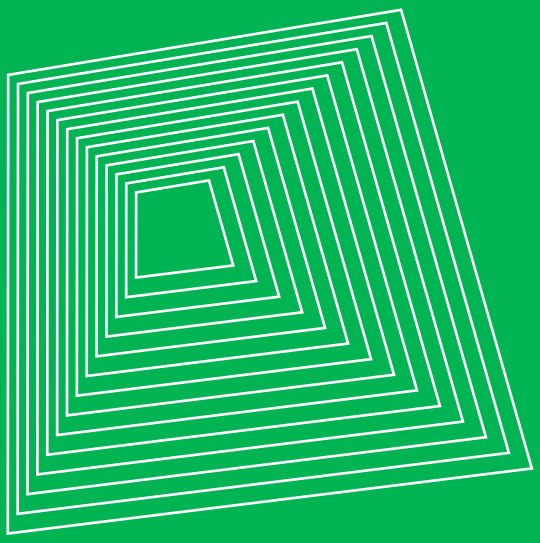
악성코드 위협 대응 솔루션
Threat Inside



# Threat Inside

EST × EST SECURITY

디지털트랜스포메이션 시대

# 기업의 성장 속도만큼 **보안위협의 확산 속도**도 빨라지고 있습니다.

점점 더 고도화되어가는 지능형 사이버 위협. 이제는 알려진 공격보다 알려지지 않은 새로운 공격들이 보다 더 다양한 형태와 방법으로 기업의 안전을 끊임없이 위협하고 있습니다. 급증하는 사이버 공격의 규모와 공격 방식의 발전에 대응할 수 있도록 기업 및 기관의 대응 체계 고도화가 시급합니다.

지능화된 위협에는 기존의 패턴 분석 방식과 정적 분석 방식 이상의 다차원 분석을 통한 정확한 악성코드 식별 정보와 이를 바탕으로 한 정밀 대응이 필요합니다.
조직으로 유입되는 의심 파일들에 대한 정확한 식별과 신속한 분석은 이제는 선택이 아닌 필수이며, 파일의 정상/악성 여부를 밝히는 데서 그치지 않고 실효적 대응책을 마련하고 연관된 위협에도 대비할 수 있어야 합니다.

# 악성코드 위협, 제대로 대응하고 계십니까?

전 세계적으로 4초에 1개꼴로 새로운 악성코드가 만들어지고 있으며, 2초마다 악성 URL이 새롭게 발견되고 있습니다. 최근의 악성코드는 과거 DDoS 공격 등 단발성 공격과는 달리, 타깃으로 삼은 기업과 기관의 시스템에 침투하기 위해 사회공학적 기법 등을 교묘하게 사용, 침투 후 잠복하면서 정보를 지속 수집하고 시스템을 파괴할 수 있는 고도화된 악성코드입니다. 암호화폐 채굴 악성코드 등 점점 더 다양한 목적과 형태의 악성코드가 증가하고 있으며, 공격자들은 수익성 좋은 악성코드들을 기존 보안 솔루션을 우회하는 기법을 활용하여 지속적으로 만들어 낼 것으로 예상됩니다.

지능형 악성코드 위협에 대응하기 위한 인텔리전스 솔루션,
사용 중이거나 도입을 검토 중이라면 몇 가지 확인이 필요합니다.

## 방대한 양의 위협, 경보 피로(Alert Fatigue)는 없습니까?

신·변종 악성코드, 다량의 데이터 트래픽 등 기업과 기관이 이미 사용 중인 보안 시스템에 쌓여 가는 이벤트와 로그들은 더 이상 사람이 분석하는 것이 불가능한 정도의 양으로 증가하고 있습니다. 인텔리전스 솔루션의 도입으로 보안 이벤트 알림이 급증하고, 분석해야 할 대상의 수는 늘어나며, 어떤 정보를 정책상 반영해야 할지 결정하기 어려워져 보안 담당자의 업무는 오히려 가중되는 상황에 이를 수 있습니다.

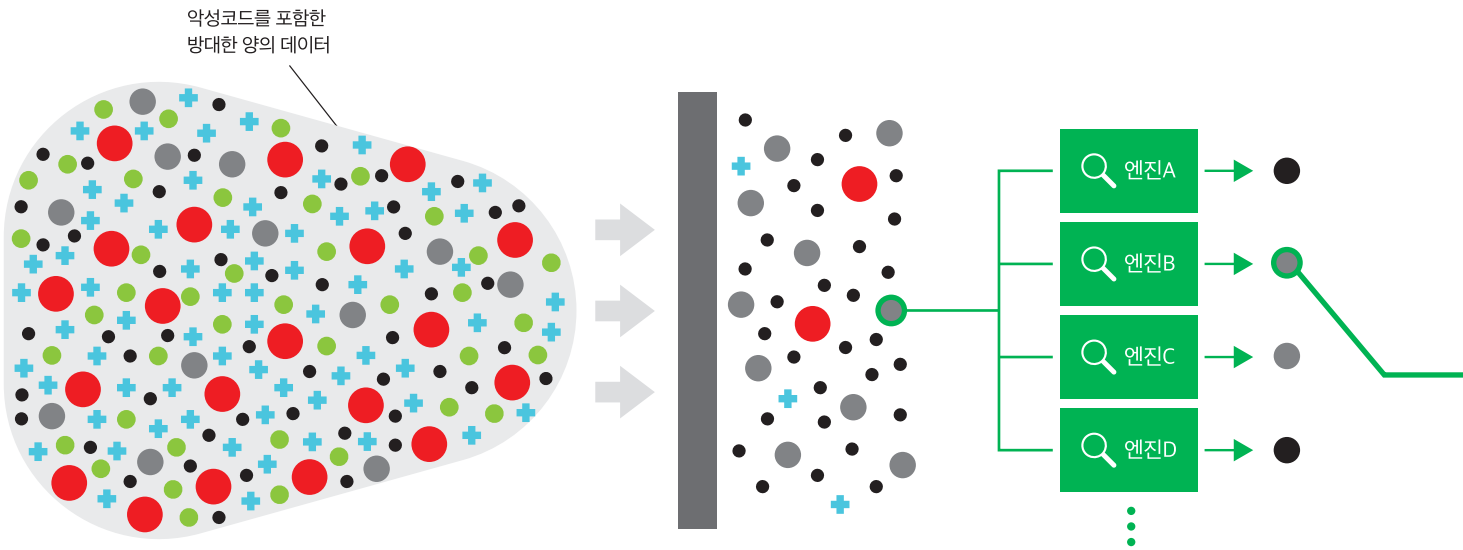
## 기존 악성코드 대응 솔루션, 위협 대응에 꼭 필요한 인텔리전스를 제공합니까?

미국 CSA(Cloud Security Alliance)의 조사에 따르면, 클라우드 서비스상 월간 발생하는 약 27억개 이벤트 가운데 이상행위 기반으로 탐지된 건은 2,542건이며, 이 중 실질적인 위협은 고작 23건이었다고 합니다(110:1의 비율). 이처럼 네트워크 계층의 이상행위 탐지와 대응 중심의 방식은 실질적인 위협을 가려내 주는 데에 한계가 있으며, 단순 평판정보 중심의 샘플 정보 공유 방식의 서비스는 수십 가지의 엔진마다 상이한 결과를 낼 수 있어 확실한 대응을 위한 인텔리전스로는 부족합니다.

솔루션의 도입으로 인해 오히려 경보 피로에 시달리거나 단순 평판정보에만 기댈 수는 없습니다. 기업과 기관이 빠르게 고도화되는 지능형 위협에 대응할 수 있으려면 지금보다 훨씬 더 많은 정보와 진보된 기술을 활용한 악성코드 위협 대응 솔루션을 갖추어야 합니다. 그리고 이를 제대로 만들어 낼 수 있는 역량과 기술, 노하우를 갖춘 기업은 많지 않습니다.

# 악성코드 위협 대응 솔루션
# Threat Inside

이스트시큐리티가 보유한 국내 최고 수준의 악성코드 분석 전문 노하우와 기술이 응집된 '악성코드 위협 대응 솔루션' Threat Inside를 소개합니다. 엔드포인트 보안 전문기술과 인공지능 딥러닝(Deep Learning) 기술을 기반으로, 악성코드 위협의 다차원 분석을 통한 유형의 판별 및 분류, 해당 위협에 대응하기 위해 반드시 필요한 인텔리전스를 제공하는 가장 확실하고 진보된 방식의 악성코드 위협 대응 솔루션입니다.




<이상행위 탐지 기반 솔루션>

<평판분석 서비스>

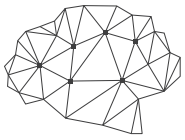
## 기존 솔루션

### 이상행위 탐지 기반 솔루션

UBEA(User Behavior & Entity Analysis)와 SIEM(Security Information & Event Management) 기반으로 주로 네트워크 계층에서의 이상행위 탐지를 통해 대응하는 방식입니다. 데이터 흐름을 통해 비정상적인 이상행위를 판별하는 방식은 방대한 양의 데이터를 한번 걸러 주는 역할은 할 수 있으나, 미탐 또는 과탐의 리스크, 과도한 양의 탐지로 인한 경보피로와 실질적 대응의 어려움 등의 한계점이 존재합니다.

### 평판분석 서비스

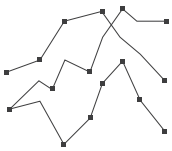
수십 개의 안티바이러스 엔진을 연동한 평판DB 기반의 분석 서비스는 일종의 '집단지성'을 활용하지만, 악성코드의 평판분석 결과는 단어 그대로 '평판'으로 참고 수준에서 활용되고 있으며, 분석 결과 이상의 인텔리전스나 대응 가이드는 제공하지 못한다는 한계가 있습니다.



## Deep Core

A.I.엔진

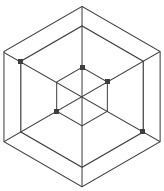
국내 사용자 수 1위 백신 '알약'을 포함한 다양한 채널을 통해 수집된 최신 악성코드를 학습한 A.I.엔진으로, 새롭게 발견된 악성코드까지 식별하고 분류해 줍니다.



## Deep Analysis

다차원 분석 시스템

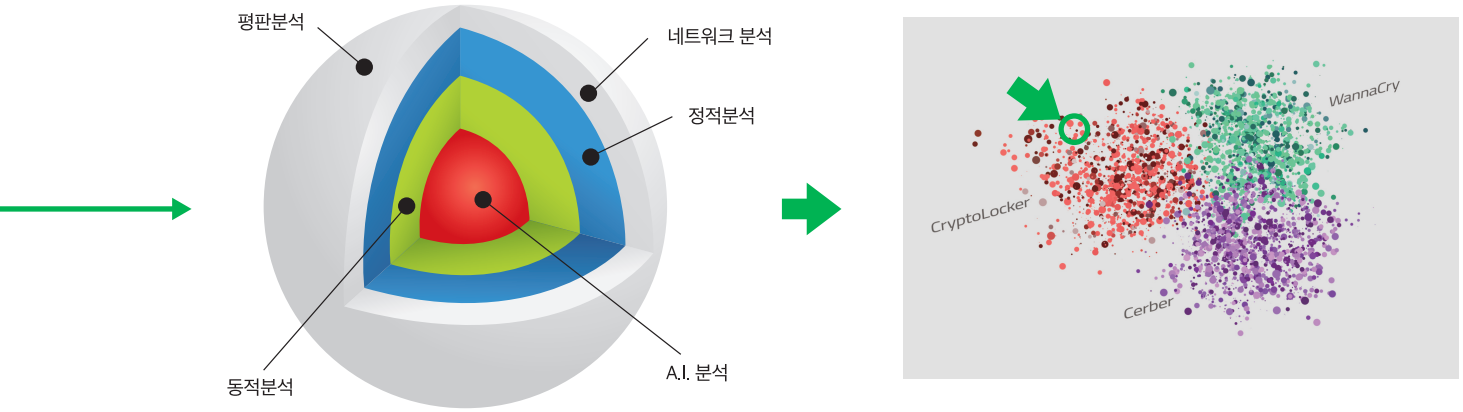
Deep Core와 함께 정적, 동적, 네트워크, 평판분석 엔진 기반의 다차원 분석 시스템으로, 악성코드 위협에 대한 심층분석과 정확한 해석이 가능합니다.



## Deep Insight

인텔리전스 리포트

악성코드의 유형별 특징과 다차원 분석 결과, 유형에 따른 구체적인 대응 방안까지 실질적인 대응 가이드를 제공하는 인텔리전스 리포트입니다.




## Threat Inside

### 악성코드 위협 대응 솔루션

악성코드 위협을 속속들이 파헤쳐 해당 위협의 대응에 반드시 필요한 인텔리전스를 제공

Threat Inside는 딥러닝 기술을 활용하여 새롭게 발견된 악성코드도 식별하고 분류합니다. A.I.분석과 함께 정적/동적/네트워크/평판분석 등 다차원 분석 기법을 적용한 분석 시스템을 통해 위협의 정체와 유형을 상세히 밝혀 주고, 해당 악성코드 위협에 대한 상세한 인텔리전스와 실효적인 대응 가이드를 실시간으로 제공합니다. 이에, 기업 및 기관의 보안담당자는 악성코드 위협에 대한 최종 판단과 대응을 빠르고 정확하게 수행할 수 있습니다.

# 악성코드의 정확한 식별과 분류를 목적으로 연구개발된 Threat Inside

악성코드의 정확한 식별과 분류는 누구나 할 수 있는 게 아닙니다.

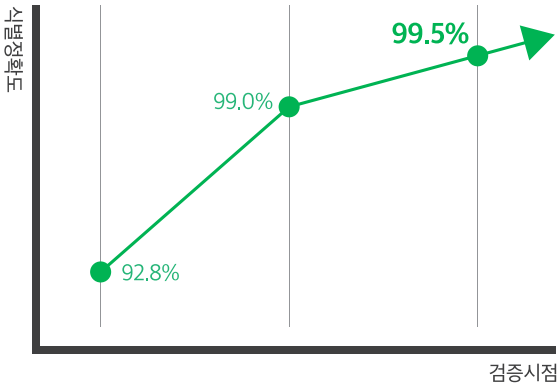
Threat Inside는 10년 이상의 엔드포인트 보안 노하우를 담은 이스트시큐리티만의 사이버 위협 인텔리전스를 기반으로 합니다.
Threat Inside는 수집된 최신 악성코드를 위협요소의 행위와 전략, 기술, 절차(TTPs)에 따른 484개 태그로 그룹핑하며,
이를 APT, 랜섬웨어를 포함한 12가지 대카테고리로 분류하고 있습니다.
또한 Threat Inside의 A.I. 엔진 'Deep Core'는 연 2억 건 이상 악성코드를 탐지/차단하고 있는 국민 백신 알약을 비롯해 국내 최다 1,600만 이상의 사용자 채널로 수집한 최신 악성코드를 학습하였습니다.

## 이스트시큐리티라서 가능한 정확한 위협 분류와 식별

### Threat Inside 다차원분석 엔진의 상세한 위협 분류


<수집된 최신 악성코드> <484개 태그로 그룹핑> <APT 등 12개로 분류>

### Threat Inside A.I. 분석 엔진의 정확한 악성코드 식별



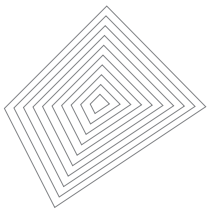

2023년까지 수집된 악성코드 데이터를 학습한 Threat Inside의 Deep Core 엔진에 이후 새로 발견된 악성코드를 검증한 결과, 99.5%의 정확도로 해당 악성코드를 식별할 수 있었습니다.

(※ 데이터셋을 학습셋/검증셋으로 나누지 않고, 학습 이후 새롭게 수집되는 악성코드로 실제 환경에서 검증한 결과)

# Threat Inside의 딥러닝 기술

이제 보안업계에서도 누구나 인공지능(A.I.)을 말하고 있습니다. 그러나 과연 A.I.가 어떤 목적을 위해, 어떤 설계 방식으로 보안 솔루션에 적용되었는지 들여다봐야 그것이 실제 가치를 창출하는 A.I.인지, 표면적으로만 주장하는 A.I.인지 판단할 수 있습니다.
Threat Inside의 딥러닝 기술은 실시간 수집된 양질의 최신 악성코드 데이터의 학습을 통해 신·변종 악성코드의 유형을 식별 및 분류하고 해당 악성코드 위협에 대응하는 실효적인 위협 인텔리전스를 제공해 줍니다.

## 01 신/변종 악성코드에 빠른 대응이 가능합니다.



이스트시큐리티는 수년간 국내 사용자 수 1위 백신 엔진을 운영하며 수집된 양질의 악성코드 데이터를 바탕으로 딥러닝 기반 A.I. 엔진 Deep Core를 자체 개발하였습니다.

Threat Inside의 Deep Core는 정적/동적 분석 결과에 비해 빠르게 악성 여부를 판단하고 딥러닝을 통해 악성코드로부터 추출된 특징들을 학습하여 실시간으로 유포 중인 악성코드에도 효과적으로 대응할 수 있도록 합니다. 또한, 새롭게 탐지된 악성코드로 학습모델을 검증하며 A.I. 엔진의 신뢰도를 높였습니다.

## 02 악성코드를 분류하여 특징과 유형에 따른 대응법을 알려줍니다.

기존 보안 솔루션들은 악성코드를 탐지하고 차단한 후, 그것이 왜 악성이며 어떤 행위를 하는지, 어떤 유형의 악성코드인지 등의 정보를 밝히고 알려주는 데에 한계가 있었습니다. 그런 이유로 기업의 보안 담당자들은 APT 공격에 대한 대응과 신속한 사후조치에 어려움을 겪었습니다.

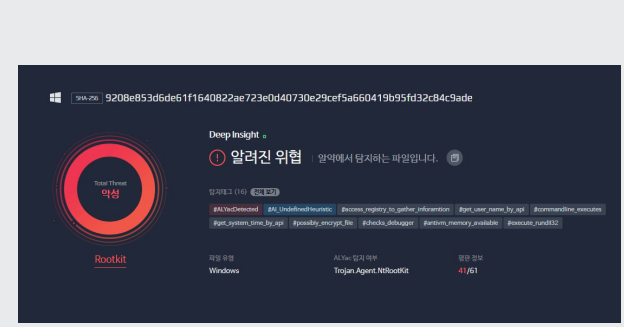
Threat Inside는 'Why'에 대한 해답을 보여 드립니다. Deep Core는 악성코드 유형이 라벨링된 샘플로 학습하는 딥러닝 기반 A.I. 엔진입니다. 따라서 알려지지 않은 샘플도 알려진 유형으로 자동 분류할 수 있습니다. 또한, 분류된 악성코드와 관련된 이슈와 이스트시큐리티 보안 전문가들의 보안 지식과 노하우가 포함된 '인텔리전스 리포트'도 함께 제공됩니다.

## 03 디지털 포렌식에 유효한 정보를 제공합니다.

Threat Inside의 Deep Core는 분석한 악성코드와 특징과 행위가 유사한 파일들을 보여 줍니다. 따라서, 보안 전문가에 의한 수동 분석을 거치지 않아도 신종 악성코드인지 혹은 어떤 악성코드의 변종인지까지도 추정할 수 있습니다. 또한, 악성코드가 누적된 유포 이력 등을 제공하여 침해대응을 위한 디지털 포렌식에 중요한 단서를 제공합니다.

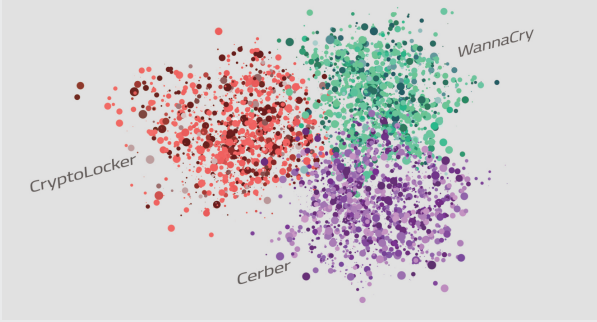
Threat Inside

# Threat Inside 위협 분석 플랫폼



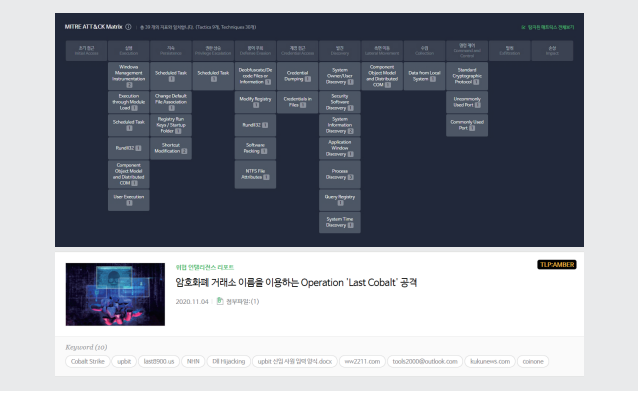

## 다차원 분석 시스템으로 분석을 더욱 정밀하게

- Threat Inside는 다차원 분석 시스템을 적용하여 탐지율과 정확도를 높였습니다.
- Deep Core와 Deep Analysis의 다양한 분석/탐지 결과를 종합하여 Total Threat(위험도, 확장명)을 판단하여, 더욱 정밀한 분석 결과를 제공합니다.



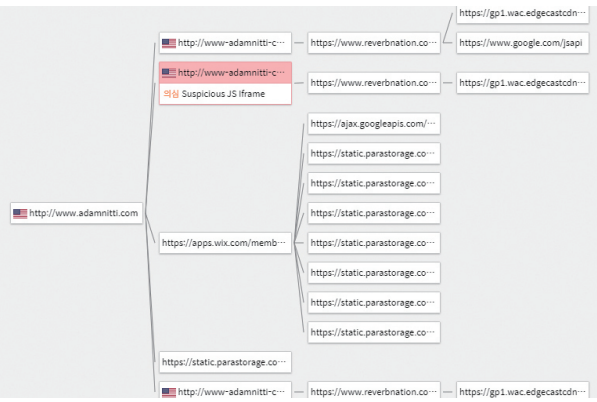

## 다중 AI 기반 엔진으로 악성코드 분류/탐지

- Deep Core AI 엔진은 딥러닝 및 다양한 모델을 기반으로 악성코드를 탐지 및 분류할 수 있습니다.
- Deep Core AI 엔진은 AIOps를 기반으로 알약 센서와 글로벌 악성코드의 데이터셋을 확보해 학습함으로써 국내 및 해외 위협을 동시에 대응합니다.




## 표준화된 분석 정보와 위협 인텔리전스 리포트

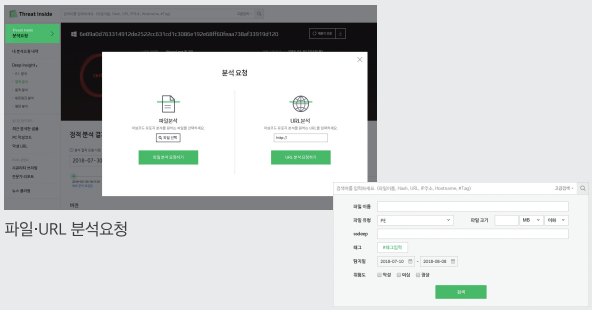
- Deep Insight는 ATT&CK Matrix 표준을 지원합니다.
- 분석 요청된 사내 위협 정보와 OSINT 및 위협 인텔리전스 리포트 간 매칭을 통해 악성 캠페인 및 APT 공격에 대한 대응 전략 수립을 지원합니다.




## Deep Insight. URL 분석 인텔리전스 리포트

- Threat Inside URL 크롤링 시스템은 URL을 수집하고 분석하여, 실시간으로 탐지된 위협 정보를 제공합니다.
- 악성 URL에서 탐지된 IP·도메인 위협 히스토리를 함께 제공하며, 위협 추적에 활용할 수 있습니다.
- 연쇄적으로 발생하는 악성 URL을 탐지하여, 악성코드 유포 정황을 파악할 수 있습니다.

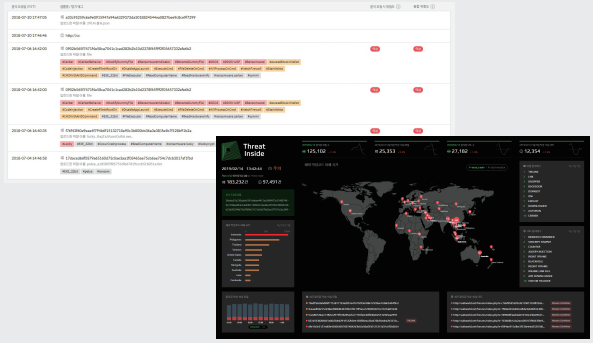
# Threat Inside 인텔리전스 서비스




파일·URL 분석요청



검색·고급검색

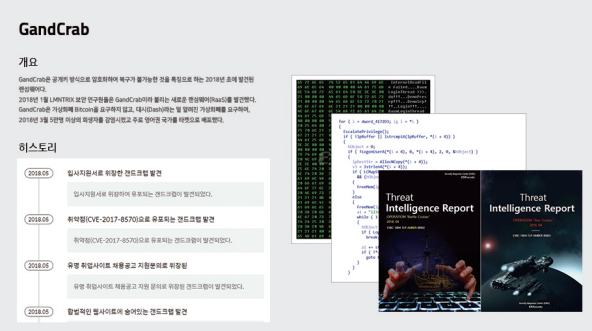


## 원하는 위협 정보를 언제, 어디서나

- 필요한 위협 정보를 실시간으로 검색하고, 의심스러운 파일과 URL은 언제든지 분석 요청할 수 있습니다.
- 해시값 외 다양한 검색 키워드를 제공하여, 원하는 위협 정보를 빠르고 정확하게 찾을 수 있습니다.

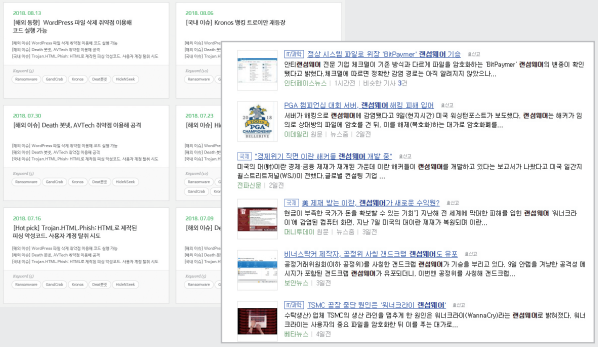
## 실시간 위협 정보와 현황을 한눈에

- 대시보드에서 위협 국가와 IP 등 공격 형태와 실시간 위협 정보를 실시간으로 제공합니다.
- 실시간 탐지 피드에서 현재 유포되고 있는 악성 샘플의 트렌드를 확인할 수 있습니다.




## ESRC에서 작성한 인텔리전스 리포트 제공

- ESRC(시큐리티대응센터) 리포트는 수년간 백신(알약)을 운영하고 대응한 경험을 바탕으로, 보안 전문가의 노하우를 전달해 드립니다.
- 실시간 이슈 분석부터, 코드 레벨의 상세 분석리포트와 TLP별 위협 인텔리전스 리포트까지, 다양한 레벨의 보안 전문 지식을 제공합니다.



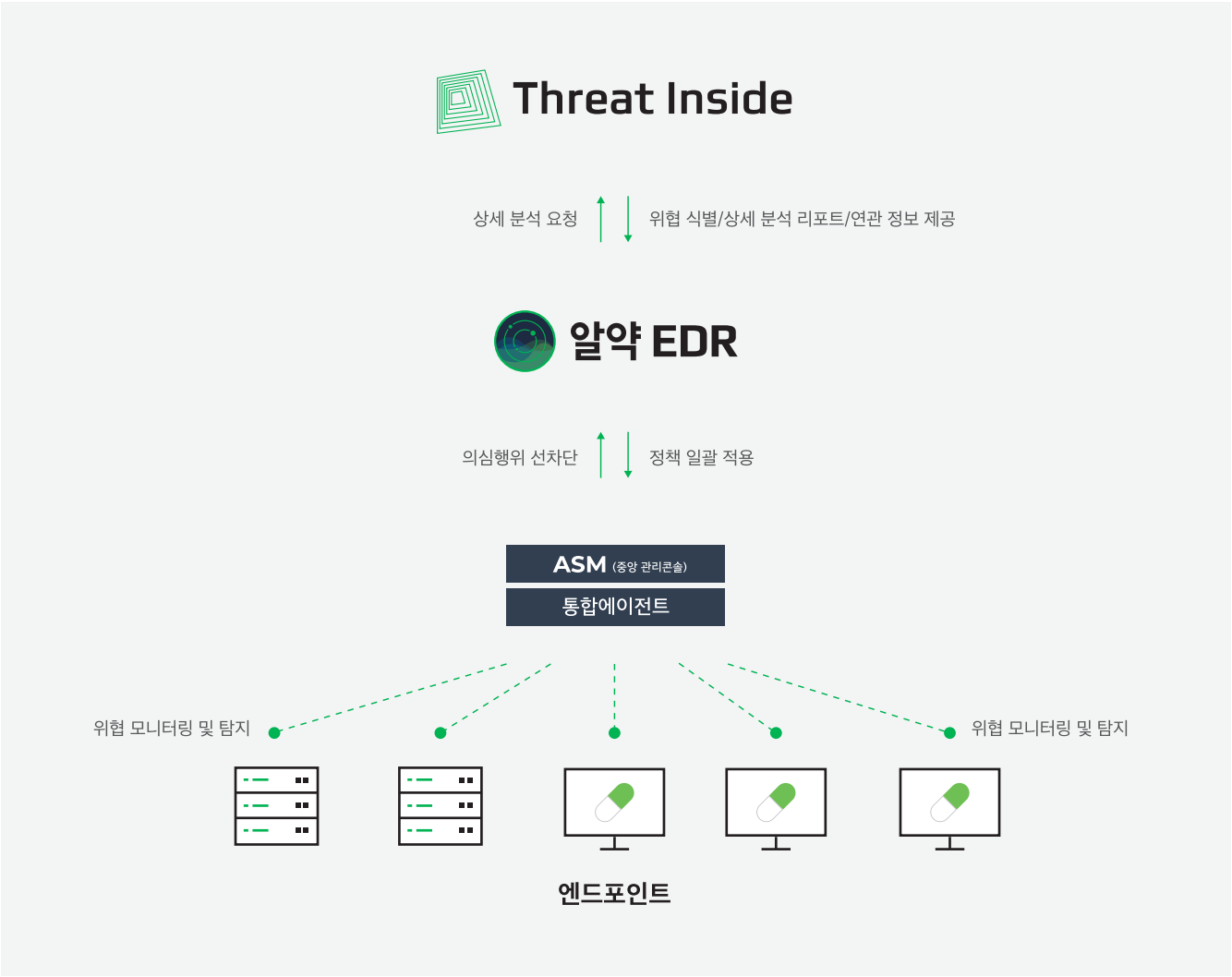
## Threat Inside만의 시큐리티 큐레이팅 서비스

- 시큐리티대응센터가 해석해 주는 최근 국내외 보안 이슈를 시큐리티 브리핑으로 제공합니다.
- 뉴스 큐레이터에서 원하는 키워드가 포함된 뉴스를 클리핑할 수 있습니다.

# Threat Inside 사용 시나리오

## 01 Threat Inside × 알약 EDR

Threat Inside는 엔드포인트 위협 정보를 선별하여 수집하고, 알려지지 않은 위협을 선제적으로 차단하는 알약 EDR과의 결합을 통해 위협 차단에서 식별로 이어지는 보안 대응 범위 확장으로 차세대 엔드포인트 보안 체계를 완성합니다.




※ Threat Inside 플랫폼은 웹콘솔과 API 서비스 형태로 제공하며 구축형으로 도입이 가능합니다.

## 02 악성코드·악성 URL 대응 및 차단

**파일·URL 분석 및 검색**
의심스러운 파일·URL
분석 요청 및 관련 키워드 검색

→

**Deep Insight.**
Deep Insight.에서 악성코드의
유형 및 특징 파악

→

**대응 및 차단**
사내 보안 정책에 반영

## 03 기존의 보안 솔루션과 API로 연동하여 보안 강화

**사내 보안 솔루션과 API 연동**
사내에서 탐지된 알 수 없는 샘플 API로 분석 요청

→

**샘플 위협 여부 판단**
Deep Insight.에서 악성코드의 유형 및 특징 파악

→

**대응 및 차단**
사내 보안 정책에 반영

## 04 Threat Inside의 정제된 리포트, 인텔리전스 서비스에서 최근 보안 이슈와 트렌드 파악

**데일리 보안 이슈 모니터링**
시큐리티 브리핑, 뉴스 큐레이터

**실시간으로 유포되는 위협 정보 파악**
실시간 탐지 피드, 대시보드

**Threat Inside에서 뉴스 검색**
이슈 컨텍스트 파악

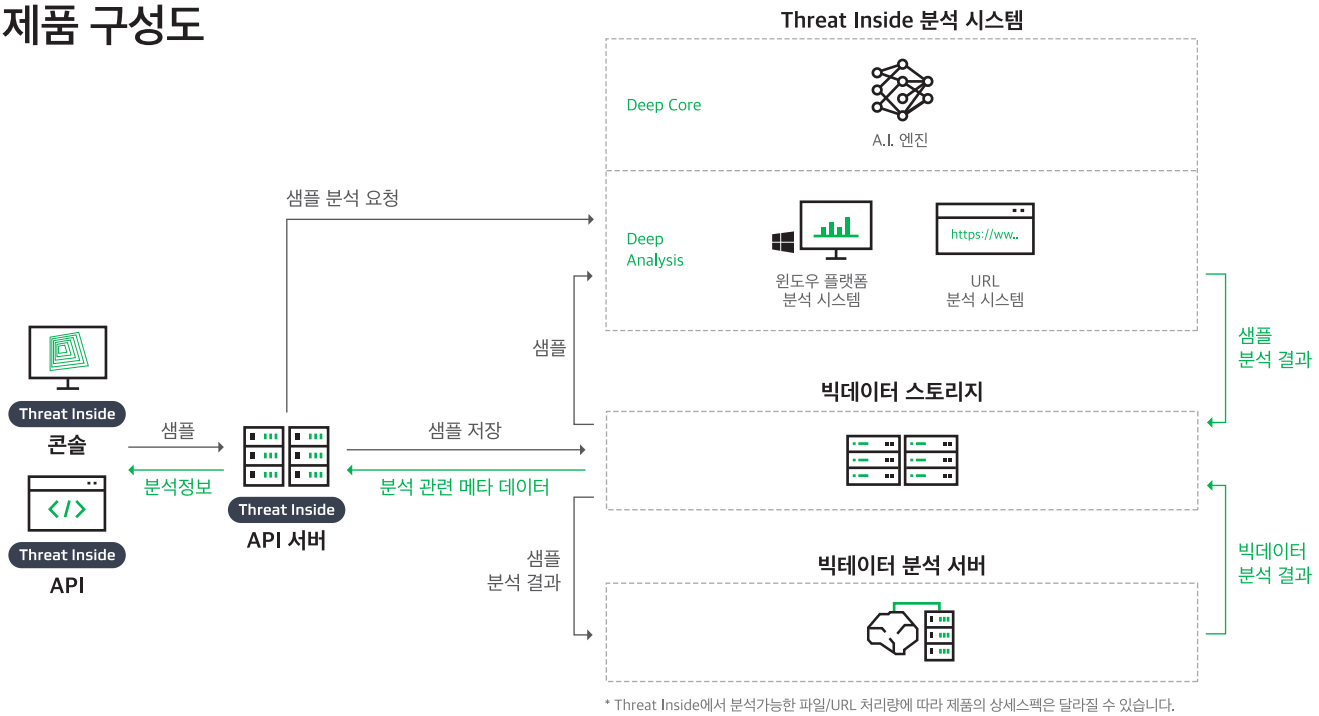
→

· 이슈 리포트
· 상세 분석 리포트
위협 이슈 분석

→

**위협 인텔리전스 리포트**
위협 추적 및 디지털 포렌식

## 제품 구성도




* Threat Inside에서 분석가능한 파일/URL 처리량에 따라 제품의 상세스펙은 달라질 수 있습니다.

We know cyber threat inside and out

EST × EST SECURITY

이스트시큐리티(주)

서울시 서초구 반포대로 3 이스트빌딩 (우)06711 www.estsecurity.com

T : 02-583-4616 F : 070-4850-9024 E : bizcenter@estsecurity.com

Threat Inside