Integrated Security

인공지능 기반 차세대 통합보안 솔루션

알약 XDR

ESTSECURITY

알약 XDR

중소/중견 및 대규모 엔터프라이즈 환경에서
고객 운영상 솔루션 기반의 맞춤형 통합보안 솔루션

알약 XDR은 다양한 보안 데이터를 통합해 실시간으로 위협을 탐지하고 자동 대응하는 차세대 보안 솔루션입니다.
다층적 분석과 공격 표면 관리로 숨겨진 위협까지 식별하며 보안 환경을 효율적으로 보호합니다.

주요기능

통합 데이터 분석 및 가시화

보안 데이터 통합으로 자산 상태 및 위협 실시간 모니터링

공격 경로, 심각도 등 다양한 시각화 옵션과 핵심 정보 제공(Cyber kill-chain, MITRE ATT&CK 등)

공격표면관리(ASM)

자산 및 주요 객체 식별과 실시간 추적

Star Graph, Tree Graph, Map 등을 통해 자산 간 연결 상태 파악

포트 변경 이력 추출, 불필요한 노드 관리로 공격 표면 축소

위협 대응 자동화

사전 정의된 6,500건 이상 규칙과 알약 전용 Playbook으로 일관된 보안 대응 수행

악성파일 격리, 침입 시도 IP 차단 등 실시간 대응 및 자동화로 보안팀 업무 효율화

Incident 관리

보안 이벤트 감지 및 신속한 대응 프로세스 제공

상세 로그와 분석 결과 기반 Incident 대응 지원

자체 탐지 패턴 및 분석 자동화

1차 상관 분석 및 경보
2차 자체 시그니처 탐지
3차 인공지능 탐지 경보

위협 인텔리전스

TIP 서비스/ 평판 수집
TIP 내장(KISA C-TAS, KCTI 등), 자체 봇 평판 정보 수집 제공

제품특장점

유연한 보안 구성 지원

단일 구성 All in One 싱글모드 지원
*센서가 되는 웹 컴포넌트 등의 보안 장비는 별도로 갖춰진 환경에서 XDR 단일 구성 가능

다중 계층 구성(멀티 로드 밸런싱 모드) 지원
*고객 환경에 따라 컨설팅 후 옵션으로 구성 가능

실시간 이벤트 모니터링

인덱스(색인)를 이용한 초고속 검색 속도를 통해 탐지 및 응답 제공

정오탐 분석

1차 연동장비(IPS, WAF 등)의 침입탐지 이벤트를 자체적으로 재분석하며 2만 개 이상의 침입탐지패턴을 활용한 2차 정오탐 검증 기능 제공

3D 대쉬보드

사이버 위협 경보단계 동적 3D 공격 정보, 사이버 킬 체인, T-section, MITRE ATT&CK, 실시간 탐지 이벤트, 추이 그래프 우려 지점 상관분석, NMS 등의 정보를 한눈에 확인하여 일일 사이버 보안 기상도로 활용 가능

도입효과

보안 위협 관리

침해 사고 분석에 필요한 다양한 툴
생성형 AI 기반 공격 도움말/포트 분석 데이터베이스
/공격자 추적 인공지능 분석 결과 등 제공으로 즉시 대응 가능

이동 매체를 통한 긴급 대응

스마트 모빌리티 지원
휴대용 디바이스에서 보안 SNS 메신저를 통한 통합 보안 관리
이벤트 확인 및 실시간 모니터링/분석/설정/조치 가능

위협 대응 시간 단축

위협 발생 시 자동화된 대응으로 즉각적인 차단 및 조치

고급화된 분석 기법과 AI/ML 기반 빠르고 정확한 위협 확인 및 분석

최소화된 수작업으로 보안팀의 업무 효율화 증대

보안 가시성 향상

다양한 보안 데이터를 통합하여 전체 환경을 한눈에 파악

확산 경로를 시각화하여 숨겨진 위협까지 식별 가능

보안 사각지대의 최소화 및 위협 탐지의 정확도 상승

자체 서버 취약성 점검 및 관리

ISMS 기반 자체 서버 취약성 점검 엔진을 통해 침해 사고 이벤트 분석 시각화 제공

발견된 취약점에 대해 원스톱 관리로 편의성 증대

유연한 스마트 보고서 생성 가능

기간 및 시간대별 인공지능 이벤트 맞춤형 분석 보고서 제공

인공지능 정오탐 분석을 통해 관리자의 이벤트 처리 의사결정 시간 단축

사용자 정의 자동화 보고서 기능 제공

도입사례

EBS 동국대학교 부산외국어대학교 동아대학교 상명대학교 아주대학교 연성대학교 세계사이버대학 S-OIL TotalEnergies KEPCO 전력연구원 CMT 씨엠티정보통신㈜ 서울성심병원 MEGAZONE CLOUD BESPIN GLOBAL 대한민국해군 KITRI 한국정보기술연구원 서울인쇄센터 이천시 OK금융그룹 smart저축은행 상상인플러스저축은행 주식회사 안전대부 레이디퍼스트론 kakaopay securities 키움YES저축은행 happy cappy KI CORES 엘로우캐피탈대부(주) 풀잎론 CashBucks

제품 필요성

이슈	해결
다수의 보안 솔루션 간 데이터 분리로 가시성 부족 각 솔루션이 개별적으로 동작해 위협 탐지 및 분석 시 누락 가능성 증가	**통합된 보안 플랫폼 제공 :** 다양한 보안 솔루션(AV, FW, IPS 등) 데이터를 알약 XDR에서 통합 분석하여 전체 네트워크와 엔드포인트 가시성 제공 **중앙화된 대시보드 :** 모든 데이터를 한 곳에서 실시간 모니터링 가능, 분석 효율성 향상
위협 탐지와 대응 속도 저하 위협 탐지가 지연되거나 분석이 부족해 침해 사고 발생 가능성 증가	**AI 기반 위협 분석 :** 머신러닝 알고리즘을 활용해 복잡한 위협 (APT, 파일리스 공격 등)을 탐지하고, 수동 개입 없이 자동화된 위협 차단 수행 **Playbook을 통한 자동화 :** 탐지된 위협에 대해 사전 정의된 Playbook에 따라 자동화된 대응 수행, 침해 대응 시간 단축
보안 경보 과부하로 인한 운영 효율성 저하 오탐이 많아 중요한 경보를 놓치거나 처리 속도가 느려짐	**경보 관리 최적화 :** 고위험 경보와 저위험 경보를 자동 분류화 해 SOC 팀의 업무 부담 감소 **우선순위 기반 처리 :** 중요 경보를 우선적으로 대응하고 오탐을 줄여 대응 리소스 최적화
보안 인력 부족으로 위협 대응의 어려움 제한된 인력으로 인해 수동 분석과 대응에 과도한 시간이 소요됨	**자동화된 프로세스 :** 반복적인 작업을 자동화하여 보안 인력의 효율성을 극대화, 리포트 자동 생성 **운영 효율성 향상 :** 자동화를 통해 운영 리소스를 줄이고 중요한 작업에 집중할 수 있는 환경 조성

ALYac XDR

ALYac Extended Detection and Response

이스트시큐리티(주) 서울시 서초구 반포대로 3 이스트빌딩 (우)06711

영업문의 : 02-583-4616 기술지원문의 : 02-441-2050

이메일 : alyacxdr@estsecurity.com 홈페이지 : www.estsecurity.com/product/xdr