지능형 보안 위협에 대한 트랜드 및 종합적인 대응 방안

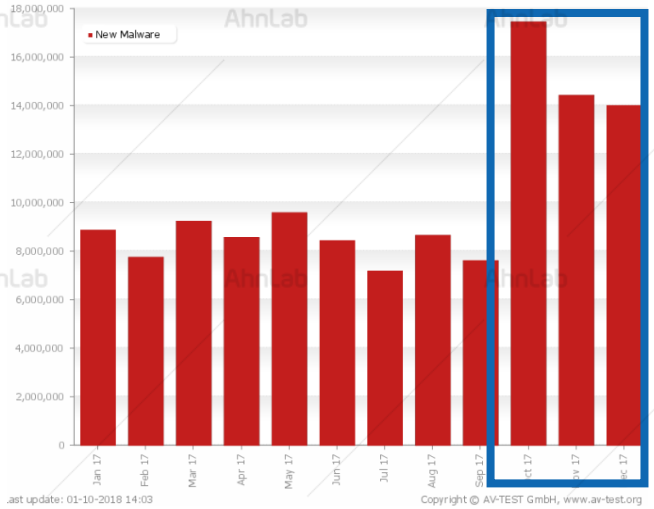
NES 2018’ 차세대 기업보안 세미나&전시회

제품기획팀 **백 민 경 부장 / Product Evangelist**

AhnLab

숫자로 보는 악성코드 동향

AhnLab



33만

2017년 하루 평균 New Malware

2017년 4분기에 발견된 Malware

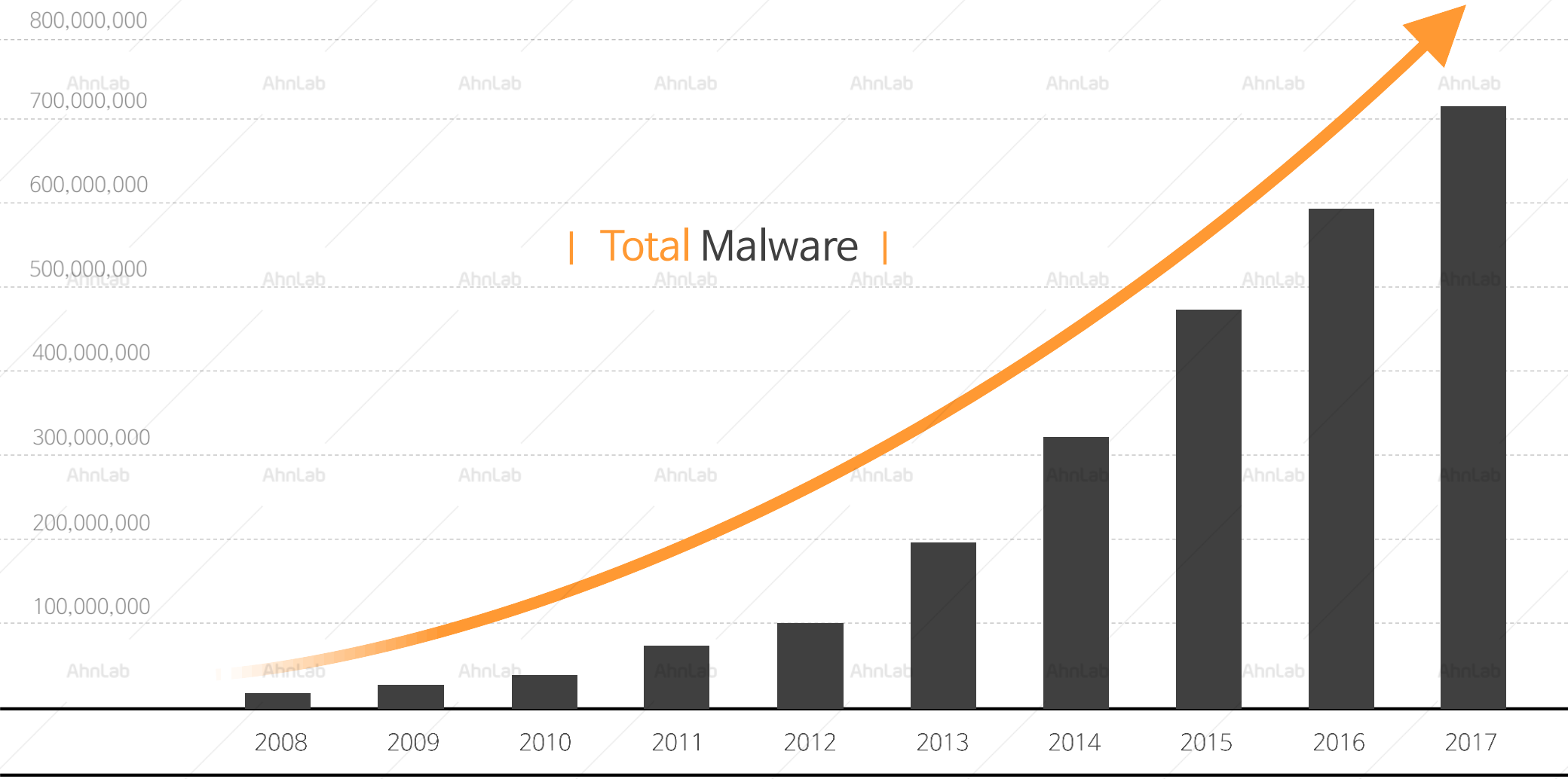
4,500만

2009년 발견된 Total Malware

※ 출처: AV-TEST GmbH, www.av-test.org

최근 10년 동안 전체 악성코드 추이

AhnLab



Last update: 01-10-2018 14:03

※ 출처: AV-TEST GmbH, www.av-test.org

악성코드 전파경로

AhnLab

Endpoint 시스템을 노리는 **다양한 악성코드**

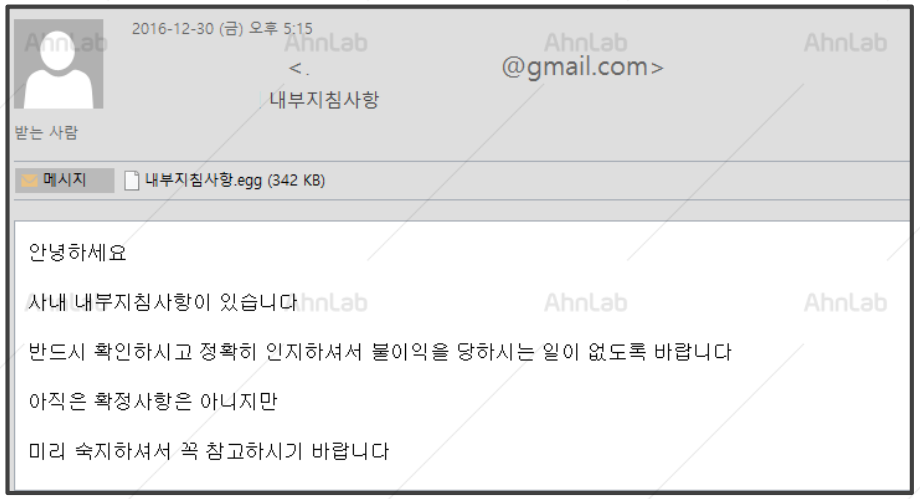
- Zero-Day 공격
- 사회공학기법
- 표적공격
- O/S, S/W 취약점

다양한 경로를 통한 **악성코드 감염 및 정보유출**

- USB
- 인터넷
- Bluetooth
- Wifi
- Print / FAX

사회공학기법

AhnLab


2016-12-30 (금) 오후 5:15
<. @gmail.com>
내부지침사항
받는 사람
메시지 내부지침사항.egg (342 KB)

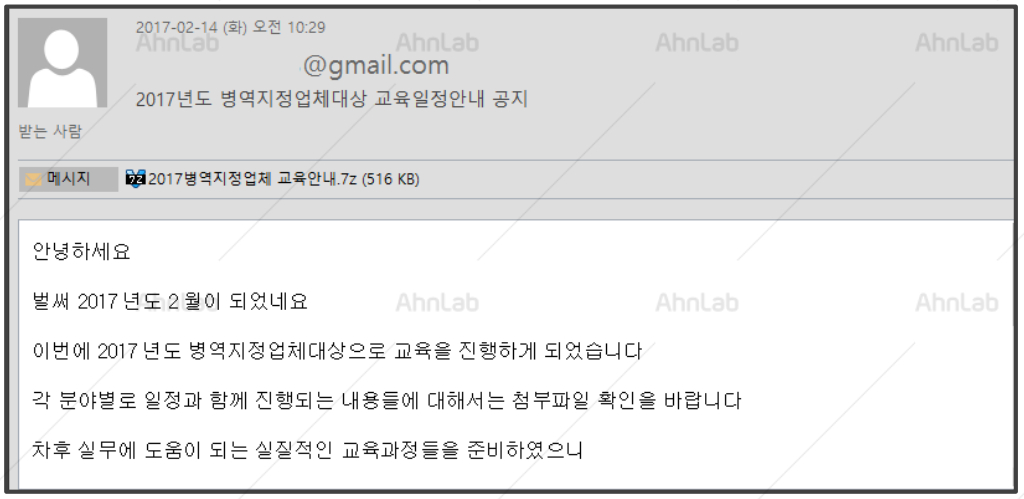
안녕하세요

사내 내부지침사항이 있습니다

반드시 확인하시고 정확히 인지하셔서 불이익을 당하시는 일이 없도록 바랍니다

아직은 확정사항은 아니지만

미리 숙지하셔서 꼭 참고하시기 바랍니다


2017-02-14 (화) 오전 10:29
@gmail.com
2017년도 병역지정업체대상 교육일정안내 공지
받는 사람
메시지 2017병역지정업체 교육안내.7z (516 KB)

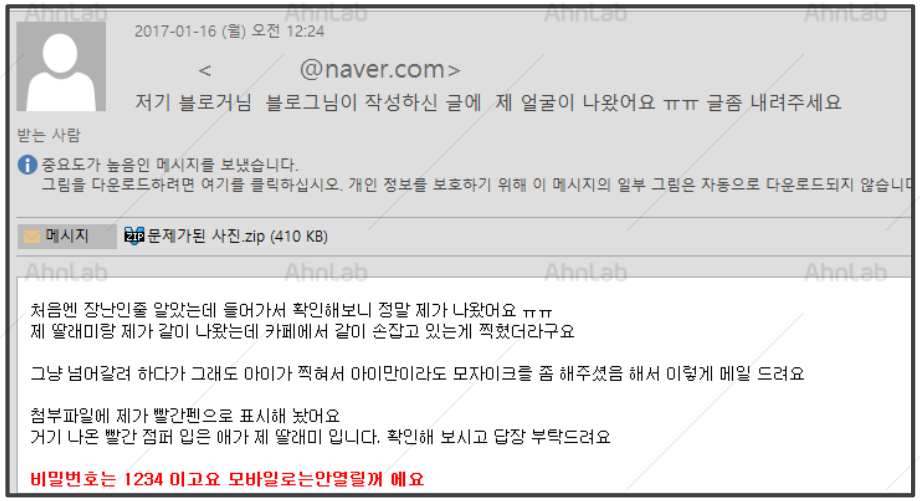
안녕하세요

벌써 2017 년도 2 월이 되었네요

이번에 2017 년도 병역지정업체대상으로 교육을 진행하게 되었습니다

각 분야별로 일정과 함께 진행되는 내용들에 대해서는 첨부파일 확인을 바랍니다

차후 실무에 도움이 되는 실질적인 교육과정들을 준비하였으니

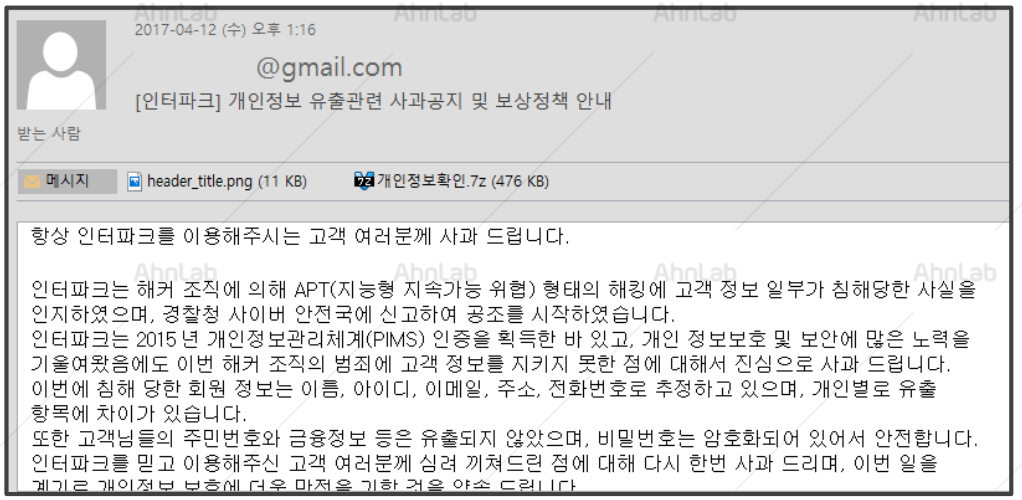

2017-01-16 (월) 오전 12:24
< @naver.com>
저기 블로거님 블로그님이 작성하신 글에 제 얼굴이 나왔어요 ㅠㅠ 글좀 내려주세요
받는 사람
중요도가 높음인 메시지를 보냈습니다.
그림을 다운로드하려면 여기를 클릭하십시오. 개인 정보를 보호하기 위해 이 메시지의 일부 그림은 자동으로 다운로드되지 않습니다
메시지 문제가된 사진.zip (410 KB)

처음엔 장난인줄 알았는데 들어가서 확인해보니 정말 제가 나왔어요 ㅠㅠ
제 딸래미랑 제가 같이 나왔는데 카페에서 같이 손잡고 있는게 찍혔더라구요

그냥 넘어갈려 하다가 그래도 아이가 찍혀서 아이만이라도 모자이크를 좀 해주셨음 해서 이렇게 메일 드려요

첨부파일에 제가 빨간펜으로 표시해 놨어요
거기 나온 빨간 점퍼 입은 애가 제 딸래미 입니다. 확인해 보시고 답장 부탁드려요

비밀번호는 1234 이고요 모바일로는안열릴꺼 에요

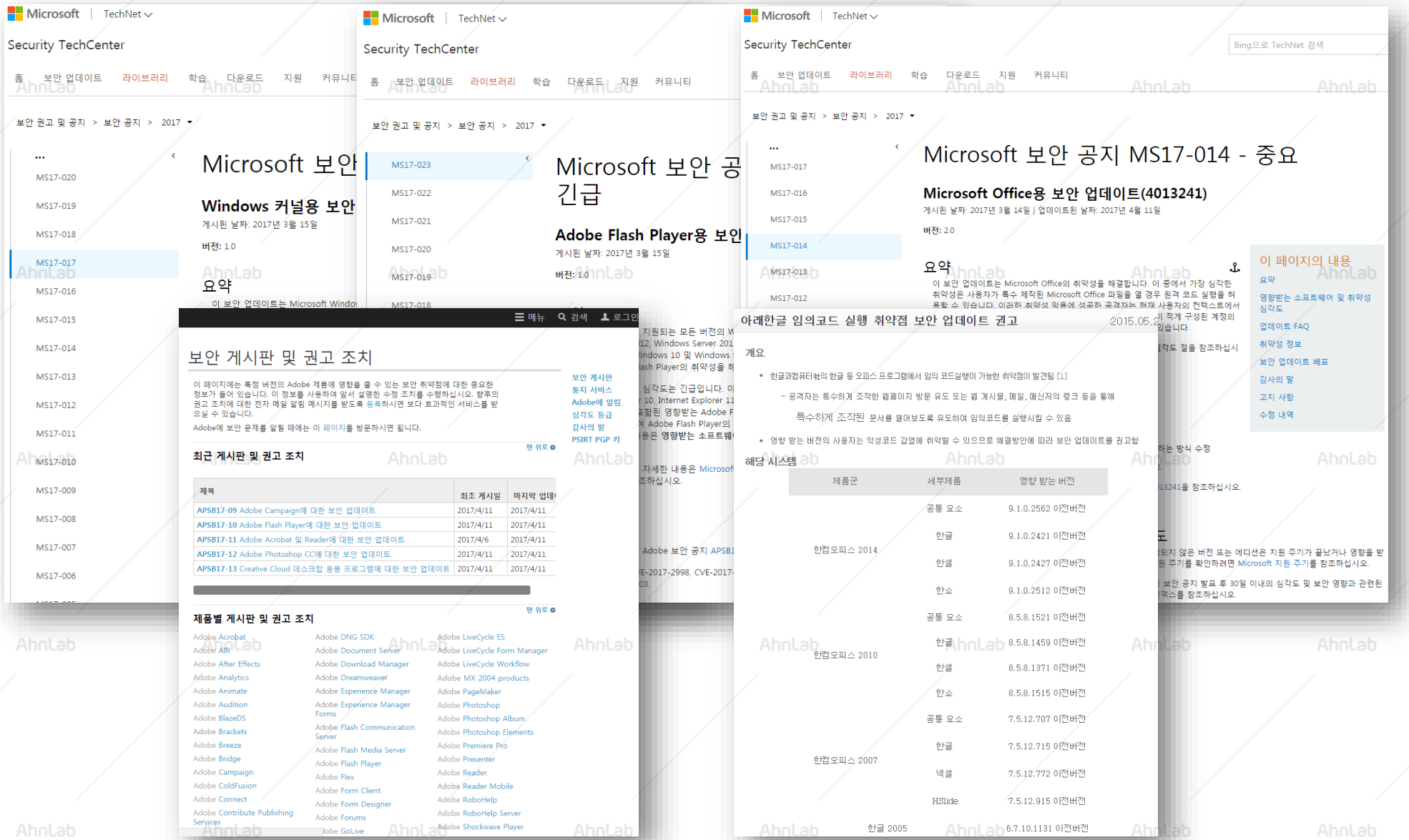

2017-04-12 (수) 오후 1:16
@gmail.com
[인터파크] 개인정보 유출관련 사과공지 및 보상정책 안내
받는 사람
메시지 header_title.png (11 KB) 개인정보확인.7z (476 KB)

항상 인터파크를 이용해주시는 고객 여러분께 사과 드립니다.

인터파크는 해커 조직에 의해 APT(지능형 지속가능 위협) 형태의 해킹에 고객 정보 일부가 침해당한 사실을 인지하였으며, 경찰청 사이버 안전국에 신고하여 공조를 시작하였습니다.
인터파크는 2015 년 개인정보관리체계(PIMS) 인증을 획득한 바 있고, 개인 정보보호 및 보안에 많은 노력을 기울여왔음에도 이번 해커 조직의 범죄에 고객 정보를 지키지 못한 점에 대해서 진심으로 사과 드립니다.
이번에 침해 당한 회원 정보는 이름, 아이디, 이메일, 주소, 전화번호로 추정하고 있으며, 개인별로 유출 항목에 차이가 있습니다.
또한 고객님들의 주민번호와 금융정보 등은 유출되지 않았으며, 비밀번호는 암호화되어 있어서 안전합니다.
인터파크를 믿고 이용해주신 고객 여러분께 심려 끼쳐드린 점에 대해 다시 한번 사과 드리며, 이번 일을 계기로 개인정보 보호에 더욱 만전을 기할 것을 약속 드립니다.

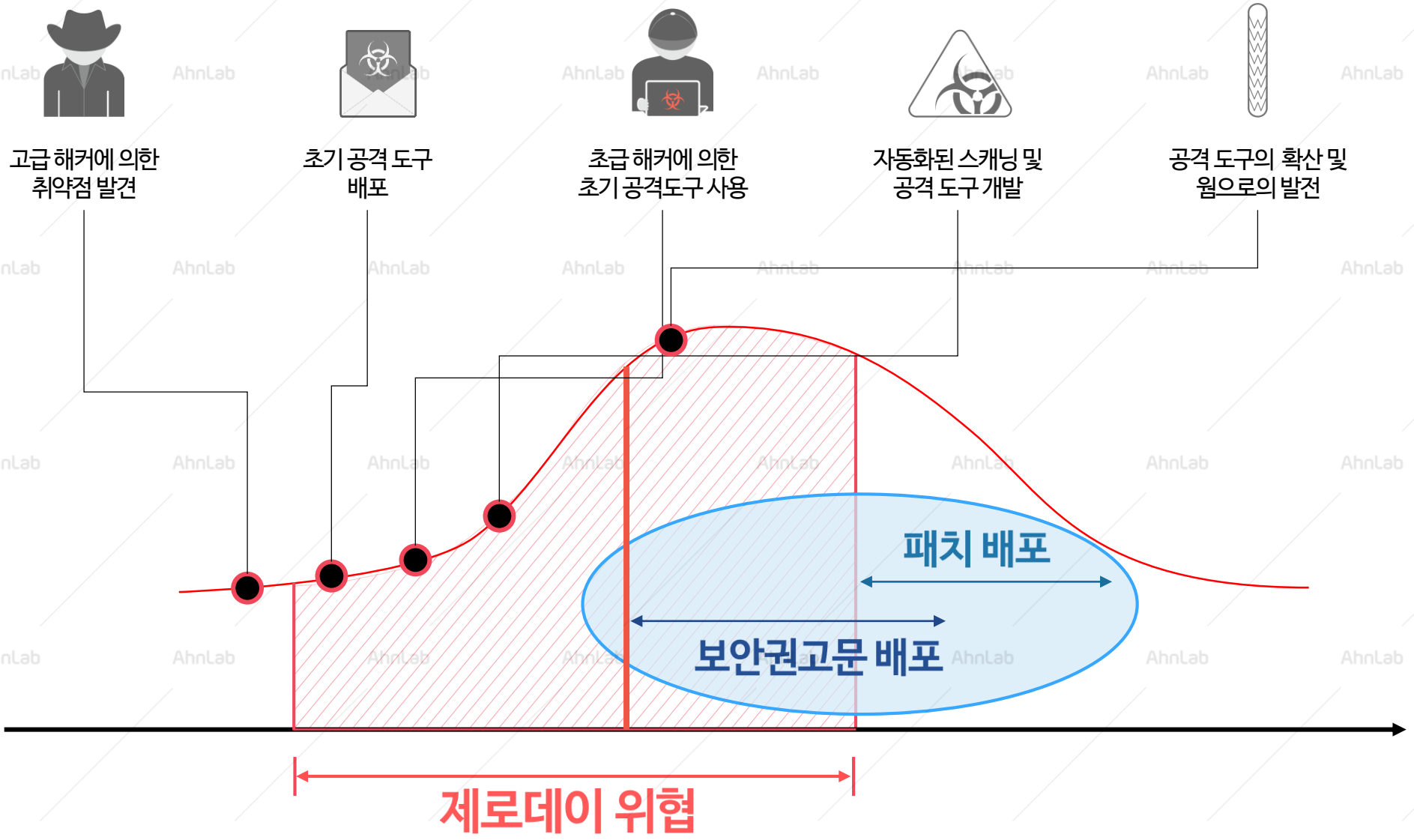
운영체제 및 응용프로그램 취약점

AhnLab



Zero-Day 공격 라이프사이클

AhnLab



보안회사 R&D 관점에서 대응

AhnLab

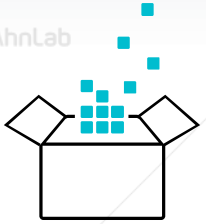
Spyware
시스템설정
2004

Trojan
변종 대량 확산
2007

Rootkit
탐지회피
2009

APT
은밀성 (Stuxnet)
2011

PUP
동의 후 탐지 필요
2010



7.7 DDoS / Phishing / Pharming
IT 확대 기반 활동
2009

Online game Hack
AV Killer / AV 대응
2012

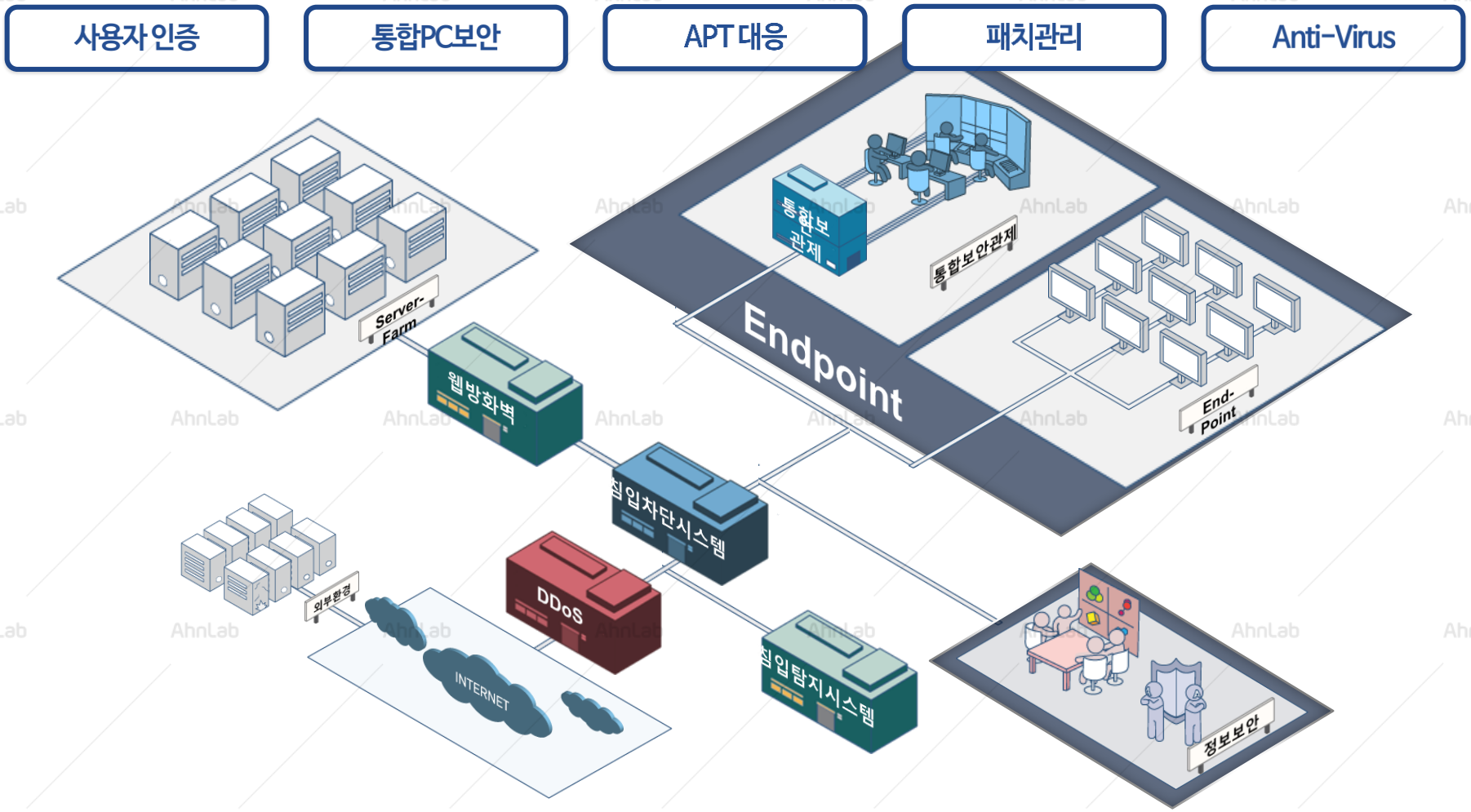
Mobile Malware
플랫폼 확장
2014

Ransomware
복구한계
2015~2017

기업 관점의 보안사고 대응

AhnLab

네트워크 보안 제품 중심의 이벤트(로그)를 통합보안관제 시스템을 이용하여 관제



그럼에도 왜 계속 피해는 발생하는가?

AhnLab

2009 7·7 DDoS

2011 3·4 DDoS

2011 금융기관 해킹 사고

2011 포털 개인정보 유출

2012 언론 해킹사고

보이지 않는 신종 악성코드가 침해사고에 핵심적인 역할 수행

- 특정 대상에 대한 표적 공격
- 최신 보안 솔루션을 구축·운영 중인 기업/기관도 해킹 발생
- 개인정보 / 내부정보 유출, 전산망 마비 등의 치명적인 유·무형 피해 발생

2016 인터넷쇼핑몰 개인정보 유출

2015 랜섬웨어

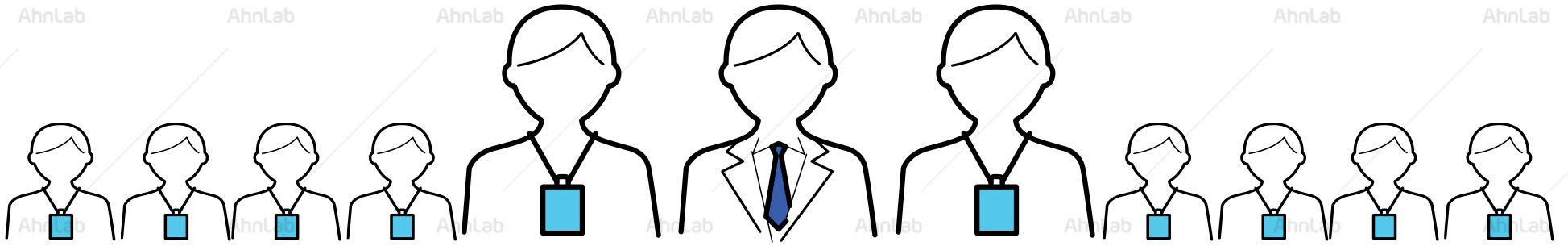
2014 기관 내부정보 유출

2013 3·20 전산망 마비

무엇이 부족할까?

AhnLab

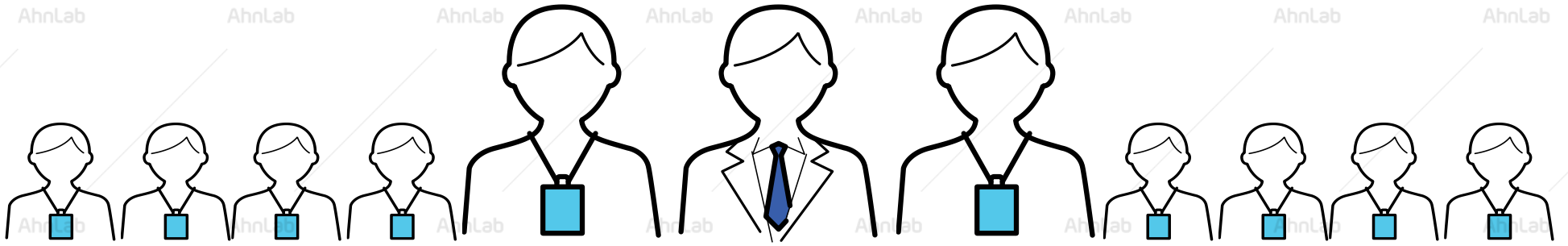
1. 엔드포인트 보안 영역별 대응 솔루션 부족
2. 보안정책 내재화 부족
3. 능동적 위협 대응방안 부족



어떻게 해야할까?

AhnLab

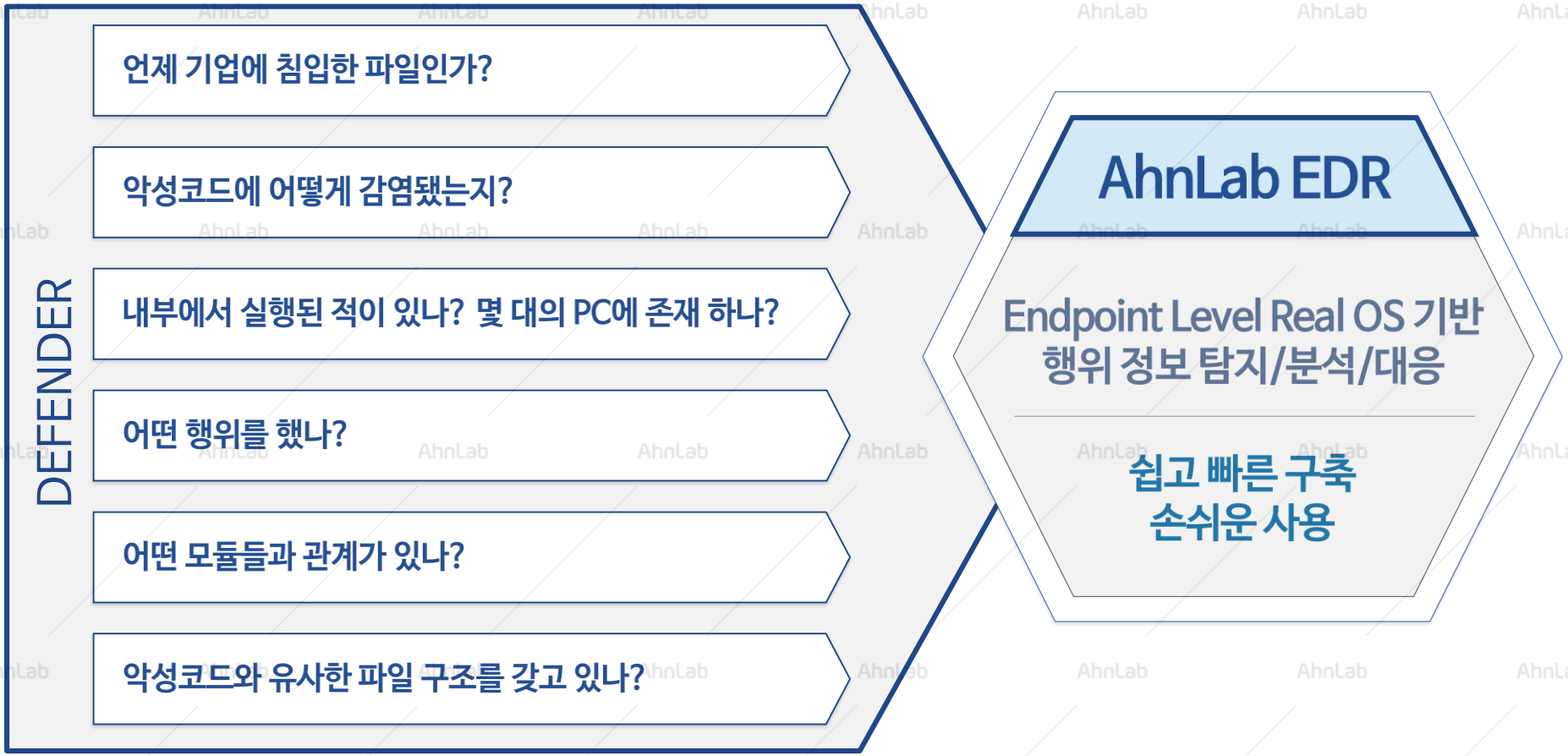
1. Endpoint Hardening을 통한 공격표면 최소화
2. 임직원 모두 자기주도 보안 실행
3. 보안 담당자의 능동적·적극적 위협 방어



AhnLab EDR: 위협 가시성 확보/대응

AhnLab

고도화되는 신 • 변종 위협에 의한 침해사고 대응력을 강화하고 잠재적인 위협을 최소화하기 위한 보완책으로
엔드포인트단에서의 위협 정보 수집 • 분석 • 대응 관점의 EDR이 주목받고 있습니다.



※EDR(Endpoint Detection & Response)이란?

엔드포인트단에서 지속적인 모니터링 및 대응을 제공하는 보안 솔루션으로, 엔드포인트단에서의 위협의 탐지, 통제, 분석, 치료 등의 기능을 제공한다.
엔드포인트 보안을 위한 보조적인 툴(tool)로서, 안티바이러스 등 기존 보안 솔루션과의 연계를 통해 더욱 효과를 발휘한다.

*출처: Gartner

AhnLab EDR

AhnLab

AhnLab EDR(Endpoint Detection & Response)은 엔드포인트 영역에 대한 지속적인 모니터링을 통해 위협 탐지 및 분석, 대응을 제공하는 엔드포인트 위협 탐지 및 대응 솔루션입니다.

- 국내 최초의 행위 기반 분석 엔진을 통한 위협 행위 분석 및 모니터링
- 엔드포인트 가시성 기반의 진일보한 위협 탐지 및 대응
- 최고의 엔드포인트 보안 및 악성코드 분석 전문 기업의 기술력이 응집된 EDR

행위 정보 탐지·분석을 통한
엔드포인트 가시성 확보 및 대응

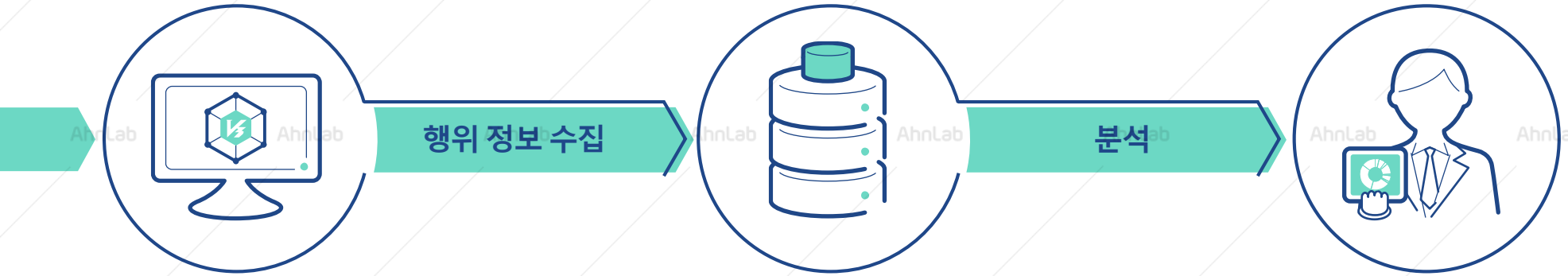
AhnLab EDR

간편한 구축, 손쉬운 운영,
더 강력한 위협 대응

AhnLab EDR: 엔드포인트 행위 정보 수집을 통한 위협 가시성 강화

AhnLab

AhnLab EDR은 안랩의 독자적인 행위 기반 엔진인 MDP 엔진을 통해
엔드포인트의 모든 행위 정보를 수집, 저장하고 탐지된 위협에 대한 유입 경로를 추적, 분석함으로써 기업 및 기관의 위협 가시성을 강화합니다.



Threat Hunting

- 특정 이벤트 중심이 아닌 전체적, 연속적인 행위 정보 수집 및 저장
- 필요 시 언제든지 위협 및 관련 정보 확인 가능 - 사후 위협 분석 가능

Centralization

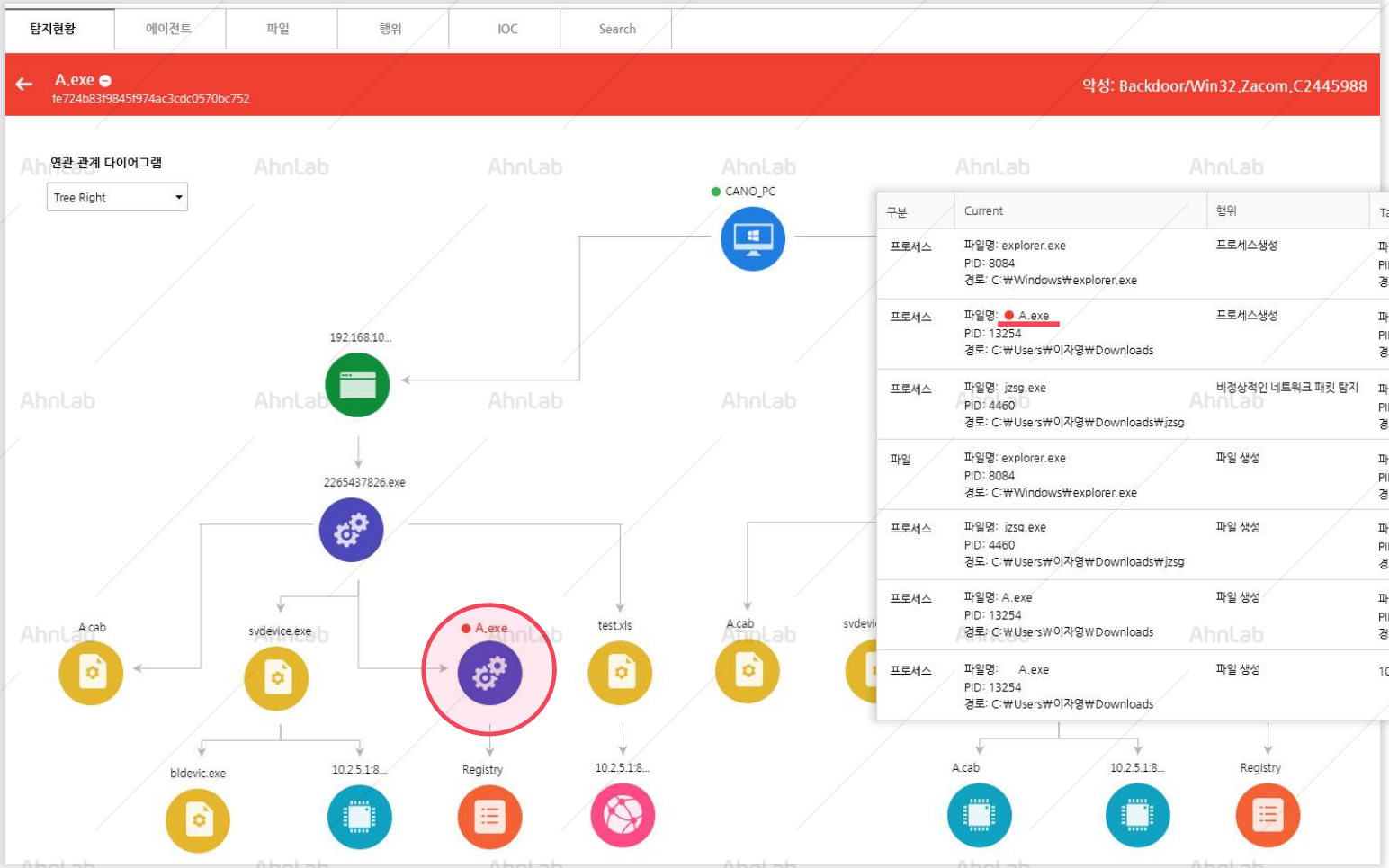
- 중앙화된 로그 저장 및 관리 - 모든 엔드포인트 로그를 중앙 서버에 저장
- 로그 관리 및 분석 편의성 향상

AhnLab EDR 주요기능 : 위협 가시성

AhnLab

위협 이벤트/ 공격 흐름도 Visibility 제공

위협에 대해 상세한 '공격 흐름도' 제공
위협의 종류, 행위 및 공격 단계에 따라 적절한 대응 및 조치가 가능
AhnLab Family 제품 사용시 연계 정책을 통한 다양한 대응정책 수립 가능



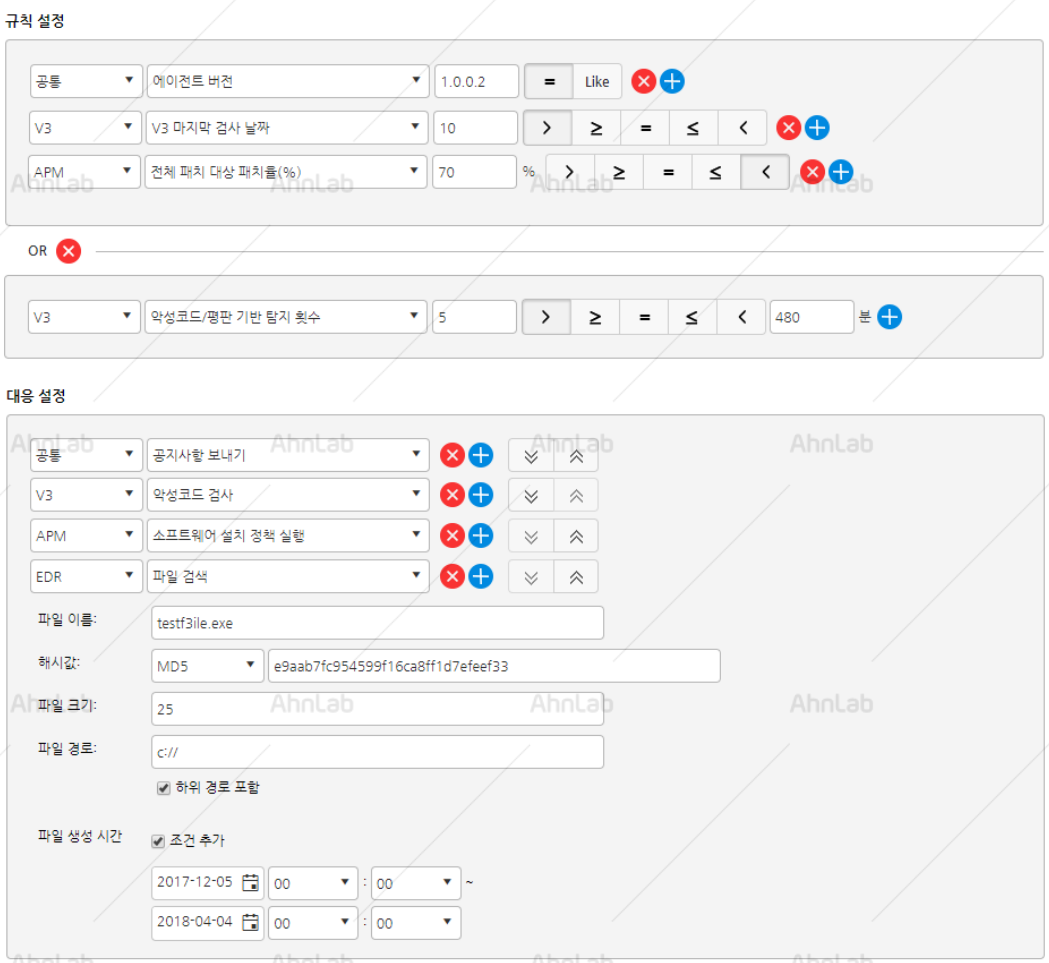
구분	Current	행위	Target	탐지 시각
프로세스	파일명: explorer.exe PID: 8084 경로: C:₩Windows₩explorer.exe	프로세스생성	파일명: A.exe PID: 13254 경로: C:₩Users₩이자영₩Downloads	2017-08-07 10:52:15
프로세스	파일명: A.exe PID: 13254 경로: C:₩Users₩이자영₩Downloads	프로세스생성	파일명: jzsg.exe PID: 4460 경로: C:₩Users₩이자영₩Downloads₩jzsg	2017-08-07 10:52:15
프로세스	파일명: jzsg.exe PID: 4460 경로: C:₩Users₩이자영₩Downloads₩jzsg	비정상적인 네트워크 패킷 탐지	파일명: explorer.exe PID: 8084 경로: C:₩Windows₩explorer.exe	2017-08-07 10:52:15
파일	파일명: explorer.exe PID: 8084 경로: C:₩Windows₩explorer.exe	파일 생성	파일명 : mizp PID : null 경로 : g:₩sample_5₩mizp	2017-08-07 10:52:15
프로세스	파일명: jzsg.exe PID: 4460 경로: C:₩Users₩이자영₩Downloads₩jzsg	파일 생성	파일명 : A.cab PID : null 경로 : g:₩sample_5₩mizp	2017-08-07 10:52:15
프로세스	파일명: A.exe PID: 13254 경로: C:₩Users₩이자영₩Downloads	파일 생성	파일명: jzsg.exe PID: 4460 경로: C:₩Users₩이자영₩Downloads₩jzsg	2017-08-07 10:52:15
프로세스	파일명: A.exe PID: 13254 경로: C:₩Users₩이자영₩Downloads	파일 생성	10.2.5.1:80	2017-08-07 10:52:15

AhnLab EDR 주요기능 : 대응

AhnLab

공격 흐름도 기반 에이전트 즉시 대응

공격흐름도를 통한 즉시 대응
프로세스, 에이전트, 파일 등에 대한 프로세스 종료/네트워크 차단 등

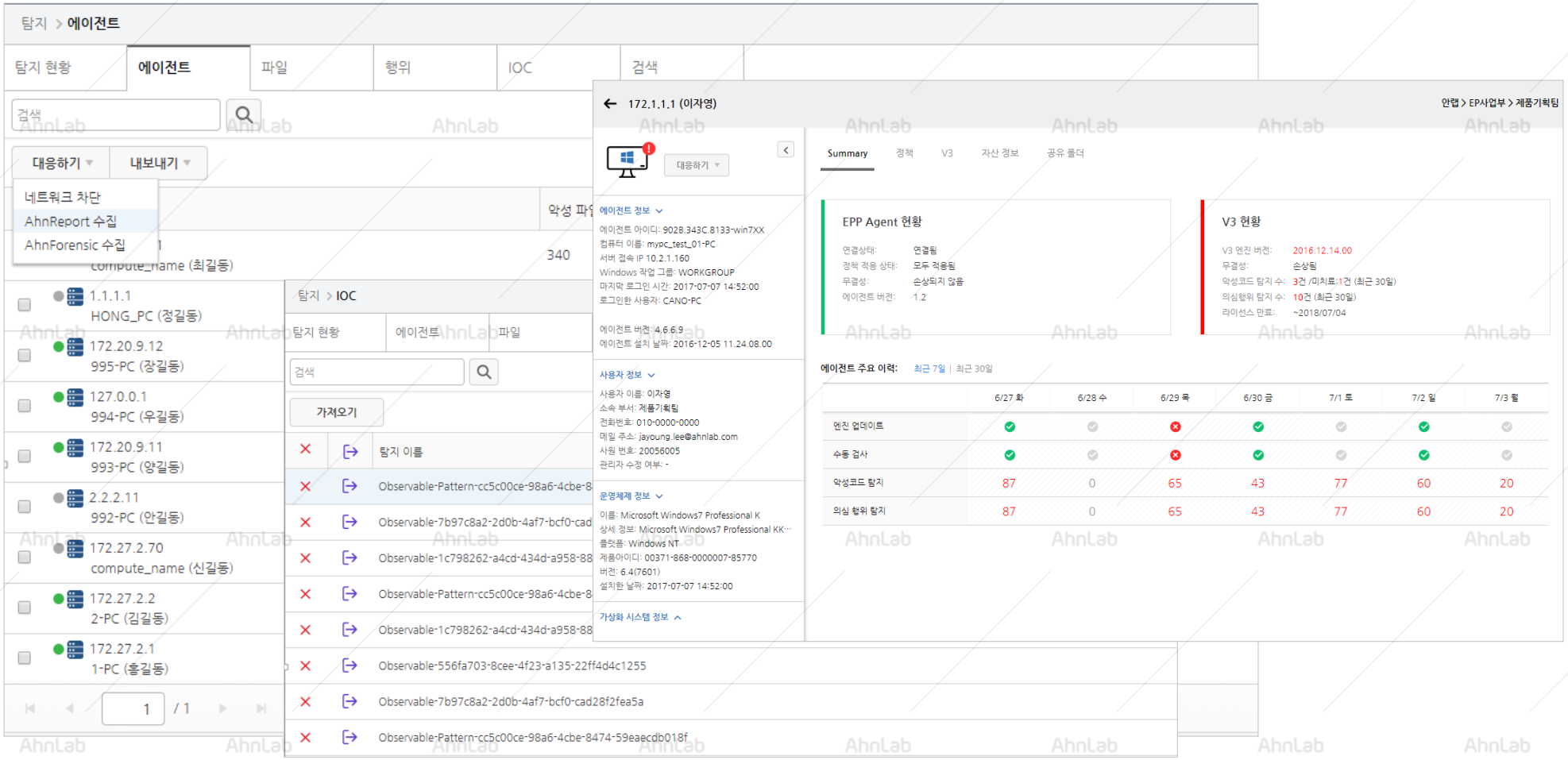


AhnLab EDR 주요기능 : 검색

AhnLab

에이전트,파일, 행위, IOC 등 검색/상세조회

에이전트, 파일, 행위 등 정보 단위로 검색, 조회, 검색결과 기준 대응 /정책 수립
IOC파일 import를 통한 검색 가능

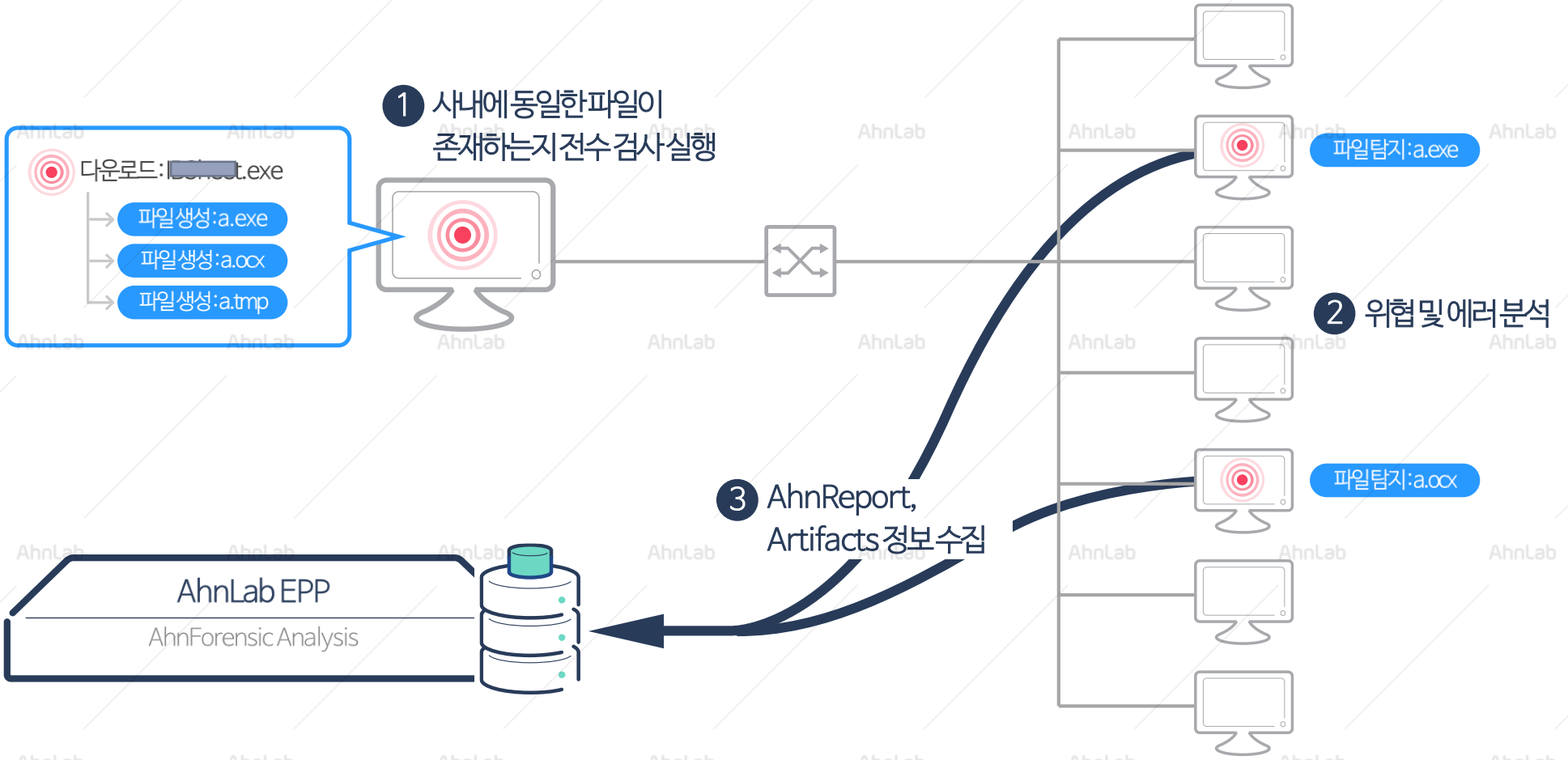


AhnLab EDR 주요기능 : 파일 수집/검사

AhnLab

파일 수집/검색

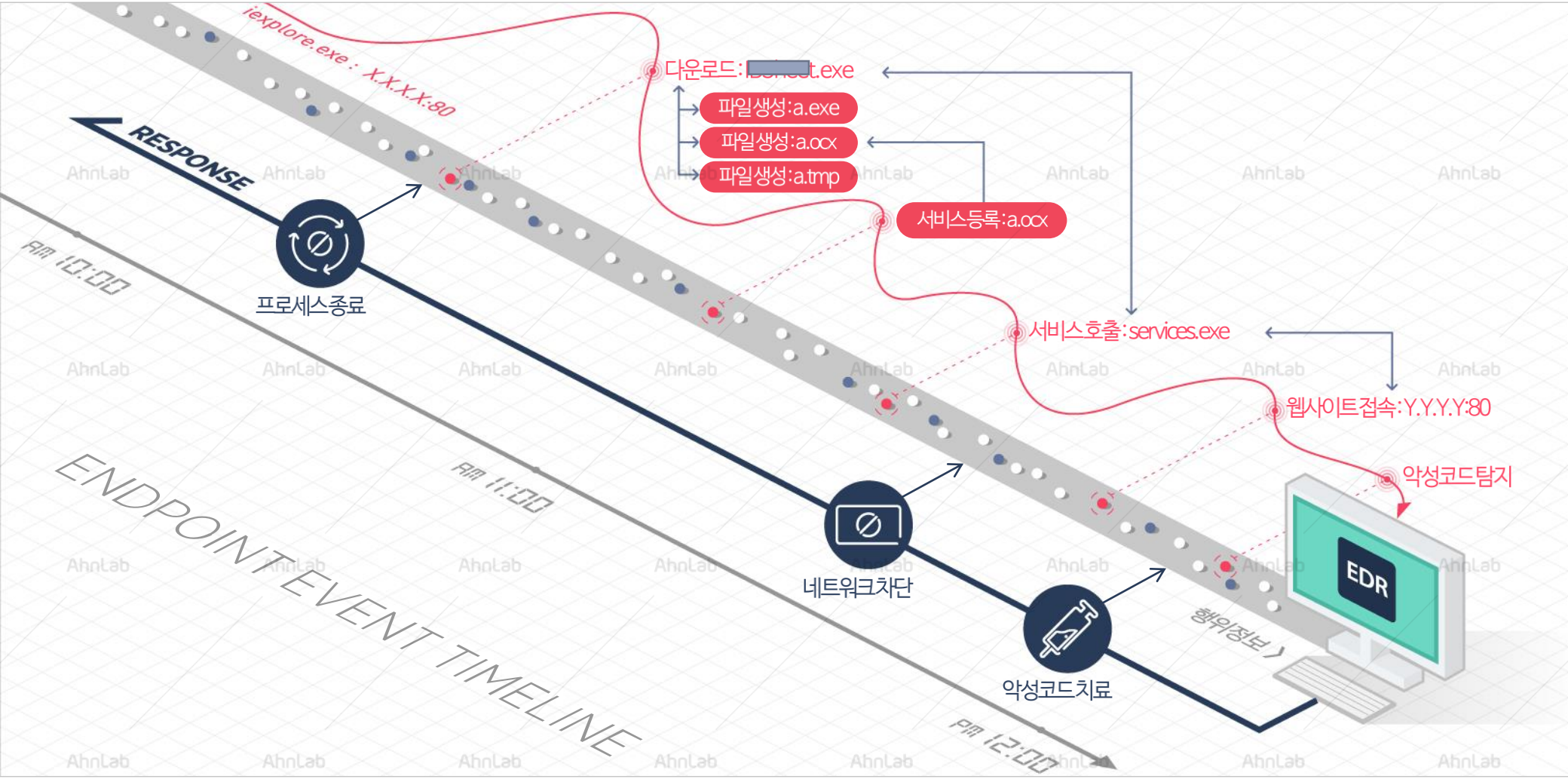
에이전트를 통한 실시간 파일 검색/ 수집 가능
수집된 파일에 대한 분석 후 대응정책 수립



특장점 - 가시성 기반의 강력한 위협 대응력

AhnLab

AhnLab EDR은 엔드포인트 레벨에서 실제 OS 기반의 행위 정보 탐지 및 분석, 위협 이벤트의 타임라인 분석을 통한 엔드포인트 위협 가시성을 제공해 기업 및 기관의 더 강력한 위협 대응력 확보에 기여합니다.



More security, More freedom

AhnLab