기술사업화 이슈&마켓

Tech-Biz Issue and Market

디지털뉴딜

출처: Frost & Sullivan Blog (ww2.frost.com) 제 234 호 | 2021.07.26

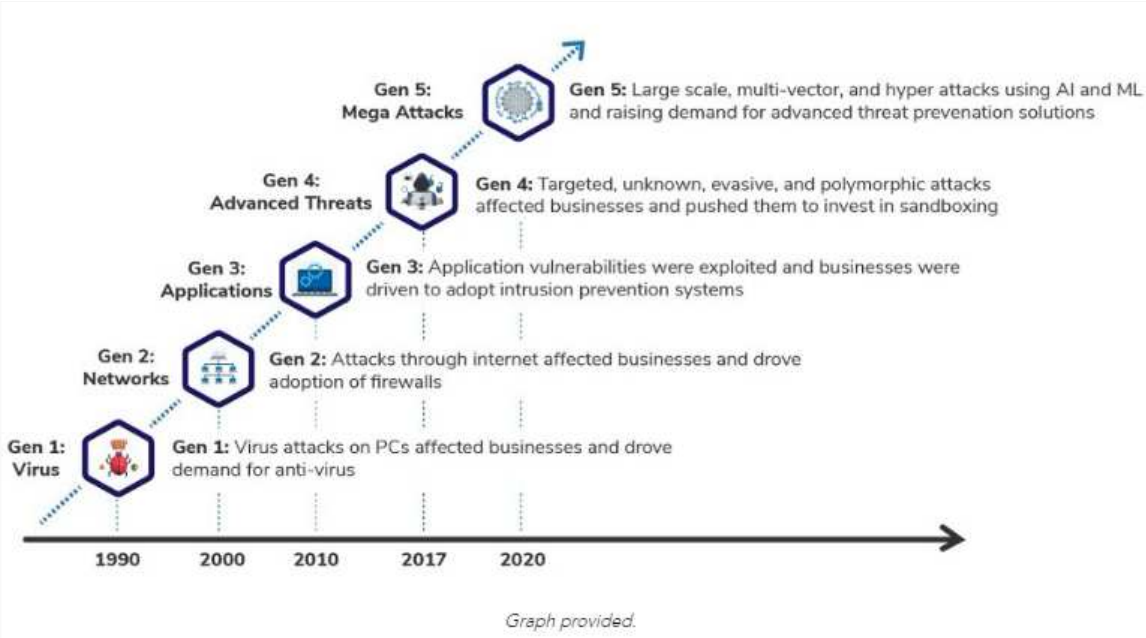
미래 정보보안 기술; 사용자 및 개체 행동분석 도구로 사이버공격에 대처

"인공지능, 기계학습을 활용하여 사이버 공격에 대처하는 UEBA에 주목"

Among the plethora of offerings, there's been a sustained buzz about user and entity behavior analytics tools. Image by Artem Oleshko / Shutterstock.com.

출처 : Frost&Sullivan Blog, Future Cyberwar: User And Entity … , Sep 3, 2020

- 컴퓨터와 인터넷 연결만 있으면 누구나 사이버 공격할 수 있으며, **사이버 전쟁**에 대응하는 **위협 방지 솔루션**을 검색하는 사례도 점차 늘어남
  - 사이버 공간 침투는 공격 벡터, 위험 인자 및 방법적 측면에서 폭넓은 스펙트럼으로 나타나고 있음
  - 사용자 인증정보를 뚫어 민감한 정보에 접근하거나 시스템에 접속 시도를 하는 것은 물론, 지리적으로 분산된 여러 곳에서 악성코드를 업로드하고 네트워크 아키텍처의 다양한 계층을 훼손하는 경우도 있음
  - 기업의 경우 이러한 공격을 당하면 감당할 수 없는 손실을 보게 됨
    - 운영 중단이 발생하면 생산성이 침해되며 물리적 안전에 위험이 발생하고 수익에 직격타를 맞게 됨
    - 또한 브랜드 가치가 하락하고 비즈니스상 핵심적인 데이터에 손실을 입을 수 있음



〈그림 1〉 갈수록 폭넓은 스펙트럼으로 나타나고 있는 사이버 공간 침투
출처 : Frost&Sullivan Blog, Future Cyberwar: User And Entity … , Sep 3, 2020

향후 **사용자 및 개체 행동분석 도구(UEBA)**가 판도를 바꿔놓을 수 있는 구원 투수로 등장함

- 현재 관찰되는 대규모, 다중 벡터 방식의 과잉(hyper) 공격은 인공지능과 기계학습을 사용함
- UEBA는 인공지능, 기계학습을 활용하여 보안 활동 및 보안 사고를 인식, 모니터링 및 상호연결로 공격에 대처함
- 보안 정보 및 이벤트 관리(SIEM) 플랫폼을 함께 사용하여 이러한 사이버 공격을 무마시킴

SIEM 플랫폼을 보완함

- 기존의 SIEM 솔루션은, 애플리케이션과 네트워크 하드웨어에서 생성된 보안 경고를 실시간으로 분석할 수 있지만, 여전히 한계가 있음
  - 지능형(advanced) 공격을 방지하도록 설계된 것이 아닌 데다, 효과적인 위협 탐지 및 대응 기능이 부족함
  - 사례가 등록되지 않은 사건은 간과하는 경향이 있고 사전에 정의된 상관관계와 필터링 규정에 의존하기 때문에 반응 시간이 느리다는 문제가 있음
  - 조직 내에서 발생하는 위협이나 위반을 감지하지 못하며 긍정 오류(false positive)를 많이 생성함
- UEBA 도구는 SIEM 솔루션과 함께 작동하며, 위에서 말한 문제점을 해결할 수 있음
  - 긍정 오류의 발생을 감소시킬 수 있으며 경고의 우선순위를 정해, 보안 전문가들이 가장 신뢰할 만하고 위험도가 높은 경고에 먼저 집중하도록 도움
  - ML 기반의 고급 알고리즘과 함께 사용될 때, 보다 장기간의 타임 라인에 걸쳐서 이벤트를 연관시키는 위험 점수(risk-scoring) 방식을 적용할 수 있음

- 적정한 보안 수준을 유지하고 미래의 사고발생 가능성을 낮추는 것을 목표로 하는 **위협 사냥(threat-hunting) 기술**의 도입
  - 위협 사냥 플랫폼은 공격이 시작된 시점부터 탐지된 시점까지의 시차를 좁히고자 작동하여, (위협의) 잠복시간(dwell time)을 대폭 단축하여 다양한 네트워크 및 시스템에서 데이터를 수집, 관리함
    - 잠재적 사이버 위협 관련 이상 징후 탐지를 자동화하는 고급 검색 기능, 시각화 기능, 분석 기능을 갖춤
    - 지능형 사이버 공격에 대한 기업의 방어를 강화하는 것을 목표로 설계됨
    - 고급 위협 사냥 기능을 통해 기업은 사고를 더 빨리 탐지, 분석, 대응, 해결할 수 있으며, 문제를 완화할 수도 있음

- **대시보드**를 통해 전체적인 위험 경관을 알 수 있음
  - UEBA 도구가 생성하는 정보 및 통찰의 깊이와 범위를 보면, 유연한 보안 대시보드의 필요성을 절감
  - 이러한 대시보드는 직원들에게 사건(incident)을 보고하고 보안 위험을 평가하는 도구를 제공함
  - 기업의 IT 위험 상태에 대한 전반적인 상황을 파악할 수 있음
    - 효과를 발휘할 수 있는 관리 보안 대시보드 구성과 사용자 맞춤형 제공은 불가능한 일이 아님
    - 이를 통해 최고 정보보안책임자(CISO)는 회사에 가장 큰 영향을 끼치는 핵심적인 보안 매트릭스를 추적·선택할 수 있고, 네트워크에 대해 최적의 결정을 내리는 데 필요한 정보를 찾을 수 있음

- **(결론)** 사이버공간 침투로 인한 위협이 점점 폭넓어지는 가운데 인공지능, 기계학습을 활용하여 사이버 공격에 대처하는 UEBA의 등장이 주목됨
  - UEBA는 인공지능, 기계학습을 활용하여 보안 활동 및 보안 사고를 인식, 모니터링 및 상호연결로 공격에 대처함
  - 보안 정보 및 이벤트 관리(SIEM) 플랫폼을 함께 사용하여 사이버 공격을 무마시킴
  - UEBA는 사용자와 개체 행동에 대한 폭넓은 가시성을 제공하므로 기업이 사이버 공격에 대한 탄력성을 높이는 것을 도와줄 수 있으며 보안 전문가의 부담도 상당히 덜어줄 수 있음