ESTsecurity
Make World More Secure with A.I.

# 알약 EDR을 통한 차세대 엔드포인트 보안 전략



이스트시큐리티 솔루션영업팀 전병승 과장

ESTsecurity

# Index

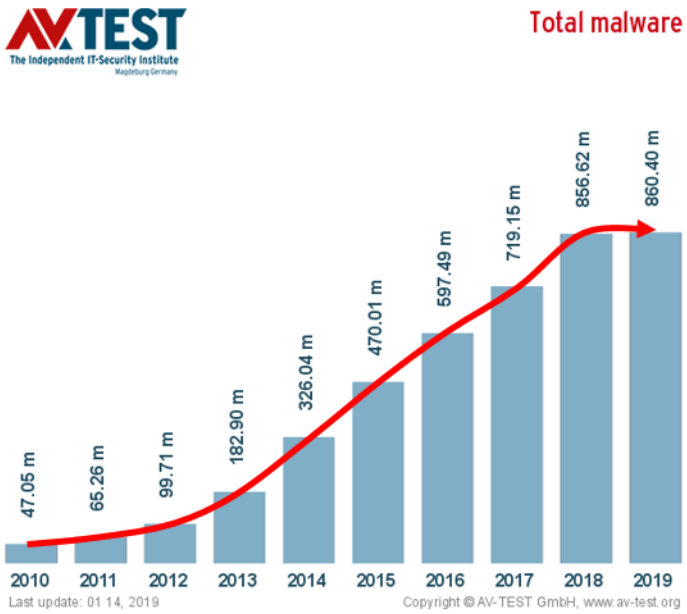
01

# 현재, 그리고 앞으로의 사이버보안

# 사이버 위협

## 지속적으로 증가하는 사이버 위협과 지능/조직화된 APT 공격

- IT 기술이 발전하고 플랫폼이 늘어나면서 공격의 대상, 종류, 방법 등 사이버 위협 요소 또한 증가하고 있습니다.
- 해가 거듭될수록 사이버 공격은 더욱 지능화되며, 제로데이 위협은  갈수록 커지고 있습니다.




출처 : AV-TEST Statistics (www.av-test.org)


### 제로데이 공격 증가

· 제로데이 취약점 공격 사상 최대 기록
· 시스템 및 애플리케이션의 취약점 악용

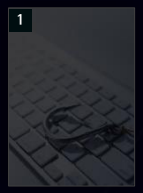

### 지능/조직화된 APT 공격

· 새로운 공격 기법 접목시켜 응용화
· 다양한 유입 경로를 통한 공격

# 2018-2019 위협 인텔리전스 리포트 (ESRC)

ESTsecurity × Threat Inside
https://www.threatinside.com

1

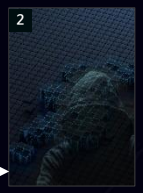


## Coin Assembly

특정 국회의원실의 가상화폐 법인자료로 위장한 표적공격 주의

2018.02

2

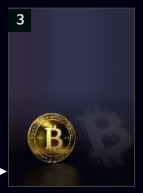


## Comeback Kimsuky

오퍼레이션 김수키(Kimsuky)의 은밀한 활동, 한국 맞춤형 APT 공격은 현재 진행형

2018.02

3



## Baby Coin

2010년 해외 대상 APT 공격자, 오퍼레이션 베이비 코인(Operation Baby Coin)으로 한국 귀환

2018.04

4

## Battle Cruiser

'오퍼레이션 배틀크루저' 다양한 취약점으로 국내외 APT 공격 지속

2018.04

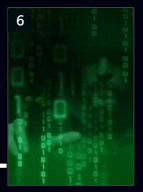
5

## Star Cruiser

국가기반 APT 그룹 '오퍼레이션 스타크루저(Operation Starcruiser)' 사이버 첩보활동 지속

2018.04

6



## One Zero

판문점 선언 관련 내용의 문서로 수행된 '작전명 원제로(Operation Onezero)' APT 공격 분석

2018.05

7

## Water Tank

안보·대북 연구기관 등을 상대로 한 APT 공격, '작전명 물 탱크(Operation Water Tank)'

2018.05

8

## Rocket Man

금성121 그룹의 최신 APT 캠페인

2018.08

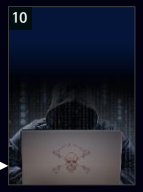
9


## Ghost Puppet

최신 APT 캠페인, 작전명 유령 꼭두각시 (Operation Ghost Puppet)

2018.09

10



## Battle Cruiser2

라자루스 최신 APT 작전 '배틀 크루저(Operation Battle Cruiser)' 재등장

2018.10

11


## Mystery Baby

한국 대상 최신 APT 공격, 작전명 미스터리 베이비(Operation Mystery Baby) 주의!

2018.11

12


## Black Bird

'오퍼레이션 블랙버드' 금성121의 모바일 침공

2018.11

13


## Decoy Plane

국제 정세 문서 파일을 미끼로 정보를 노리는 '오퍼레이션 디코이 플레인(Operation Decoy Plane)'

2018.12

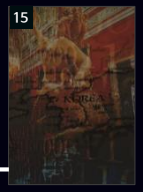
14


## Black Limousine

안보·외교·통일 관련 분야를 겨냥한 APT 공격, '작전명 블랙 리무진' 주의

2018.12

15



## Hunter Adonis

암호화폐 내용의 Konni APT 캠페인과 '오퍼레이션 헌터 아도니스'

2019.01

16


## Korean Sword

금성121(Geumseong121) 정부기반 APT그룹, '코리안 스워드(Operation Korean Sword) 작전' 수행 중

2019.01

17


## Magic Carpet

라자루스 그룹의 공격은 현재 진행형, 'Operation Magic Carpet'

2019.01

18


## Cobra Venom

통일부 기자단을 상대로 한 APT공격, 오퍼레이션 코브라 베놈(Operation Cobra Venom)

2019.02


## Fake Capsule

일요일 수행된 APT 변종 공격, 오퍼레이션 페이크 캡슐(Operation Fake Capsule) 주의

2019.02


## Extreme Job

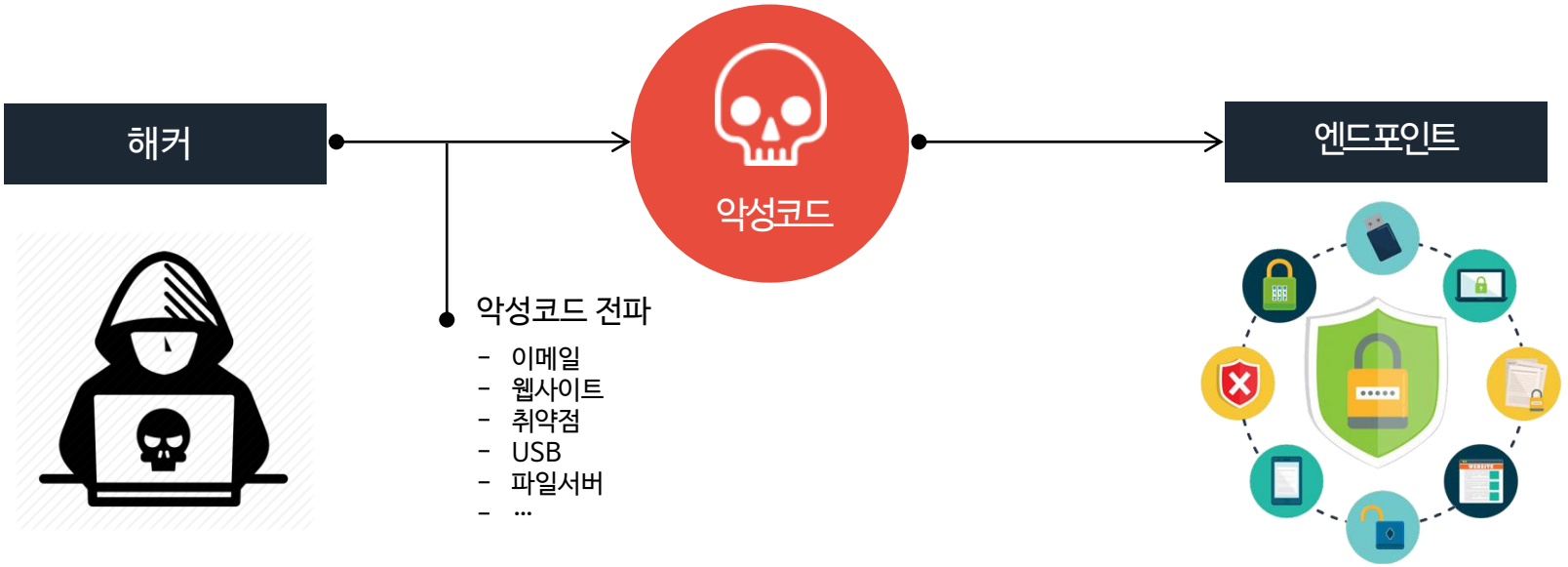
라자루스 APT 조직, 오퍼레이션 익스트림 잡(Operation Extreme Job)으로 공격 수행

2019.01

# 왜 엔드포인트 보안이 중요할까요?

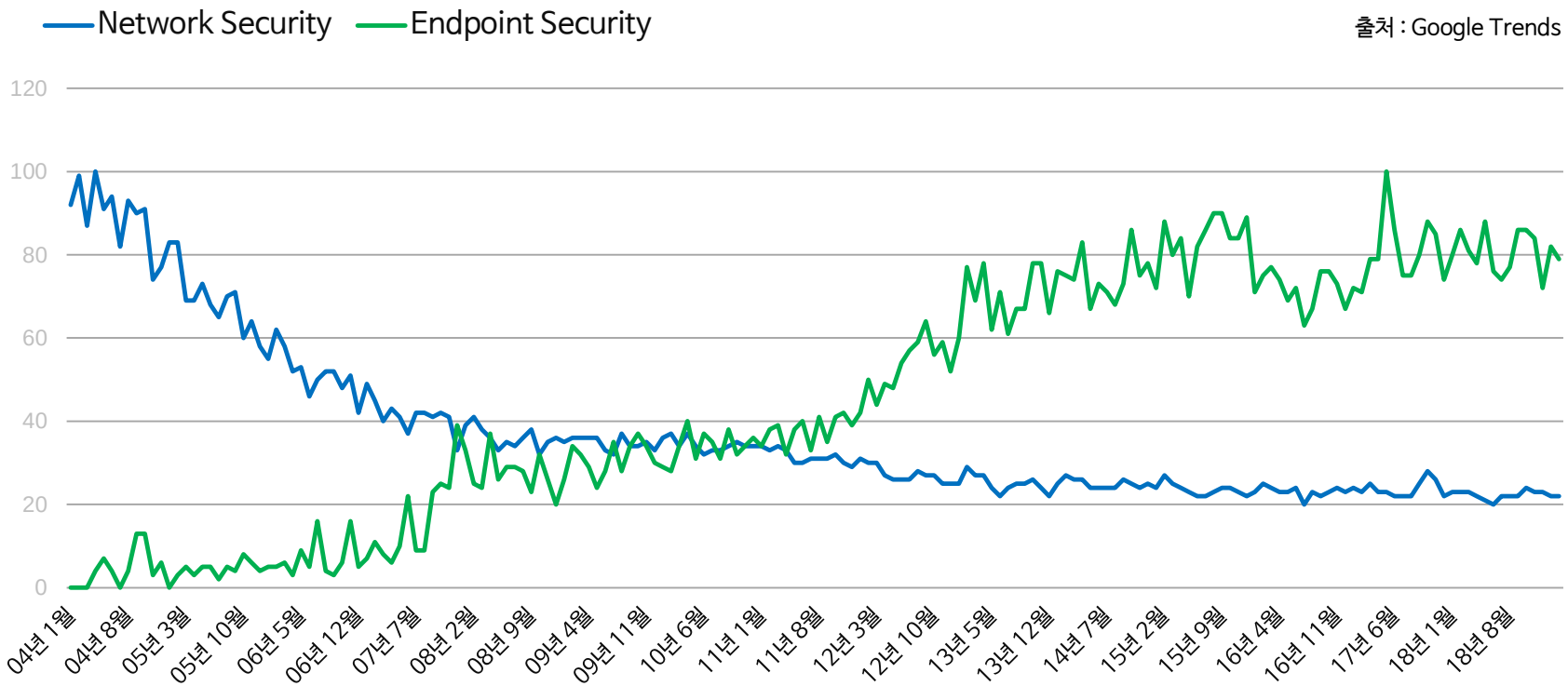
## 대부분의 보안 사고는 엔드포인트 타깃

이메일, 웹사이트, USB, 파일 서버 등 경로는 다르지만 최종적으로 목표하는 타겟은 엔드포인트입니다.
엔드포인트에 악성코드를 심는 것이 공격의 최우선 목표이기 때문에 엔드포인트 보안에 신경 써야 합니다.



## Google Trends 검색 결과

- 지난 15년 동안 엔드포인트 보안과 네트워크 보안은 반비례적인 모습을 보임
- 시간이 지날수록 엔드포인트 보안에 이슈가 더 집중되고 있으며 중요성을 나타냄




Before
Ransomware
After

ESTsecurity

2018년 이스트시큐리티

# 알약 랜섬웨어 행위기반 차단 누적 통계


* 알약 패턴탐지 건수는 제외한 수치입니다

**연간** 평균 차단 건수
2,490,635건

**월간** 평균 차단 건수
207,553건

**일간** 평균 차단 건수
6,824건

1시간 평균 차단 건수
284건

ESTsecurity

| Before | After |
| --- | --- |
| Reactive | Proactive |
| Signature | Non-Signature |
| Known | Unknown |

02

# EDR이란?

# EDR (Endpoint Detection & Response) 정의

ESTsecurity

공항에서는 출입국 심사 시 사전에 작성된 Black List를 통해 탑승자의 탑승 허용/불가 여부를 결정합니다.
이것은 백신의 시그니쳐 엔진을 통한 악성코드 탐지 과정과 유사합니다.

사전에 정해진 목록을 통해서 위협 여부를 판별하는 것은 신속하고 정확하게 위협을 예방할 수 있는 방법이지만,
목록에 누락된 위협에 대해서는 대응할 수 있는 방법이 없다는 단점이 있습니다.

# EDR (Endpoint Detection & Response) 정의

ESTsecurity

최근 공항에서도 보안 강화와 선제 대응을 위해 CCTV를 설치하여 사각 지대를 최소화하고 행동감지요원을 배치하여 공항 내 거동 수상자를 식별하게 되는데, 이것이 엔드포인트 보안에서의 EDR 역할이라고 볼 수 있습니다.

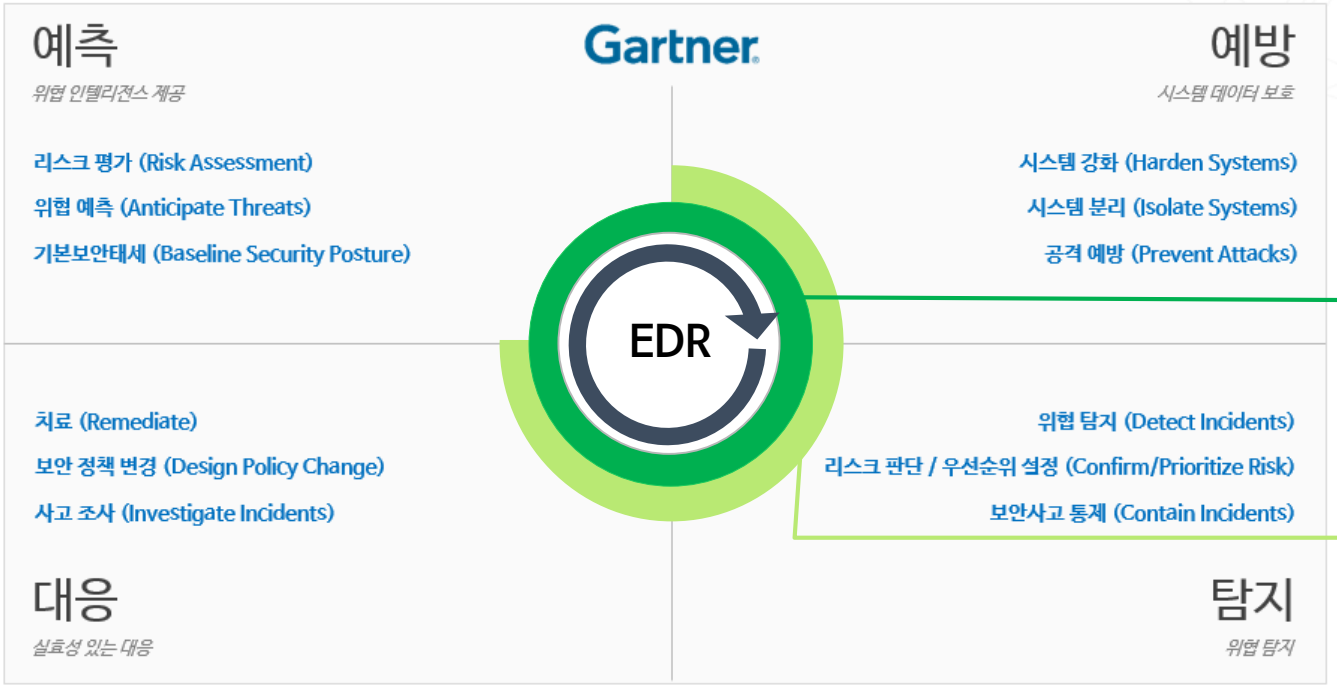
EDR은 공항을 감시하는 CCTV처럼 엔드포인트에서 발생하는 모든 위협을 모니터링하고 수집하여 가시성을 확보하고, 거동 수상자를 검문하는 행동 감지 요원처럼 시스템을 위협하는 의심스러운 행위를 포착하여 대응 방법을 제시합니다.

# EDR (Endpoint Detection & Response) 정의

EDR은 엔드포인트 영역에서 지속적인 모니터링과 대응 방법을 제공하는 보안솔루션입니다.

가트너는 아래와 같이 예측-예방-대응-탐지를 EDR의 주요 기술로 정의하고 있으며,

대부분의 EDR 제품이 위협의 지속적인 감시를 통한 가시성 확보와 대응 기능을 주요 기능으로 제공합니다.




**가시성 확보**

- 이벤트 수집
- 위협 분석
- 위협 흐름도 제공

**차단 및 치료**

- 행위 기반 차단
- 프로세스 종료
- 네트워크 차단

가트너 EDR 기술 정의

EDR 제공 기능

# EDR (Endpoint Detection & Response) 정의

EDR과 기존 백신 솔루션의 가장 큰 차이 또한 가시성 확보 영역과 대응 기능의 범위인데,

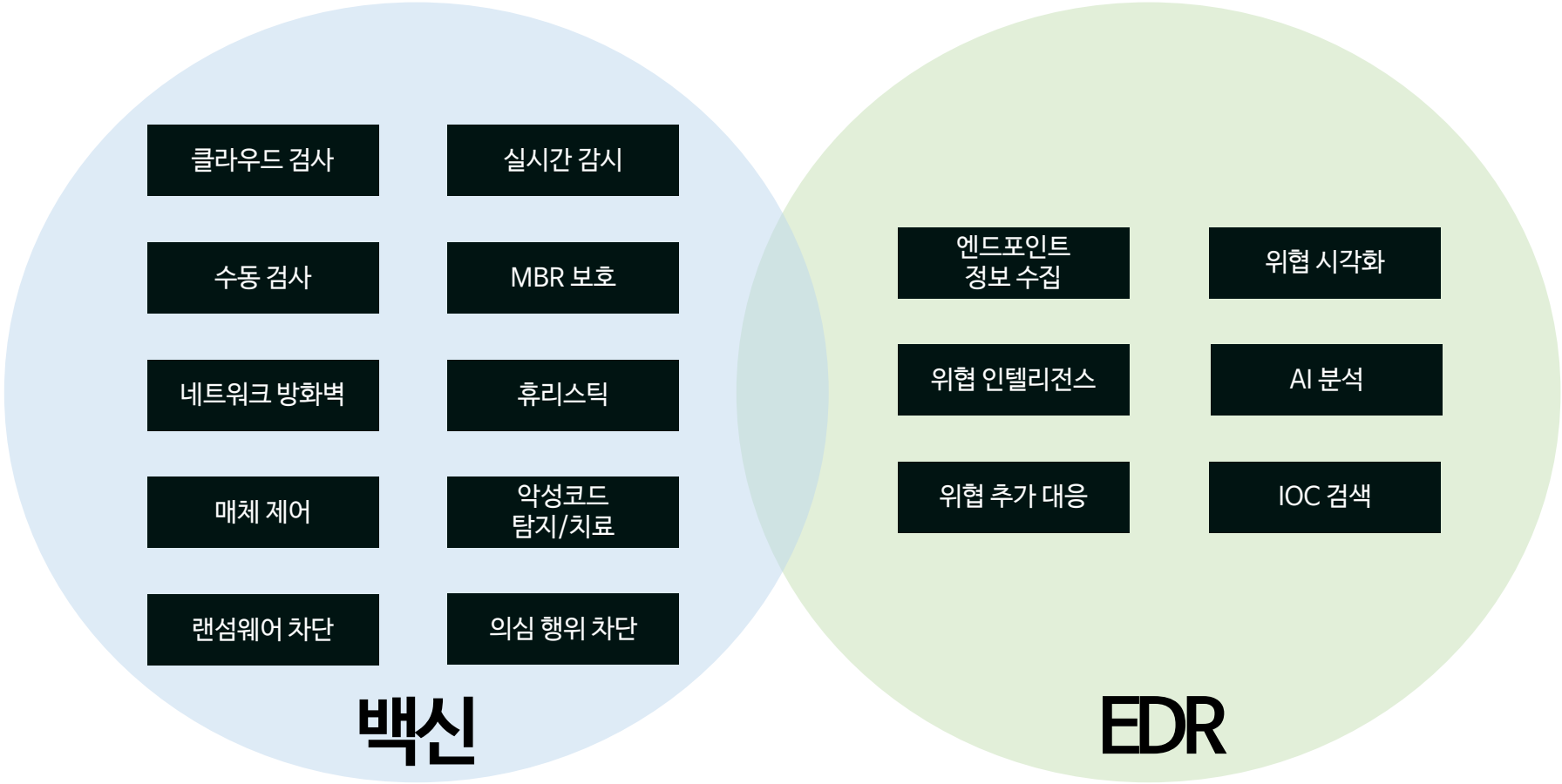
EDR은 백신에서 파악하지 못한 위협을 효과적으로 파악하고 실질적으로 대응하는 것을 목표로 합니다.

| | 백신 | EDR |
|---|---|---|
| 위협 탐지/차단 방식 | 시그니처 DB | 행위 기반 (의심 행위, 악성 행위) |
| 알려진 위협 탐지 | O | △ |
| 알려지지 않은 위협 차단 | X | O |
| 악성 파일 치료 여부 | O | O |
| 엔드포인트 가시성 확보 | X<br>(가시성 확보 한계, 감염 경로 확인 불가) | O |
| 추가 대응 | X | 프로세스 종료, 네트워크 차단 |

# EDR (Endpoint Detection & Response) 정의

ESTsecurity

보안 관리자는 백신과 EDR을 함께 사용함으로서 위협 대응 범위를 확장할 수 있습니다.

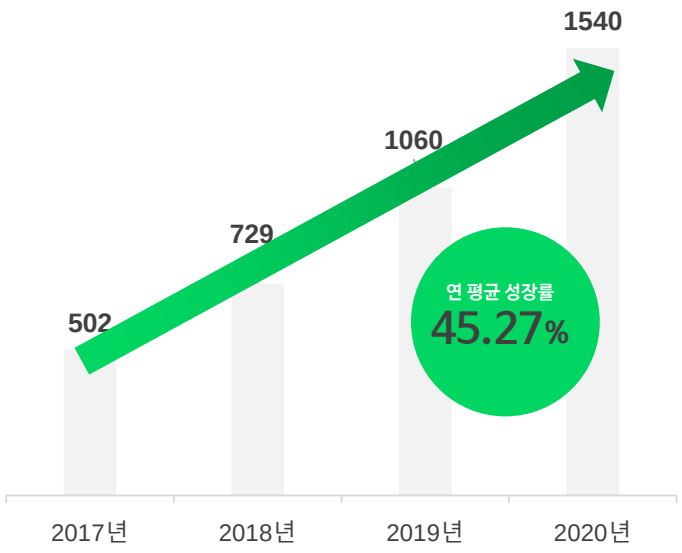


# EDR시장 현황 및 전망

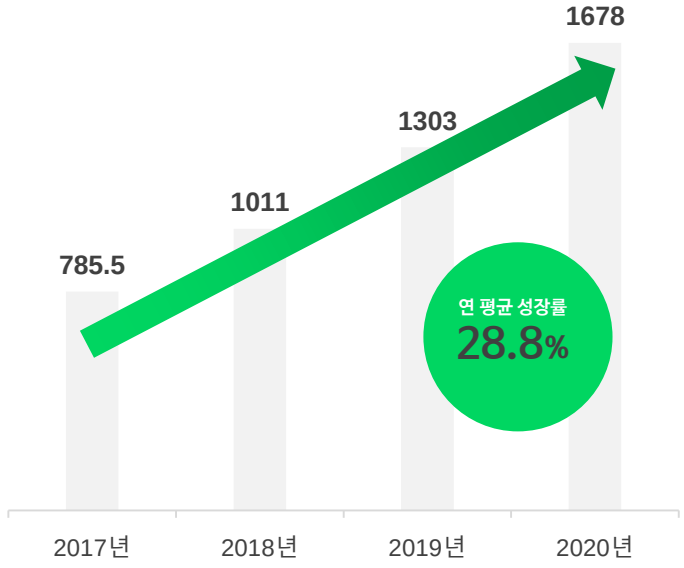
엔드포인트 탐지 및 대응 솔루션인 EDR은 최근 글로벌 보안 시장에서 가장 큰 폭으로 성장하고 있습니다.

## [EDR 시장규모]

(단위 : Million USD)



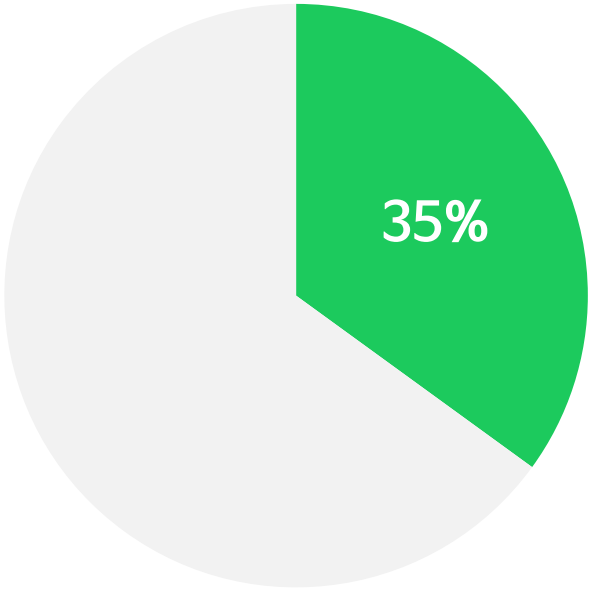

출처: 글로벌 시장조사기관 'Gartner' (2017)




출처: 글로벌 시장조사기관 'The Insight Partners' (2018)

# EDR시장 현황 및 전망

## 글로벌시장 EDR 도입률




출처: 글로벌 시장조사기관 'ESG' (2017)

## 가트너가 예측한 2020년 EDR시장

- 대규모 기업 전체의 80%
- 중간 규모 기관들 전체의 25%
- 소규모 기관/기업의 10%

**〉〉 모두 EDR 에 투자 할 것이라고 전망**

출처: 글로벌 시장조사기관 'Gartner' (2017)

# 시장에는 어떤 EDR 제품들이 있을까요?


# 기존 EDR 솔루션의 한계

## 01 평판 분석의 한계

- 없거나 다른 제품을 연동해야 함
- 평판 조회 결과를 활용함
- 평판 조회 시 샘플이 공유되는 문제

## 02 드라이버 문제

- 모니터링을 위한 별도 드라이버 설치 필요
- 이에 따른 중복 / 충돌 이슈 발생
- 유저 레벨만 지원하는 제품도 있음

## 03 에이전트, 관리콘솔 중복

- Antivirus 기능을 위한 별도의 에이전트 필요
- 별도의 관리 콘솔 필요
- 비효율적인 자원 낭비 발생

## 04 과도한 관리 리소스

- 과도한 Alert 정책
- 악성코드 행위를 차단하지 못하고 Alert만 제공
- 관리 포인트가 많고 대응 과정이 복잡함

03

# 이스트시큐리티의 EDR

# 이스트시큐리티의 핵심 경쟁력

이스트시큐리티는
**진보된 엔드포인트 보안 기술과 전문성**을 기반으로 성장해 나가고 있습니다.

ESTsecurity

**1,600만+**
사용자(센서)를 통한
악성코드 빅데이터 보유

**딥러닝**
알고리즘 기반
첨단 인텔리전스 보안

**ESRC***
국내 최고 전문성의
악성코드 분석가 풀 보유

**엔드포인트**
10년 이상의 '알약' 사업 통한
엔드포인트 보안 전문성 보유

* ESRC : ESTsecurity Security Response Center

# 기존 EDR의 한계점 해결

## 01 자체 엔진

- 자체 개발 엔진으로 알려진 위협 탐지
- 과탐 / 오탐 최소화 정책
- 평판 분석은 추가 로만 제공

## 02 커널 레벨 드라이버

- 기존 알약에서 사용하는 드라이버 공유
- 중복 / 충돌 이슈 없음
- 효율적인 체계 유지 가능

## 03 통합에이전트 / 관리콘솔

- Antivirus를 포함한 통합 에이전트 지원
- 하나의 통합 관리 콘솔 지원
- 효율적인 보안 운영이 가능

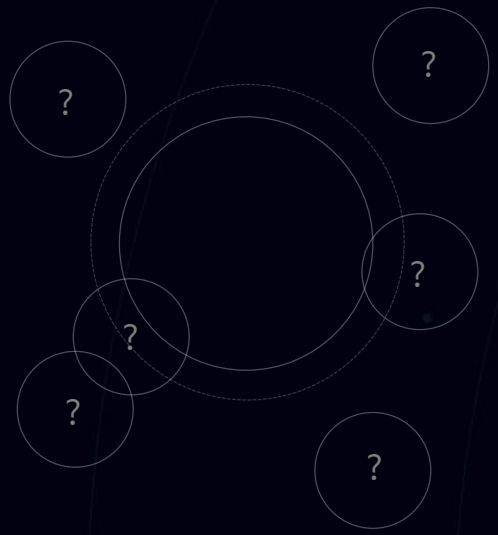
## 04 관리 리소스 최소화

- 탐지 위협에 따른 차단/대응 프로세스
- 선 차단, 후 Alert
- 과탐 / 오탐 방지를 통한 Alert 최소화

# Issue(1)

## 평판분석의한계

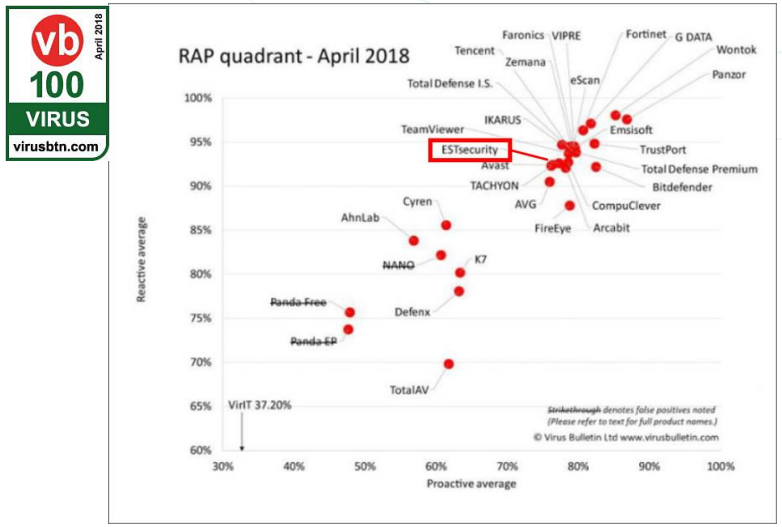
-없거나다른제품을연동해야함
-평판조회결과를활용함
-평판조회시샘플이공유되는문제




# Solution(1)

## 자체엔진

-자체개발엔진으로알려진위협탐지
-과탐/오탐최소화정책
-평판분석은추가정보로만제공




* RAP(Reactive Detection and Proactive Detection) 테스트
Reactive Detection: 업데이트 시점을 기준으로 그 이전에 수집된 악성코드 진단율 측정
Proactive Detection: 업데이트 중단한 시점 이후에 수집된 샘플로 진단율 측정

# Issue(2)

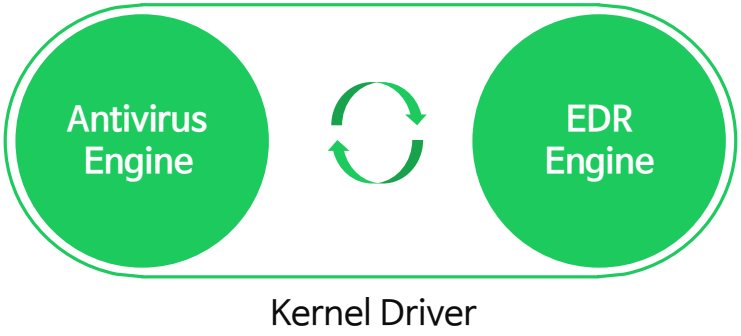
## 유저레벨드라이버

-모니터링을위한별도드라이버설치필요
-이에따른중복/충돌이슈발생
-유저레벨만지원하는제품도있음


# Solution(2)

## 커널레벨드라이버

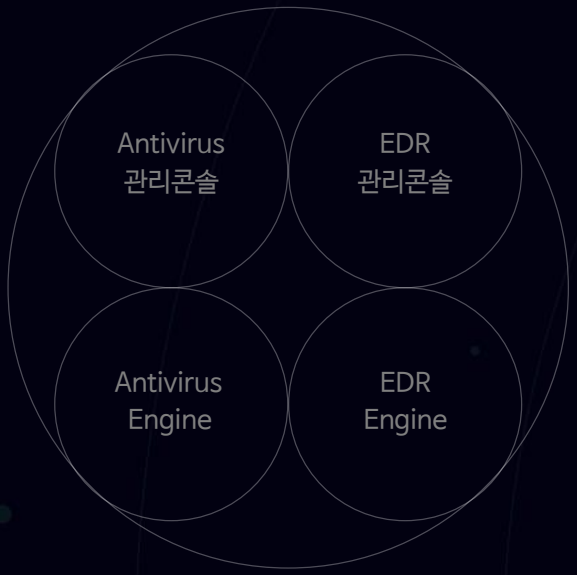
-기존알약에서사용하는드라이버공유
-중복/충돌이슈없음
-효율적인체계유지가능



# Issue(3)

## 에이전트, 관리콘솔 중복

- Antivirus 기능을 위한 별도의 에이전트 필요
- 별도의 관리콘솔 필요
- 비효율적인 자원 낭비 발생




Two & Two

# Solution(3)

## 통합에이전트/관리콘솔

- Antivirus를 포함한 통합에이전트 지원
- 하나의 통합관리콘솔 지원
- 효율적인 보안운영이 가능


One & One

# Issue(4)

## 과도한관리리소스

-과도한Alert정책
-악성코드행위를차단하지못하고Alert만제공
-관리포인트가많고대응과정이복잡함


# Solution(4)

## 관리리소스최소화

-탐지위협에따른차단/대응프로세스
-선차단,후Alert
-과탐/오탐방지를통한Alert최소화

# 주요 기능

알약 EDR은 EDR의 필수 요소와 관련한 다양한 기능을 제공합니다.

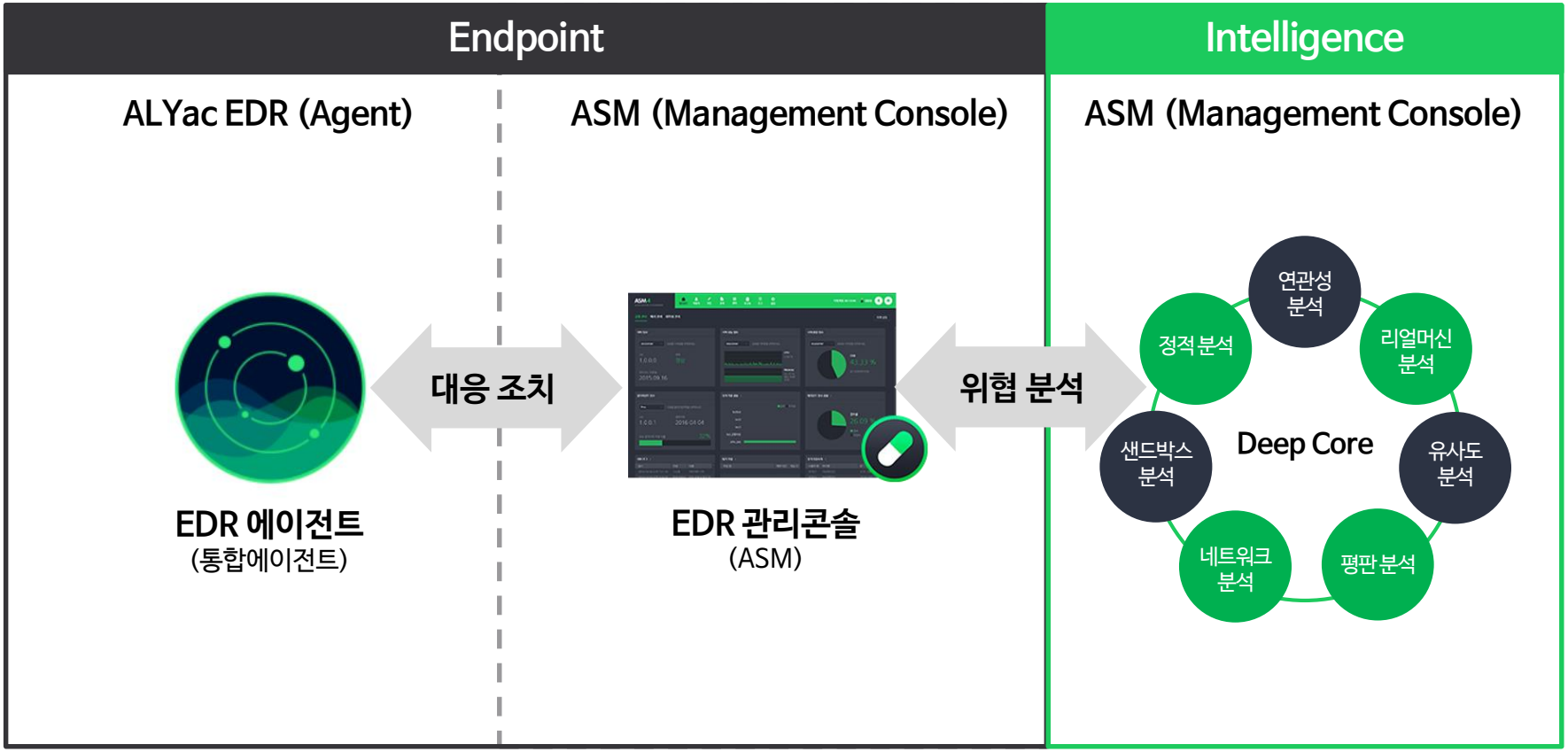
| 분류 | 주요 기능 |
|---|---|
| 수집 | 차단/탐지 파일 실시간 자동 수집 |
| | 파일 정보 / 메모리 / 레지스트리 / 서비스 / 드라이버 / 프로세스 정보 수집 |
| | 시스템/어플리케이션/보안 로그 수집 |
| 탐지 | 알려진 위협 실시간 탐지 |
| | 알려지지 않은 위협 실시간 차단 (랜섬웨어, Fileless, exploit,) |
| 대응 | 에이전트 프로세스 종료 |
| | 에이전트 네트워크 차단 / 격리 예외 처리 |
| | 에이전트 원격 제어 |
| | BlackList/WhiteList 기능 제공 |
| 분석 | 다양한 조건으로 파일 정보 검색 () |
| | 파일 다운로드 기능 |
| | 위협 흐름도 제공 |
| | 탐지/분석 결과 알림 |
| 관리 | 대시보드 제공( 실시간 위협 현황, 서버 상태 모니터링) |
| | 사용자 권한 관리 |
| | 인사 DB연동 |
| | 수집 서버 접근 감사 로그 |
| | 사용자 정의 보고서 |

# 알약 EDR의 특징




# 특장점 (엔드포인트와 인텔리전스의 결합)

자사 인텔리전스 서비스인 Threat Inside와의 결합을 통해 탐지력과 대응력을 강화시켰습니다.



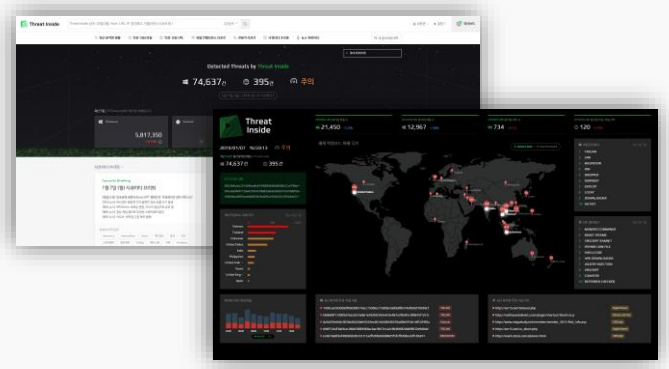
04

# 위협 인텔리전스
# Threat Inside

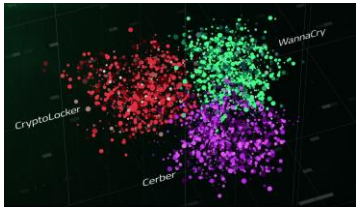
ESTsecurity

# Threat Inside

"악성코드와관련된
사이버위협인텔리전스를제공하는
악성코드위협대응서비스"



## 01 Deep Core – A.I.엔진




딥러닝기반
A.I.엔진으로
악성코드유형분류

## 02 Deep Analysis – 다차원분석


## 03 Deep Insight – 위협인텔리전스리포트

9b5b364a32c759ada38bdc4cbfaad3ed8dc333f87796e27eef52a96d43c821a2

재분석 요청


gandcrab

**Deep Insight**

## 알려지지 않은 위협

Threat Inside가 위협 요소를 탐지하는 파일입니다.

Hash

MD5 | SHA-1 | SHA-256 | SSDeep | ImpHash

탐지태그 (10) 전체보기

#Gandcrab #Ransomware #ModifyDummyFile #RenameDummyFile #Ransom #TerminateTrapProcess

### Anti-Virus Info

| 알약 탐지명 | 알약 탐지 건수 (지난 30일) | 평판 분석 2018-11-06 10:43 조회 |
|---|---|---|
| Trojan.Ransom.GandCrab | 107 | 조회결과 없음 |

### Summary

| 파일 유형 | 리소스 언어 | 디지털 서명 |
|---|---|---|
| Windows | United States | 서명 정보 없음 |

IOC IOC와 매칭되는 ESRC 리포트가 1개 있습니다.

IOC IOC와 일치하는 인텔리전스 리포트

위협 인텔리전스 리포트

2018. 10. 05

갠드크랩(GandCrab) 랜섬웨어 집중해부

#Ransomware #Sage #Trojan #GandCrab #랜섬웨어 #Trojan.Ransom.GandCrab

TLP:AMBER

상세 분석 리포트

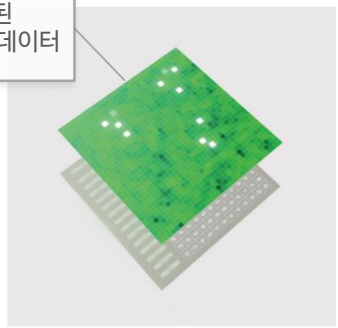
2019. 02. 27

이미지를 드롭하는 GandCrab 5.0.4 발견!

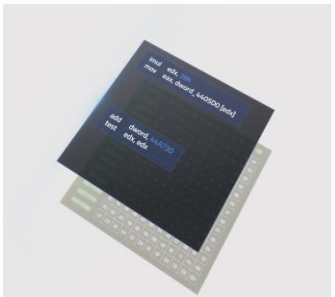
#GandCrab #CVE-2017-8570 #Trojan.Ransom.GandCrab #갠드크랩 #배송장(한진택배).egg #입사지원서.doc #러시아다크웹

# Threat Inside의 딥러닝 기술

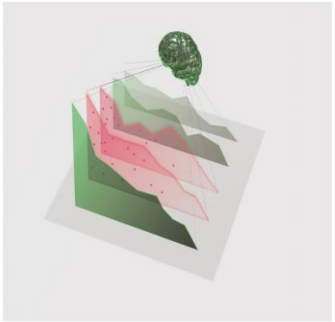
실시간으로 수집된
최신 악성코드 빅데이터



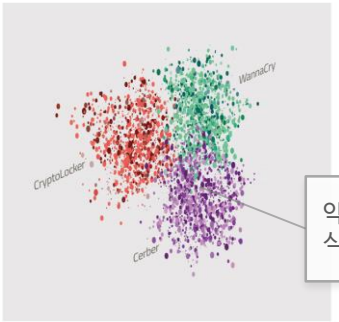
바이너리 파일
전체로부터
CNN기반 딥러닝 학습



시퀀스 패턴을 찾아
딥러닝 학습



함수 유사성 탐지




유사 악성코드
클러스터링,
탐지명 부여

악성코드의 정확한
식별과 분류

# Deep Core – A.I.엔진

## Top Tag 기반의 Precision 값을 기준으로 99.5% 확률로 위협을 정확하게 분류하고 있습니다.

-〉 해당 결과는 한 데이터셋 내에서 학습셋과 검증셋을 나누지 않고 학습 이후 새롭게 수집되는 샘플셋을 기준으로 나온 검증 결과입니다.

〉〉 **Timeline 기반의 Evaluation 기법을** 사용함 (기존에 많이 사용되는 X(교차) Evaluation 기법은 공격자들의 우회 기법에 대해 검증하는데 제한적)

〉〉 2018년 6월 테스트 결과 : 3월~4월 샘플로 학습한 엔진으로 학습되지 않은 5월 수집 샘플을 검사한 결과 : **92.8%**

〉〉 2018년 8월 테스트 결과 : 3월~6월 샘플로 학습한 엔진으로 학습되지 않은 7월 수집 샘플을 검사한 결과 : **99.0%**

〉〉 2018년 10월 테스트 결과 : 3월~9월 샘플로 학습한 엔진으로 학습되지 않은 9월 수집 샘플을 검사한 결과 : **99.5%** (지속적인 정확도 증가)

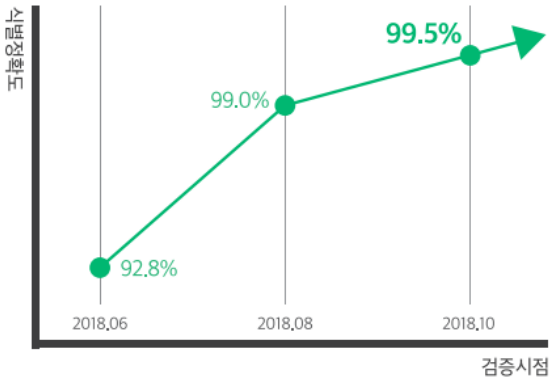
## 12개의 대분류와 100개의 소분류로 악성코드를 정확히 판별합니다.

-〉 Threat Inside에서 분류 가능한 전체 분류는 총 484개이며, Deep Core에서는 이 중 100개의 소분류를 확진하고 있습니다.

-〉 확진 가능한 분류 체계는 학습이 거듭 될 수록 지속 증가 중 입니다.

-〉 분류되는 유형에는 Ransomware, Banker, Spyware 등의 악성코드 분류와 APT NorthKorea, China 등 APT 그룹에 대한 분류가 모두 포함되어 있습니다.

**(1) 탐지/분류 결과**




**(2) 위협 분류 체계**


빅데이터 기반의 샘플 | 소분류 : 100개 | 대분류 : 12개

# Deep Insight – 위협 인텔리전스 리포트

**이스트시큐리티 대응센터(ESRC)에서는 국가기반 위협그룹에 대한**

**체계적인 인텔리전스 연구와 추적을 통해"위협 인텔리전스 리포트"를 발행하고 있습니다.**

- 위협 인텔리전스 리포트는 APT 관련 사건을 심층적으로 분석하고 추적하여 최상위 레벨의 종합 인텔리전스를 제공합니다.
- 보고서에는 공격자의 전략, 기술, 절차(TTPs)에 따른 체계적인 코드레벨 분석 내용과 원본 샘플, 침해지표(IOC)를 포함하고 있습니다.


위협 인텔리전스 리포트 2018.12.19

안보·외교·통일 관련 분야를 겨냥한 APT 공격, '작전명 블랙 리무진' 주의

증견선언 | 개인정보활용동의서 | 미국_정상회담_전망_및_대비 | padosori.co.kr/_controller/admin/upload_sec/down.php

artndesign2.cafe24.com/skin_board/s_build_cafeblog/exp_include/img.png | rentcartoday.com/home/skin_member/mem_standard/lib/upload/down.php

FF9EFF561FD793DDB9011CF7006D5F6C | 8332BE776617364C16868C1AD6B4EFE7 TLP:AMBER

위협 인텔리전스 리포트 2018.12.17

국제 정세 문서 파일을 미끼로 정보를 노리는 '오퍼레이션 디코이 플레인(Operation Decoy Plane)'

Konni | phpschboy.prohosts.org | jams481.site.bz | minvostokarzvitia.webatu.com | dowhelsitjs.netau.net | patchfilepacks.net23.net

member-daumchk.netai.net | donkeydancehome.freeiz.com | 59D39C774D48137D2A91E286F47626F0 | BC95C7A5713760EB7D39CA0976F2FFD5 TLP:AMBER

위협 인텔리전스 리포트 2018.12.03

'오퍼레이션 블랙버드' 금성121의 모바일 침공

Spyware | APT | 금성121 | 오퍼레이션_블랙버드 | 모바일_스파이 | OperationBlackbird TLP:AMBER

**해외 인용 사례 (ESRC – Threat Intelligence Report)**

- N. Korean hackers suspected of continuing attacks amid friendly inter-Korean relations
- North Korean hacker group infiltrates popular South Korean
- Alien Vault : Operation Mystery Baby
- Alien Vault : Operation Ghost Puppet
- Geumseong121が政府を騙って北朝鮮関連団体に調査依頼のデコイで仕掛けている模様。
- 韓国で新たな規制法案も：度重なる大手取引所ハッキング被害
- 借南北韓離散家庭團聚　黑客發釣魚攻擊
- Вредонос KevDroid способен тайно записывать телефонные звонки жертв
- دژیم طبض یناهنپ ار اهسمت هک یرازفادب فشک

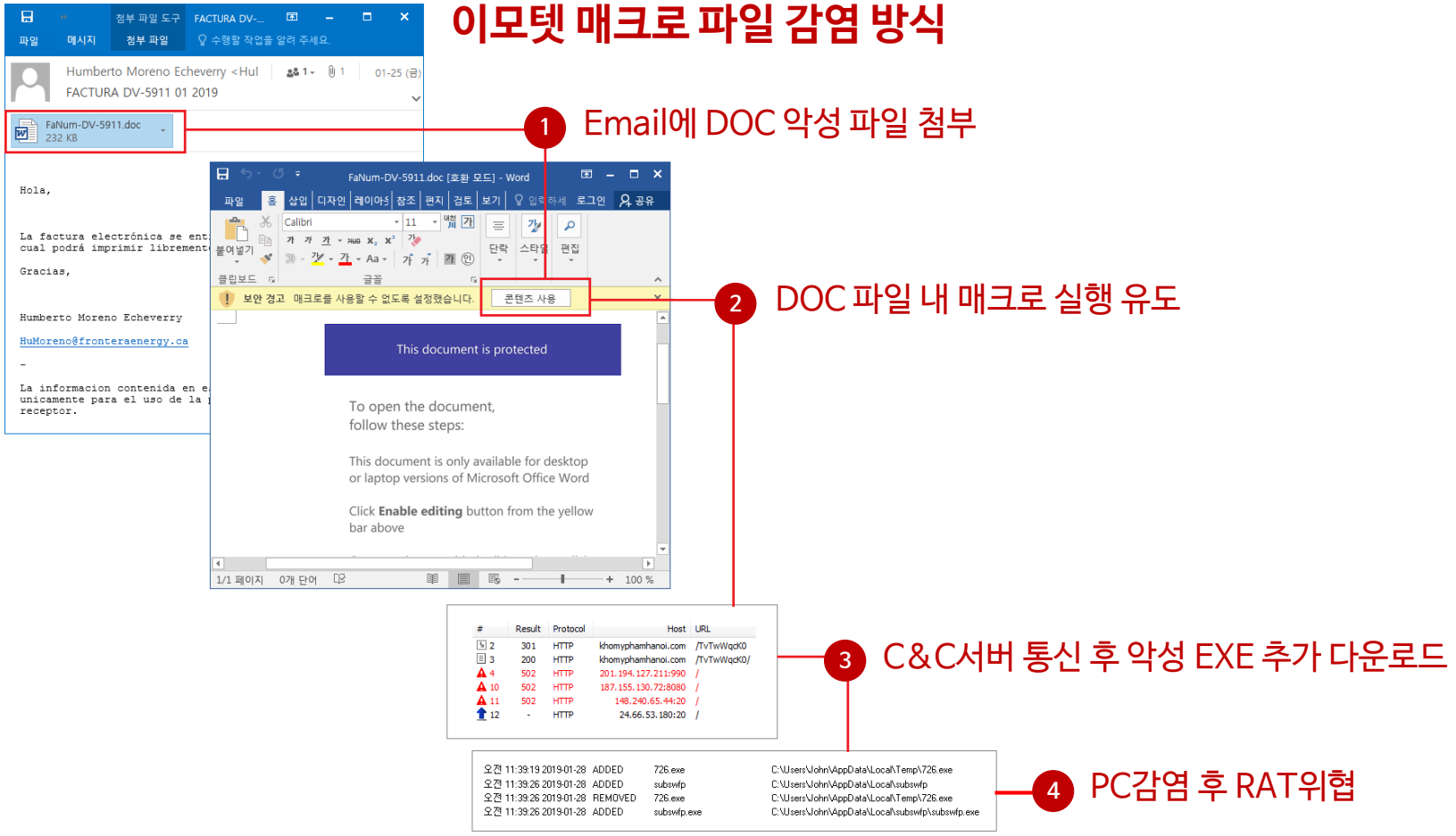
05

# 위협 탐지 / 대응 시나리오

# 위협 탐지 대응 시나리오

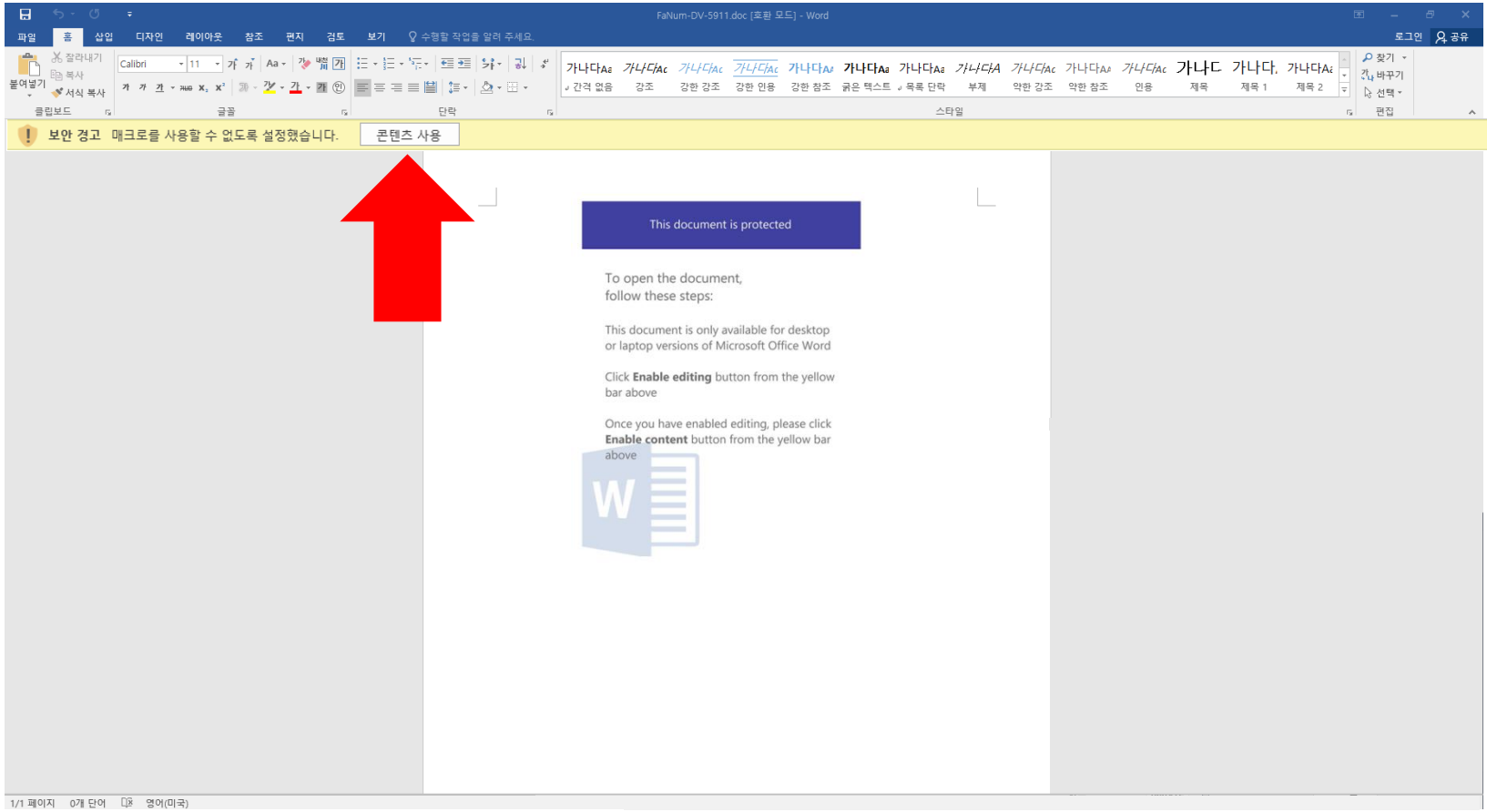
ESTsecurity

알약 EDR이 [매크로 실행]을 통해 배포된 Emotet악성코드를 차단하는 과정을 소개합니다.



# 위협 탐지 대응 시나리오

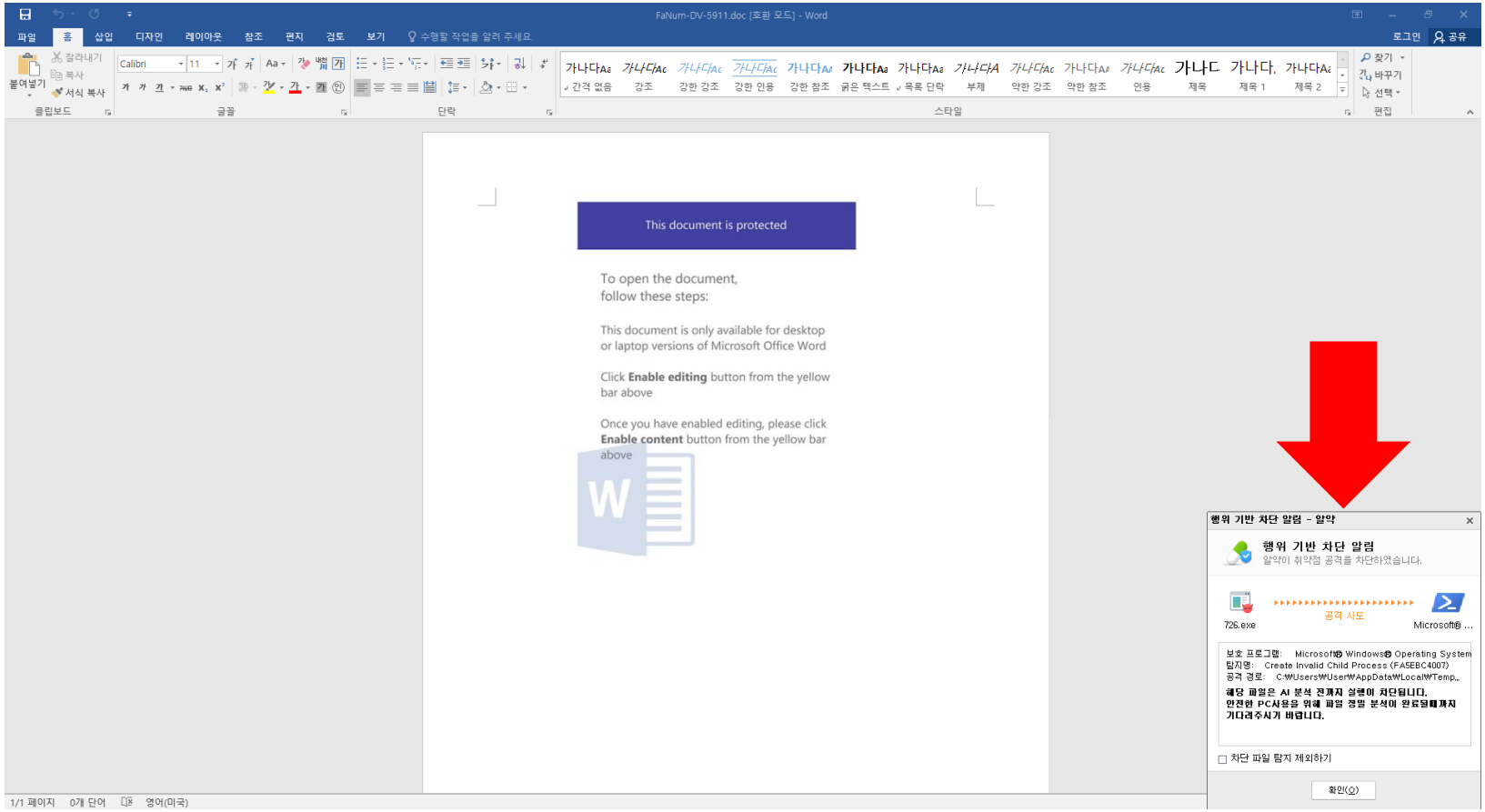
사용자가 메일에 첨부된 DOC 파일 다운로드 후 파일에 포함된 **매크로를 활성화**하면
파워쉘 명령이 실행되며 **악성파일이 다운로드**됩니다.



# 위협 탐지 대응 시나리오

ESTsecurity

알약 EDR은 파워쉘의 다운로드 동작을 의심 행위로 판단하고,
파워쉘이 다운로드한 악성 파일의 **실행을 차단**합니다.



# 위협 탐지 대응 시나리오

실행이 차단된 악성파일은 Threat Inside로 전송되어 정밀 분석됩니다.

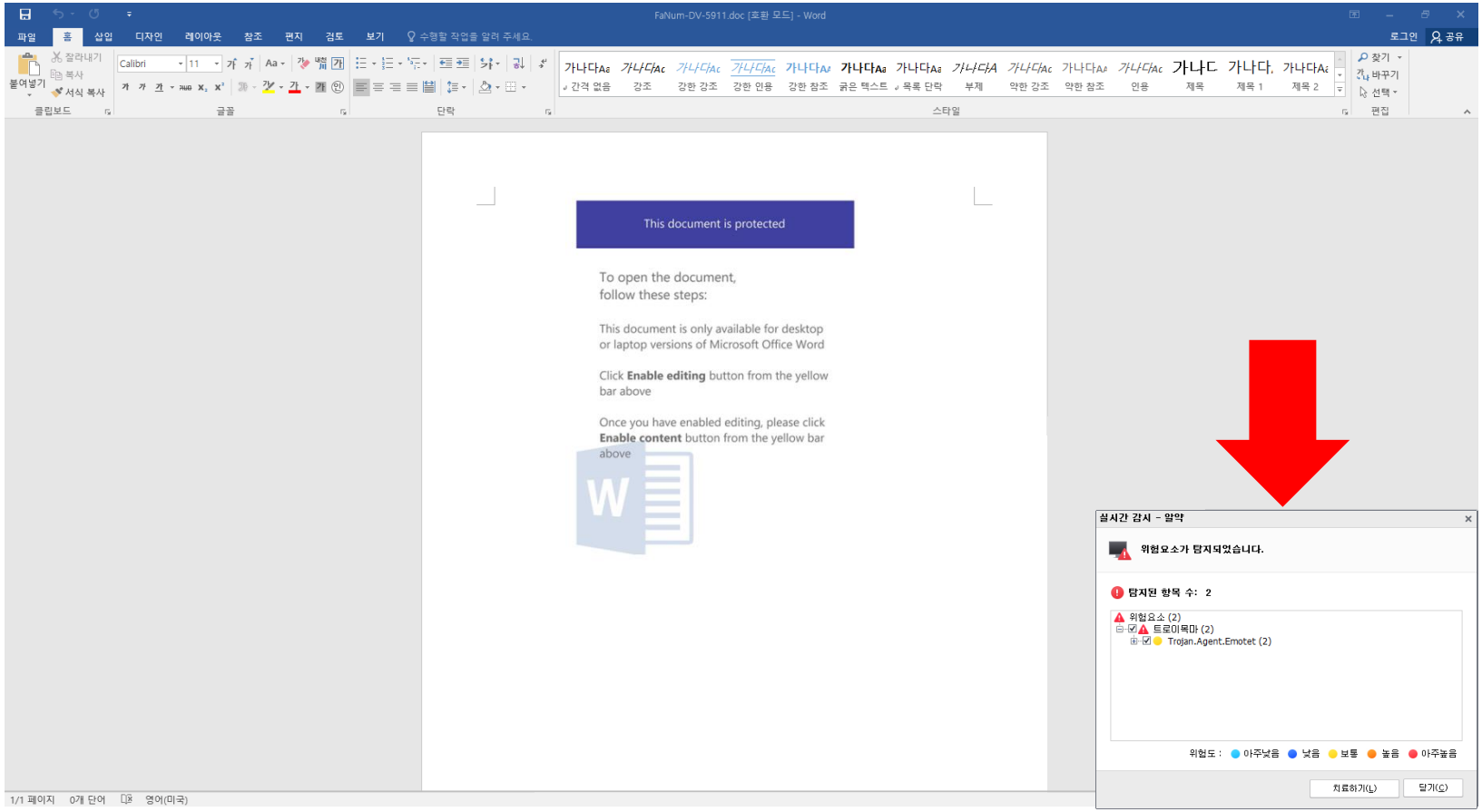

**탐지에 따른 대응 프로세스**

| 탐지 방식 | 탐지 대상 | 위협 레벨 | 행위 / 로그 종류 | ALYac EDR | Threat Inside |
|---|---|---|---|---|---|
| 시그니쳐 | Known | 악성 (Black List) | - | 차단 | 샘플 분석 리포트<br>연관 리포트 |
| | | 안전 (White List) | - | - | - |
| 행위 / 로그 기반 | UnKnown | 악성 | 확실한 악성 행위<br>(Exploit, 랜섬웨어 동작 등) | 차단 | 샘플 분석 리포트<br>연관 리포트 |
| | | 의심 | 의심스러운 행위<br>(MBR변조, 파일드랍 등) | 실행지연 -> 차단 / 허용<br>(상세 분석 결과에 따라) | 샘플 분석 리포트<br>연관 리포트 |
| | | 주의 | 일반적이지 않은 행위<br>(호스트 변조, 매체접근, 쉘스크립트 등) | 차단 / 허용<br>(관리자 정책에 따라) | 샘플 분석 리포트<br>연관 리포트 |

# 위협 탐지 대응 시나리오

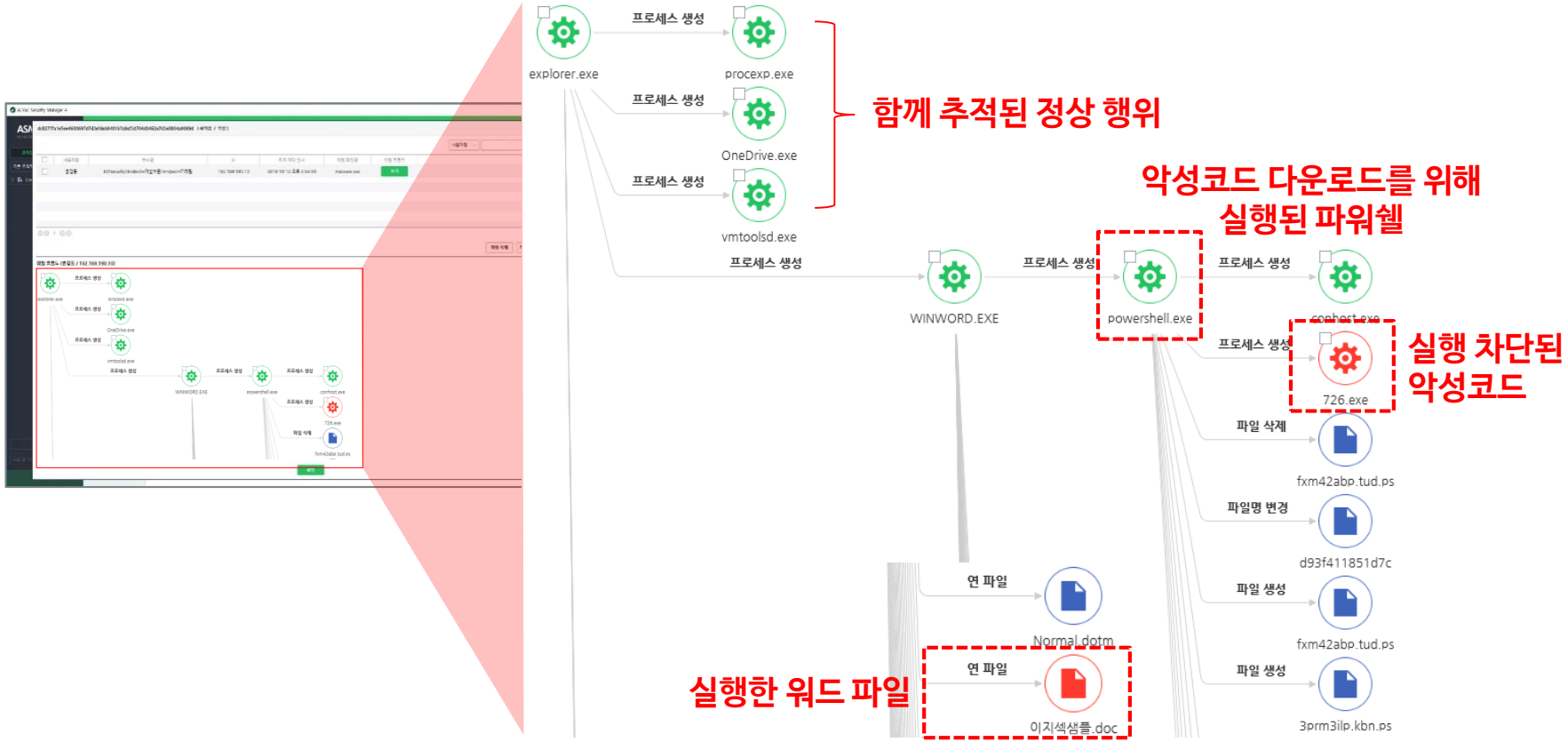
ESTsecurity

분석 결과는 알약 AIS엔진에 반영되어
알약 EDR이 악성파일을 **실시간으로 탐지하고 치료합니다.**



# 위협 탐지 대응 시나리오

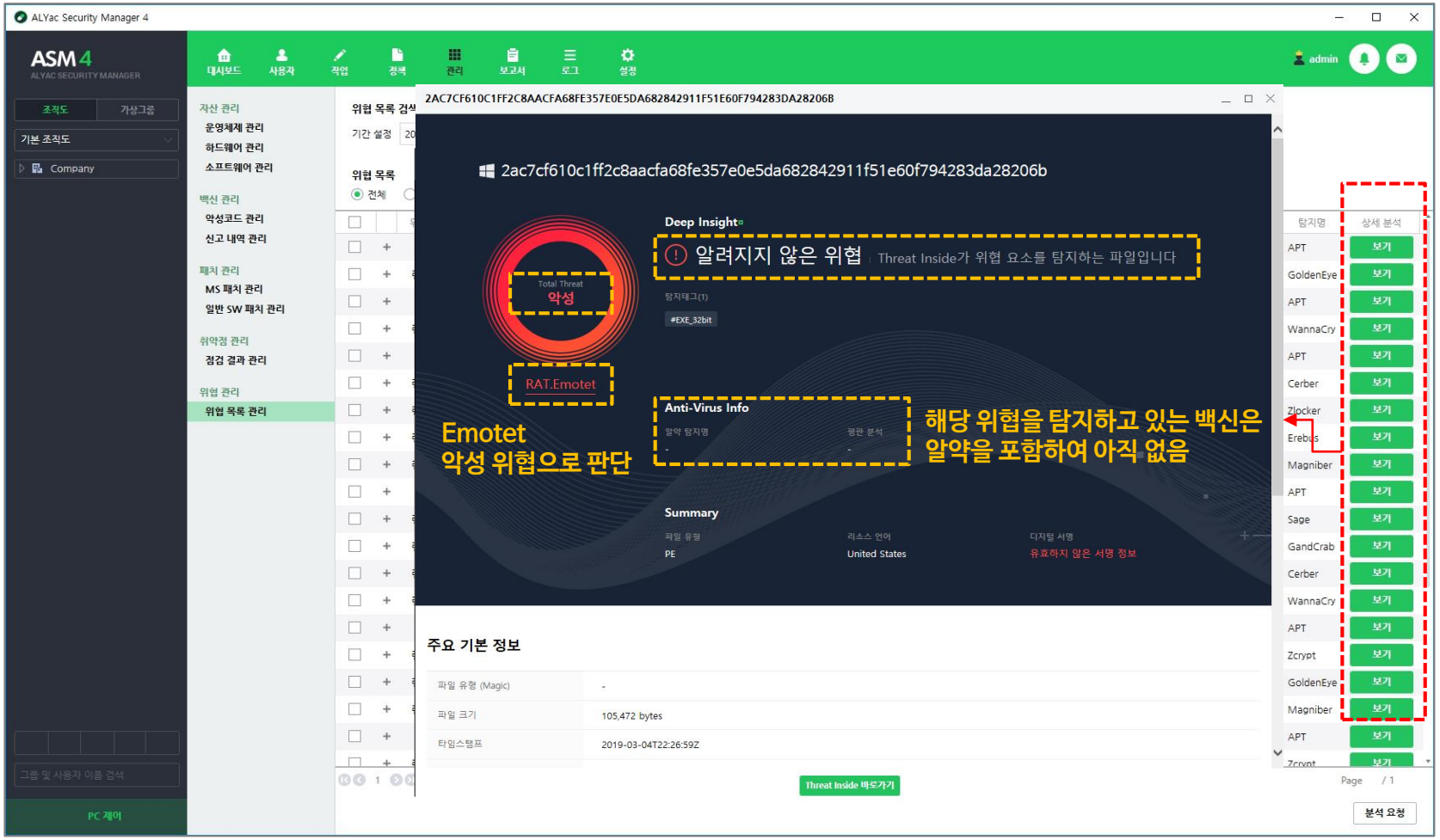
관리 콘솔인 ASM에서 차단된 악성파일의 **위협 흐름도**를 확인할 수 있으며,
프로세스 종료, 네트워크 차단 명령 등의 **대응 명령**을 내릴 수 있습니다.



# 위협 탐지 대응 시나리오

ESTsecurity

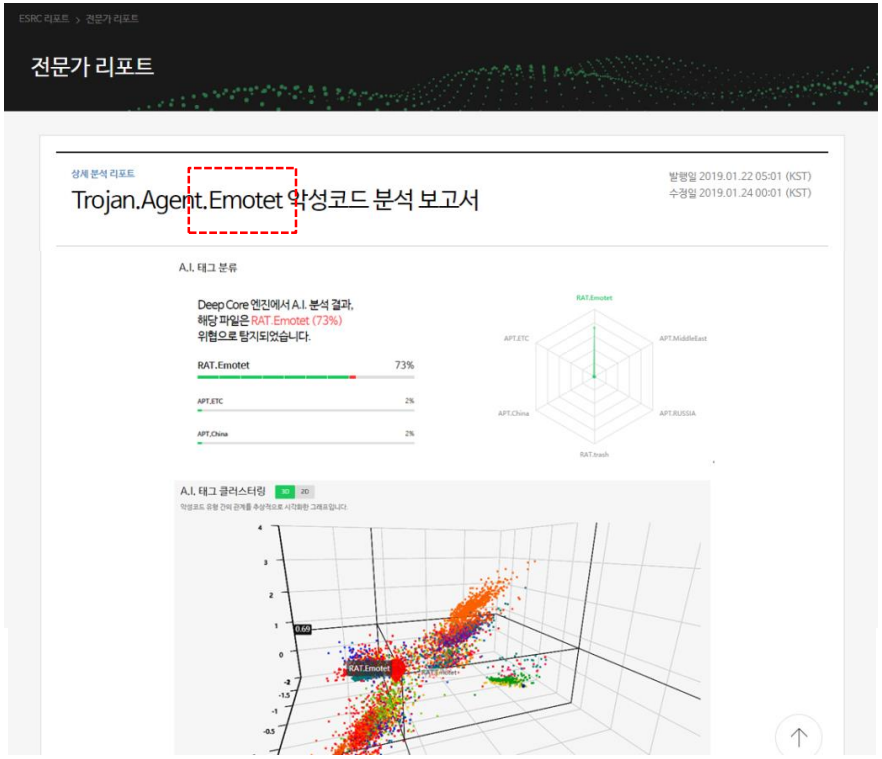
차단된 의심 파일에 대한 Threat Inside 분석 결과를 확인할 수 있습니다.

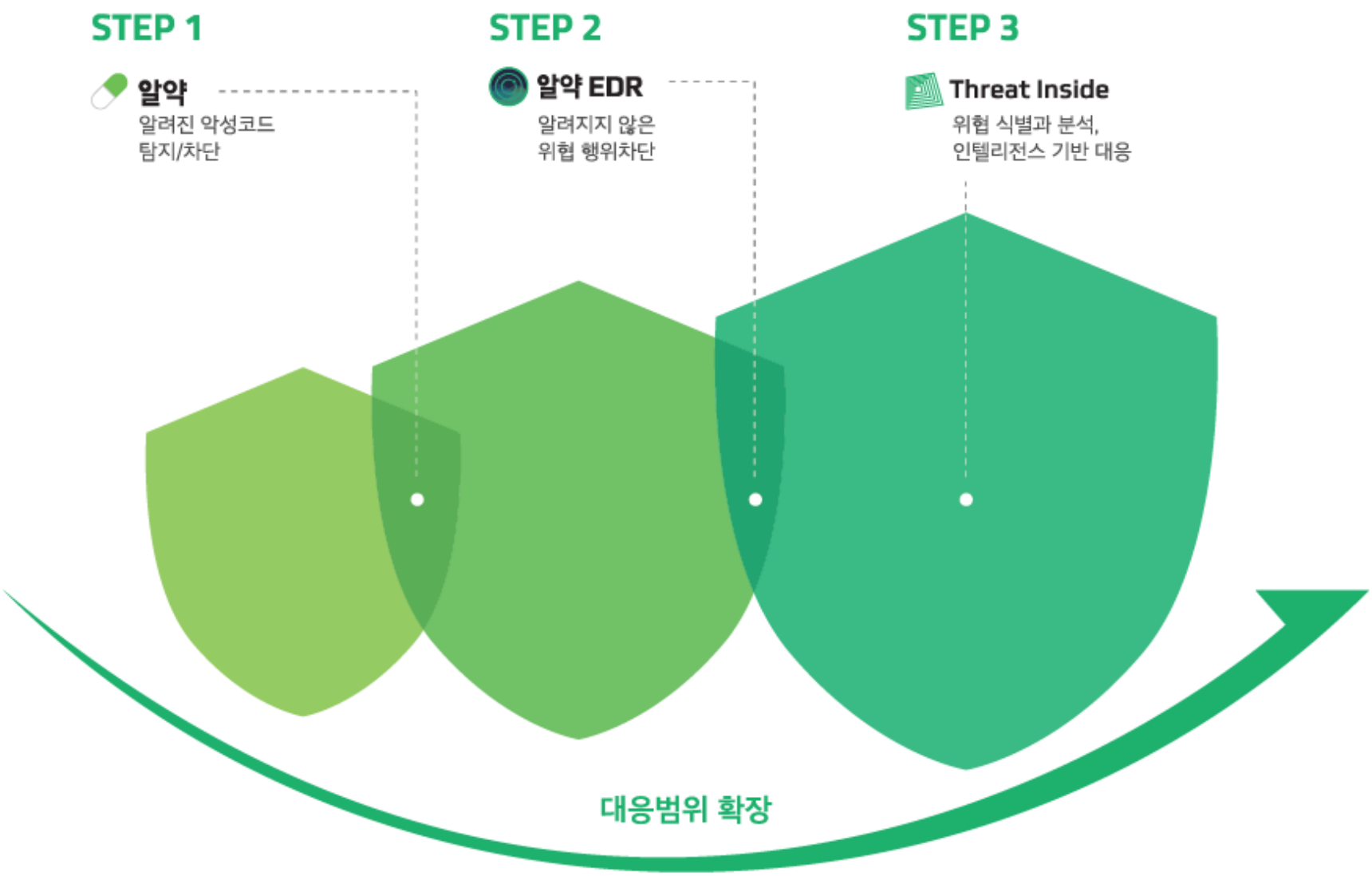


# 위협 탐지 대응 시나리오

ESTsecurity

Threat Inside 사이트를 통해 **악성코드 심층 분석 결과**와
대응 방법이 포함된 **분석 리포트**를 확인할 수 있습니다.





STEP 1
알약
알려진 악성코드
탐지/차단
STEP 2
알약 EDR
알려지지 않은
위협 행위차단
STEP 3
Threat Inside
위협 식별과 분석,
인텔리전스 기반 대응
대응범위 확장

ESTsecurity
Make World More Secure with A.I.

# 감사합니다.