연구진 및 매거진

지식채널e　EBS

EBS방송　신문/기사　세미나(패널토론)

THE UNIVERSITY OF CHICAGO　Carnegie Mellon University

카네기멜론/시카고 대학 연구진 공동 개발
전사 임직원의 단일 솔루션 연구/개발

JASON an AhnLab Company

SECURITY INTELLIGENCE

Insight in everything we analyze

고객사 / 파트너

그룹사　삼성전자　SAMSUNG BIOLOGICS　삼성전기　LG이노텍　LG생활건강　SK hynix　GS Mbiz　CJ 엘스케어　CJ 올리브네트웍스　HYUNDAI AutoEver

금융사　농협　삼성카드CS　애큐온　DGB캐피탈　MIRAE ASSET　Kbank

기업　HYBE　kakaogames　GC녹십자　SOUL SYSTEMS　ASTRON SECURITY

공공기관　HF 한국주택금융공사　국군사이버사령부　국방통합데이터센터　한국신용정보원 Korea Credit Information Services

JASON an AhnLab Company

제이슨은 IT시스템 이상징후(보안위협, 정보유출 그리고 IT장애 등)를 통합 관리함과 동시에 완전 자동을 위한 시스템과 서비스를 제공합니다.

서울특별시 마포구 양화로 61 두암빌딩 7,8층 / 02-6402-4640 / hjlee@jasonsystem.co.kr

AI 이상징후시스템

JMachine

AI / TDIR / SIEM / UEBA / PRIVACY / LOG

IT Security. IT Operation.

www.jasonsystem.co.kr

도입효과 *Implementation Effect*

JMachine 이상징후 특장점

통합보안 체계구현
보안관제(SIEM), 내부자정보유출(UEBA), 개인정보오남용(PRIVACY) 탐지/대응 관리에 대한 시스템 통합 및 UI 단일화

인공지능 정밀탐지 및 종합분석
인공지능은 단순 임계치 기반의 탐지체계를 AI학습과 자동탐지 체계로 고도화
위협탐지의 AI 정밀화, 탐지결과의 AI 종합분석 실현

전략적 내·외부 위협 관리
내/외부 보안위협에 대한 전략적 보안운영 관리 가능
예시) 해킹공격으로 탈취한 직원계정(SIEM)으로 다운로드 받은 대량 고객정보(PRIVACY)를 외부로 무단 반출(UEBA)하는 행위

AI 자동대응
종합분석한 AI는 보안알림, 정보유출자 소명요청, 침해공격 티케팅, SOAR로의 연계대응 등을 자동화 처리

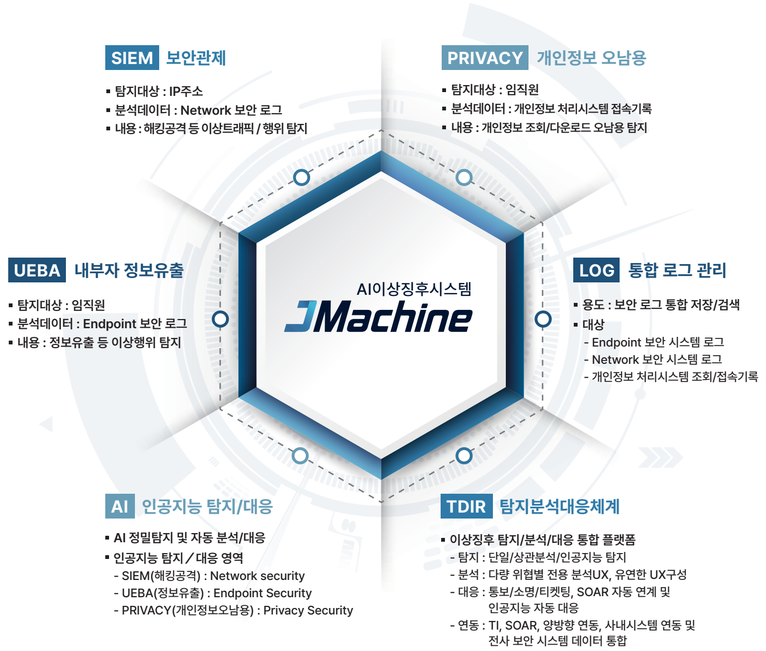
JSearch 빅 데이터 특장점

빅데이터 확장성
저장서버 추가 시, 저장 용량 무제한 확장
검색서버 추가 시, 검색 및 분석 부하 분산처리
전세계 모든 시스템 데이터를 수집 가능한 모듈 제공

빅데이터 안정성
클러스터링 기술은 서버 장애 시에도 데이터는 안전하게 보관되며,
데이터 수집/저장/검색 기능의 연속성 유지

빅데이터 시각화
다양한 차트/통계/데이터의 시각화 제공
3차원 토폴로지 대시보드 기능 제공
인공지능 분석결과 차트 제공

시스템 용도 *System Purpose*



SIEM 보안관제
- 탐지대상 : IP주소
- 분석데이터 : Network 보안 로그
- 내용 : 해킹공격 등 이상트래픽 / 행위 탐지

PRIVACY 개인정보 오남용
- 탐지대상 : 임직원
- 분석데이터 : 개인정보 처리시스템 접속기록
- 내용 : 개인정보 조회/다운로드 오남용 탐지

UEBA 내부자 정보유출
- 탐지대상 : 임직원
- 분석데이터 : Endpoint 보안 로그
- 내용 : 정보유출 등 이상행위 탐지

LOG 통합 로그 관리
- 용도 : 보안 로그 통합 저장/검색
- 대상
  - Endpoint 보안 시스템 로그
  - Network 보안 시스템 로그
  - 개인정보 처리시스템 조회/접속기록

AI 인공지능 탐지/대응
- AI 정밀탐지 및 자동 분석/대응
- 인공지능 탐지 / 대응 영역
  - SIEM(해킹공격) : Network security
  - UEBA(정보유출) : Endpoint Security
  - PRIVACY(개인정보오남용) : Privacy Security

TDIR 탐지분석대응체계
- 이상징후 탐지/분석/대응 통합 플랫폼
  - 탐지 : 단일/상관분석/인공지능 탐지
  - 분석 : 다량 위협별 전용 분석UX, 유연한 UX구성
  - 대응 : 통보/소명/티켓팅, SOAR 자동 연계 및 인공지능 자동 대응
  - 연동 : TI, SOAR, 양방향 연동, 사내시스템 연동 및 전사 보안 시스템 데이터 통합

시스템 모델 *System Model*

시스템종류	AI	SIEM / 정보유출 개인정보오남용	로그 통합 관리
주요 기술	인공지능	이상징후	빅데이터
제품 모델	JMachine 20/50/100	JMachine Lite	JSearch
제품 기능	▪ AI Risk Scoring (종합 분석) ▪ AI 시나리오 탐지 ▪ AI 분석 (유사도, 관계도) ▪ AI 대응 (정오탐 의결 및 자동대응) ▪ AI 파일 유통 추적 ▪ XAI *JMachine Lite기능 전체 포함	▪ 시나리오 탐지 ▪ 이벤트 분석 ▪ 대시보드 / 보고서 ▪ 대응 (소명, 조사CASE, 통보) ▪ 알림 (Email, SMS, SNS, 메신저) *JSearch 기능 전체 포함	▪ 빅데이터 수집 보안/업무시스템 및 클라우드, 온프라미스의 로그 및 성능정보 ▪ 빅데이터 저장/보관/검색 클러스링 데이터 복제저장 1년이상 장기간 보관 및 검색 ▪ 빅데이터 및 통계 정보의 시각화

주요기능 *Key Features*

ARTIFCIAL INTELLIGENCE
빅데이터와 인공지능 기술을 통한 이상징후 관제업무 자동화 및 미래 예측 관제
담당자가 직접 화면을 구성할 수 있는 사용자 정의 분석 화면 제공

01 AI 정밀 탐지
정밀 탐지 주요 기능 4가지
*탐지대상 : IP주소 및 임직원

- ☑ 기밀정보 유통 및 유출경로 분석
- ☑ 전사 대비 이상행위 탐지
- ☑ 시간 대별 이상행위 탐지
- ☑ 행위 패턴 이상 탐지

02 AI 자동 대응
AI 분석결과에 따른 4가지 자동 대응 조치

- ☑ 내부자 유출 : AI 자동 소명요청
- ☑ 해킹공격 : AI 자동 티켓팅
- ☑ 일반보안위협 : AI 자동 통보
- ☑ SOAR : AI 양방향 연계

03 보고서
정기점검 및 보고업무 자동화

- ☑ 담당자별 보고서 자동 발송
- ☑ 보고서 템플릿 기능
- ☑ 보고서 내용 모듈화

04 이벤트 대응 애널라이저
위협별 전용 분석화면 신속한 위협분석

- ☑ 분석에 필요한 필수정보 자동 제공
- ☑ 위협별 분석화면 자동 구성
- ☑ 다양한 차트 등 시각화 제공

05 대시보드
유연한 분석 UX 분석 정보 및 시각화의 유연성

- ☑ 관리자 대시보드
- ☑ 운영자 대시보드
- ☑ 차트형 대시보드
- ☑ 2차원 토폴로지 대시보드
- ☑ 3차원 토폴로지 대시보드

06 AI 종합 분석
AI Risk Scoring의 종합 분석 6가지 관점

- ☑ 매우 위험한 행위
- ☑ 다량의 위험 행위
- ☑ 과거 대비 이상행위
- ☑ 팀원 대비 이상행위
- ☑ 고위험군 탐지대상
- ☑ 기밀정보 취급 여부