на мрежата.
По-уязвими са към техники за укриване на сигурността на мрежата.	Не могат да се изпълняват върху криптиран трафик.
	Не могат да определят дали атаката е била успешна.

Проблеми

- IDS наблюдава, но каквото “вижда” може да не бъде това, което крайната система получава.
- IDS не “вижда” укриване на атаки чрез вмъкване и за да открие такава атака:
  - IDS трябва да деасемблира напълно пакетите,
  - IDS трябва да "нормализира“ фрагментираните пакети.
  - Примери….

Атака чрез вмъкване

Атакуващият праща:

IDS “вижда”:

Жертвата получава:

Bad checksum, TTL

Атака чрез избягване

Атакуващият праща:

IDS “вижда”:

Жертвата получава:

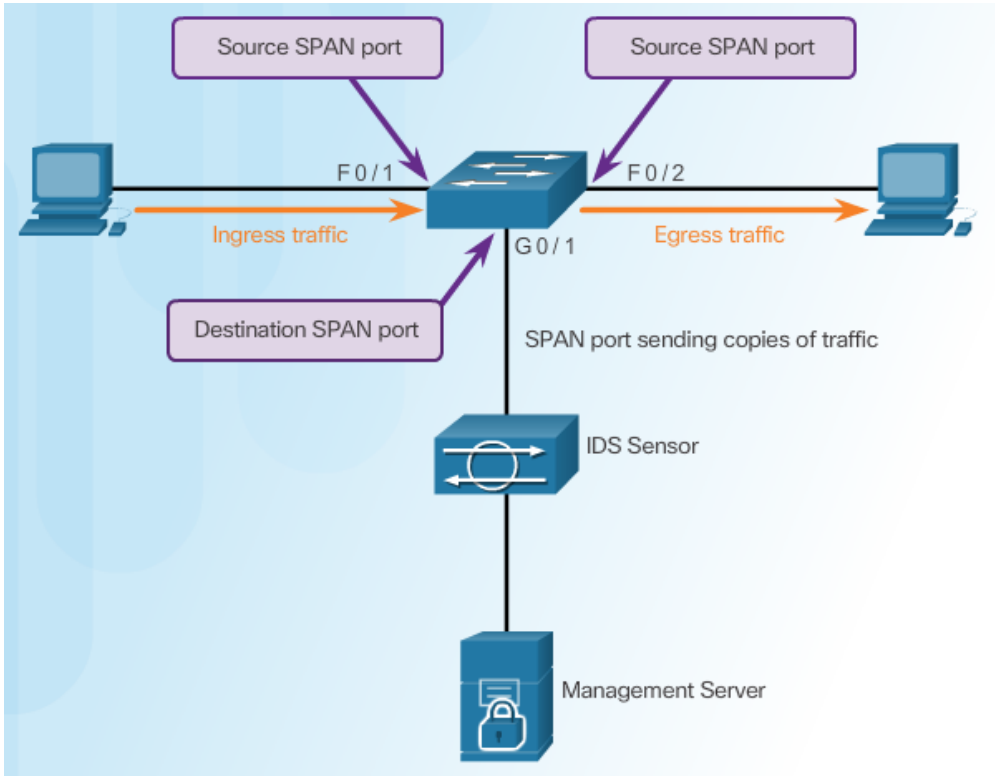
Fragmentation overlap

IDS се различават по:

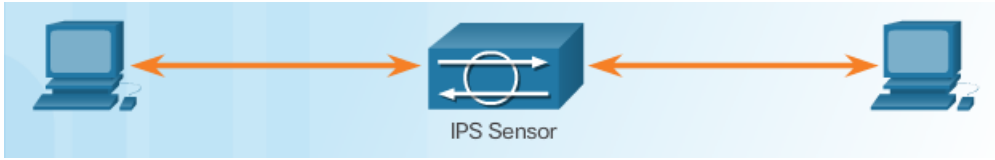
- Метод на засичане – зависи от характеристиките на анализатора
- Реакция на IDS към атаката
- Одит на входната информация, която IDS анализира
- Механизъм на засичане
- Начин на употреба:
  - Real-time;
  - Offline.

Режими на работа

- Случаен режим (IDS)



- Инлайн режим (IPS)

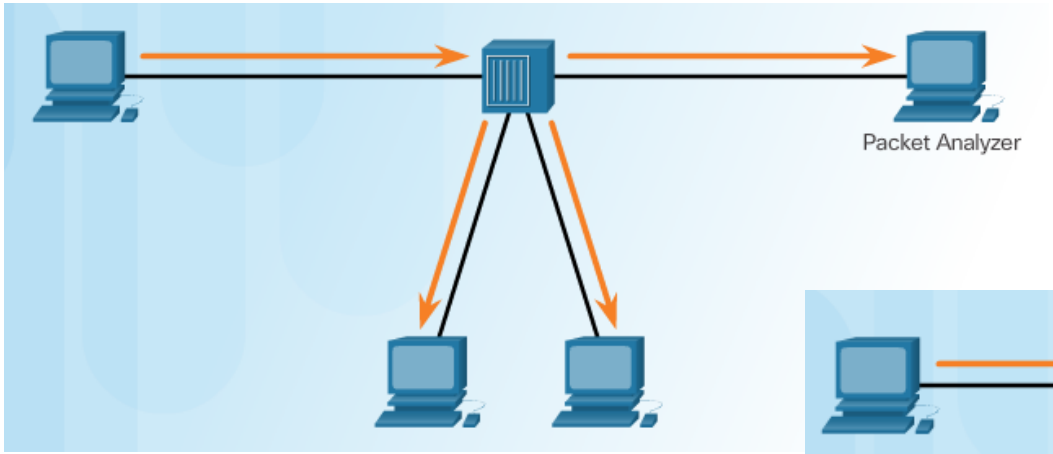


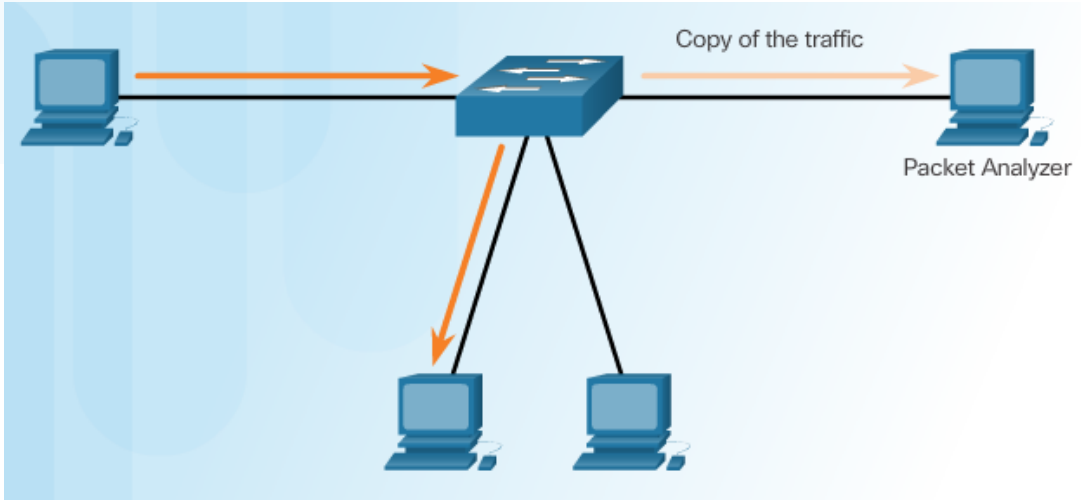
По отношение на време

- IDS в реално време
  - Анализират данни, докато сесията е активна
  - Вдига аларма в момента, в който атаката се случва
- Off-line IDS
  - Анализира данните след като информацията е събрана
  - Полезна за разбирането на естеството на атаката

IDS наблюдение с Port Mirroring

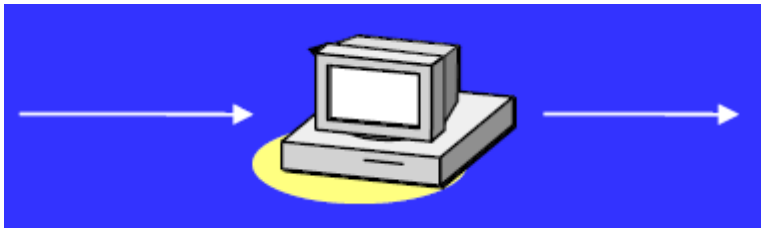
- Снифер, в мрежа с концентратор
- Снифер в мрежа с комутатор, но с port mirroring



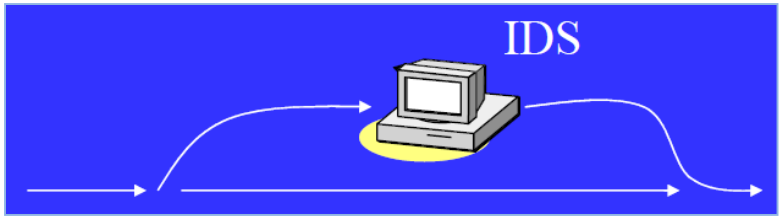


Firewall или мрежова IDS

- Firewall
  - Активно филтрира пакети
  - Успешно спира атака



- Мрежова IDS
  - Пасивно наблюдение
  - Не спира атаката



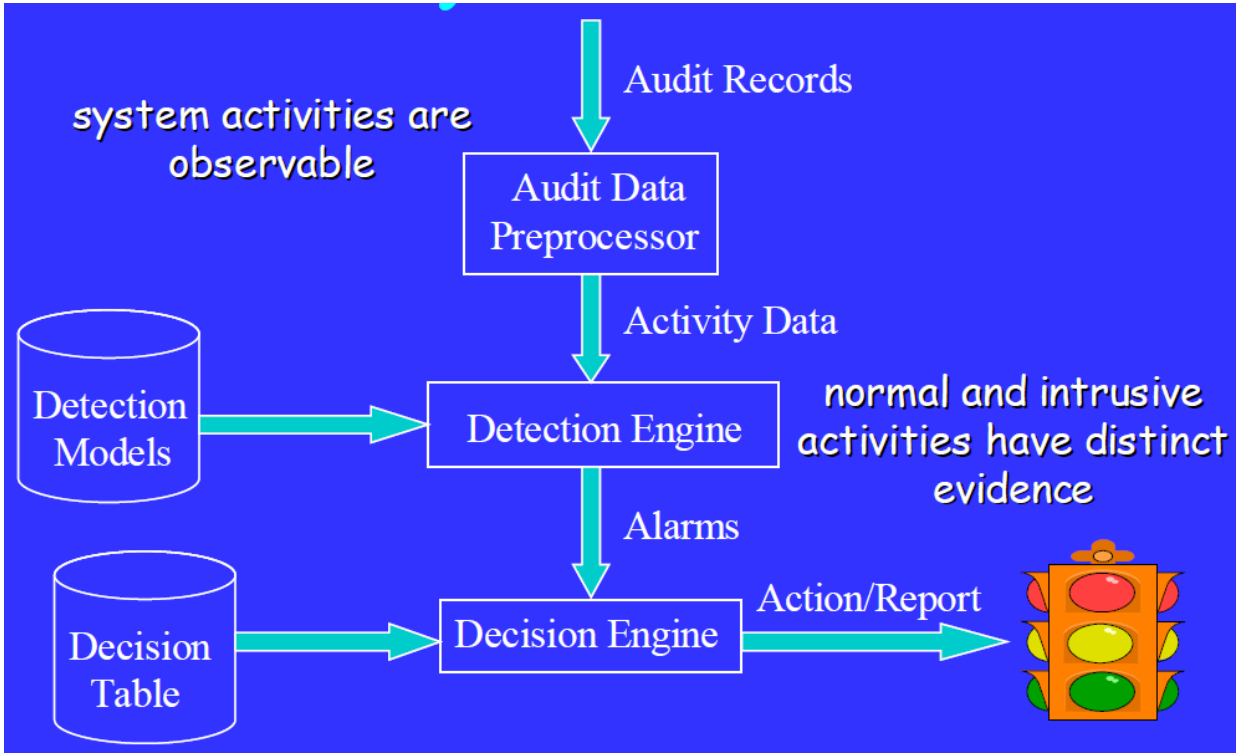
  - DoS атака при Мрежова IDS
    - Висока консумация на ресурси – процесор, памет, bandwidth
    - Злоупотреба с реактивни IDS - лъжливи положителни индикации, атаки, причиняващи нередности или "грешни" пакети / връзки

Изисквания към мрежова IDS

- Висока скорост за наблюдение на голям обем трафик
- Да не отхвърля пакети, отговарящи на филтъра
- Да изпраща аларми в реално време
- IDS е разделена от политиките
- IDS е с възможност за разширения
- Широк обхват за детектиране
- Икономично използване на ресурси
- Устойчива на стрес
- Устойчива на атаки върху самата IDS

Компоненти на IDS

- Филтрира се информацията, необходима за анализ и се формират данните, които описват съответните действия
- На базата на модели за разпознаване се определя дали е атака
- Ако е атака се изпраща сигнал, че има проблем
- На база на определени знания се определя каква да бъде реакцията на системата- блокиране трафик от/към IP адрес….
- Динамично се определят нови правила



Реализация на засичане

- State-based IDS – идентифицира въздействията на състоянието на системата
- Transition-based IDS – наблюдава събития, които предизвикват преминаване на системата от едно състояние в друго

Анализ на състоянието или промяната на системата:

- Non-perturbing- странична оценка на уязвимостта
- Pro-active –анализира ясни, задействащи промяната събития

Избор на решение за IPS

Фактори за избор на IPS сензор:

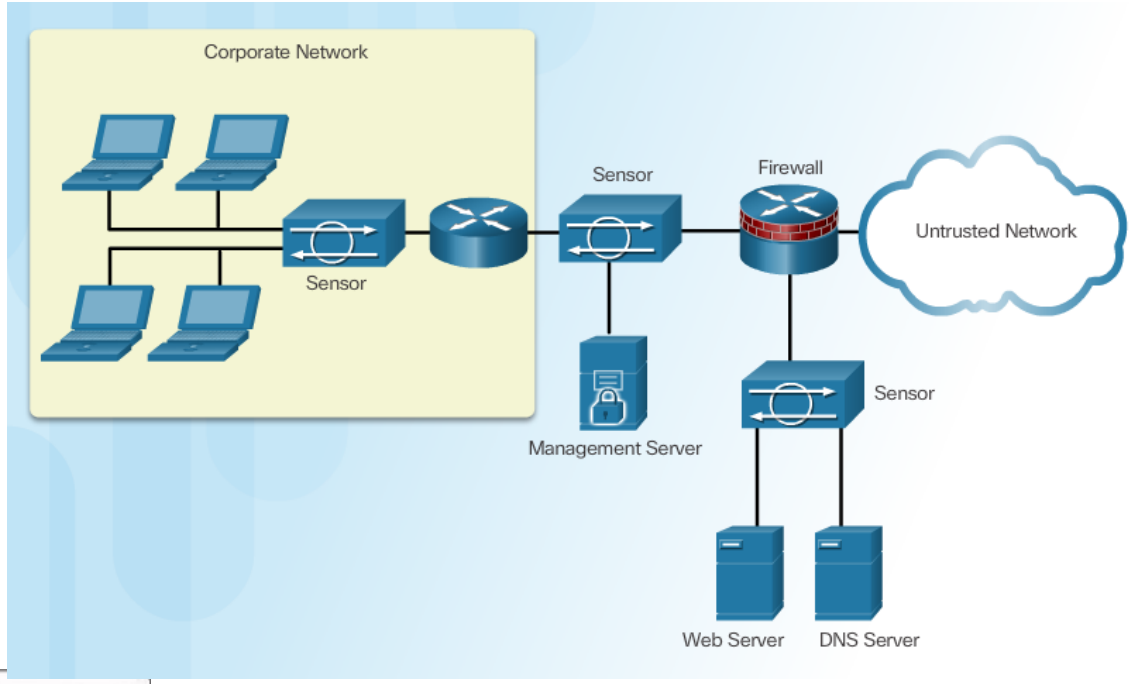
- Размер на мрежовия трафик
- Топология на мрежата
- Бюджет, заделен за сигурност
- Наличен персонал по сигурността, който управлява IPS

Хост-базирани и мрежово-базирани IPS

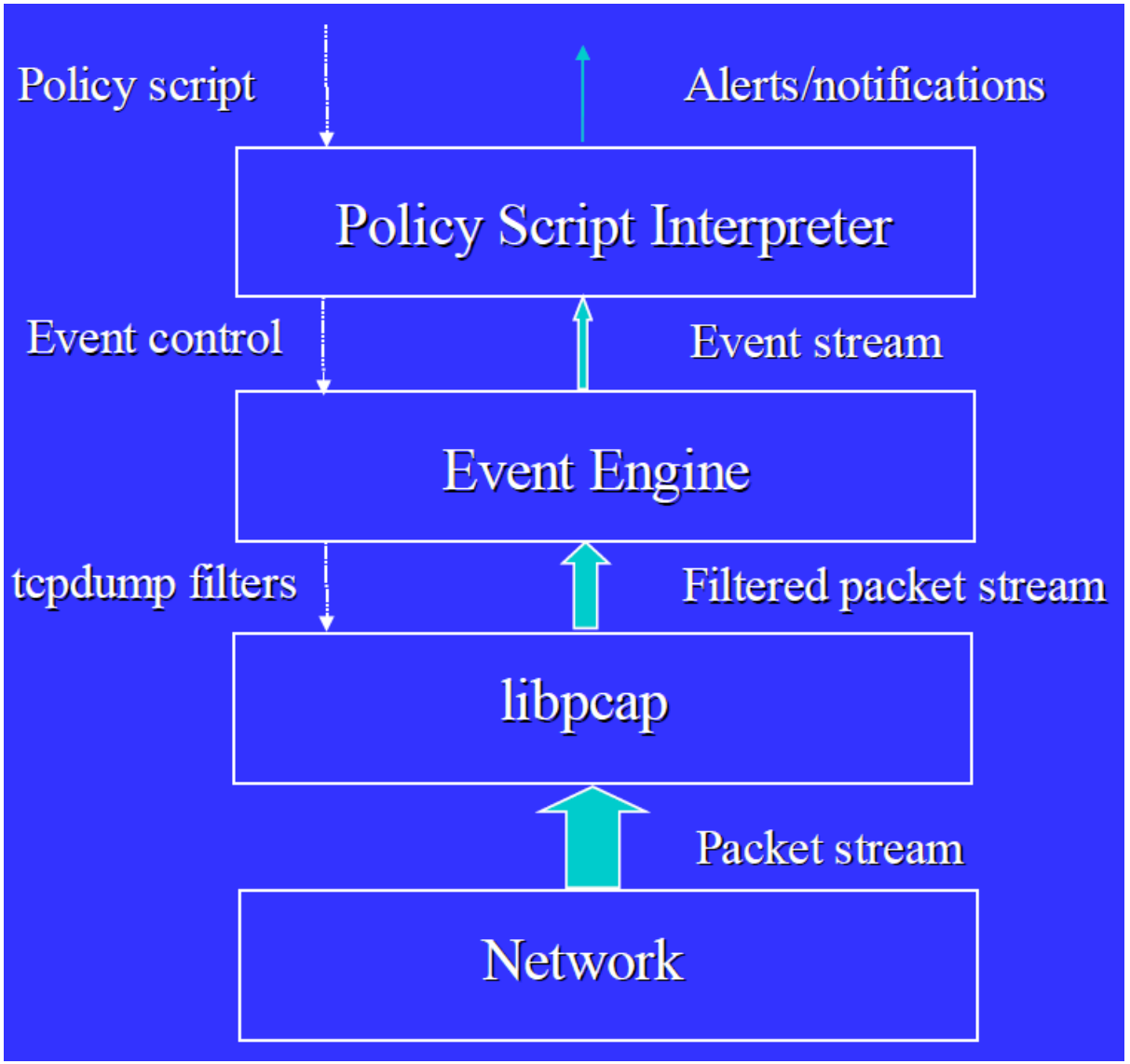
	Предимства	Недостатъци
Хост-базирани IPS реализират се с агенти на самата машина (Windows Registry Scanner; Process Explorer)	•Осигурява специфична защита чрез ОС на хоста •Осигурява защита на ниво ОС и приложения •Защитава хоста след като съобщението е декриптирано •Водят лог-файл и анализират събитията •Генерират аларми	•Зависими са от ОС •Трябва да се инсталират на всички хостове
Мрежово базирани IPS	•Ценово ефективни •Независими от ОС	•Не могат да се изпълняват над криптиран трафик •Трябва да спрат злонамерения трафик преди да постъпи в хоста

Мрежово-базирани IPS

Примери: Cisco IPS AIM and Network Module Enhanced (IPS NME), Cisco ASA AIP-SSM, Cisco IPS 4300 Series Sensors, Cisco Catalyst 6500 Series IDSM-2



Архитектура на мрежово-базирани IDS



Мрежово-базирани IDS

Събира следните данни:

- Подпис ID
- IP адрес на атакуващия
- Порт на атакуващия
- Максимален размер на сегмент
- IP адрес на жертвата
- Порт на жертвата
- Версия на сигнатурата
- TCP опции
- Репутация на резултата
- Оценка на риска

Видове детекции

- Основана на шаблони (Pattern-based)
- Основана на аномалии (Anomaly-based)
- Основана на политики (Policy-based)
- Основана на следене на порт (Honey port-based)
- Основана на знания (Knowledge-based):
  - Експертни системи
  - Анализ на сигнатури
  - Мрежи на Петри
  - Анализ, основан на преминаване през състояния

Предимства/Недостатъци

Тип засичане	Предимства	Недостатъци
Pattern-based	•Лесно конфигуриране •Малък брой фалшиво позитивни детекции •Добър дизайн на сигнатурите	•Не детектва непознати сигнатури •Генерира фалшиво позитивни детекции •Трябва да се създават, обновяват и настройват сигнатури
Anomaly-based	•Прост и надежден •Политики, нагодени според ползвателя	•Общо извеждане •Политиките трябва да бъдат създадени
Policy-based	•Лесно конфигуриране •Може да открива непознати атаки	•Трудно се профилират типовете активност в голяма мрежа •Профилът на трафика трябва да е постоянен
Honey port-based	•През порта се следят атаките •Разсейва и притеснява атакуващия •Забавя и парира атаките •Събира информация за атаките	•Заделя се отделен порт за сървъра •На натоварването на сървъра не трябва да се вярва

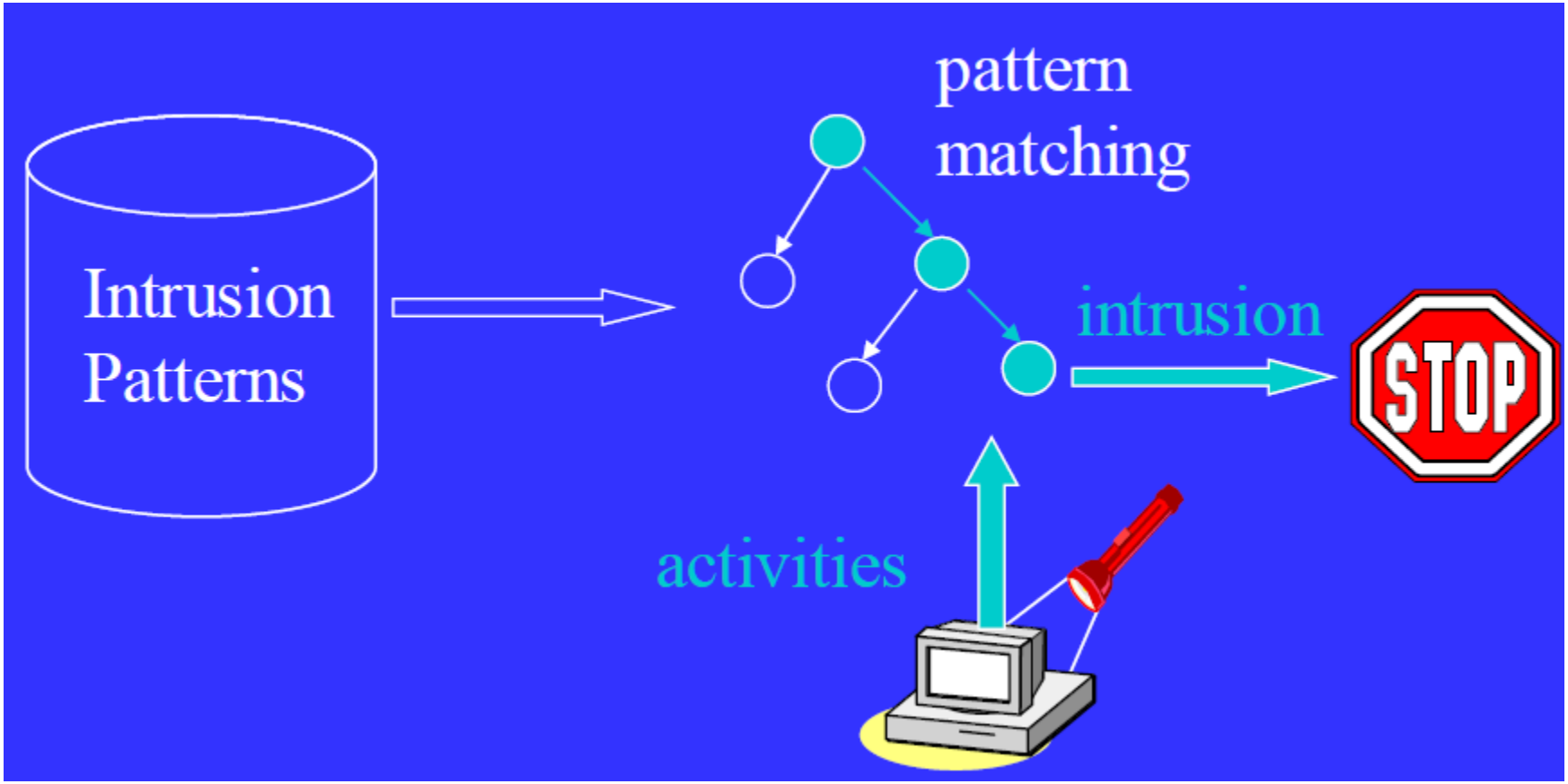
Сигнатури

- Сигнатурата е набор от правила, които IDS и IPS използват за откриване на типична дейност за проникване в системата.
- Когато са идентифицирани нови заплахи, трябва да бъдат създадени и качени в IPS нови сигнатури.
- Сигнатурният файл съдържа пакет от мрежови сигнатури.

Сигнатури

- Атрибути на сигнатурата:
  - Type (Тип)
  - Trigger (аларма)
  - Action (действие)
- Видове сигнатури:
  - **Atomic** - това е простият вид сигнатура, която се състои от един пакет, дейност или събитие, което се изследва, за да се определи дали то отговаря на конфигурираната сигнатура. Ако отговорът е да, се задейства аларма и се извършва действието.
  - **Composite** - поредица от операции, разпределени в няколко хоста през произволен период от време

Сигнатури



- По-малко неверни положителни детекции (но все още има)
- Не може да открива нови атаки, сигнатурите трябва да се обновяват често

Основана на шаблони (Pattern-based)

Atomic	Composite
нито едно състояние не е задължено да разглежда шаблона, за да определи дали следва да се приложи действието на сигнатурата	Трябва да съдържа състояние или няколко елемента, а да определи дали следва да се приложи действието на сигнатурата

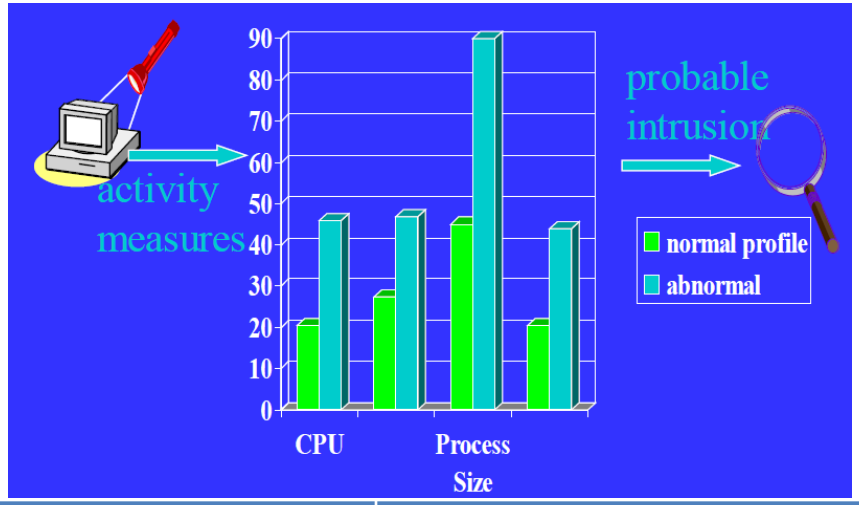
- Пример

Atomic	Composite
Откриване на ARP request с source_MAC=FF:FF:FF:FF:FF:FF	Откриване на стринг “confidential” в няколко пакета от една TCP сесия

Основана на аномалии (Anomaly-Based)

Atomic	Composite
Не изисква състояние, за да определи дейността, която се отклонява от нормалния профил	Трябва да съдържа състояние, за да определи дали дейността се отклонява от нормалния профил

- Пример



Atomic	Composite
Откриване на трафик, който е за дестинационен порт, който не е в нормалния профил; Source_IP=Destination_IP	Проверява съответствието на протокола за HTTP трафика.

Основана на политики (Policy-based)

Atomic	Composite
Не изисква състояние, за да определи нежелано поведение	Предшестваща дейност (състояние) се изисква, за да се определи нежеланото поведение

- Пример

Atomic	Composite
Откриване на ненормално големи фрагментирани пакети, които представляват само последен фрагмент	SunUnix хост изпраща RPC заявка до отдалечен хост без да осъществи начално обръщение към Sun PortMapper програмата.

Trigger (аларма)/ Action (действие)

Alarm Type	Network Activity	IPS Activity	Outcome
False positive	Normal user traffic	Alarm generated	Tune alarm
False negative	Attack traffic	No alarm generated	Tune alarm
True positive	Attack traffic	Alarm generated	Ideal setting
True negative	Normal user traffic	No alarm generated	Ideal setting

Category	Specific Alert
Generating an alert	Produce alert
	Produce verbose alert
Logging the activity	Log attacker packets
	Log pair packets
	Log victim packets
Dropping or preventing the activity	Deny attacker inline
	Deny connection inline
	Deny packet inline
Resetting a TCP connection	Reset TCP connection
Blocking future activity	Request block connection
	Request block host
	Request SNMP trap
Allow the activity	This action will permit the traffic to appear as normal based on configured exceptions. An example would be allowing alerts from an approved IT scanning host.

Лог файл за последващ анализ

Specific Alert	Description
Log attacker packets	This action starts IP logging on packets that contain the attacker address and sends an alert. An alert will be written to the Event Store, even if the Produce Alert action is not selected.
Log pair packets	This action starts IP logging on packets that contain the attacker and victim address pair. An alert will be written to the Event Store, even if the Produce Alert action is not selected.
Log victim packets	This action starts IP logging on packets that contain the victim address and sends an alert. An alert will be written to the Event Store, even if the Produce Alert action is not selected.

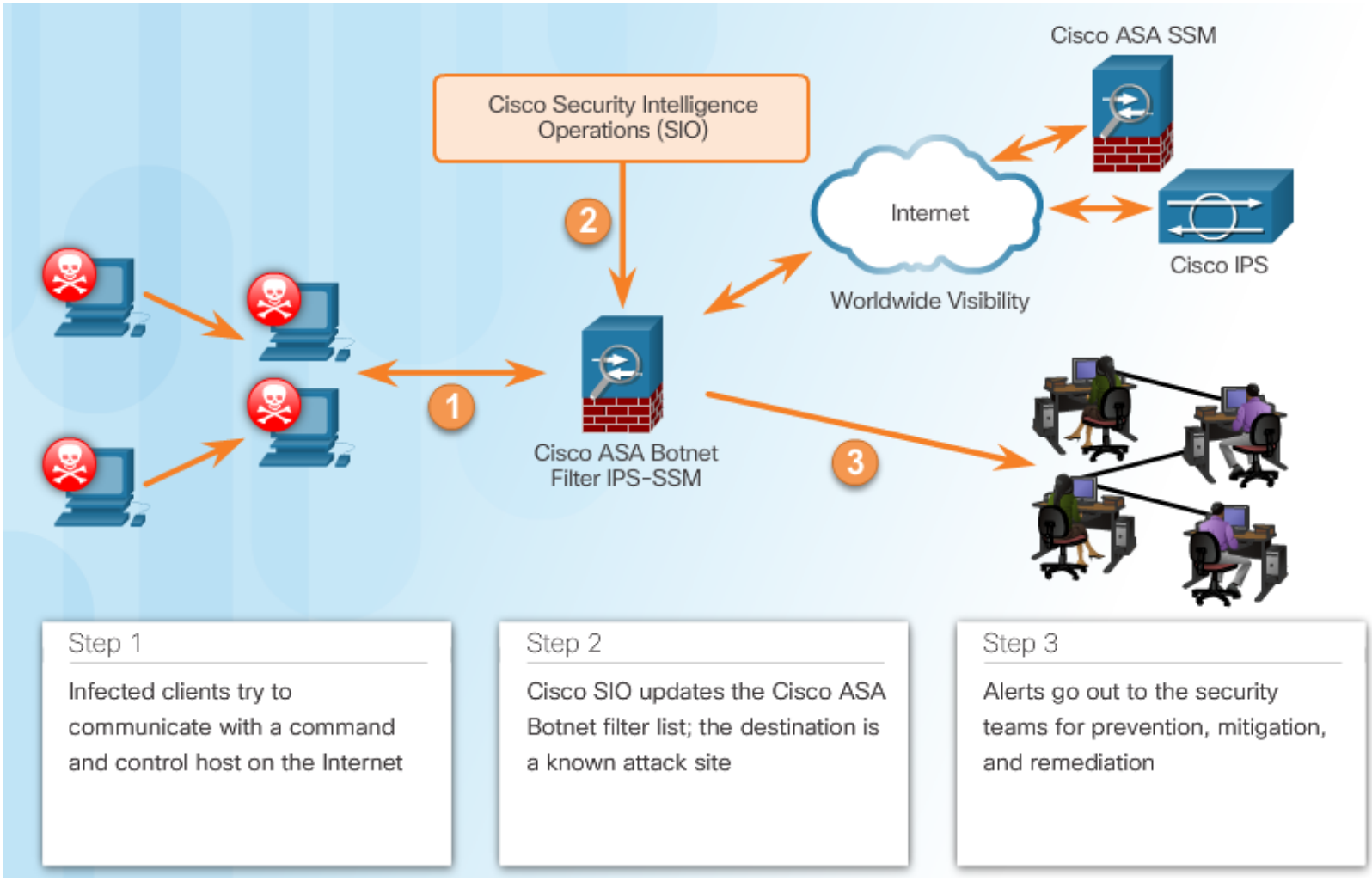
Забранителни действия

Specific Alert	Description
Deny attacker inline	• This action terminates the current packet and future packets from this attacker address for a specified period of time. • The sensor maintains a list of the attackers currently being denied by the system. • Entries may be removed from the list manually or automatically based on a timer. • The timer is a sliding timer for each entry. Therefore, if attacker A is currently being denied, but issues another attack, the timer for attacker A is reset and attacker A remains on the denied attacker list until the timer expires. • If the denied attacker list is at capacity and cannot add a new entry, the packet is still denied.
Deny connection inline	This action terminates the current packet and future packets on this TCP flow.
Deny packet inline	This action terminates the packet.

Specific Alert	Description
Reset TCP connection	This action sends TCP resets to hijack and terminate the TCP flow.
Request block connection	This action sends a request to a blocking device to block this connection.
Request block host	This action sends a request to a blocking device to block this attacker host.
Request SNMP trap	This action sends a request to the notification application component of the sensor to perform Simple Network Management Protocol (SNMP) notification. An alert will be written to the Event Store, even if the Produce Alert action is not selected.

Пример

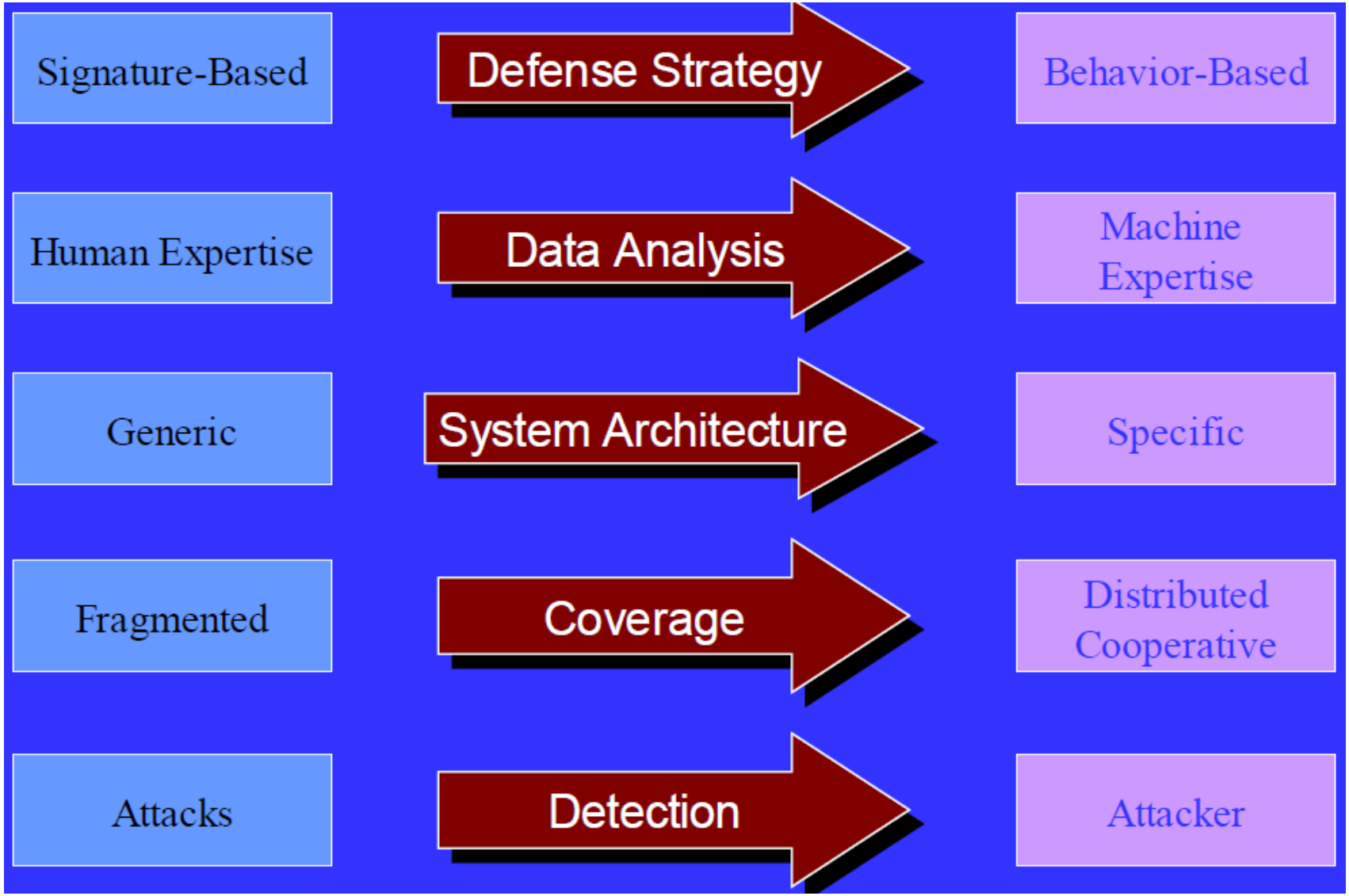
- Reputations, Blacklists, Traffic Filters



Съвременни средства за IT сигурност

- Създава се списък с неправилно поведение:
  - Дефиниции на вируси
  - SPAM филтри
  - Blacklists
  - IDS сигнатури
  - политики
- Предоставят се тези списъци на IDS
- Те сигнализират за:
  - Поведение, което не се вписва в шаблона
  - Когато системата е на път да се срине
  - При закъснения
  - При претоварване с административен трафик
  - Лъжливи положителни аларми

Перспективи



Въпроси ?

Благодаря за вниманието !