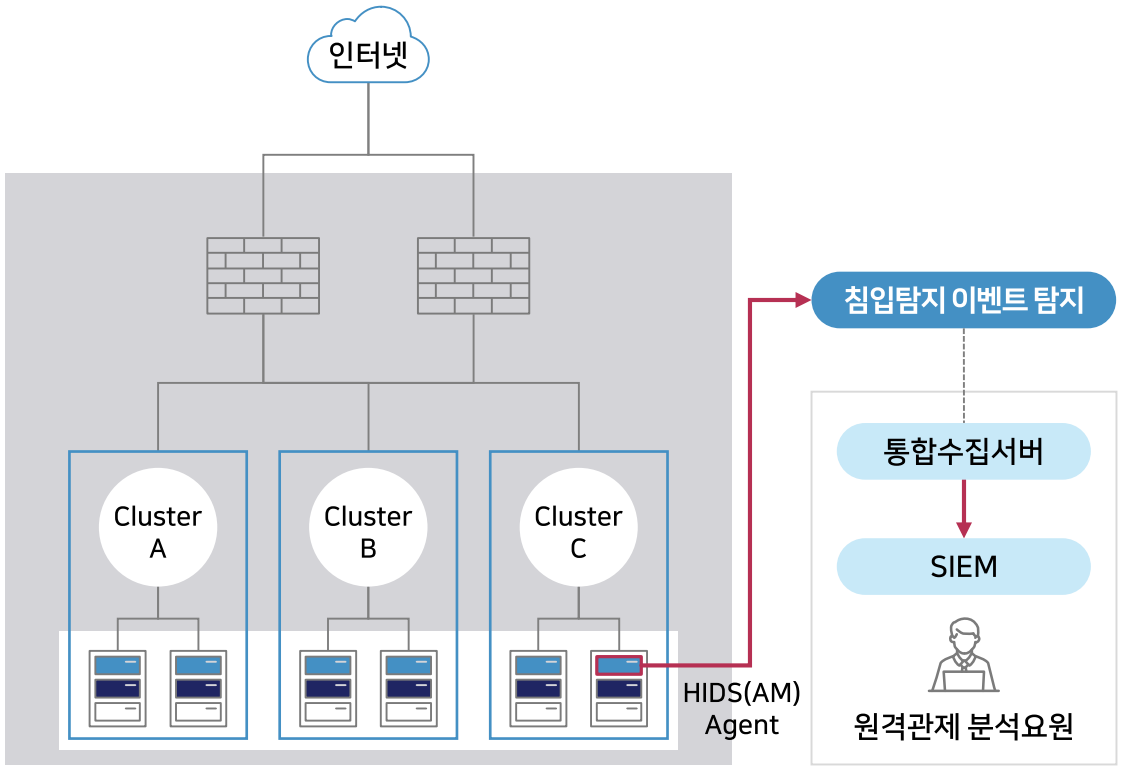
보안관제 서비스 – 침입탐지 관제

침입탐지 관제는 HIDS (Host-based Intrusion Detection System)의 보안 이벤트와 웹방화벽 탐지 로그를
상관 분석하여 패턴기반으로 로그 비정상 여부를 확인하며, 외부에서 접근하는 침입 여부를 탐지 예방하는 서비스 입니다

침입탐지 관제 구성



로그수집 및 이벤트 탐지/경보 체계

로그 수집	• HIDS Agent를 통해 암호화하여 통합수집서버로 전송 (탐지 로그)		
이벤트탐지	• 홈페이지에 GET/POST 방식으로 접근하는 침입 여부를 탐지 • 패턴기반으로 비정상 여부 탐지 • 웹 방화벽(WAF) 탐지 로그와 상관 분석 실시		
경보/통보 기준	일반	확인	긴급
	• 스캔성 이벤트 등 공격 의심 행위 • 메일 통보	• 미성공 웹해킹 공격 • SQL Injection, XSS 등 • 이벤트 상세 분석 • 확인 요청(메일)	• 성공한 웹해킹 공격 • 이벤트 상세 분석 • 상황보고 (유선/SMS/메일)