openbase

Security Monitoring Service

원격 보안관제 서비스

오픈베이스 원격 보안관제 서비스의 핵심 3요소

1 유지보수와 결합된 통합보안 관제서비스

- 보안 솔루션 구축→보안관제→유지보수 및 대응으로 연결되는 원스탑 서비스
- 보안관제서비스와 유지보수 전문인력의 협업을 통한 신속한 장애 대응

기존 유지보수 프로세스

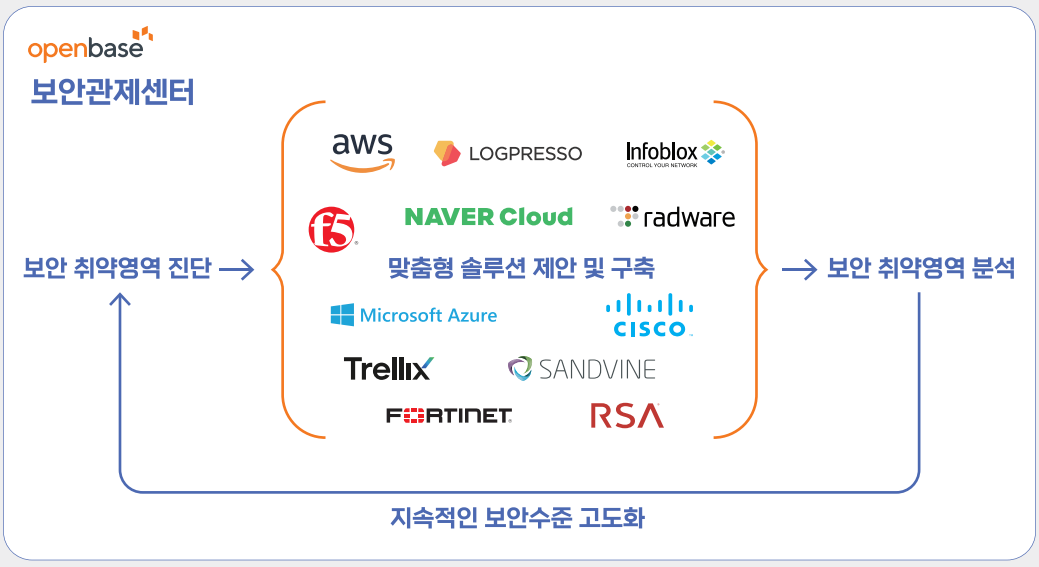
장애발생 → 장애 발견 (고객사) → 장애처리 요청 (고객사) → 장애대응(유지보수 담당)

변경 후 유지보수 프로세스

장애발생 → 실시간 탐지/통보/장애처리 요청 (관제센터→ 고객사, 유지보수 담당) → 장애대응(유지보수 담당)

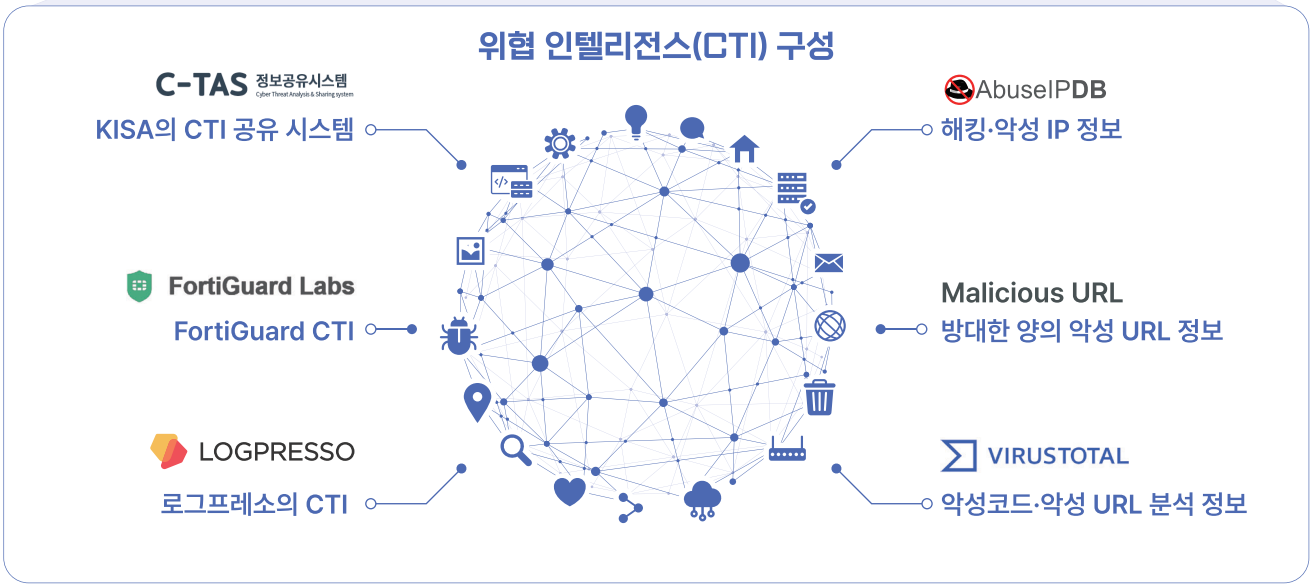
2 시스템 구축부터 관제서비스까지 All-In-One

- 고객사의 요구사항과 환경에 맞춘 관제시스템 제공(서비스형 / 시스템 구축 형)
- 관제를 통한 보안 취약영역 진단 후 솔루션 구축을 통한 보완까지 모두 제공하여 고객사의 전체적인 보안 수준을 고도화 하는 All-in-One 서비스



3

AI/빅데이터 기반의 보안관제 및 분석 시스템



- 시장을 선도하는 상용 보안솔루션을 조합한 보안관제시스템 구현
- 다양한 글로벌 인텔리전스들과 연계된 위협분석시스템
- AI/빅데이터 기술을 적용한 침해위협 분석/대응서비스
- NMS를 이용한 네트워크,시스템 실시간 모니터링(장애시 24시간 SMS/Call 자동 통보)

원격 보안관제 서비스 방식과 효과

보안관제 서비스 대상

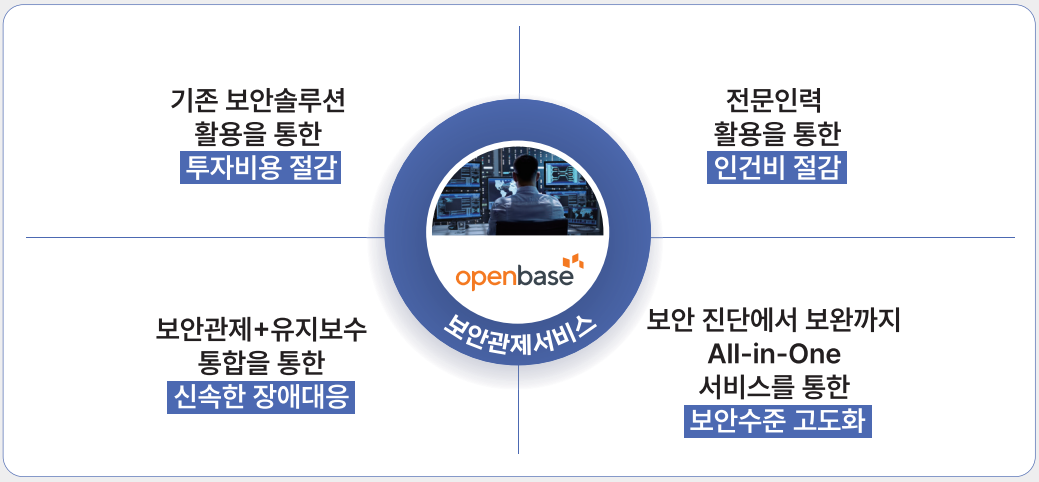
- 오픈베이스를 통해 구축 / 유지보수 중인 솔루션
  - Fortinet FortiGate (UTM), F5 AWAF(웹방화벽), CIsco IPS, 네트워크 장비 등
- 그 외 관제가 필요한 보안 솔루션 (이기종 IDS, IPS 장비 등)

보안관제 제공서비스

- 관제 대상장비의 로그 수집을 통한 원격 보안관제서비스
  - 침해위협 탐지 분석 서비스
- NMS 기반의 네트워크, 시스템 상태 모니터링 서비스
  - 네트워크 장비 CPU, 메모리, 장애여부 등 24시간 감시 및 SMS, 전화 자동 통보 서비스
- 최신 취약점, 분석정보 등 신속한 정보공유를 위한 위협정보 공유 서비스
  - 정보공유 포털 운영
- 보안 이벤트 및 분석 보고서(일간/월간) 제공

보안관제 프로세스

기대효과



보안관제 서비스 종류

보안 관제 서비스 종류

F/W 관제서비스 (Managed Firewall Service)

- 방화벽 가용성 모니터링(CPU, Memory 등)
- 방화벽 장애 여부 모니터링
- 장애시 24시간 자동 대응(SMS, 전화)

F/W UTM 관제서비스 (Managed UTM Service)

- 방화벽 가용성 모니터링
- 방화벽에서 제공하는 IPS, Anti-Virus 분석 및 모니터링

WAF 관제서비스 (Managed WAF Service)

- Bots 및 기타 공격 도구를 통한 자동화 공격 차단
- OWASP TOP 10 Web Application 공격 분석 및 모니터링

NMS 관제서비스 (Network Management Service)

- 네트워크 장비에 대한 가용성 모니터링 (CPU, Memory, Port등)
- 네트워크 장비 장애 여부 모니터링
- 장애시 24시간 자동 대응(SMS, 전화)

안티 랜섬웨어 서비스 (Anti-ransomware Service)

- 행위 기반의 차세대 랜섬웨어 탐지·차단 서비스
- 원본파일 자동백업/복구, 프로세스>서비스> 커널레벨 3단계방어

정보 공유 서비스

일간 레포트 제공 (Daily Analysis Report)

- 일간 분석보고서 / NMS 장애 보고서 제공

정보공유 포털 서비스 (Information Sharing Portal Service)

- 신규 취약점, 보안뉴스, 보안공지 등 제공

서비스 준비중

악성메일 모의훈련 서비스 (Malicious Email Training Service)

- 기업내 악성코드 감염 방지 이메일 훈련 서비스
- 모의훈련을 통한 직원들의 피해 예방 및 보안의식 제고

홈페이지 모니터링 서비스 (Homepage Monitoring Service)

- 홈페이지 서비스에 대한 장애 여부 모니터링

지능형 AI 분석 서비스 (Intelligence AI Analysis Service)

- 기존 시그니처 방식 + 차세대 AI 분석 솔루션 적용
- 기존 방식으로 탐지되는 않은 변형된 신규 침해위협 탐지
- HTTP 구문분석을 통한 웹공격 자동 분석

㈜오픈베이스
문의하실 곳
주소 서울시 서초구 양재동 매헌로 16 하이브랜드 빌딩 4F 홈페이지 www.openbase.co.kr
메일 soc@openbase.co.kr 유선 02-3404-5671