**IDS (Intrusion Detection System)** – это система обнаружения вторжений, которая выявляет несанкционированный доступ или управление компьютерной системой, анализируя сетевой или системный трафик.

**Сетевая IDS (NIDS)** – это система, которая отслеживает сетевой трафик для выявления угроз DoS, сканирование портов или попытки проникновения.

**Отличие пассивных и активных IDS**:  
***Пассивные*** IDS фиксируют нарушения и отправляют уведомления администратору. ***Активные*** IDS автоматически принимают меры по предотвращению угроз, такие как разрыв соединений или настройка межсетевого экрана.

**Snort** – это бесплатная сетевая система предотвращения и обнаружения вторжений (IPS/IDS) с открытым исходным кодом, которая анализирует сетевой трафик в реальном времени и фиксирует подозрительную активность.  
(Выполняет обнаружение попыток атак, таких как переполнение буфера, сканирование портов, атаки на веб-приложения и зондирование SMB).

***Правила*** Snort состоят из заголовка, где указывается действие (например, alert), и параметров, описывающих условия срабатывания (например, IP-адреса, порты, контент). При совпадении с условиями правило генерирует оповещение или другие действия.  
Правила пишутся на специальном языке, который включает заголовок и параметры. Например:  
alert tcp any any -> any any (msg:"Example"; content:"test"; sid:123;)

**SIEM (Security Information and Event Management)** – это система управления информацией и событиями безопасности, объединяющая анализ событий, корреляцию данных и мониторинг безопасности.  
(Используется для обнаружения угроз, управления логами, анализа событий в реальном времени и подготовки отчётов для обеспечения безопасности IT-инфраструктуры).

**Отличие SIEM от IDS**:  
IDS фокусируется на анализе сетевого трафика и обнаружении вторжений, тогда как SIEM объединяет данные из разных источников, выполняет их корреляцию и предоставляет интегрированный анализ событий безопасности.

**SIEM** используют в организациях с высоким уровнем требований к безопасности: банках, правительственных учреждениях, крупных корпорациях и центрах обработки данных.

**Преимущества:**

1. Оперативно выявляет угрозы
2. Проводит глубокий анализ событий
3. Улучшает аудит безопасности

**Недостатки:**

1. Высокая стоимость внедрения
2. Сложность настройки
3. Потребность в квалифицированных специалистах для управления