THE ENTERPRISE IMMUNE SYSTEM

사이버 면역 시스템

The World’s Leading Cyber AI

Darktrace

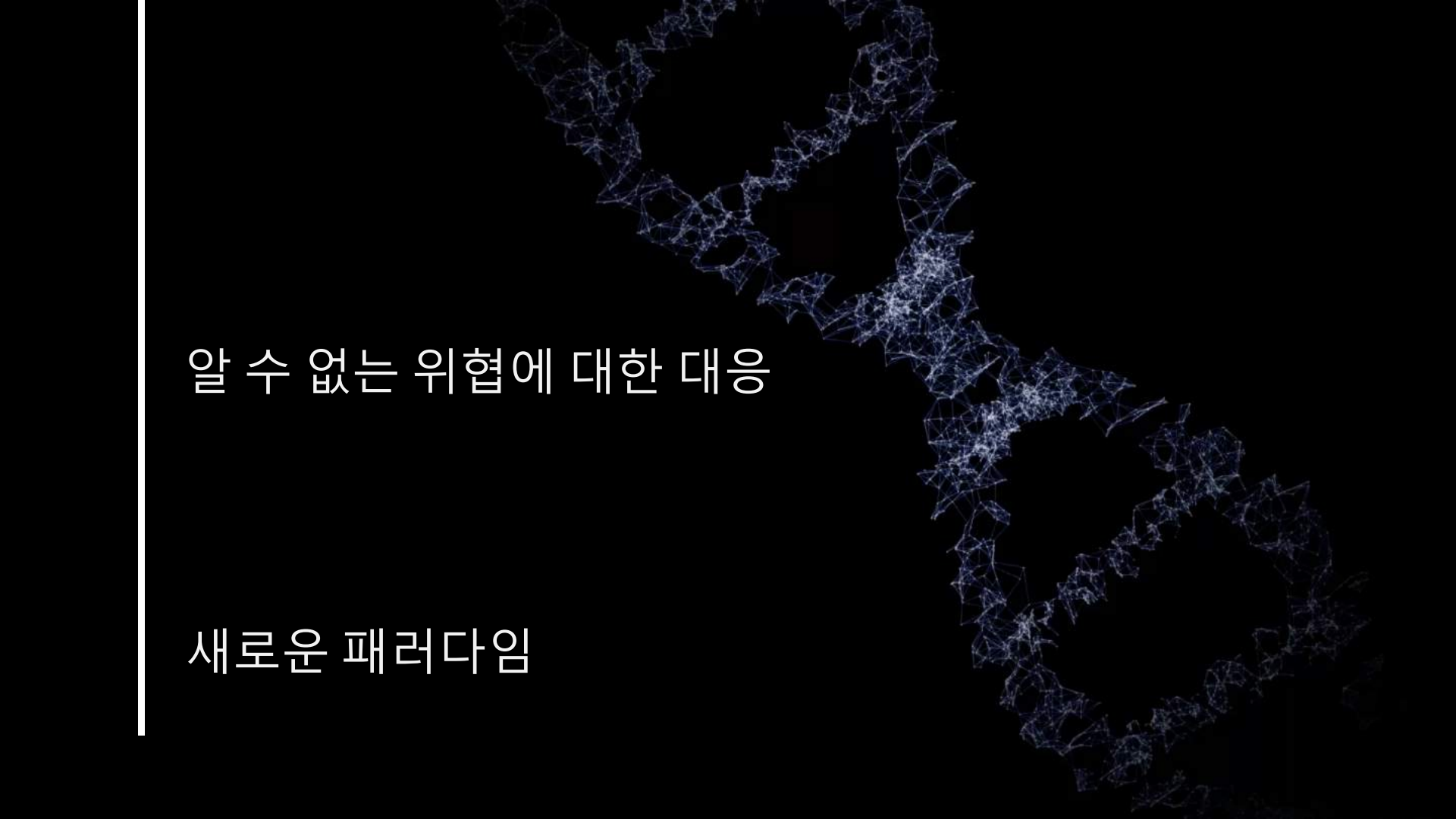
DARKTRACE

영국 캠브리지에서 2013년 7월 설립

- 2015년 10월 한국지사 설립
- 유명 수학자들과 영국/미국 정보요원

들의 협업으로 시작

- 머신러닝과 수학적 알고리듬에서 착안
- 약 2000여개 이상 수상 실적



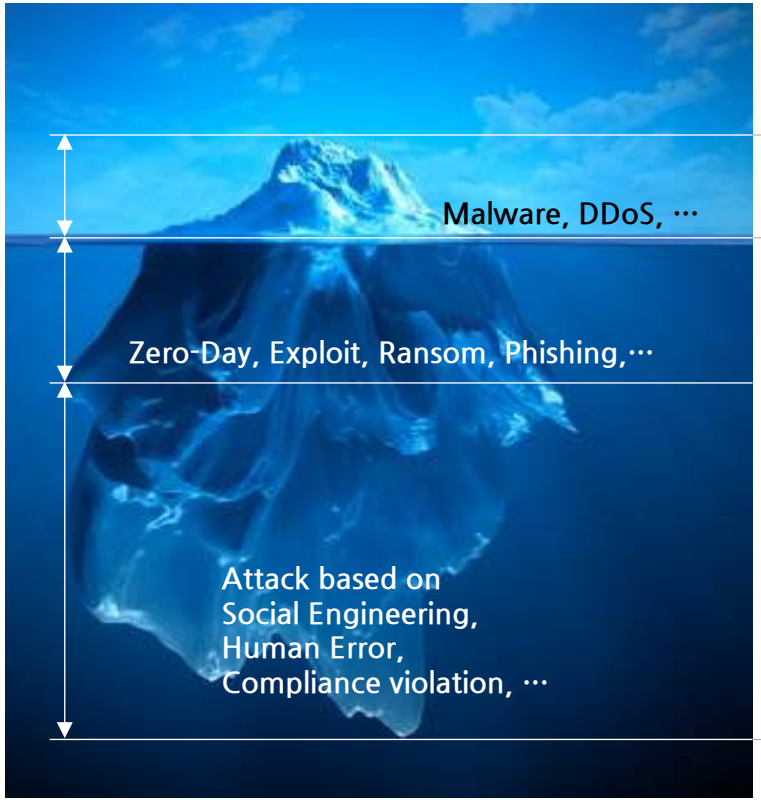
알 수 없는 위협에 대한 대응

새로운 패러다임

새로운 패러다임의 필요

DARKTRACE

[알려지지 않거나 경험한 적 없는 위협 대응 기술은 필연]



위협의 식별	대응 기술/방안
알려진 위협 Known Threat	시그니쳐,룰,시나리오
알려지지 않은 위협 UnKnown Threat	머신 러닝 자동화
비정형위협 Unusual / UnSeen Threat	No Rule, No Signature

Why Rules Don’t Work?

DARKTRACE

룰 기반의 접근방식

- 대상 PC가 오늘 새로운 호스트와 통신 했는가?
- 대상 PC가 알려진 악성 사이트에 접속 했는가?
- 대상 유저가 새로운 PC에서 로그인 했는가?
- 대상 PC가 알려진 스캐닝 방법으로 내부 통신을 했는가?
- 대상 PC가 내부 정보를 다운받기 위해 시도하고 실패 했는가?
- 대상 PC가 알려진 취약성을 이용해 다른 내부 접속을 했는가?
- 대상 문서가 알려진 악성 프로그램을 포함하고 있는가?

룰 기반의 한계점

- 알려진 모든 공격에 대한 DB가 있어야 함
- **어제의 공격을 포함한 모든 정보가 업데이트 되어야 있어야 함**
- **알려지지 않은 신종 공격에 대한 추측(Guess)에 의존해야 함**
- 고객사의 업무 흐름을 100% 이해하고 튜닝 해야함
- **너무 많은 오탐이 발생 함**
- 전담 인력이 항상 관리 해야 함

알 수 없는 방대한 공격 벡터

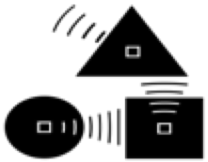
DARKTRACE

Advanced Persistent Threats
지능적 지속 위협
제로 데이성 공격은 10번의 시도중 9번은 성공할 정도로 탐지가 거의 불가능 합니다.

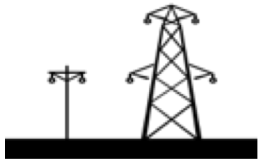
Mobile Security & Protection
모바일 장치 보안 및 보호
모바일 장치의 사용이 증가함에 따라, 스팸, scam 및 위협이 이러한 장치에 맞게 조정 될 것이며 Bootkits과 같은 모바일 멀웨어는 제거하기 더욱 힘들어 질 것입니다.

Social Media Protection(SNS)
소셜 미디어
전자 메일은 여전히 중요한 공격 백터이고, 소셜 미디어를 통한 scam은 70%이상이 수동으로 공유가 됩니다.

Internet of Things
사물 간 인터넷 (IoT)
사물 간 인터넷에 사용되는 허브, 스위치, 라우터들은 인터넷연결과 저장 및 처리가 가능하며 네트워크를 공격하기 위한 수단으로 사용됩니다.



Insider Threats
내부 위협
조직원은 물론 민감한 정보에 액세스 할 수있는 관리자와 같이 권한이 부여 된 사용자는 조직에 가장 큰 내부 위협 요소가 될 수 있습니다. 손상된 계정 자격 증명 또는 누군가의 계정이 도용 된 경우 또한 내부 위협이 될 수 있습니다.



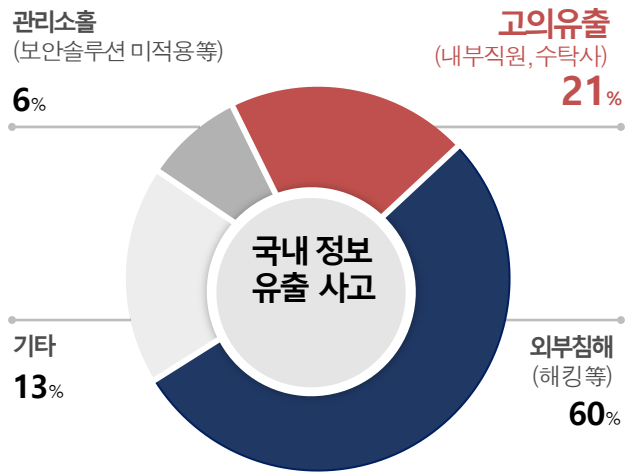
Critical Infrastructure
주요 기반 시설 공격
가장 중요한 추세로는 악성코드를 사용하여 감시 제어 데이터 수집 시스템 (SCADA) 및 홈리스 관리 정보 시스템(HMIS) 등을 감염 시켜 데이터를 탈취하는 공격 등이 있습니다.

내부자 위협 대응기술 부족

DARKTRACE

내부자에 의한 유출사고는 전체 유출사고의 21%에 달하는 주요 위협 원인이나
현재 보안기술의 핵심 대응 목표에서 벗어나 있음으로, 이에 대한 기술적 대응책 마련 필요

유출사고의 21%는 내부고의유출



출처 : PASCON 2015, KISA "국내 정보유출사고('11~'14) 유형/원인별 분석

현재의 내부자 위협 대응기술은 시나리오 기반의 방어에 집중

- 시나리오 유출 / 제약에 따른 우회 위협 존재
- 생각의 한계를 뛰어넘는 유출기법 대응불가

Machine Learning / BigData 기반
내부자의 이상행위 탐지필요

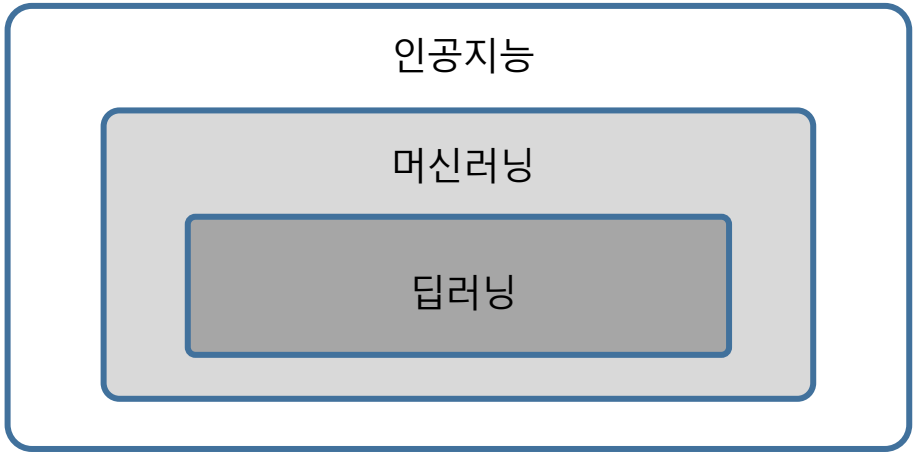
- **BigData :**
  내부 통신정보 수집/분석
- **Machine Learning :**
  평소와 다른 이상행위 자동탐지

클라우드 주요 위협 – Cloud Security Alliance(CSA) 보고서

DARKTRACE

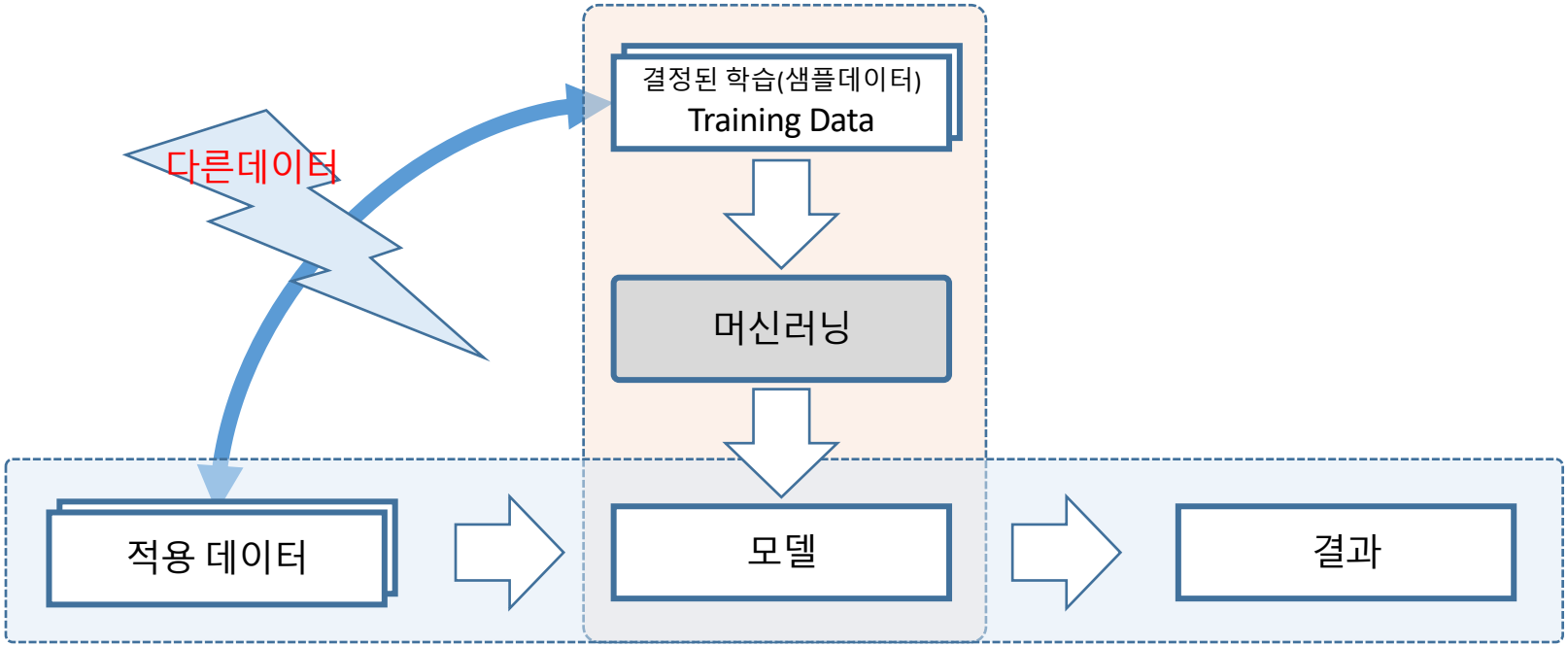
인공지능과 머신러닝

DARKTRACE



머신러닝의 난제

학습 과정 (Modeling)
추론 (Inference)
일반화 (Generalization)



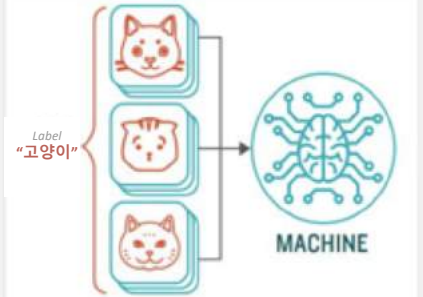
Machine Learning & AI – Enterprise Immune System

DARKTRACE

지도 학습 동작 방법

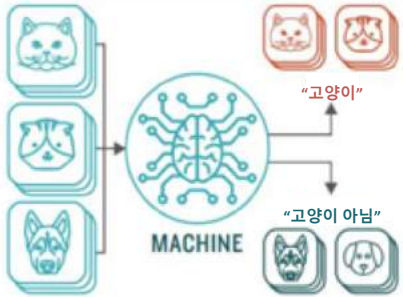
STEP 1

데이터에 대한 **레이블(Label)-명시적인 정답-이 주어진 상태에서 컴퓨터를 학습시키는 방법**

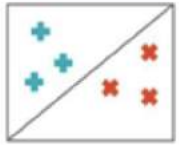


STEP 2

레이블(label)이 지정되지 않은 테스트 데이터셋 (test set)을 이용해서, 학습된 알고리즘이 얼마나 정확히 예측)하는지를 측정

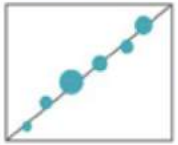


TYPES OF PROBLEMS TO WHICH IT'S SUITED



사전 분류

아이템 카테고리 별 분류



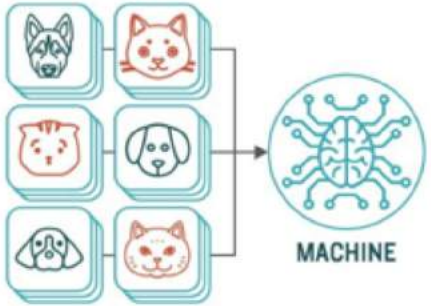
회귀 분석

실제적 가치 비교 (원화, 무게 등)

비지도 학습 동작 방법

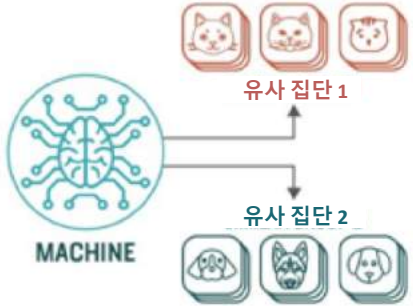
STEP 1

데이터에 대한 레이블(Label)-명시적인 정답-이 주어지지 상태에서 컴퓨터를 학습



STEP 2

비지도 학습은 데이터의 숨겨진(Hidden) 특징(Feature)이나 구조를 발견



TYPES OF PROBLEMS TO WHICH IT'S SUITED

군집화

비슷한 특징으로 집단 분류

예시: 아래와 데이터가 무작위로 분포되어 있을때, 이 데이터를 비슷한 특성을 가진 세가지 부류로 묶는 클러스터링

이상행위 탐지

평소와 다른 것을 구분

예시: 한 번도 접속한 적이 없는 곳으로 지속적으로 C&C통신

비지도 학습 기반 머신 러닝

DARKTRACE

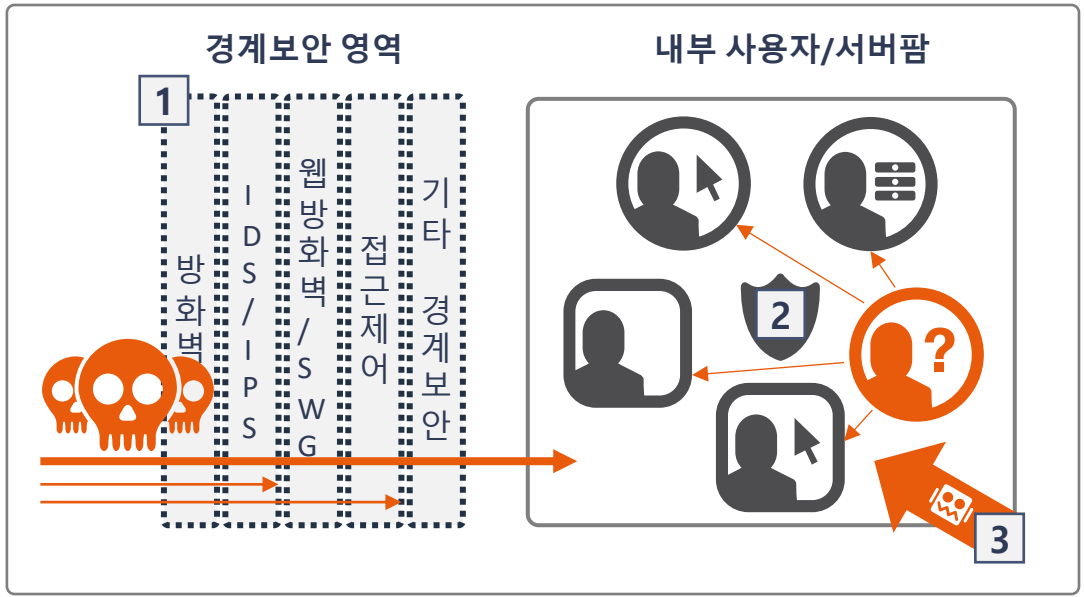
머신러닝엔진은 사람의 개입을 최소화하고 현재 많은 보안 대응 체계가 채택하고 있는 시그니처와 룰기반의 접근방법을 따르지 않습니다

Thought 사고 – 과거의 정보를 학습하여 판단에 필요한 인사이트를 제시합니다.
Real Time 실시간 – 시스템은 현재시점을 분석합니다.
Self-Improving 자가개선 – 새롭게 학습되는 정보를 통해 스스로 개선해 나갑니다

	Unsupervised Learning 비지도학습	**Supervised Learning 지도학습**
정의	• **학습 시 출력 값에 대한 정보 없이(교사 없이) 진행되는 학습** • **군집화, 밀도 추정, 차원축소, 특징 추출 등이 필요한 문제에 적합**	• 출력 결과 값을 미리 알려주는 '교사(supervised)'가 존재하는 학습 • 주로 인식, 분류, 진단, 예측 등의 문제 해결에 적합
사례	**동물과 관련된 데이터가 입력되면 수집된 데이터로부터 특징을 추출, 군집화, 추정을 통해 서로 다른 종으로 구분하여 분류**	파충류, 포유류 등 종에 대한 분류지표와 기준을 이미 입력시킨 후 컴퓨터로 하여금 어떤 종이 파충류인지 또는 포유류인지 분류

진화하는 위협 방어를 위한 발상의 전환이 필요

DARKTRACE



현재까지의 위협방어에 대한 접근 방법의 한계

1 경계보안의 강화를 통한 방어체계의 한계

많은 기업들과 기관들이 인터넷과 인트라넷/서버팜의 경계 구간의 강화를 통한 위협대응을 수행하고 있지만, 계속적으로 진화하는 공격의 방어와 대응에 한계가 있습니다.

2 행위에 대한 정상 및 합법여부 정의의 어려움

정상 및 합법적 행위여부를 정의하기 위한 많은 행위규칙(Rule)과 위협식별을 위한 시그니처들로부터 벗어난 다양한 행위들이 존재하고 있습니다.

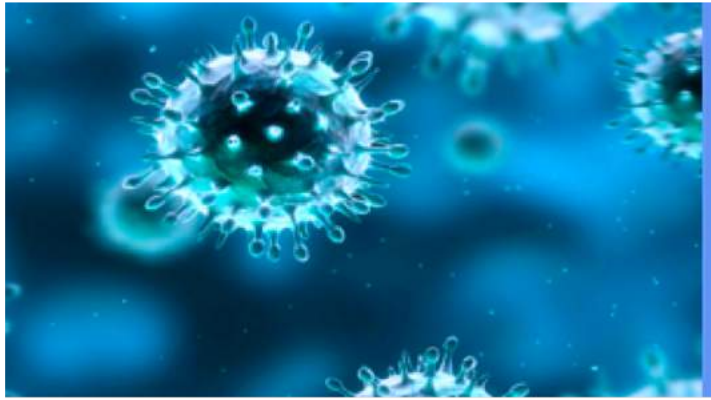
3 시스템과 기술을 뛰어 넘는 새로운 위협의 등장

악성코드, 봇넷, 사이버 범죄등의 종착지는 사람입니다. 인적 요소에 의한 내부정보탈취, 시스템파괴 및 다양한 위협의 발생빈도가 지속적으로 증가하고 있습니다.

Rule, Signature, Sandbox 등
알려지고 공유된 인텔리전스 기반을 보완할 새로운 접근방법 필요

새로운 접근: 면역시스템

DARKTRACE



Human Immune System

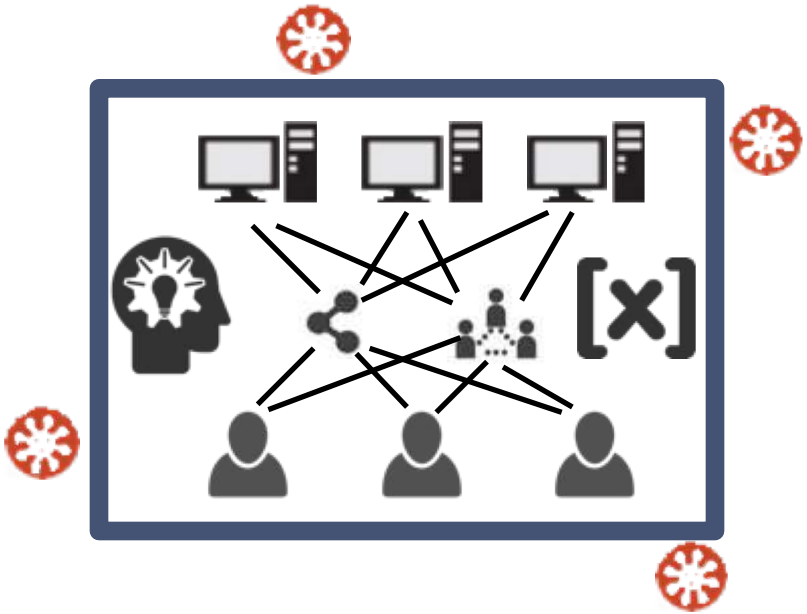
정상상태를 알고 있고, 이를 통해서 스스로 아픈 곳을
인지 하는 사람의 면역체계처럼
네트워크의 정상적인 상태 를 알고 있다면 비정상적인
행위는 쉽게 탐지 할 수 있습니다

Enterprise Immune System

생체 면역체계와 유사한 구조를 가진 EIS는 고급 수학공식과
머신러닝 기반 고도화된 기술을 통해
사이버 위협을 탐지 및 분석합니다.

정상 행위 자동 학습을 통한 비정상 행위 탐지

DARKTRACE



차세대 엔터프라이즈 면역 시스템

- **네트워크, 사용자, 디바이스의 다양한 행위에 대한 자동학습**

위협에 대한 개별요소들의 종합적인 연관상태를 분석하고 학습하여 정상상태와 비정상적인 상태를 식별한 후 규칙이나 시그니처를 기반으로 한 전통적인 시스템이 탐지하지 못한 위협과 공격을 식별합니다.시스템은 네트워크의 정상적인 상태를 학습하여 위협에 민감하게 반응하고 대응할 수 있는 보안 '면역체계"를 강화할 수 있습니다.

- **네트워크, 사용자, 디바이스에 대한 수학적 확률엔진의 '비정상적 행위' 순환적 확률 추론**

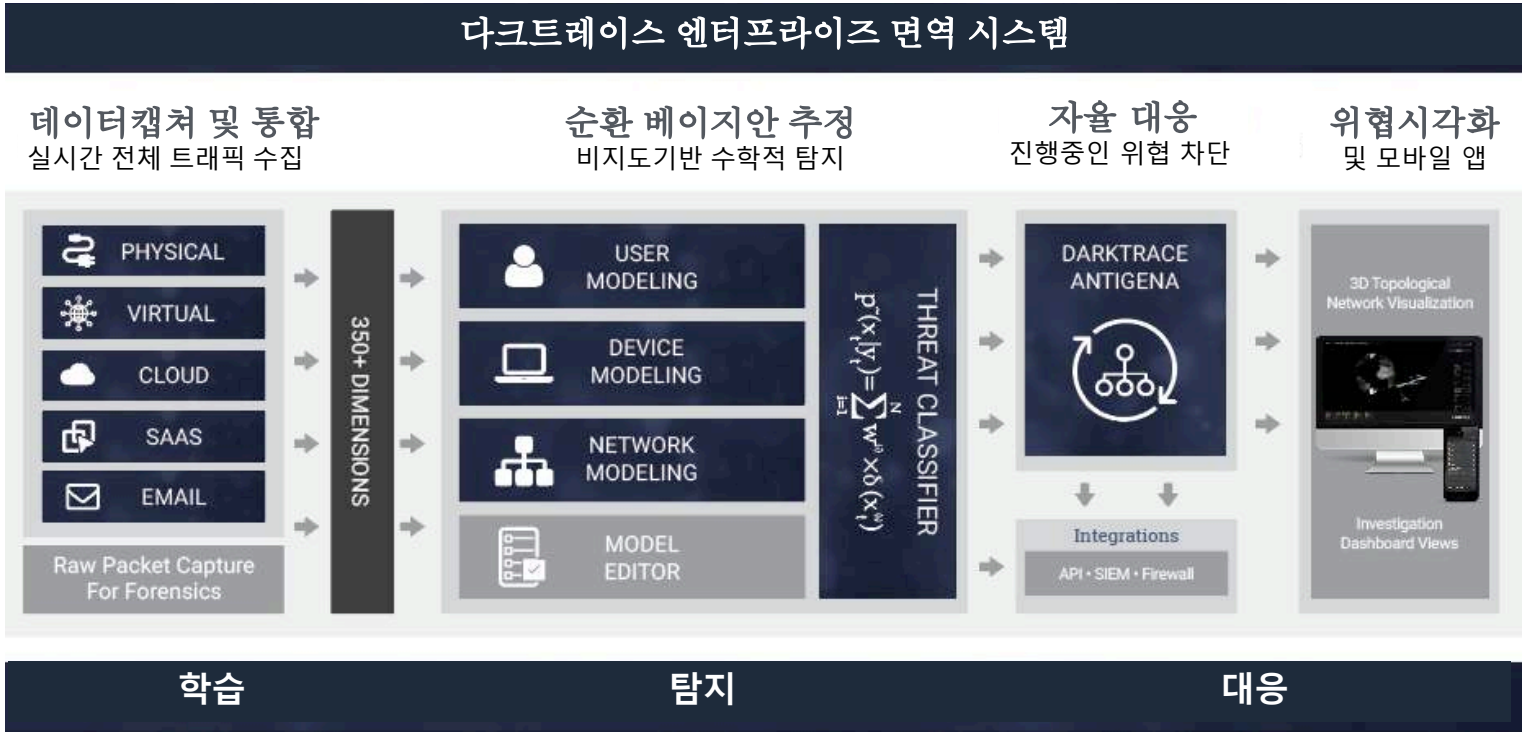
베이지안 순환 확률 모형(RBE), 순차적 몬테카를로(sMC), LASSO 모델등을 통해 고객 네트워크를 사용하는 사용자, 디바이스 및 행위에 대한 수학적 확률을 계산하여 지속적으로 '정상'상태를 확인하고 계산합니다.

인체의 면역기능을 응용한 네트워크, 사용자, 디바이스 기반 정상행위학습기반의 건강한 면역체계 구축

다크트레이스 솔루션 아키텍처

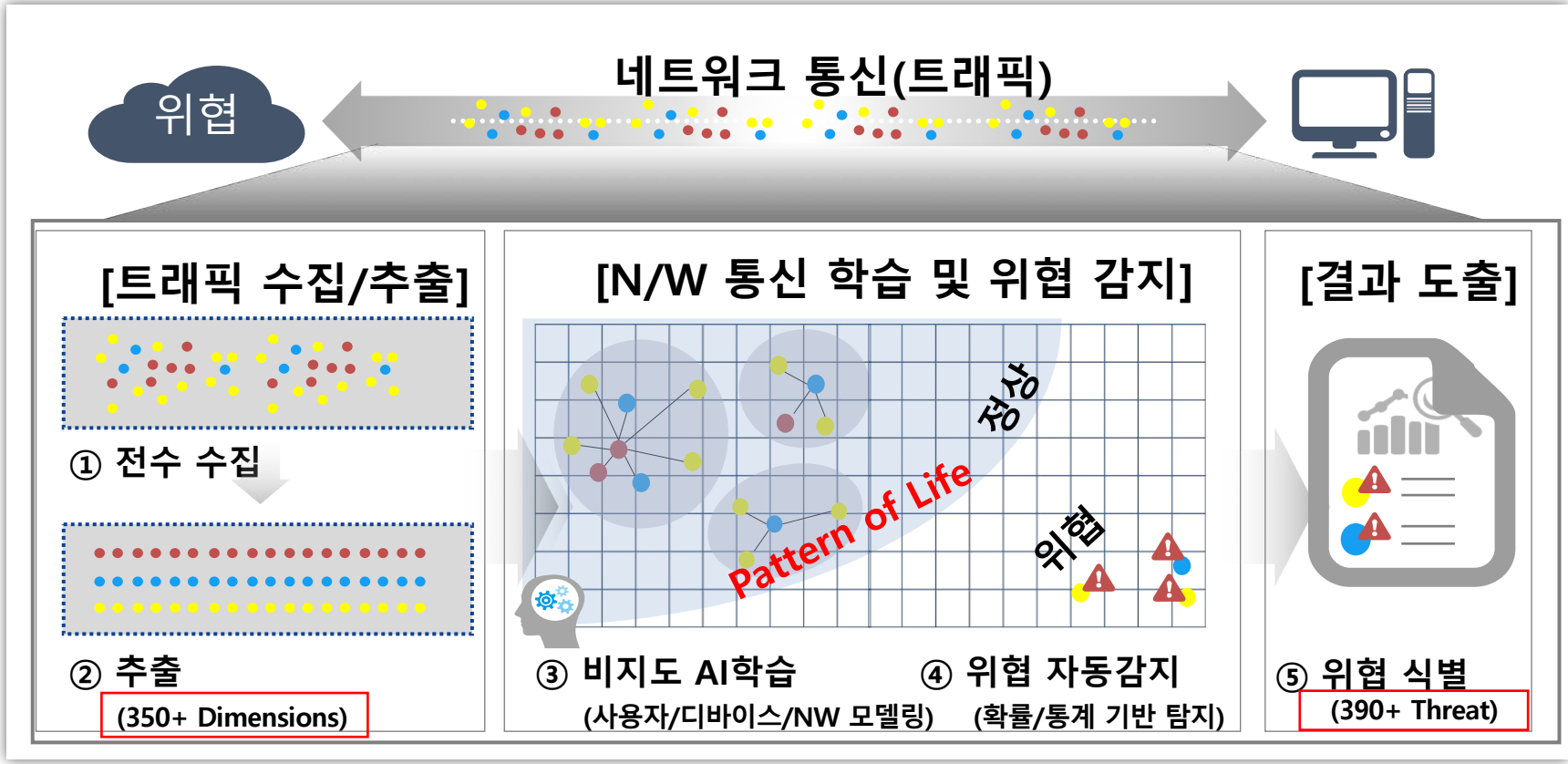
DARKTRACE

진화하는 위협을 방어하기 위해서는 새로운 접근법이 필요합니다.



1. 다크트레이스 Enterprise Immune System

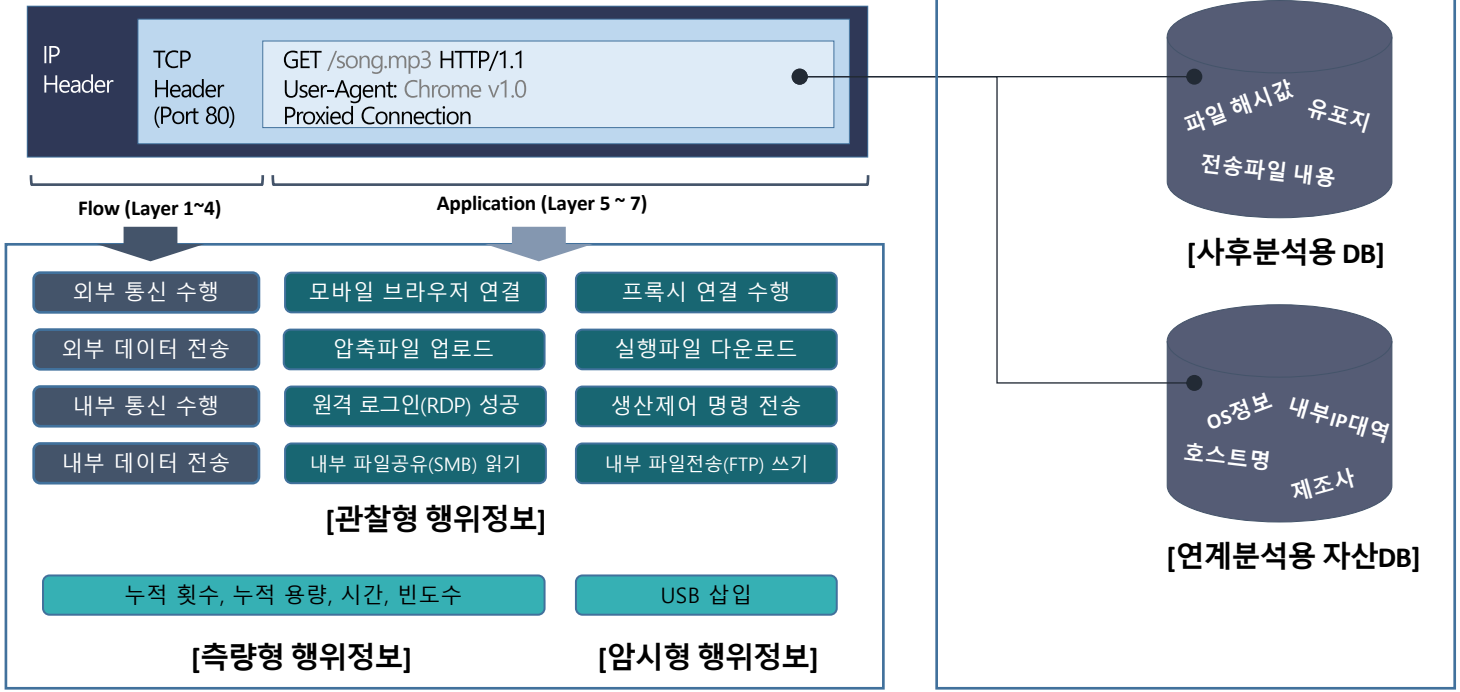
DARKTRACE



심층 트래픽 분석기술(DPI)

DARKTRACE

개별 네트워크에 최적화된 학습과 정확한 탐지를 뒷받침



350여종의 풍부한 학습지표

사후분석을 위한 재가공

자가학습을 통해 스스로 발전하며 오과탐을 최소화하는

DARKTRACE

고급 이상행위 탐지기술(Unsupervised Machine Learning)

행위 자체의 수상함
: Beaconing, DGA

군집 내에서의 유별성
: Clustering

과거 패턴과의 불일치
: Single Extreme Feature,
Multi Extreme Feature

전체에서의 희귀성
: Rareness

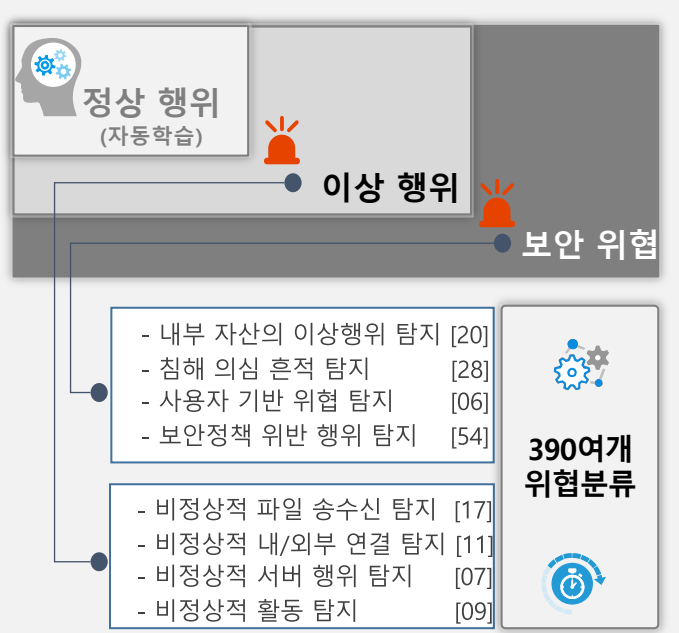
회귀적 베이즈 추론 기반의 위협 확률 계산 (Classifier)

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)} = \frac{L(A|B)P(A)}{P(B)}$$

15% 60% 95%

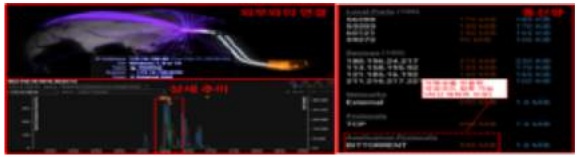
사용자의 이해도와 활용도를 높이는Explainable AI 기술 (XAI) DARKTRACE

[250여개의 검증된 보안위협 분류 모델]



1단계: 탐지 사유 및 가이드 확인

2단계: 정황 및 통계 확인



3단계: 상세 통신내용에 대한 추가 확인

※ 관련 PCAP파일 추출로 증거 확보 가능

사용자 + 디바이스 + 네트워크 행위 학습/추론/시각화

DARKTRACE

기존 보안 솔루션과의 탐지 방식 비교

DARKTRACE

기존 보안 장비

증상 : 악성 링크가 포함된 구글 문서 -> User agent및 IP 기반으로 리다이렉션

제시한 해결책

1. 관련된 모든 URL과 도메인 차단
2. 확인된 샘플의 AV Signature
3. 해당 User Agent에 대한 IPS룰

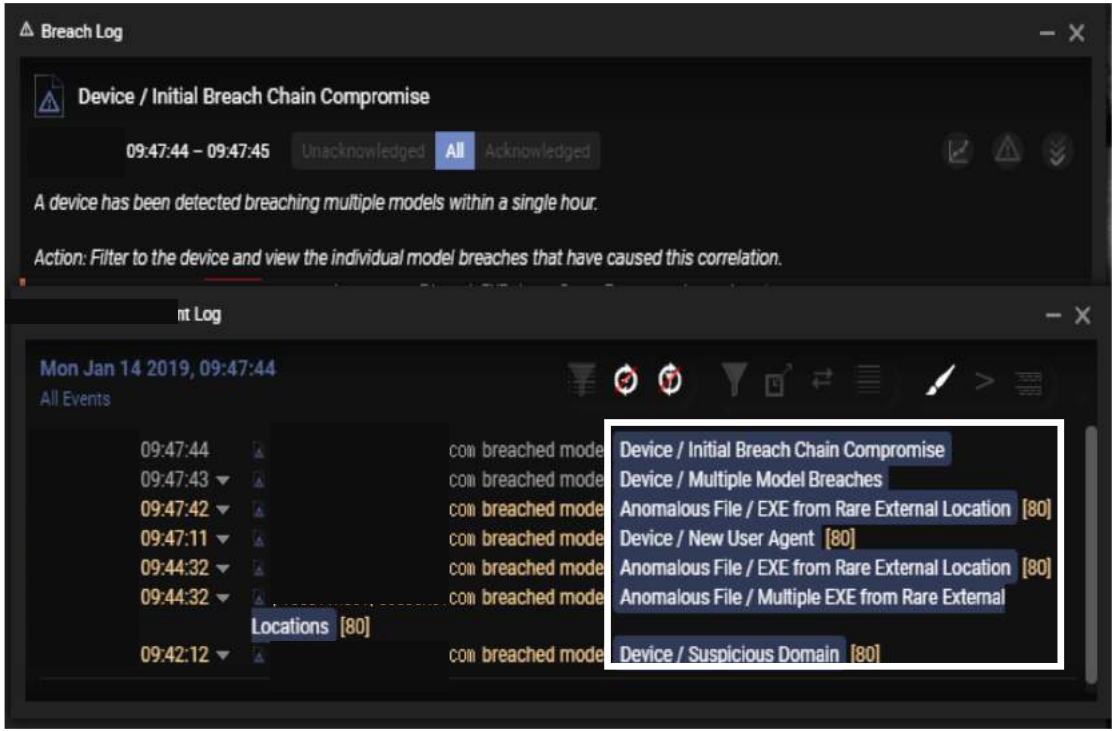
URL과 도메인, User Agent을 변경한 변종 위협 탐지 및 차단은?

https://www. .com/blog/threat-research/cookie-maker-inside-the-google-docs-malicious-network.html

기존 보안 솔루션과의 탐지 방식 비교

DARKTRACE

1. 의심스러운 도메인 접속
2. 희귀성이 높은 외부로 리다이렉션
3. 희귀성이 높은 외부 도메인에서 EXE파일 다운로드
4. New User Agent 발견
5. 하나의 Chain 이벤트 생성



다크트레이스 가치-핵심기술의 차별성

DARKTRACE

DARKTRACE

구분	기존 솔루션 제약사항	다크트레이스 특화기능
모든 IP통신 장치에 대한 행위분석 자동화 (디바이스)	• 주로 업무용PC 및 엔드포인트 행위중심 대응 (Windows, Linux, Mac 운영체계 기반) • IP 카메라, 프린터, IP Phone, Fax 등 IP통신에 따른 취약 공격대상의 행위분석 불가	모니터링/분석 구간내의 **모든 IP통신 디바이스**에 대한 이상 행위 탐지 및 분석대응
라이프사이클 학습을 통한 행동기반 탐지 (사용자)	• 사용자의 행위에 의해 발생 가능한 모든 경우의 수를 Rule, Pattern화 할 수 없음 • 내부자 위협 대응에 필요한 모델링 지원의 한계	• 네트워크상의 모든 행위에 대한 **라이프사이클 학습 및 이상행위의 식별** 자동화 • **망분리 환경에서의 비정형 위협**의 내부망 보호
지능형 공격 대응력 확대 (실시간 운영성능)	• 유출/침해에 대한 지능형 지속공격 방어를 위한 인텔리전스, Reputation DB의 지속적인 증가 및 관리 한계 (전담업무 대응능력의 한계) • 공격방어를 위한 인텔리전스 유지 및 성능 한계	• 수학적 이상행위분석 및 패턴식별을 위한 딥러닝 실행 (No Rule & No Signature) / 자동분석 • **경량의 실시간 대응력** 확보
직관적인 위협상황 시각화 및 재현(Dynamic 3D)	• Incident 에 대한 연관성 확인 및 추정에 대한 시간/인력 체증	상황재연 및 연결성에 대한 **보안이벤트 시각화를 통한 직관적 관리/대응**

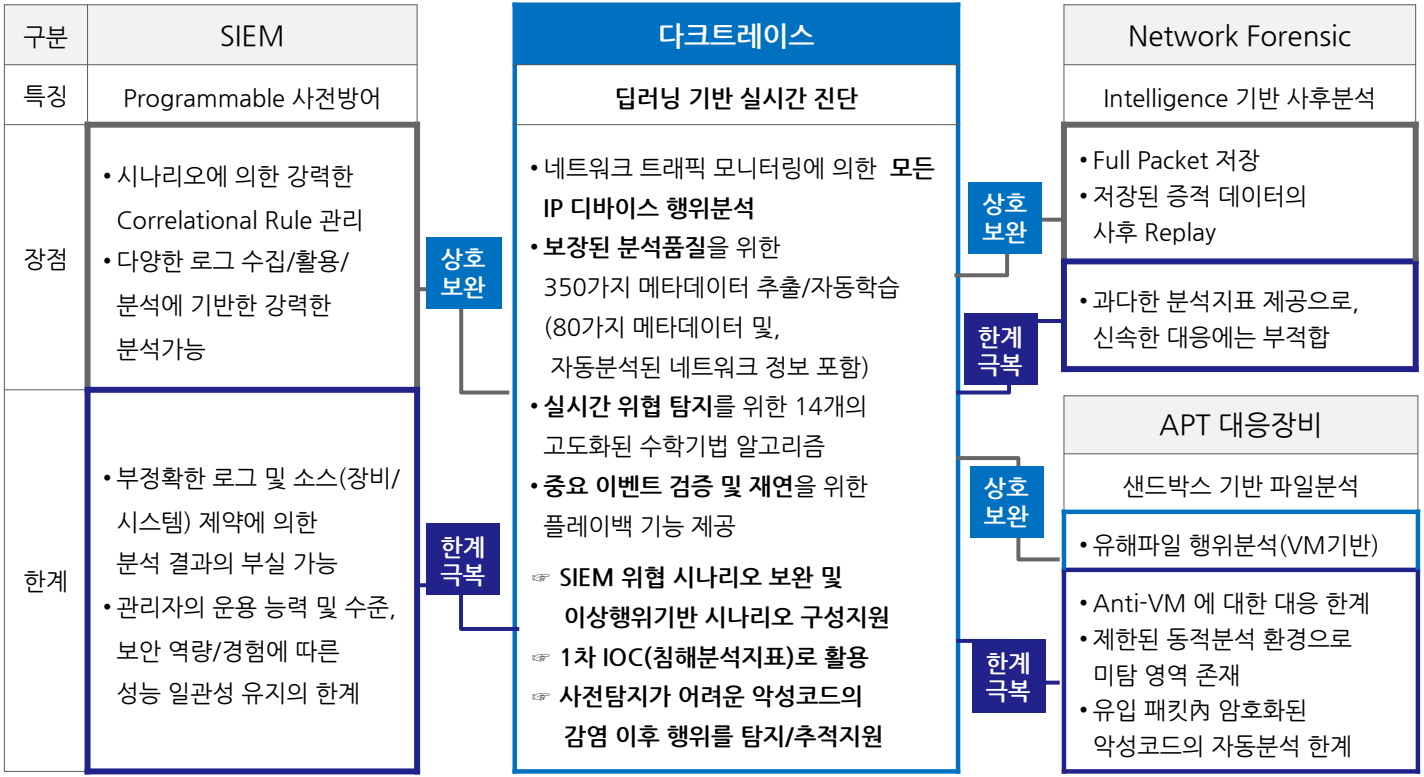
기존 운용중인 보안 솔루션과의 시너지

DARKTRACE

통합보안관리효과 극대화를 위한 보완/협력 모델의 중심

DARKTRACE

다크트레이스 + SIEM + Forensic + APT



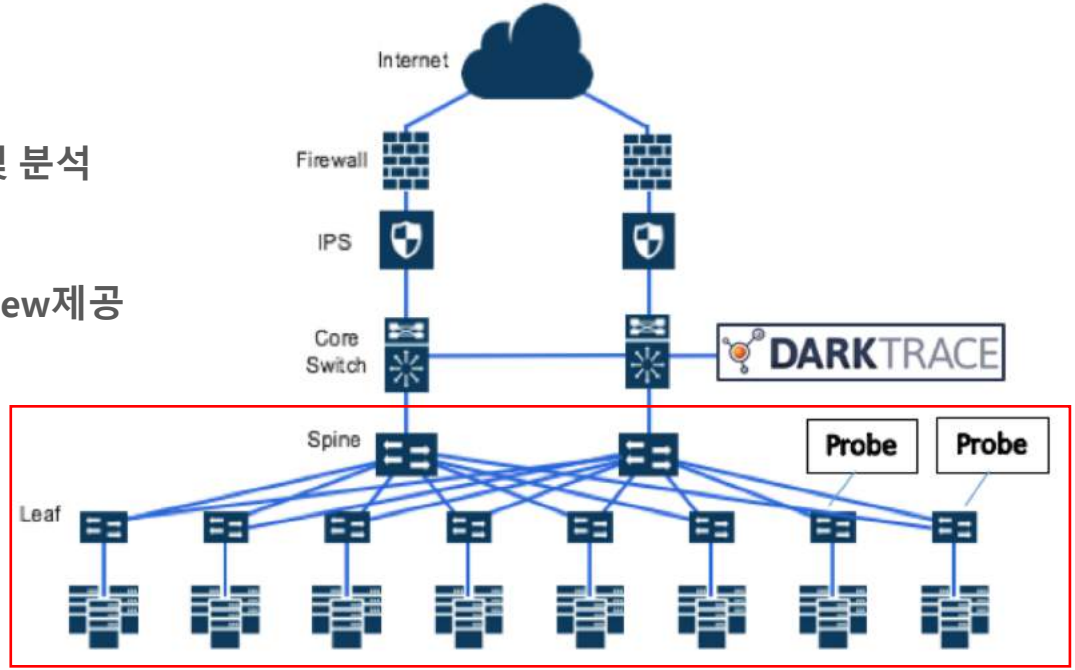
계층적 어플라이언스 구조 지원 : 다양한 구성 가능

Darktrace Unified View Server
대규모의 통합된 네트워크 view 및 분석

Darktrace Master Appliance
Probe들의 데이터를 취합/분석/view제공

Darktrace vSensor
가상환경에서의 데이터 수집 SW

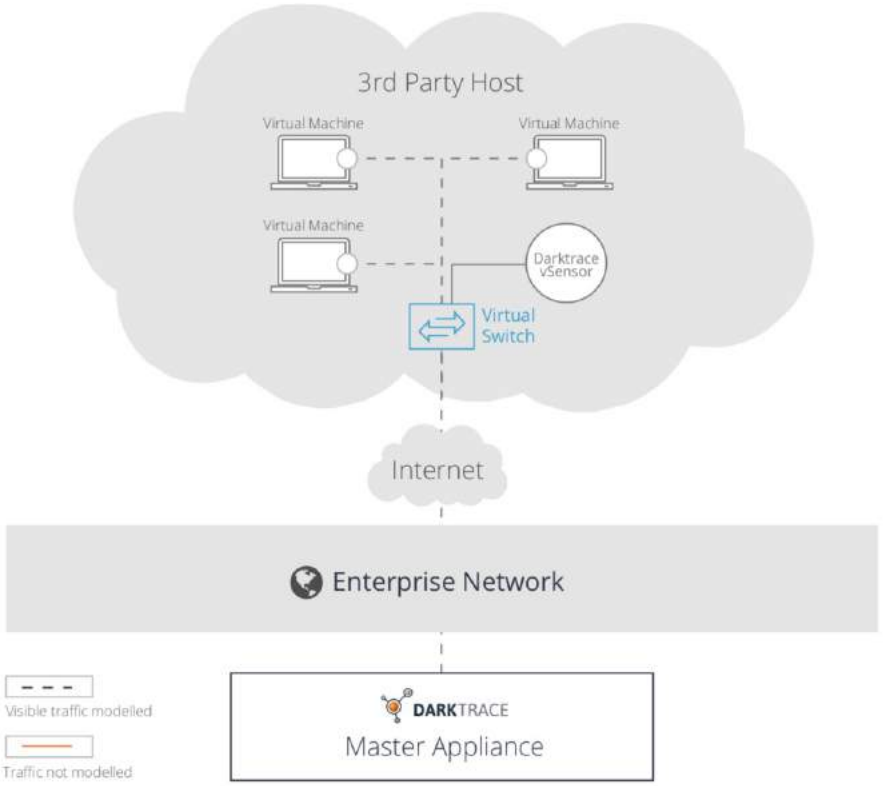
Darktrace Probe
데이터 수집



다크트레이스 클라우드 - 하이브리드 아키텍쳐 구성

DARKTRACE

1. Darktrace Master Appliance 설치
2. 미러링을 통해 사내 네트워크 비지도 학습
3. 클라우드 서버에 **vSensor 및 OS-Sensor 설치**
4. OS-Sensor가 클라우드 트래픽을 캡처해서 vSensor로 전달
5. vSensor가 Darktrace Master Appliance로 메타데이터 전송
6. 마스터 장비로 클라우드 서버 및 사내 네트워크 학습, 군집화(clustering) 및 탐지



다크트레이스 어플라이언스

DARKTRACE

[Model별 주요 Specification]

구분	DCIP-S	DCIP-M	DCIP-X2	DCIP-Z
크기	1U (Half-Depth)	1U	2U	2U
지원가능 네트워크	max 300 Mbps	max 2 Gbps	max 5 Gbps	max 5 Gbps
라이선스 디바이스	Up to 1,000	Up to 8,000	Up to 36,000	Up to 50,000
분당 지원 가능 최대 커넥션	2,000 conns. /min	50,000 conns. /min	100,000 conns. /min	250,000conns /min

자율 대응 모듈

'The Machine Fights back'

비정상 행위 차단 기능 (멀웨어, 랜섬웨어 활동 등)
실시간 자율 대응으로 기업 네트워크, 이메일 상의 이상행위 차단

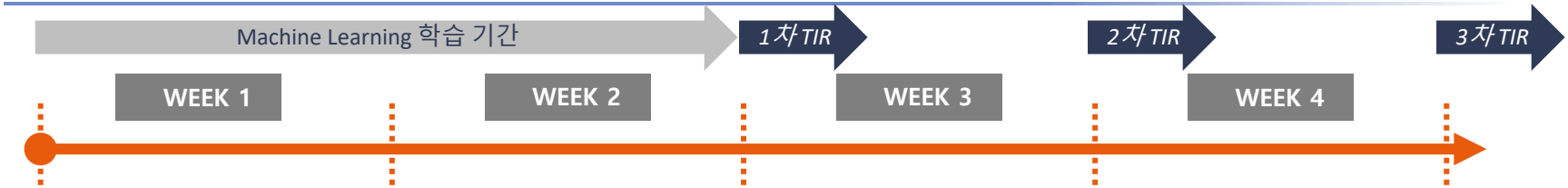
비정상Connection 지연
이상행위(데이터 유출 등) 지연

이메일 서버 트래픽 분석
머신러닝을 통한 이메일 서버 분석

리마크 기능
디바이스 및 사용자에 마크하여 정밀 분석 가능

Active Defense Report (ARD) 제공
Proof of Value 기간 동안 총 3번의 ARD 제공

PoV (Proof of Value)타임라인



	WEEK 1	WEEK 2	WEEK 3	WEEK 4
Steps	▪ **[Pre-POV]** POV 준비 설문 작성 및 다크트레이스 코리아 전달 ▪ **[Day 1]** 장비 입고 및 설치 (1시간 미만) ▪ **[Week 1]** 다크트레이스의 Threat Visualizer를 통하여 네트워크 토폴로지 및 네트워크상의 장치들에 대한 Full Visibility를 3D 그래픽 UI로 확인 ▪ 조직내에 일어나고 있는 네트워크 흐름에 대한 가시성 확인	▪ Threat Notification Center (위협 보고 창)의 최초 접속 가능 ▪ 비정상 사용자 및 조직구성원에 행위를 확인 가능 ▪ 조직내 사용자 계정정보가 어떻게 사용되고 있는지 확인 ▪ **[End of Week 2] 주간 Threat Intelligence Report의 초판 발행**	▪ Threat Notification Center의 모든 기능 접속 가능 ▪ **다크트레이스 UI사용 트레이닝 제공** ▪ 다른 보안장비를 우회하여 들어오는 보안 위협에 대한 확인 ▪ **[End of Week 3] 주간 TIR 2차 발행**	▪ [End of Week 4] 주간 TIR 3차 (마지막) 부 발행 ▪ POV Q&A미팅 ▪ 장비 철수 확인서 작성 ▪ 장비 내 Data Wipeout ▪ 장비 철수 및 후속 Meeting 조율
Your Resource	▪ **다크트레이스 담당 영업 (AM)** ▪ **다크트레이스 컨설턴트 (CT)**	▪ **다크트레이스 컨설턴트 (CT)** ▪ **위협 전담 애널리스트 (CA)**	▪ **다크트레이스 컨설턴트 (CT)** ▪ **위협 전담 애널리스트 (CA)**	▪ **다크트레이스 영업 (AM)** ▪ **다크트레이스 컨설턴트 (CT)** ▪ **다크트레이스 SME**

국내 주요 고객사

DARKTRACE

Public

국세청

KBRI 한국뇌연구원

금융위원회 금융정보분석원

한국서부발전㈜

BPA 부산항만공사 BUSAN PORT AUTHORITY

한국동서발전㈜

NSR 국가보안기술연구소

K water 한국수자원공사

한국지역난방공사

KOMIPO 한국중부발전

The Way to Better Living 길이 열리는 화성시

Enterprise/Etc

yogiyo

Hyundai Oilbank

SAMSUNG 삼성SDS

SAMSUNG 삼성전자

Hanwha S&C

Hanwha | TOTAL

SFA

KT&G

POSTECH 포항공과대학교

Finance

KB생명

DGB생명

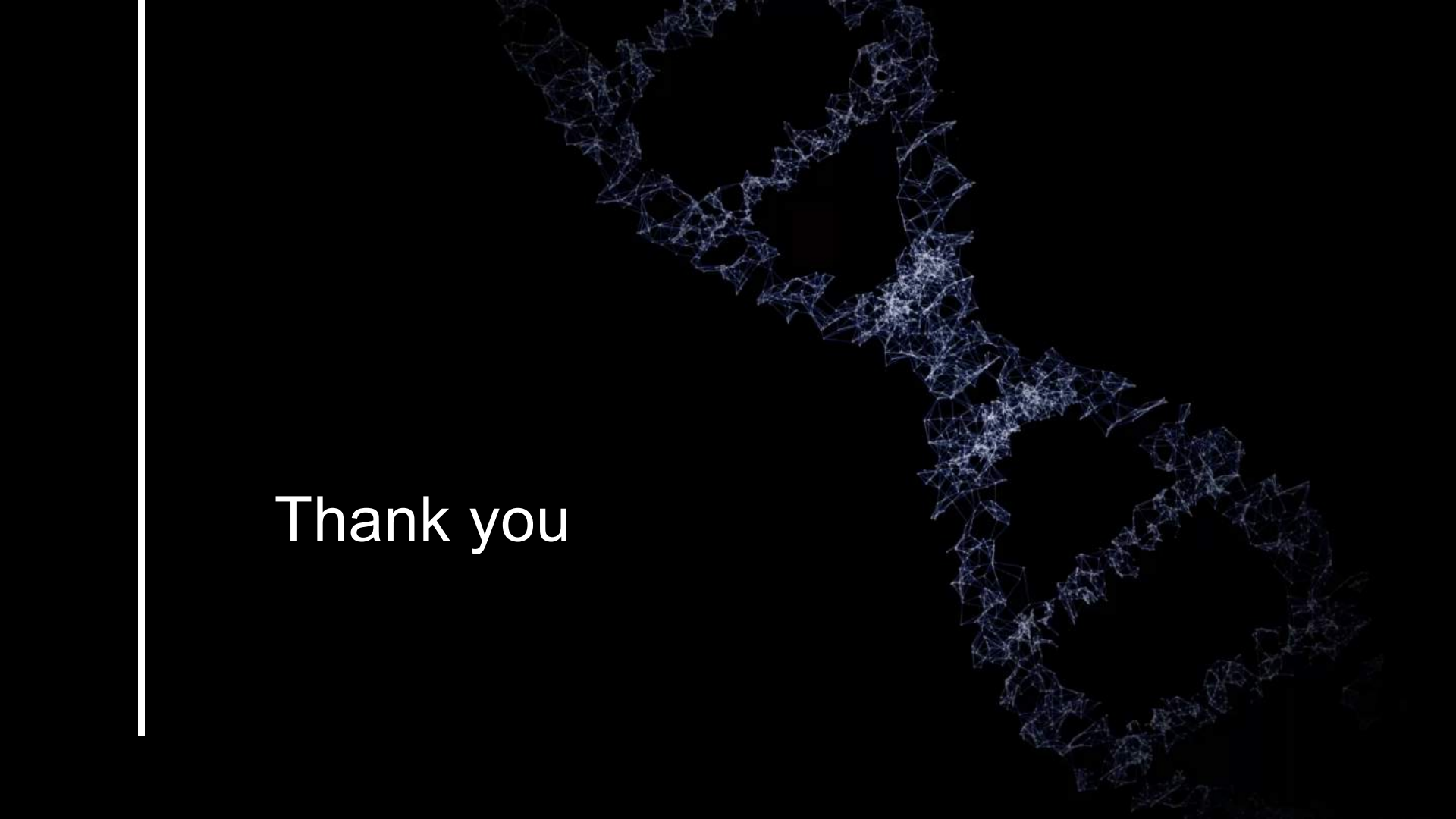
Hyundai Card 현대카드

우리카드

KB국민은행

NH농협손해보험

해외 주요 고객사 (약 7,000 고객)


Thank you