G-PRIVACY 2021
2021 정부·공공·기업 개인정보보호&정보보안 컨퍼런스

EDR / NDR 이후, XDR 플랫폼 출현배경과 현재 … 그리고, 고려사항

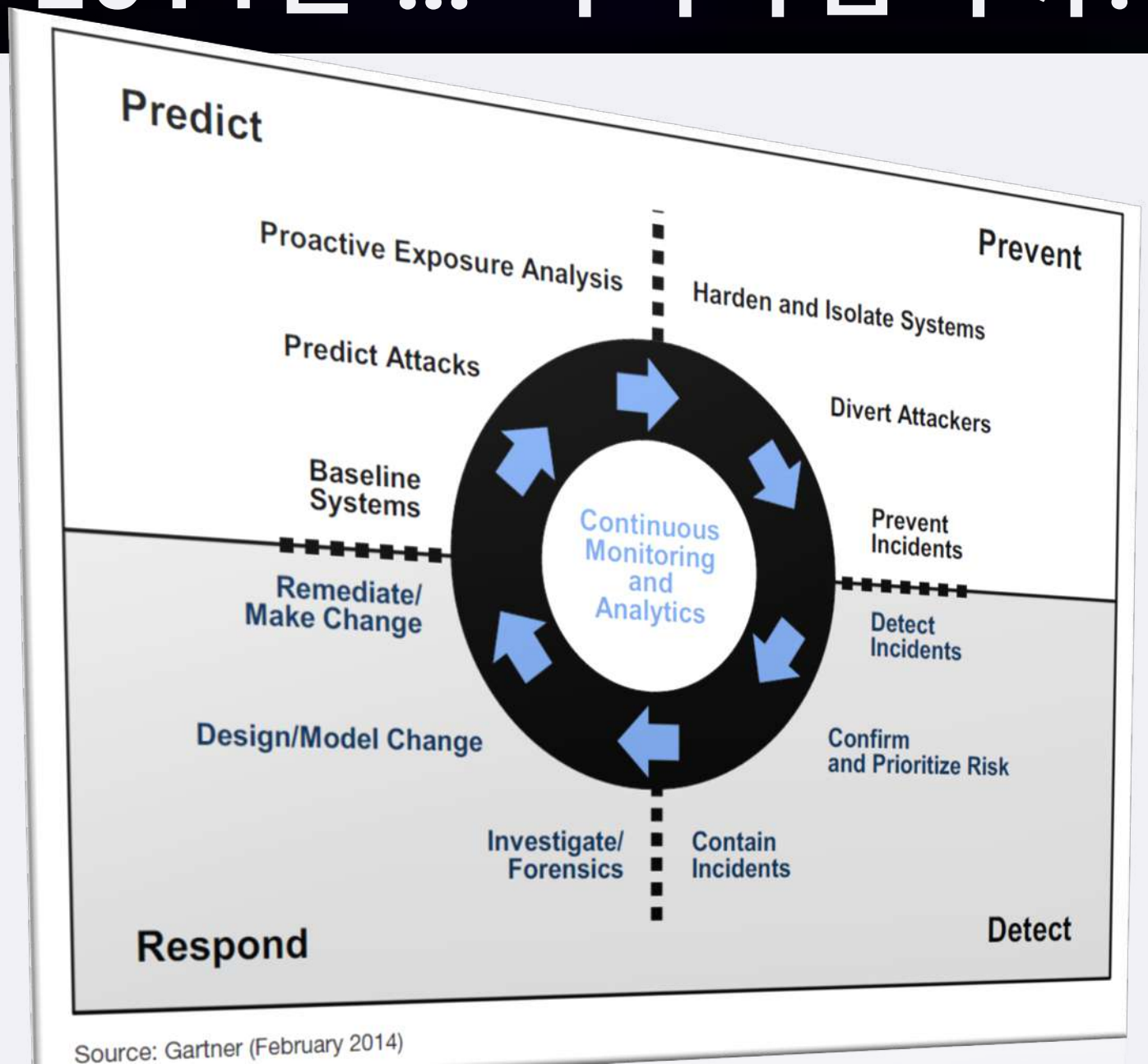
권영목 대표 / Paul Kwon
파고네트웍스 / PAGO Networks, Inc.
PAGO DeepACT 매니지드 탐지 및 대응 센터

PAGO NETWORKS

STELLAR CYBER®

파고네트웍스가
초기에 경험한 내용을 바탕으로,
오늘 주제의 출발점을
먼저 살펴보겠습니다

2014년 … 기억나십니까?



Source: Gartner (February 2014)

Gartner®

“Adaptive Security Architecture”

PAGO NETWORKS STELLAR CYBER®

2014년 … Adaptive Security Architecture

Gartner®

“Adaptive Security Architecture”

Incident Response

Continuous Response

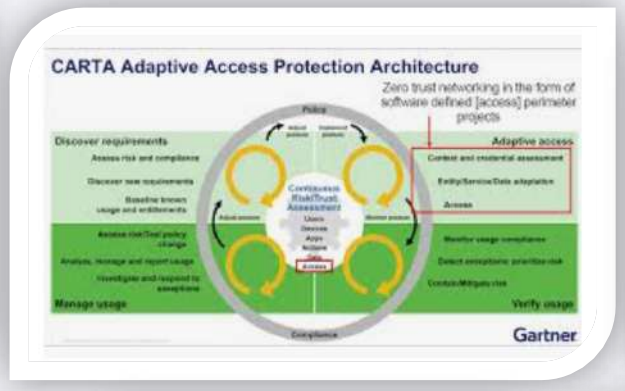
시스템은 이미 침해당했다고 가정

지속적인 위협탐지 모니터링 필요

적절하고, 빠른 대응 필요 (Response, Remediation)

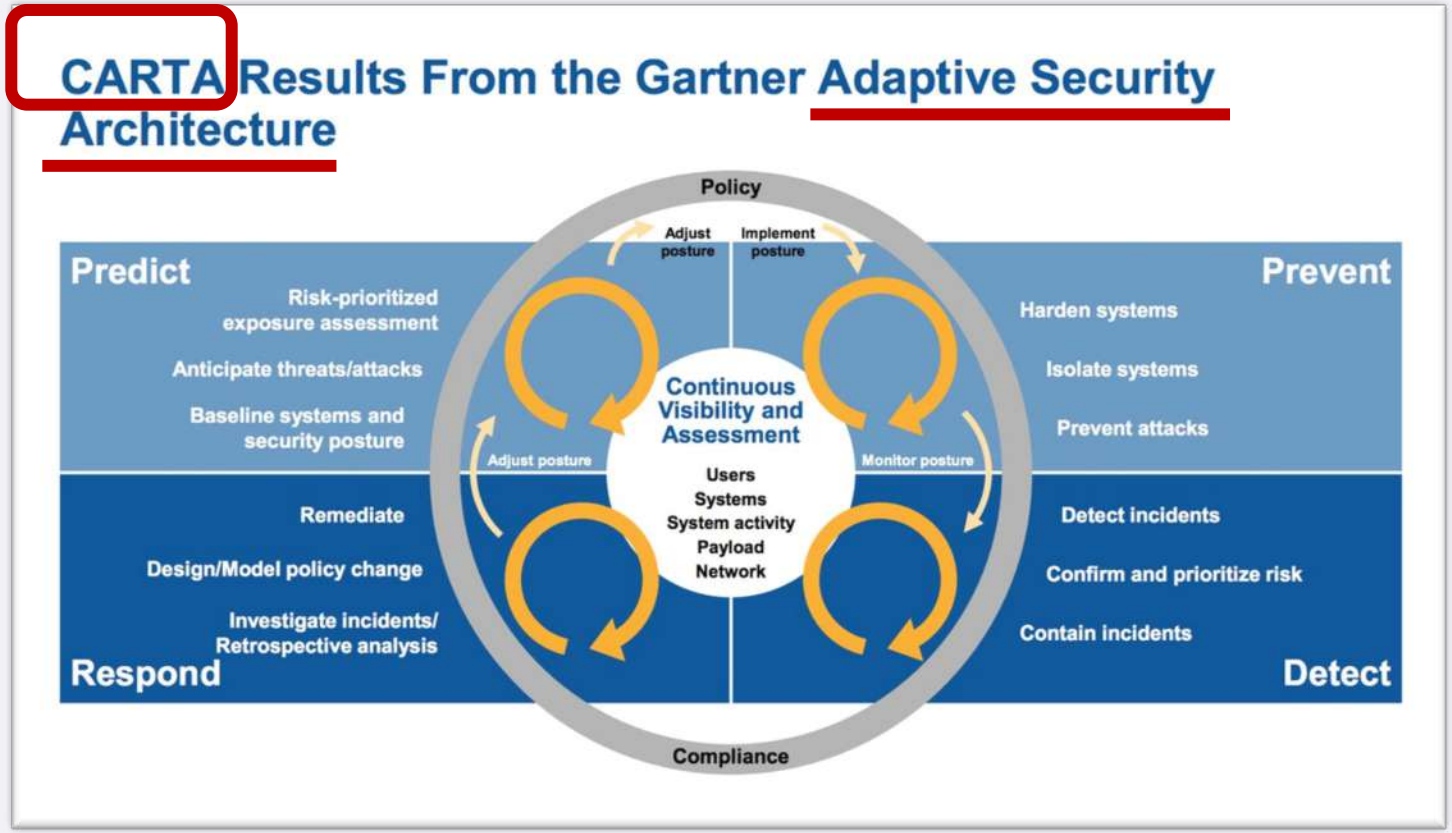
PAGO NETWORKS STELLAR CYBER

거의 5년간 …



상당수 국/내외 보안 기업이 적극 활용 !!

참고로, 현재는 … CARTA 방향성으로 진화



Gartner®

"Continuous Adaptive Risk and Trust Assessment"

당시... 보안 솔루션과 현실 (2015 ~)

탐지

분석

대응

보안 솔루션 급증

탐지 / 대응 보안 스택

- EDR / NDR
- NG-SIEM
- SOAR
- NG-Log Management
- IR Forensics
- Anomaly Detection

실효성 !?

그런데, 현실적인 고객 반응은?

ILLUSTRATION: MICHAEL GLENWOOD

- 방향성과 트렌드는 맞지만, 기업에서 실제 적용이 상당히 어려움
- 위협 대응 프로세스 정립이 쉽지 않음

실제로, 파고네트웍스 창업 준비할 때 (2016년)

탐지/대응 엔드포인트 보안 한국 시장 조사

EDR

당시 잠재 고객 반응

이걸로
다 막을 수 있어요 ?

지금 당장은 ..
탐지/대응 보다 ..
보호/차단 비율을 더 높여야 해요 !!!

경험 그리고, 판단

아직 이르다

실제로, 파고네트웍스 창업 준비할 때 (2016년)

예상대로
2016년 ~ 2018년
EDR 벤더사와 고객들이
모두 **"시행 착오"**를 겪습니다

탐지 **분석** **대응** **보호, 차단 용도**

절차, 프로세스 준비X **목적이 틀림**

파고네트웍스의 선택은 ? (2017년)

머신러닝 / 딥러닝 기반,
EPP (Endpoint Protection Platform)
솔루션

실제로, 보호(Protection) 비율이 상승했는가 ?

공통 사항

- **기존 보안솔루션 유지**
  - 기존 엔드포인트 보안
  - 기존 네트워크 보안
  - 기존 보안 관제

+

- **AI 엔드포인트 보안 탑재**
  - 추가 위협(멀웨어) 탐지
  - Known / Unknown 혼합

AI 보안제품 이용한
실제 고객사 프로젝트 기반
(by 파고네트웍스, 2020년)

탐지 (Detection),
대응 (Response)
EDR / NDR
다양한 탐지/대응 플랫폼의
제자리 찾아가기

다음 단계는 ....

당시
잠재 고객 반응

이걸로
다 막을 수 있어요 ?

지금 당장은 ..
탐지/대응 보다 ..
보호/차단 비율을 더
높여야 해요 !!!

엔드포인트
Protection Rate
최대화 방안
먼저 제안

BlackBerry
deepinstinct

머신러닝 / 딥러닝 기반,
EPP (Endpoint Protection Platform)
솔루션

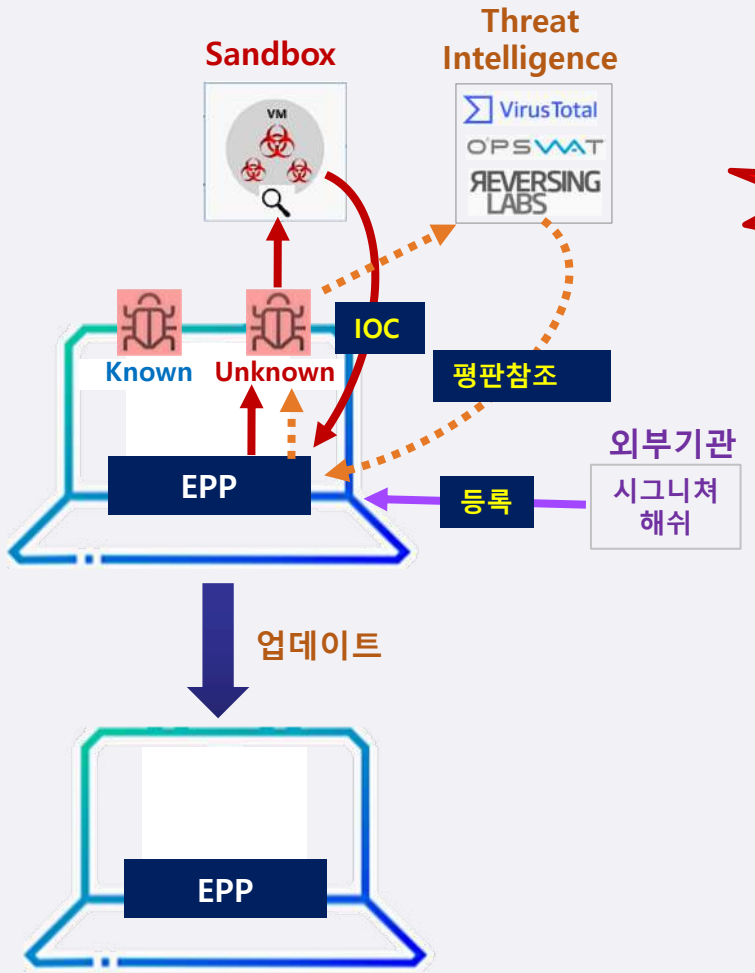
파고 EPP 고도화 고객도
탐지/대응 단계, 고민 시작

고객사 요구사항 – 1 (질문)

EPP 솔루션 고도화 이후,
엔드포인트
Protection Rate 를 높였는데,

EPP 고도화 하지 못한 시스템은 어떻게 Protection Rate 를 높이나요?

다른 솔루션 도입하지 않고
대응할 수 있는
방법이 있나요?



일반적인 EPP 고도화 목적

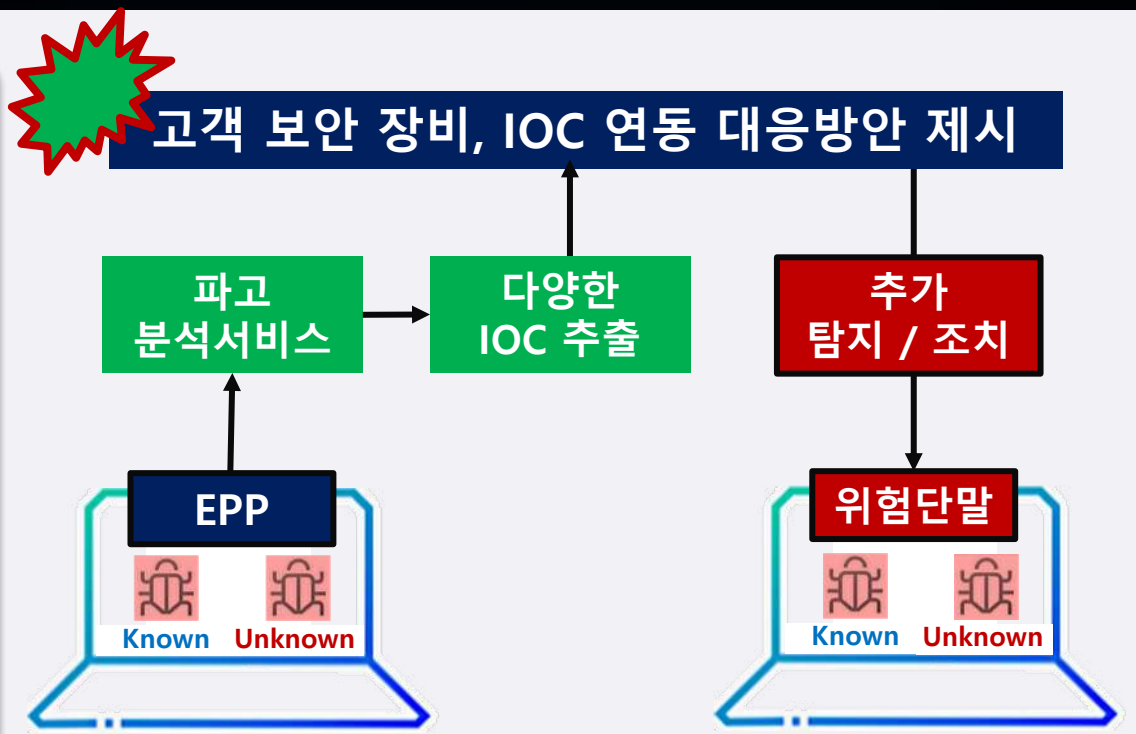
- EPP 설치된 시스템의, 자체보호
- 다른 EPP 설치된 시스템에, IOC 공유

EPP 미설치 시스템
엔드포인트
고도화
사각지대 존재

Unmanaged, Invisible 시스템

고객사 요구사항 – 1 (대응 방안 제시)

- 고객사에서 **EPP가 실제로 차단한 모든 멀웨어로부터 추가정보** 추출
  - 구체적인 멀웨어 "종류 / 목적" 조사
  - IOC 추출
    - IP, URL, C2
    - 프로세스
    - 스크립트
    - 레지스트리
    - 특정 파일
    - 파워쉘
- 고객사 보안솔루션과 실질적인 **위협정보 연동/대응 방안** 제시
  - Firewall
  - NAC
  - 자산관리 솔루션
  - 패치관리 솔루션



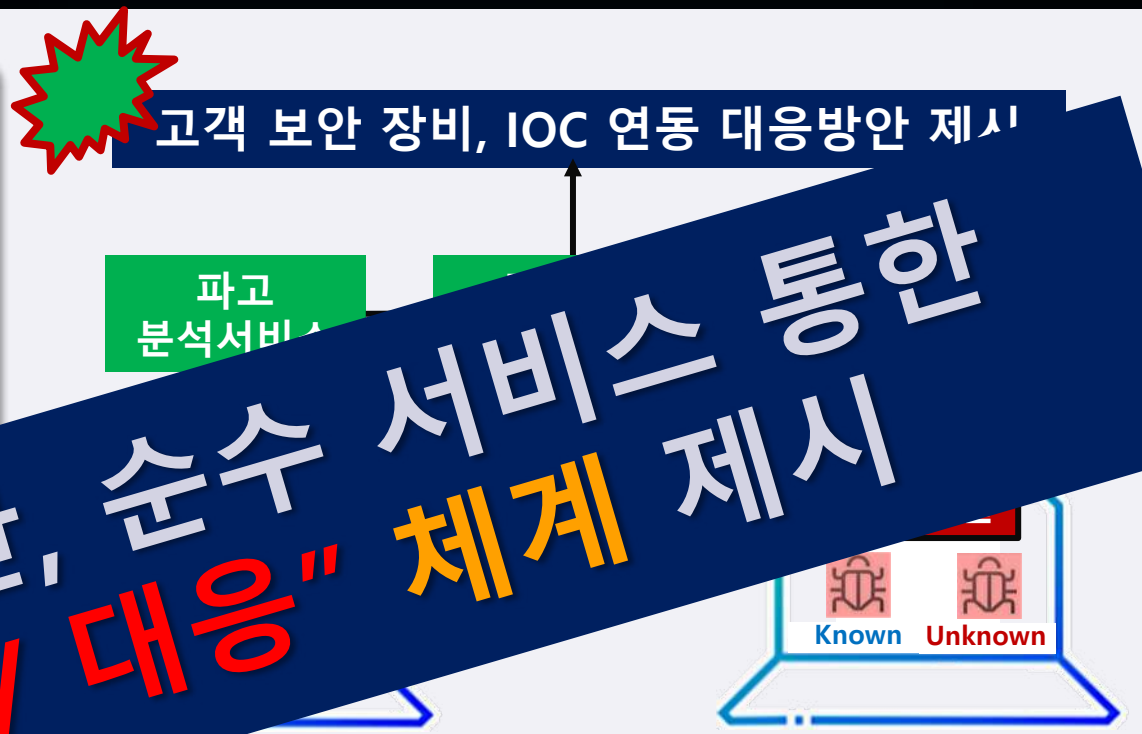
EPP + 매니지드 서비스 도입 이후

- 성공적으로 차단된 멀웨어의, 구체적인 정보 추출
- 공격 시도한(차단된) 위협의 구체적인 가시성 제공
- EPP 미설치된, 시스템 보호를 위한, 탐지 / 대응방안 제시
- 실질적인 IOC 창출 및 공유 / 연동 체계 제시

고객사 요구사항 – 1 (대응 방안 제시)

- 고객사에서 **EPP가 실제로 차단한 모든 멀웨어로부터 추가정보 추출**
  - 구체적인 멀웨어 "종류 / 목적" 조사
  - IOC 추출
    - IP, URL, C2
    - 프로세스
    - 스크립트
    - 레지스트리
    - 특정 파일
    - 파워쉘
- 제시
  - 관리 솔루션

EDR 솔루션은 아니지만, 순수 서비스 통한 또 다른 수준의 "탐지 / 대응" 체계 제시



EPP + 매니지드 서비스 도입 이후

- 성공적으로 차단된 멀웨어의, 구체적인 정보 추출
- 공격 시도한(차단된) 위협의 구체적인 가시성 제공
- EPP 미설치된, 시스템 보호를 위한, 탐지 / 대응방안 제시
- 실질적인 IOC 창출 및 공유 / 연동 체계 제시

고객사 요구사항 – 2 (질문)

엔드포인트
Protection Rate를
많이 높였어요.

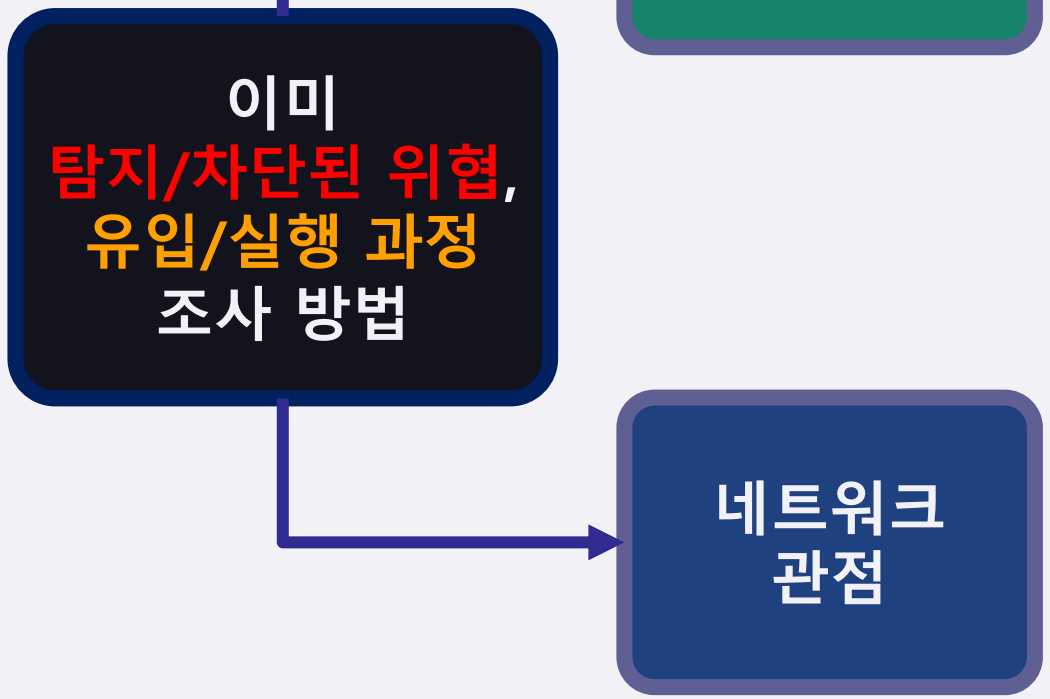
그런데,
탐지/차단된
위협 유입경로는
어떻게 되나요?

위협 관련, "육하 원칙" 을 알면,
엔터프라이즈 보안성을
추가로 더 강화할 수 있기 때문

- 누가 (Who)
- 언제 (When)
- 어디서 (Where)
- 무엇을 (What)
- 어떻게 (How)
- 왜 (Why)

추가
보안성
강화 위해
필요

고객사 요구사항 – 2 (대응 방안 제시)



- 침투 / 실행 순서 및 경로
- 사용자 권한
- 시스템 권한
- 어떤 애플리케이션 통해서
- 관련 파일
- 관련 레지스트리
- 관련 프로세스
- 관련 스크립트
- 관련 명령어
- 관련 목적지(C2)

➡ **EDR**

- FW 로그 조사
- NW 트래픽 조사
- 주변 시스템 로그 조사

➡ **NDR**
SIEM
SOAR
(Playbook)

고객사 요구사항 – 3 (질문)

엔드포인트
보안 솔루션이
탐지/차단하지 못한
위협을

조기에
발견하고, **대응** 할 수 있는
방법이 있나요?

위협이 있는데도, **탐지 못한건지 ?**
위협 자체가 안들어와서 **깨끗한건지 ?**

- 우리 인프라는 문제 없나요?

보이지
않는 적이
가장
두려움

고객사 요구사항 – 3 (대응 방안 제시)

언제 나타날지 모르는, 알기 어려운 위협을 어떻게 탐지/대응 할 것인가?

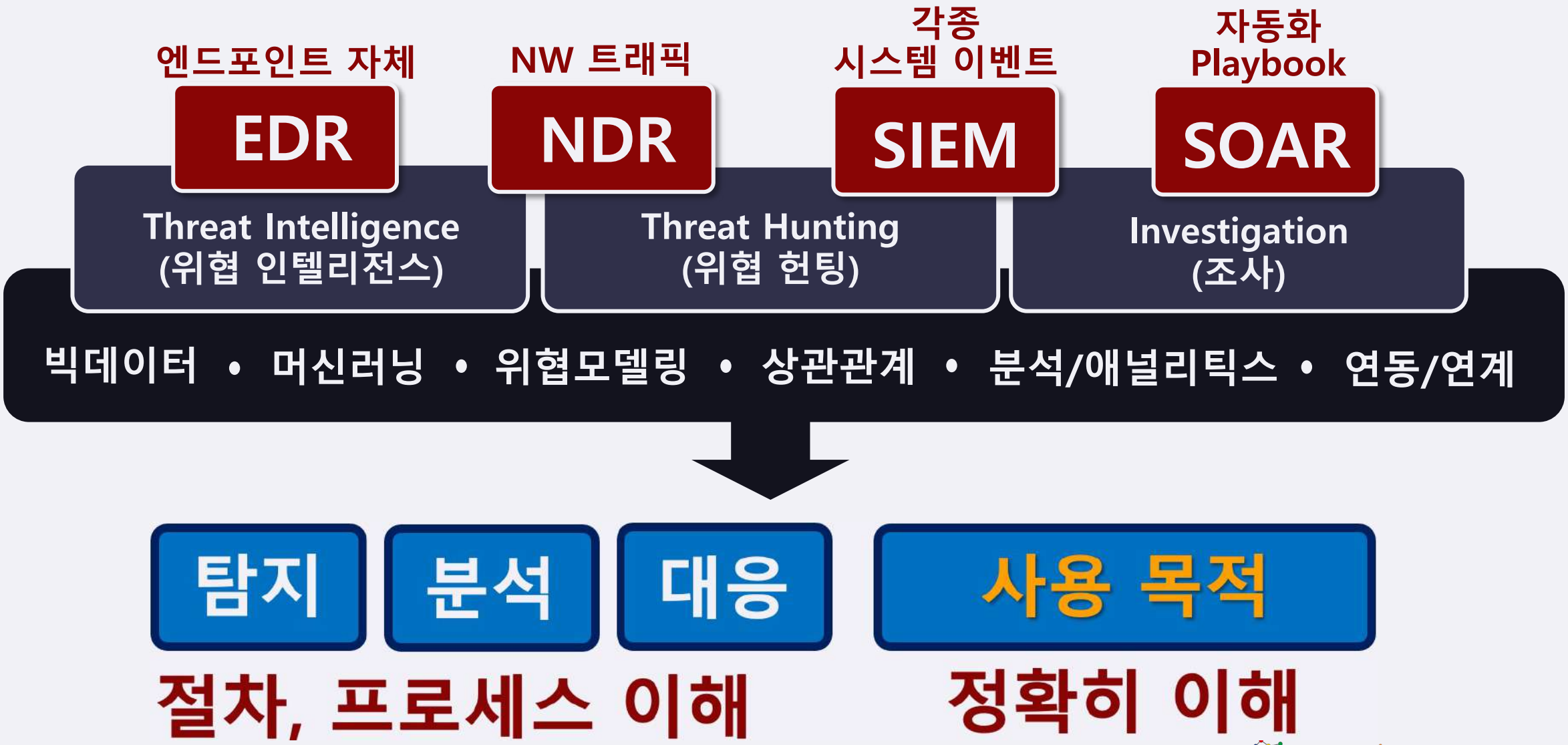
Gartner 방법론

- Adaptive Security Architecture
- CARTA (Continuous Adaptive Risk & Trust Assessment

엔드포인트 자체	NW 트래픽	각종 시스템 이벤트	자동화 Playbook
EDR	NDR	SIEM	SOAR
Threat Intelligence (위협 인텔리전스)	Threat Hunting (위협 헌팅)		Investigation (조사)

빅데이터 • 머신러닝 • 위협모델링 • 상관관계 • 분석/애널리틱스 • 연동/연계

탐지 / 대응 플랫폼 - 제자리 찾아가는 중 !!



그런데,
무엇을 더
고려해야 할까요?

XDR 출현
(통합 보안분석, 탐지/대응 플랫폼)

파고네트웍스 - 전략 1단계 (2017~2020)

AI - Machine Learning
엔드포인트 프로텍션 플랫폼

CYLANCE
BlackBerry

OT / ICS 환경의 PC, Server | Datacenter Server | Cloud Server

deepinstinct
BEFORE YOU KNOW IT

Server | User PC , VDI | POS KIOSK | Mobile

AI - Deep Learning
엔드포인트 프로텍션 플랫폼

PAGO NETWORKS

DeepACT

매니지드 탐지 및 대응 서비스 플랫폼

DeepACTOR
(Threat Research /분석가)

DeepACT 대쉬보드 / 콘솔

DeepACT IOC, TIDB
타 보안 솔루션 연동 체계

- Firewall
- EPP / EDR
- NTA / NDR
- SIEM / SOAR

엔드포인트
Protection Rate 최대화
실제 사례 증명 !!

DeepACT 커뮤니티
(IOC/위협정보 상호공유)

- For
  PAGO Customers
  (DeepACT Community)
- For
  Non-PAGO Customers

PAGO NETWORKS STELLAR CYBER

파고네트웍스 - 전략 2단계 (2021~)

AI - Machine Learning
엔드포인트 프로텍션 플랫폼

CYLANCE
BlackBerry

OT / ICS 환경의 PC, Server
Datacenter Server
Cloud Server

deepinstinct
BEFORE YOU KNOW IT

Server
User PC , VDI
POS KIOSK
Mobile

AI - Deep Learning
엔드포인트 프로텍션 플랫폼

PAGO NETWORKS

DeepACT
매니지드 탐지 및 대응 서비스 플랫폼

XDR
통합 플랫폼

SIEM
NDR
EBA
UBA
ATH
SOAR

DATA LAKE

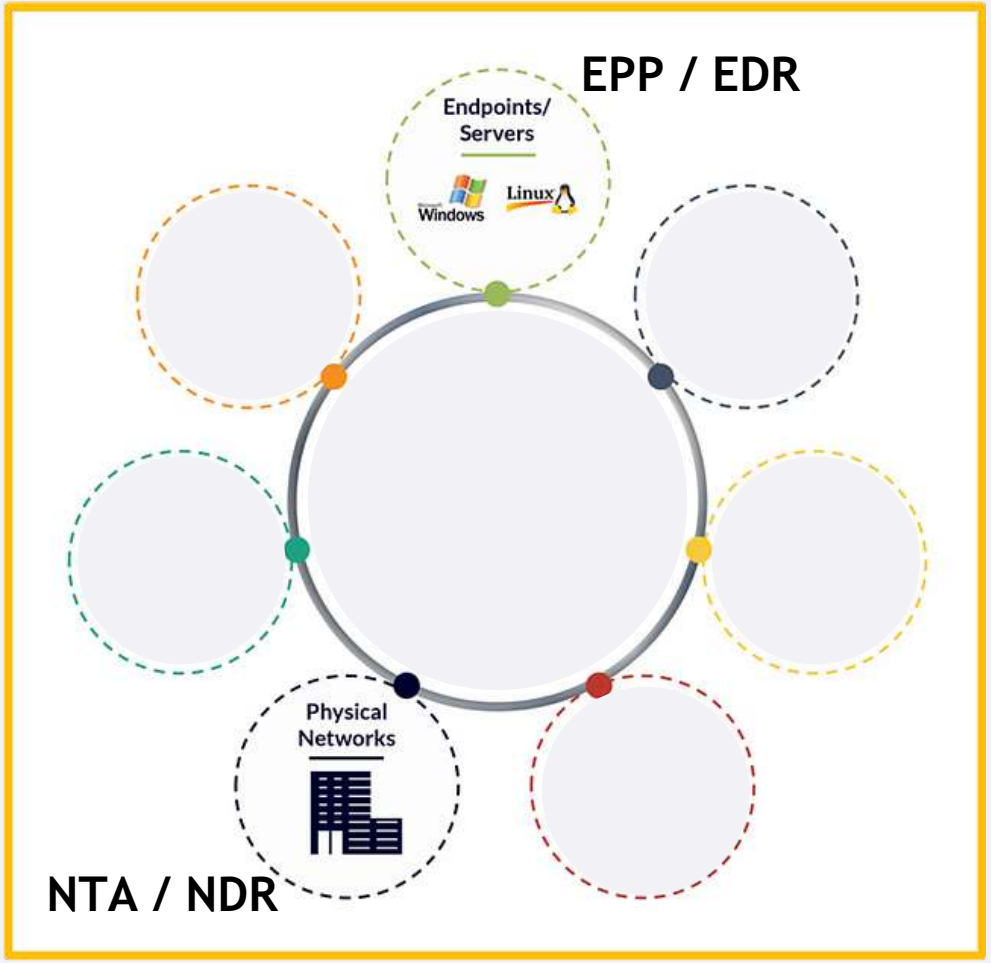
RAW DATA - EVENTS - ASSETS

NETWORKS
ENDPOINTS
CLOUD
APPLICATION
USERS

DATA SOURCES

XDR 이해 ➔ X = eXtended (데이터 소스 확장)

- **eXtended Detection & Response**



XDR 이해 ➔ X = eXtended (데이터 소스 확장)

- eXtended Detection & Response

XDR

엔드포인트 자체	NW 트래픽	각종 시스템 이벤트	자동화 Playbook
EDR	NDR	SIEM	SOAR
Threat Intelligence (위협 인텔리전스)	Threat Hunting (위협 헌팅)	Investigation (조사)	

빅데이터 • 머신러닝 • 위협모델링 • 상관관계 • 분석/애널리틱스 • 연동/연계

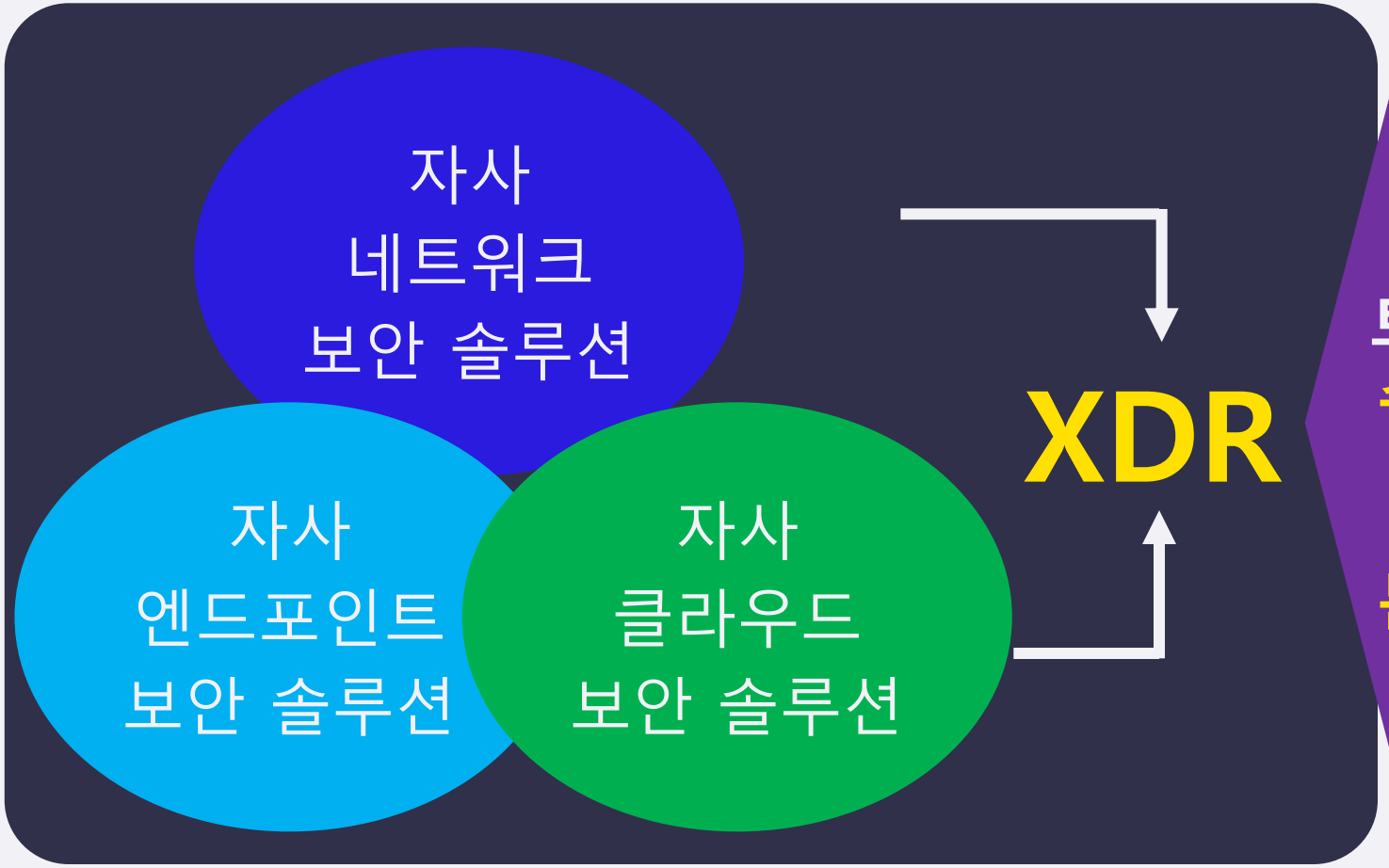
01	**COLLECT (수집)** 네트워크 / 시큐리티 센서, 에이전트 센서 이용
02	**DETECT (탐지)** 크리티컬 위협 탐지. 위한, 머신러닝 적용
03	**INVESTIGATE (조사)** 외부 위협, 내부 위협 조사를 위한 히스토리 데이터 검색
04	**RESPOND (대응)** 방화벽 연동, 알람 발생, 자동화된 보고서 생성

XDR 고려사항

통합 보안분석, 탐지/대응 플랫폼

XDR 플랫폼 주요 흐름 (특정 벤더 중심)

자사 제품 중심, XDR 고려사항



타시스템
트래픽, 이벤트
수용 제약 존재

상관관계
분석 제약 존재

타 벤더
네트워크
보안 솔루션

타 벤더
엔드포인트
보안 솔루션

OS,
애플리케이션

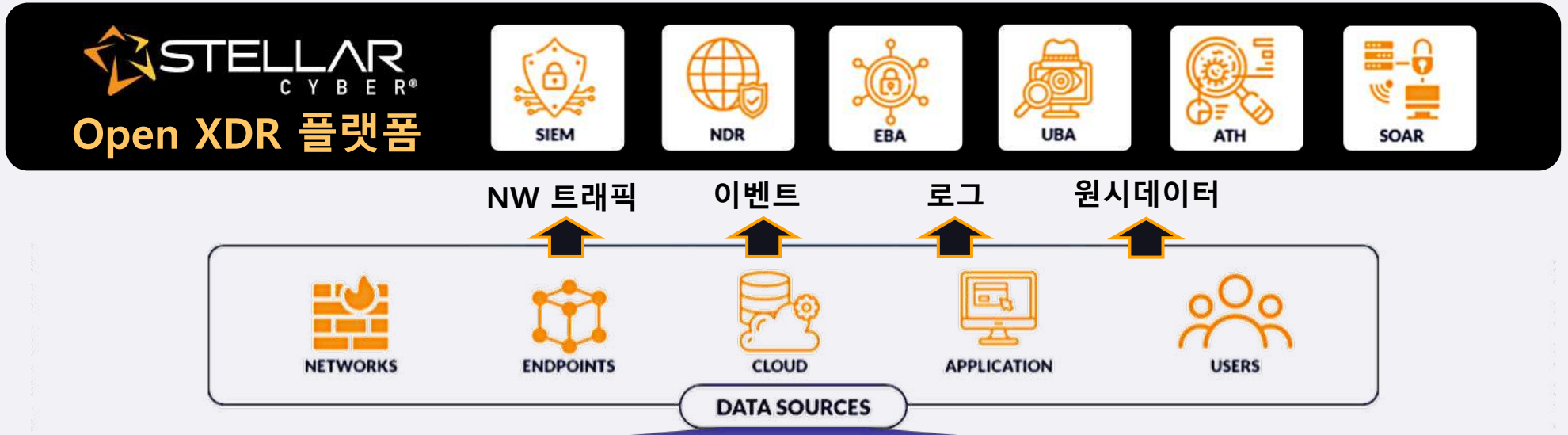
XDR 플랫폼 제대로 작동하려면 …

- 이기종
- 정형
- 비정형

✓ 데이터,
✓ 트래픽,
✓ 이벤트,
✓ 로그,

빅데이터
+
AI
+
MDR
SOC
플랫폼

Open XDR 플랫폼 조건



다양한 벤더 연동
종속성 없음

데이터 소스
유형 상관 없음

빅데이터, ML 기반
이기종 데이터 분석

SOC 기반, 통합 위협
탐지/대응 플랫폼

매니지드 탐지 및 대응 서비스 제시

PAGO NETWORKS

DeepACT

매니지드 탐지 및 대응 센터

MDR-as-a-Service | SOC-as-a-Service

STELLAR CYBER

Open XDR 플랫폼

SIEM | NDR | EBA | UBA | ATH | SOAR

NW 트래픽 | 이벤트 | 로그 | 원시데이터

NETWORKS | ENDPOINTS | CLOUD | APPLICATION | USERS

DATA SOURCES

다양한 벤더 연동 **종속성 없음**	데이터 소스 **유형 상관 없음**	빅데이터, ML 기반 **이기종 데이터 분석**	SOC 기반, 통합 위협 탐지/대응 플랫폼

PAGO NETWORKS STELLAR CYBER

PAGO DeepACT – 매니지드 탐지/대응

PAGO 매니지드 탐지/대응 서비스 개요

- 더 많은 소스로부터
- 더 깊게
- 더 자세히
- 이미 탐지된 위협 대상 추가 분석
- 아직 탐지되지 않은 위협 헌팅

- 예측 대응
- 능동 대응
- 보고서
- 가이드 라인
- 연동 (수동 / 자동)

PAGO MDR 서비스 제공 범위 (For 모든 고객)

PAGO NETWORKS DeepACT

- 위협 클리닝 서비스
- 정책 설정 서비스 (파고네트웍스가 제안/적용한 보안 솔루션 정책 설정)
- 긴급 위협 대응 서비스 (멀웨어, 이메일, 악성문서 등에서 크리티컬한 목적의 위협 경우)
- 온-디맨드 위협 분석 및 대응 서비스 (제품과 상관없이, 고객이 의뢰해온 위협 분석)
- 탐지 / 차단된 위협으로부터, IOC 추출 및 TIDB 생성 (Threat Insights DB)
- DeepACT 커뮤니티 운영 (for Sharing IOC, As Threat Intelligence Source)
- 위협 헌팅 서비스 (using IOC from BlackBerry, Deep Instinct, Stellar Cyber)
- 타겟팅 침해여부 진단 서비스 (예 – Hafnium 침해여부 진단 서비스)
- 타겟팅 사고대응 서비스 (예 – 특정 서버/시스템 침해사고 발생 시, 고객 의뢰의 경우)
- 보안 연동 서비스 (예 : Managed FW 정책 서비스, TI-Exchange 서비스, SOAR 서비스)

PAGO DeepACT 탐지/대응 서비스 목적

이미
기업 업무 환경에
침투해 있는
위협(멀웨어)
탐지, 능동대응

새로이
기업 업무 환경에
침투하는
위협(멀웨어)
탐지/격리, 능동대응

고객과 협업 및 위협 공동대응 플랫폼 구축

프로텍션 극대화, 위협 클리닝, 지속적인 보안성

DeepACT
매니지드탐지 및 대응

PAGO NETWORKS

MDR-as-a-Service

SOC-as-a-Service

영업문의 - Sales@pagonetworks.com

기술문의 - Tech@pagonetworks.com