IGLOO

WEBMON

종합 모니터링을 통해 웹사이트·홈페이지 위변조 발생을 탐지하는

홈페이지 위변조 모니터링 솔루션

Background

웹을 활용한 비즈니스가 기업 운영에 있어 선택이 아닌 필수가 되었습니다.

IT 관리자가 운영해야 하는 웹사이트는 점차 많아지고 있으며, 그에 따라 관리의 중요성 또한 높아지고 있습니다.
위변조 탐지 성능 뿐만 아니라 위변조 여부에 대한 분석 기능을 제공하여 운영자의 업무 효율성을 높임은 물론
침해사고 발생시 즉각 대응 및 보고가 가능한 운영환경을 제공해야 합니다.

Overview

오픈 서비스인 웹은 항상 위험에 노출되어 있습니다.

24시간 365일 빈틈 없이 웹사이트·홈페이지를 모니터링하는 웹몬(WEBMON) 솔루션 도입을 통해, 운영 중인 홈페이지의 위변조 발생 여부를 실시간 탐지하고 이상 행위 포착 시 선제적으로 대응 및 보고할 수 있습니다. 또한 유연한 탐지 정책 적용 및 다양한 탐지 이력 점검으로 홈페이지 통합 관리의 효율성을 극대화할 수 있습니다.

외부 위험성

- 해킹을 통한 악성코드 삽입
- 웹사이트·홈페이지 위변조
- 악성코드 유포지로 악용
- 사전 차단 유형의 보안대책 한계
- 늦은 인지로 인한 2차 피해 위험

물적 위험성

- 네트워크인터페이스카드(NIC), 전원 등 하드웨어 불량
- 네트워크 장비 설정 이상 등
- 기타 웹 서비스의 물리적 구간에 발생 가능한 위험성

인적 위험성

- 관리자, 운영자의 사소한 실수, 계획되지 않은 작업
- 운영 서비스 안전 불감증
- 파악되지 않은 영역의 위험성

Why WEBMON

01

보안성 강화

웹사이트 위변조 탐지 관리

해킹을 통한 악성코드 삽입 등 외부 공격 위험성에 노출되어 있는 고객사 웹사이트의 위변조를 탐지하여 웹서비스의 보안성 강화

02

서비스 연속성 보장

웹서비스의 안정적인 실시간 운영관리

웹사이트의 접속 장애 및 이상 징후 판단으로 고객사의 홈페이지가 안정적으로 운영되고 접속될 수 있도록 서비스 연속성 보장

03

관리의 편의성

사용자 접근관리 및 이슈사항에 대한 직관적인 모니터링 운영환경

감시 대상 사이트를 지속적으로 모니터링하여 침해사고 발생 시 즉각적인 대응 및 보고가 가능한 운영환경을 제공하여 편의성 보장

Features

01 대시보드 기능

- 사이트/그룹/통합 대시보드를 통한 직관적인 모니터링 환경 제공
- 보안/장애 알람 이벤트 처리 및 분석이 가능한 사이트별 종합 정보 제공
- 크롤러 상태 및 시스템 자원 정보 제공
- 실시간 이벤트 기반 사이트의 상태 정보 제공
- 최근 이벤트에 대한 상태 및 추이 그래프 제공

02 모니터링 및 분석 기능

- 탐지 정책에 의해 탐지된 이벤트 분석 및 처리
- 웹페이지 화면 캡처를 통한 증적 자료 저장
- 심층 분석을 통한 장애 이벤트 상세 분석 조회
- 외부 API를 통한 구글링 노출 정보 저장 및 조회
- 현재와 이전 소스코드의 라인 단위 변경 비교
- 이벤트 데이터 상세내역 및 현황 통계 조회
- 추이 분석 데이터를 통한 알람 이벤트 시각화 조회

03 통계 기능

- 사이트별 이벤트 현황 통계 차트 제공
- 사이트별 월간 분석 및 알람 통계 제공

04 보안 탐지 기능

- 파일 문자열 변경에 대한 임계값 초과 탐지
- 해시 코드 기반 이미지 파일 생성 및 변경 탐지
- 서브(1Depth) URL 자동 추출 및 이상 탐지
- 파일 사이즈 변경에 대한 임계값 초과 탐지
- 패턴 매칭 기반 웹페이지 이상 문자열 탐지
- 외부 API(Google Safe Browsing)를 통해 위험성 있는 URL 링크 식별 탐지

05 장애 탐지 기능

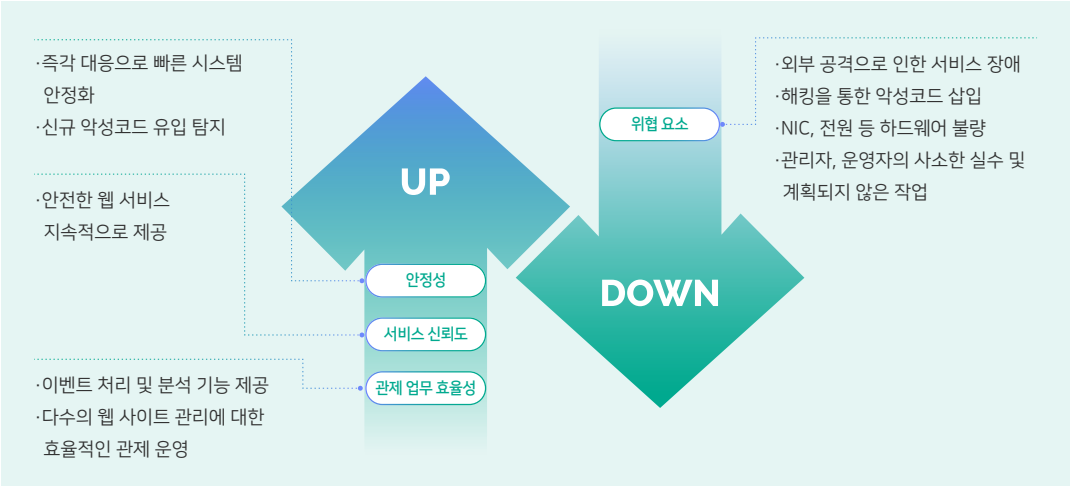
- 접속 상태(오류, 단절) 체크 및 이상 탐지
- 소스코드의 최소 파일 사이즈 체크 및 이상 탐지
- 접속 시간 체크 및 접속 지연 상태 탐지
- DNS 정보(IP, 응답시간) 체크 및 이상 탐지

06 시스템 관리 기능

- 사용자 권한 설정 관리
- 사용자 사용 이력 조회 관리
- 사이트별 크롤러 수집 설정 및 상태 관리
- 사용자 공지사항 관리
- 사이트 및 사이트 그룹에 대한 관리
- 이벤트 탐지 정책 설정 및 예외 처리 관리

Benefits

홈페이지 위변조 모니터링 시스템 도입 시 서비스 운영환경 개선으로 외부의 위협 요소에 대한 즉각 대응을 통해 안정성, 서비스 신뢰도, 업무 효율성 등을 높이는 기대효과가 있습니다.



1999년 보안 벤처 기업으로 시작한 이글루코퍼레이션은 국내 최초 보안 정보 및 이벤트 관리(SIEM) 솔루션을 시작으로 수많은 정보보호 핵심 중추 기관과 기업에 보안 솔루션 및 서비스를 제공하며 정보보안 시장의 성장을 이끌어왔습니다. 또한, 디지털 전환 시대 흐름에 맞는 꾸준한 기술 고도화 및 미래 기술 준비를 통해 사업 영역을 확장해 나가며 보안을 넘어 인공지능, 클라우드, 빅데이터 분야를 아우르는 종합 IT 기업으로 성장했습니다. 이글루코퍼레이션은 세계의 고객에게 고유의 보안과 데이터 역량에 기반한 최적의 솔루션, 서비스를 제공하며 급변하는 비즈니스 환경에 최적화된 혁신적인 디지털 경험을 선사하는 기업으로 나아가고자 합니다.

서울특별시 송파구 정의로8길 7 한스빌딩 6층 | TEL 02-3452-8814 | FAX 02-3452-8815 | www.igloo.co.kr

IGLOO