MORE SECURITY
MORE FREEDOM

AhnLab

보안 트렌드 및 AhnLab 통합 솔루션/서비스 소개

Case별로 살펴본 주요 보안대응전략

MORE SECURITY
MORE FREEDOM

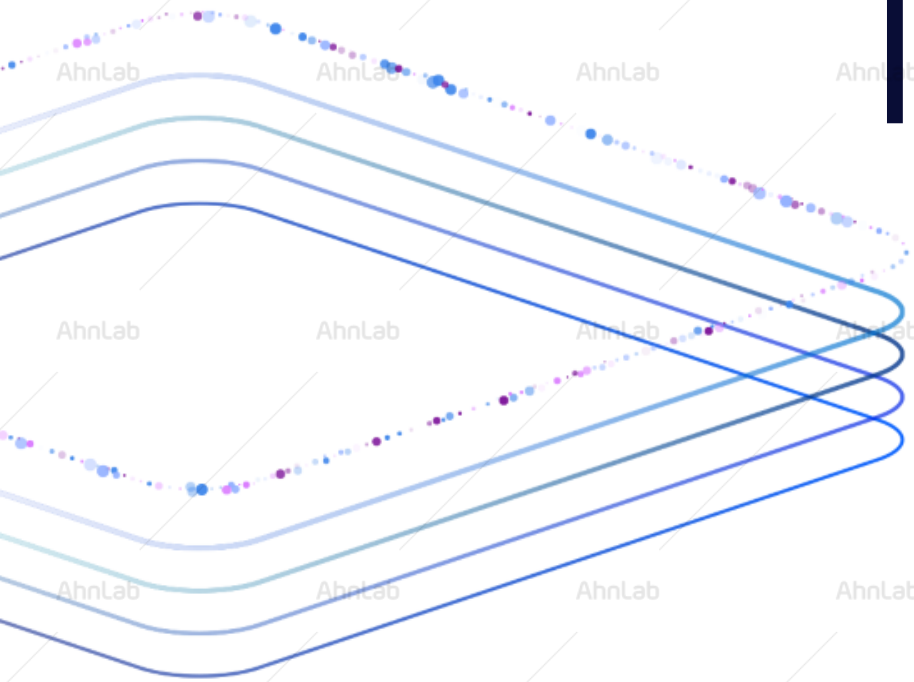
CONTENTS

안랩의 보안 아키텍처를 담은
AhnLab 통합 솔루션/서비스 맵

Case별로 살펴본 주요 보안대응전략

AhnLab

MORE SECURITY
MORE FREEDOM



보안 트렌드 변화

- 변화하는 보안 트렌드
- 무엇이, 어떻게 변화하나?
- 보안 영역의 결합

안랩의 보안 아키텍처를 담은
AhnLab 통합 솔루션/서비스 맵

Case별로 살펴본 주요 보안대응전략

AhnLab

01 변화하는 보안 트렌드

지금까지 보안은 **경계 보안 중심**

AS-IS

외부위협의 **방어**와
내부유출의 **통제**에 포커스 …

Detection

외부 위협 방어

TO-BE

대응(Response) 중심
솔루션 **통합**과 **연동**

Prevention

내부 유출 통제

정보자산을 지키기 위한
Traditional 솔루션들 …

Unified Security

플랫폼과 플랫폼의 연동

Consolidation

솔루션들의 유기적인 통합

02 무엇이, 어떻게 변화하나?

위협의 예방

위협의 초기 **식별**과 **대응**

위협 완화

리스크 통제와 **거버넌스 확보**

Protect & Detect

Threat hunting & Respond

위협 원점에 대한
탐지-분석-대응

위협과 리스크에 대한
통합관리

Point Solution 간 정보 통합 + 연동을 통한

통합적인

Threat Detection & Response

레이어 별
포인트 솔루션 구성

오케스트레이션 및
거버넌스

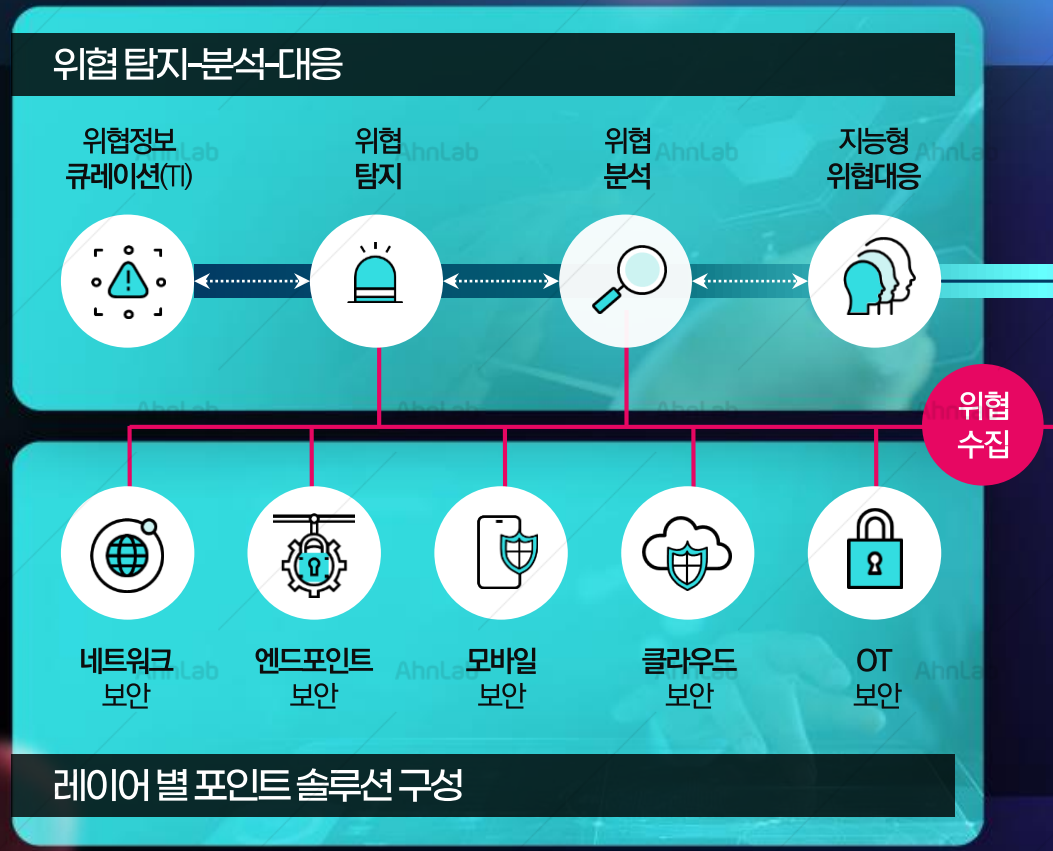
Resilience

Governance & Visibility

03 보안 영역의 결합

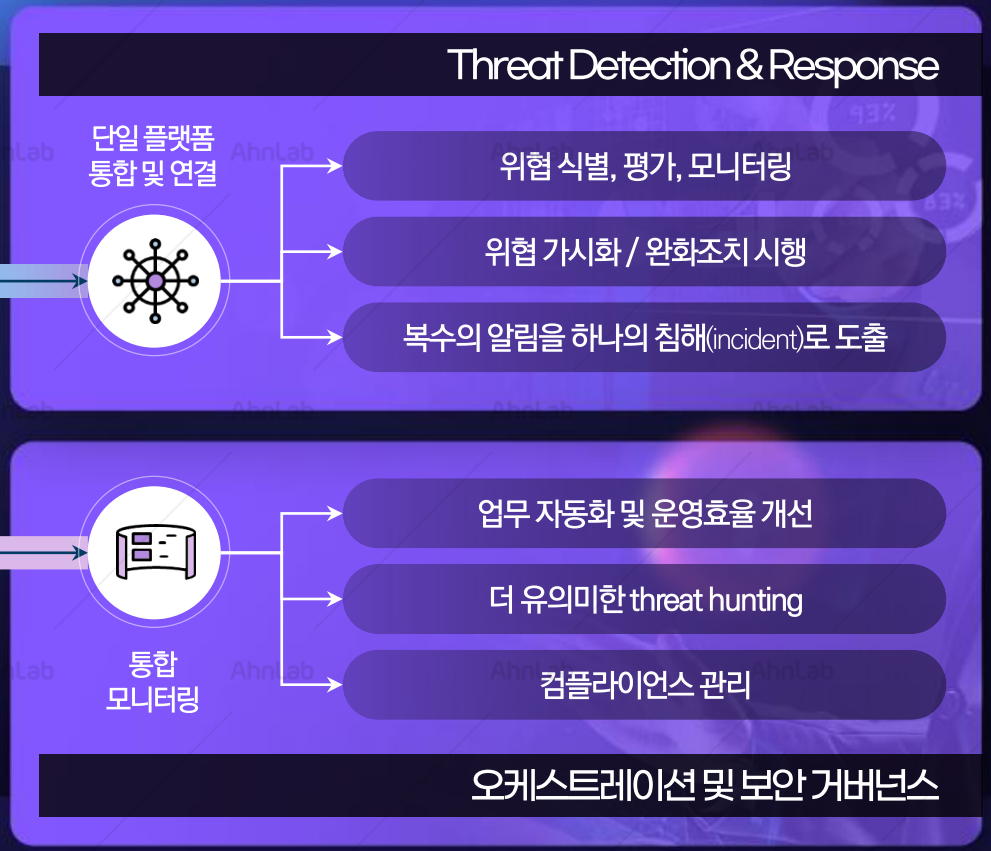
유기적 통합

효과적 대응을 위한 솔루션 유기적 **통합**

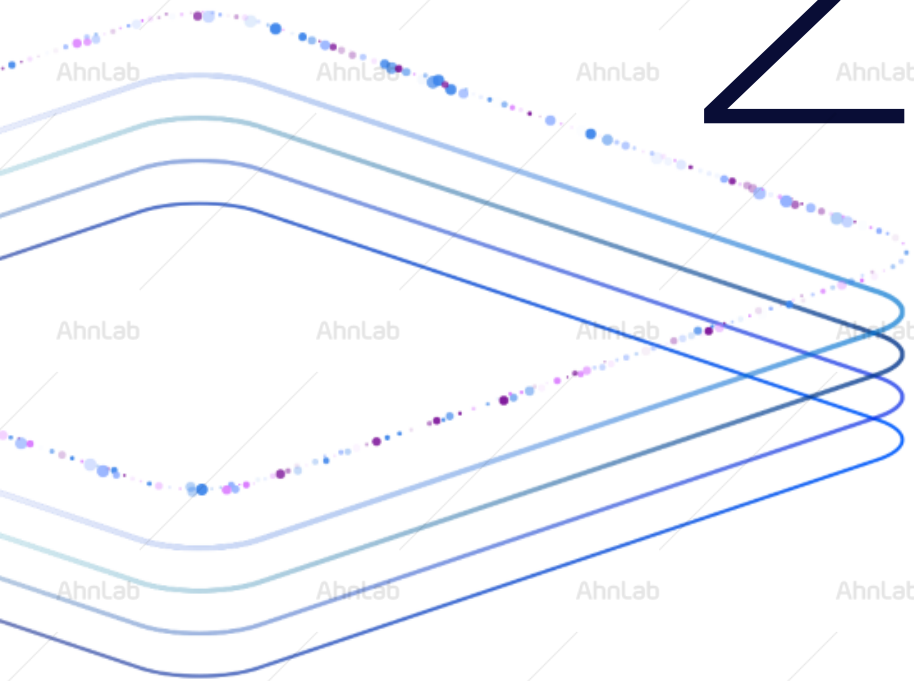


플랫폼 연동

리스크 통제와 거버넌스 확보를 위한 플랫폼 **연동**



MORE SECURITY
MORE FREEDOM



2 통합 솔루션/서비스 맵

- AhnLab이 그리는 보안 아키텍처
- AhnLab 보안 솔루션/서비스 매핑
- 아키텍처 레이어 구성

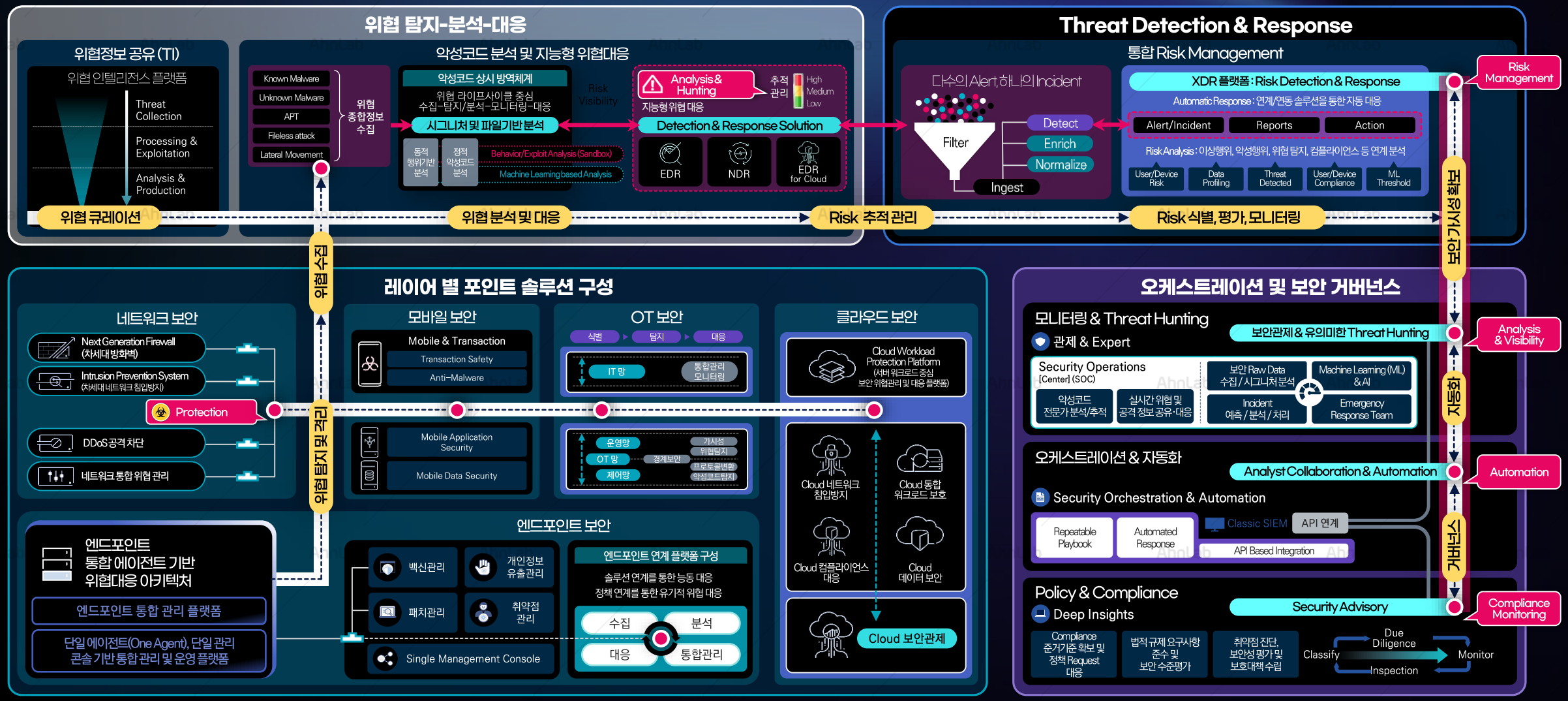
안랩의 보안 아키텍처를 담은
AhnLab 통합 솔루션/서비스 맵

Case별로 살펴본 주요 보안대응전략

AhnLab

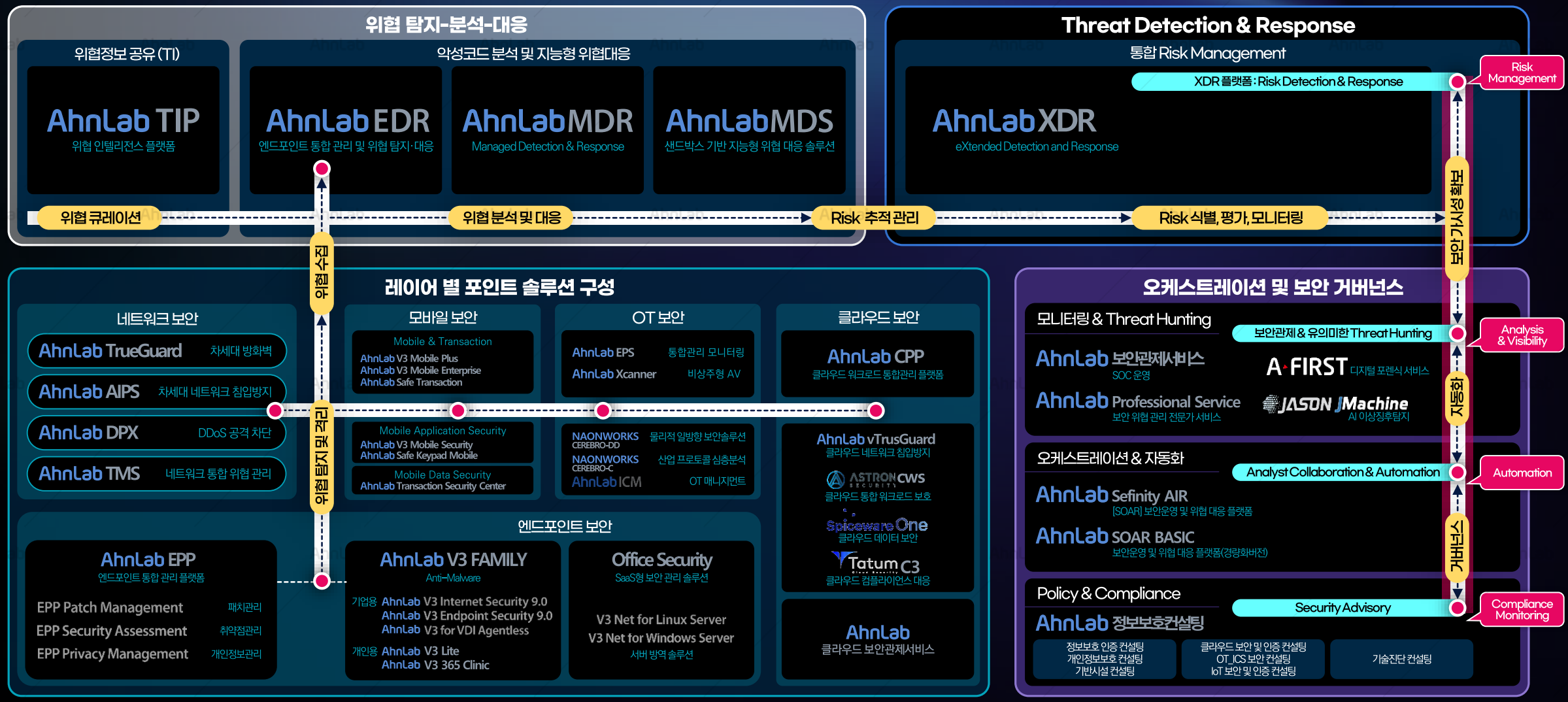
More security More freedom

01 AhnLab이 그리는 보안 아키텍처



AhnLab

02 AhnLab 보안 솔루션/서비스 매핑



네트워크 보안영역

More security / More freedom

차세대 네트워크 방화벽

차세대 방화벽 (NG Firewall)

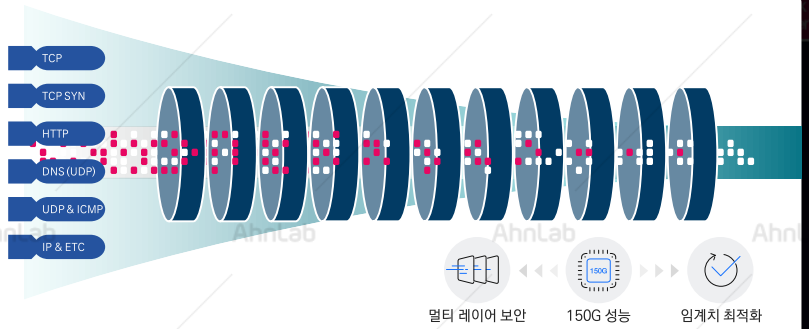
AhnLab TrusGuard

Firewall	IPS	Application Control	C&C 서버 탐지/차단
SSL VPN (PC / Mobile)	Proactive & Comprehensive	High Performance & Flexibility	Anti-Malware (파일 기반 / 패킷 기반)
DLP (Data Loss Prevention)			SSL Inspection (암호화된 트래픽 인지)
Anti-Spam			IPSec VPN
지역 기반 차단			Web Filtering

DDoS 공격 차단

DDoS 공격 차단 솔루션

AhnLab DPX



네트워크 통합 위협관리

네트워크 통합 위협 관리 시스템

AhnLab TMS

효율적 정책관리 / 신속 탐지/대응 / 플랫폼 기반 / 심층 위협분석 / 통합 이벤트 관리 / 위협 가시성 — TMS

차세대 네트워크 침입방지

차세대 네트워크 침입방지

AhnLab AIPS

Next-Gen IPS / Anomaly Detection / High Performance / Malware / Threat Intelligence / Open API

네트워크 트래픽 분석

Network Detection & Response

Quad Miners / NETWORK BLACKBOX

100% Full 패킷 캡처
네트워크 행위 가시화
실시간 이상징후 탐지
고성능 패킷 스트림 저장

Web Application Firewall

AI WAF

MONITORAPP / AIWAF

모든 웹 트래픽 검사 / 비정상 접근 탐지 차단 / Unkwown Attack 선제적 방어 / Trafic Inspection 기술 기반

엔드포인트 보안영역

More security / More freedom

안티 멀웨어

안티멀웨어

기업 PC 보안	서버 보안
V3 Internet Security	V3 Net for Windows Server
V3 Endpoint Security	V3 Net for Unix/Linux Server
가정용 PC보안	**VDI 보안**
V3 365 Clinic	V3 for VDI

엔드포인트 보안 플랫폼

엔드포인트 플랫폼

단일 매니지먼트 기반의
차세대 엔드포인트 보안 플랫폼

중앙관리	패치관리
AhnLab EPP	EPP Patch Management
취약점관리 및 조치	**개인정보 유출 방지**
EPP Security Assessment	EPP Privacy Management

- 위협관리 및 대응을 위한 연계 정책 설정을 통해 조직의 환경에 최적화된 엔드포인트 보안 운영

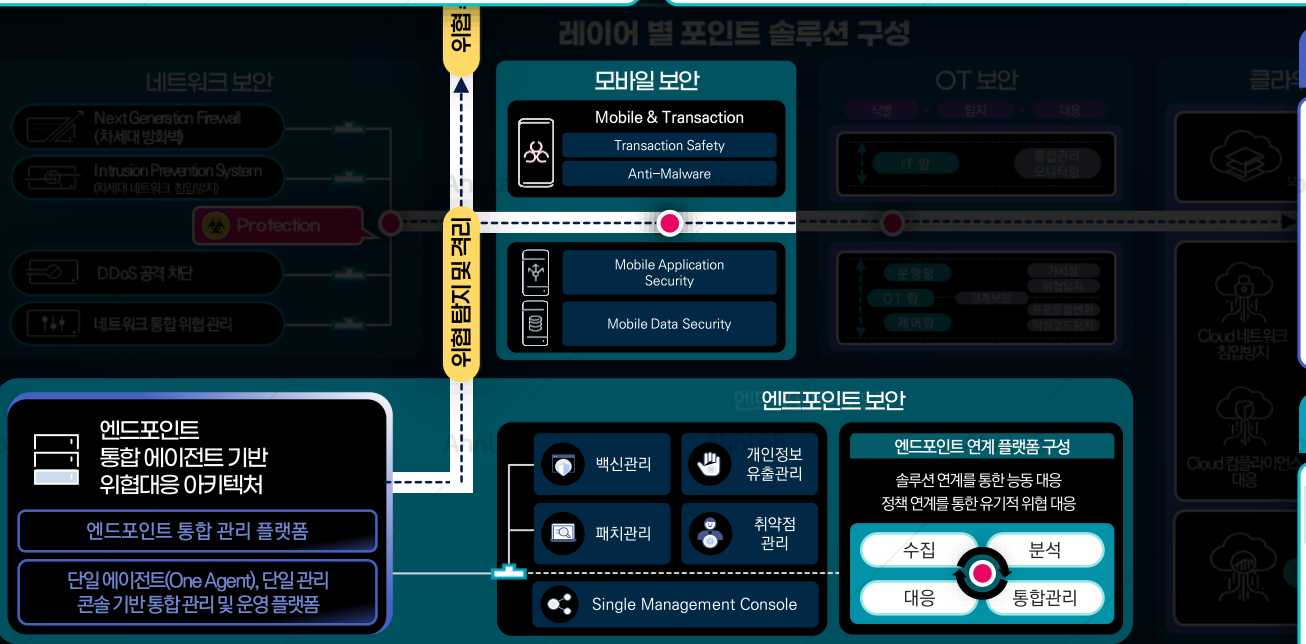
SMB 단말보안

엔드포인트 통합관리

다양한 엔드포인트
보안 솔루션의 통합 관리

SaaS형 보안관리
Office Security
SMB 보안
기업용 PC주치의

레이어 별 포인트 솔루션 구성



모바일 보안

모바일 AV	모바일 트랜잭션 보안
V3 Mobile Security	V3 Mobile Plus
모바일 오피스 환경 보안	**모바일 보안 엔진**
V3 Mobile Enterprise	Mobile Engine SDK

인증관리

Next Authentication Platform **Whykeykey**

Ydentity

생체기반인증
Ydentity

개인정보보호

개인정보보호 통합관리

클라우드 기반의 더 강력한 **개인정보 유출 방지**

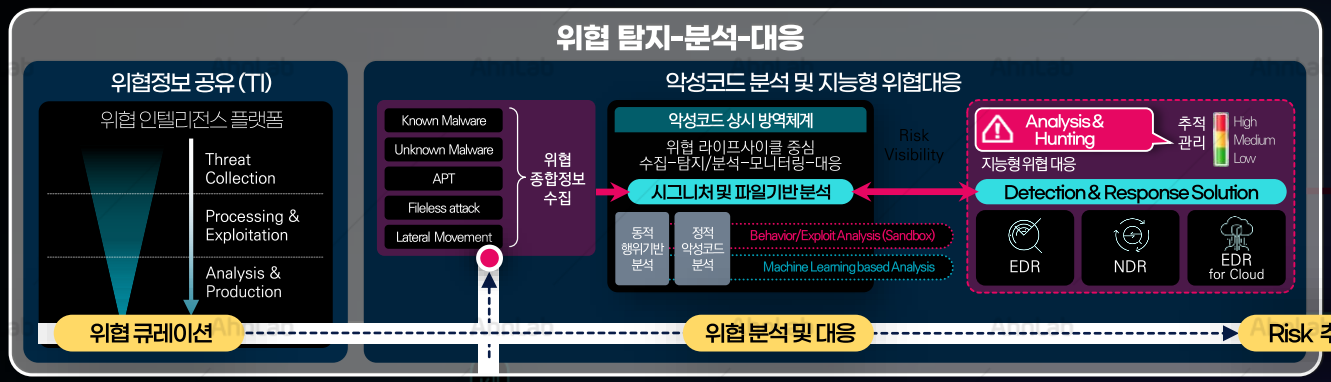
클라우드 개인정보 보호 | Spiceware

개인정보수집·탐지·암호화
PII CDE
개인정보 가명·익명처리
PII ANP

지능형 위협 대응 영역

More security / More freedom

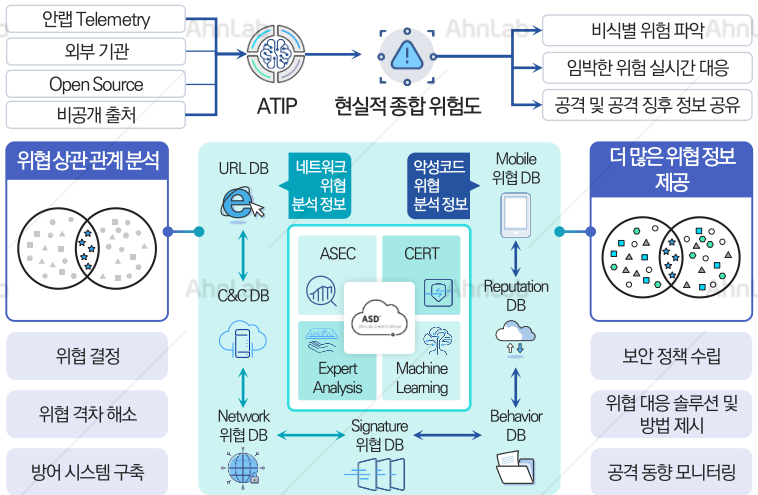
위협 탐지-분석-대응



위협 인텔리전스 플랫폼

AhnLab TIP

전문 기술 및 노하우가 결합된 시큐리티 인프라 기반
THREAT INTELLIGENCE PLATFORM



엔드포인트 위협탐지 및 대응

AhnLab EDR

행위 정보 탐지·분석을 통한
엔드포인트 가시성 확보 및 대응

간편한 구축, 손쉬운 운영
더 강력한 위협 대응

MDR (Managed Detection & Response)

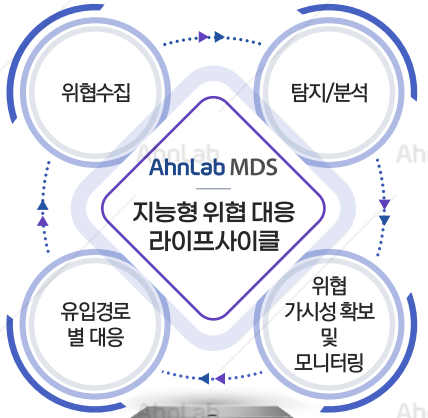
AhnLab MDR

설치된 EDR에서 탐지된 위협 이벤트를 위험도(경고, High) 기준으로
모니터링하여, **전문가가 원격에서 위협을 직접 분석 및 대응**

APT 대응

AhnLab MDS

샌드박스 기반
지능형 위협 대응



네트워크 기반 공격 대응	엔드포인트 기반 공격 대응	이메일 기반 공격 대응	망연계/ 파일 서버 대응
• 이상 트래픽 탐지 및 차단	• 악성코드 삭제 /실행 보류 • 의심 파일 추출 시스템 격리	• 이메일 격리 기능 • 이메일 필터링 연계	• 망연계 솔루션 연동 • 3rd party 솔루션 연계

- 주요 경로를 통해 유입되는 위협 수집
- 멀티엔진 기반의 다단계 분석 모듈 제공

수집 → 탐지/분석

APT 대응 절차

대응 → 모니터링

- 네트워크 에이전트 기반 위협 대응
- 직관적인 위협 가시성
- 지속적인 위협 모니터링

클라우드 영역

More security / More freedom

클라우드 보안 플랫폼

AhnLab CPP

클라우드 플랫폼 | 애플리케이션 제어 | 네트워크 침입 공격 방어 | 안티멀웨어

중앙관리	애플리케이션 실행 허용	네트워크 침입 방어·방화벽	악성코드 탐지·대응
CPP Management	Application Control	Host IPS	V3 Net

AhnLab vTrusGuard 클라우드 차세대 방화벽

NGFW for Cloud
클라우드 환경에 최적화된 차세대 방화벽 기술을 기반으로 위협을 최소화하여 클라우드 보호

AhnLab vAIPS 클라우드 위협대응시스템

클라우드 위협 탐지
클라우드 위협을 다양한 탐지 방법과 가속 기술을 바탕으로 정확하게 탐지하여 대응

AhnLab vTMS 클라우드 위협관리플랫폼

위협정보 모니터링 및 대응
위협대응시스템과 연동하여 다양한 클라우드 위협 정보를 모니터링하고 분석하여 대응

MONITORAPP | AIONCLOUD **클라우드 WAF**

ASTRON SECURITY **클라우드 통합 워크로드 보호**

클라우드 환경 최적화 웹 방화벽	CSPM+CWPP
AIWAF-VE (VM) / AI ON CLOUD (SECaaS)	ASTRON CWS

클라우드 데이터 보안

Spiceware One

클라우드 데이터 통합보안
Spiceware One

Risk 추적 관리

클라우드 보안

Cloud Workload Protection Platform
(서버 워크로드 중심 보안 위협관리 및 대응 플랫폼)

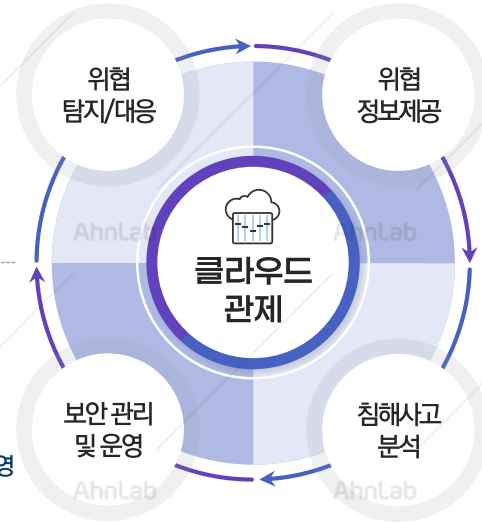
Cloud 네트워크 침입방지 | Cloud 통합 워크로드 보호 | Cloud 컴플라이언스 대응 | Cloud 데이터 보안

Cloud 보안관제

클라우드 관제

클라우드 환경 **실시간 보안 위협 탐지/대응**

안랩의 정보보안 **동향, 취약점 정보 제공**



효율적이고 체계적인 **클라우드 운영 지원**

클라우드 침해사고 발생 시 **정확한 원인 분석**

오케스트레이션 & 자동화
Analyst Collaboration & Automation
Security Orchestration & Automation
Repeatable Playbook | Automated Response | API 연계 | API Based Integration
Automation

Policy & Compliance
Deep Insights
Security Advisory
Compliance Monitoring
Classify | Due Diligence | Inspection | Monitor

클라우드 컴플라이언스

클라우드 정보보호 컨설팅
클라우드 인프라 취약점 점검
클라우드 환경 모의침투 테스트
클라우드서비스 보안 인증(SaaS) 컨설팅
기업의 클라우드 서비스 이용 사전 컨설팅 및 클라우드 서비스 안전성 점검 및 확보조치

컴플라이언스 준수

전자금융거래법, 신용정보법 등에 따른 암호화, 데이터 위, 변조 방지 등

기술적, 관리적 보호조치를 준수

- 클라우드 환경 컴플라이언스와 클라우드 보안인증 획득 및 개인정보보호를 위한 Cloud Compliance Consulting

C3

클라우드 컴플라이언스 점검 자동화

Tatum C3

CSPM기반 클라우드 보안 컴플라이언스관리 자동화

Cloud Compliance Checker

OT & ICS 영역

특수목적시스템 보안통제 및 산업용 서비스 제어

AhnLab 보안 위협 분석 기술 | NAONWORKS 산업용 프로토콜 분석

식별 | 탐지 | 대응

OT 보안

운영망

엔드포인트

- AhnLab EPS (엔드포인트 자산/프로세스 식별)
- AhnLab EPS (악성코드 검사/비인가 프로세스 탐지)
- AhnLab EPS (Whitelist 제어/매체 제어)
- AhnLab Xcanner (비상주형 악성코드 검사/치료)

네트워크

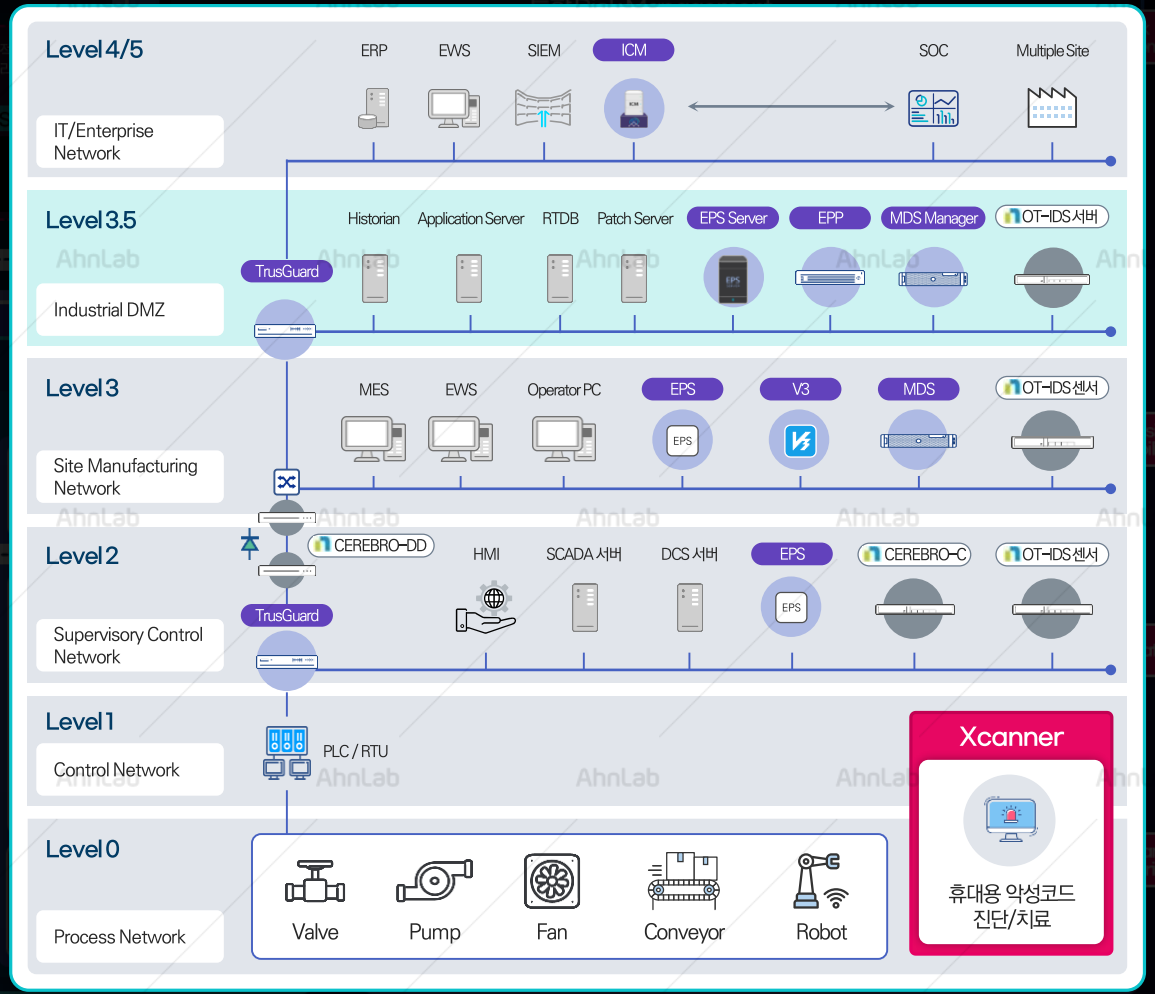
- CEREBRO-IDS (OT자산/트래픽 식별)
- CEREBRO-IDS (보안 위협 탐지)
- AhnLab MDS (생산망 파일 분석/감염장비 탐지)
- AhnLab TrusGuard (비인가 트래픽 탐지)
- CEREBRO-DD (일방향 데이터 전송)
- AhnLab TrusGuard (비인가 트래픽 차단)

제어망

ICS 설비

- CEREBRO-IDS (OT자산/트래픽 식별)
- CEREBRO-C (OT프로토콜 변환)
- CEREBRO-IDS (OT프로토콜 분석/위협 탐지)
- ICS 설비 업체 대응

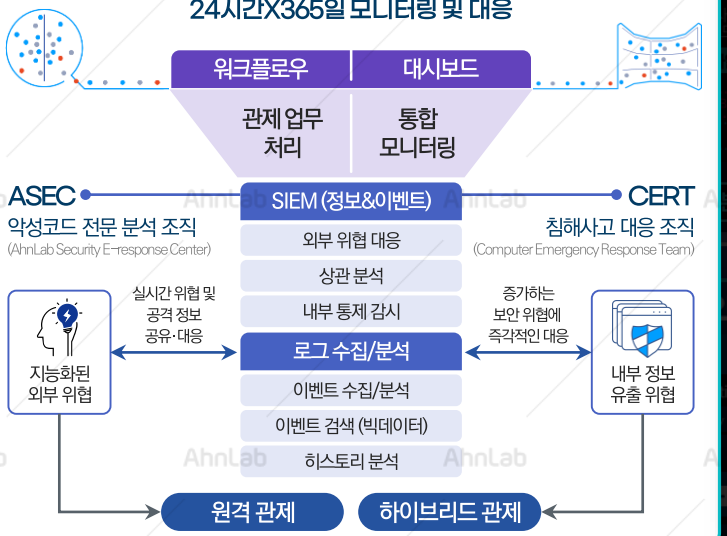
※ SCADA, HMI는 AhnLab EPS/Xcanner를 통한 엔드포인트의 식별/탐지/대응을 제공합니다.



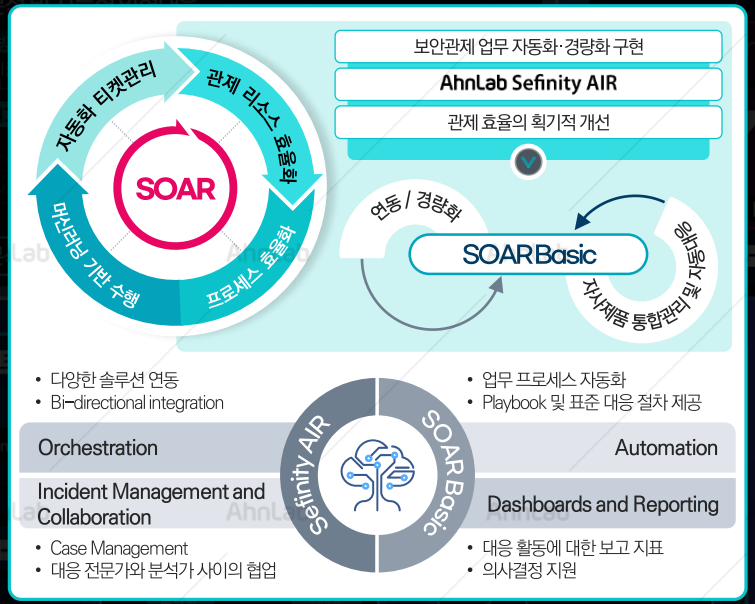
보안관제 / 자동화&오케스트레이션 영역

보안 관제

자체 시큐리티대응센터(ASEC)와 침해사고대응팀(CERT)을 통한
24시간X365일 모니터링 및 대응



자동화&오케스트레이션 (SOAR)

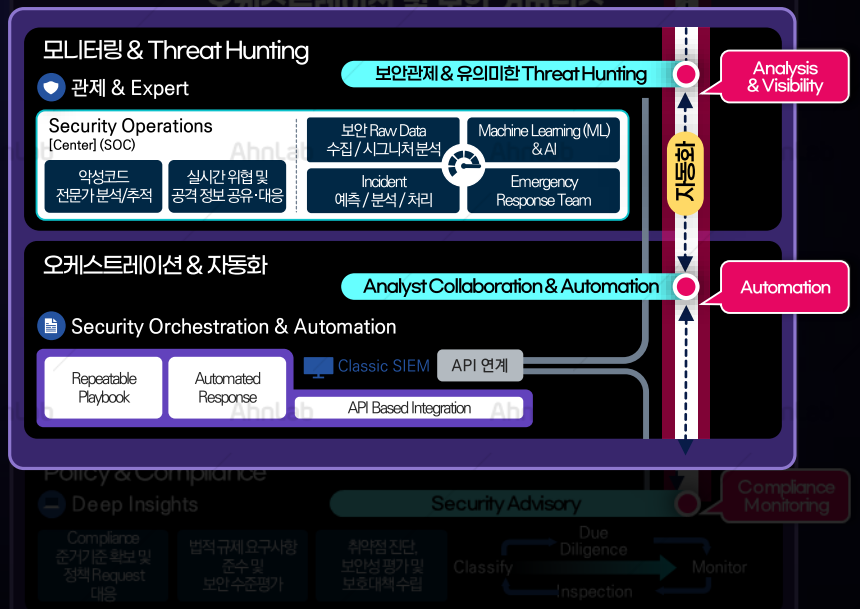


AI이상징후 탐지

JASON JMachine — AI 이상징후 탐지

빅데이터 + AI

JMachine



Professional Service

보안 솔루션 운용 최적화	보안 위협 분석·대응	정보보안 교육
데이터 분석 서비스	의심 시스템 진단 서비스	AhnLab Professional Service
전문가 온디멘드 서비스	악성코드 전문가 분석 서비스	정보보안 교육 서비스
보안 감사 사전 점검 서비스	A-FIRST 포렌식 서비스	

정보보호 컨설팅 영역

기술적 진단

기술진단 컨설팅

기술진단 컨설팅	
ICS 보안컨설팅	모바일앱 보안 진단
시스템/웹 취약점 진단	APT 이메일 모의훈련
모의해킹 컨설팅	DDoS 공격 모의훈련

시뮬레이션 진단 — 안전성 검증

다양한 위협요소를 사전 도출하고 대응방안을 제시

정보보호 체계 종합적 진단

- 보안진단을 통해 위협을 분석하고, 대책을 수립하여 최적의 정보보호 시스템을 구축하기 위한 방안을 제시

개인정보보호 및 인증지원

개인정보보호 & 인증

개인정보 컨설팅	인증 지원 컨설팅
개인정보보호 컨설팅	PIA (개인정보영향평가)
개인정보 보유·노출 검색 포렌식	ISMS-P
개인정보 수탁업체 보안진단	ISO/IEC 27001

관리체계 확보 — PIA 대응

개인정보 생명주기에서의 문제점 도출 및 개선

개인정보보호 관리체계 진단

- 조직의 개인정보보호 현황을 진단하고 개인정보 관리 프로세스, 인적·물적 자원, 법적 요구사항을 파악하여 안전한 개인정보 처리 전략을 제시

컴플라이언스 진단

컴플라이언스 대응

컴플라이언스 진단 컨설팅
주요정보통신기반시설 보호
전자금융기반시설 취약점 분석·평가
정보보호 종합 컨설팅

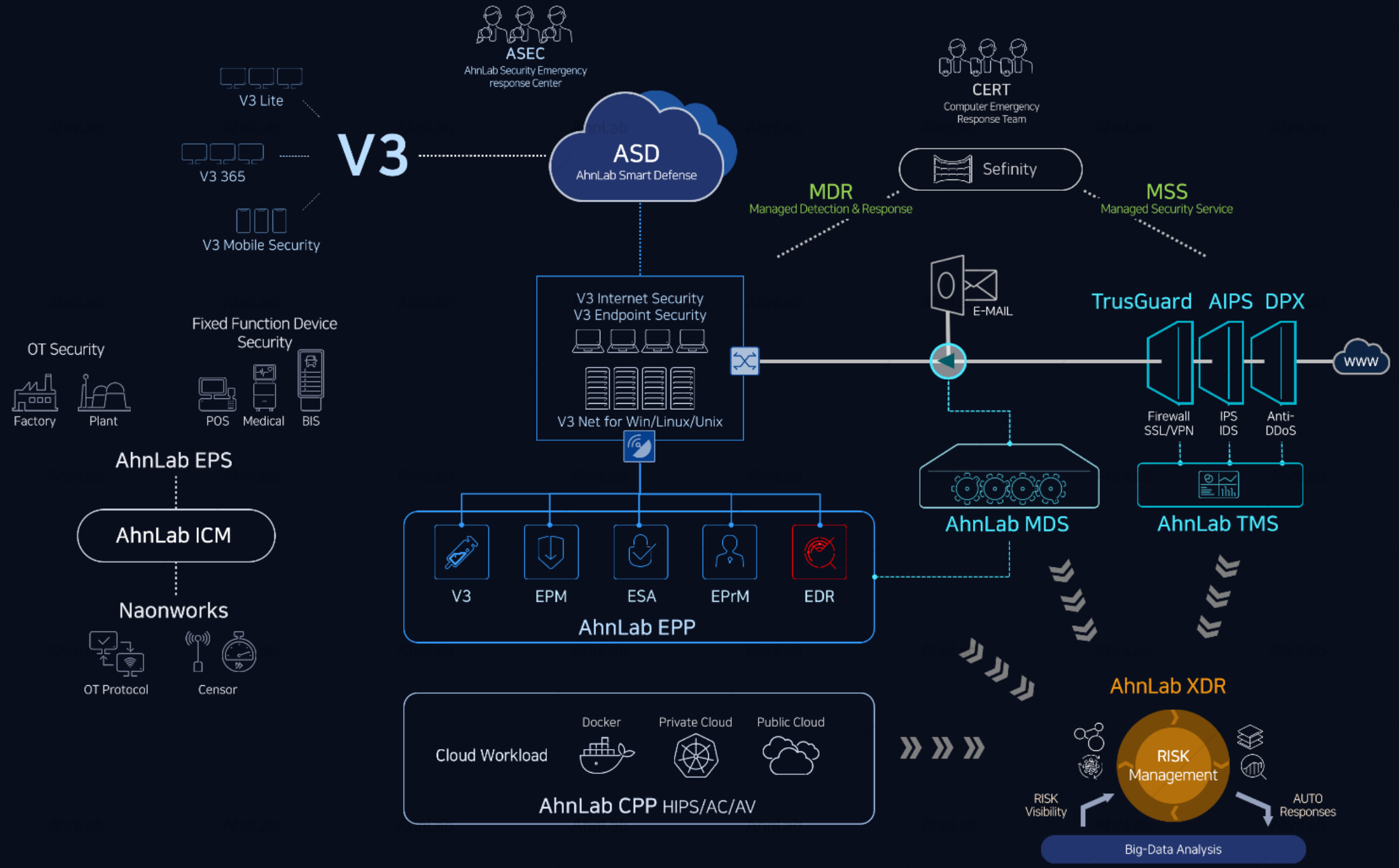
법적 준거성 확보 — 준거기준 대응

정보보호 관리체계의 법적 안정성 확보

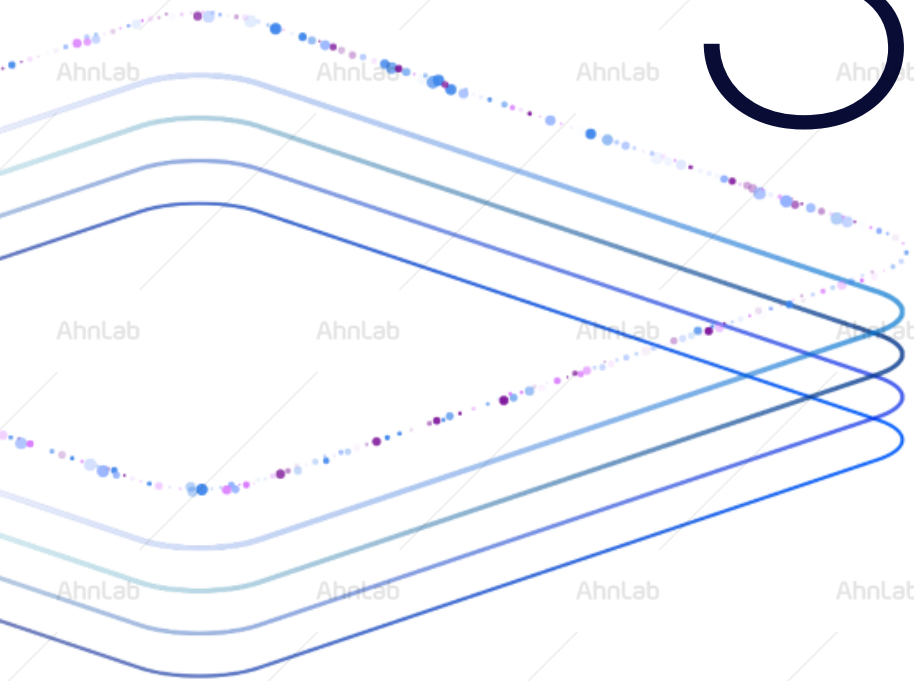
법제도적 정책·지침·절차수정 및 보완

- 조직의 정보보호 관리체계에 대한 외부기관의 객관적인 평가를 취득할 수 있도록 지원하는 서비스

AhnLab Product & Service



MORE SECURITY
MORE FREEDOM



3 Case별로 살펴본 주요 대응전략

Case #1 ___ 사회공학기법을 활용한 지능화 공격에 대한 대응체계

Case #2 ___ 랜섬웨어 다단계 대응체계

Case #3 ___ 침해사고 대응을 위한 상시 모니터링 체계

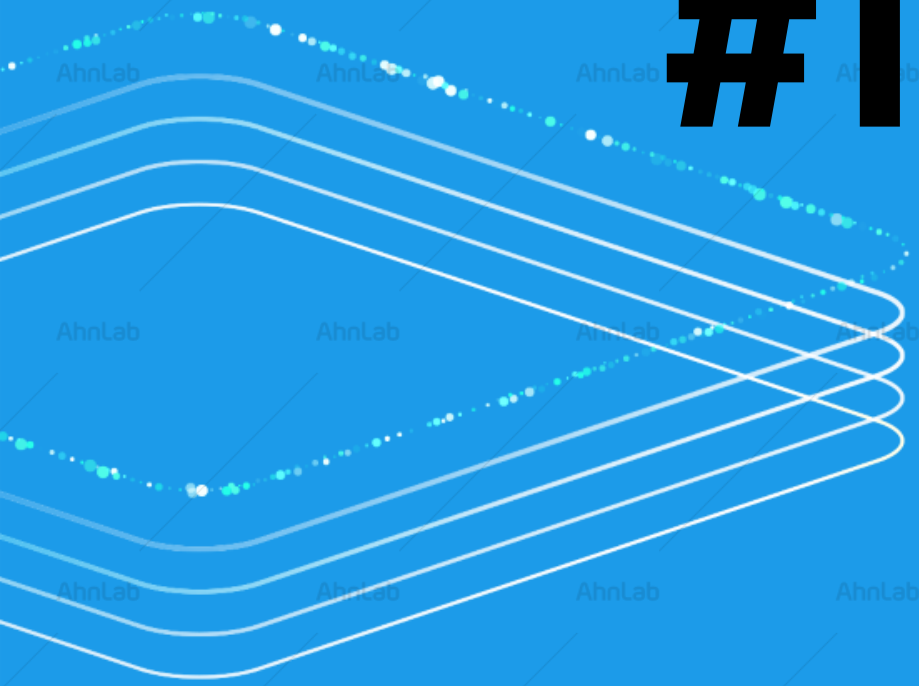
Case #4 ___ SOAR Basic 활용 AhnLab 솔루션 연계 및 자동화

안랩의 보안 아키텍처를 담은
AhnLab 통합 솔루션/서비스 맵

Case별로 살펴본 주요 보안대응전략

AhnLab

MORE SECURITY
MORE FREEDOM



3-1. Case #1 사회공학기법을 활용한 지능화 공격에 대한 대응체계

1 _____ 사회공학기법의 공격
2 _____ 무엇이 문제인가?
3 _____ 어떻게 대응할 것인가?
4 _____ 문제해결 솔루션 조합
5 _____ 통합적 스피어피싱 대응 전략
6 _____ 사회공학기법 공격 대응 체계의 완성

1 사회공학기법의 **공격**

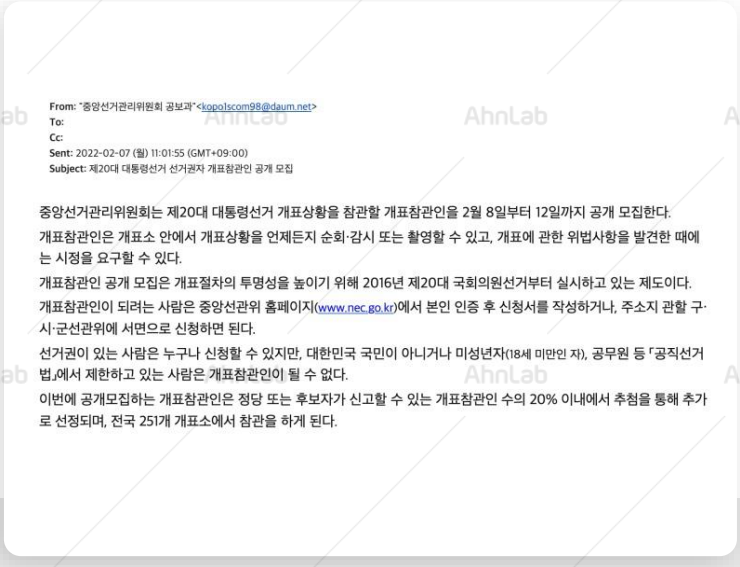
MORE SECURITY
MORE FREEDOM

1 사회공학기법의 공격

MORE SECURITY
MORE FREEDOM

Case #1 대통령 선거 관련 스피어 피싱

사용자를 속이는 메일 발송



From: "중앙선거관리위원회 공보과"<kopo1scom98@daum.net>
To:
Cc:
Sent: 2022-02-07 (월) 11:01:55 (GMT+09:00)
Subject: 제20대 대통령선거 선거권자 개표참관인 공개 모집

중앙선거관리위원회는 제20대 대통령선거 개표상황을 참관할 개표참관인을 2월 8일부터 12일까지 공개 모집한다.

개표참관인은 개표소 안에서 개표상황을 언제든지 순회·감시 또는 촬영할 수 있고, 개표에 관한 위법사항을 발견한 때에는 시정을 요구할 수 있다.

개표참관인 공개 모집은 개표절차의 투명성을 높이기 위해 2016년 제20대 국회의원선거부터 실시하고 있는 제도이다.

개표참관인이 되려는 사람은 중앙선관위 홈페이지(www.nec.go.kr)에서 본인 인증 후 신청서를 작성하거나, 주소지 관할 구·시·군선관위에 서면으로 신청하면 된다.

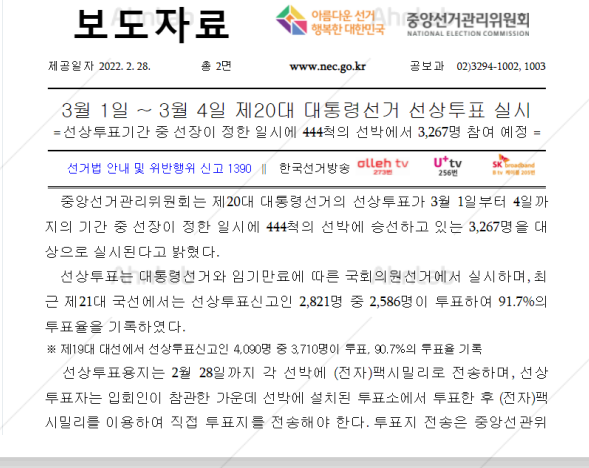
선거권이 있는 사람은 누구나 신청할 수 있지만, 대한민국 국민이 아니거나 미성년자(18세 미만인 자), 공무원 등 「공직선거법」에서 제한하고 있는 사람은 개표참관인이 될 수 없다.

이번에 공개모집하는 개표참관인은 정당 또는 후보자가 신고할 수 있는 개표참관인 수의 20% 이내에서 추첨을 통해 추가로 선정되며, 전국 251개 개표소에서 참관을 하게 된다.

공격 방식 사회공학기법을 이용한 스피어 피싱

대응 방안 사용자 보안의식 강화

사용자 첨부파일 실행 유도



보도자료

아름다운 선거 행복한 대한민국 중앙선거관리위원회 NATIONAL ELECTION COMMISSION

제공일자 2022. 2. 28. 총 2면 www.nec.go.kr 공보과 02)3294-1002, 1003

3월 1일 ~ 3월 4일 제20대 대통령선거 선상투표 실시

= 선상투표기간 중 선장이 정한 일시에 444척의 선박에서 3,267명 참여 예정 =

선거법 안내 및 위반행위 신고 1390 ‖ 한국선거방송 olleh tv U+tv SK broadband

중앙선거관리위원회는 제20대 대통령선거의 선상투표가 3월 1일부터 4일까지의 기간 중 선장이 정한 일시에 444척의 선박에 승선하고 있는 3,267명을 대상으로 실시된다고 밝혔다.

선상투표는 대통령선거와 임기만료에 따른 국회의원선거에서 실시하며, 최근 제21대 국선에서는 선상투표신고인 2,821명 중 2,586명이 투표하여 91.7%의 투표율을 기록하였다.

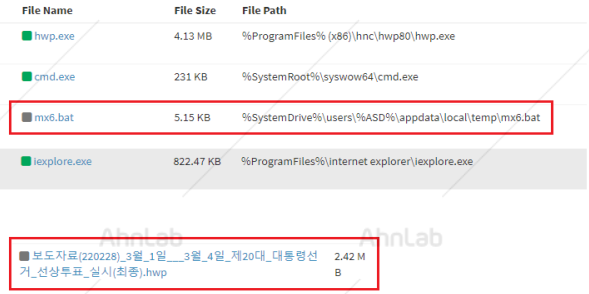
※ 제19대 대선에서 선상투표신고인 4,090명 중 3,710명이 투표, 90.7%의 투표율 기록

선상투표용지는 2월 28일까지 각 선박에 (전자)팩시밀리로 전송하며, 선상투표자는 입회인이 참관한 가운데 선박에 설치된 투표소에서 투표한 후 (전자)팩시밀리를 이용하여 직접 투표지를 전송해야 한다. 투표지 전송은 중앙선관위

공격 방식 사회공학기법을 이용한 첨부파일

대응 방안 APT 대응 솔루션을 통한 메일방역 체계 강화

응용프로그램 취약점을 이용한 침해공격 파일 실행



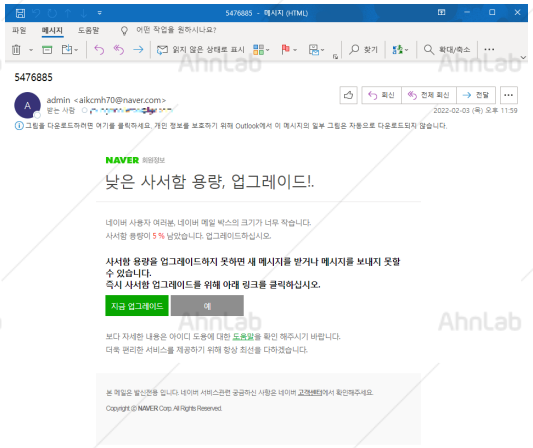
File Name	File Size	File Path
hwp.exe	4.13 MB	%ProgramFiles% (x86)\hnc\hwp80\hwp.exe
cmd.exe	231 KB	%SystemRoot%\syswow64\cmd.exe
mx6.bat	5.15 KB	%SystemDrive%\users\%ASD%\appdata\local\temp\mx6.bat
iexplore.exe	822.47 KB	%ProgramFiles%\internet explorer\iexplore.exe
보도자료(220228)_3월_1일___3월_4일_제20대_대통령선거_선상투표_실시(최종).hwp	2.42 MB	

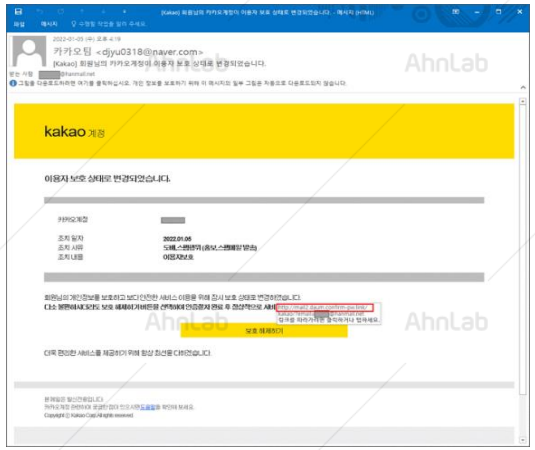
공격 방식 Endpoint 취약점을 노리는 공격

대응 방안 Endpoint 취약점 제거

Case #2 사용자의 관심 사항에 대하여 클릭을 유도하는 스피어 피싱

사용자를 속이는 메일 발송





피싱사이트를 통한 로그인 계정 정보 탈취

공격 방식 사회공학기법을 이용한 스피어 피싱

대응 방안 사용자 보안의식 강화

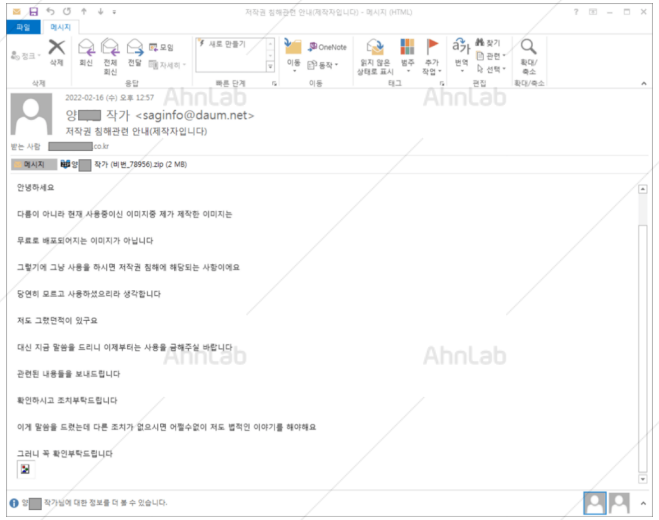
공격 방식 사용자 정보 입력 유도를 통한 계정정보 탈취

대응 방안 사용자 보안의식 강화

MORE SECURITY
MORE FREEDOM

Case #3 사용자에게 위법사항을 거짓으로 협박하는 피싱 메일

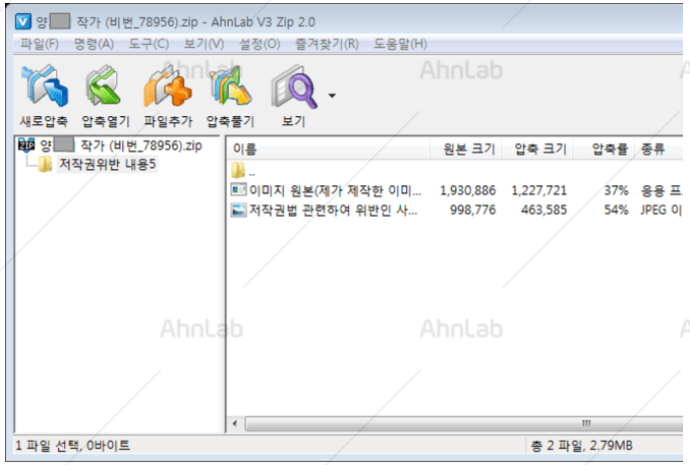
사용자에게 거짓 협박 메일 발송



공격 방식 ○ 사회공학기법을 이용한 스피어 피싱

대응 방안 ○ 사용자 보안의식 강화

스팸차단 솔루션을 우회하기 위한 암호 압축파일 첨부



공격 방식 ○ 스팸차단 솔루션 우회

대응 방안 ○ APT 대응 솔루션을 통한 메일방역 체계 강화

응용프로그램 취약점을 이용한 침해공격 파일 실행

공격 방식 ○ 사용자의 낮은 보안 의식 및 Endpoint 취약점을 노리는 공격

대응 방안 ○ 사용자 보안의식 강화 Endpoint 취약점 제거

기존 스팸차단 솔루션의 명확한 한계

대부분 구축되어 운영되고 있는 스팸차단 솔루션은
최신 사회공학기법을 활용한 공격에 대응 불가

기존 스팸차단 솔루션

광고성 스팸 차단
단순 악성코드 차단

사회공학기법

시스템의 취약점을 노린
사회공학기법에 취약

해결책 체계 개선

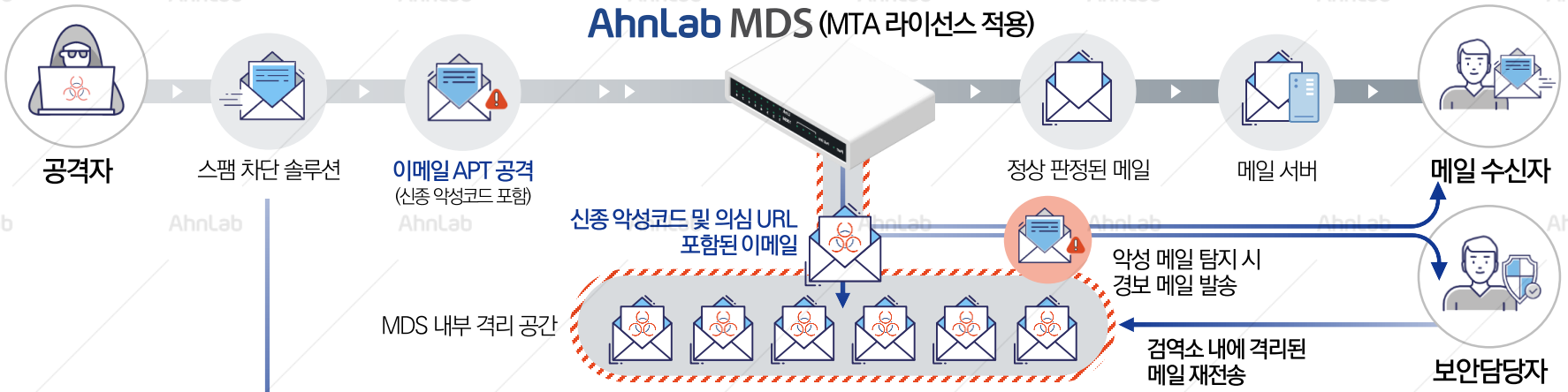
침투공격을 정밀하게
탐지 - 분석 - 대응할 수 있는
지능형 위협대응 솔루션 필요

3 어떻게 대응할 것인가?

MORE SECURITY
MORE FREEDOM

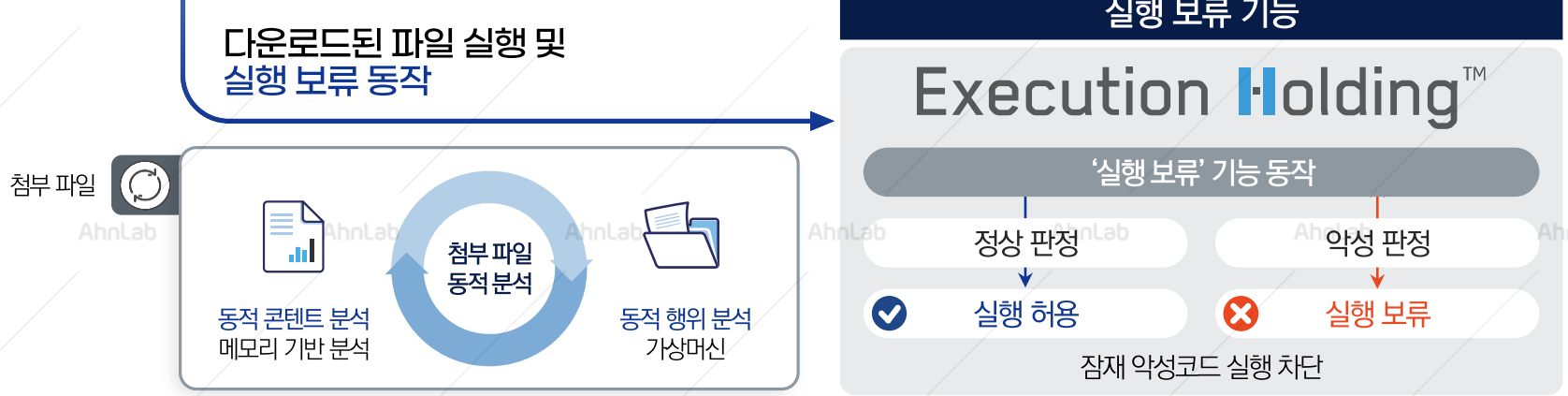
대응방안. 01

이메일 격리



대응방안. 02

실행 보류

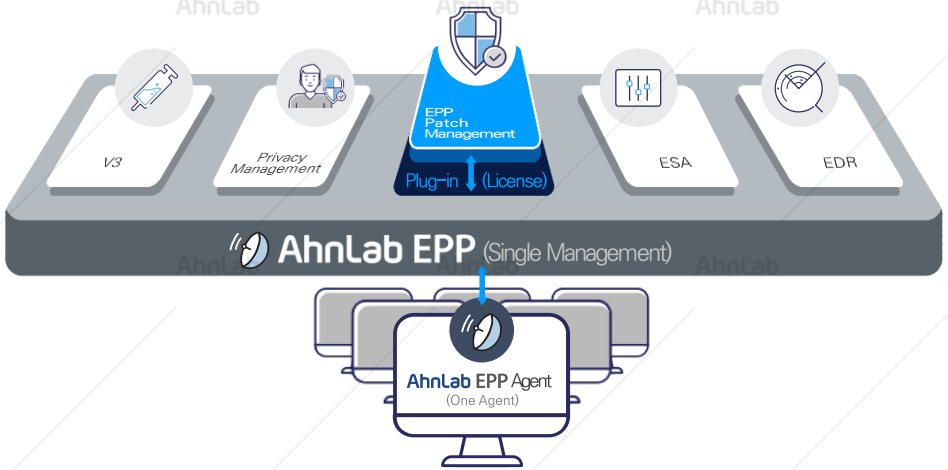


3 어떻게 대응할 것인가?

MORE SECURITY
MORE FREEDOM

대응방안. 03

실시간 패치관리



패치관리 필요

- 각종 보안 패치에 대한 실시간 관리
- 보안 정책을 위반한 엔드포인트 시스템에 대한 중앙 관리 및 조치
- 보안 솔루션 연계를 통한 엔드포인트 시스템 하드닝(System Hardening)
- Patch Lab을 통해 검증·분석한 안전한 패치적용

대응방안. 04

상태점검 및 자동조치

보안상태 점검 ▶ 자동조치 실시

상태점검 및 자동조치

- 정책에 따라 모든 개별 PC의 보안 상태를 안전하게 유도 및 관리
- 취약항목의 자동조치를 통해 전반적인 보안 수준을 강화(hardening)
- 취약점 자동/강제 조치
  - 취약한 PC의 네트워크 차단
  - 실시간 강제 점검 명령 수행

4 문제해결 솔루션 조합

MORE SECURITY
MORE FREEDOM

이메일 격리

샌드박스 기반의 지능형 위협 대응 솔루션

이메일 기반 공격 대응

- 이메일 격리 기능
- 이메일 필터링 연계

실행 보류

네트워크 기반 공격 대응

- 이상 트래픽 탐지 및 차단

엔드포인트 기반 공격 대응

- 악성코드 삭제 / 실행 보류
- 의심 파일 추출
- 시스템 격리

AhnLab MDS

AhnLab EPP Patch Management

- 구축 및 확장 **편의성**
- 믿을 수 있는 **패치 안전성**
- **플랫폼 기반**의 효율적인 통합 관리
- 폭넓은 패치 **지원 범위**
- 편리한 **모니터링** 및 다양한 **리포트**
- **가시성 기반**의 패치 및 SW 관리

실시간 패치관리

AhnLab EPP Security Assessment

- **원클릭**으로 쉽고 간편하게
- 효율적인 엔드포인트 **취약점 관리**
- 관리자와 PC사용자의 **업무 효율성 극대화**

중앙에서 개별 PC의 **보안 상태를 한 눈에 파악**	다양한 취약점에 대한 **사전 대응 조치 가능**	정보보안 관련 규제 **대응 및 준수**

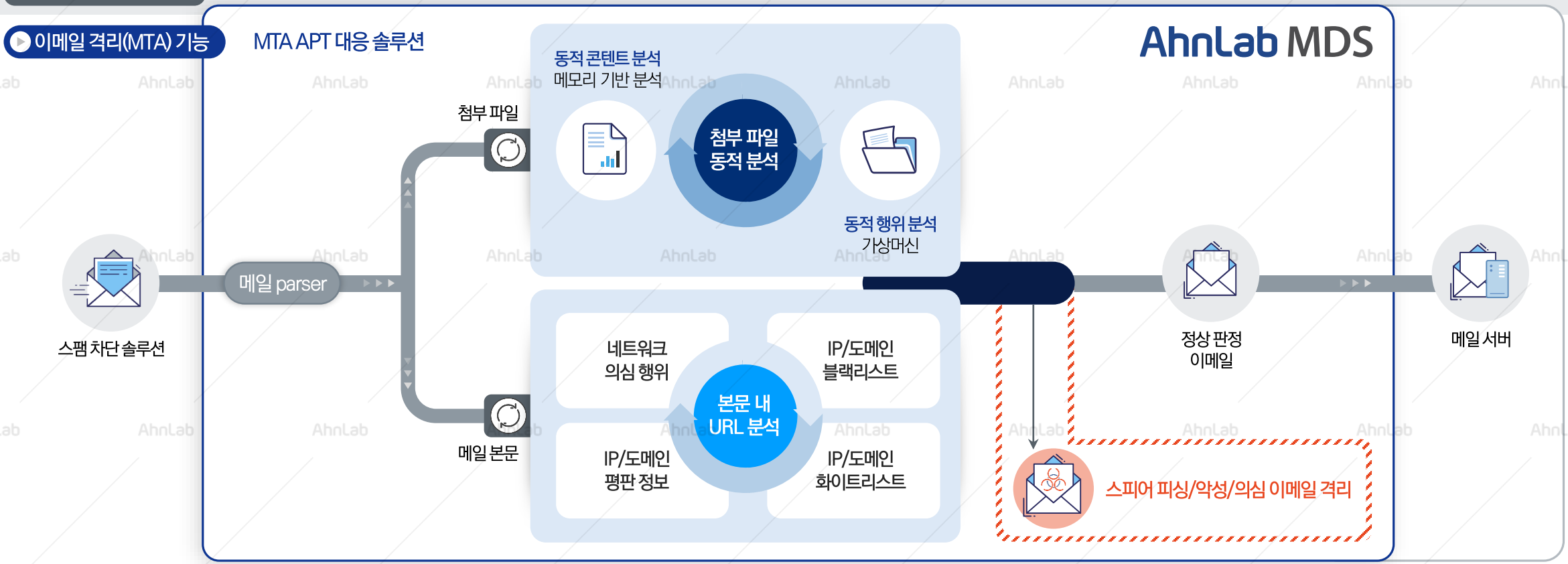
상태점검 및 자동조치

5 통합적 스피어 피싱 대응 전략 > ① Network 영역

MORE SECURITY
MORE FREEDOM

Network 영역

- MTA APT 대응 솔루션 구축 :
  Unknown 악성코드, 암호 압축파일, 악의적 URL 등 APT 공격 기법을 사용하는 스피어 피싱 메일 대응



5 통합적 스피어 피싱 대응 전략 > ② Endpoint 영역 (1/2)

MORE SECURITY
MORE FREEDOM

Endpoint 영역

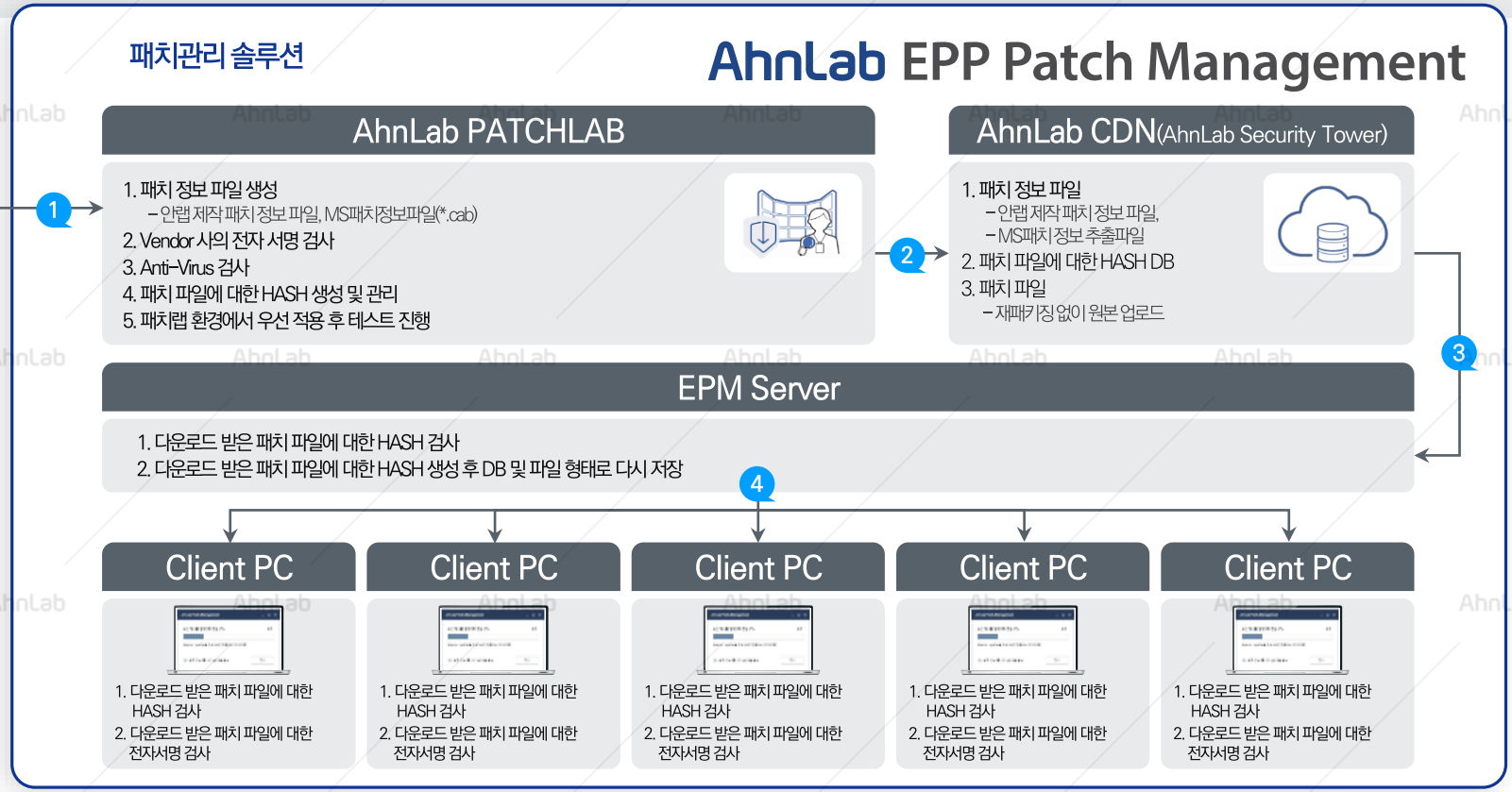
- PMS 솔루션 구축 : 운용체제 및 응용프로그램에 대한 보안패치 실행
- Zero-Day 취약점 해결을 위한 상시 관리 모니터링

Endpoint PMS 기능

OS/Application Vendor

Microsoft, ORACLE, 한글과컴퓨터, Adobe, ETC…

구분		상세버전
운영체제 (OS)	Windows Desktop	– Windows XP SP3/Vista/7/8(8.1)/10/10 IoT Enterprise * 상기 OS의 x86/x64 호환 모드 지원
	Windows Server	– Window Server 2008(x86/x64) / 2008R2(x64) – Window Server 2012(x64) / 2012R2(x64) – Window Server 2016(x64) – Window Server 2019(x64)
애플리케이션 (Application)	Web browser	– Internet Explorer 7/8/9/10/11 – Chrome, Firefox, Chromium Edge
	MS Office	– MS Office 2003/2007/2010/2013/2016 – 2007 Microsoft Office Suite – Microsoft Office Compatibility Pack – Microsoft Office Proofing Tools Kit 2007/2010 – MS Excel Viewer 2003/2007 – MS Word Viewer 2003 – MS Power Point Viewer 2003/2007/2010 – MS Visio Viewer 2007/2010
	Adobe Flash Player	– Adobe Flash Player – Active X – Adobe Flash Player – Chromium PPAPI
	Adobe ShockWave Player	– Adobe Shock Wave Player
	Adobe Reader	– Adobe Reader 9/10/11/DC
	Adobe AIR	– Adobe AIR
	JAVA	–JAVA SE Runtime Environment7/8/9
	.NET Framework	– .NET Framework 4.5/4.6/4.7/4.8
	한컴오피스	– 한글과 컴퓨터 한/글2007 – 한글과 컴퓨터 오피스 2007 – 한컴오피스 한/글 2010SE+ / 2014VP / NEO – 한컴오피스 2010 SE+ / 2014VP / NEO/2017
	그 외	– Windows Defender, iTunes, Bandizip



5 통합적 스피어 피싱 대응 전략 > ② Endpoint 영역 (2/2)

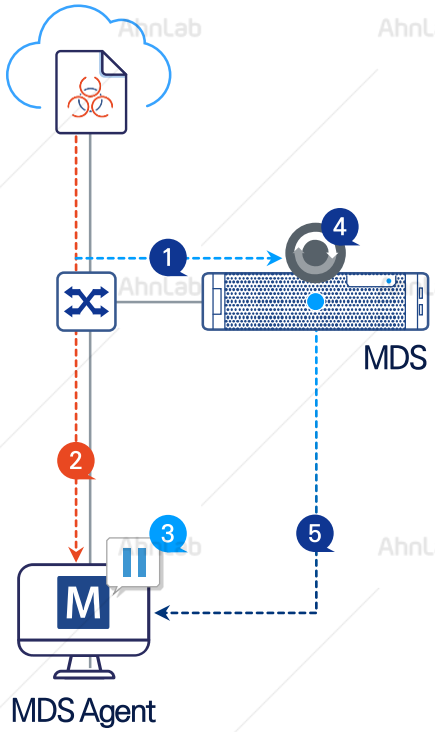
MORE SECURITY
MORE FREEDOM

Endpoint 영역

• Endpoint APT 솔루션 구축 :
실행보류를 통한 Unknown 악성코드 실행 차단

Endpoint Agent 기능

Endpoint APT 솔루션



1 트래픽 미러링 및 분석 시작

2 PC내 파일 다운로드

분석 소요 시간

1 다운로드된 파일 실행 및 실행 보류 동작

4 분석 완료 및 악성 판정

5 삭제 명령 전달

대응 소요 시간

AhnLab MDS

Execution Holding™

실행 보류 기능

'실행 보류' 기능 동작

정상 판정 → 실행 허용

악성 판정 → 실행 보류

잠재 악성코드 실행 차단

5 통합적 스피어 피싱 대응 전략 > ③ 사용자 영역

MORE SECURITY
MORE FREEDOM

사용자 영역

- **Endpoint Security Assessment 솔루션 구축 :** 상시 Endpoint 취약점 자가점검 및 조치 활동 등을 통한 자가주도 보안 활동
- **정보보안 교육 및 자가주도 보안활동 설문 실행 :** 사용자 보안의식 향상을 위한 주기적인 정보보안 교육 및 설문 조사

Endpoint 보안 취약점 점검 솔루션

AhnLab EPP Security Assessment

- 자가주도 보안 활동
- 주기적 설문을 통한 보안의식 향상

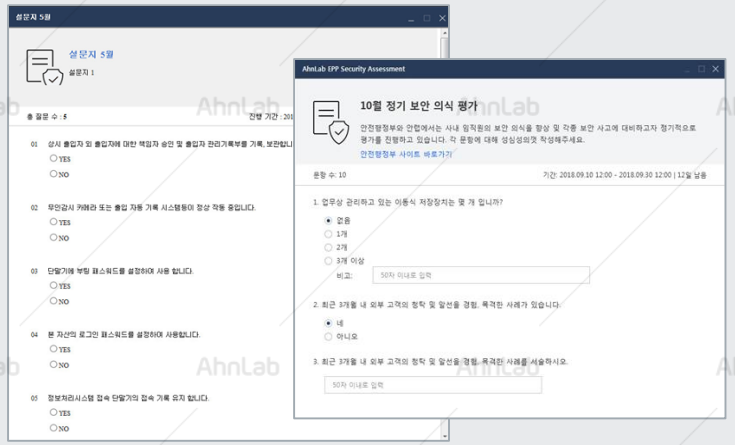
기본 점검 항목 15

보안 업데이트 4개	• 악성코드 백신 설치 및 실행 점검 • 악성코드 백신의 최신 보안 패치 점검 • 운영체제, MS Office의 최신 보안 패치 설치 여부 점검 • 한글 프로그램 최신 보안 패치 설치 여부 점검
패스워드 안전성 2개	• 로그온 패스워드 안전성 여부 점검 • 로그온 패스워드의 분기 1회 이상 변경 여부 점검
화면보호기, 공유폴더 설정 2개	• 화면보호기 설정 여부 점검 • 사용자 공유 폴더 설정 여부 점검
보안 프로그램 설치 2개	• USB 자동 실행 허용 여부 점검 • 미사용(3개월) ActiveX 프로그램 존재 여부 점검
관리자 추가 항목 5개	• PDF 프로그램의 최신 보안 패치 설치 여부 점검 • 편집 프로그램(MS 워드, 한글, PDF) 설치 여부 점검 • 무선랜 카드 설치 점검 • 보안 USB 설치 여부 점검 • 비인가 프로그램 설치 여부 점검

확장 점검 항목 52

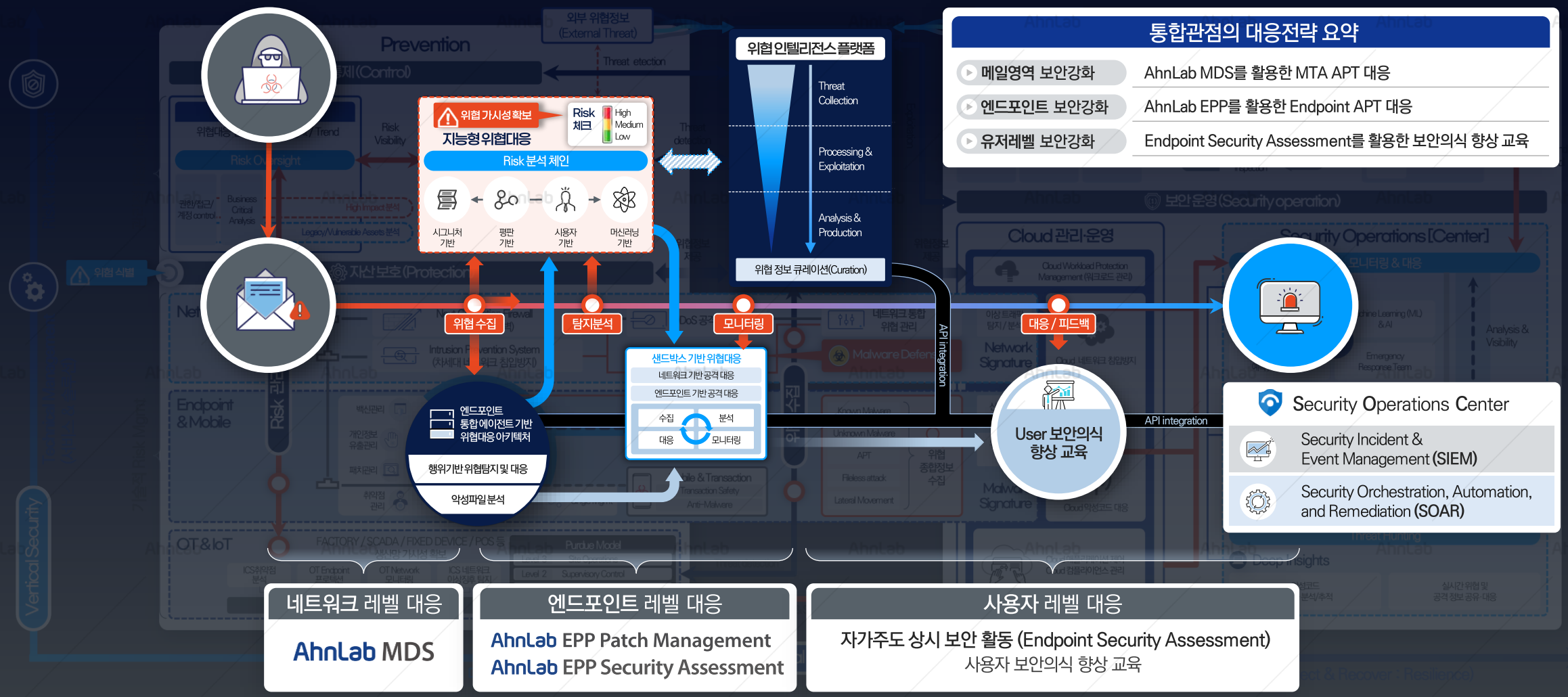
계정 설정 점검 8개	• 윈도우 자동 로그온 • 장기 미접속 계정 존재 여부 점검 • Guest 계정, Administrator 계정 사용 점검
로컬 보안 정책 점검 3개	• 패스워드 최대/최소 사용 기간 설정 여부 점검 • Windows 로그온 실패 횟수 초과 시 계정 잠금 설정 여부 점검
윈도우 설정 점검 5개	• Windows 자동 업데이트 설정 여부 점검 • 사용자 계정 컨트롤(UAC) 사용 여부 점검 • 모든 미디어 및 장치 자동 실행 설정 점검
네트워크 설정 점검 12개	• 원격 데스크톱 포트 변경 • 인터넷 연결 공유 여부 점검 • Hosts 파일 내 비허용 IP 점검, 비허용 DNS 설정 점검 • 방화벽 사용/웹서비스 실행 FTP 서비스 실행 점검
웹 브라우저 설정 점검 14개	• IE 자동 암호 입력 여부, 자동 로그인 설정 여부 • IE ActiveX 컨트롤 및 플러그인 실행 점검 • IE 신뢰할 수 있는 사이트 목록의 취약성 점검
기타 점검 항목 10개	• 전체 공유 권한의 공유 폴더 사용 점검 • 모든 미디어 및 장치 자동 실행 설정 점검 • 장치 드라이버 설치 시 서명 점검 • Adobe Flash Player, Adobe Air, JAVA(jre) 최신 보안 패치 여부 점검

설문 생성 및 배포

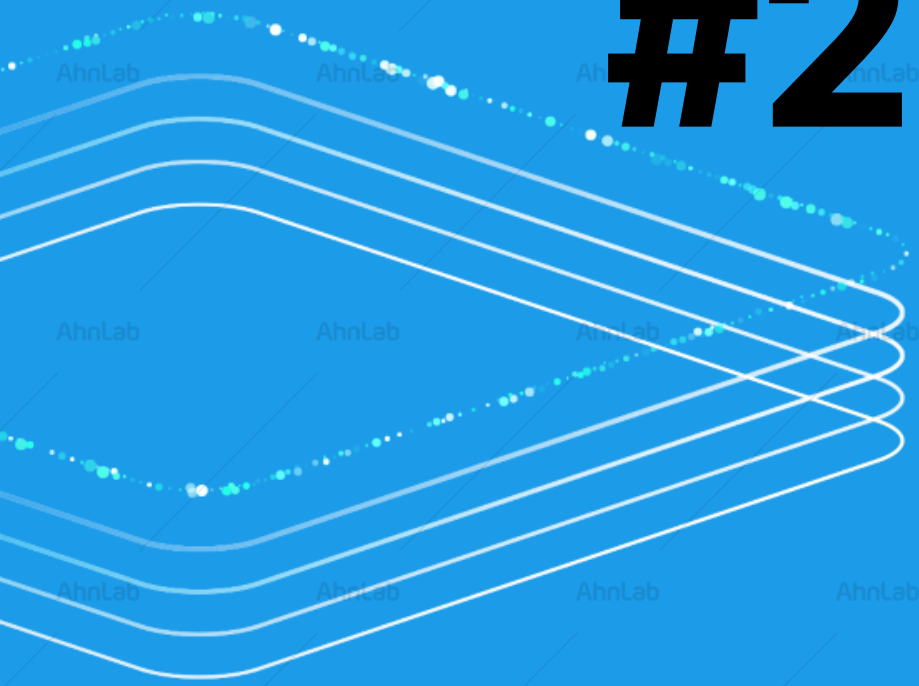


6 사회공학기법 공격의 대응체계 완성

MORE SECURITY
MORE FREEDOM



MORE SECURITY
MORE FREEDOM



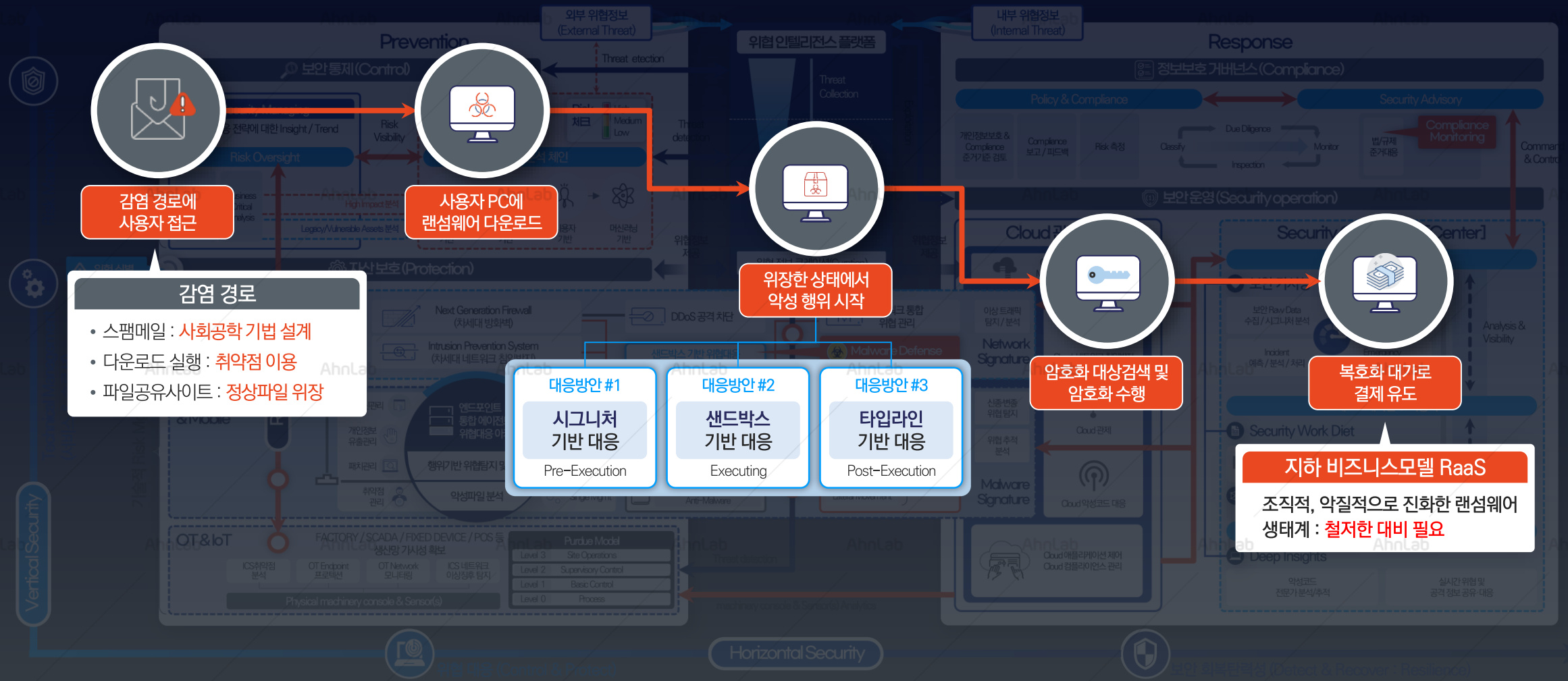
3-2. Case #2

신종 랜섬웨어 다단계 대응 체계

1 _____ 신종 랜섬웨어의 감염경로
2 _____ 랜섬웨어 주요 공격 유형
3 _____ 무엇이 문제인가?
4 _____ 어떻게 대응할 것인가?
5 _____ 문제해결 솔루션 조합
6 _____ 랜섬웨어 대응체계 완성

1 신종 랜섬웨어의 **감염경로**

MORE SECURITY
MORE FREEDOM



2 랜섬웨어 주요 공격전술 유형

MORE SECURITY
MORE FREEDOM

Attack Case 01

- 피싱(Phishing) 사이트 접속
- 사용자 열람 유도 문서파일
- 다운로드 링크 삽입
- 암호화 압축파일, 문서 첨부

Attack Case 02

- 워터링 홀 (Watering Hole)
- RDP (Remote Desktop Protocol)
- 무료 유틸리티 툴 배포 사이트
- 웹 브라우저 취약점

Attack Case 03

- USB, 외장디스크
- OS 취약점을 통한 내부 확산
- BitLocker
- VPN 계정 탈취

2 랜섬웨어 주요 공격전술 유형 > ① Network

MORE SECURITY
MORE FREEDOM

워터링 홀 (Watering Hole)

- 기업/기관에서 **업무 관련 접속할 가능성이 높은 사이트를 해킹해 악성코드를 유포**하는 방법
- 불특정 다수를 대상으로 하지 않고 **특정 타켓을 목적**으로 하기 때문에 감염 성공 시 랜섬웨어 공격 시도할 가능성이 높음

RDP (Remote Desktop Protocol)

- 네트워크 스캔을 통해 **오픈 된 외부 시스템(원격 데스크탑)의 포트 정보를 수집 및 인증 시도**하여 시스템 접속
- **핵심 서버 확인 후 랜섬웨어 공격**을 시도하며, 이미 노출된 수 만대의 RDP 정보(IP, 인증정보)가 다크웹을 통해 거래

무료 유틸리티 툴 배포 사이트

- 검색 포탈을 통하거나 직접 웹 사이트를 운영하면서 **유틸리티 툴을 가장한 악성코드를 만들어 유포** (PDF 변환, 유튜브 동영상 다운로드 프로그램 등)
- **프로그램 설치와 함께 악성코드도 설치**되며 사용자 PC에 일정기간 잠복 후 랜섬웨어 감염 시도

웹 브라우저 취약점 (Fileless Attack)

- **웹 브라우저(IE, 크롬 등) 취약점을 이용**하여 정상 사이트 내 광고배너 또는 평판도가 낮은 사이트에 취약점 코드(악성코드)를 삽입
- **사이트 접속 시 강제로 랜섬웨어 동작 코드를 삽입**하여 PC의 파일을 암호화하며, 파일기반 분석 보안솔루션에서는 대응 불가

피싱(Phishing) 사이트 접속

- 메일 또는 첨부 문서의 링크를 통해 **피싱 사이트로 접속하여 이메일 계정 및 패스워드를 입력**하도록 유도
- **입력된 계정 정보는 공격자 DB에 저장**되어 해당 계정으로 랜섬웨어를 발송하거나 업무메일로 위장된 스캠(금융사기) 메일 발송

사용자 열람을 유도하는 문서파일

- 이력서, 고발장, 범칙금 등 **업무관련 문서로 위장된 악성 문서파일**을 메일로 발송
- 사용자가 문서 열람 시 **문서에 포함된 악성 매크로 또는 본문에 삽입된 악성코드 실행을 유도**하여 랜섬웨어 공격 및 암호화 동작을 수행

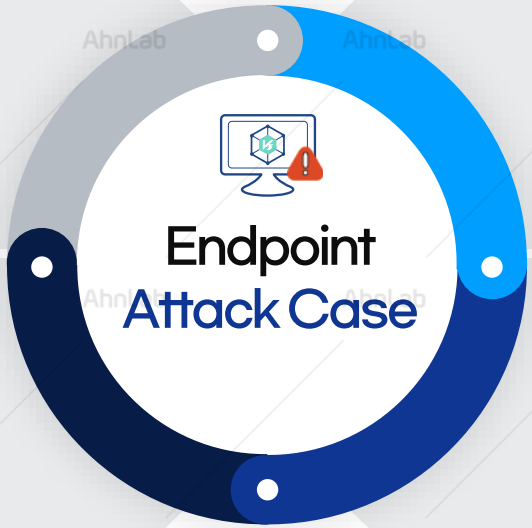
다운로드 링크 삽입

- 업무 또는 정상 메일로 위장된 **메일에 대용량 다운로드 또는 단축 URL로 변환한 파일 다운로드 링크를 삽입**하여 발송
- **보안솔루션 탐지 우회**를 위해 정상 파일 첨부링크를 야간에 메일 발송 후 업무시간에 악성코드로 교체하는 **시간차 공격 방법**도 존재

암호화 압축, 암호화 문서 첨부

- 메일 제목이나 본문에 패스워드를 기록하고 **암호화 압축 또는 패스워드 걸린 문서파일 첨부**
- 사용자가 **암호화 압축을 해제 후 파일 실행 시** 랜섬웨어에 감염 (주로 egg, alz 압축 확장자를 사용)

MORE SECURITY
MORE FREEDOM



USB, 외장디스크

- 외부에 일부러 흘린 **악성코드에 감염된 USB**를 기업 내부 사용자가 USB를 습득한 후 **내부 반입하여 PC에 연결하도록 유도**
- **PC에 연결한 USB는 모두 악성코드에 감염**되며, USB를 연결한 **다른 PC에도 동일하게 악성코드를 확산**

OS 취약점을 통한 내부 확산

- **OS 취약점**을 이용해 동일 네트워크에 연결된 PC간 악성코드 유포 및 설치되며, **단시간에 대량의 PC를 대상으로 감염 확산**
- **최신 패치가 되어 있지 않은 시스템**이 많을수록 **제로데이 취약점에 치명적**이므로 더욱 주의가 필요

BitLocker

- BitLocker는 Windows에서 기본으로 제공하는 **디스크 암호화 기능**이며, 패스워드 인증 이후에 USB나 디스크 드라이브가 활성화
- BitLocker 기능을 활용해 랜섬웨어 악성코드 없이, 주요 데이터가저장되거나 서비스 운영중인 **시스템의 디스크 및 드라이브를 암호화하고 패스워드 제공 비용을 요구**

VPN 계정 탈취

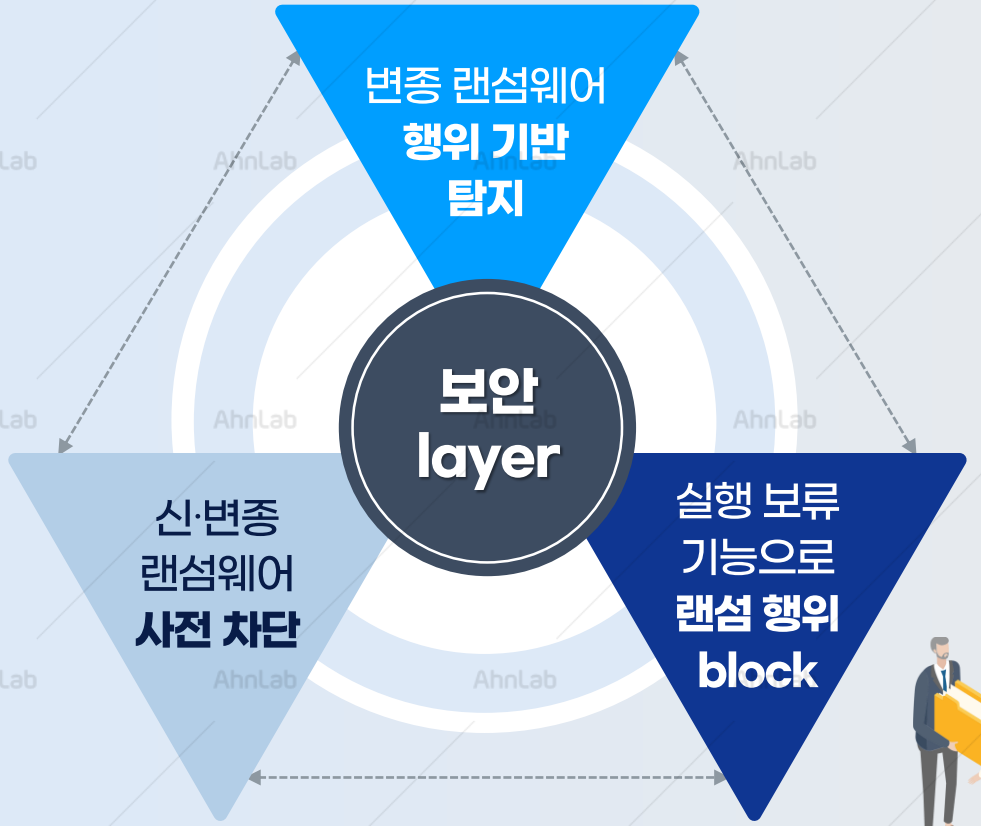
- 재택근무 환경 확산으로 **외부에서 VPN을 통해 내부 업무시스템에 접속**하여 업무를 진행
- 재택 근무 PC에 악성코드를 설치하여 **VPN 계정 정보를 탈취**하고, **내부 주요 시스템 접근권한 획득 및 랜섬웨어 공격**을 시도함

3 무엇이 문제인가?

MORE SECURITY
MORE FREEDOM

기존 보안솔루션	한계점
Firewall & NGFW	허용된 주소, 프로토콜, 어플리케이션을 통한 랜섬웨어 유입 차단 불가
IDS & IPS	탐지 패턴화 되지 않은 신·변종 랜섬웨어 탐지 불가
AV	신·변종 랜섬웨어 탐지 및 차단 불가
APT 솔루션 (NW sandbox)	신·변종 랜섬웨어 탐지하더라도 엔드포인트 레벨에서 랜섬 행위 피해 (파일 암호화 등) 사전 차단 불가

추가되어야 할 보안 layer



4 어떻게 대응할 것인가?

MORE SECURITY
MORE FREEDOM

대응방안. 01 시그니처 기반대응

Pre-Execution

행위기반 탐지

다차원 분석 플랫폼 기반의 행위기반 대응
- 행위 기반 평판 기반 분석 수행
- 제로데이 취약점 원천 차단
- 신/변종 악성코드까지 사전에 진단 사전 방역

V3
- V3 수동 업데이트
- 네트워크 완전 차단
- 네트워크 완전 차단 해제
- 악성코드 검사
- 시스템 최적화

AND

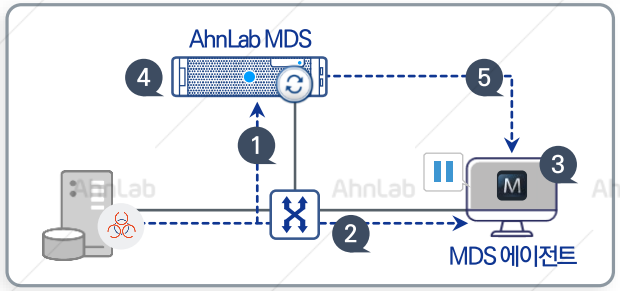
EPM
- 패치 실행
- 소프트웨어 설치 점검

엔드포인트 하드닝

실시간 패치관리 및 엔드포인트 하드닝
- 패치관리를 통한 최신 랜섬웨어 대응
- 엔드포인트 보안 솔루션 연계를 통한 엔드포인트 시스템 하드닝 (System Hardening)

대응방안. 02 샌드박스 기반 대응

Executing



랜섬웨어 실행 차단 및 '파일 암호화 등' 사전 방지

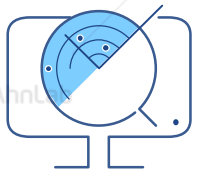
1. 트래픽 수집 및 샌드박스 분석 시작
2. PC내 랜섬웨어 의심 파일 다운로드
3. 다운로드된 의심 파일 실행 보류 동작 (Execution Holding™)
4. 샌드박스 분석 완료 및 악성 판정
5. 삭제 명령 전달

분석소요시간 ← → 대응소요시간

대응방안. 03 타임라인 기반 대응

Post-Execution

- 언제 조직 내부로 침입한 파일인가?
- 어떻게 악성코드에 감염됐는가?
- 악성코드와 유사한 파일 구조를 갖고 있는가?



타임라인 기반 정보수집

- 파일이 유입된 이후 실행된 적이 있는가?
- 동일한 파일이 얼마나 많은 시스템에 존재하는가?
- 어떤 모듈(들)과 관계 있는가?
- 어떤 행위를 했는가?

엔드포인트 위협 행위 정보 수집

행위 정보 탐지·분석을 통한 엔드포인트 가시성 확보 및 대응
- 사용자 PC에서 발생한 OS, 네트워크 이벤트 수집 및 실시간 분석으로 랜섬웨어 의심 행위 탐지
- 백신 및 APT 대응 솔루션에서 탐지된 악성 이벤트에 대한 침투경로 및 데이터 제공
- VSS 롤백 기능을 활용한 암호화 파일 복원

5 문제해결 솔루션 조합

MORE SECURITY
MORE FREEDOM

대응방안.01
시그니처 기반대응

Pre-Execution

AhnLab V3 Internet Security 9.0

행위기반 진단
Anti-Virus 엔진

AhnLab EPP Patch Management

플랫폼 기반의
패치 관리

대응방안.02
샌드박스 기반 대응

Executing

AhnLab MDS

랜섬웨어 실행 차단 및 파일 암호화 등
실행 보류(Execution Holding) 동작

Unknown file
Execution Holding™

- 의심 파일에 대한 실행 보류/차단
- 분석장비(MDS)에 파일 업로드 및 분석 요청
- 분석 결과에 따른 자동/수동 삭제 및 조치

대응방안.03
타임라인 기반 대응

Post-Execution

AhnLab EDR

행위 정보 탐지·분석을 통한
엔드포인트 가시성 확보 및 대응

사전차단

실행보류

위협헌팅

5 문제해결 솔루션 조합 (타깃 메일 발송 사례)

MORE SECURITY
MORE FREEDOM

01 스피어피싱 메일 발송

공격자

외부 인터넷

내부 네트워크

국세청 사칭 메일

04 C&C 통신 (해커 명령 전달)

스팸 솔루션

방화벽

랜섬노트 (협박 및 비용 요구)

첨부 문서 매크로 실행 유도

PE 다운로드

백도어 설치

MACRO/
VBA 실행

Ammyy
Downloader

Ammyy
Backdoor

Cobalt
Strike

AD
서버 장악

Ransomware
전사 서버/PC 유포

02 사용자 첨부문서 열람

03 해킹툴 및 백도어 설치

05 시스템 침투 및 이동

06 Ransomware 감염

5 문제해결 솔루션 조합 (타깃 메일 발송 사례)

MORE SECURITY
MORE FREEDOM

사전대응 AhnLab APT 이메일 모의훈련

내부 직원 메일 모의훈련

- 환경 분석, 시나리오 협의
- 스피어피싱 훈련 메일 발송
- 훈련 결과 및 교육 방안 가이드

Solution 01 AhnLab MDS MTA

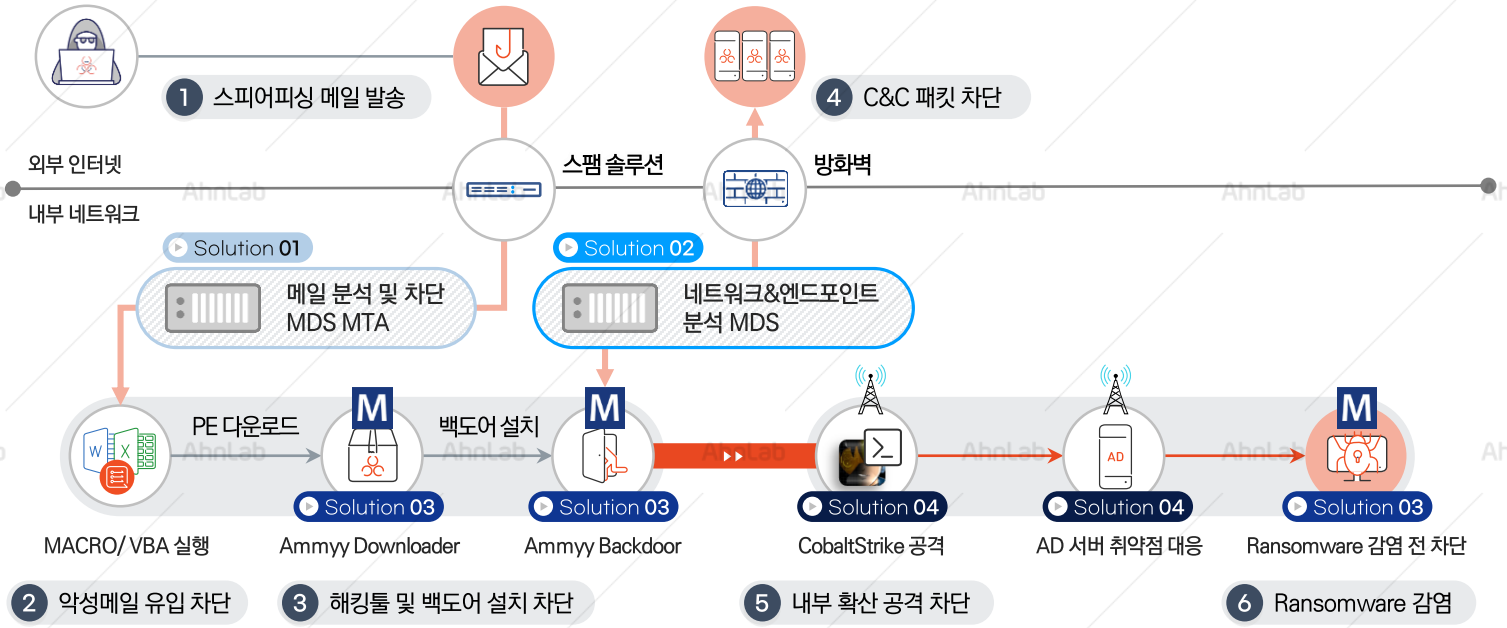
메일 실시간 분석 악성메일 격리

- 샌드박스 랜섬웨어 분석환경 탑재
- 첨부파일, 본문 링크 정적/동적 분석
- 정상 파일/링크 스케줄링 재분석
- 피싱, 스캠 메일 분석

Solution 02 AhnLab MDS

네트워크 모니터링 C&C 트래픽 탐지/차단

- 네트워크 패킷 분석, 프로토콜별 이동 파일 수집
- Blacklist 기반 악성 URL 차단
- 네트워크 취약점 트래픽 탐지
- 랜섬웨어 감염 의심 시스템, PC 감지



Solution 03 AhnLab MDS Agent

PC/서버에 설치되는 해킹 툴 탐지/차단

- PC/서버에 유입 후 실행되는 파일 실시간 검사
- 해킹툴, 백도어 설치 차단
- 알려진 & 신변종 랜섬웨어 샌드박스 분석
- 랜섬웨어 감염 전 차단

Solution 04 AhnLab EPP/ESA/EPM

AD 서버 확산 공격 대응/PC Hardening

- OS 패스워드 복잡도/변경 주기 관리
- 보안프로그램 삭제 차단 및 삭제 시도 로깅
- OS, Application 취약점 자동 패치
- 보안 규정 위반 서버에 대한 경보

5 문제해결 솔루션 조합 (재택 PC 위협 사례)

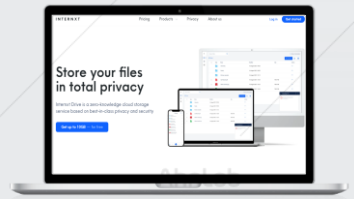
MORE SECURITY
MORE FREEDOM

01 인터넷 악성코드 유포

02 재택 PC 악성코드 감염

04 내부 기밀 정보 유출

웹 스토리지 사이트 업로드



외부 인터넷

불법 프로그램
다운로드

웹브라우저
인증정보 저장

VPN 접속 계정 탈취

내부 네트워크

05 랜섬웨어 암호화 공격

랜섬노트 메세지

주요 시스템 대상
랜섬웨어 감염

03 VPN 로그인 및 내부 환경 스캔

다크웹 정보 유출

06 랜섬/정보유출 이중 협박

5 문제해결 솔루션 조합 (재택 PC 위협 사례)

MORE SECURITY
MORE FREEDOM

Solution 01 AhnLab V3/EPM/ESA

재택 PC 보안 강화

- 최신 백신/OS 패치 유지
- 악성코드 감염 실시간 차단
- 재택 보안 One Agent 통합 관리
- AhnLab TrusGuard와 연동 PC 보안점수 수치화 제공

Solution 02 AhnLab TrusGuard

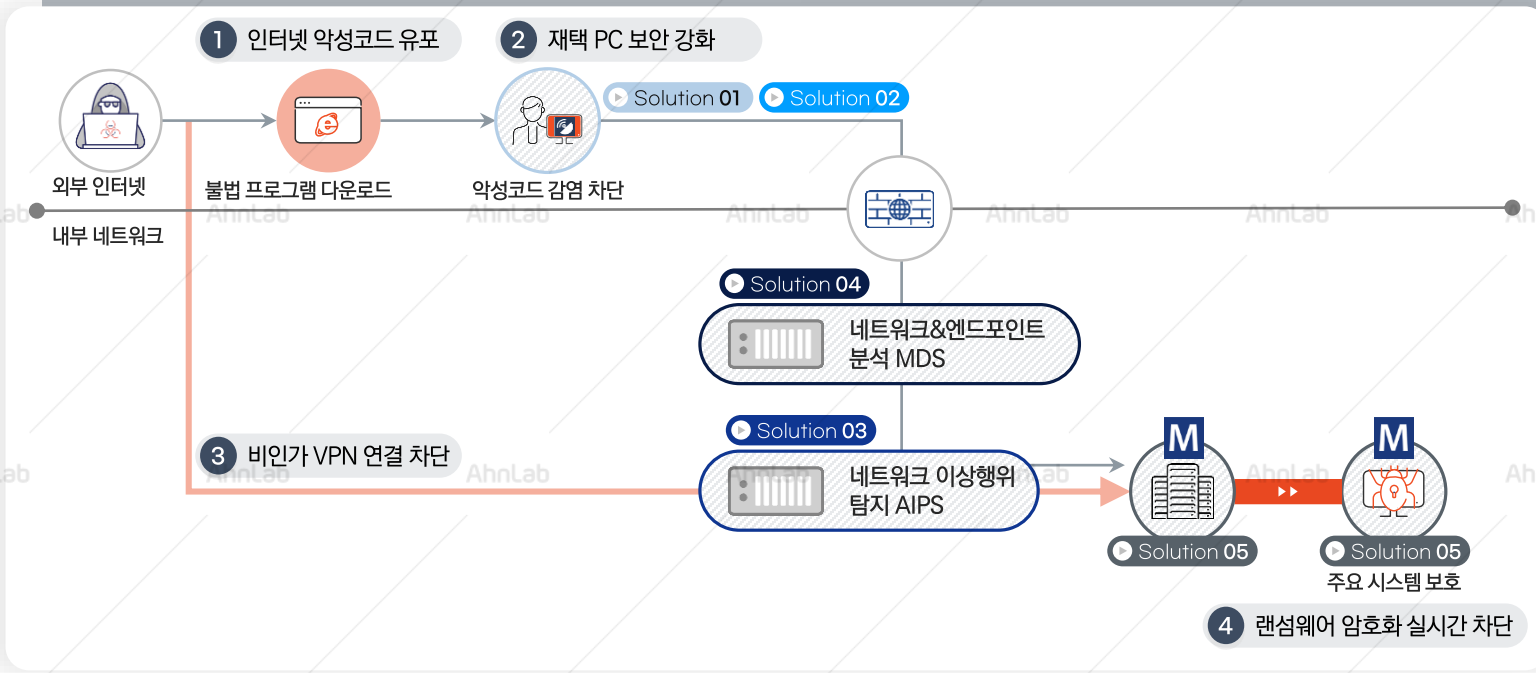
SSL VPN 인증 및 보안성 향상

- 2-Factor 인증 제공, 인증 실패 횟수 제한
- 접속 전 해킹툴 탐지, 접속 후 캐시 정보 자동삭제
- 사용자별/그룹별 접근서버 제어
- AhnLab ESA와 연동. PC 보안점수 검증 후 로그인 허용

Solution 03 AhnLab AIPS

네트워크 이상행위 감지

- 네트워크 이상행위 감지 및 차단
- 설정된 Security Zone을 기반으로 유해 사이트, 웹 취약점 등 관련된 모든 공격을 방어
- 설정한 임계치 기준으로 트래픽을 학습하고 자동으로 공격 패턴을 추출



Solution 04 AhnLab MDS

네트워크 모니터링 C&C 트래픽 탐지/차단

- 네트워크 패킷 분석, 프로토콜별 이동 파일 수집
- Blacklist 기반 악성 URL 차단
- 네트워크 취약점 트래픽 탐지
- 랜섬웨어 감염 의심 시스템, PC 감지

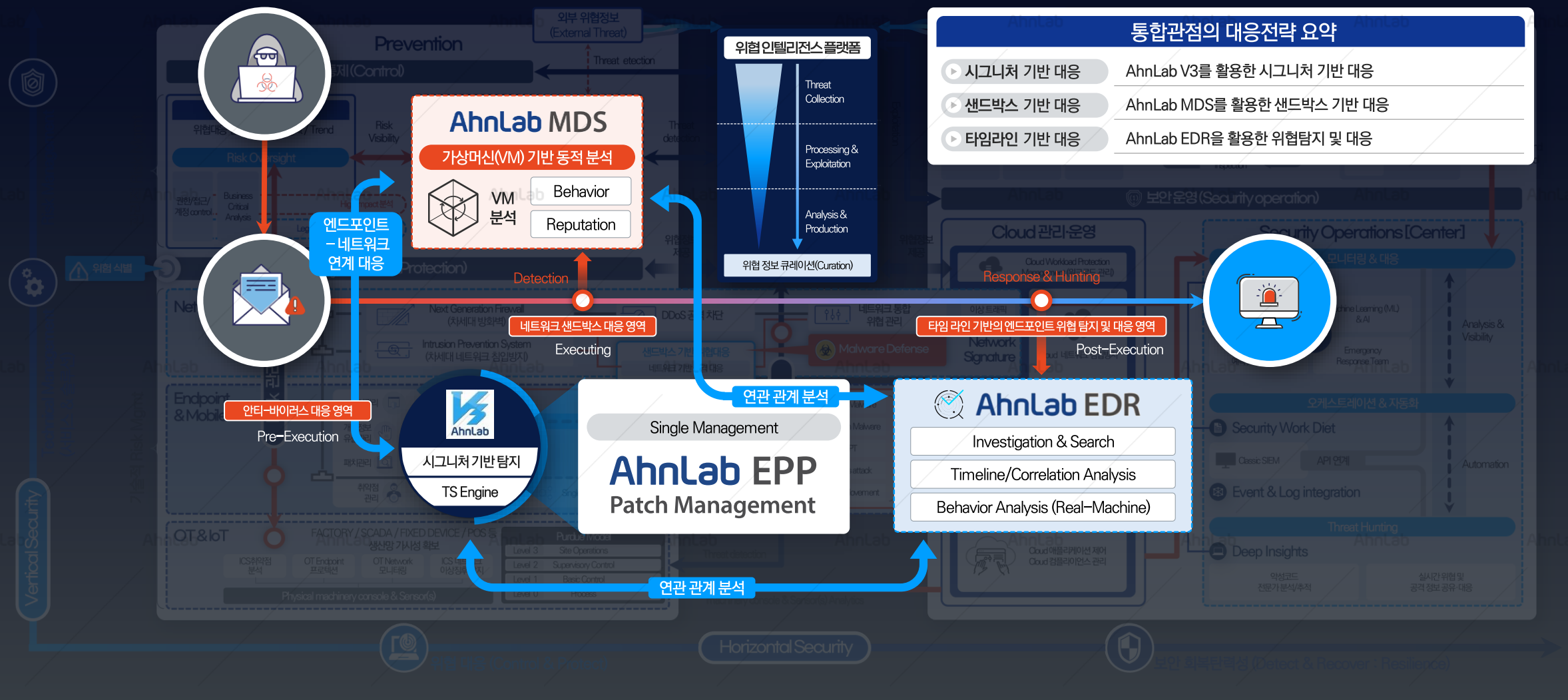
Solution 05 AhnLab MDS Agent

공격에 활용되는 툴 및 랜섬웨어 감염 차단

- PC/서버에 유입 후 실행되는 파일 실시간 검사
- 해킹툴, 백도어 설치 차단
- 알려진 & 신변종 랜섬웨어 샌드박스 분석
- 랜섬웨어 감염 전 차단

5 랜섬웨어 대응체계 완성

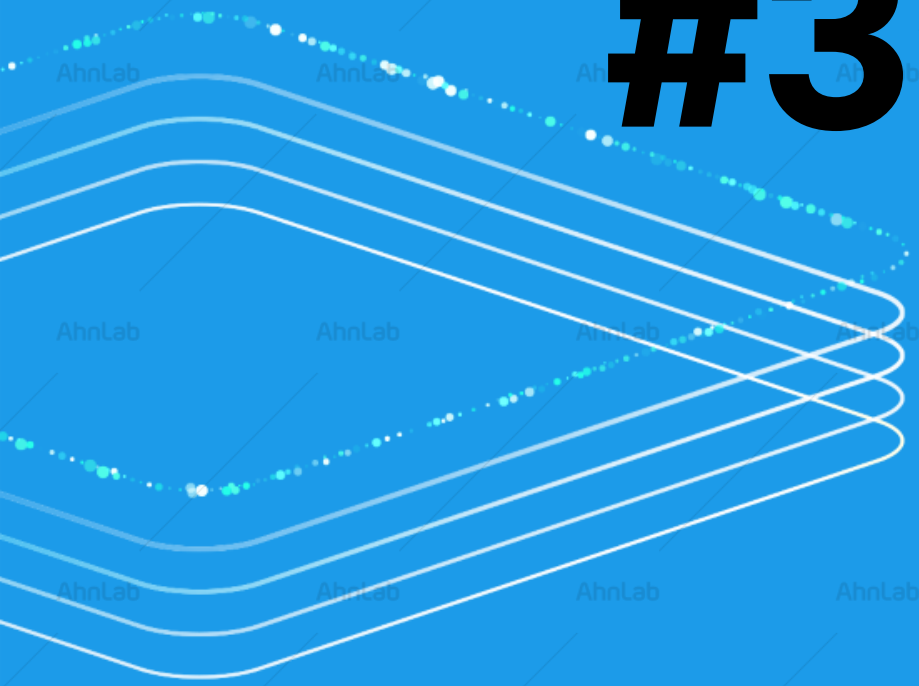
MORE SECURITY
MORE FREEDOM



통합관점의 대응전략 요약

시그니처 기반 대응	AhnLab V3를 활용한 시그니처 기반 대응
샌드박스 기반 대응	AhnLab MDS를 활용한 샌드박스 기반 대응
타임라인 기반 대응	AhnLab EDR을 활용한 위협탐지 및 대응

MORE SECURITY
MORE FREEDOM



3-3. Case #3 침해사고 대응을 위한 상시 모니터링 체계

1 ____ 집요한 엔드포인트 공격
2 ____ 무엇이 문제인가?
3 ____ 어떻게 대응할 것인가?
4 ____ 문제해결 방안
5 ____ 문제해결 솔루션
6 ____ 침해사고 분석 대응체계 완성

1 집요한 엔드포인트 공격

MORE SECURITY
MORE FREEDOM

2 무엇이 문제인가?

MORE SECURITY
MORE FREEDOM

기존 보안솔루션

전통적 솔루션은 역부족

✓시그니처 기반 탐지 불가

✓정상파일을 이용한 공격대응 불가

공격기법 정교화, 고도화

파일리스 악성코드의 증가로
스캔 대상을 찾지못해 탐지, 차단 불가

공격 흔적 삭제로
명확한 침해 원인 분석이 불가능

위협 경로 모니터링과
분석·대응 속도 지연

핵심은 행위기반 탐지와 위협 시각화 분석

알려지지 않은 위협 대응 한계

침해사고 인지에만 오랜 기간 소요

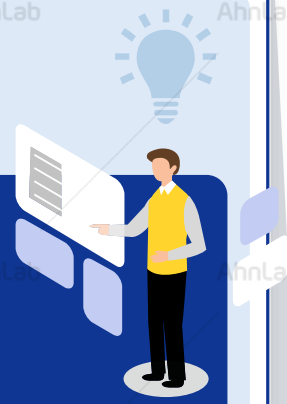
침해 사고를 인지해도 높은 수준의 포렌식 분석 기술 필요

분석 및 조사에 고비용 발생

추가되어야 할 보안 layer

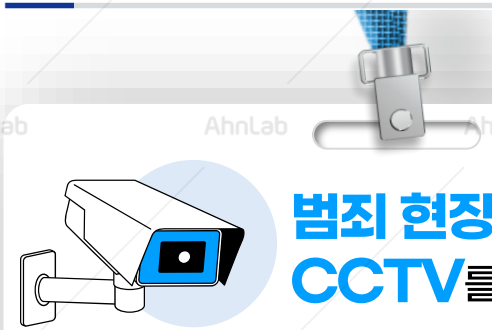
사이버 위협에 대한 CCTV 설치를 통해
상시 감시/사후 조사 Needs 발생

엔드포인트 대상 상시 이벤트 로그 모니터링 및 분석 체계 필요



3 어떻게 대응할 것인가?

MORE SECURITY
MORE FREEDOM



범죄 현장에 CCTV를 설치하자

CCTV : EDR

범죄현장 : 엔드포인트

침해 사고 예방 또는 단순 대응이 아닌
엔드포인트 레벨의 지속적인 모니터링 및 위협 정보 수집을 통한 대응력 강화

EDR(Endpoint Detection & Response) 기술은 엔드포인트단에서 지속적이며
연속적인 모니터링 및 위협 정보 수집, 분석을 수행함으로써
위협의 잠복 기간(Dwell Time)을 최소화하여 잠재적인 피해를 방지

- Endpoint 의 **로깅 강화**
  - Who, When, Where, What, How
  - 파일 / 네트워크 / 레지스트리 / 프로세스 / 네트워크 / 레지스트리
- 침해 조사에 필요한 정보를 **안정적으로 상시 수집**
- 별도 시스템에 **로그 백업**

4 문제해결 방안

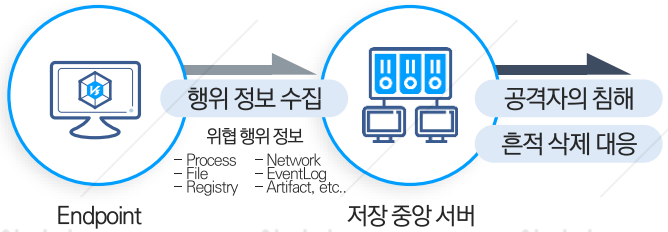
MORE SECURITY
MORE FREEDOM

대응방안.01 위협 행위정보 수집 및 저장

Centralization

위협 행위 정보 수집

- Endpoint에서 발생한 행위 정보 수집
  - 프로세스, 파일, 레지스트리, 네트워크 연결 등 위협과 관계된 행위에 대한 정보 자동 수집
  - 시스템 이벤트로그, 타임라인 정보 등 다양한 행위 정보 자동 / 수동 수집

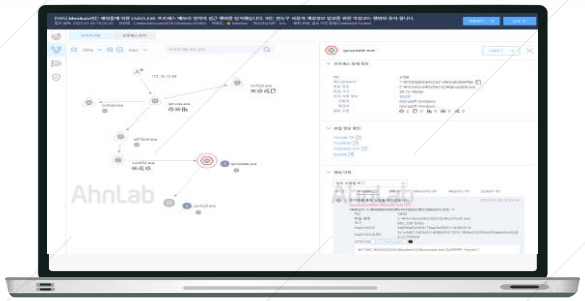


위협 행위 정보 저장

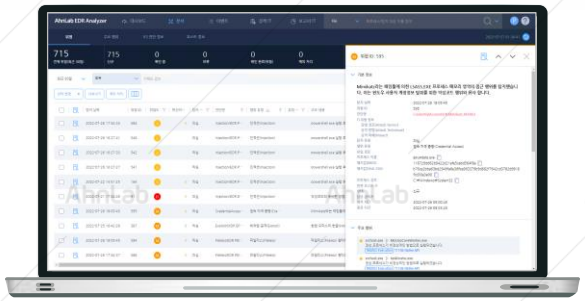
- Endpoint 발생 위협관련 행위 정보 저장
  - 침해 공격 시 발생한 흔적 에 대한 별도 보관
  - 침해사고 발생 시 포렌식 활용
  - 수집 정보를 분석 및 침해공격 의심행위 상시 모니터링

대응방안.02 위협 가시성 확보

Visibility



- 위협 종류, 경로, 행위, 연관성, 위험도 등 상세한 위협 가시성 확보
- 정상 파일을 이용한 공격 의심행위 탐지
- 권한을 가진 계정에서 발생하는 공격 의심행위 탐지
- 의심행위에 대한 아티팩트 기반의 타임라인 분석



대응방안.03 상시 위협 모니터링

Threat Hunting

Threat Hunting을 통한
상시 위협 모니터링

▶ 행위 유형별 Unknown 탐지 현황 [최근 30일 ▼]

랜섬웨어	인젝션	권한상승	네트워크접속	정보탈취
0	1	0	0	0

시스템설정변경	파일리스(Fileless)	취약점	기타
21	13	0	2

Threat Hunting

- 행위정보 분석을 통한 상시 위협 모니터링 수행
  - 다양한 침해공격 의심행위에 대한 상시 분석 결과 제공
  - 위협 가시성 확보를 통한 공격 흐름 전반에 대한 이해 제공
  - 위협 종류, 유입 경로, 행위, 연관 관계 등 상세한 정보 파악 및 대응

5 문제해결 솔루션

MORE SECURITY
MORE FREEDOM

AhnLab EDR

EDR은 엔드포인트 영역에서 지속적인 모니터링과 대응을 제공하는 보안 솔루션

EDR의 주요 제공 기능

✓보안 침해 탐지 / 보안 침해 조사

✓엔드포인트 영역에서의 보안 통제

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

→ 엔드포인트 행위 정보 수집을 통한 **위협 가시성 강화**

Centralization

✓중앙화된 로그 저장 및 관리 – 모든 엔드포인트 로그를 중앙 서버에 저장

✓로그 관리 및 분석 편의성 향상

→ 사고 발생 이전부터 엔드포인트에서 발생하는 **위협 관련 행위 정보 모두 수집**

5 문제해결 솔루션

MORE SECURITY
MORE FREEDOM

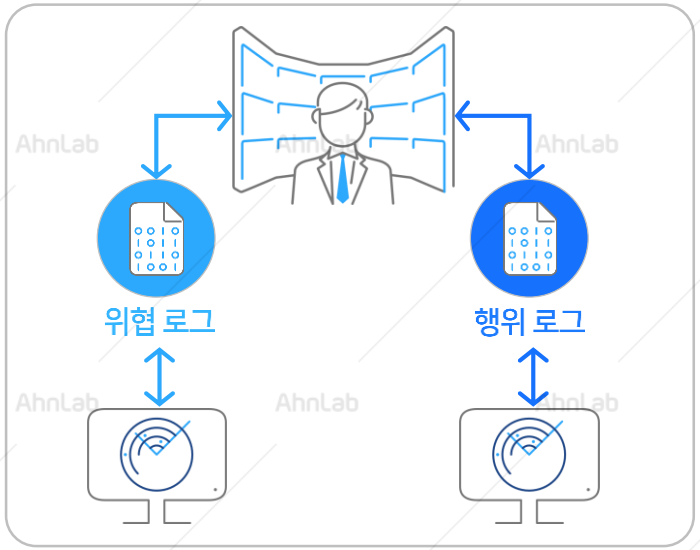
MDR Basic 서비스 무상 제공 대상

- EPP, V3, EDR 2.0 제품을 모두 보유한 고객

주요 내용

- 분석 대상
  - MDR Basic : EDR 위협 위험도(High) 기준
  - MDR Premium : 모든 위협 이벤트
- 분석 방안: 전문가가 위협 및 주요 행위 로그 분석
- 위협 분석 보고서, 월간 통계 보고서 제공

AhnLab 원격 관제 센터

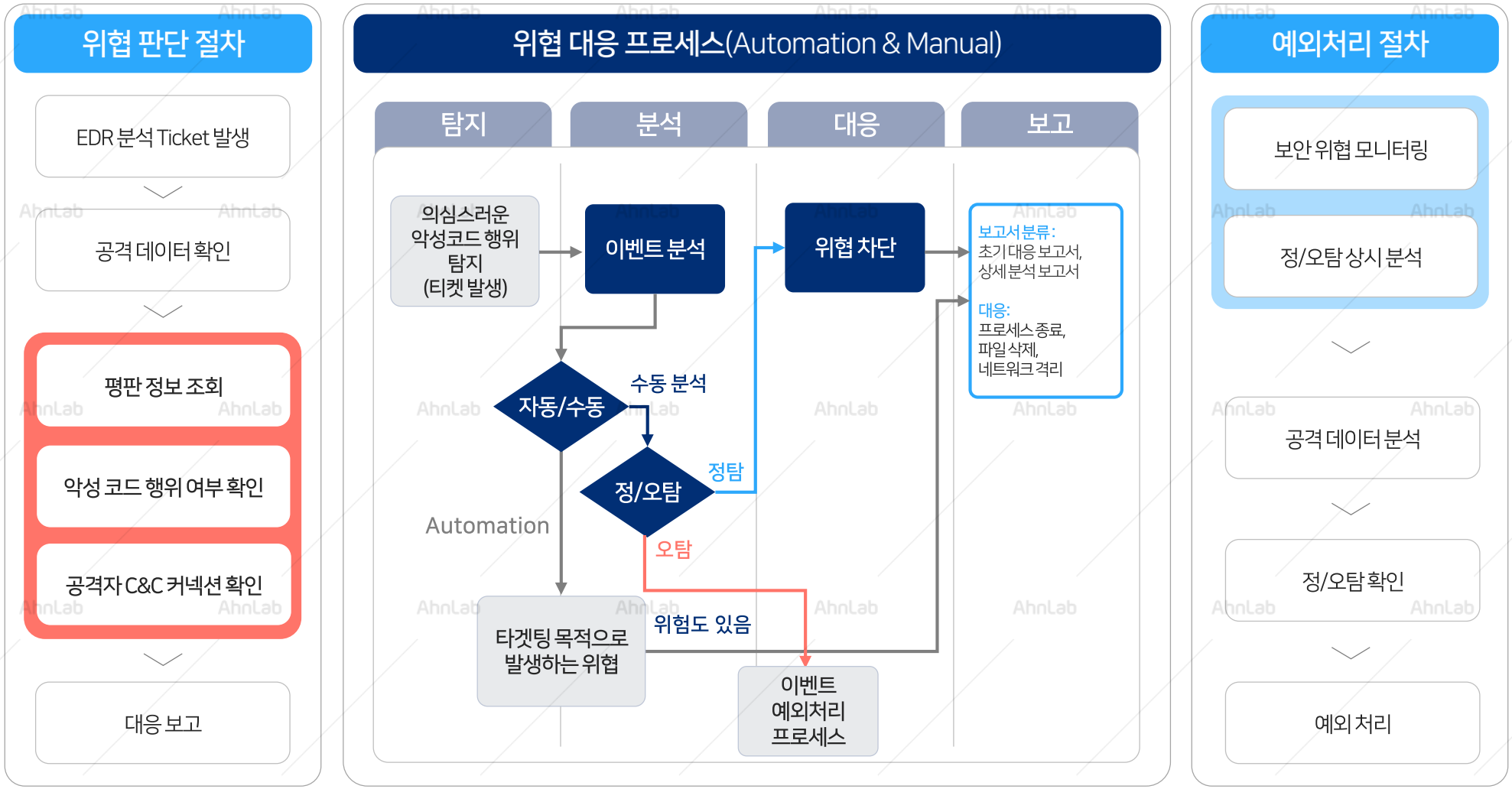


서비스 프로세스

고객 서비스 환경 분석 > EDR 연동 일정 협의 및 준비 > AhnLab Sefinity 연동 (원격관제 플랫폼) > EDR에서 발생하는 이벤트 필터링 > 발생 이벤트 순차 분석/대응 > 분석 보고서 제공

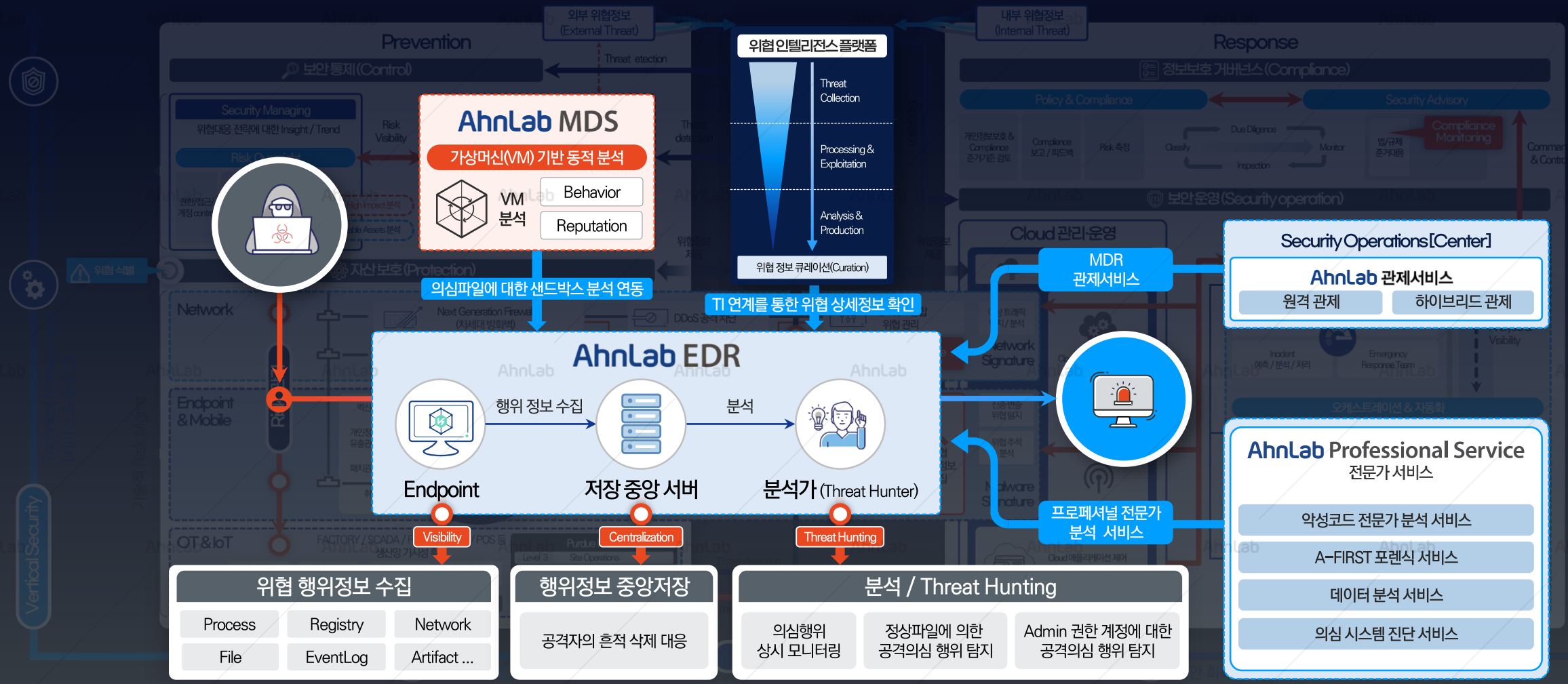
5 문제해결 솔루션

MORE SECURITY
MORE FREEDOM

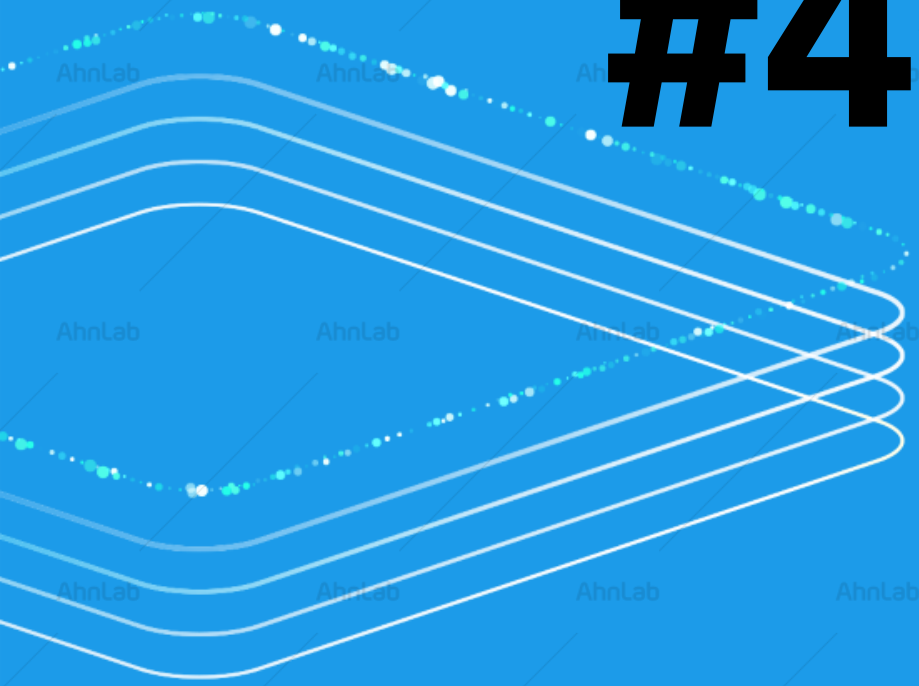


6 침해사고 분석 대응체계 완성

MORE SECURITY
MORE FREEDOM



MORE SECURITY
MORE FREEDOM



3-4. Case #4

SOAR Basic 활용 AhnLab 솔루션 연계 및 자동화

1 ____ 무엇이 문제인가?

2 ____ 문제해결 솔루션

3 ____ 솔루션 활용 예시

AhnLab

1 무엇이 문제인가?

MORE SECURITY
MORE FREEDOM

다수의 이기종 장비 관리로 인한
일관되고 소모적인 업무를
개선할 순 없을까

공격 기법의 고도화 및
다양화되는 공격기법으로 인한
보안 위협 대응의 한계는?

코로나 펜데믹으로
사업 구성원의 격리로 인한
업무 공백은

SIEM 이나 SOAR 가 없는
작은 조직에서도
통합 대응이 가능할까?

IT 현업 **업무 부하를**
절감할 수 있는
지능화, 자동화는 없을까?

관제 요원이나 분석가가 없는데
새로운 솔루션 도입은
어떻게 하지

2 문제해결 솔루션

MORE SECURITY
MORE FREEDOM

AhnLab SOAR Basic

2 문제해결 솔루션

MORE SECURITY
MORE FREEDOM

전통적인 SOAR	구분	AhnLab SOAR Basic
구축형 (3 - 6개월 소요)	도입 방식	설치형
SIEM 또는 ESM 필요	연동 방식	안랩의 솔루션
3rd Party 솔루션 지원 하지만 개발 필요 할 수 있음	연동 App	안랩의 솔루션
기존 대응 프로세스 분석 후 사용자 또는 벤더 지원 형태의 구현 필요	플레이북 구현	사전 정의된 시나리오 기반 플레이북 제공
지원	플레이북 편집	지원 X
사용자 또는 벤더 지원 형태의 관리 필요	플레이북 업데이트	컨텐츠 업데이트 방식
고가의 도입 비용	도입 비용	구독형, 월과금 형태의 과금 지불 방식

2 문제해결 솔루션

MORE SECURITY
MORE FREEDOM

AhnLab SOAR Basic

내장 플레이북
주기적인 업데이트 제공

구분	Playbook 명	활용 솔루션	시나리오 개요
위협 대응	이상 트래픽 발생 단말에 탐지 및 대응	TG + TMS + MDS + EDR	대상 단말에서 발생하는 이상 트래픽 원인 분석 및 재발 방지
	APT 의심 공격 대응	V3 + EPP + TG + EDR + MDS	APT로 의심되는 공격에 대한 근거 데이터 분석
	유해 사이트 접근 탐지	AIPS/TG+V3+ESA+EPM+EPrM+EDR	유해사이트 접속 단말에 대한 자동 대응
	외부 위협 정보의 조직 대응 현황 관리	TI + MDS + EDR	수집된 IOC 정보를 활용하여 조직 대응 현황 관리
	내부서버 접근 취약 단말 관리 1,2,3	EDR+ESA+TG	중요 서버에 접근하는 대상 단말의 취약점 관리
	AIPS 공격자 TOP5 대응 1, 2	AIPS + TIP + TG + V3 + EDR	AIPS에서 탐지된 Top5 공격자에 대한 대응
보안 강화	타겟형 피싱 사이트 자동 대응	MDS + TG + V3	타겟형 피싱사이트 자동 대응
운영 관리	악성코드 감염대응	V3 + EDR (TG)	악성코드에 감염된 단말에 대한 자동 대응
	보안 취약점 대응	EPM + EDR (TG)	대상 단말에 대한 보안 취약점 패치 관리
	네트워크 공격 대응	V3 + EDR (TG)	네트워크 침입이 발생 시 단말의 PC상태 점검
	개인정보 유출 감사 대응 1, 2	EPRM + V3	개인정보 유출이 의심되는 상황에 대한 대응
	PC 보안 점검 취약 사용자 대응 1, 2, 3	ESA	단말의 보안 점검 및 취약점 관리
	보안 수준 평가 취약 사용자 대응 1, 2	ESA	단말의 보안 수준평가 관리
	장기 미접속자 확인	V3	장기 미 접속 단말에 관리
	V3 엔진 업데이트 장기 미 실행자 조회	V3	V3 엔진 업데이트 장기 미실행자에 대한 자동 조치

3 솔루션 활용 예시

MORE SECURITY
MORE FREEDOM

AS-IS without playbook

① 취약점 탐지 및 차단

- 취약점 공격 발생
- NW 경계보안을 위한 TrusGuard, AIPS를 통한 위협 탐지 및 차단

② 담당자 알림

- 악성으로 판정 시 후속 조치를 위한 담당자 알림
- 담당자가 탐지 이벤트를 인지한 시점 부터 대응 조치 시작

③ 이벤트 분석

- 탐지 로그 상세 분석
- 이슈 발생 단말에 대한 각 보안 솔루션 이벤트 수집
- 수집한 이벤트별 상세 분석 및 영향도 평가

보안 담당자 수작업

④ 취약점 점검 및 조치

- 이슈 발생 엔드포인트에 대한 취약점 점검 및 취약점 해결을 취한 조치 방안 적용
- V3, EPM, EDR 등의 EP 보안 솔루션의 현황 점검 및 패치 실행

보안 담당자 수작업

⑤ 전사 대상 현황 조사

- 동일 이슈 발생 현황 분석을 위한 네트워크 및 엔드포인트 보안 솔루션 접속 후 로그수집
- 수집된 로그에 대한 분석 수행

보안 담당자 수작업

⑥ 보고서 작성

- 취약점 관리 및 대응 보고서 작성

보안 담당자 수작업

3 솔루션 활용 예시

MORE SECURITY
MORE FREEDOM

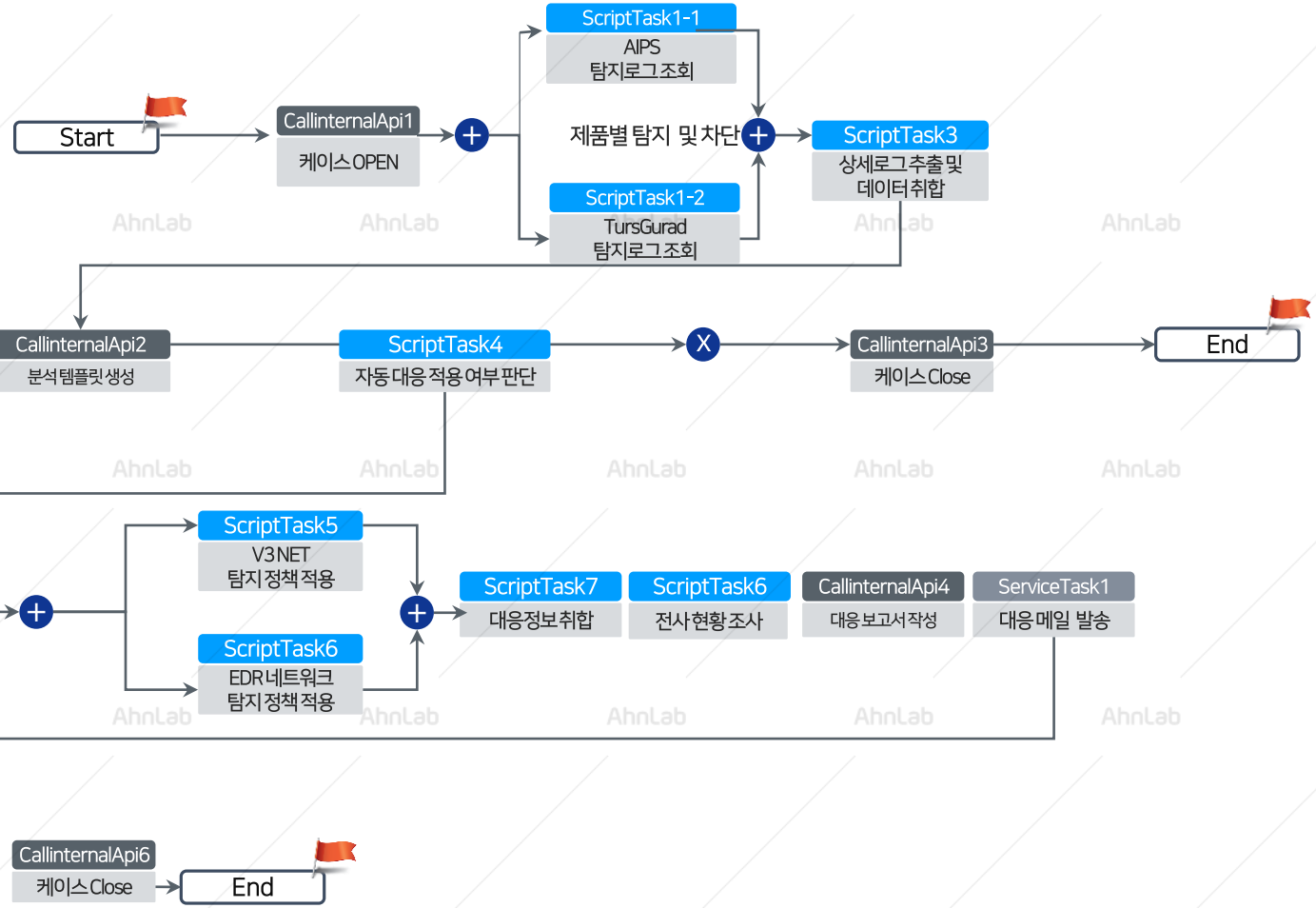
Playbook

취약점 공격 탐지

이벤트 분석

대응

종료



AhnLab SOAR BASIC의 Playbook 설정을 통한 내.외부를 통한 취약점 공격 발생 시 자동 대응

- AIPS를 통한 취약점 공격 탐지 및 차단
- TursGuard를 통한 취약점 공격 탐지 및 차단
- 수집 데이터 취합

이벤트 분석

- 분석 템플릿 생성
- 자동 대응 적용 여부 판단

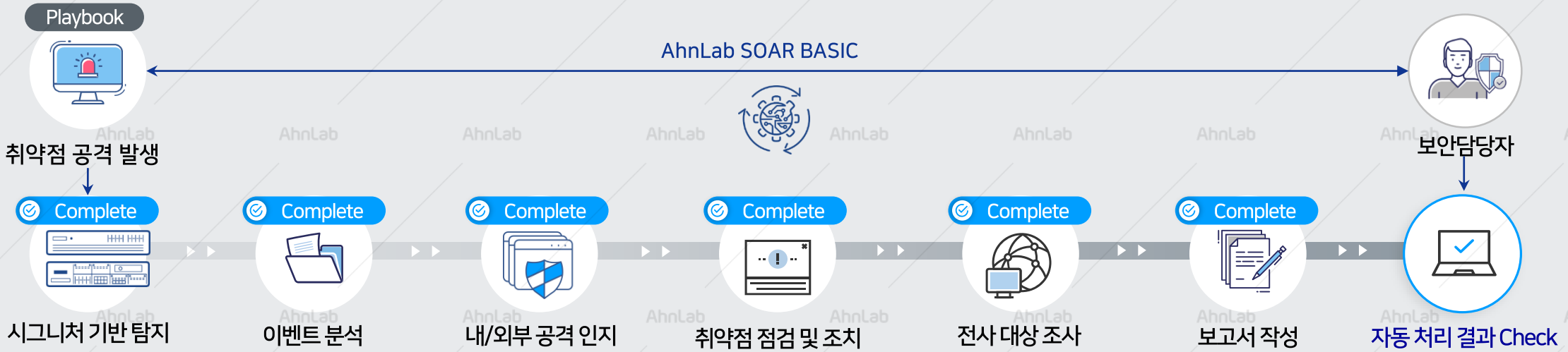
대응

- V3 를 통한 탐지 정책 적용
- EDR을 통한 네트워크 탐지 및 격리 정책 적용
- 내/외부 공격 인지 및 내부에서의 공격인 경우 내부 단말 조사 및 대응
- 대응 정보 취합 및 담당자에게 대응 조치 방안 알림 전송
- 대응 보고서 작성
- 관리자에게 취약점 탐지 및 차단 대응 보고서 메일 발송

3 솔루션 활용 예시

MORE SECURITY
MORE FREEDOM

TO-BE with playbook



1 취약점 공격 탐지 및 차단

- 취약점 공격 발생
- NW 경계보안을 위한 TrusGuard, AIPS를 통한 위협 탐지 및 차단

2 이벤트 분석

- 탐지 로그 상세 분석
- 이슈 발생 단말에 대한 각 보안 솔루션 이벤트 수집
- 수집한 이벤트별 상세 분석 및 영향도 평가

3 내/외부 공격 인지

- 출발지를 기준으로 내.외부 공격 인지
- 내부인 경우 단말 조사 및 격리
- 외부인 경우 ATIP 조회

4 취약점 점검 및 조치

- 이슈 발생 엔드포인트에 대한 취약점 점검 및 취약점 해결을 취한 조치 방안 적용
- V3, EPM, EDR 등의 EP 보안 솔루션의 현황 점검 및 패치 실행

5 전사 대상 현황 조사 및 대응

- 동일 이슈 발생 현황 분석을 위한 네트워크 및 엔드포인트 보안 솔루션 접속 후 로그수집
- 수집된 로그에 대한 분석 수행 및 대응

6 보고서 작성

- 개인정보보호 관리 및 대응 보고서 작성

Playbook을 통한 자동화 / 보안 담당자는 Playbook을 통해 자동 분석 처리 결과에 대한 결과만 확인

APPENDIX

APPENDIX

MORE SECURITY
MORE FREEDOM

V3·MDS·EDR 중에 하나만 있으면 될까요?

역할이 각각 따로 있습니다.

AhnLab V3

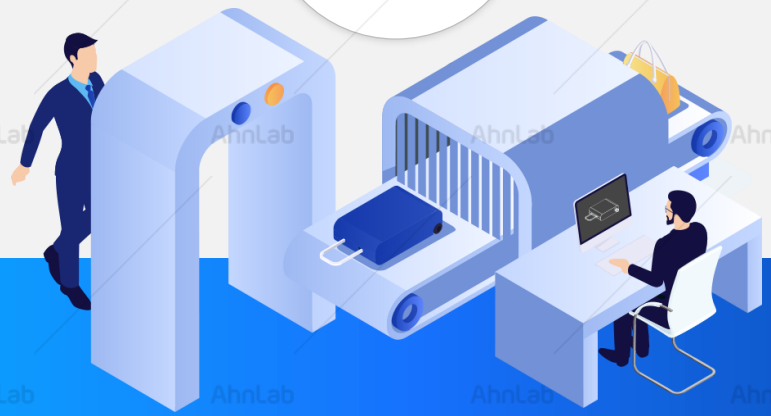
STEP 01

여권 검사 = 블랙리스트 기반 차단

V3는 시그니처를 기반으로
알려져 있는 악성코드를 빠르게 탐지합니다.

AhnLab MDS

STEP 02



Xray 검사 = 샌드박스 기반 탐지

MDS는 샌드박스 가상환경을 이용하여
알려지지 않은 위협을 정확하게 탐지합니다.

AhnLab EDR

STEP 03

CCTV 검사 = 행위 모니터링 탐지

EDR은 모든 행위를 모니터링하고 탐지하며
위협을 추적하여 분석합니다.

APPENDIX

MORE SECURITY
MORE FREEDOM

한국을 대표하는 정보보안 기업 안랩

엔드포인트 보안/파일 분석은 안랩이 제일 잘합니다

AhnLab V3

V3는 알려진 악성코드(파일)를
가장 빠르게 대응합니다.

#알려진 악성파일 #시그니처(DB)
#엔드포인트 보안

AhnLab MDS

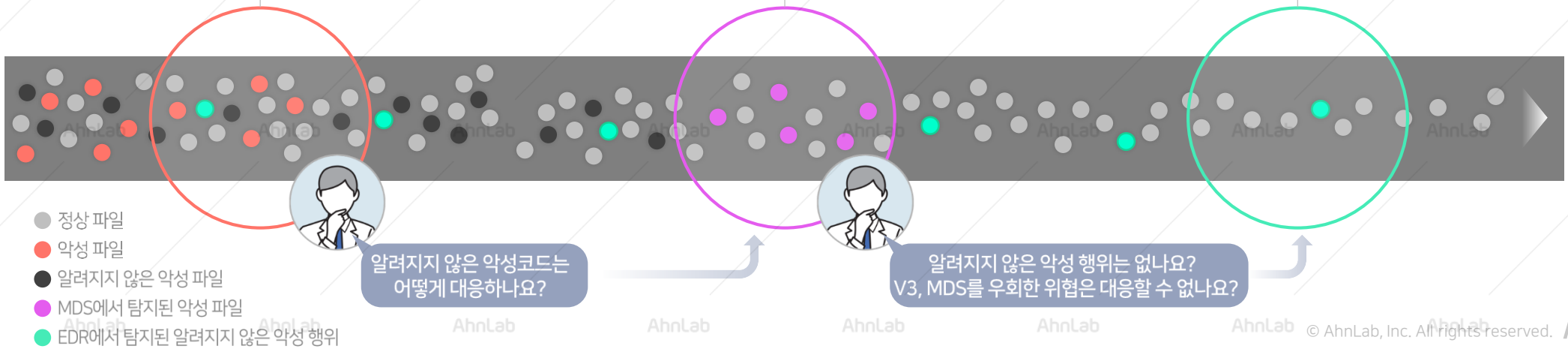
MDS는 알려지지 않은 악성코드(파일)를
탐지하고 대응할 수 있습니다.

#알려지지 않은 악성파일
#샌드박스 #네트워크 보안

AhnLab EDR

EDR은 엔드포인트에서 발생하는
모든 행위를 감시하고 저장합니다.

#알려지지 않은 악성 행위 #모든 행위 수집
#엔드포인트 보안 #수집-분석-대응-관리

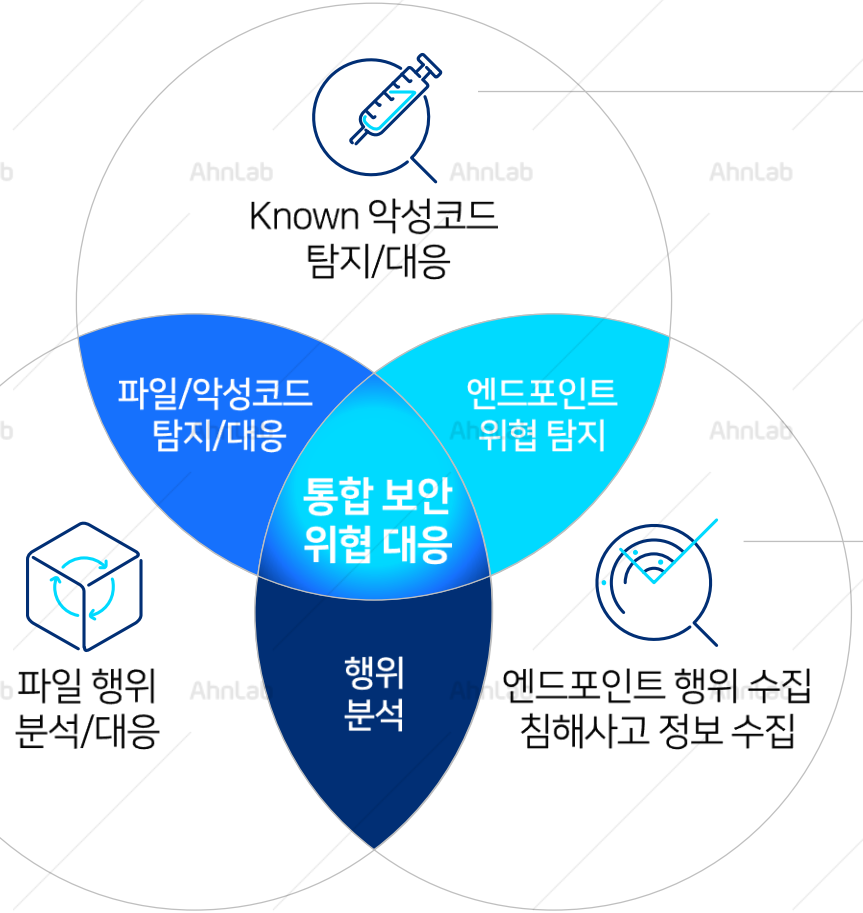


APPENDIX

MORE SECURITY
MORE FREEDOM

통합 보안 위협 대응, V3·MDS·EDR이 함께합니다

3개 제품
모두 필요합니다

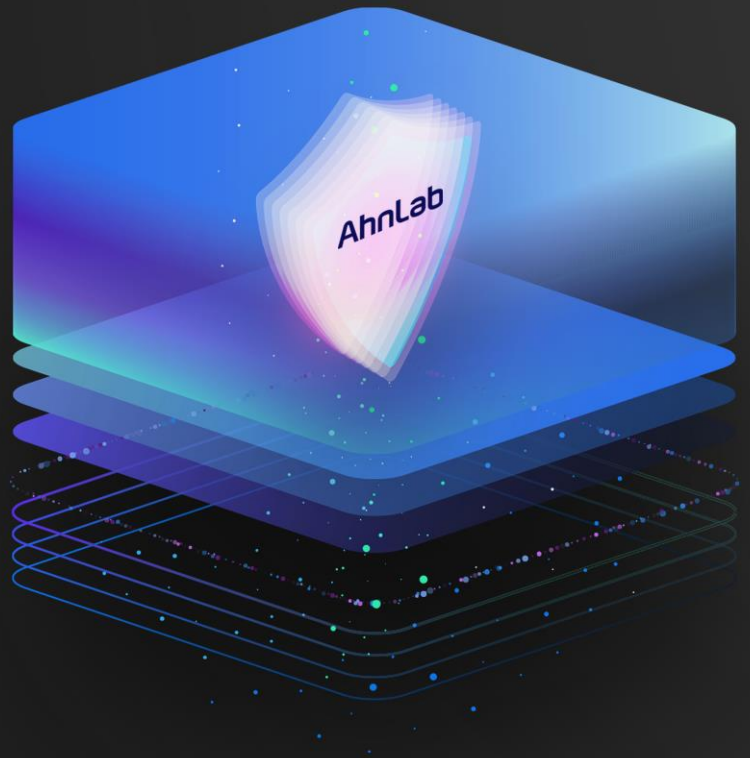


V3
알려진 악성 파일은 V3로 대응합니다.
가장 기본적이고 효율적인 보안은 PC·서버에
설치된 V3를 통한 보안 입니다.

MDS
알려지지 않은 악성 파일은 MDS로 대응합니다.
내 PC에서 악성 파일을 실행하는 것은 위험하므로
별도의 가상공간에서 파일을 실행합니다.
새로운 파일이라도 알려진 행위를 포함하므로
MDS로 대응 가능합니다.

EDR
V3, MDS를 우회하거나 알려지지 않은 악성
행위에 대한 탐지는 EDR을 통해 수행합니다.
침해사고의 시작은 엔드포인트에서 시작합니다.
모든 행위를 수집해야 분석/대응할 수 있고
엔드포인트를 관리할 수 있습니다.

MORE SECURITY
MORE FREEDOM



AhnLab

THANK YOU