두 가지 접근법: 파일 vs. 메모리

탐지 방식	장점	단점	공격자 회피 난이도
정적 탐지 (Static) 파일 기준	빠른 검사, 알려진 서명에 대한 높은 정확도	패킹/암호화에 취약, 신규 변종 누락 위험	**낮음 (Low)** 간단한 패커나 인코딩으로 우회 가능
메모리 기반 탐지 (Memory-based) 프로세스 기준	난독화 우회 (복호화된 실제 코드 탐지), **실행 행위 기반 탐지** (파일리스 공격 대응)	실시간 스캔 오버헤드 발생 가능, 전문 분석 도구 필요	**높음 (High)** 핵심 코드 로직 자체를 변경해야 함

정적 탐지는 "파일이 어떻게 생겼는가"를 보지만, 메모리 탐지는 "프로세스가 실제 무엇을 하는가"를 파악합니다.