침입탐지시스템의 오용탐지 기법이 사용하는 6가지 방법론

오용탐지는 다음과 같은 6가지 방법론을 사용한다.
1., 전문가 시스템, 전문가시스템은 공격에 관한 규칙집합을 가지고 있어 감사 이벤트가 전문가시스템 내에서 의미를 가지는 사실로 변환이 된다.
2, 시그니쳐 분석. 시그너쳐 분석은 전문가시스템과 동일한 방식으로 지식을 획득하지만 지식을 사용하는 방식이 다르다.
3, 페트리넷이다. 쿠마의 기존 패턴 매칭 방법을 개선한 것이다.
4, 상태전이분석. 상태전이분석은 공격을 목표와 상태 전이의 집합으로 기술하며 상태전이 다이어그램으로 표현한 것이다.
5, 신경망. 신경망은 타당한 방법으로 새로운 입력 출력쌍을 얻기 위해 두 집합의 정보간 관련성을 학습하고 일반화한다.
6, 유전 알고리즘. 유전 알고리즘은 자연 선택의 원리와 자연계의 생물 유전학에 기본 이론을 둔다.