

CYREN

Sandbox Array



제품 소개

끊임없이 진화하는 APT 공격과 악성코드, 랜섬웨어 등은 기존 백신과 1세대 Sandbox를 우회하여 공격합니다. CYREN Sandbox array의 글로벌 데이터 수집-사전탐지-분석기술은 알려지지 않은 APT 공격과 악성코드에 가장 빠르고 효과적으로 대응할 수 있습니다.



CYREN 클라우드 Sandbox array API를 이용한 APT 공격 방어

사이버 공격은 끊임없이 진화하고 있으며, 기존 백신처럼 1세대 보안 수단으로는 모든 위협에 대응할 수 없습니다. 또한, 이러한 공격의 60%는 중소기업에 대상으로 하고 있습니다. CYREN Sandbox array는 보안 벤더 및 중소기업에서도 간편하게 도입하여 APT 공격에 대응할 수 있는 클라우드 기반의 Sandbox입니다.

주요기능

1 CYREN Sandbox array 도입 효과

- API 연동만으로 도입 가능하여 개발 리소스가 대폭 감소됩니다.
- 사용한 만큼만 비용 지불하여 도입비용이 대폭 감소합니다.
- 각종 보안제품에 빠른 적용 가능합니다.

2 정교한 분석 기술

- 의심 파일, 악성코드, 이메일, URL 등을 다차원 분석하여 리포트를 제공합니다.
- 정적분석, 다중시간 실행, 동적 분석 등으로 모든 APT 공격 대응 가능합니다.

3 유지보수 비용 절감

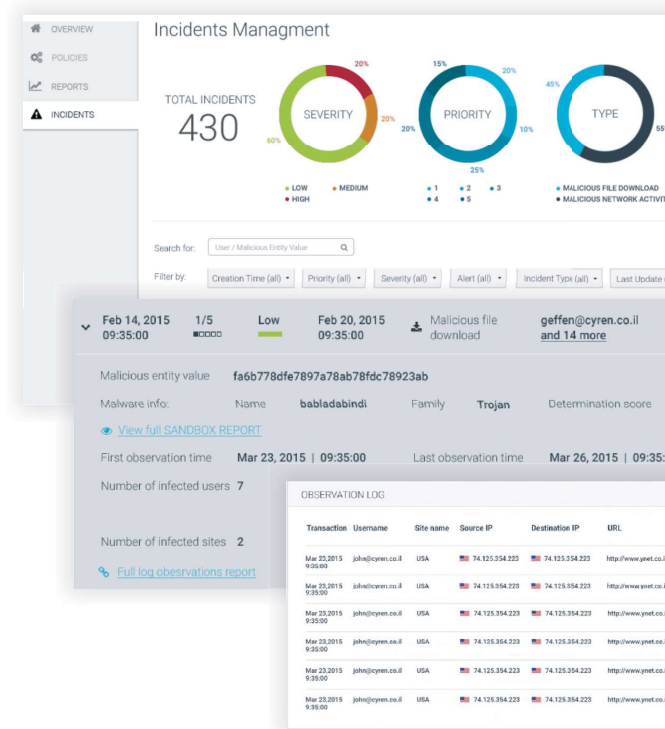
- Sandbox Array는 도입고객이 업데이트, 패치 등을 별도 적용할 필요가 없는 클라우드 기반의 플랫폼입니다.

4 확장성

- 트래픽과 사용량에 관계 없는 확장성을 제공하여 피크타임에 집중되는 부하가 없습니다.
- 시스템 확장 시 추가 장비 도입 없이 즉시 확장 가능합니다.

5 관리자 리포트

- 관리용 대시보드 제공, APT 공격 분석 리포트 제공
- 의심스러운 파일의 네트워크 활동 내역, 시스템 파일 변경내역, 메모리 분석내역 및 연결 국가 등 세부내역을 제공하여 기업에서 효율적인 보안정책을 수립할 수 있습니다.



(CYREN Sandbox Array 사건 관리 대시보드, Forensic 리포트)

제품강점



탐지 성능

- 다양한 OS 동시 비교 분석
- 물리 HW 비교 분석
- AI 기술을 기반으로 자동화된 분석
- 다단계 분석을 통하여 빈틈없는 탐지력을 제공



무한 확장성

- 어떠한 경우에도 중지 없는 고가용성
- 피크타임에도 성능 저하 없는 확장성
- 글로벌 데이터센터 배치로 해외에서도 빠르고 정확한 분석



빠른 분석 속도

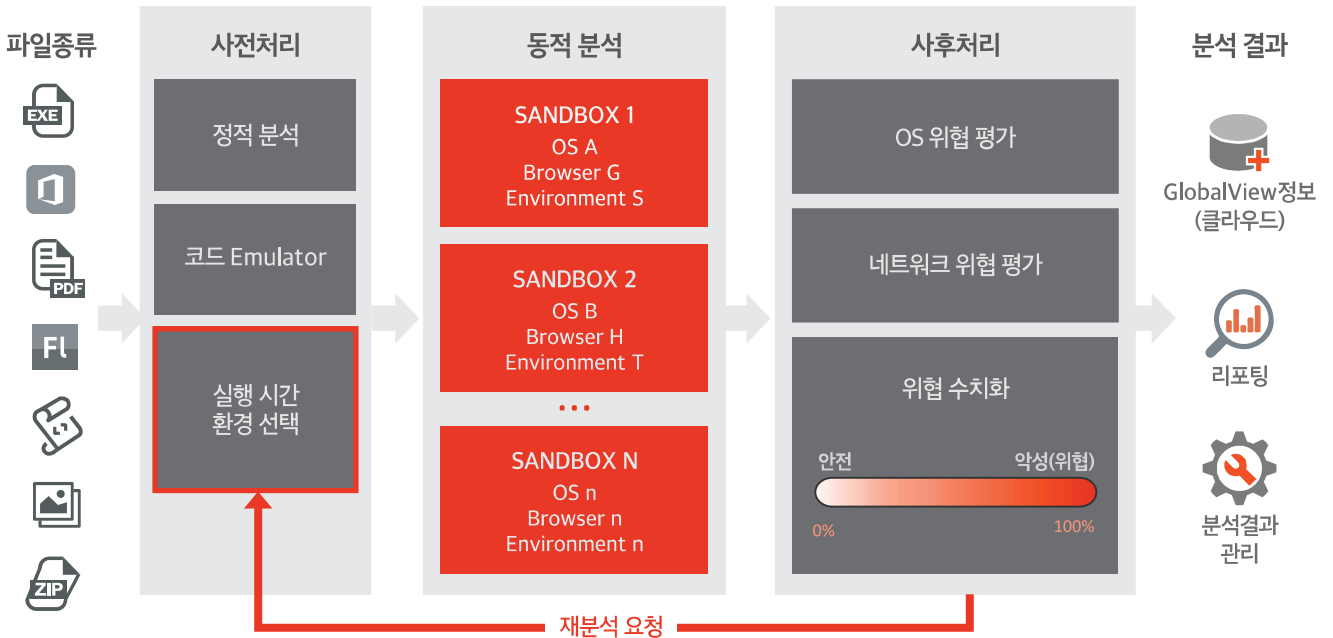
- 다양한 OS 환경에서 동시에 동적 분석을 수행하여 가장 빠른 분석 결과 제공
- 세계에서 가장 많은 분석 DB 보유



상세한 리포트

- 다양한 환경에서 분석된 결과를 통합 리포트로 제공
- 위협도 레벨, 파일분석 결과 등을 제공하여 통합 위협 정보를 리포트

Sandbox array 동작방식



1 예측 분석

예측/정적분석 기술로 대상 파일의 예상 행동을 예상하여 적합한 Sandbox array를 선택

2 동적 분석

선택된 각 Sandbox에서 동적 분석을 수행하여 악의적인 행동 감시 및 모든 행위 예측

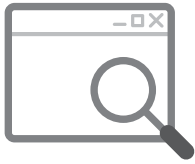
3 종합 분석

다양한 운영체제, 브라우저, 가상환경, 물리 환경 등에서 분석된 이상 행위, 행동 분석 결과를 종합적인 위험점수로 판단

4 정보제공

분석된 결과를 바탕으로 리포트 생성 후 제공

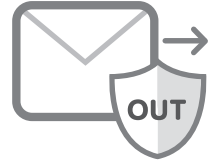
CYREN



URL Filtering



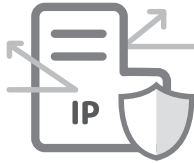
Anti Spam
In bound



Anti Spam
Out bound



Anti Virus



IP Reputation



Phishing
Feed



Virus Outbreak
Detection



Mobile Security



Sandbox Array



글로벌 OEM팀

☎ 전화: 02-6051-1042 ✉ 이메일: cyren@jiran.com

(고객지원시간: 평일 오전 09:00 ~ 오후 06:00)