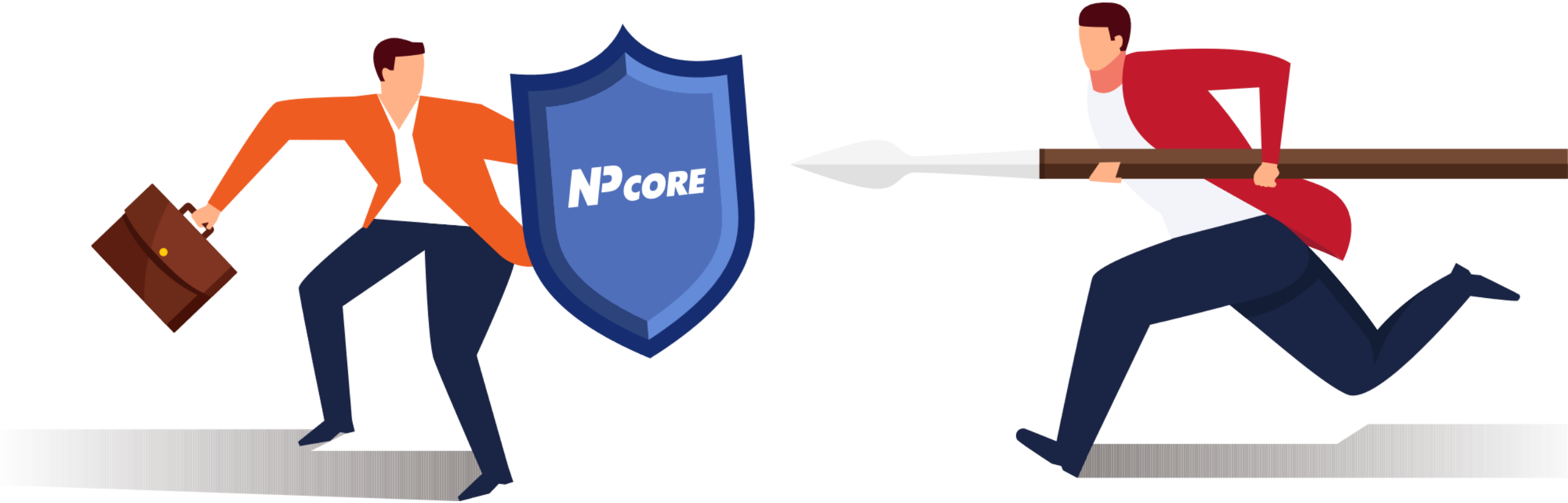
‘만약’이 아니라 ‘언제’ 해킹 당할까 - XDR의 중요성

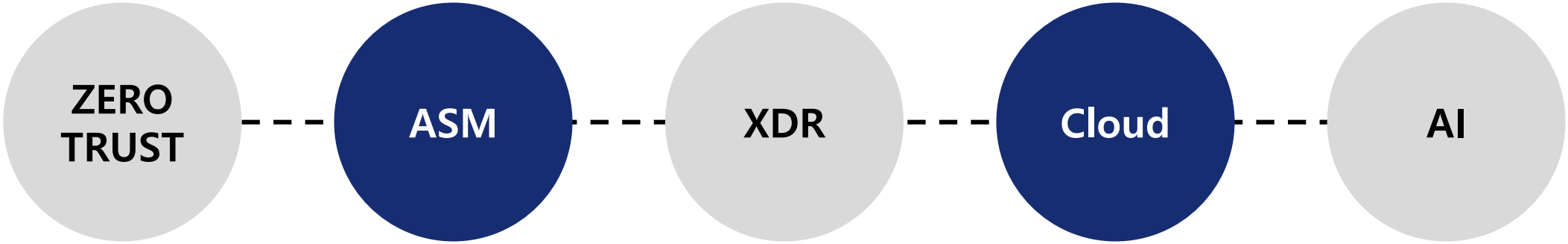
Not ‘if’ but ‘when’ – Importance of XDR

NPCORE CSO (해외전략이사) 백세현 (David Sehyeon Baek)

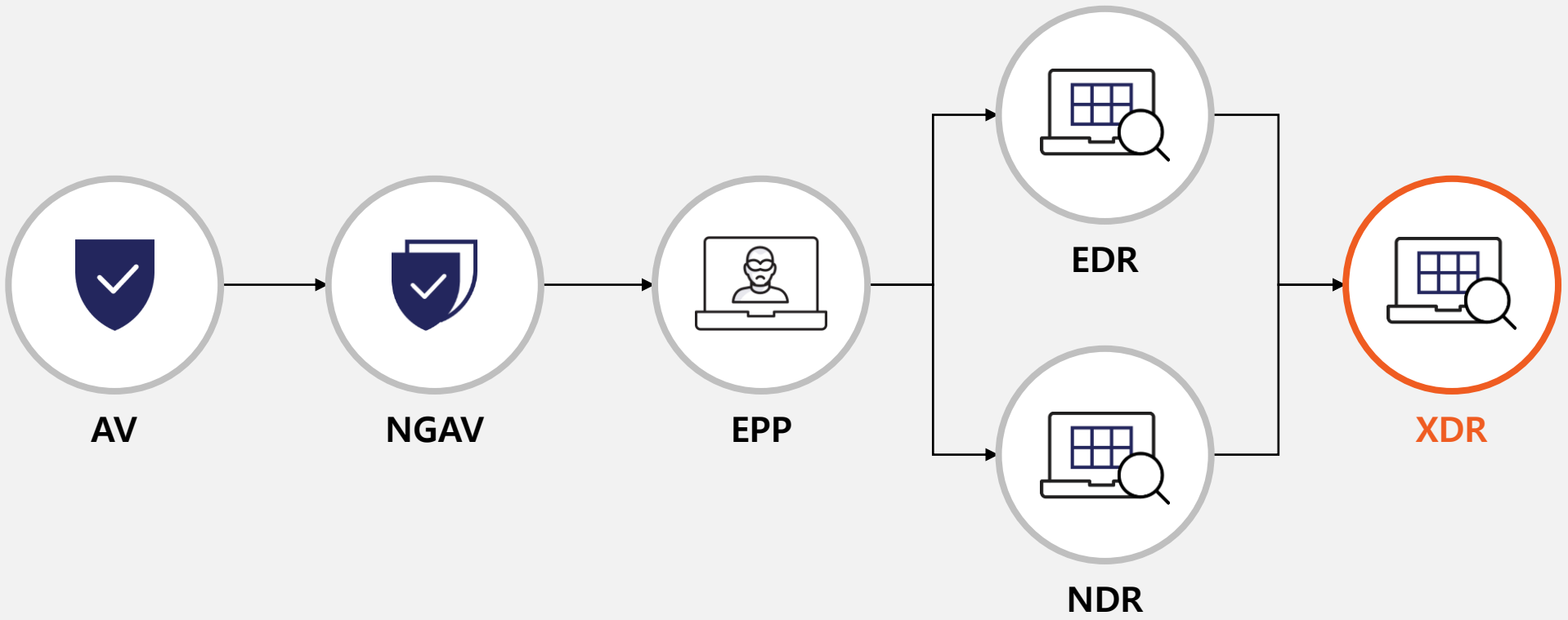
‘만약’이 아니라 ‘언제’ 해킹 당할까



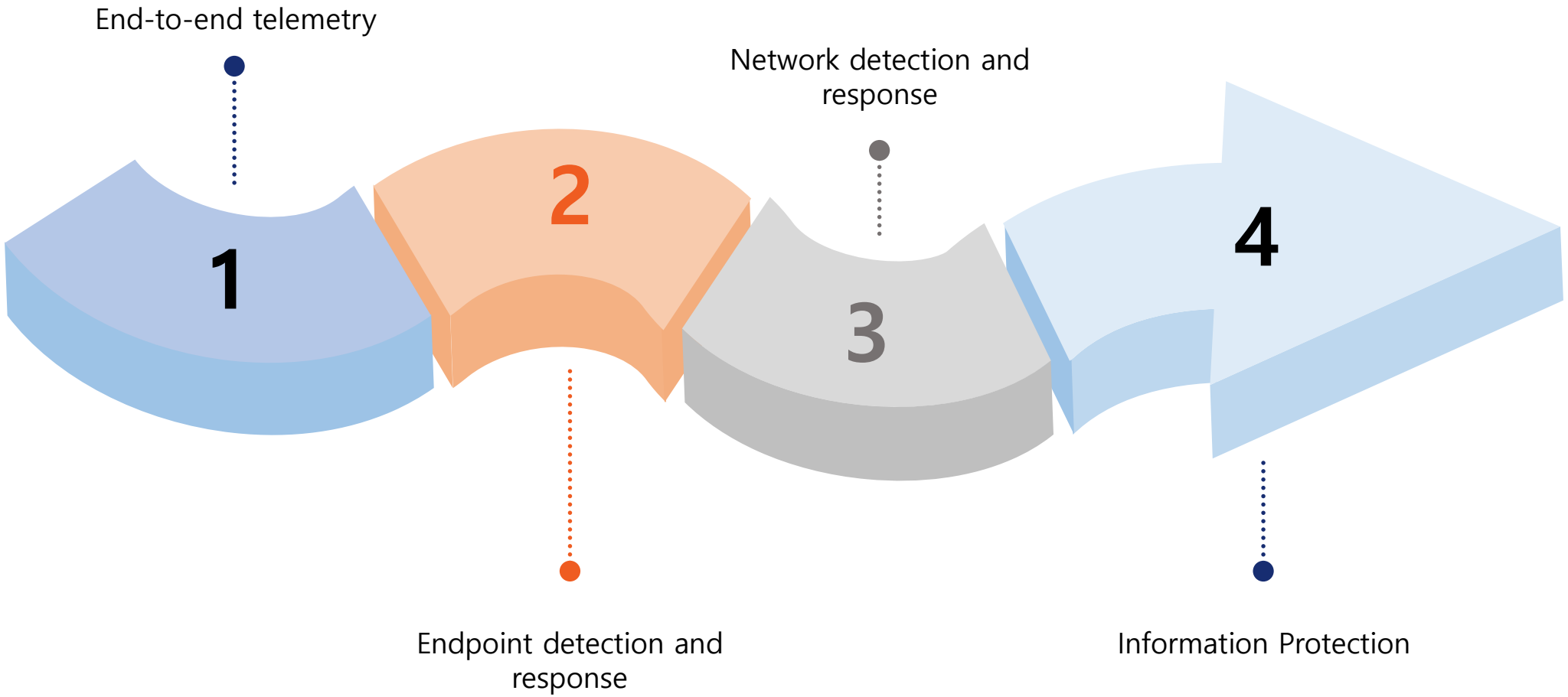
주요 키워드



AV부터 XDR까지



Silos, Alert Fatigue, Missed Attacks



SIEM vs. SOAR vs. EDR vs. NDR

SIEM

- 복잡성 (Complexity)
- 오탐 (False positives and negatives)
- 통합의 어려움 (Integration challenges – data silos, inconsistent data, reduced visibility)
- 부족한 확장성 (Scalability)
- 전문성과 트레이닝 (Expertise & training)

SOAR

- 복잡성 (Complexity)
- 오탐 (False positives)
- 통합의 어려움 (Integration challenges)
- 유연성의 결여 (Lack of flexibility)
- 모든 것의 자동화에 한계 (Human oversight)
- 전문인력 감축문제

EDR

- 엔드포인트만 커버가 가능 (Limited coverage)
- 복잡성 (Complexity)
- 오탐 (False positives and negatives) (Recall > Precision)
- 통합의 어려움 (Integration challenges)
- 방대한 정보량으로 인해 로그 저장 한계

NDR

- 복잡성 (Complexity)
- 오탐 (False positives and negatives)
- 제한적 가시성 (Limited Visibility)
- 통합의 어려움 (Integration challenges)
- 전문성과 트레이닝 (Expertise & training)

XDR의 정보 수집 범위

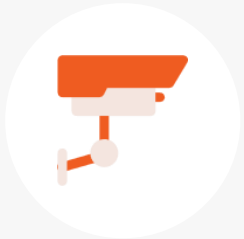
EDR (Endpoint Detection Response)

- 홈 CCTV -

단말 (집안)에서 발생 되고 있는 정보 수집

- 네트워크 행위
- 파일 행위
- 프로세스 행위
- 레지스트리 행위
- 어플리케이션 / 사용자 등

NDR (Network Detection Response)



- 도로 CCTV -

네트워크·클라우드 (도로/지역)에서 발생되고 있는 정보 수집

- 패킷 네트워크 어플리케이션
- 패킷 메타 데이터 및 파일
- 패킷 데이터 정보 등
- FW 로그 / NW 트래픽 등

EDR + NDR

=

XDR

집안과 도로의 상황(정보) 수집

사건 발생 시 연관 지어 한번에 파악 / 대응

XDR의 정보 수집 범위

	Open XDR	Native XDR
구성	• 여러 제조사의 제품을 통합	• 단일 제조사의 제품을 통합
장점	• 각 영역의 최고의 보안 제품 구성 가능	• 제품간 연동 및 구성 시간의 단축 • 솔루션간 연속성 확보
단점	• 이기종 연동에 대한 작업 필요	• 단일 제조사 통합에 종속
대상	**보안 제품의 제조사가 다양하며 기존 솔루션을 전면 교체하고 싶지 않은 고객**	**동종 제조사의 보안 제품 구성이 많은 고객**

XDR의 장점 - 속도

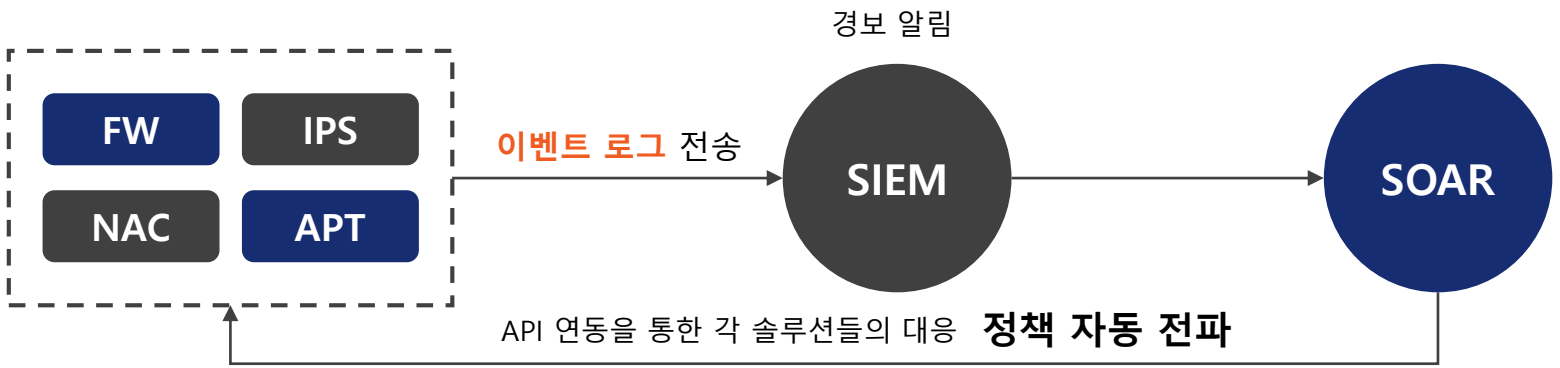
1. 데이터 소스의 상호 연관을 통해 평균 탐지 시간을 단축
2. 분류를 가속화, 조사 및 범위 지정 시간을 줄여서 평균 조사 시간 단축
3. 간단하고 빠르며 관련성이 높은 자동화를 구현, 평균 대응 시간 단축

XDR의 장점 - 정보

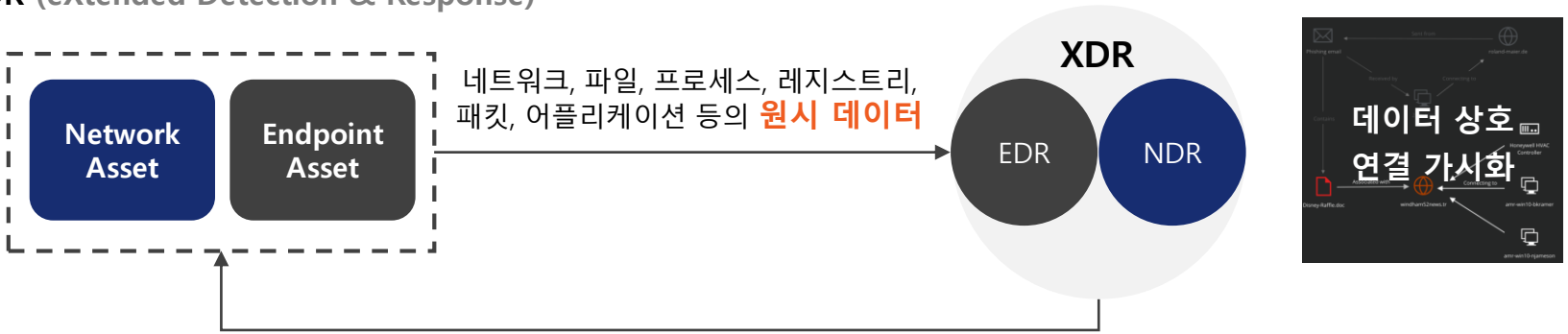
1. 단말 및 네트워크에서 발생 되는 모든 이벤트 수집
2. 각각의 솔루션이 아닌 전체 보안에 대한 가시성 향상
3. 사이버 공격 발생 시, 연동 분석을 통한 공격 현황 파악 및 대응판단

SIEM / SOAR / XDR

- **SIEM** (Security Information and Event Management) **/ SOAR** (Security Orchestration, Automation, and Response)



- **XDR** (eXtended Detection & Response)



SIEM / SOAR / XDR

SIEM / SOAR

전체 중요 이벤트 로그는 수집하나
전체적인 상호 연관 분석이 쉽지 않다.

- **SIEM**
  - 각 보안 장비로 부터 특정 이벤트 로그를 받음
  - 특정 이벤트 발생 시, 관리자에게 알람
  - 관리자는 알림 확인 후, 각 보안 장비로 이동 후 따로 정책 조치
- **SOAR**
  - 각 보안 장비로 부터 특정 이벤트 로그를 받음
  - 특정 이벤트 발생 시, 관리자에게 알람
  - 기존 각 장비와 API 연동으로 기준에 따른 자동적 정책 조치

XDR

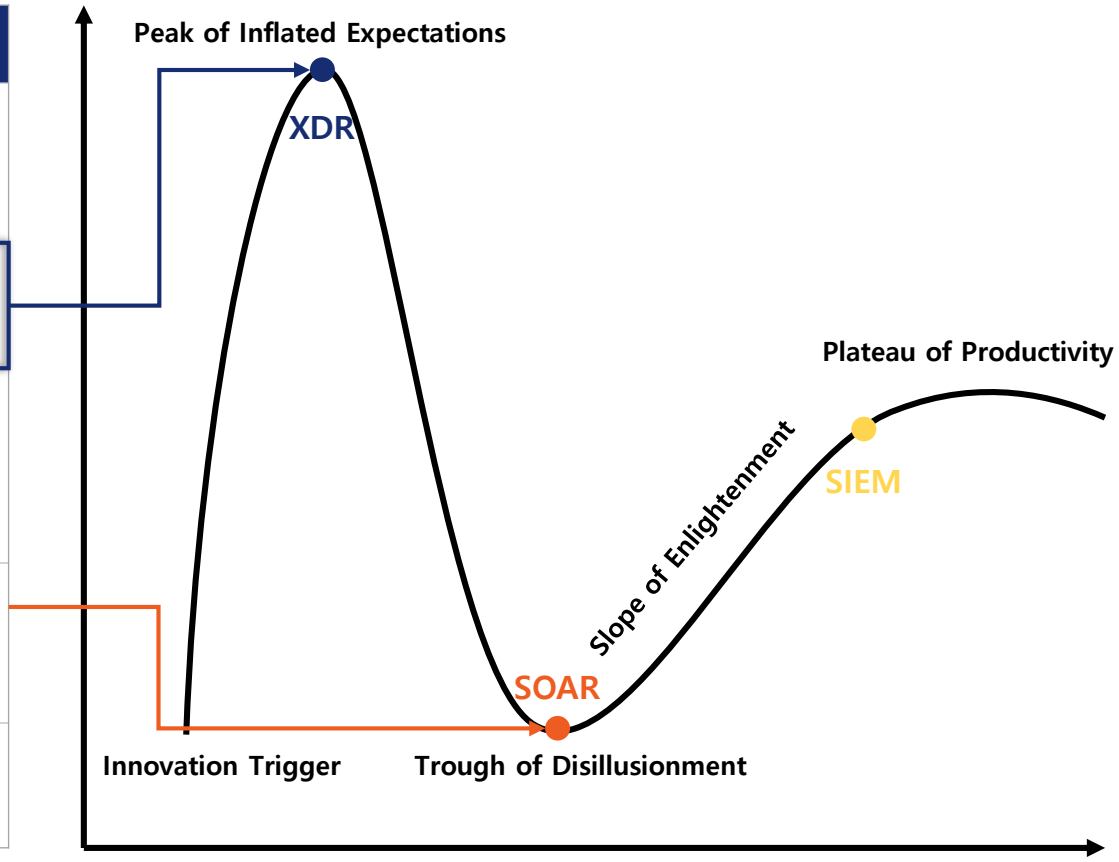
가시화를 통해 전체적인
연동 진행/흐름을 파악할 수 있다.

- **XDR**
  - EDR 및 NDR로 부터 항시 행위 로그를 받음
  - EDR 과 NDR에서 받은 항시 로그들을 데이터 상호화 연결하여 가시화
  - 상호 연결된 행위에 대한 특이사항 및 특정 장비에서의 이벤트 발생 시, 전체적인 가시화된 흐름/진행도 제공
  - 기존 각 장비의 API 연동을 통해 Lite 한 자동적 정책 조치

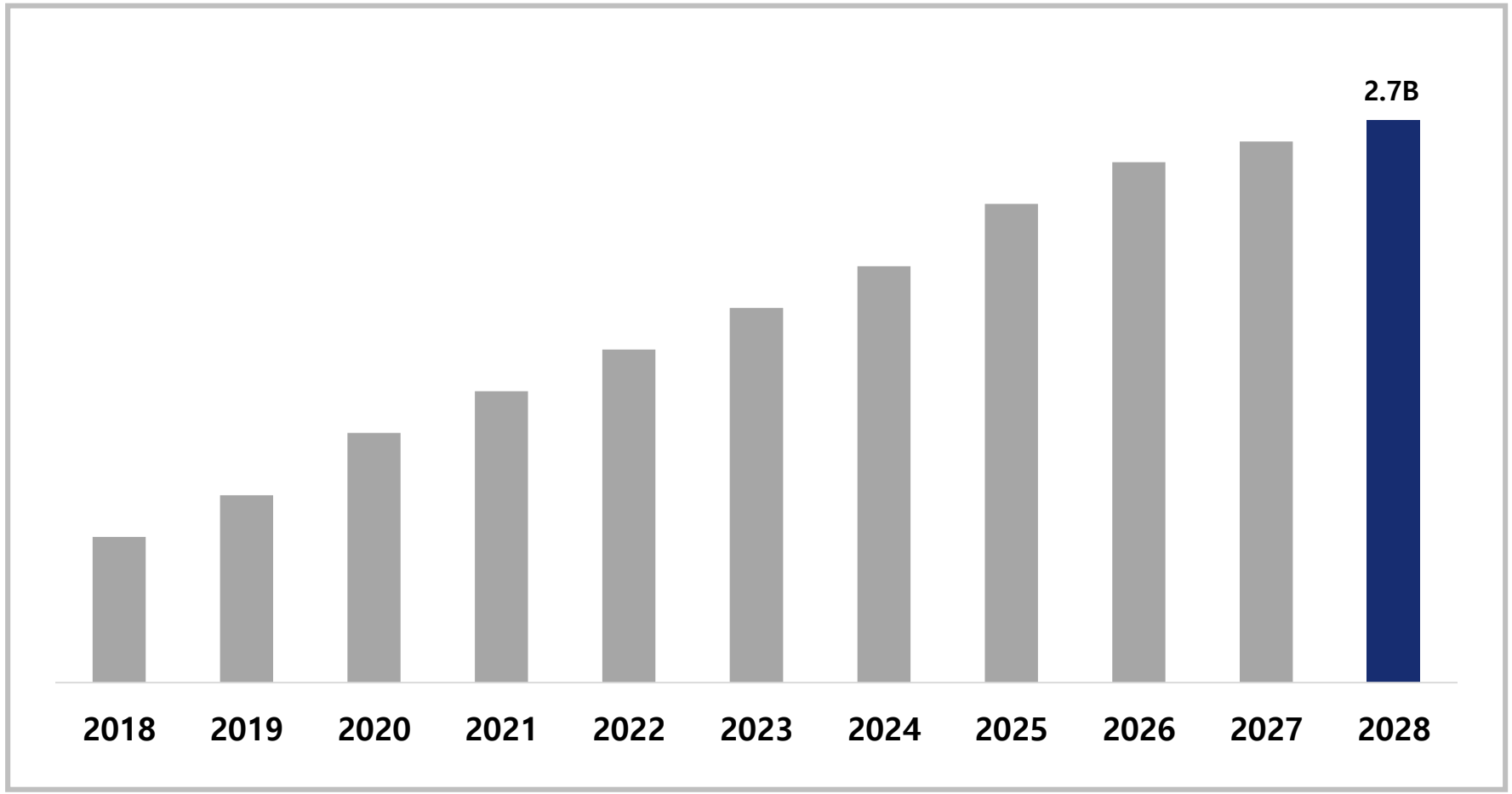
현시점의 XDR

*기술의 하이프 곡선 (Hype Cycle) 모형 5단계

단계	명칭	설명
1	기술 촉발 (Technology Trigger)	잠재적 기술이 관심을 받기 시작하는 시기. 초기 단계의 개념적 모델과 미디어의 관심이 대중의 관심을 불러 일으킨다. 상용화된 제품은 없고 상업적 가치도 아직 증명되지 않은 상태이다.
2	부풀려진 기대의 정점 (Peak of Inflated Expectations)	초기의 대중성이 일부의 성공적 사례와 다수의 실패 사례를 양산해낸다. 일부 기업이 실제 사업에 착수하지만, 대부분의 기업들은 관망한다.
3	환멸 단계 (Trough of Disillusionment)	실험 및 구현이 결과물을 내놓은 데 실패함에 따라 관심이 시들해진다. 제품화를 시도한 주체들은 포기하거나 실패한다. 살아남은 사업 주체들이 소비자들을 만족시킬만한 제품의 향상에 성공한 경우에만 투자가 지속된다.
4	계몽 단계 (Slope of Enlightenment)	기술의 수익 모델을 보여주는 좋은 사례들이 늘어나고 더 잘 이해되기 시작한다. 2-3세대 제품들이 출시된다. 더 많은 기업들이 사업에 투자하기 시작한다. 보수적인 기업들은 여전히 유보적인 입장을 취한다.
5	생산성 안정 단계 (Plateau of Productivity)	기술이 시장의 주류로 자리잡기 시작한다. 사업자의 생존 가능성을 평가하기 위한 기준이 명확해진다. 시장에서 성과를 거두기 시작한다.



XDR의 시장규모 (2028)



Source: Adroit Market Research @ 2021

XDR구현의 핵심사항

1. 현재 사용중인 보안 도구들과의 통합 (Integration with existing security tools)

EDR, SIEM, TIPs 등 – 각기 다른 보안 제품이기에 데이터 포맷, API, 프로토콜 등이 각기 달라서 어떻게 잘 통합하느냐가 관건

2. 데이터 품질과 상관관계 (Data quality and correlation)

XDR은 위협탐지 및 대응을 위해 다양한 소스의 데이터에 의존
XDR이 효과적으로 작동하려면 이러한 데이터의 품질 확보, 효과적인 상호 연관이 중요
데이터 출처가 다르고 형식이 다르고 처리 수준이 다를 수 있기에 이 부분 주의 요망

XDR구현의 핵심사항

3. 확장성 및 성능 (Scalability and performance)

여러 소스의 대량의 데이터를 실시간으로 처리해야 함
엔드포인트와 클라우드 환경의 수가 증가함에 따라 이 부분을 잘 처리할 필요가 있음

4. 오탐 및 미탐 (False positives and false negatives) 최소화

XDR은 머신러닝 알고리즘에 의존해서 작동하기 때문에 오탐 및 미탐 가능성 농후
오탐 및 미탐이 일어나기 쉬운 만큼 이를 최소화시킬 수 있는 XDR이 시장의 승자

5. 가격 (Cost)

XDR은 인프라, 인력, 지속적인 유지보수 측면에서 상당한 투자가 필요 누가 가격을 낮
추면서 품질은 유지할 수 있느냐가 관건

XDR의 시장 전략


최고의 가시성
(Best Visibility)
운영효율성 (Operational Efficiency)
가격경쟁력
(Price Leadership)
기술의 고도화
(Technological Sophistication)
원활한 고객경험
(Seamless Customer Experience)

Thank you

Not ‘if’ but ‘when’ – Importance of XDR