행위를 수집하고, 위협을 사냥하라!

2020년 전망 금융 IT Innovation 컨퍼런스

EP 컨설팅팀 **백민경 부장**

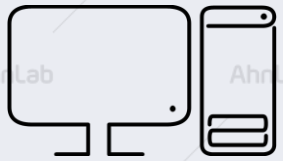
AhnLab

CONTENTS

AhnLab

Endpoint란?

AhnLab



[Desktop]

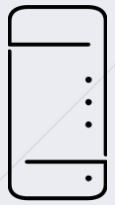
End 라는 단어가 주는 의미

끝, 마지막, 꼴찌, 중요하지 않은, 끄트머리

[Laptop]

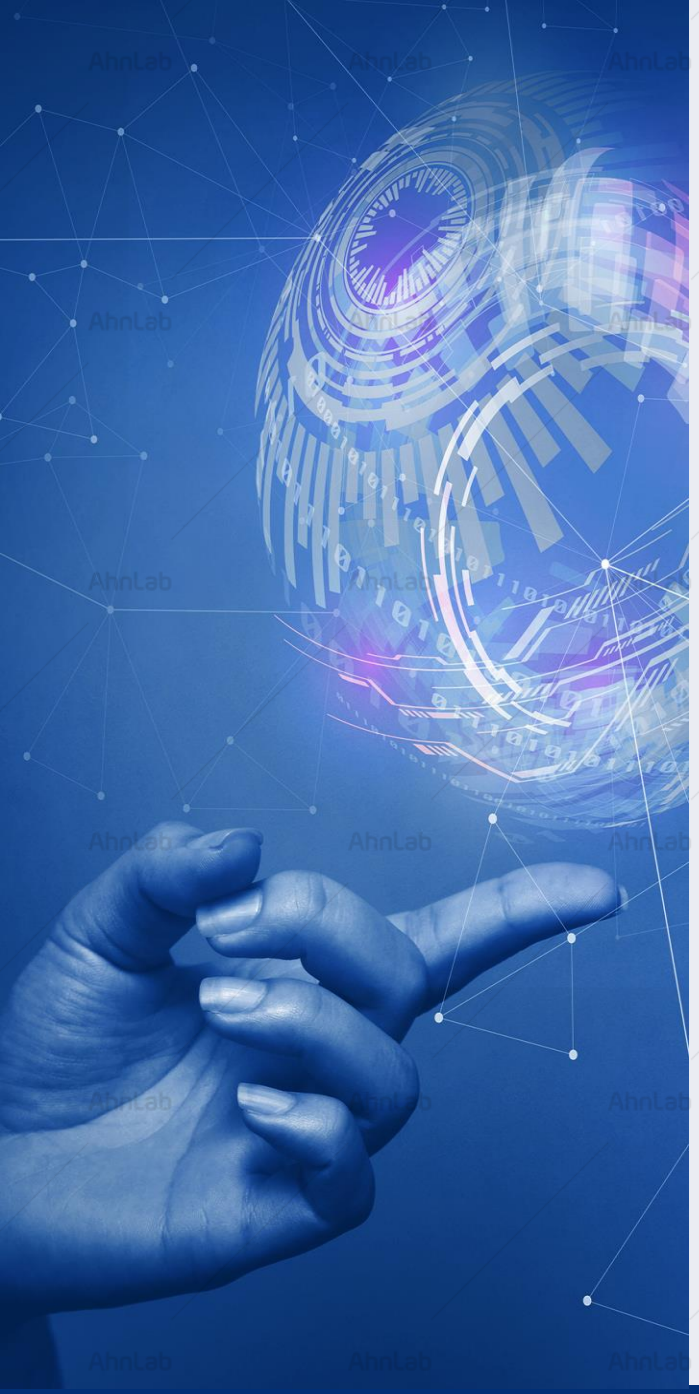
IT에서 Endpoint의 의미

네트워크에 연결된 단말 장치



[Server]

[Mobile Device]



AhnLab

공통점은?

사람이 사용하는 기기

네트워크에 연결돼 있음

다양한 인터넷 서비스를 사용 — 웹, 이메일, SNS 등

보안 체계에서 가장 취약 지점은 **사람**

Social Engineering(사회공학) 해킹

웹 : Watering Hole Attack
이메일 : Spear Phishing
전화 : Voice Phishing
문자 : Smishing

Endpoint Hardening

AhnLab

유입 방어

Firewall
IDS / IPS
Web Firewall
Anti-DDoS
Anti-Spam
N/W Sandbox

탐지 대응

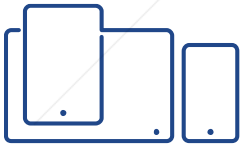
Anti-Virus
Endpoint Sandbox
Host IP, Host Firewall

유출 방어

DLP (Web, Email, USB)
DRM
Device Control

망 구분

물리적 망 분리
VDI
망 연계



Endpoint Hardening

데이터 보호

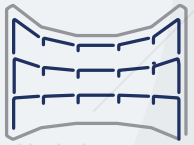
SSL
DB Encryption
Personal Privacy Protection

인증 강화

NAC
OTP (Multi Factor Authentication)
접근 통제 시스템 | SSO

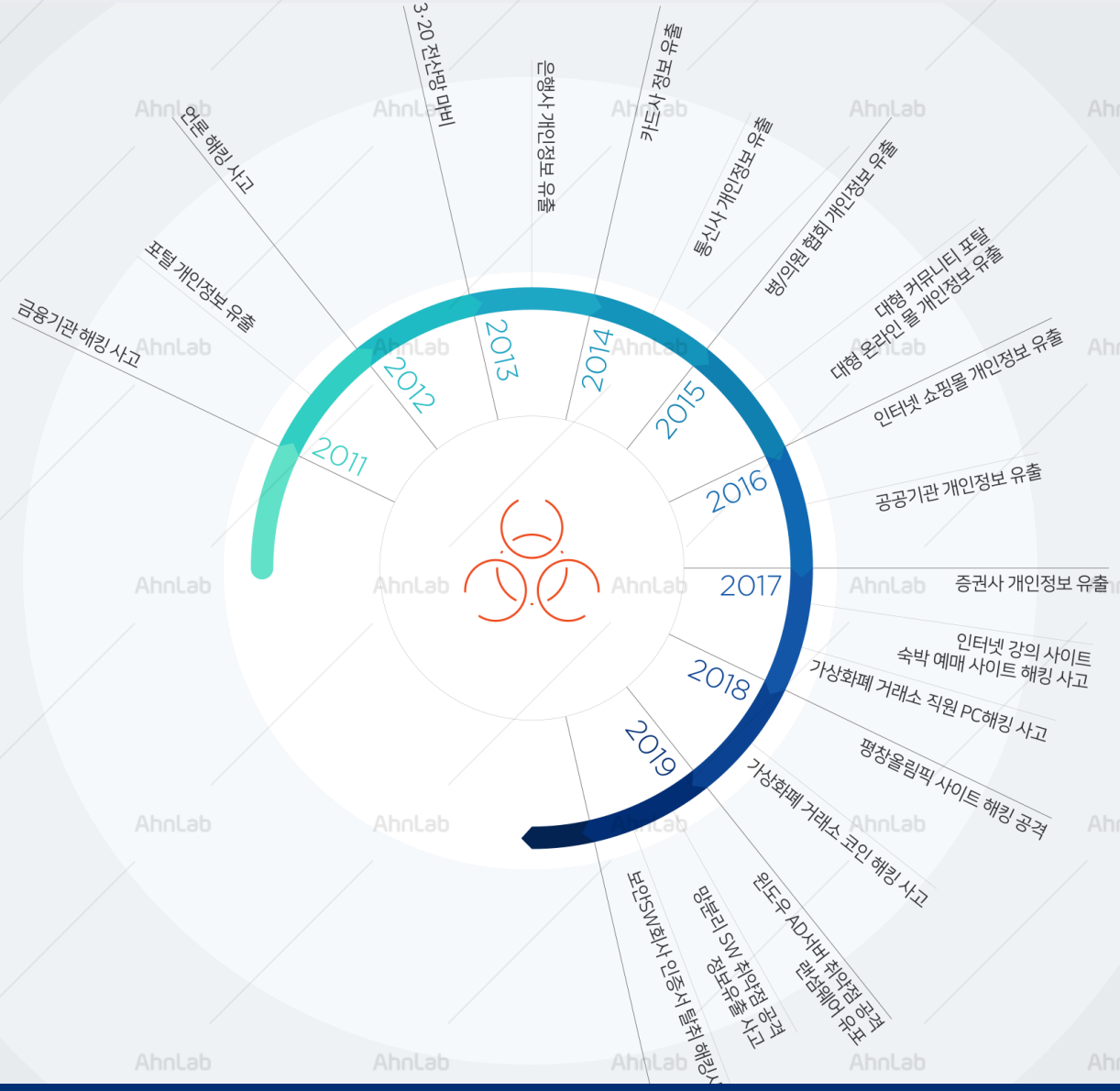
취약점 제거

PMS
취약점 점검
모의해킹



보안 운영 관리

반복되는 침해 사고 사례



공격자들의 목적

AhnLab

공격 목적

약탈	협박
기밀 자료	침해 사실 공개
개인 정보	
게임 머니	DoS
암호 화폐	랜섬웨어
CPU	

금전 이익

공격과 방어는 애초부터 방어가 불리한 게임이다.

침해 사고 분석

AhnLab

흔적 분석만으로 침해 사고 분석을 성공할 수 있을까?

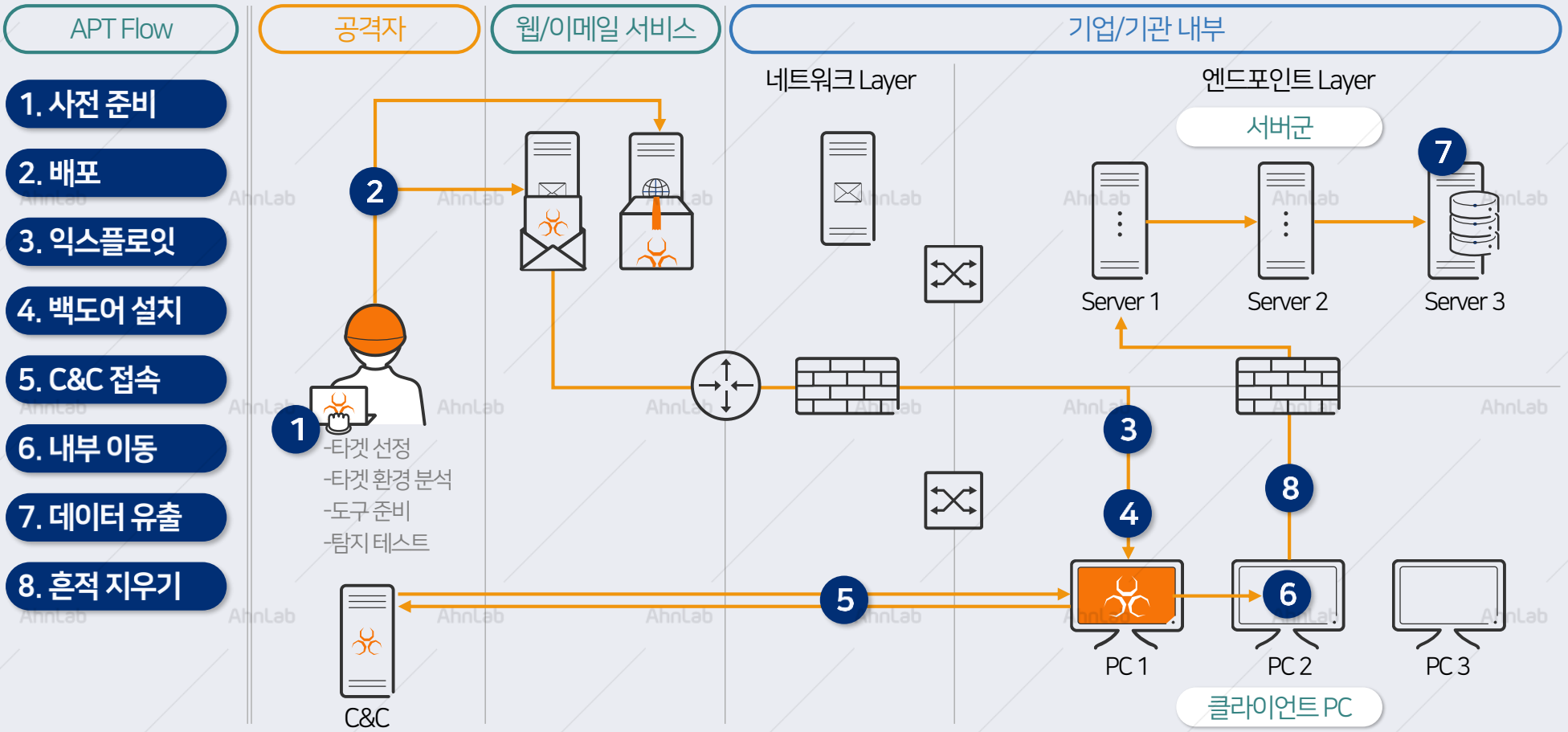
침해 사고 분석의 성공과 실패

AhnLab

현장이 잘 보존 되어있고, **로그가 존재**하는 경우
침해 원인과 과정을 성공적으로 분석할 가능성이 높아진다.

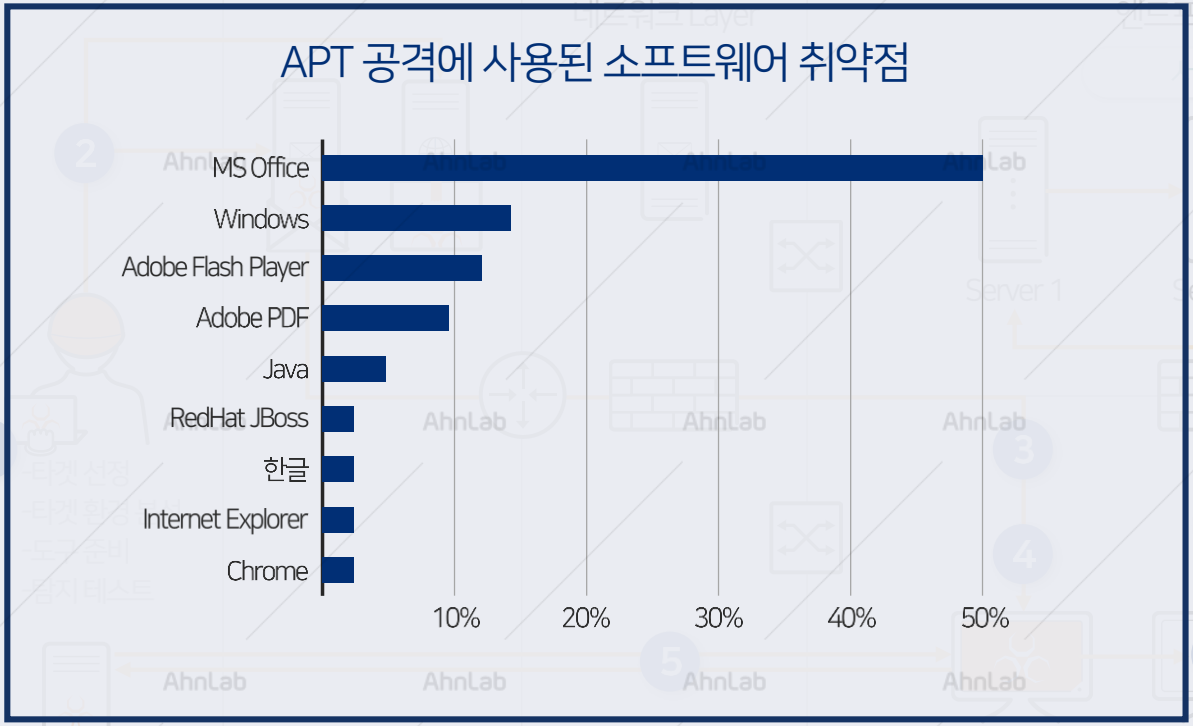
침해 사고 사례

AhnLab



침해 사고 사례

AhnLab



침해 사고 인지가 늦어지는 이유

AhnLab

악성 코드 탐지 시 **원인 파악 없이 증상만 치료**

감염 시 시스템 포맷, VDI 초기화

특히 망 분리 환경의 경우 인터넷 망 시스템의 악성코드 감염을 대수롭게 않게 여김

내부망 침해 시에는 악성코드 보다 정상 파일 **LOLBins가 사용되는 추세**

LOLBins : Living Off the Land Binaries (or Libraries, Scripts)

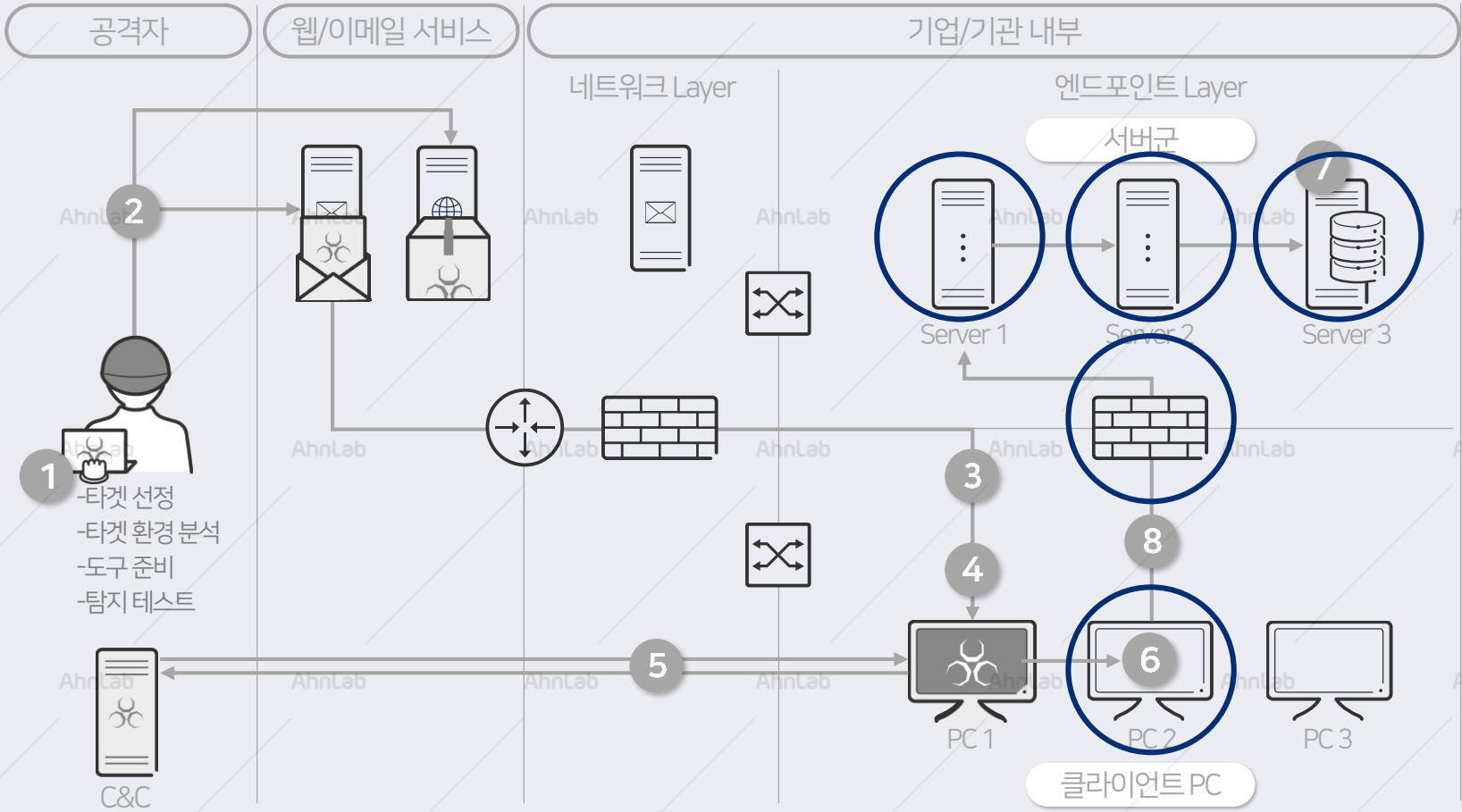
파일 자체의 악성 여부를 판단하는 방식의 백신으로는 탐지가 어려움

(정상을 가장한 엔드포인트 단말의 악성 행위 탐지 한계)

조직 내부에서 **침해 인지를 위한 활동**(Threat Hunting)**을 하지 않음**

침해 사고 사례 : 공격자 행위 역추적

AhnLab



공격자 추적

Server 3 (DB)

- 침해 인지
- DB 접근 로그 조사

Server 2 (SSH)

- SSH 로그 조사

Server 1 (Windows)

- 시스템내 의심 파일 흔적
- 로그가 삭제되어있음

Firewall

- 방화벽 로그 확인

PC 2

- 시스템내 의심 파일 흔적
- 로그가 삭제되어있음
- 더 이상 추적 불가!

외부 위협을 방어하기 위해서는 . . .

AhnLab

피해 발생 전 인지하기

침해 인지 시간 단축
피해 범위 및 규모 축소

최초 유입 차단하기

Endpoint Hardening

사후에 추적하기

침해 원인 파악 /
재발 방지

실질적 취약점 해소 / 유사 침해 재발 방지

피해 발생 전 인지하기

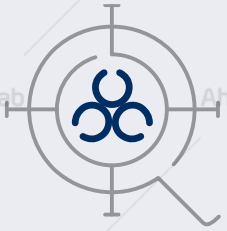
AhnLab

Threat Hunting

공격자가 공격 목표물에 도달하기 전에 찾아내자

로그 점검 / 확보

로그가 잘 기록되고, 잘 보관되고 있는가
Host에서 발생되는 행위 로그 수집 (EDR 유형의 솔루션)



침해 이벤트 분석

보안 솔루션에서 실시간으로 탐지한 악성 이벤트 확인
(Anti-Virus, IDS/IPS 등)
관제 서비스

통계 / 패턴 데이터 분석

명확히 악성으로 탐지되지 않는 행위 확인
과거 이력 분석 (타임라인)
통계, 패턴 분석
조직 내부에서 해결해야 함

사후에 추적하기

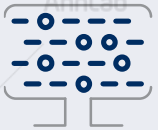
AhnLab

분석 목표는?

침해 원인 파악

공격자의 침입 경로
(= Root Cause = 취약점 = 공격자가 사용한 위협)

피해 범위 파악



분석 대상은?

목표를 해결하기 위한 모든 관련 데이터를 분석한다.

악성코드, 로그, 디스크, 메모리, 모바일기기 등

이제 보안 팀 인력에게 분석하라고 하면 될까? 또는 포렌식 분석가들을 부르면 될까?

분석 조직을 자체 보유하기 어렵다.
점점 분석이 어려운 환경이 되어 가고 있다.

AhnLab

범죄 현장에 CCTV를 설치하자

Endpoint EDR

Endpoint 의 로깅 강화

- Who, When, Where, What, How
- 파일
- 네트워크
- 레지스트리
- 프로세스
- 시스템 설정
- 사용자 행위

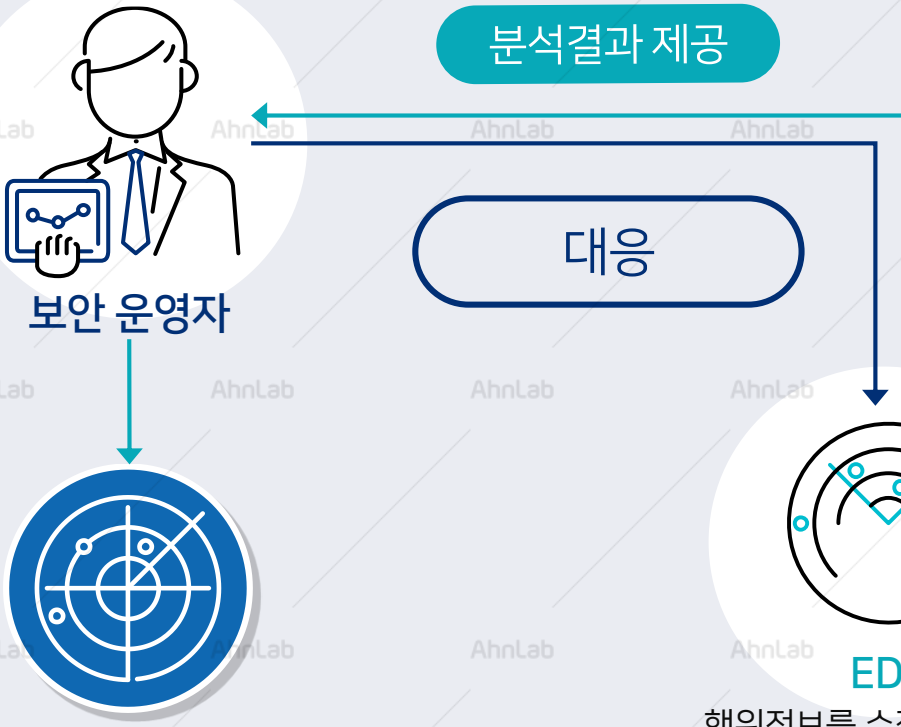
침해 조사에 필요한 정보를 안정적으로 상시 수집

별도 시스템에 로그 백업

Threat Hunting과 사고 분석에 활용

보안 위협 탐지 및 대응 주체

AhnLab



Endpoint Hardening Solution

보안 솔루션이 탐지하고 대응

EDR

행위정보를 수집, 저장, 분석

사고 발생 확률을 낮추기 위한
공격 표면 최소화

엔드포인트 상시 행위 수집을 위한
CCTV 설치

사고를 추적하여
원인 파악 및 재발방지

사고 발생 인지 시간 단축을 통한
피해 범위 및 규모 축소

More security, More freedom

AhnLab