"제로트러스트 성공 전략
: XDR의 핵심 역할과 필요성"

NPCore
New Paradigm Core

* 핵심 전달 메시지

XDR의 개념과 필요성

- XDR의 기원과 탄생배경
- 다양한 관점에서 XDR의 이해
- XDR 관련 기술
- XDR 필요성, 고려사항

ZTA 이해와 과제

- 구현 관점에서 ZTA 파악
- ZTA 이슈와 과제 도출

XDR 기반의 ZTA 구현

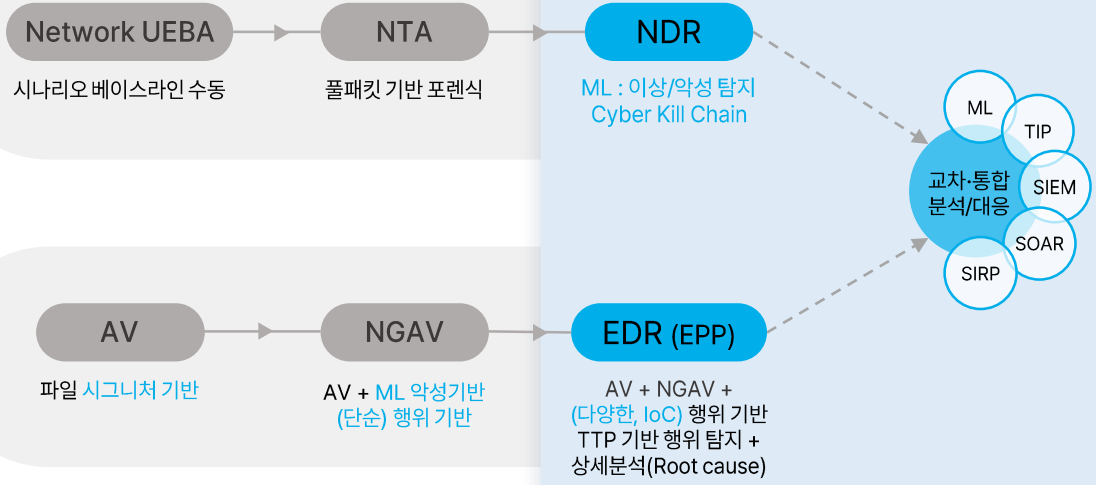
- XDR 기반의 적합성
- 구체적인 구현 장점 / 방안

1

XDR의 개념과 필요성

1. XDR의 개념 : DR 시리즈

NDR, EDR, XDR 발전과정, 비교



- Network / Endpoint 원시로그 자체 수집
- 보안 솔루션 이벤트 로그 수집
- 교차 분석 (N, E, N+E, N+E+other)
- SIEM / SOAR로 분석·대응 자동화
- 최신 분석 기술 (비지도, 지도, 딥러닝, 생성형 AI)
- Zero Trust와 최적의 연동 체계

XDR(e**X**tended **D**etection & **R**esponse)

1. XDR의 개념 : XDR 이해

탐지 모델 관점 > XDR은 Network, Endpoint 교차 분석 가능

NDR

- 조직에서 거의 접속하지 않은 **사이트**에서 **파일**을 다운로드 단말기를 찾았습니다.
- 멀웨어가 HTTP를 사용해서 외부 **C&C 서버**에 접속이 의심되는 **통신**을 탐지했습니다.

EDR

setup.exe 라는 프로세스에서 다음과 같은 의심행위가 탐지되었습니다.
▸ Fork되는 자식 프로세스가 **네트워크 행위**를 함 ▸ 레지스트리 런키에 **어떤 값**을 등록함
▸ 파일 해시 값이 외부 **악성 평판 정보**와 일치함

XDR

- **NDR** #123-1 공격 관련 endpoint 프로세스가 더욱 의심스러워 단말을 탐지했습니다.
  프로세스에 ▸ 디지털 서명 값이 없습니다. ▸ 이 프로세스가 windows/system 폴더에 어떤 파일을 write했습니다.
  ▸ 해당 프로세스 파일 해시가 과거 AI 분석결과와 일치합니다.
- 과거 **특정 보안사고** (Campaign Lite Wizard Spider 1) 관련 경고들이 2개의 단말에서 탐지되었습니다.
  자식 프로세스가 네트워크 행위 함 / 해당 프로세스가 레지스트리 런키에 어떤 값 등록 / 자식 **프로세스**가 네트워크 행위
  + 2개의 단말이 외부 1개의 서버를 거의 같은 시간대에 접속했고, 서로 **통신**을 했습니다.

1. XDR의 개념 : XDR 이해

분석/대응 관점 > 수동

NDR

- 조직에서 거의 접속하지 않은 **사이트**에서 **파일**을 다운로드 단말기를 찾았습니다.
- 멀웨어가 HTTP를 사용해서 외부 **C&C 서버**에 접속이 의심되는 **통신**을 탐지했습니다.

- 외부/내부 평판정보 조회
- 방화벽 로그에서 과거 로그 분석 (다른 단말 접속 여부)

- 외부/내부 평판정보 조회 (멀티백신 분석결과)
- 멀웨어 샌드박스 분석
  (https://anyrun.de/img/video-2.webm)

- PCAP 분석 (TCP Stream, UDP 페이로드 등)

Wireshark · Follow TCP Stream (tcp.stream eq 0) · VMware Network Adapter VMnet8

```
GET / HTTP/1.0
Host: 200.200.200.4
Accept: text/html, text/plain, text/css, text/sgml, */*;q=0.01
Accept-Language: en
User-Agent: Lynx/2.8.8dev.15 libwww-FM/2.14 SSL-MM/1.4.1 OpenSSL

HTTP/1.1 200 OK
Date: Mon, 12 Dec 2022 22:42:45 GMT
Server: Apache/2.4.6 (CentOS)
Last-Modified: Mon, 12 Dec 2022 22:25:50 GMT
ETag: "16-5efa8fc5104c0"
Accept-Ranges: bytes
Content-Length: 22
Connection: close
Content-Type: text/html; charset=UTF-8
```

1. XDR의 개념 : XDR 이해

분석/대응 관점 > 수동

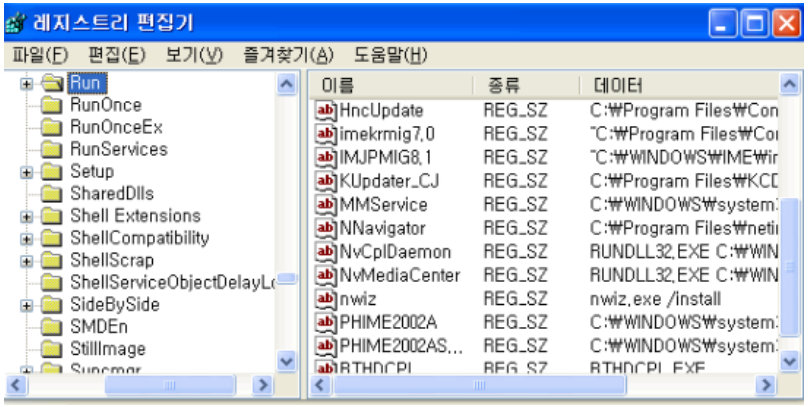
- 외부/내부 평판정보 조회
- 방화벽 로그에서 과거 로그 분석(다른 단말 접속 여부)

- run 등록 값 확인 (정상 프로세스 여부)

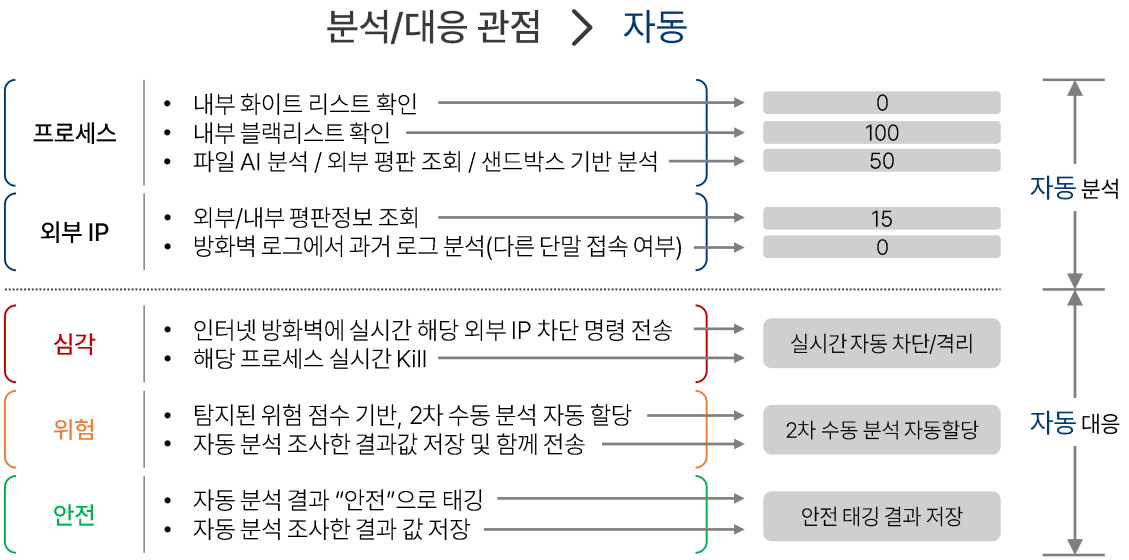
EDR

setup.exe 라는 프로세스에서 다음과 같은 의심행위가 탐지되었습니다.
▸ Fork되는 자식 프로세스가 **네트워크 행위**를 함 ▸ 레지스트리 런키에 **어떤 값**을 등록함
▸ 파일 해시 값이 외부 **악성 평판 정보**와 일치함

- 외부/내부 평판정보 조회 (멀티백신 분석결과)
- 멀웨어 샌드박스 분석
  (https://anyrun.de/img/video-2.webm)



1. XDR의 개념 : XDR 이해

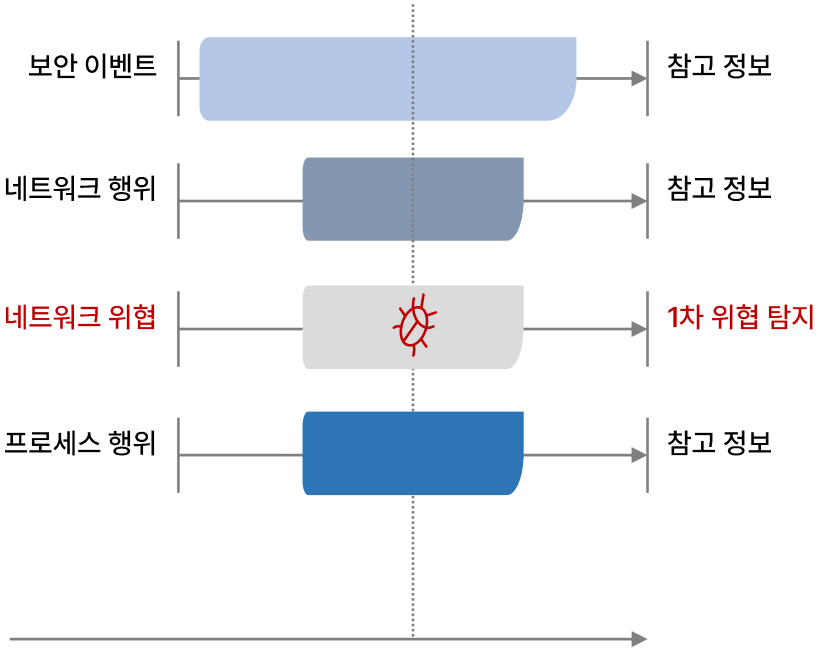


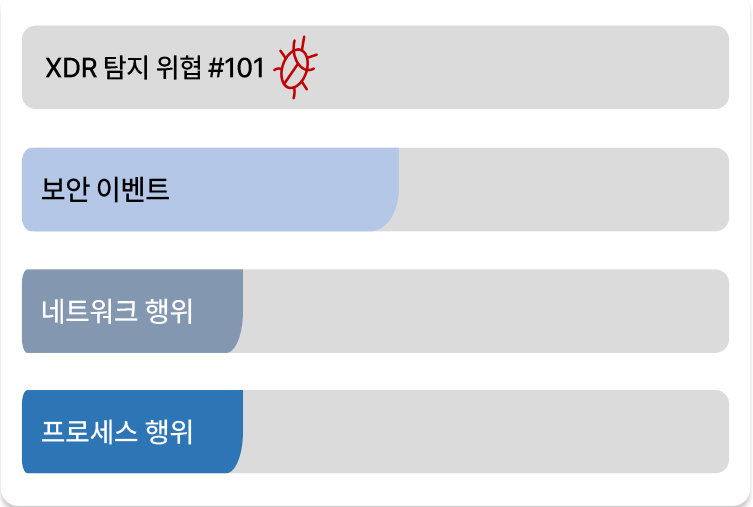
XDR

- **NDR** #123-1 공격 관련 endpoint 프로세스가 더욱 의심스러워 단말을 탐지했습니다.
  프로세스에 ▸ 디지털 서명 값이 없습니다. ▸ 이 프로세스가 windows/system 폴더에 어떤 파일을 write했습니다.
  ▸ 해당 프로세스 파일 해시가 과거 AI 분석결과와 일치합니다.
- 과거 **특정 보안사고** (Campaign Lite Wizard Spider 1) 관련 경고들이 2개의 단말에서 탐지되었습니다.
  자식 프로세스가 네트워크 행위 함 / 해당 프로세스가 레지스트리 런키에 어떤 값 등록 / 자식 **프로세스**가 네트워크 행위
  + 2개의 단말이 외부 1개의 서버를 거의 같은 시간대에 접속했고, 서로 **통신**을 했습니다.

1. XDR의 개념 : XDR 이해

분석 관점 > 교차 정보



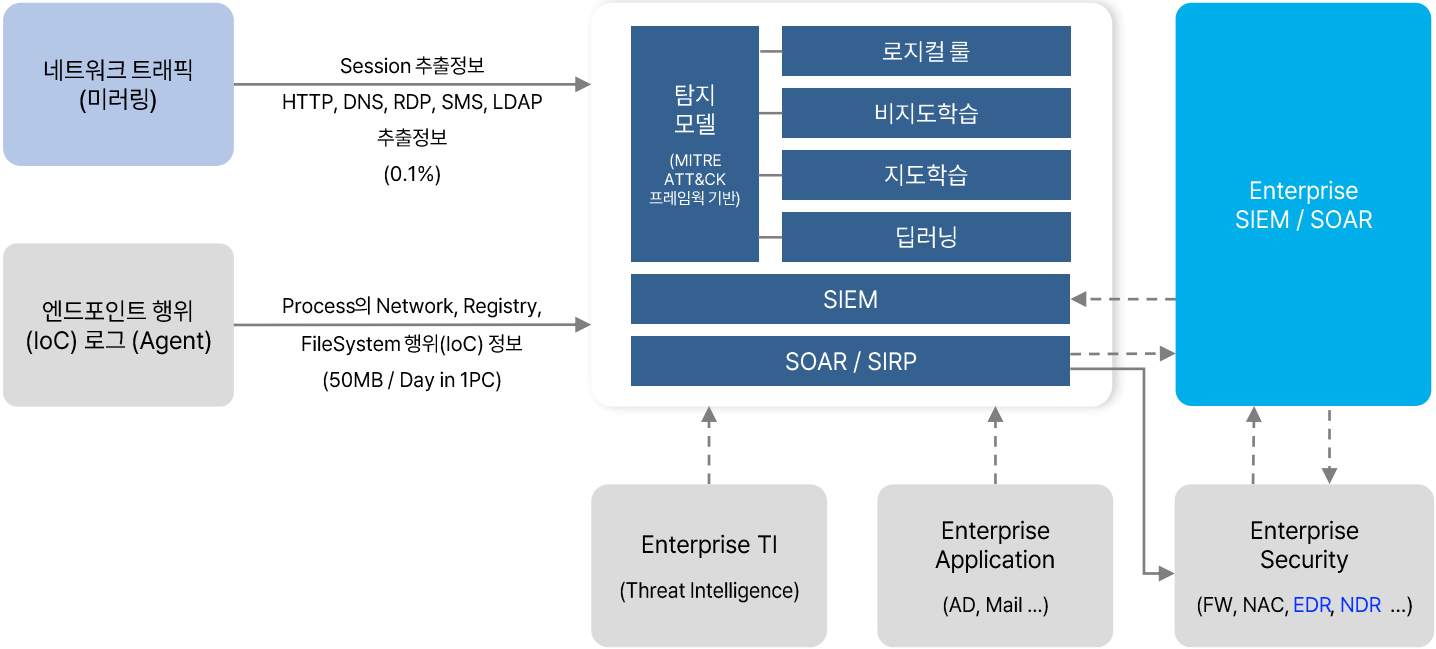


1. XDR의 개념 : XDR 이해 (특징)

필수 사항 Mandatory	옵션 사항 Optional	배제 사항 Excluded
Endpoint, Network 원시로그 모두 수집	Full SIEM / SOAR	Endpoint, Network 원시로그 수집 불가 또는 하나만 제공하는 경우
2개의 수집 기능은 XDR 벤더 자체 제공	Network Forensic (full packet 저장)	ML 기술 활용 미흡 (시그니처 방식이나 사람이 룰을 정의하는 방식)
Network, Endpoint 교차 분석	Sandbox 기반 악성파일 분석	
외부 시스템과 유연한 연동 • 타 시스템 원시로그, 탐지 로그 수집 • 다양한 연동으로 탐지결과 전송 • 다양한 방법으로 API 차단/격리 연동	딥러닝 기반 악성파일 분석	
자동화된 대응	분석 시 관련된 참고정보 제시	
ML(Machine Learning) 기술 활용		

1. XDR의 개념 : XDR 이해 (특징)

동작 방식 및 구성



1. XDR의 개념 : XDR 이해 (특징)

XDR 필요성과 고려사항

필요성

탐지 강화

- 페러다임 : 사전 차단 → 사후 탐지
- 영역 및 대상 : 경계 → 내부, 단말, 클라우드
- 기술 : 시그니처 → 행위 (순서, ML(AI), 교차, 상관)
- 수집 : 보안탐지이벤트 → 네트워크, 단말 행위-raw 데이터

SIEM 신규 도입?

- XDR은 SIEM이 포함되어 있음
- 보다 신개념 XDR 검토
- NDR, EDR도 한 번에

SIEM 고도화

- 대상 : 네트워크 트래픽, 단말기 대상 확장
- 기술 : 시그니처, 상관분석 → 행위, ML(AI)로 룰 고도화

고려사항

중복성 방지

- NDR, EDR 과의 중복성 고려
- SIEM / SOAR 와의 중복성 고려

아키텍처

- 레거시 시스템에서 부족한 것? → 탐지 모델(룰), 교차 분석/대응
- 탐지 : XDR의 탐지 결과를 기존 SIEM으로? Or not
- 분석/대응 : 네트워크, 단말 교차분석을 SIEM에? Or other layer?

연동

- 수집 : 레거시 NDR, EDR에서 행위(raw)데이터, 탐지결과 수집 연동
- 대응 : 레거시 보안장비에 차단, 격리 등을 위한 연동

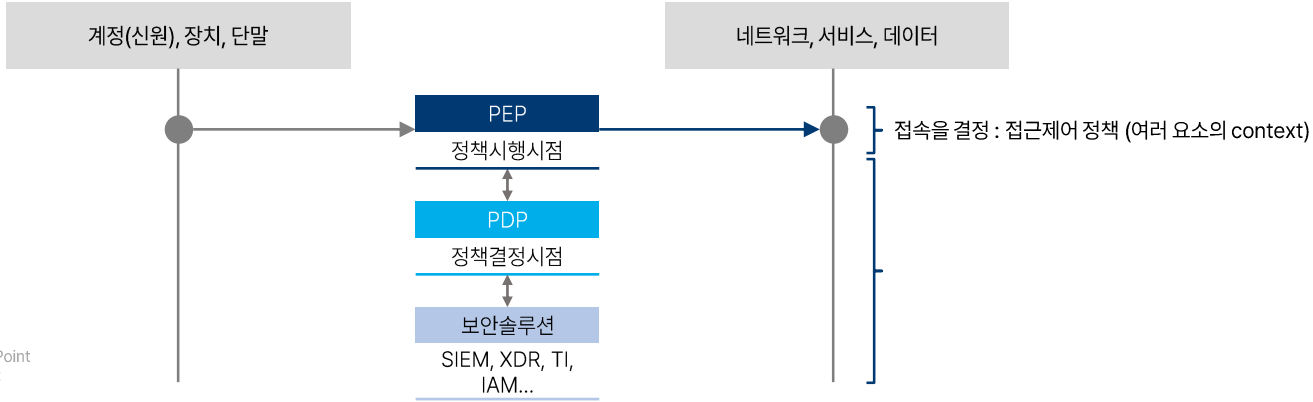
2

ZTA
(Zero Trust Acrchitecture)
이해와 과제

2. ZTA 이해와 과제 : ZTA ?

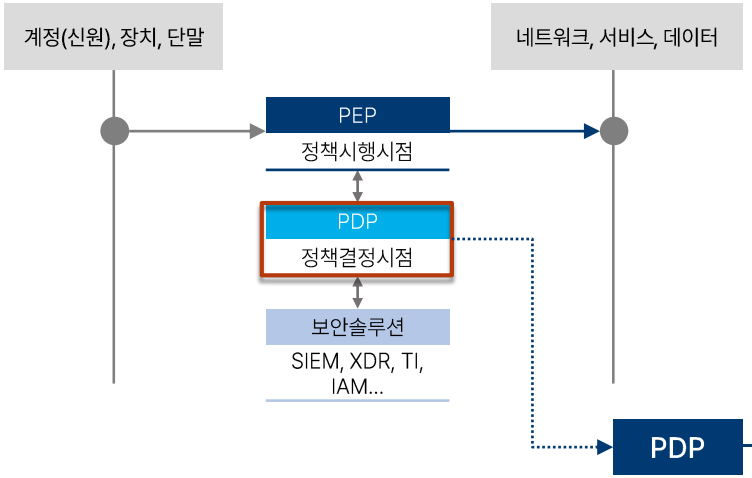
ZT개념을 사용한 기업 사이버보안 계획으로 컴포넘트간 관계, 워크플로우 설계, 접근 정책이 포함됨
(NIST SP 800-207, '20년)

ZT(Zero Trus) : 정보 시스템 및 서비스에 대한 접속 요구가 있을 때 네트워크가 이미 침해된 것으로 간주하고, 주어진 권한을 정확하고 최소한으로 부여하는데 있어서 불확실성을 최소화하도록 설계된 개념 및 아이디어 모음

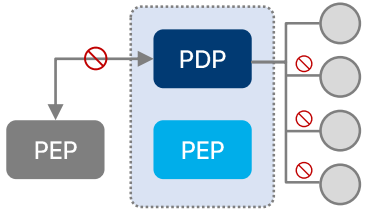


- PEP : Policy Enforcement Point
- PDP : Policy Decision Point

2. ZTA 이해와 과제 : 現 PDP 이슈

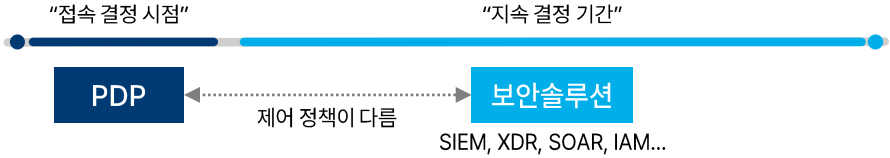


1 PEP 관리서버에 PDP 구현 → 다양한 정책 구현의 한계



- PDP가 별도의 솔루션, 시스템이 아닌 PEP의 관리서버 내 일부 기능(연동모듈) 으로 구현되어 솔루션의 정체성에 벗어나는 데이터 연동을 꺼려함
- 특정 PEP 벤더에서 개발한 PDP는 다른 벤더의 PEP와 연동에 소극적으로 개별적을 PDP 개발·운영되는 것이 현실

2 "접속 결정"의 PDP 정책과 "지속 결정"을 위한 모니터링 정책 연계 없음



통합 PDP 필요

3

XDR 기반의 ZTA 구현

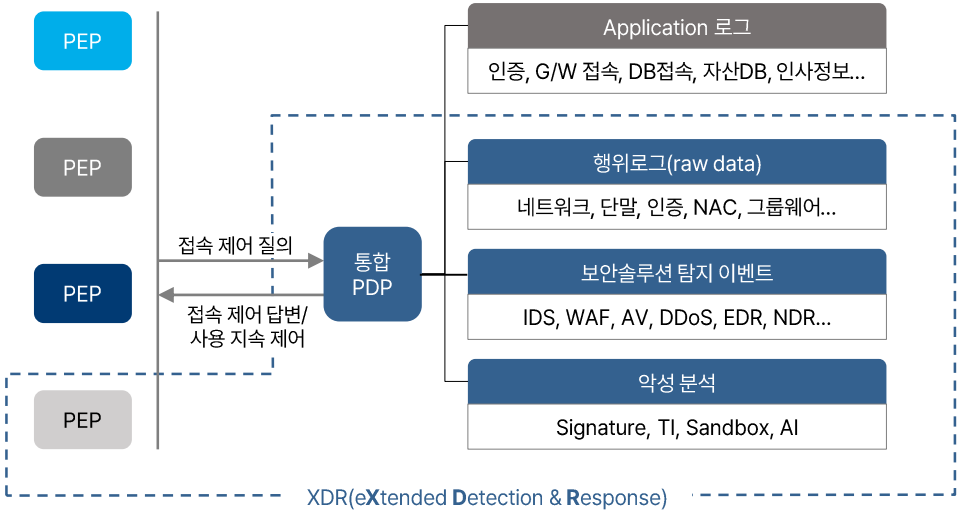
16

3. 통합 PDP로서 XDR 적합성

"어떤 솔루션에서 **통합 PDP역할**을 하면 좋을까?"

구분		IAM Identity and Access Management	NAC Network Access Control	SSL VPN	SIEM Security Information Event Management	XDR eXtended Detection & Response
다양한 데이터 수집	사용자 상황, 인사 정보	●		●	●	●
	단말 보안상태 정보		●	●	●	●
	다양한 보안 이벤트 로그 수집				●	●
	행위 데이터 수집 (raw Data)					●
탐지 결과 데이터	컴플라이언스 (정책 준수)	●	●	●	●	●
	IDS, DDoS, WAF, Anti-APT...				●	●
	EDR				●	●
	NDR				●	●
분석, 대응	Net. End. - 교차 분석 (raw Data 필요)					●
	상관분석	▲	▲	▲	●	●
	타 제품과의 연동 우수성 (수집, 대응)	▲	▲	▲	●	●

3. 구현 방안



1 : 1(N) 연동 한계 ➡ N : N 연동

(특정) 단일 현 보안상태 정보 활용 ➡ **다 각도 현** 보안 상태 또는 보안상태 **이력** 활용

PEP 별 ZT 모니터링 ➡ PEP 통합 ZT 모니터링

통합 PDP 정책

대상

- 장치,단말 (IP, MAC, Host, Host-ID)
- User (실명, 계정, 소속, 직급)

⊕⊖

조건

- 시간
- 국가
- 위치
- 인증 수단
- 프로세스 악성 여부
- 프로세스 취약성
- 메모리 상태 (프로세스)
- 비인가 접속 시도 이력
- 보안 준수 여부
- 과거 보안/사용 이력
- 위협 지속 점수

⊕⊖

리소스

- 네트워크
- 서비스
- 데이터
- 리소스 별 가중치 (중요도)

⊕⊖

대응

- 접속-허용
- 접속-거절
- 접속-허용 후 경고
- 지속 - 차단
- 지속 – 허용 후 소명

⊕⊖

* 마치며

(주)엔피코어는 XDR 회사입니다.

ZeroTrust, XDR은 단순하게 패키지, 장비를 구축하는 것이 아닙니다.

긴밀한 소통을 통해 맞춤형 XDR 기반 ZeroTrust 체계를 구축하시죠.

joseph@npcore.com

NPCore
New Paradigm Core

Thank YOU

AI기반 신·변종 악성코드 및 랜섬웨어 대응 솔루션 전문기업

HQ. 07217 서울 영등포구 당산로 171, 701호 (당산동4가, 금강펜테리움IT타워)

M. sales@npcore.com

T. 02-1544-5317

F. 02-413-5317

VIETNAM. 15th floor, block B, Song Da Building, 18 Pham Hung street, My Dinh 1 Ward, Nam Tu Liem district, Ha Noi city.

T. +84-4-3837-8554