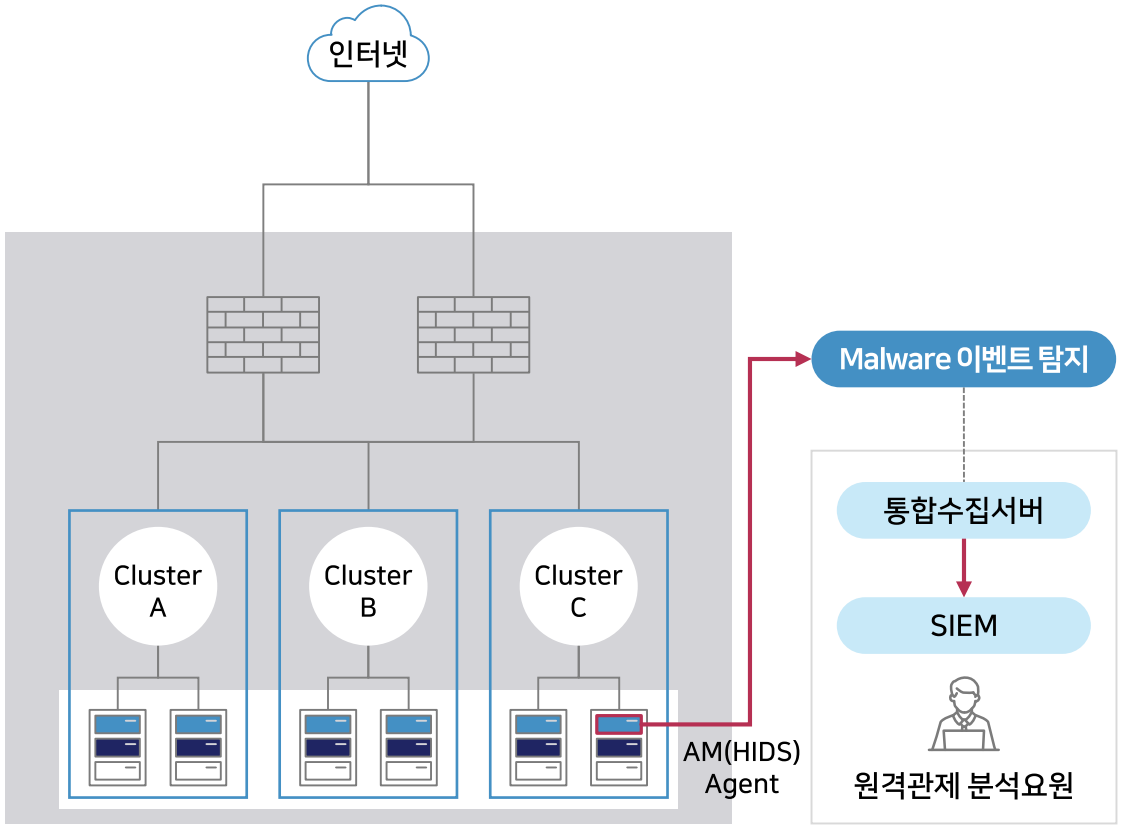
보안관제 서비스 – Anti-Malware 관제

Anti-Malware 관제는 웹서버 내 파일정보를 분석하여 악성코드 감염여부를 탐지하는 서비스 입니다

Anti-Malware 관제 구성

예시



로그수집 및 이벤트 탐지/경보 체계

로그 수집	• Anti-Malware Agent(HIDS와 동일한 Agent 사용)을 통해 암호화하여 통합수집서버로 전송 (탐지 로그)		
이벤트탐지	• Host에 악성코드 파일 존재여부 탐지 • 상용 악성코드 및 악성코드 의심 패턴 탐지		
경보/통보 기준	일반	확인	긴급
	• 악성코드 (위험도:낮음) • 악성의심 구문 또는 스크립트가 포함된 파일 탐지 • 메일 통보	• 악성코드 (위험도:높음) • 솔루션에서 상용 악성코드로 탐지 • 확인 요청(메일)	• 악성코드 (위험도:긴급) • APT, Backdoor 등 시스템에 심각한 영향을 미치는 악성코드 탐지 • 상황보고 (유선/SMS/메일)