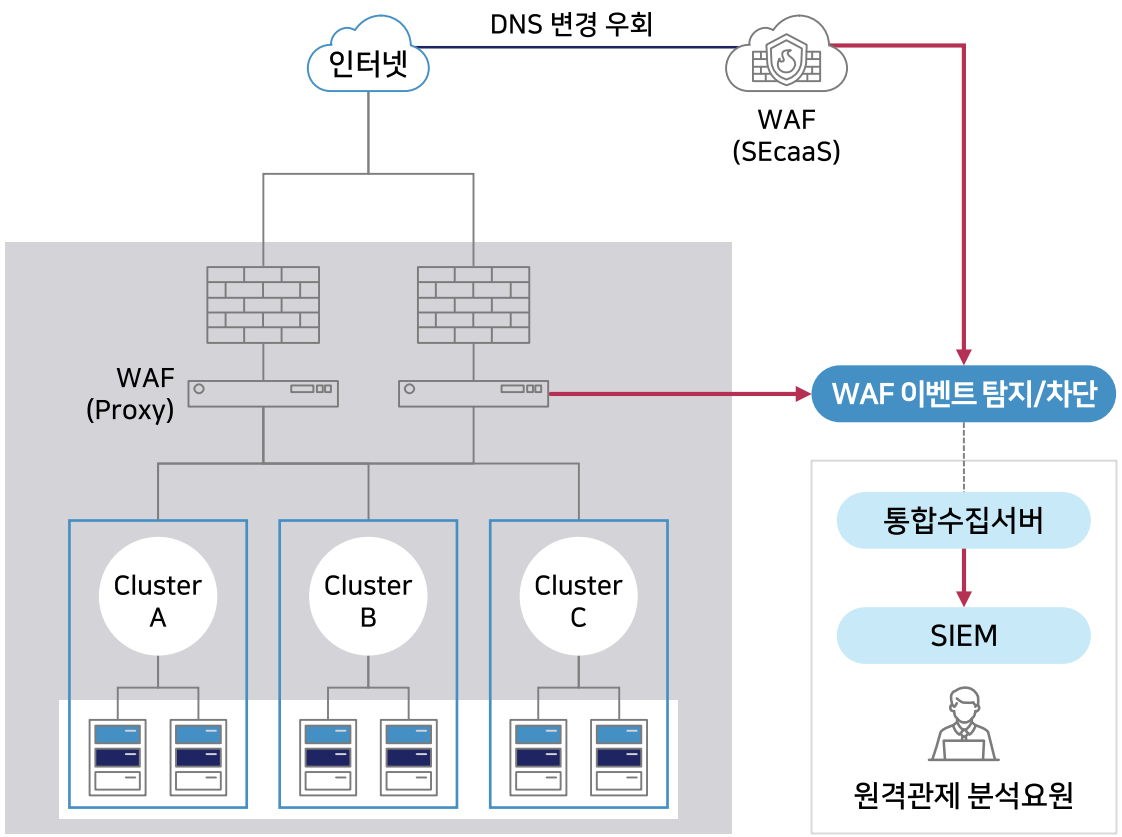
보안관제 서비스 – 웹방화벽 관제

웹방화벽 관제는 웹 취약점 공격을 탐지하여 신속히 조치하며, 예방활동을 통해 고객사 서비스를 보호합니다

WAF 관제 구성

예시



로그수집 및 이벤트 탐지/경보 체계

로그 수집	• WAF(SEcaaS)의 보안 이벤트는 Scrubbing Center에서 통합수집서버로 전송 (탐지 로그) • WAF(Proxy)의 보안 이벤트는 방화벽 VPN을 통해 암호화하여 통합수집서버로 전송 (탐지 로그)		
이벤트탐지	• OWASP 관련 Rule 기반 웹해킹 공격 탐지 • IDS 탐지 로그와 상관 분석 실시 • 고객 협의 후 공격 탐지 이벤트 및 Black-List에 대한 차단 가능		
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)