RSA NetWitness

실시간 이상/침해행위를 탐지 및 분석하는
SIEM+NDR+EDR 통합 기반 차세대 보안관제 플랫폼

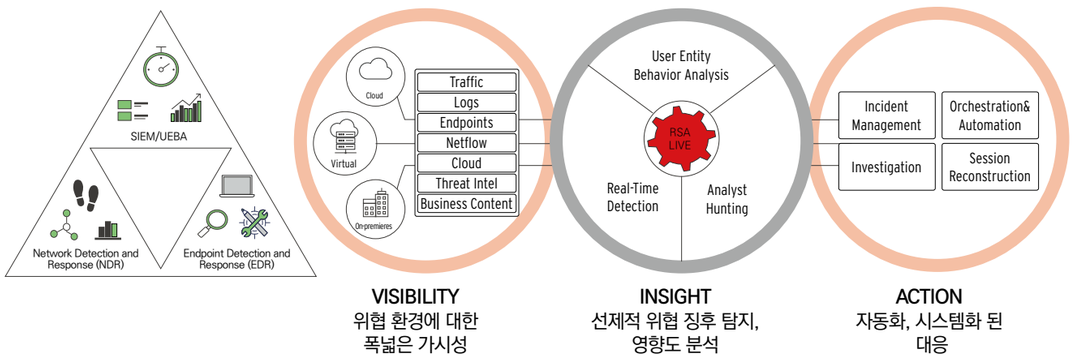
인프라에서 수집 가능한 모든 데이터(Log, Network, Endpoint)를 수집하여,
실시간으로 이상행위를 탐지, 다양한 메타데이터를 기반으로 분석,
플레이북을 활용한 대응을 제공하는 차세대 통합 보안 관제 솔루션.
온프레미스, 가상화, 클라우드등 다양한 인프라 환경을 지원하며,
SaaS 영역으로 확장.

제조사 : RSA

제품 개요

· Gartner's SOC Visibility Triad에서 권고하는 3가지 핵심 보안 관제 기능 (SIEM, NDR, EDR)을 단일 플랫폼으로 통합 제공 => XDR (eXtended Detection & Response)
· 네트워크, 로그, 엔드포인트에 이르기까지 완벽한 가시성을 통해 실시간으로 이상 행위를 탐지 및 분석하는 효율적인 보안 관제 환경 제공
· 이상행위 탐지는 시그니처 룰 탐지, 멀티 이벤트 상관분석(correlation) 탐지, AI머신러닝(UEBA) 탐지등을 활용하여 촘촘한 탐지체계 제공
· Orchestrator(SOAR)를 통해 탐지된 위협의 체계적인 분석(플레이북)과 관제 자동화(Automation)을 통해 관제의 효율성 증대

Gatner's SOC Visibility Triad **NetWitness Platform 차세대 보안 관제 플랫폼**



특장점

검증된 XDR 솔루션	증거 기반으로 실시간 위협/이상 행위 탐지 및 분석	관제 고도화 및 APT 대응 고도화에 기여
미국 국토안보부 산하 사이버보안센터가 개발한 '실시간으로 네트워크내 이상행위를 분석하는 네트워크 포렌식 솔루션' 으로 시작하여, 네트워크 뿐만 아니라 로그, 엔드포인트 등 모든 이벤트를 통합하여 포괄적 가시성을 제공하며, 이상행위를 상관 분석 룰과 AI머신러닝기능을 통해 실시간으로 탐지하고 대응 (NDR + SIEM + EDR + UEBA => XDR)	패킷 및 로그, 엔드포인트 데이터를 실시간으로 수집하며, 마찬가지로 실시간으로 네트워크 및 로그, 넷플로우, 엔드포인트 영역의 위협 및 이상 행위를 탐지. 이때, 사후 분석이 아닌 실시간 분석으로, 공격이 실제로 이어지기전에 보안 및 관제 담당자분들이 보안 위협 행위에 빠른 대응 및 조치하는데 기여	기업/기관 전산망 전반에 대한 실시간 가시성을 제공하기에 보안성을 제고. 아울러 기존 도입한 APT 대응 솔루션을 우회 및 변종 하여 들어오는 공격까지 실시간 탐지 및 분석하여, 현재 보유하고 있는 APT 대응 솔루션을 더욱 효과적으로 활용할 수 있게끔 보완

주요 기능

NDR (Network Detection & Response)	관련 분야 국내외 기업, 금융, 정부 및 공공기관 최다 구축사례를 보유한 검증된 솔루션으로, 증거 기반으로 실시간 네트워크 이상행위를 수집, 탐지, 분석, 대응 기능을 제공
SIEM (Security Information & Event Management)	다양한 보안 솔루션 및 IT 자산의 로그를 실시간으로 수집하여 이상행위를 탐지하고 분석, 대응하는 기능을 제공
EDR (Endpoint Detection & Response)	엔드포인트의 스캔 정보를 엔드포인트 서버로 전송하여 분석하는 가벼운 에이전트 구조로써, 커널모드 뿐만 아니라 시스템 드라이버 모드까지 스캔하여 이상행위를 수집, 탐지, 분석, 대응 기능을 제공
UEBA (User & Entity Behavior Analytics)	비지도방식의 AI머신러닝를 통해 평상시 행위를 학습하여 기준선에서 벗어난 의심행위를 자동으로 탐지하고, 다양한 보안 모델링을 적용하여 오탐을 줄여줌
SOAR (Security Orchestration, Automation and Response)	탐지된 사건의 처리 과정을 체계화(플레이북)하여 이상행위 분석의 품질을 향상시키고, 처리과정에 반복되고 정의가능한 이벤트를 자동화(오토메이션)하여 관제 효율성을 높여줌

도입효과

01 공격자가 전산망과 업무에 피해를 입히기 이전에 탐지, 분석 및 대응

02 침해사건에 대한 면밀한 조사, 보안대응 우선순위 설정 및 효과적 사후 조치

03 가용 보안인력의 최적 운영참여로 예측하지 못한 미래 위협 대응

04 전체 전산망 가시성 확보와 업무 연계로 기존 도입된 보안 솔루션의 활용성 개선