보안관제의 진화 전형 보여주는 'RSA NetWitness'

NDR·SIEM 넘어 EDR·UEBA까지 통합

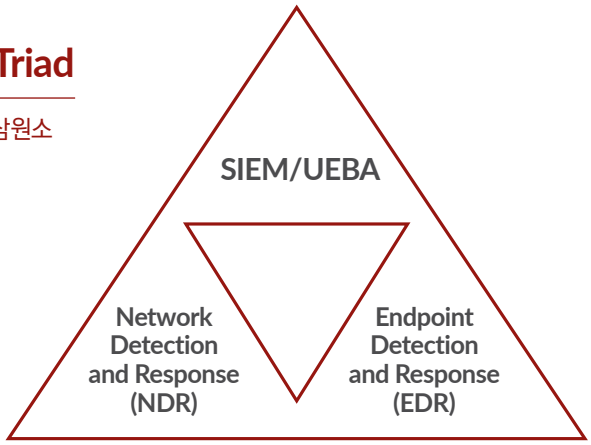
통합보안관제 플랫폼이 빠르게 진화하고 있다.

사이버위협이 계속 정교해지고 침입 경로도 다양화되면서 보안사고를 부르는 위협들을 총체적으로 수집하기 위해 네트워크부터 엔드포인트까지 망라하는 것은 물론, 행위 분석과 머신러닝 분석 기술까지 활용해 빠르고 지능적으로 분석해 효과적으로 탐지·대응할 수 있는 통합 플랫폼으로 변모하고 있다.

가트너 역시 지난 2019년에 발간한 위협 탐지 대응을 위한 네트워크 중심 접근방식 적용 리포트에서 '보안운영센터(SOC, 보안관제센터) 가시성 삼원소(SOC Visibility Triad)'을 제시했다. 그 세 가지 핵심 구성요소가 바로 네트워크 탐지 대응(NDR), 보안정보이벤트관리(SIEM)와 사용자·엔터티 행위 분석(UEBA), 엔드포인트 위협 탐지 대응(EDR)이다.

Gartner's SOC Visibility Triad

가트너가 제시한 가시성 삼원소



Source: Gartner Report "Applying Network Centric Approaches for Threat Detection and Response"; published in March 2019

네트워크부터 엔드포인트에서 나오는 실시간 패킷·트래픽 정보부터 프로세스, 파일 정보, 로그 등 다양한 데이터를 수집·추출하고 상관분석 해야 이상징후와 위협에 대한 가시성을 빠르게 확보해 대응하는 것이 중요하기 때문이다.

많은 보안업체들이 사이버위협 탐지·분석·대응 플랫폼을 제공하고 있지만, 가트너가 제시하는 이같은 보안관제 플랫폼의 요소를 모두 갖춘 제품으로는 대표적으로 RSA 넷위트니스를 꼽을 수 있다.

RSA 넷위트니스(NetWitness)는 국내에서도 약 10년 전부터공급돼 많은 대기업 제조사와 금융사, 주요 인터넷 기업들이 사용하고 있는 보안 솔루션이다.

NDR에서 SIEM, UEBA, EDR까지, 10년 간 이뤄진 RSA 넷위트니스 플랫폼의 진화

초창기에는 네트워크 보안 모니터링과 분석을 수행하는 플랫폼으로 네트워크 포렌식에 강점을 가진 솔루션으로 선보였다. 네트워크 포렌식 솔루션은 보안사고가 발생한 후 조사·분석 용도로 주로 사용됐다. 시간이 지나면서 RSA 넷위트니스 플랫폼은 모든 트래픽 원본을 저장해 사후 조사·분석에만 활용하는 것이 아니라 실시간 NDR 시스템으로 발전했고, 방화벽과 네트워크 장비 등 주요 시스템에서 나오는 실시간 로그와 이벤트 정보를 취합하고 연관성을 분석해 실시간 경보체계까지 구현하는 보안정보이벤트관리(SIEM) 시스템까지 통합됐다.

이에 더해 엔드포인트 위협 탐지(EDR), 머신러닝 기술이 결합된 사용자·엔터티행위분석(UEBA) 기술까지 합쳐졌다.

기업의 네트워크 경계가 허물어지면서 다방면에서 들어오는 수많은 위협정보를 모아 빠르고 정교하게 분석해 효과적인 보안관제에 필요한 위협 인텔리전스와 폭넓은 가시성을 확보하기 위한 진화라고 할 수 있다.

이에 따라 RSA 넷위트니스는 네트워크 트래픽(패킷·플로우), 로그, 엔드포인트 정보까지 저장하는 동시에 실시간으로 연관성 분석을 수행할 수 있게 됐고, 나아가 머신러닝 기반 분석 기반 위협 탐지까지 가능하게 됐다.

조남용 RSA코리아 이사는 "RSA 넷위트니스는 SOC에서 필요로하는 모든 요소를 '빌트인(Built-in)'하는데 10년 가까운 기간이 걸렸다. 단순히 '볼트온(Bolt-on)'하는 연동 수준의 통합과는 차별화된다"라면서 "모듈화된 방식으로 기업은 필요한 기능만 선택해 편리하게 구축하고 추가할 수 있게 했지만 NDR과 SIEM, EDR이 모두 한몸으로, 데이터베이스(DB)까지 하나로 사용해 매우 상세한 수준의 연관성 분석과 탐지가 가능하다"고 강조했다. 이어 "각자 솔루션별로 탐지해 나중에 모아보고 분석하는 방식과는 정교한 탐지 수준이 다를 수밖에 없다"며 "만일 EDR에서 탐지한 개별 행위만으로는 위험도 수준이 중하로 볼 수 있지만 연관성 분석으로 통합해보면 최상위 위협이라는 것을 판단할 수 있다"고 덧붙였다.

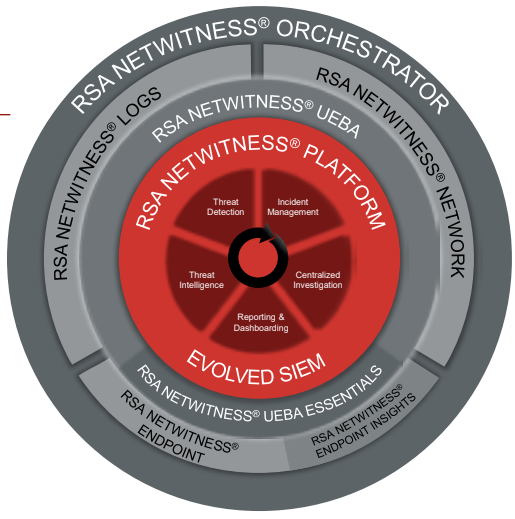
RSA는 지난 2011년 4월 EMC의 보안사업부 당시 넷위트니스를 인수했다. 이후 당시 확보하고 있던 SIEM 솔루션인 'RSA 인비전'과 통합했다. 2012년에는 실리시움시큐리티(Silicium Security)를 인수해 엔드포인트까지 위협 모니터링과 분석 역량을 넓혔다. 이 회사 인수로 RSA는 엔드포인트까지 위협 가시성과 대응능력을 확장했고, 시그니처에 의존하지 않고도 지능형 위협과 그로 인한 영향을 보다 잘 탐지할 수 있는 EDR 기술을 확보해 발빠르게 시장에 출시했다. RSA는 당시 제품명인 '이캣(ECAT)'을 '넷위트니스 엔드포인트'로 변경하고, 연동되는 형태로 제공하다 3년 전 넷위트니스 플랫폼의 구성요소로 완전히 통합했다.

RSA가 가장 최근에 인수한 업체는 임베디드 UEBA 선도업체인 포트스케일(Fortscale)이다. 사이버위협을 더욱 잘 탐지하고 위험성이 큰 위협을 식별해 대응하는 프로세스를 보다 효율적으로 만들기 위한 투자 일환으로 지난 2018년에 인수했다.

이에 더해 RSA는 지난해 보안 운영 자동화 대응(SOAR) 솔루션인 '넷위트니스 오케스트레이터'도 출시해 넷위트니스 플랫폼과 연동해 사용할 수 있도록 제공한다. 이를 통해 대량의 복잡한 위협 분석·처리·대응 처리과정을 자동화해 보안관제 인력과 위협분석 전문가들의 단순 반복 업무 효율성을 높일 수 있다.

RSA NetWitness Platform

RSA의 차세대 보안 관제 플랫폼



모듈화 시스템 구성으로 필요에 따라 쉽게 구축, 단계별 확장 가능해 위협 탐지·대응 수준 고도화

RSA 넷위트니스는 단일화된 통합 플랫폼이지만 네트워크(NDR), 로그(SIEM), 엔드포인트(EDR)와 분석 플랫폼 등 각 기능과 역할에 따라 모듈화된 시스템으로 구성돼 있다. 때문에 기업의 보안 위협 환경과 수준에 따라 필요한 기능을 먼저 구축하고 확대하기 쉽다. 만일 NDR만을 먼저 사용하던 기업이라면 나중에 SIEM이나 EDR 모듈을 추가하거나 연동하기가 쉽다. 이같은 방식으로 단계적으로 보안관제체계를 고도화할 수 있다.

최근 확장 구축 사례가 더 많아지고 있다는 게 RSA코리아의 설명이다. 더욱이 넷위트니스 플랫폼에서 제공하는 다양한 기능을 사용하는 기업들도 늘어나고 있다. 아모레퍼시픽이 대표적으로 넷위트니스 플랫폼을 도입해 세가지 모듈을 사용하고 있다.

아모레퍼시픽 정보보안팀 조재윤 차장은 RSA 본사의 고객사례 인터뷰(영상)에서 "RSA 넷위트니스 플랫폼을 사용하지 않았다면 내부에서 일어나는 공격들을 전혀 볼 수 없는 상황이었고 발견했던 악성코드나 데이터 유출을 보지도 막거나 찾을 수도 없었을 것"이라며 "고객 입장에서는 수집된 개인정보가 안전하게 지켜지는 것 외부에 노출 안된다는 혜택을 얻을 수 있을 것"이라고 설명했다.

조남용 이사는 "많은 고객사들이 RSA 넷위트니스 플랫폼을 도입한 뒤에 특정 위협을 탐지할 수 있게 됐다고 피드백을 해주시는 게 아니라 전체 보안관제가 달라지고, 위협 탐지와 대응 체계의 단계와 수준이 향상됐다는 이야기를 해준다"라면서 "재구매와 추가로 솔루션을 도입하는 비율도 상당히 높다는 점에서 인정을 받고 있다"고 말했다.

한편, RSA는 ▲넷위트니스 플랫폼 외에도 ▲통합위험관리 솔루션 'RSA 아처(Archer)' ▲다중요소인증(MFA) 솔루션인 'RSA 시큐어아이디 액세스(SecureID Access)' ▲온라인 사기방지 솔루션인 'RSA 프로드&리스크 인텔리전스(Fraud and Risk Intelligence)' 제품군을 제공한다. By

RSA코리아
서울 강남구 테헤란로 152 강남파이낸스센터
전화: 02-2125-7000 웹사이트: https://www.rsa.com/ko-kr

RSA

바이라인네트워크
서울특별시 마포구 토정로 5길 30(합정동 356-21번지) 2층
전화: 02-761-1928 이메일: byline@byline.network 취재/글 : 이유지 기자 yjlee@byline.network
웹사이트: byline.network, bylineplus.com

Byline Network SPECIAL REPORT