개인정보보호를 위한 엔드포인트 행위 분석과 연계 분석

안랩 **명재열 부장**

G-PRIVACY 2019
2019 공공기관 · 금융 · 기업 개인정보보호&정보보안 컨퍼런스
A Track, 4/10(수) 오후 1시 45분~2시 20분

AhnLab

Contents

AhnLab

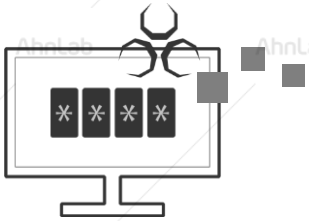
개인정보 유출

AhnLab

포털 및 SNS 접속

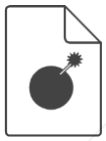
플래시플레이어
익스플로잇 발생

악성코드 동작



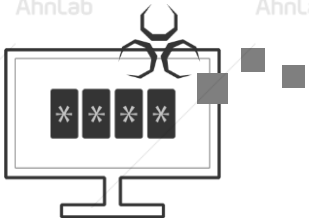
개인정보 유출

이메일 수신,
악성코드 다운로드



비실행형 첨부 문서 기반의
익스플로잇 발생

클라이언트 PC 잠복

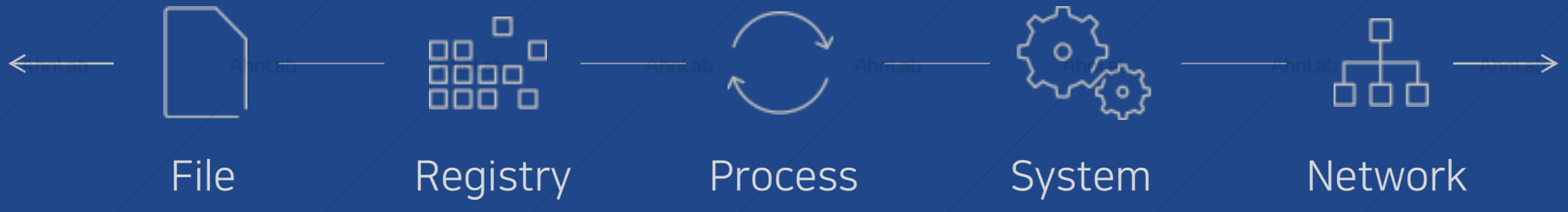


개인정보 유출

엔드포인트의 행위 정보 수집

AhnLab

모든 행위



엔드포인트의 행위 정보 수집

AhnLab

엔드포인트 안정성

Threat Hunting

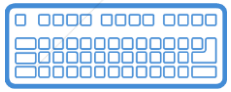
Centralization

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

행위 정보 분석

AhnLab

시간 기반
행위 상관 분석



사용자 정의 룰

빅데이터 분석

의심스러운 행위 필터링

AhnLab

랜섬웨어
의심행위

비정상적인
실행

파일
다운로드

자동실행
구성

방화벽
설정 변경

최근
생성파일

메모리
쓰기 시도

인젝션
시도

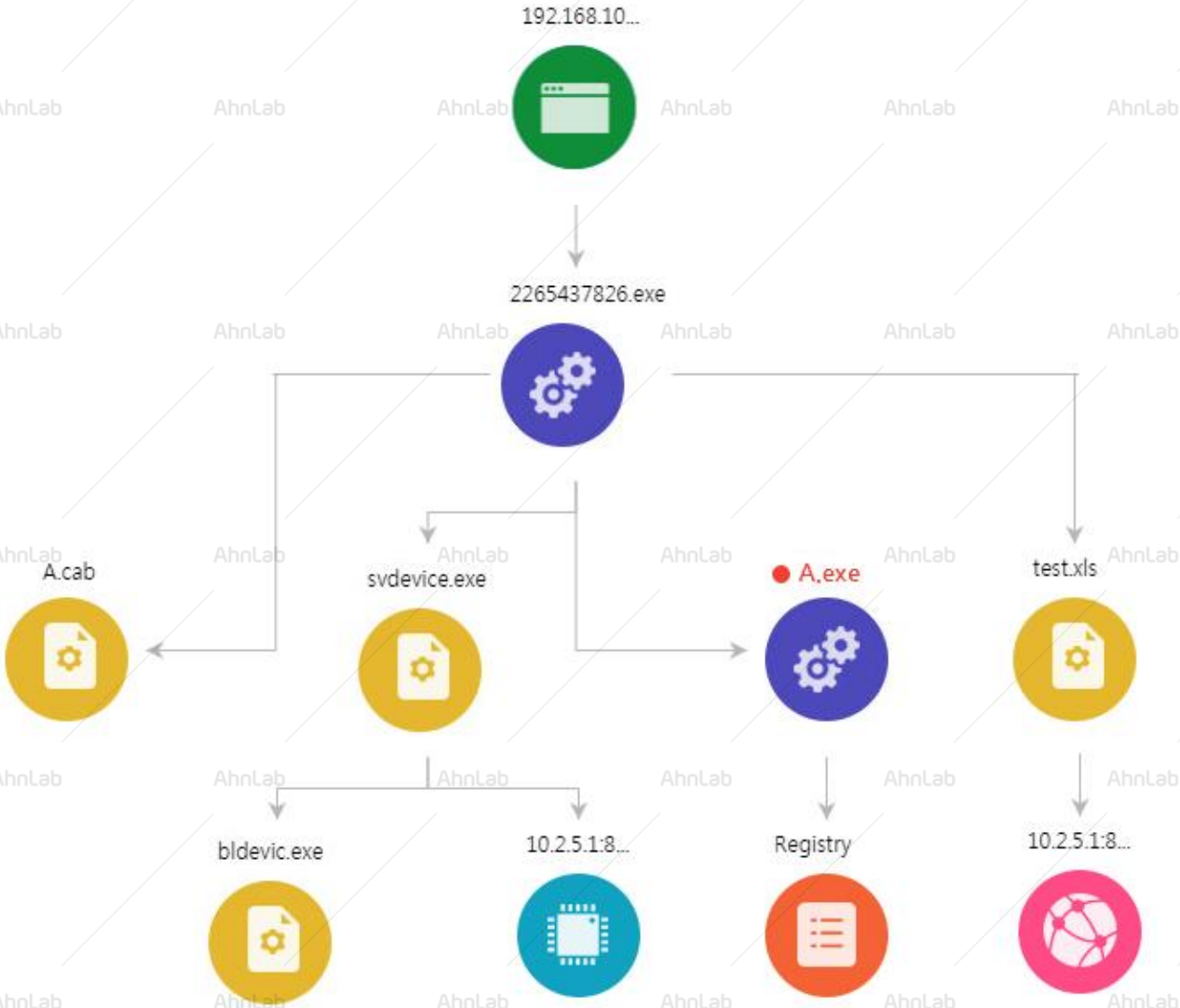
보안설정
변경

DDoS
행위

■ ■ ■

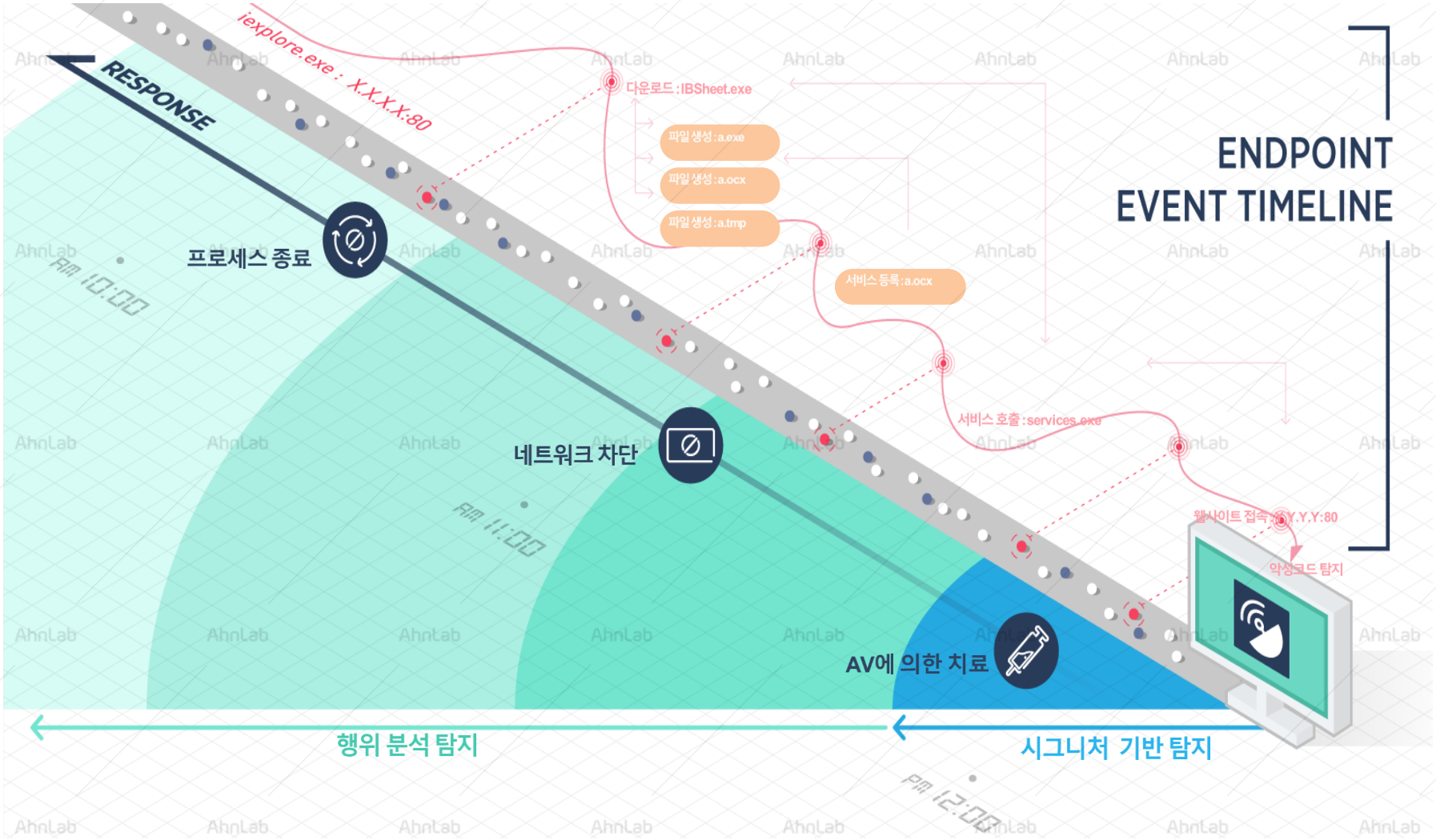
행위 상관 분석

AhnLab



시간 순서 기반 행위 분석

AhnLab

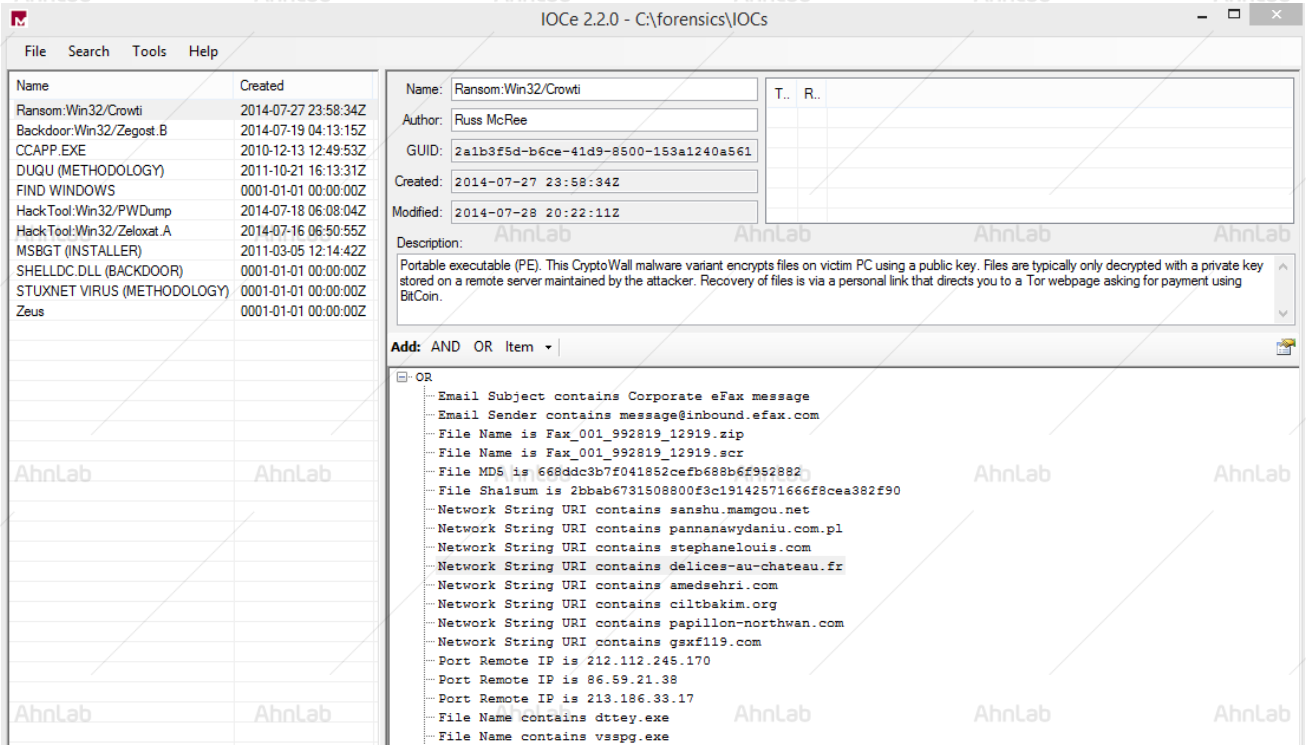


IOC 기반 분석

AhnLab

IOC *Indicator Of Compromise*

악성코드, 해킹에 대한 흔적을 일정한 포맷으로 정리

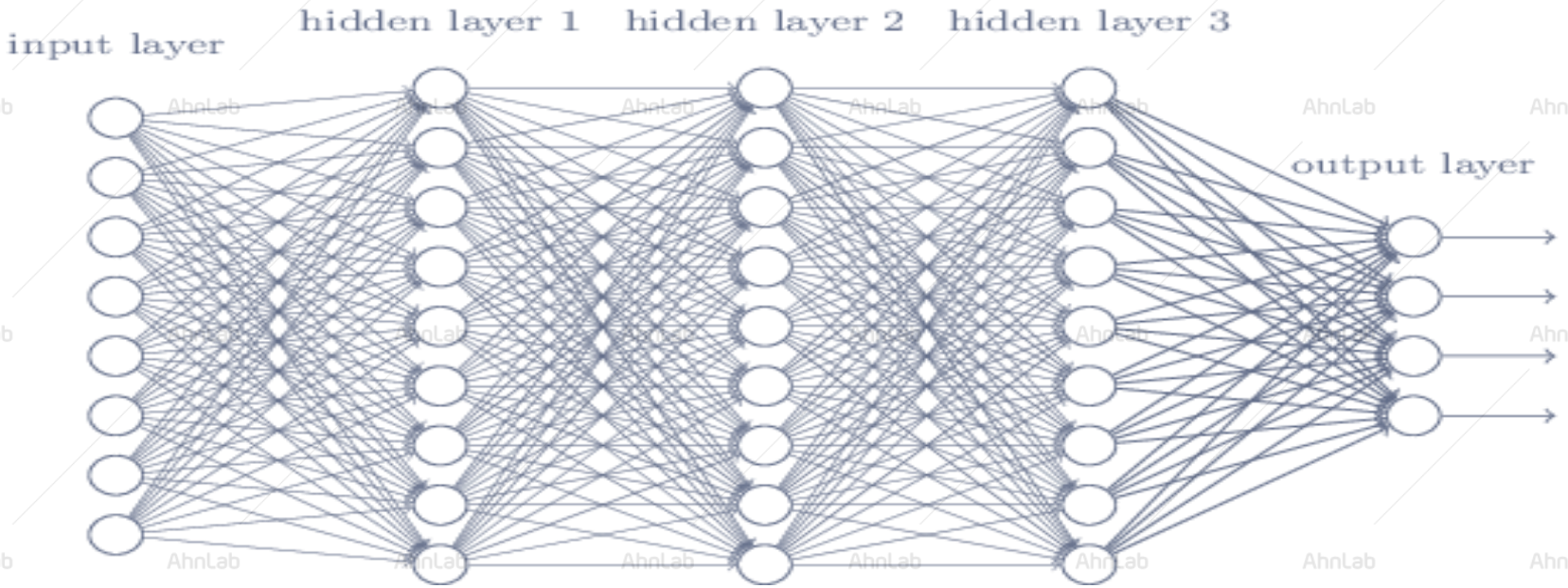


머신러닝 기반 분석

AhnLab

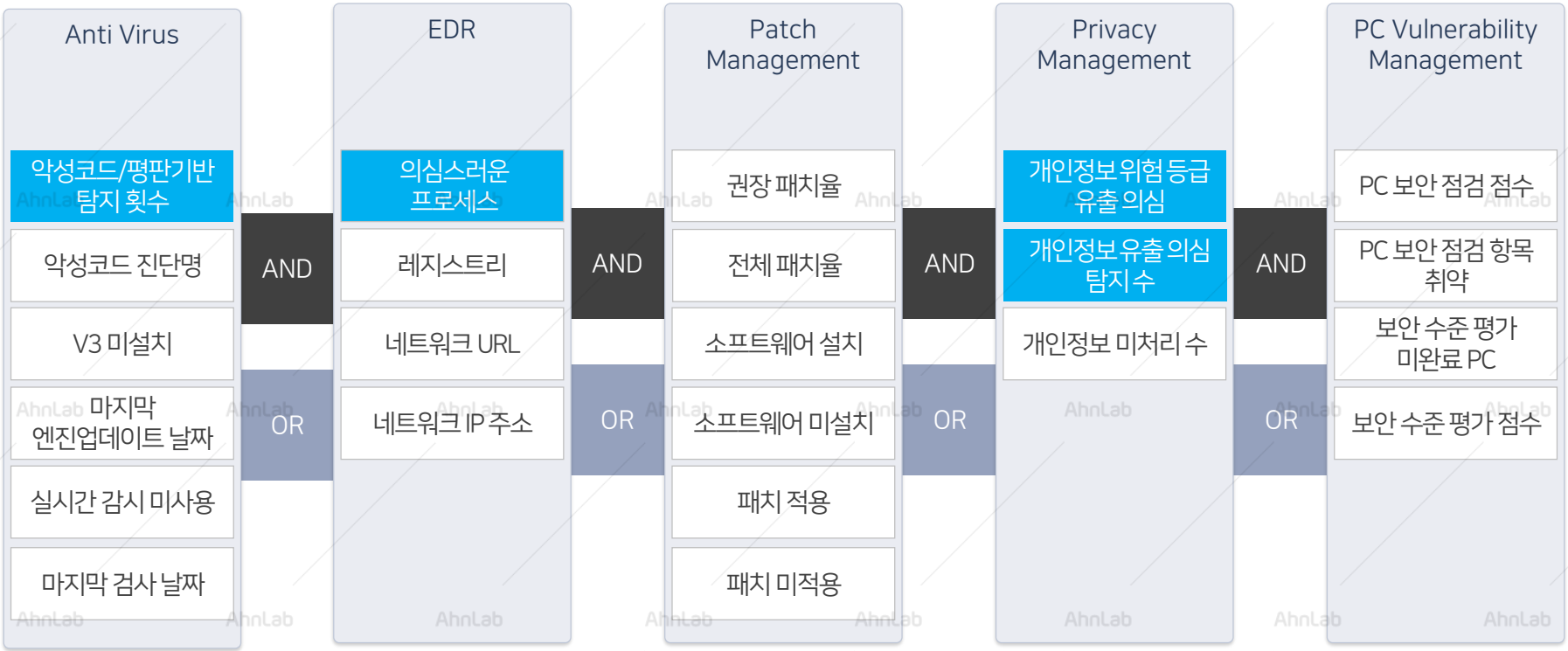
수학적 알고리즘

의심 행위 예측



연관 분석

AhnLab


Anti Virus
악성코드/평판기반 탐지 횟수
악성코드 진단명
V3 미설치
마지막 엔진업데이트 날짜
실시간 감시 미사용
마지막 검사 날짜
AND
OR
EDR
의심스러운 프로세스
레지스트리
네트워크 URL
네트워크 IP 주소
AND
OR
Patch Management
권장 패치율
전체 패치율
소프트웨어 설치
소프트웨어 미설치
패치 적용
패치 미적용
AND
OR
Privacy Management
개인정보 위험 등급 유출 의심
개인정보 유출 의심 탐지 수
개인정보 미처리 수
AND
OR
PC Vulnerability Management
PC 보안 점검 점수
PC 보안 점검 항목 취약
보안 수준 평가 미완료 PC
보안 수준 평가 점수

개인정보 유출 사고와 행위정보 분석

AhnLab

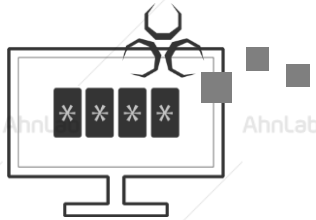
포털 및 SNS 접속

EDR 탐지
네트워크 연결 정보

플래시플레이어
익스플로잇 발생

악성코드 동작

EPP 탐지
악성코드 탐지

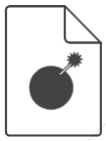


개인정보 유출

EPP
개인정보 유출 탐지

이메일 수신,
악성코드 다운로드

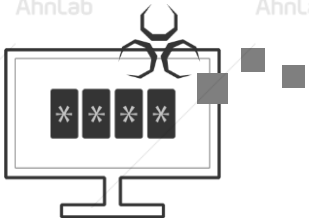
EDR 탐지
파일 유입 (다운로드)



비실행형 첨부 문서 기반의
익스플로잇 발생

클라이언트 PC 잠복

EDR 탐지
은닉행위 탐지



개인정보 유출

EPP
개인정보 유출 탐지

탐지 보안 침해 탐지

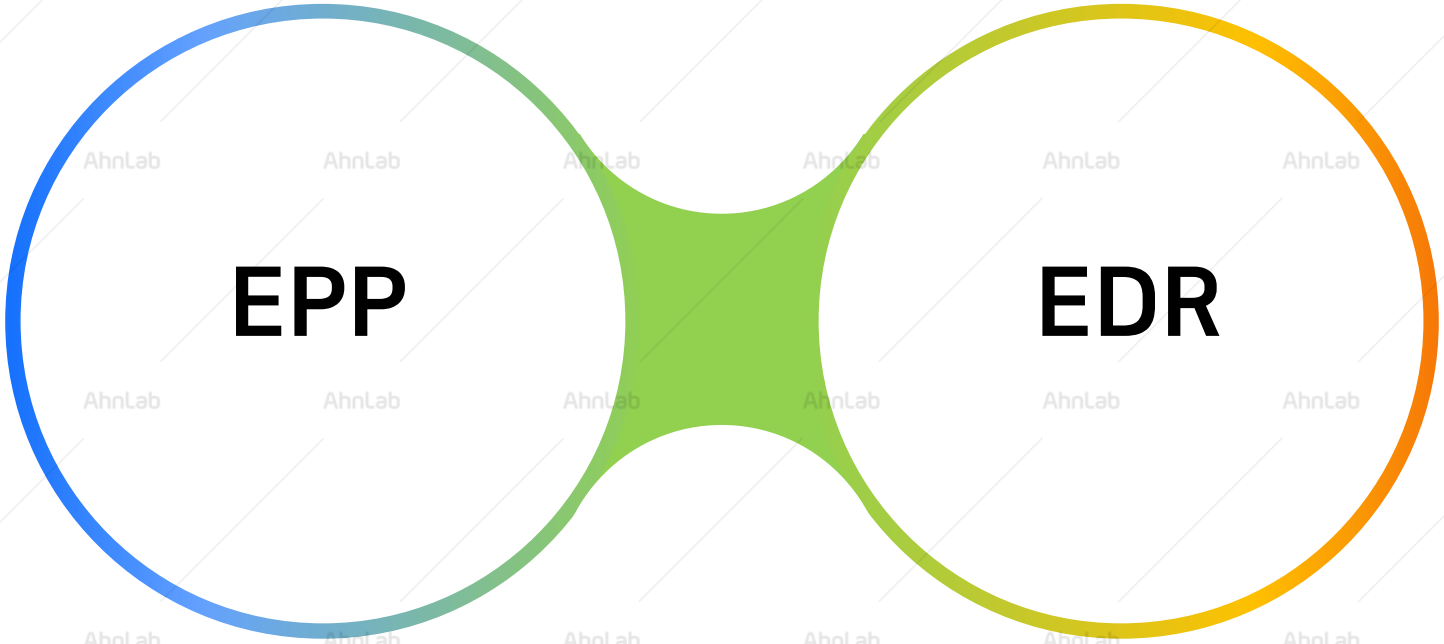
분석 보안 침해 조사

방지 엔드포인트에서의 보안 침해 억제

대응 치료를 통한 감염 이전 상태로의 회복

EPP & EDR

AhnLab



Endpoint Protection Platform

Malware를 방지하고 신뢰할 수 있는 응용
프로그램의 악의적인 활동을 탐지 및 차단하며
동적으로 대응하는 데 필요한 조사 및 치료 기능을 제공

More security, More freedom

AhnLab