AI기반 신·변종 악성코드 및 랜섬웨어 대응 솔루션 전문기업

주식회사 엔피코어
회사소개 및 제품소개서

NDCore
New Paradigm Core

Contents

NDCore
New Paradigm Core

1

회사소개

1. 회사소개

엔피코어는 신·변종 악성코드(APT) 대응 AI기반 보안솔루션을 제공하는 정보보안 기업입니다.

기업명	주식회사 엔피코어
소 재 지	서울특별시 영등포구 당산로 171, 701호 (당산동 4가, 금강펜테리움 IT타워)
대표이사	한 승 철
설 립 일	2008년 11월 19일
산업분야	사이버보안
주요제품	정보보안솔루션 (신·변종 악성코드 대응 솔루션)
홈페이지	www.npcore.com

회사신용도

BBB-

기술등급

TI-1

우수한 기술력과 미래 성장 가능성이 높은 수준임을 인정

글로벌 영업현황

7개국 진출

1. 주요 연혁

2023년 엔피코어는 공공분야 APT 대응제품 판매 1위를 달성하였습니다.

2008 – 2013

2013 'ZombieZERO V2.0' GS인증

2013 'ZombieZERO Inspector V2.0' 국내 CC인증 획득

2011 'ZombieZERO V2.0' 국내 CC인증 획득

2010 중소기업청 벤처기업 지정

2009 기업부설연구소 NP연구소 설립

2008 주식회사 엔피코어 설립

2014 - 2018

2018 수출유망중소기업 지정, 중소벤처기업부

2018 기술역량 우수기업 인증(T4), 한국기업데이터

2017 'ZombieZERO Inspector V3.0' GS인증

2017 나라장터 종합쇼핑몰 방화벽장치
지능형위협대응솔루션 상품등록

2017 미국 연방조달벤더(SAM) 등록

2016 우수 연구개발 유공 기업 선정, 서울특별시장

2016 'ZombieZERO Inspector V3.0' 국내 CC인증

2016 제4회 '수출 첫걸음상' 수상

2015 '창조기술대상' 우수상 수상

2015 미국 메릴랜드주에 법인 설립(NPCore, LLC)

2014 베트남 하노이 지사 설립

2019 - 2023

2023 Pre IPO 80억 유치

2023 기술역량 우수기업 인증(TI-1), NICE평가정보

2023 'ZombieZERO Inspector V4.0' 보안기능 인증, KTC

2023 품질경영시스템 인증(ISO 9001:2015), ICR

2023 청년친화강소기업 선정, 고용노동부

2022 벤처기업 인증, 벤처기업협회

2022 'ZombieZERO Inspector V4.0' GS 인증, KTC

2021 혁신기업 국가대표 1000, 과학기술정보통신부

2020 정보통신공사업 등록

2019 MSA 솔루션 런칭 (MTA+SSL+APT 통합장비)

2019 SECaaS 솔루션 런칭 (클라우드형 APT)

2019 'ZombieZERO Inspector V4.0' 국제 CC인증

1. 주요 사업

엔피코어는 AI기반 행위분석 기술을 통하여 APT 및 보안 위협 (랜섬웨어 등)을 사전에 탐지/차단하는 제품 및 솔루션을 제공합니다.

Email, 네트워크, Endpoint 등의 다양한 루트로 공격
내부 정보를 탈취하거나 랜섬웨어 감염으로
금전적 보상 요구

정보수집 확산 C&C통신

침입 데이터 접근 데이터 유출

백신과 같은 안티바이러스는 시그니처 기반의 패턴 매칭 방식으로
보유한 정보에 의존하여 알려진 악성코드에만 대응하기 때문에
APT 및 신·변종 악성코드의 위협 대응이 어려움

정보 보안의 **최대 위협 APT** (Advanced Persistent Threat)

- 해커가 다양한 보안 위협을 특정 기업이나 조직의 네트워크에 지속적으로 가하는 공격.
- 알려지지 않은 신 · 변종 악성코드, 고유 패턴이나 방식이 없는 비정상 행위의 공격.
  (Ransomware · Backdoor · Bootkit · Exploit 등)

공격기법

안티바이러스 대응 방법

2

제품소개
ZombieZERO APT&EDR

NDCore
New Paradigm Core

2. ZombieZERO APT&EDR

AI기반 신·변종 악성코드 대응 솔루션 Zombie ZERO는 악성코드가 유입될 수 있는 다양한 경로에 솔루션 구축이 가능합니다.

APT Security

- Network APT
- Email APT
- File APT
- 통합관리 솔루션

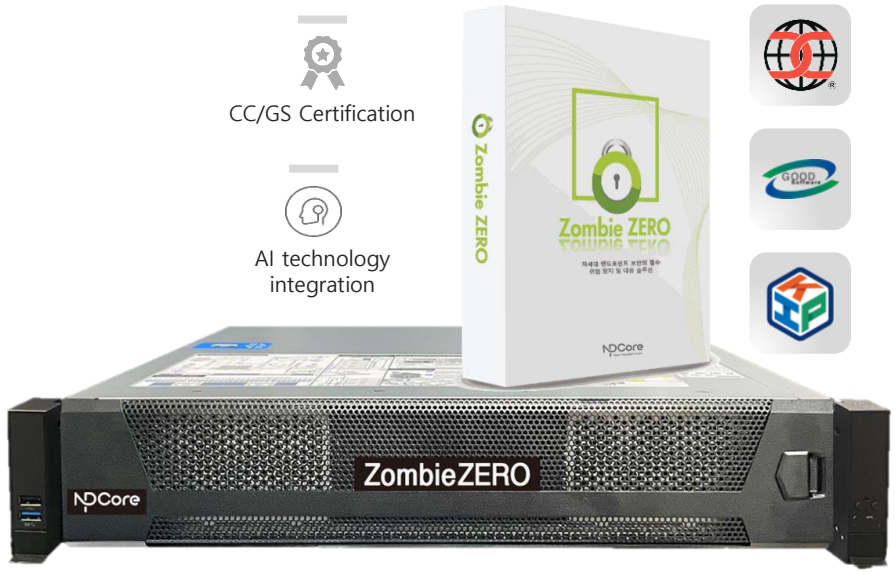
EDR Security

- EDR
- SECaaS

실제 제품 이미지

CC/GS Certification

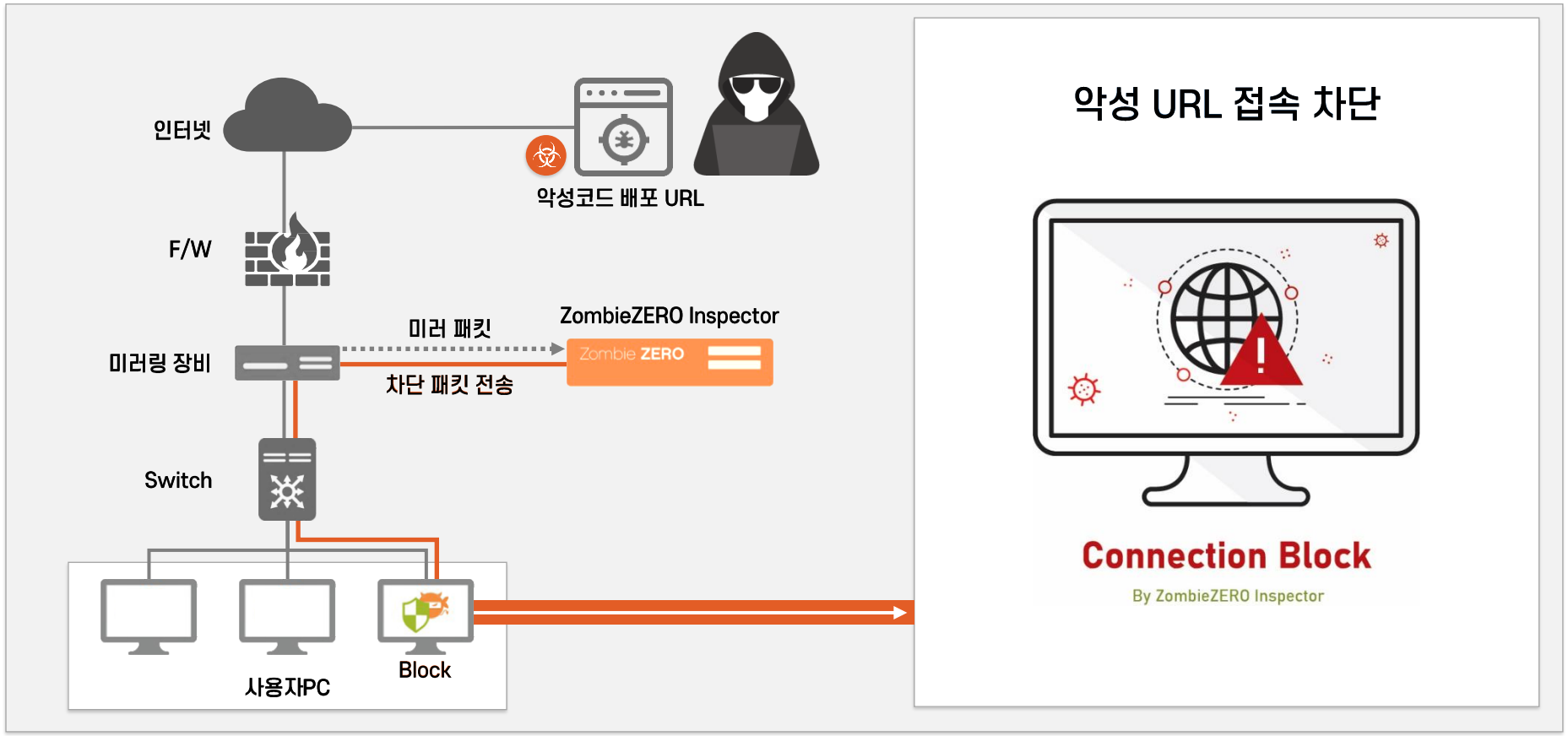
AI technology integration



2. 네트워크 APT

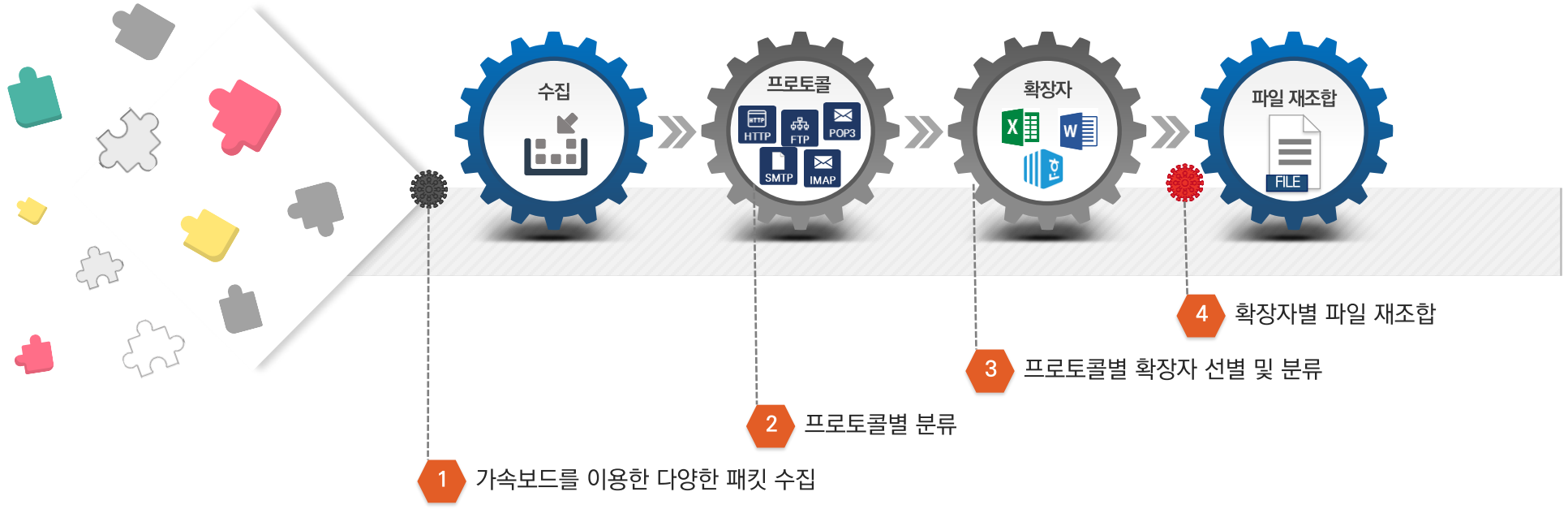
네트워크 트래픽을 통하여 유입되는 악성코드를 탐지/차단하는 APT 솔루션

- 네트워크 트래픽을 <u>가속보드를 이용하여 수집</u>하고, 이에 대한 악성코드를 탐지/분석하여 차단
- C&C 서버 접속 및 악성코드 배포 사이트 URL 접속 차단 등 <u>실시간 차단</u>



2. 네트워크 APT

수집 전용 가속보드를 사용하여 유실 없는 네트워크 패킷 수집 및 파일 재조합



수집 가속 보드 장점

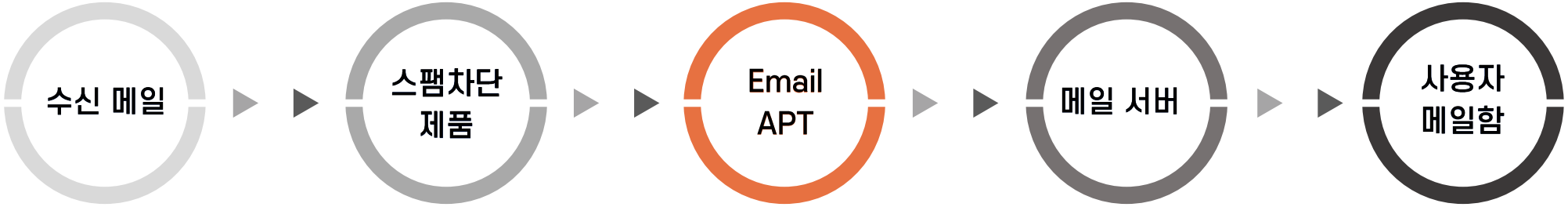
- 네트워크상 다중 지점에서 실시간 데이터를 수집, 하나의 분석 스트림으로 병합하여 분석 데이터의 상관 관계를 보다 쉽게 설정
- 나노초 정밀도로 모든 이더넷 프레임의 타임스탬핑
- 지능형 기능으로 CPU 부하가 극히 낮은 상태에서 애플리케이션 성능 가속

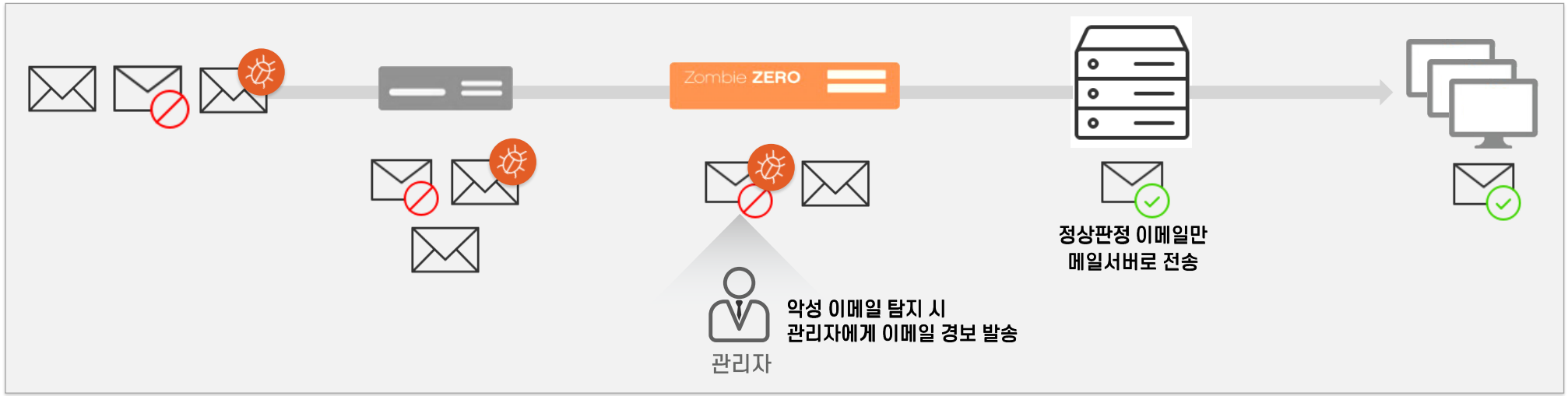
지원 : 1GbE 4port / 10GbE 2port / 10GbE 4port

2. 이메일 APT

이메일을 통하여 유입되는 악성코드를 탐지/차단하는 APT 솔루션

- 이메일을 통해 유입되는 악성코드 탐지/차단하는 MTA와 APT 통합 솔루션
- 이메일 첨부파일 및 URL 분석 후 **정상메일만 메일서버로 전송**

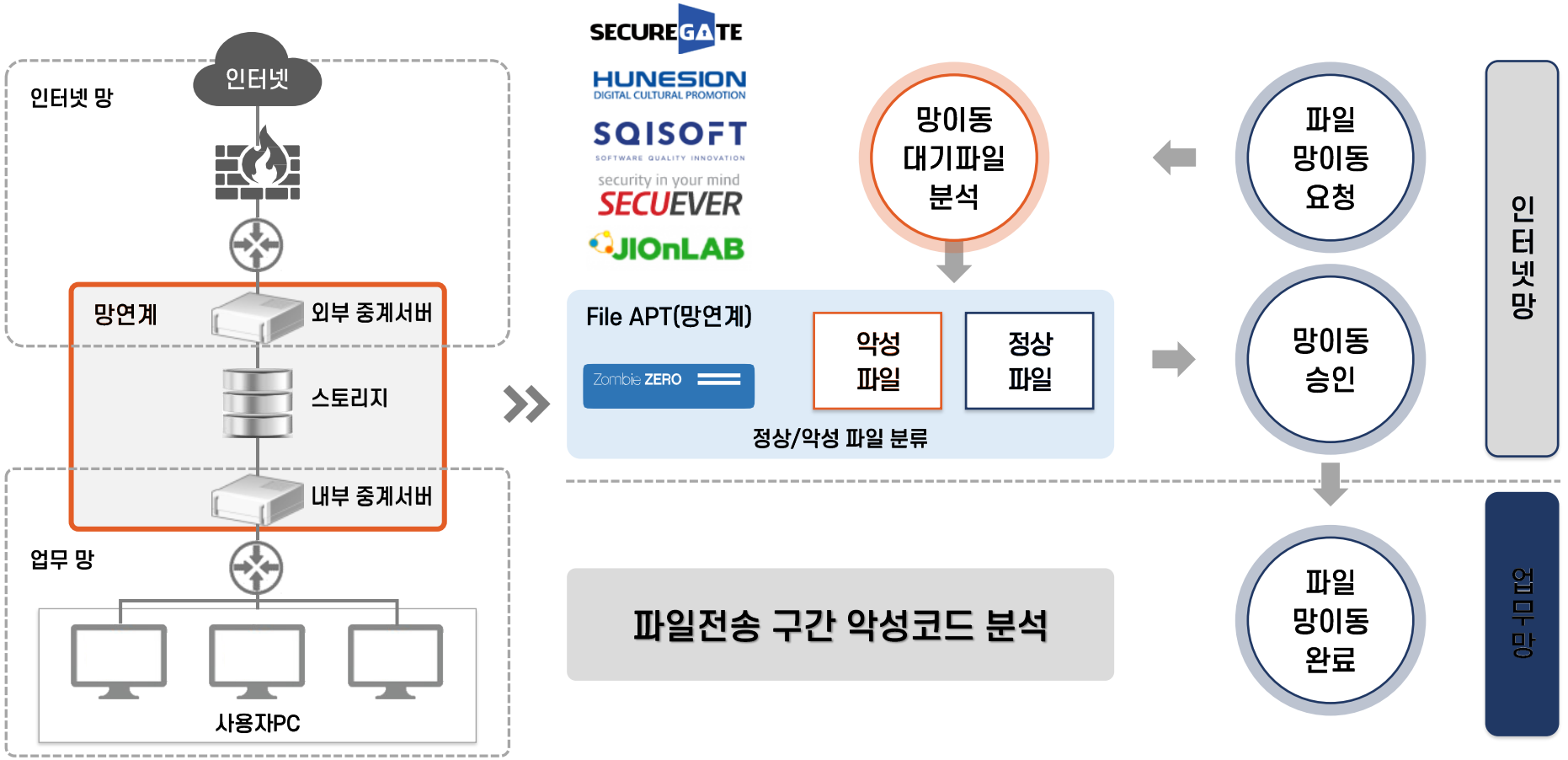




2. 파일 APT

이메일을 통하여 유입되는 악성코드를 탐지/차단하는 APT 솔루션

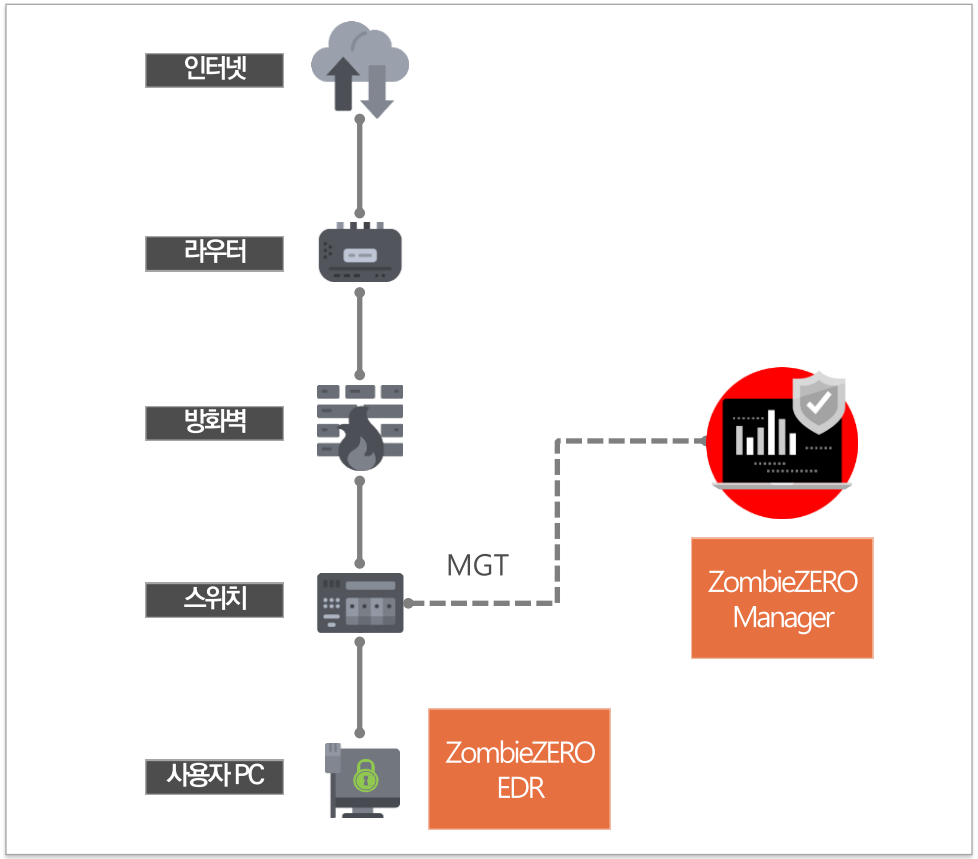
- 망연계 솔루션과 연동하여 <u>이동 대기중인 파일을 분석</u>
- 분석된 파일을 분류하여 <u>정상으로 판단된 파일만</u> 업무망으로 전송



2. EDR

PC,서버 등 사용자 구간을 통하여 유입되는 악성코드를 탐지/차단하는 APT솔루션

- Endpoint(사용자PC)단에서 APT 공격 탐지/차단 솔루션
- 랜섬웨어 / 백신 등 다양한 보안 솔루션으로의 확장 운영 가능



1. IOC 기반 위협 행위 탐지 (MITRE ATT&CK 분류)
2. 사용자 PC에 신규 파일 유입 및 실행
3. 분석 서버로 파일 업로드
4. 4단계 파일 분석
5. 분석 결과 정책 배포
6. **정상 파일 경우 파일 실행**
   악성 파일 경우 차단 / 격리

IOC 기반 위협 행위 지속 탐지 (MITRE ATT&CK 분류)

2. EDR

단말단에서 발생 되는 랜섬웨어 행위 탐지/차단 및 실행보류 기능을 통해 검증된 파일만 실행

랜섬웨어 행위 탐지/차단

실시간 랜섬웨어 행위를 탐지하며 차단
파일 암호화 및 위변조 대응

ZeroTrust 보안

신규 파일의 유입 또는 위협 파일 실행 시
파일의 실행을 보류하여 분석 서버로 정보 업로드

Bitdefender의 AV 기능

글로벌 백신 Bitdefender의 AV 기능 지원
악성코드의 신속한 사전 탐지

2. EDR

파일 변조 직전의 순간, 일반 프로세스가 접근 할 수 없는 보안 폴더에 파일 백업

실시간 순간 백업

EDR은 악성코드를 사전에 탐지/차단하는 보안솔루션 이지만,
순간 백업 기능을 통하여 더욱 완벽한 정보 보안을 제공함

2. EDR

사용자 단말의 네트워크, 파일, 프로세스, 레지스트리 행위에 대한 IOC 침해지표 탐지

타입 : Process

이벤트 : Create
Parent-PID : 2068
Parent-경로 : C:\Windows\System32\svchost.exe
Parent-MD5 : f586835082f632dc8d9404d83bc16316
PID : 2296
경로 : C:\Program Files (x86)\Google\Update\GoogleUpdate.exe
MD5 : 59ea38acbca05610bfee326da3f2d96b
Params : "C:\Program Files (x86)\Google\Update\GoogleUpdate.exe" /ua /installsource scheduler
Dll Name : null
Thread : null
세션 : A59819EC07998E50C0797171EB280E3C
위험도 :

MITRE	설명	Tactics

타입 : File

PID : 2652
경로 : C:\Users\npcore\Desktop\그램전달\gocleansetup151.exe
MD5 : 96d8c9c4e3126074875 61c6391508941
이벤트 : Write
파일 : C:\Users\npcore\AppData\Local\Temp\nshCA4C.tmp\UserInfo.dll
세션 : A59819EC07998E50C0797171EB280E3C
위험도 :

MITRE	설명	Tactics
T1204	User Execution	Execution

타입 : Network

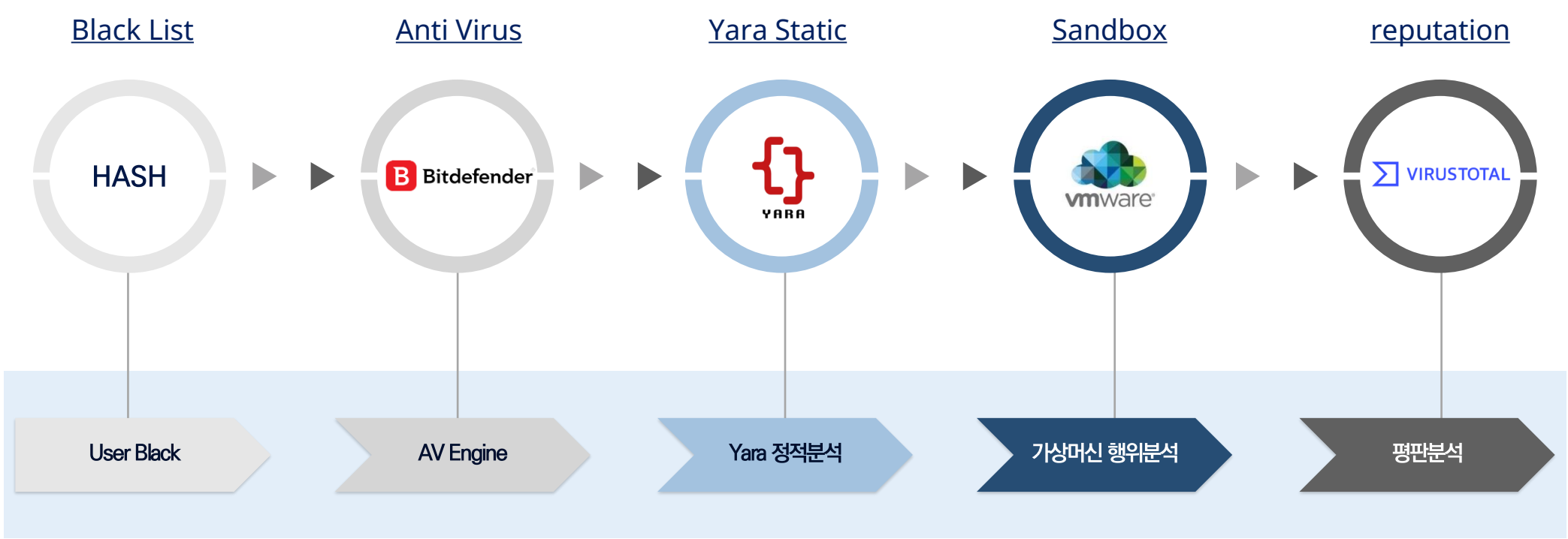
PID : 2560
경로 : C:\Program Files\Google\Chrome\Application\chrome.exe
MD5 : aa2e522a405cb5a295d3502c4ff6ca39
이벤트 : HTTP
URL : www.ten-1097.comwww.ten-1097.com /ajax.jongmok_list.php
IP : 107.154.131.98
포트 : 80
세션 : A59819EC07998E50C0797171EB280E3C
위험도 :

MITRE	설명	Tactics
T1041	Exfiltration Over C2 Channel	Exfiltration

※ IOC 침해지표 탐지 로그

2. 공통 특징 - 다차원분석

시그니처/정적/동적분석 등의 알려지지 않은 악성코드 다차원 분석



2. 공통 특징 - 다차원분석

시그니처/정적/동적분석 등의 알려지지 않은 악성코드 다차원 분석

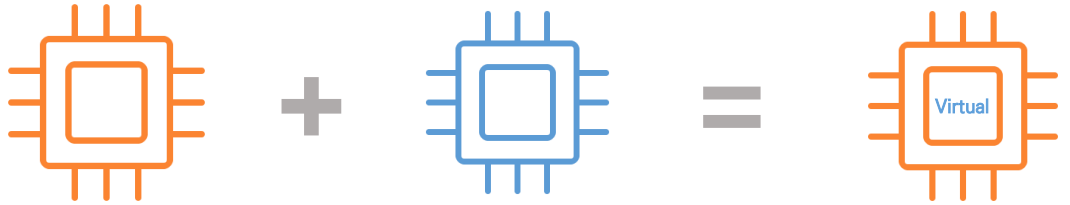
- Yara Rule 기반 **정적 분석**을 이용한 악성 패턴 탐지
- 사용자 환경과 유사한 가상머신를 이용한 파일 실행 및 **행위 분석**

2. 공통 특징 – 가상머신 우회방지

가상머신을 우회하는 악성코드의 행위를 유도하여 동적 행위 탐지 분석

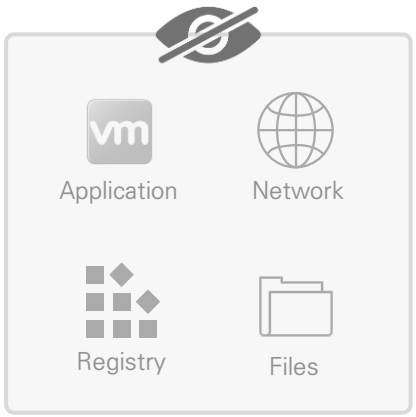
- 적은 비용의 가상머신 구성으로 <u>리얼머신 구성과의 동일 효과 제공</u>

가상머신 우회 방지 기술



Real Machine	Virtual	Fake Real Machine
BFEBFBFF000306C3 Physical CPUID	0FABFBFF000306C3 Running Inside Hypervisor	BFEBFBFF000306C3 Running Inside Real Machine

리얼머신의 CPUID 정보로 변경
(EAX/EBX/ECX/EDX)



가상머신 고유정보 숨기기

- 가상머신의 CPUID 정보를 **리얼머신의 CPUID 정보로 변경, 가상머신 고유정보 숨기기** 등의 우회 방지 기술
- 가상머신 우회 방지 기술을 통하여 악성코드는 **가상머신을 리얼머신으로 인식**하여 악성 행위를 실행

2. 공통 특징 – MITRE ATT&CK 분류

표준화된 MITRE ATT&CK 분류에 맞는 악성 코드의 카테고리화 적용

- 악성코드의 공격 방법(전술)에 대해 확인 가능

MITRE

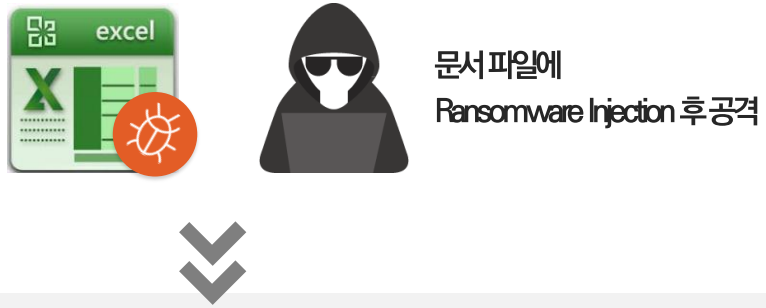
ATT&CK™
Adversarial Tactics, Techniques & Common Knowledge

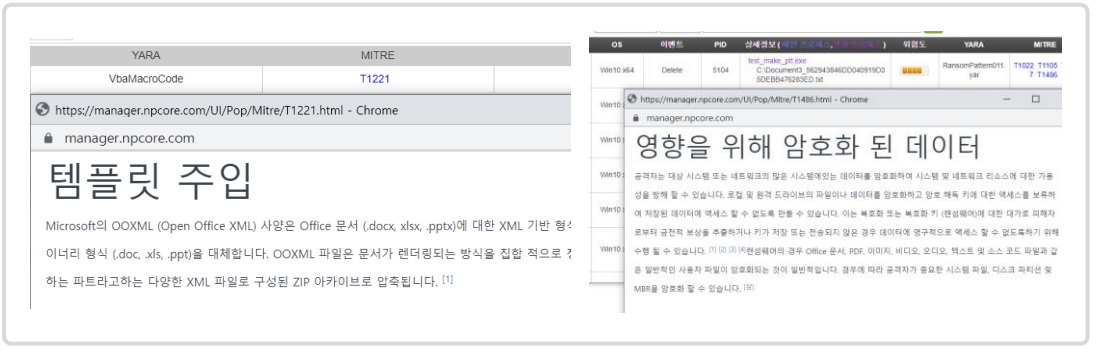
공격의 결과가 아닌
진행중 공격에 대한 기술 및 방법의 형태 모니터링

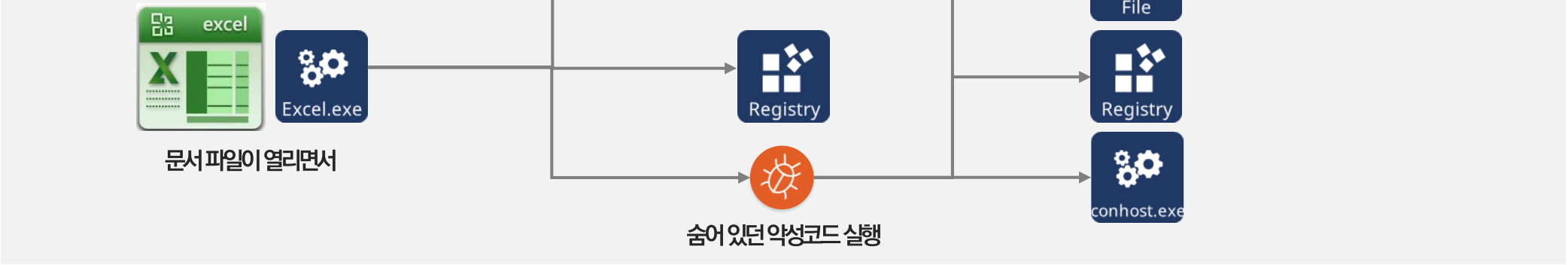
2. 공통 특징 – 악성코드 공격 형태 분석

악성 행위 공격에 대한 흐름도 제공

- 탐지된 근거 정보를 확인 할 수 있는 페이지(링크) 제공







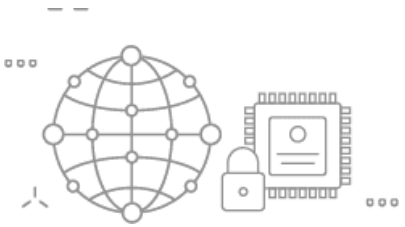
2. 공통 특징 – 글로벌 탐지 패턴

국내 및 글로벌 패턴 라이브 업데이트 지원

- 위협에 대한 증거 기반의 지식(위협 인텔리전스)를 활용한 대응

Pattern, Rule, Detect, Malware

US	United States	167794
RU	Russian Federation	27473
DE	Germany	21267
GB	United Kingdom	12870
NL	Netherlands	12173
CN	China	11903
CA	Canada	7494
JP	Japan	7402
FR	France	5916
RO	Romania	5255



MALSHARE | Bitdefender | VirusShare | SHODAN | VIRUSTOTAL

Spyse | VirusSign | c-tas 위협정보 종합분석 | 교육사이버위협 정보공유시스템

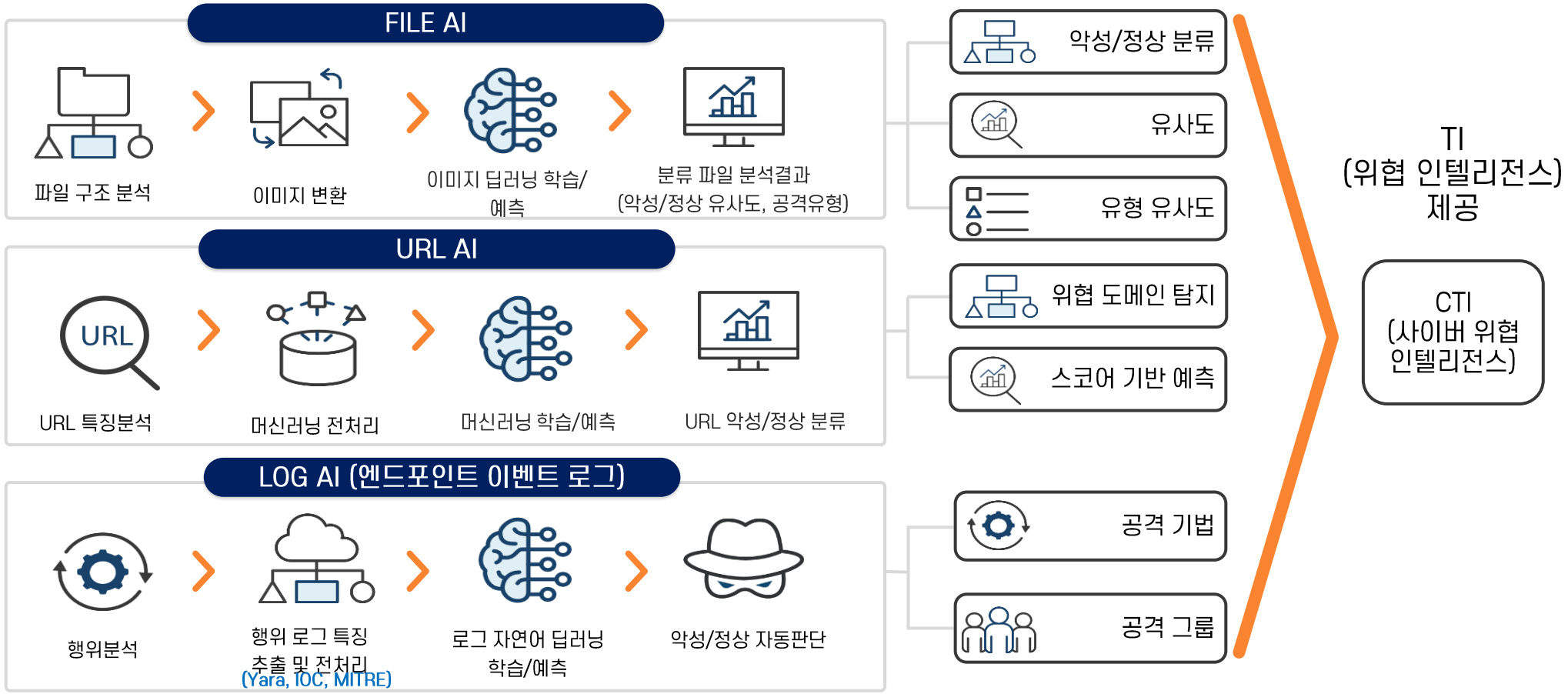
3

제품소개
ZombieZERO XDR

NDCore
New Paradigm Core

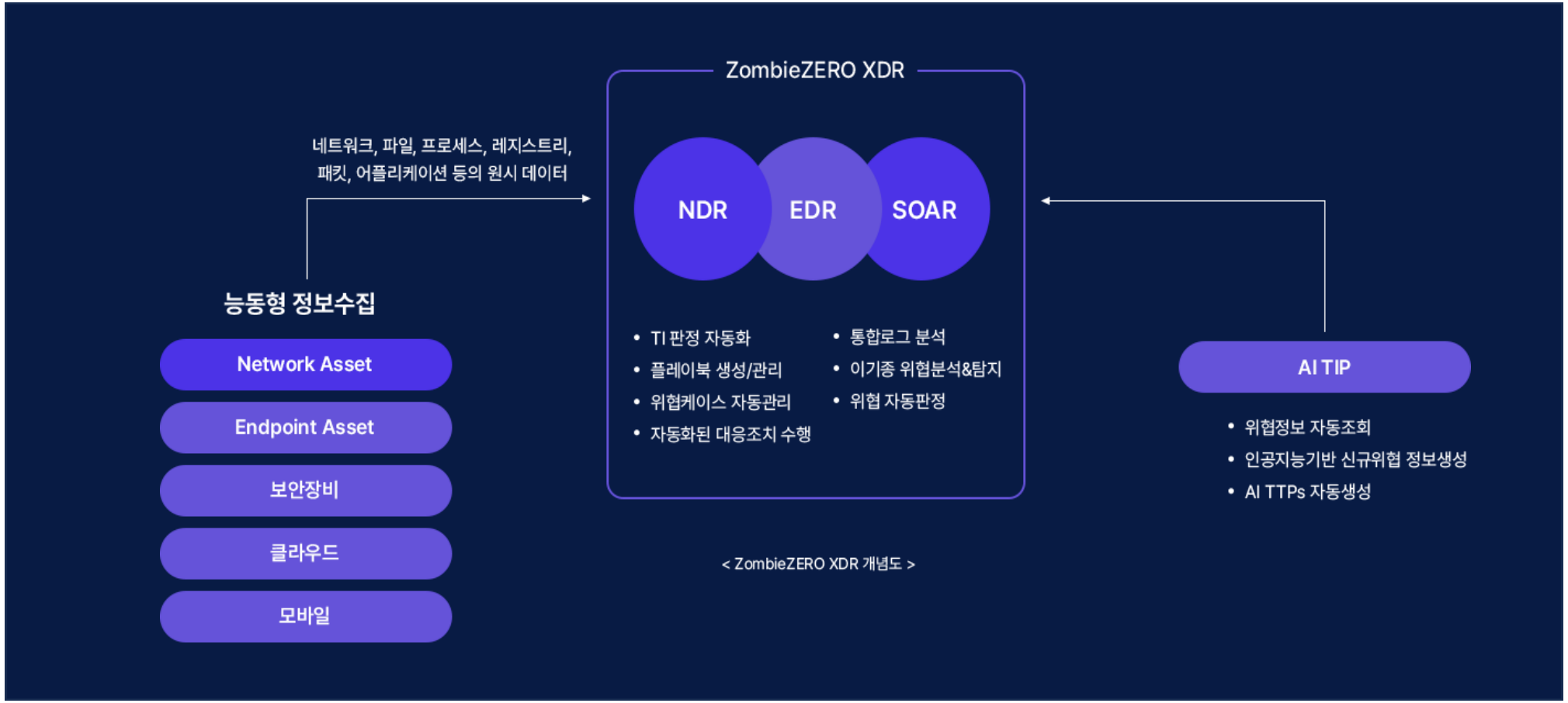
3. ZombieZERO XDR 핵심기술

자동화된 위협판단과 대응전략을 위한 AI기술로 이미지기반 악성코드 유사도분석 기술, 앙상블을 통한 위협 URL 예측 및 스코어링 기술, 자연어 기반의 공격기법 및 공격그룹 자동식별 기술을 활용



3. ZombieZERO XDR 개념도

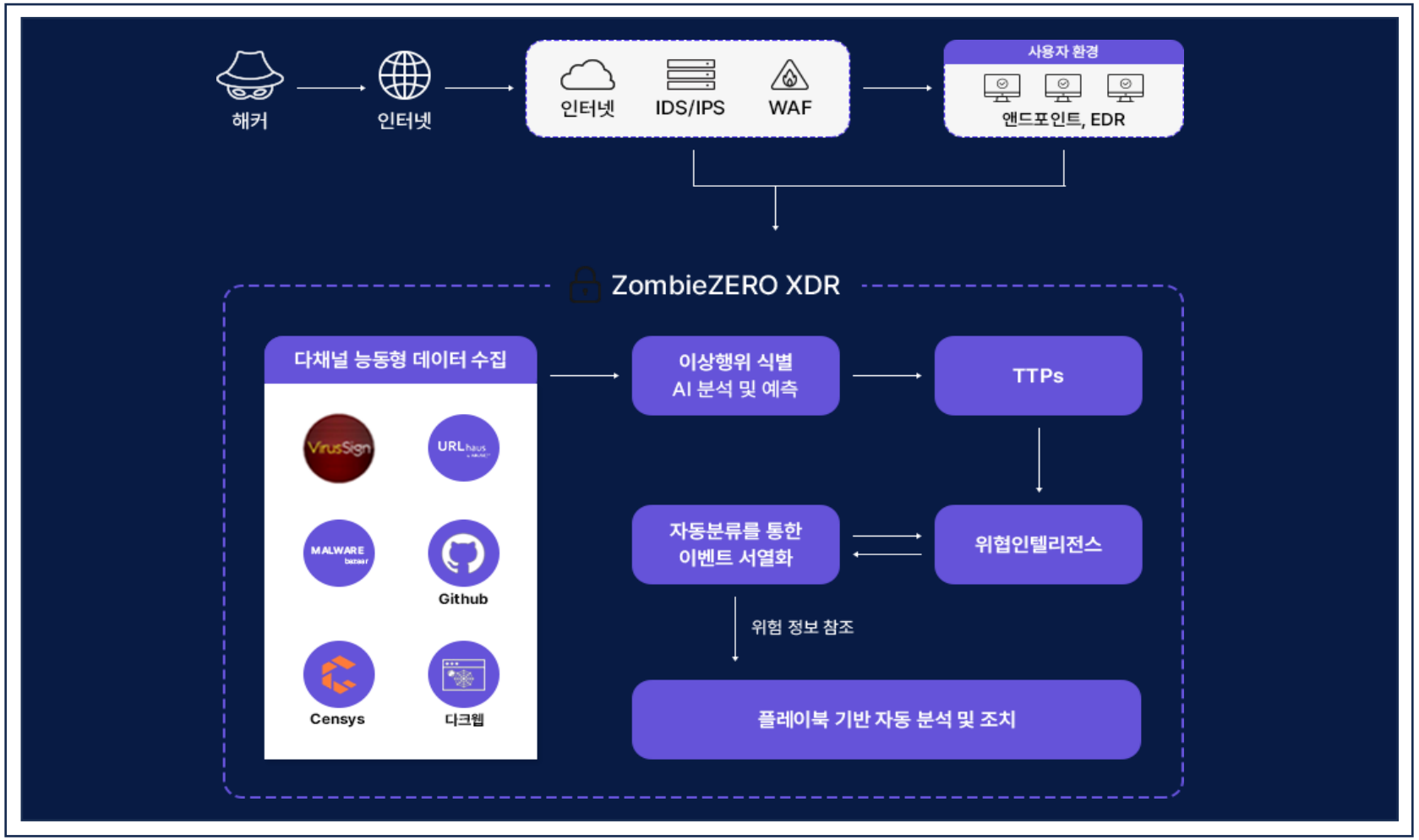
관제자동화의 핵심요소를 통합하고 AI와 TIP기술을 융합하여 능동형 대응이 가능합니다.



< ZombieZERO XDR 개념도 >

3. ZombieZERO XDR 구성도

능동형 데이터 수집과 자동화된 위협 판단 기술을 결합(AI-TIP)하여 전문 분석가 없이도 보안위협을 자동으로 판단하고 대응하는 차세대 플랫폼입니다.



3. ZombieZERO XDR 주요기능

XDR은 보안 요소별 탐지체계에서 엔드포인트를 포함한 모든 보안요소를 통합&확장하여 위협의 실체를 탐지합니다.

기능구분	구현방식
위협판정, 위협케이스 관리	Auto
대응조치	Auto
침해위협조사	Auto Analysis
공격자 식별	Auto Analysis
공격유형 분류	Auto Analysis
정보수집	엔드포인트/네트워크/보안장비
위협인텔리전스 생성	위협헌팅 기반 [사고정보, 악성코드 유사도, 위협사이트 예측, 공격기법, 공격그룹] 제공

3. ZombieZERO XDR 특장점

능동형 데이터 수집과 자동화된 위협 판단 기술을 결합(AI-TIP)하여 전문 분석가 없이도 보안위협을 자동으로 판단하고 대응하는 차세대 플랫폼입니다.

전문적이지 않은 / 적은 인원이라도 신속하고 정확한 위협 대응이 가능

- APT 대응 솔루션별 분석 결과를 바탕으로 파일 수집/파일 분석/결과 (허용/차단/격리)를 통해서 악성 파일별 분석 시나리오 확인
- 행위 정보는 시계열 그래프를 통하여 직관적으로 분석 가능
- 데이터를 통합 관리 내역을 SIEM/ESM 등에 전달하여 탐지 및 대응 능력 향상에 기여

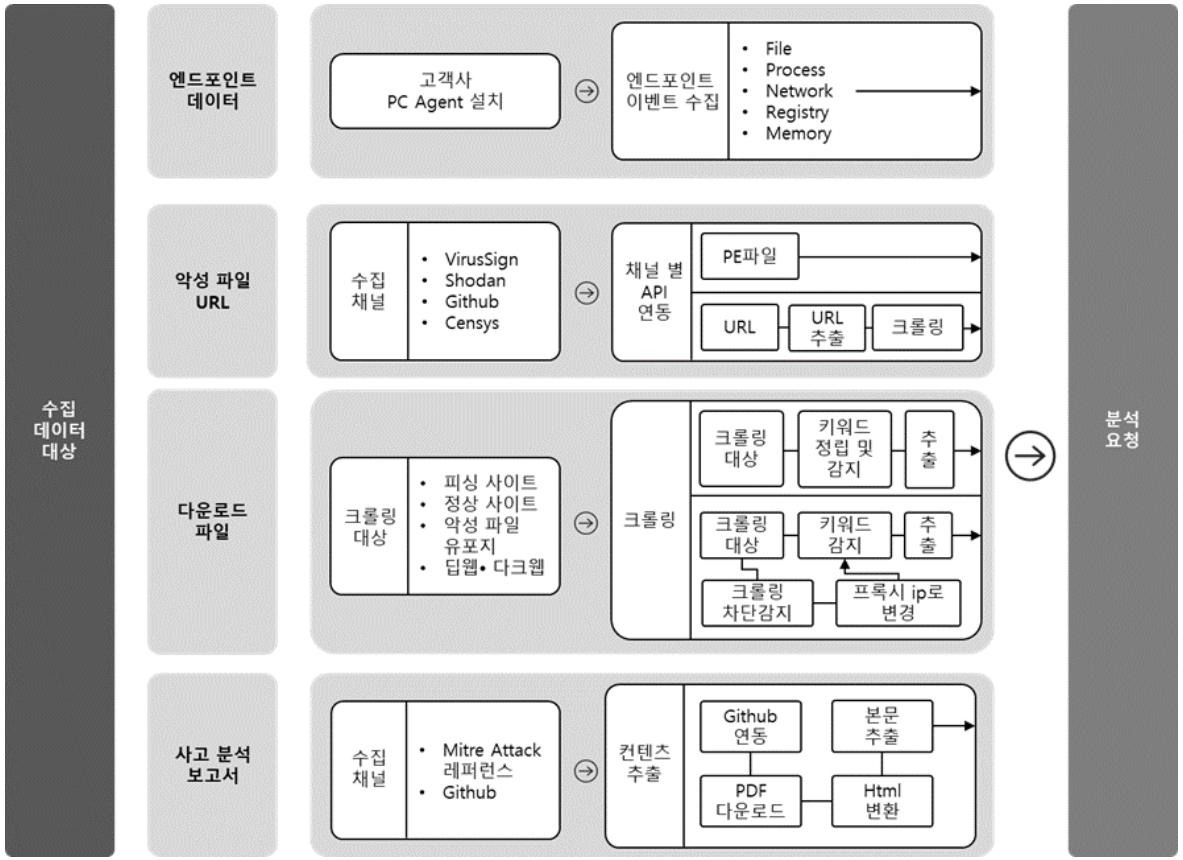
예상되는 위협의 가시성 확보를 통해 Cyber Kill Chain 전략수립 가능

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

3. ZombieZERO XDR 주요기능 - 수집

사이버 위협탐지를 위한 다채널 능동형 데이터 수집 및 OSINT와 다크웹, 딥웹 정보수집

사이버 위협 탐지를 위한 데이터 수집



사이버 위협탐지를 위한 다채널 능동형 데이터 수집 및 OSINT와 다크웹, 딥웹 정보수집

- Agent 기반 엔드포인트 이벤트 수집
- 다수의 크롤링 실행을 위한 컨테이너기반의 크롤링 적용
- 크롤링 회피기술 우회를 위한 프록시 기술 적용
- 의심스러운 URL, IP, Domain의 내부 정보 수집을 위한 크롤링 연동

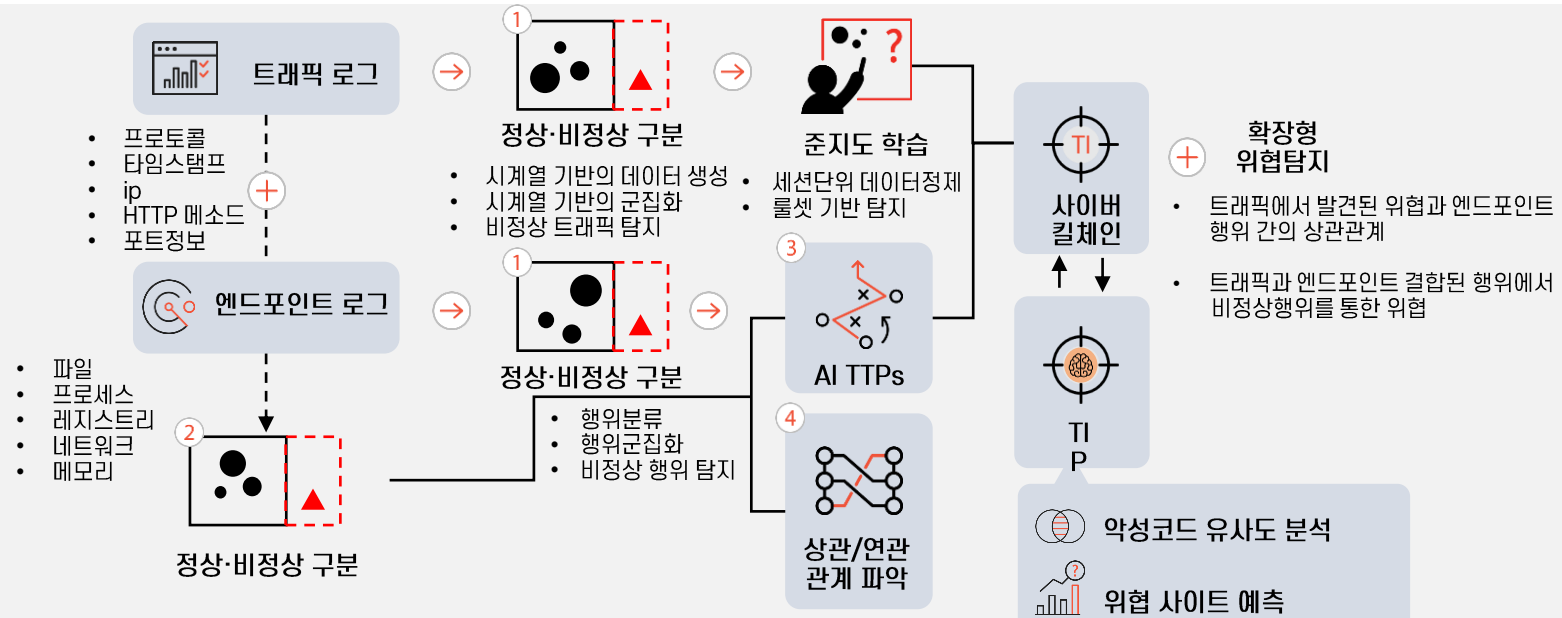
- 신규 TI 생성 :

1. 공개정보출처(OSINT)에서 수집된 URL, Domain 크롤링
2. 다크웹 및 딥웹 접속을 위한 토르기반의 크롤러
3. Showdan, Github, Censys와 모듈 연동

3. ZombieZERO XDR 주요기능 - 전처리

사이버 공격에 대한 확장된 위협정보(데이터) 생성과정

사이버 공격에 대한 확장된 위협정보(데이터) 생성과정



- 사이버킬체인 : 사이버 공격을 방어하기 위한 적극적인 방어 전략으로 사이버 공격을 프로세스 상으로 분석해 각 공격 단계에서 조직에게 가해지는 위협 요소들을 파악하고 공격자의 목적과 의도, 활동을 분쇄, 완화시켜 조직의 회복 탄력성을 확보하는 전략
- AI TTPS(Tactics Technics Procedures) : 인공지능기반으로 도출된 공격전략전술행위
- TIP(Threat Intelligence Platform) : 위협인텔리전스 플랫폼
- XDR(eXtended Detection and Response) : 확장된 탐지와 위협 자동판단&대응이 가능한 기술

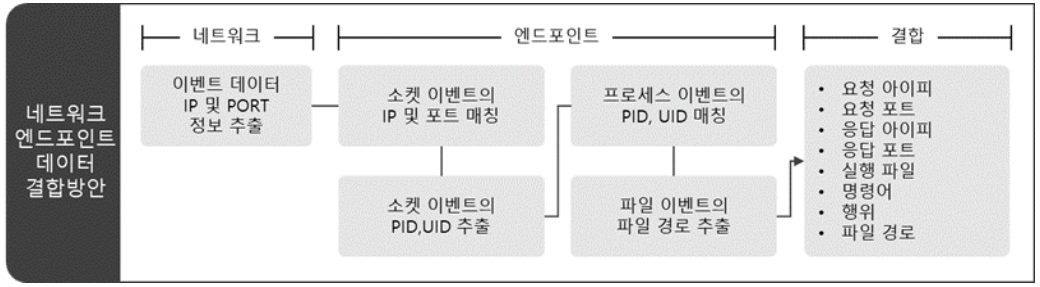
3. ZombieZERO XDR 주요기능 - 분석

TTPs기반의 탐지기술을 개발하고 네트워크 데이터와 엔드포인트 수집정보를 결합하여 위협 상관/연계 관계를 파악할 수 있는 기술

TTPs기반의 탐지기술을 개발하고 네트워크 데이터와 엔드포인트 수집정보를 결합하여 위협 상관/연계 관계를 파악할 수 있는 기술

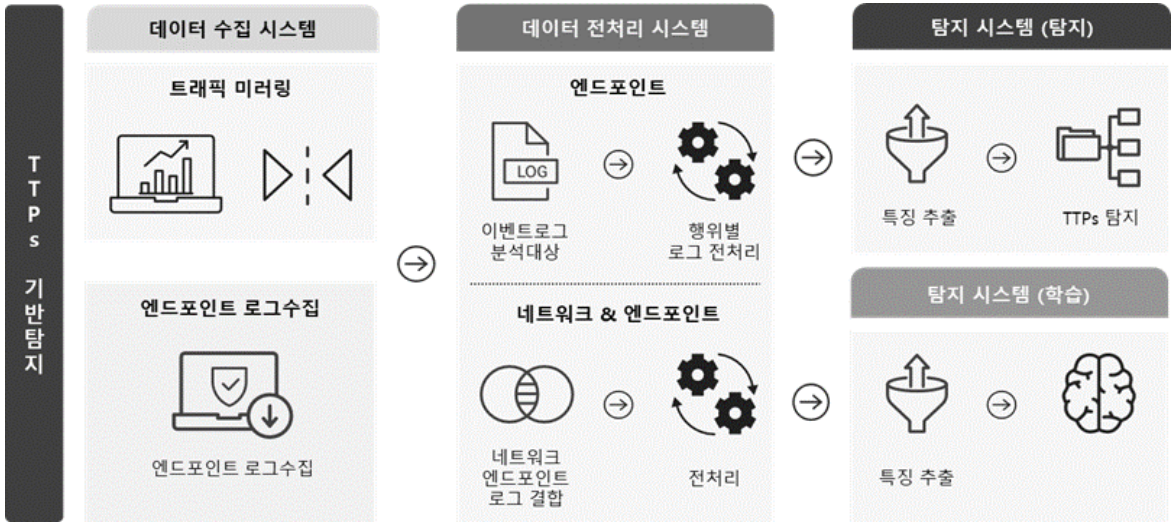
✓TTPs : Tactics(공격전략), Techniques(기술), Procedures(과정)
해커의 공격 전략과 기술, 해킹이 진행되는 과정을 담은 보고서

네트워크 데이터와 엔드포인트 결합 방안



- 네트워크 & 엔드포인트 통합대상 행위기반 위협탐지
- 엔드포인트 이벤트로그의 위협 분석을 위한 NLP기반의 위협탐지 분석 기술 적용
- 엔드포인트 이벤트로그의 행위 타입별 변환방법 적용
- 이벤트로그 위협 탐지를 위한 딥러닝 모델

TTPs기반의 탐지 프로세스

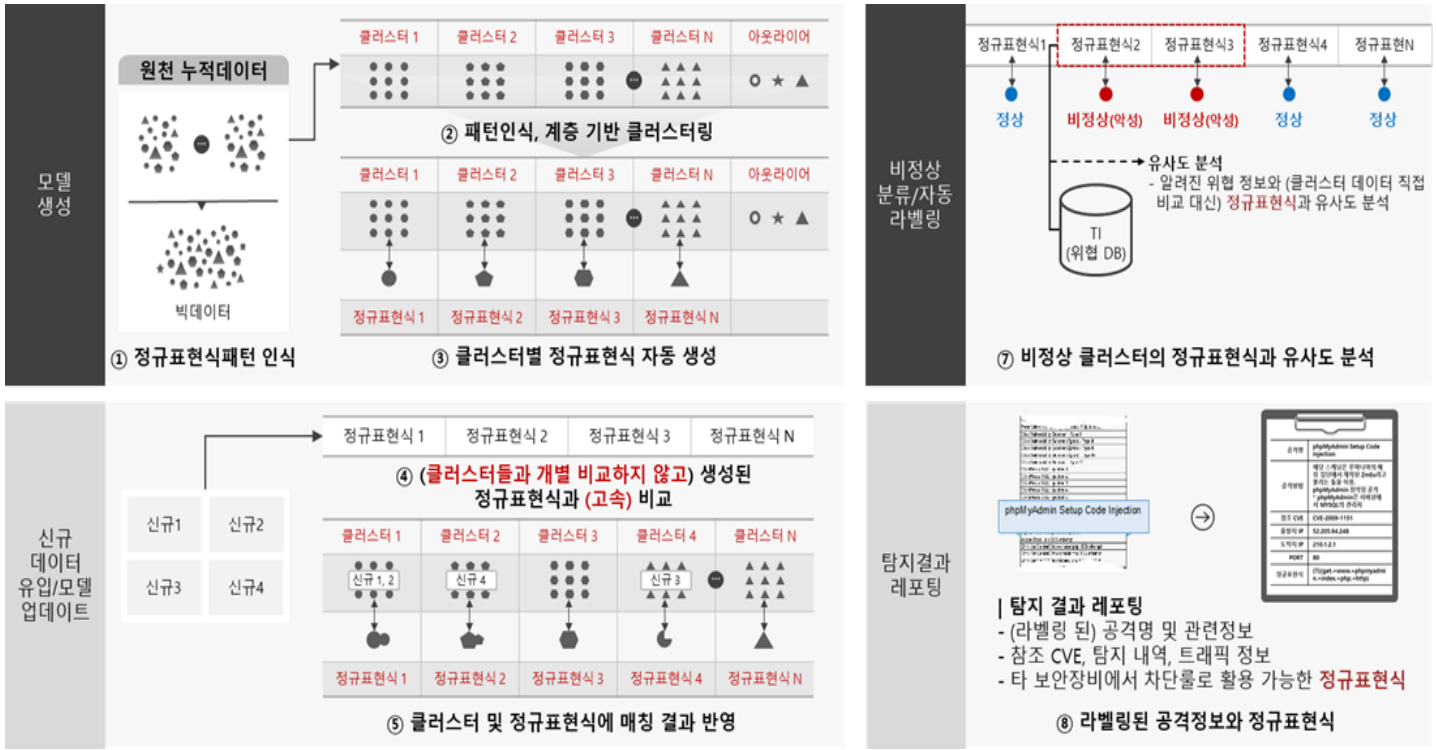


- 네트워크 트래픽 로그 위협 분석을 위해 NLP 모델을 활용한 트래픽 로그 데이터 마이닝 방법
- 네트워크 & 엔드포인트 통합대상의 행위기반 위협탐지를 위한 NLP기반의 위협 탐지 분석 기술

3. ZombieZERO XDR 주요기능 - 분석

사이버킬체인과 TI를 참조하여 탐지된 위협대응과 우선 대응할 이벤트 서열화를 위한 네트워크 탐지결과 자동분류 기술

사이버 위협 탐지를 위한 사이버 킬 체인 기반 탐지 기술



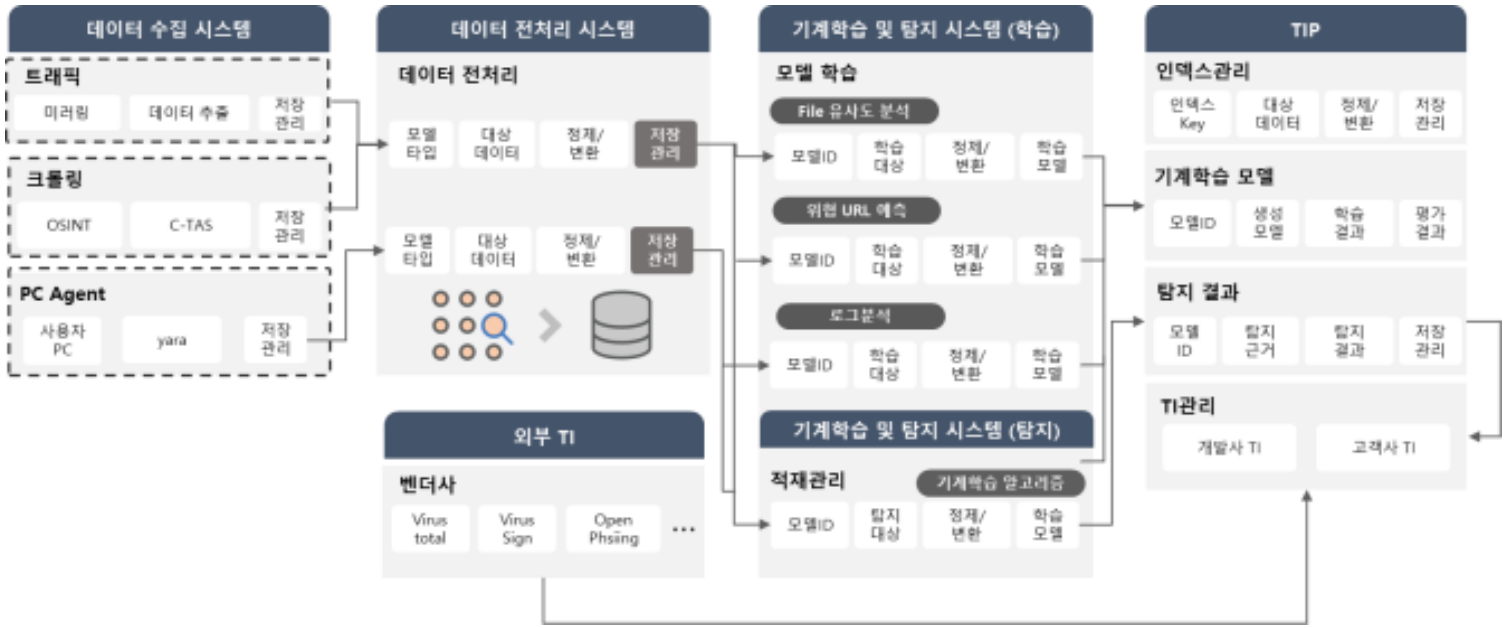
사이버킬체인과 TI를 참조하여 탐지된 위협 대응과 우선 대응할 이벤트 서열화를 위한 네트워크 탐지결과 자동분류 기술

- 웹 서버 대상 비정상 통신 탐지를 위한 비지도학습 정규표현식 자동 생성 기술 기반 고속의 패턴인식 클러스터링 기술 적용
- 비정상 통신 탐지 후 자동 라벨링을 위한 알려진 위협과 유사도 분석기술 적용
- 사이버킬체인 기반 비정상 탐지 모델에 의한 네트워크 데이터 대상 시계열 클러스터링 기술
- 목적 별 데이터 생성 정책 정의
- 목적 별 최적의 시계열 클러스터링 알고리즘 선택
- 전체 시계열 클러스터링 수행을 위한 알고리즘 성능 확보

3. ZombieZERO XDR 주요기능 - TIP

사이버킬체인 탐지 결과에서 탐지근거정보 제공이 가능한 TIP

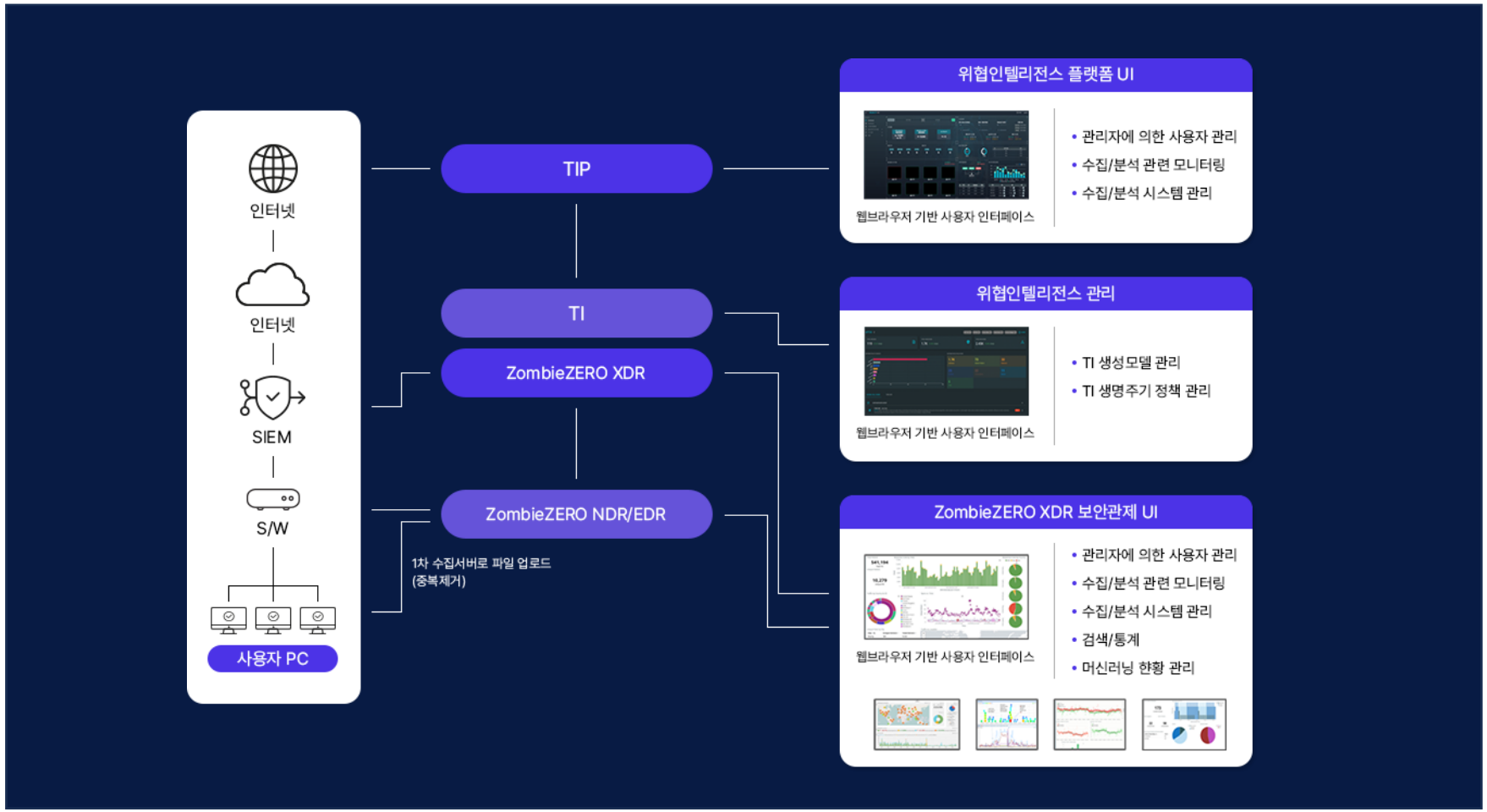
사이버킬체인 탐지 결과에서 탐지근거정보 제공이 가능한 TIP



- 공개정보출처에서 수집된 의심스러운 URL, 도메인에서 수집된 PE파일을 색상 채널을 포함된 이미지로 변환하는 기법
- 위협 사이트 URL, 도메인 특징 추출 기술 적용
- 파일의 악성유무 탐지와 유형 분류를 위한 딥러닝 기반의 모델
- 위협 사이트 탐지를 위한 머신러닝 기반의 위협 탐지 모델
- 공격기법 데이터 생성을 위해 위협분석 보고서의 내용추출 및 분석을 위한 머신러닝 모델링
- 파일의 위협정보 자동 생산을 위한 이미지 기반 파일 악성 및 유형정보 데이터 생성
- 공개정보출처(OSINT)에서 수집된 위협 분석 보고서의 공격기법 정보 데이터 생성

3. ZombieZERO XDR 주요기능 - 대응

관제자동화의 핵심요소를 통합하고 AI와 TIP기술을 융합하여 능동형 대응이 가능합니다.



3. ZombieZERO XDR 주요기능 - 기대효과

XDR의 기술적, 경제적, 사회적 측면의 기대효과

기술적 측면

- APT 공격 대응에 적합한 기술적 방안
- 신규 위협의 유사도의 정밀성을 향상
- 학습 / 비지도기반의 위협 탐지를 통해 탐지율 향상
- 다양한 보안 분야에 적용이 가능한 빅데이터 처리
- AI기반의 능동적으로 생성하는 기술
- 침해사고 케이스별 자동대응

경제적, 산업적 측면

- 신속한 분석을 위한 '악성코드 자동분석 및 대응' 기술의 효과적인 솔루션 제시
- 유사(변종) 악성코드의 유사도 분석 시장은 현재 성장 단계이므로 원천기술 확보
- 확장형 위협탐지 보안제품으로 보안체계 구축 및 운영 비용 감소 기대
- 능동적 대응으로 관리비용 절감 및 효율적인 인력 활용 기대

사회적 측면

- 정보보호 산업육성 및 기술 선진국으로서 위상을 확립
- 악성코드로부터 안전한 업무 환경 조성
- 조기 대응을 통해서 기업 및 조직을 공격으로부터 보호
- 피해로부터 막대한 경제적 손실을 최소화

4

인증 및 수상

4. 인증 및 특허

국제 CC인증 / 혁신제품 인증 / GS인증 / ISO 인증 / 보안기능확인서 등을 보유하고 있으며 미국 2건, 일본 1건을 포함하여 15건의 특허를 등록하였습니다.

인증내역

- “ZombieZERO Inspector V4.0” GS 인증
- “ZombieZERO Inspector V3.0” GS 인증
- “ZombieZERO Inspector V4.0” 국제CC EAL2 인증
- “ZombieZERO Inspector V4.0” ISO 9001 인증

특허내역

국내·외 특허 15건 등록

- APPARATUS AND METHOD FOR BLOCKING ZOMBIE BEHAVIOR PROCESS (미국)
- MALICIOUS CODE DEACTIVATING APPARATUS AND METHOD OF OPERATING THE SAME (미국)
- HACKING PREVENTION SYSTEM FOR MOBILE TERMINAL AND METHOD THEREFOR (일본)
- 악성행위 탐지를 위한 클라우드 기반 가상화 장치, 시스템 및 운영 방법
- 이미지 기반 악성코드 탐지 방법 및 장치와 이를 이용하는 인공지능 기반 엔드포인트 위협탐지 및 대응 시스템

4. 수상 내역

엔피코어는 정보보안 시장에서 우수한 기술을 인정받아 9개의 수상을 거두었습니다.

지능형 지속위협대응 시스템 구축 감사장

정보보호산업발전 유공자

우수연구개발 유공자

수출 첫걸음상 수상

창조기술대상 우수상 수상

글로벌벤처기업 은상

SW신사업 아이디어 공모대회 우수상

5

고객사 레퍼런스

5. 고객 레퍼런스

엔피코어는 국내 뿐만 아니라 해외 시장 진출을 통한 다양한 영업과 판매활동을 활발히 진행하고 있습니다.

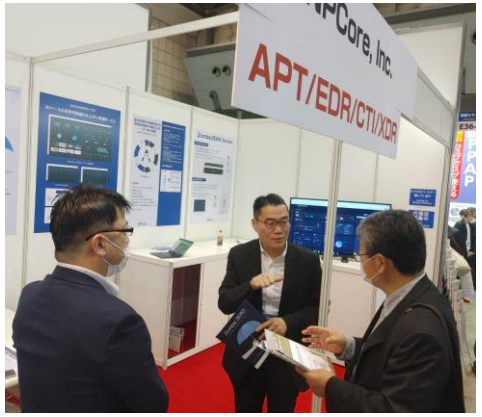
Korean National Police Agency	Prosecution Office	Ministry Of National Defense	Korea Post	Seoul Guarantee Insurance	National Fire Agency
Korea Inclusive Finance Agency	The Korean Teachers' Credit Union	Gyeongsangnam-do	Gyeongsangbuk-do	Seoul Metropolitan Office Of Education	Gyeonggido Office Of Education
BUSAN Metropolitan City Office Of Education	INCHEON Metropolitan City Office Of Education	Gyeongsangbuk-do Office Of Education	JEOLLANAMDO Office Of Education	DAEGU Metropolitan Office Of Education	Korea Student Aid Foundation
KYONG GI University	Dongduk Women's University	OSB Savings Bank	BNK Kyongnam Bank	Financial Services Commission	Posco
JTBC Broadcast Stations	Ls Mtron Industrial Machinery Company	VHS Medical Center	Seoul Medical Center	Jeju National University Hospital	Indosat Ooredoo
Kamisu City Hall, Japan	Royal Malaysia Police	Vietnam Posts And Telecom Group	Vietnam Cryptography University	Ministry Of Transport	Skylake Golf Resort

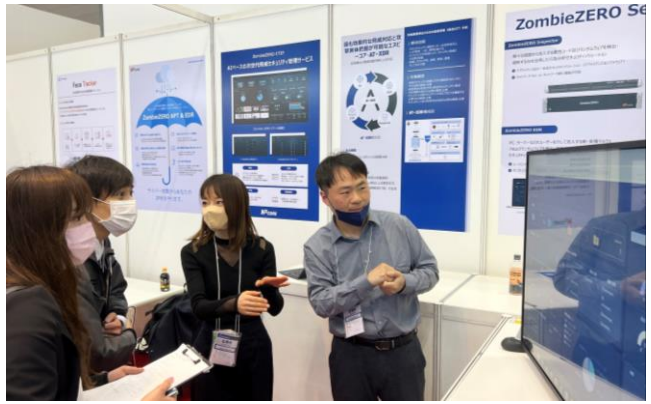
6

글로벌 영업&마케팅

6. 전시회 참가

Japan IT Week Spring 2023, VIETNAM SECURITY SUMMIT 2023, AIBP Conference in Indonesia, AI Expo in Singapore 2023 등
동남아에서 개최된 다수의 전시회 참가하여 동남아시아 시장 내 기업 네이밍과 브랜드 홍보를 하였습니다.





6. 글로벌 영업현황

엔피코어는 우수한 파트너들과 함께 글로벌 정보보안 전문기업으로 도약하고 있습니다.

총판영업

아이티윈, 파이오링크, 대신정보통신 등 우수한 총판과 협업을 통하여 공공, 기업, 금융권 등에 판매

해외영업 네트워크

국제 CC인증 획득 및 우수한 파트너과의 계약을 통하여 미국 및 동남아지역 네트워크를 구축하여 해외 판매를 위한 요구사항 충족 및 영업기회 발굴

해외진출 국가

미국, 베트남 합작법인 및 싱가포르 거점 설립을 통해 싱가포르, 베트남, 태국, 인도네시아, 말레이시아 등의 동남아시아 뿐만 아니라 일본으로 확대 중

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