More security,
More freedom

보안 환경 변화에 따른 보안 트렌드
안랩이 바라보는 XDR은?

안랩 솔루션컨설팅팀 **백민경 부장** / CISSP

AhnLab

Table of Contents

AhnLab

변화하는 보안 트렌드

지금까지 보안은 **경계 보안 중심**

AS-IS

외부위협의 방어와 내부유출의 통제에 포커스

Detection
외부 위협 방어

Prevention
내부 유출 통제

TO-BE

대응(Response) 중심 솔루션 통합과 연동

Unified Security
플랫폼과 플랫폼의 연동

Consolidation
솔루션들의 유기적인 통합

정보자산을 지키기 위한 Traditional 솔루션들

무엇이, 어떻게 변화하나?

위협의 예방

위협의 초기 식별과 대응

위협 완화

리스크 통제와 거버넌스 확보

위협 원점에 대한
탐지-분석-대응

Protect & Detect ▶▶▶ Threat hunting & Respond

위협과 리스크에 대한
통합관리

Point Solution 의 **연계** + **연동** 기반

통합적인

Threat Detection & Response

레이어 별
포인트 솔루션 구성

Resilience ◀◀◀ Governance & Visibility

오케스트레이션 및
거버넌스

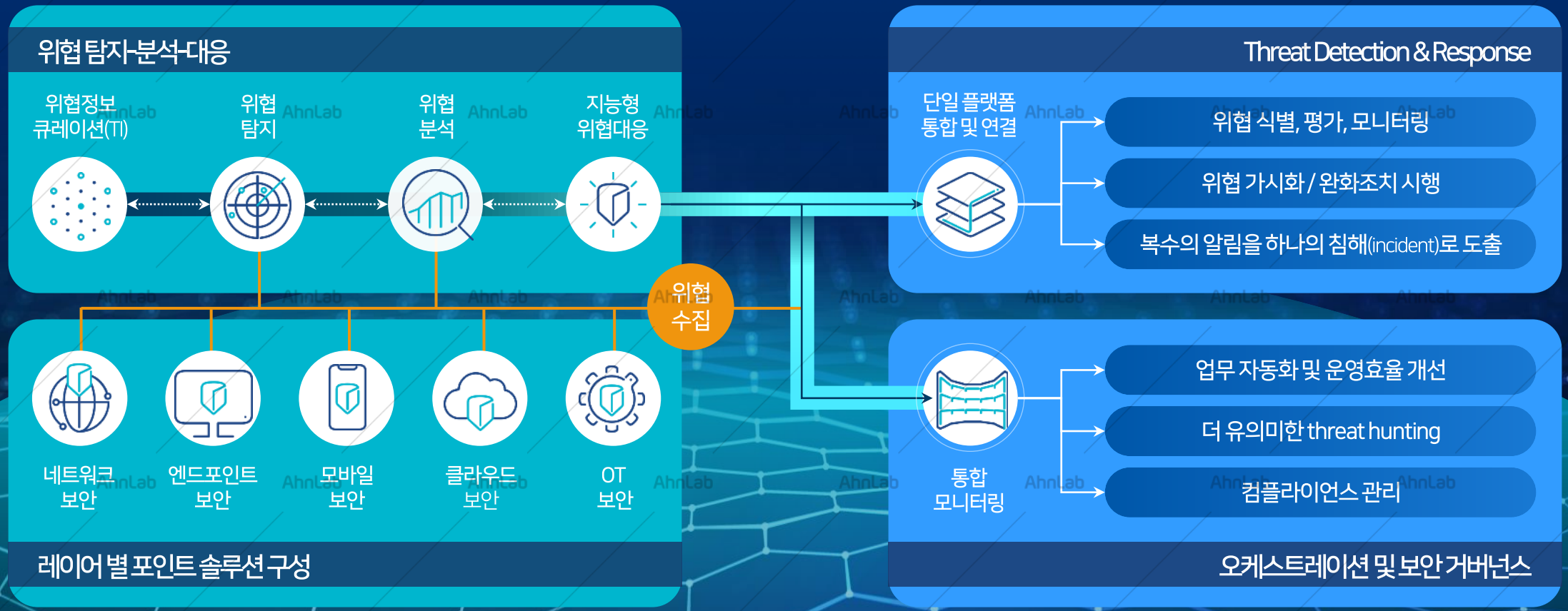
무엇이, 어떻게 변화하나?

유기적 통합

효과적 대응을 위한 솔루션 유기적 통합

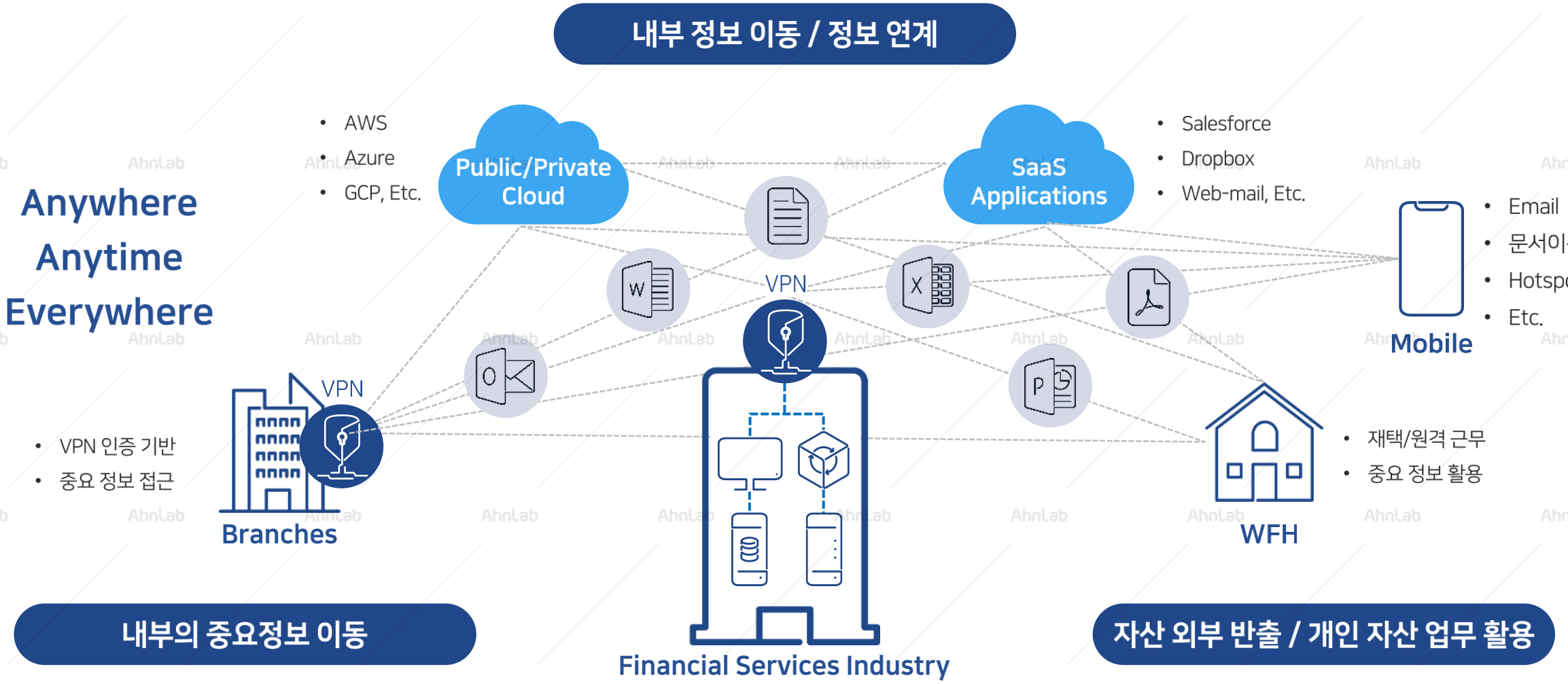
플랫폼 연동

리스크 통제와 거버넌스 확보를 위한 플랫폼 연동



보안 환경 변화로 인한 어려움

클라우드 업무환경 확대, 언제 어디서나 업무를 할 수 있는 환경 구축 → 보안 측면에서는 관리해야 할 포인트 증가



보안 환경 변화에 대응을 위한 XDR

각 영역에서 최고의 제품 도입(Best of Breed), 이기종 보안 솔루션 운영 → 관리 영역 증가, 보안의 Silo화

* source : Gartner, 2022

Detection & Response

외부 위협 탐지/대응, 내부 유출 통제 관점 (Detection & Prevention) → 중요자산을 보호하는 대응(Detection & Response) 중심으로 변화
각 영역에서의 Detection & Response → 연계.통합 관점의 Detection & Response로 진화

EDR	NDR	MDR	MXDR
Endpoint	Network	Managed	Managed eXtended

XDR
(eXtended Detection & Response)

- **Endpoint + Network + Cloud + 3rd Party**
- **단순 연계.연동인 아닌, Context 분석**

XDR: Overview

XDR이란?

- eXtended Detection & Response
- 복수의 텔레메트리를 자동으로 수집하고 상호 연결하는 탐지 & 대응 플랫폼
- 기존 각각 분리되어 있던 솔루션을 단일 플랫폼으로 통합 및 연결

XDR의 역할

- 복수의 알림을 하나의 침해(incident)로 도출
- 여러 형태의 탐지 옵션 제시
- 자동화된 대응을 바탕으로 보안 운영의 효율성과 생산성 개선

XDR, SIEM, SOAR

- XDR: 벤더가 통합된 보안 플랫폼과 탐지 & 역량을 제공 – 벤더가 지속 관리
- SIEM & SOAR: 기 구축된 솔루션들의 이벤트 통합 관리 & 대응 – 고객이 직접 구성

XDR: Overview

단일 플랫폼으로 통합 및 연결 → 데이터 커넥트/데이터 정규화

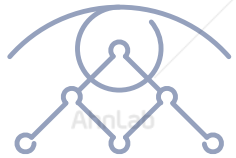
하나의 침해로 도출 → 연관/상관 관계 분석, Context 분석

자동화 된 대응 → 연계/연동 대응

XDR: Risk Management

확보 된 자산 가시성을 기반으로 지속적인 Risk 확인 및 관리

빠르게 확인하고 조치해야 할 Risk의 우선순위를 Score로 제공




자산/사용자 가시성 확보

- 물리적/논리적 자산
- 기업 및 개인보유 자산
- 문서 등 중요 정보
- User가 보유한 자산/사용 시간
- 계정 사용 자산/사용 시간

모니터링

- 자산 변동/신규 자산 접속
- 계정 변동 사항
- 데이터의 외부 전송, 복사
- 비정상 행위 탐지
- 사용자 이상 행동 (패턴)
- 위협 의심 징후

분석/평가

- Risk 시나리오 분석
- Context 분석
- 거버넌스/컴플라이언스 분석
- User/Asset 이상행위 분석

시간 장소 자산 사람

확인 및 조치

- 우선순위에 따른 Alert
- Risk 심각도, 영향도 확인
- 가이드 및 조치 진행
- 자동/수동 조치
- Report 확인

XDR의 핵심 : Data Analysis Platform

여러 벤더 통합 가능

XDR Front End


Firewall


NDR


SWG


EPP/EDR


UEM


SEG


DLP


CWPP


IAM


CASB

단일 벤더

XDR Back End


Cloud Delivered


Data Lake


Automation


Threat Intelligence


APIs


Orchestration

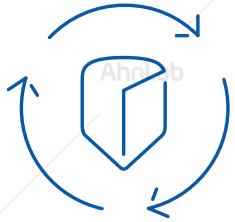

Advanced Analytics


Incident Investigations


Response Workflow

- 이기종 Data 수집, 정규화, 분석, 모니터링, 연계 대응
- ML 임계치, 내부 영향도 확인, Risk Scenario, Risk Scoring

Data Integration & Normalization

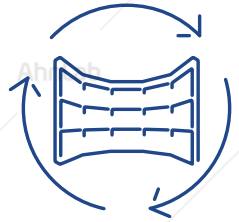


Native XDR

전통적인 보안 벤더에서 진행하는 형태

Consolidation | 단일 벤더 구성

Point Solution간 긴밀한 통합 탐지/대응



Open XDR

Data 수집/분석을 하는 벤더에서 진행하는 형태

Best-of-Breed | 각 영역 최고의 다수 벤더 구성

여러 벤더 Point Solution 정보 통합/연동 대응

통합과 자동화 측면으로 확대하는 특징

빅데이터 로그 관리 / 분석 기능 확대

Silo 최소화
위협 우선순위 식별
Risk 관리

위협 탐지와 대응 측면으로 확대하는 특징

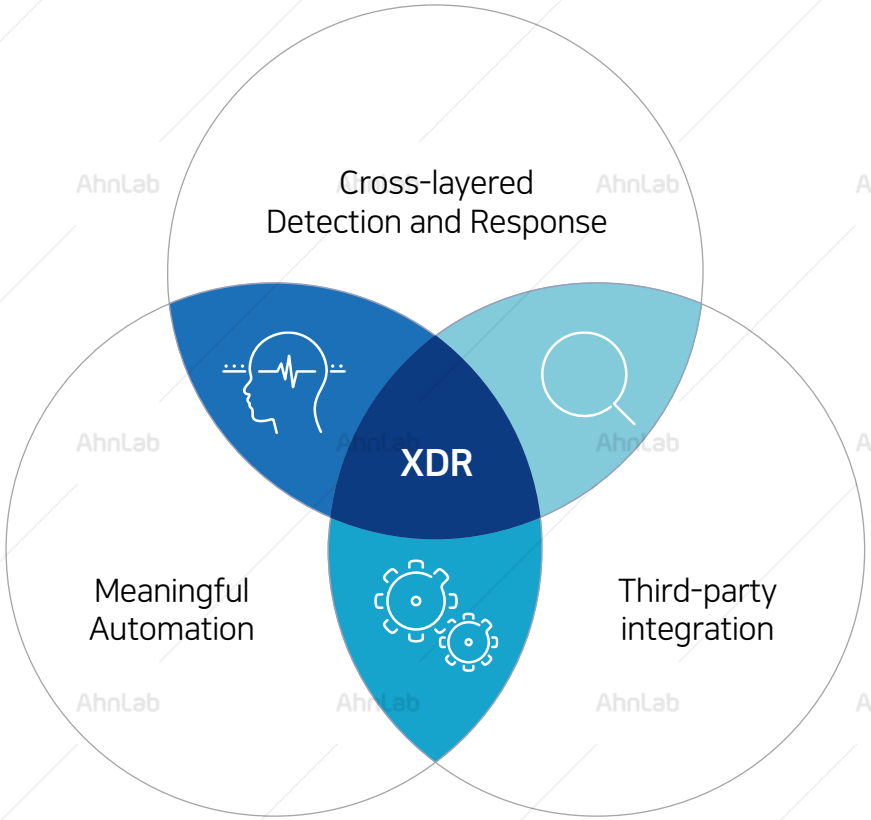
Endpoint Telemetry 및 보안 제품 연동 확대

공통적인 숙제

이기종 데이터 통합 및 정규화

XDR에서 제공해야 할 핵심 요소

XDR(eXtended Detection and Response)은 크게 3가지 요소를 기반으로 제공



Cross-layered Detection and Response

- 기업은 일반적으로 수십개의 보안 솔루션 운영, 위협이 격리되지 않을 가능성 높음
  ex) 피싱 이메일 → 취약한 엔드포인트 활용 → 인가되지 않은 클라우드 접근 발생
- 공격 사례를 이해하고 대응하기 위해 다양한 영역의 보안 로그를 연계분석 해야함

Third-party Integration

- 고객 설문조사 결과 기업의 92.2%가 5 ~ 99개의 보안 솔루션 사용
- 평균 12.5개의 벤더 운영

Meaningful Automation

- 분석가는 매일 여러 가지 알림 처리
- 분석가의 시간은 한정적이며, 가장 높은 리스크 우선순위 지정 필요
- 필요시 추가 조사 및 자동화된 대응이 가능한 솔루션 필요

Risk 관점으로…

보안 관점의 변화

(악성행위 중심의 Black 관점 → User · Data 중심 Risk 기반 접근)

A형간염검사 결과지

성명		주민번호		등록번호	
주소				검진일	2019-07-17

검사구분	검 사 명	결 과	판 정	단 위	참 고 치
면역혈청검사	A형간염항체(IgM)Anti-HAV	음성	정상		음성
	A형간염항체(IgG)Anti-HAV	양성	정상		음성,양성
	[illegible]면항원,일반(HBs Ag)	음성	정상		음성
	B형간염[illegible]항체,일반(HBs Ab)	양성	정상		음성,약양성,양성
판정	정상A				
소 견	B형간염:항체양성 A형간염: 항체, 양성(있음)으로 예방접종 불필요함.				

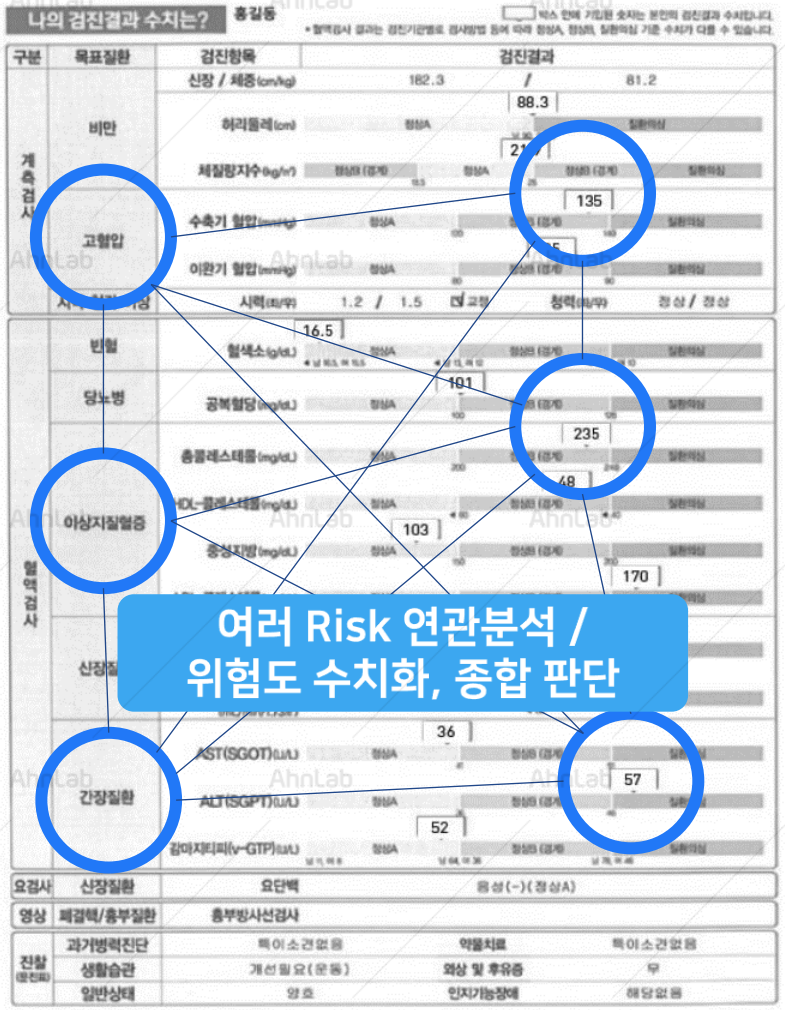
관점의 변화

제품 관점에서 특정 영역 모니터링 → 정상/악성 여부 판단

V3 = 독감 / EDR = 코로나(PCR, 역학조사)

XDR = 종합건강검진

종합적인 결과 기반 – 건강의 Risk 관리



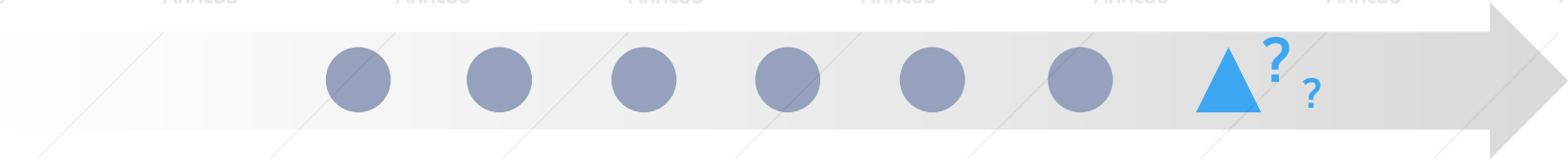
* source : https://brunch.co.kr/@jish201403ekrr/4

XDR에서의 Risk

XDR은 분석된 결과를 바탕으로 Risk일 확률이 높은 Alert을 선별하여 관리자가 확인할 수 있도록 지원

XDR에서 Risk는 악성의 개념이 아닌 위협이 될 수 있는 가능성이 높은 정보

Point Solution의 단편적인 로그가 아닌 상황(Context) 분석에 의한 Risk 가능성 확인



" 평소 출력을 많이 하지 않던 직원이 어느 날 많은 양의 문서를 출력하는 것이 악성행위인가? "
실제 계정이 탈취되어 발생한 일 일수도 있고…정상 업무를 하는 중일 수도 있음

평소와 다른 패턴이기에 확인이 필요한 것

보안담당자가 확인해야 할 Alert이 너무 많으면 확인이 어려울 수 있음

수 많은 Alert 중에 정말 확인이 필요한 Risk를 찾아서 관리자에게 알림을 주는 것이 XDR의 핵심

다수의 Alert, 하나의 Incident

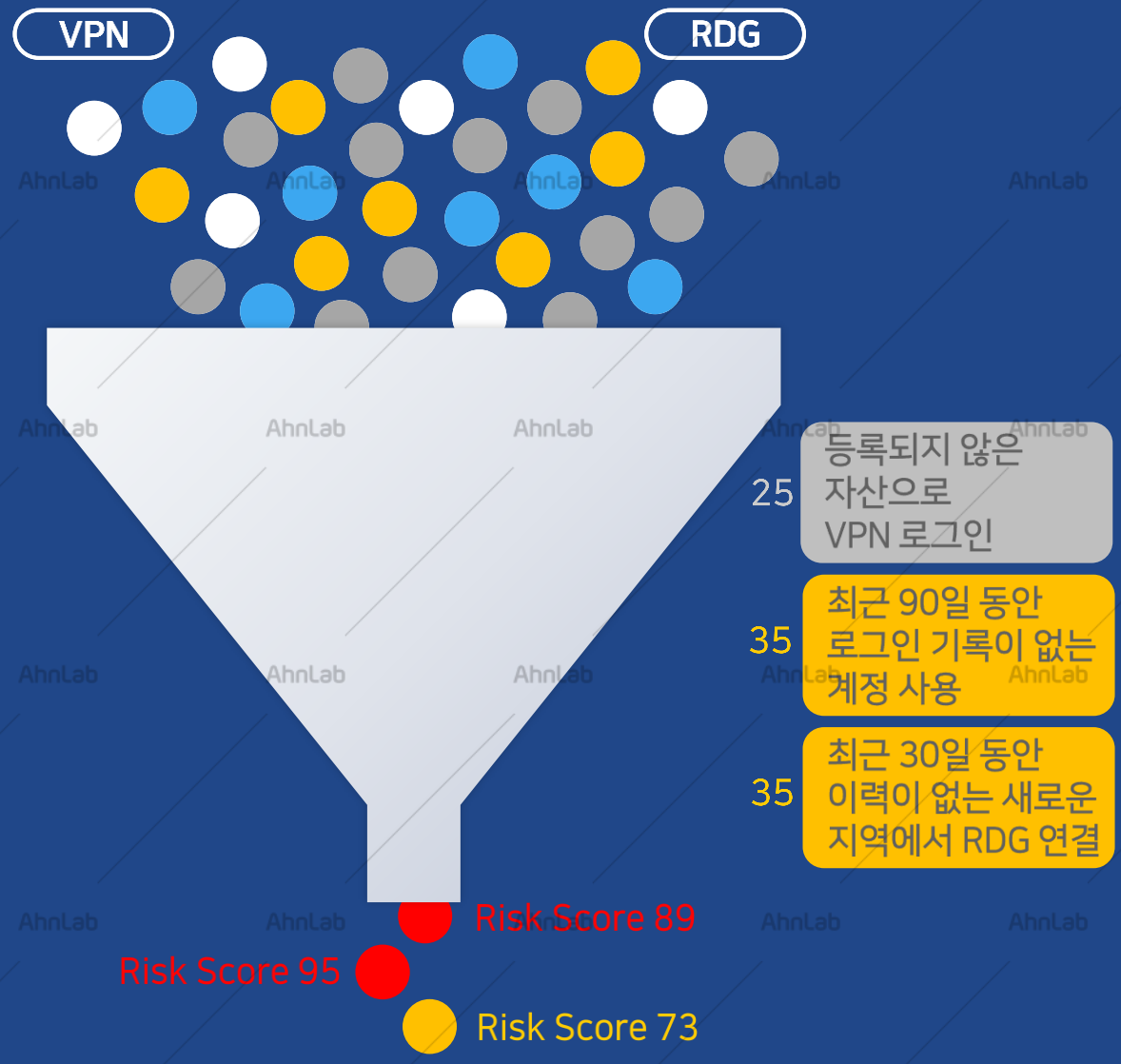
Ingest 원시 데이터 형태의 로그 데이터 수집

Filter 불필요한 데이터 제거, 데이터 종류 구분

Normalize 서로 다른 이기종 시스템에서 수집한 데이터를 공통 스키마 형태로 정규화

Enrich 로그 데이터 항목에서 부가적인 데이터 보강 처리

Detect 상관관계 분석에 의한 Risk 탐지



안랩이 바라보는 XDR

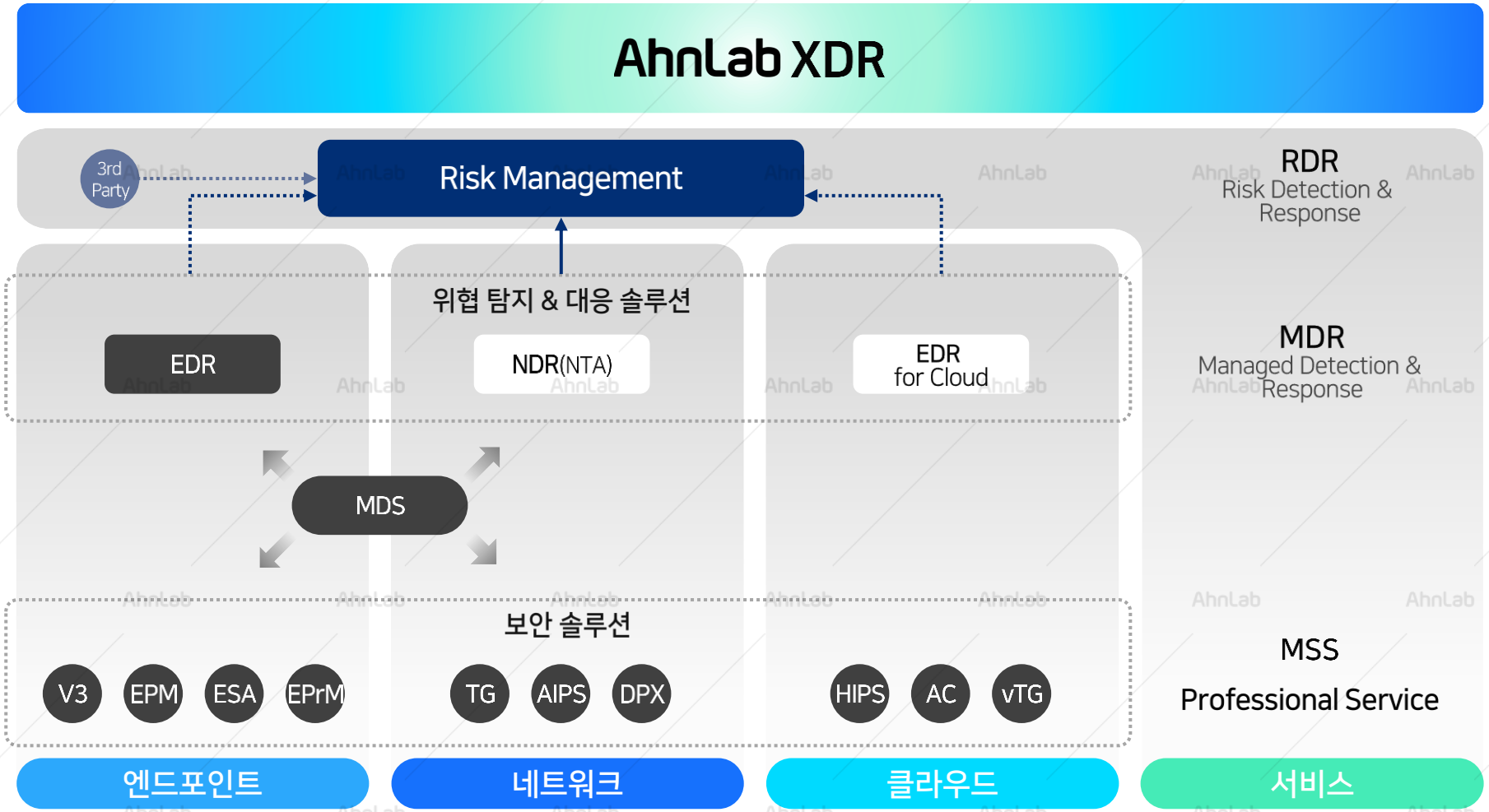
위협 탐지/차단 (Detection & Prevention) → 분석 – 추적 – 예측 – 대응 방안 추천 (Detection & Response)의 Risk 관리의 개념으로 진화

기업 내 Endpoint, Network, Cloud 및 3rd Party 솔루션의 Data Integration – Normalization – Context Analysis – Risk Scoring - Response

03 위협 예측 및 대응 방안 추천

02 위협 분석 및 추적

01 위협 차단



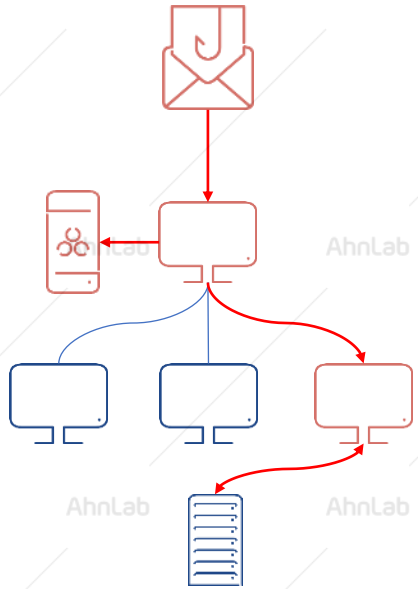
AhnLab XDR : AI & Automation

AI 적용을 통한 시나리오 분석, 위험 평가, 추천 대응 → **보안 관리자가 XDR을 활용하여 기존의 Silo 환경을 개선하고, 쉽게 사내 Risk를 관리**

Asset (User, Device) 마다 Risk로 판단하기 위한 기준은 정하기 어려움. Risk를 탐지하기 위해서는 여러 가지의 Rule이 아니라 AI를 통한 Risk 판단이 필요함

01 AI 시나리오 분석

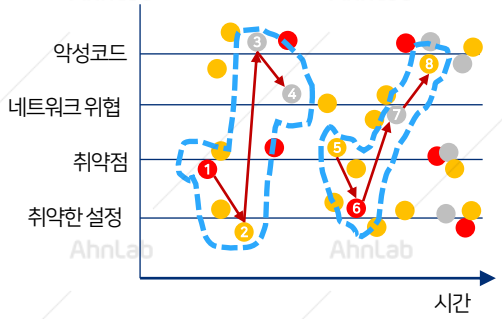
시나리오 기반 AI 분석



전문 분석가의 개입 없이 AI 알고리즘을 통해
사전 정의된 시나리오에 따라 위협 분석 자동 진행

02 AI 위험 평가

AI 정밀 탐지를 통해 고 위험도 위협 탐지



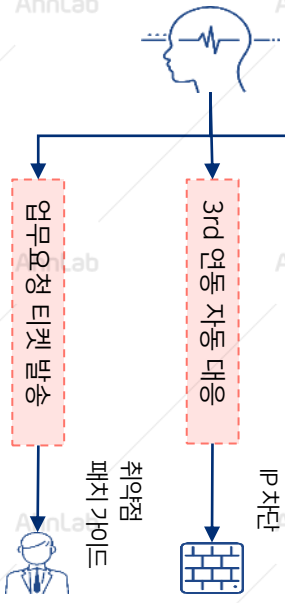
1 2 3 4 (Risk Score : 98)
+ 임직원을 통한 데이터 유출 위협

5 6 7 8 (Risk Score : 87)
+ 계정탈취, 비인가 장치 접속 위협

시나리오 분석을 통해 확인된 다양한 위협 중
AI 위험 평가를 통해 위협의 우선순위를 자동으로 평가

03 AI 추천 대응

AI 추천 대응을 통한 빠른 대응



평소 담당자의 대응 패턴을 학습하여 최적의 대응 방안 추천
추천된 대응 방안을 활용한 자동 또는 수동 대응

AhnLab XDR : Risk Score

User와 Asset에서 탐지된 내용을 종합적으로 분석하고 각 항목에 부여된 Score를 기반으로 조치 우선순위 제공

고객사 산업군과 환경을 고려한 가중치 보정 기능 제공

고객사 보안 담당자의 Risk Factor 가중치 보정
(Ex. 접속 위반 : 20% → 30%)

=

Risk Score
95

탐지 시나리오 Score

LV1 ~ LV5
각 시나리오에 반영 된 LV Score

자산 가치

1 ~ 5
Risk Score가 부여 된 운영 자산의
중요도에 따른 Score

Base Score

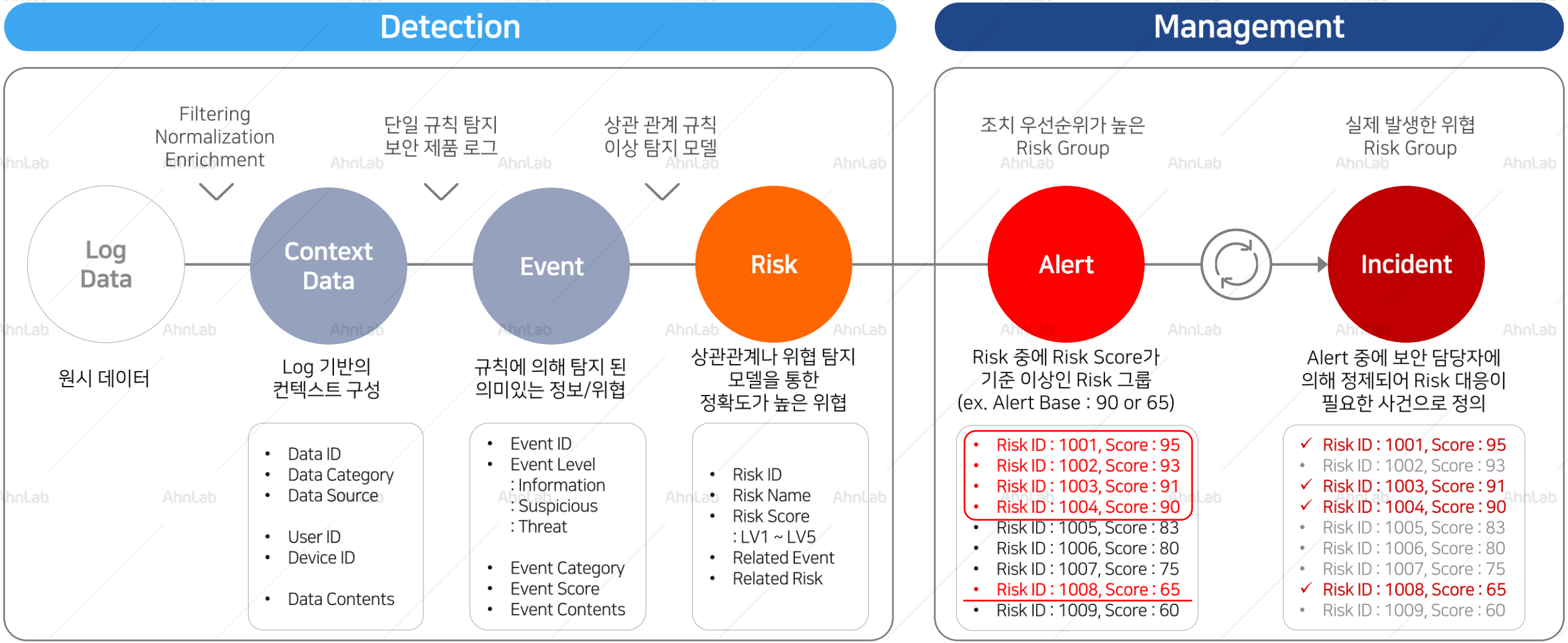
Risk Factor 가중치

Risk Score가 부여 된 User/Asset의
접속 위반, 데이터 위반 등
Risk Factor로 규정 된 항목의 가중치 Score

Final Score

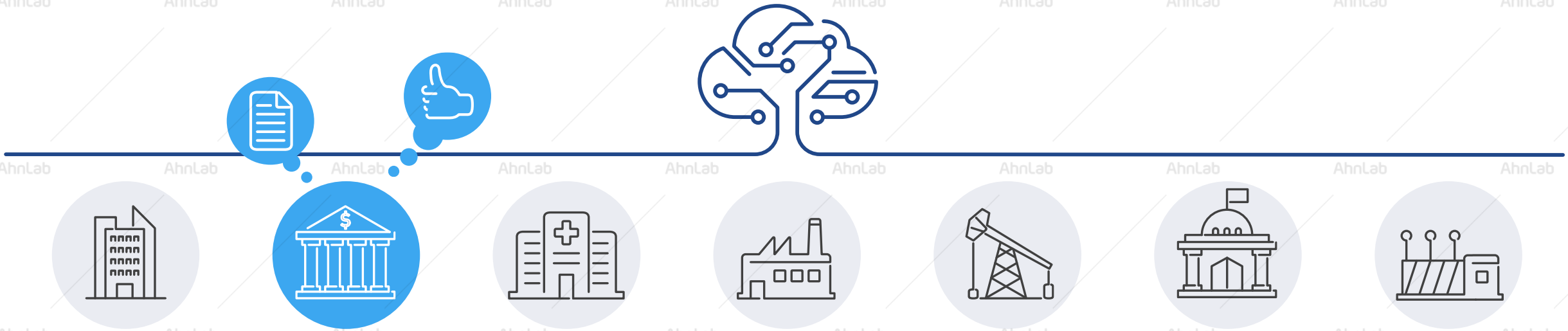
AhnLab XDR : Risk Management (1/2)

대응해야 할 Risk를 선별하고, 조치해야 할 우선 순위를 제공하는 Risk Management



AhnLab XDR : Risk Management (2/2)

다양한 정보와 노하우 공유를 통한 지속적인 운영 지원



우리 회사가 속한 산업군에서의 Risk 수준 확인

보안담당자가 적용한 시나리오 등 공유와 이를 통한 산업군 전반의 보안 강화

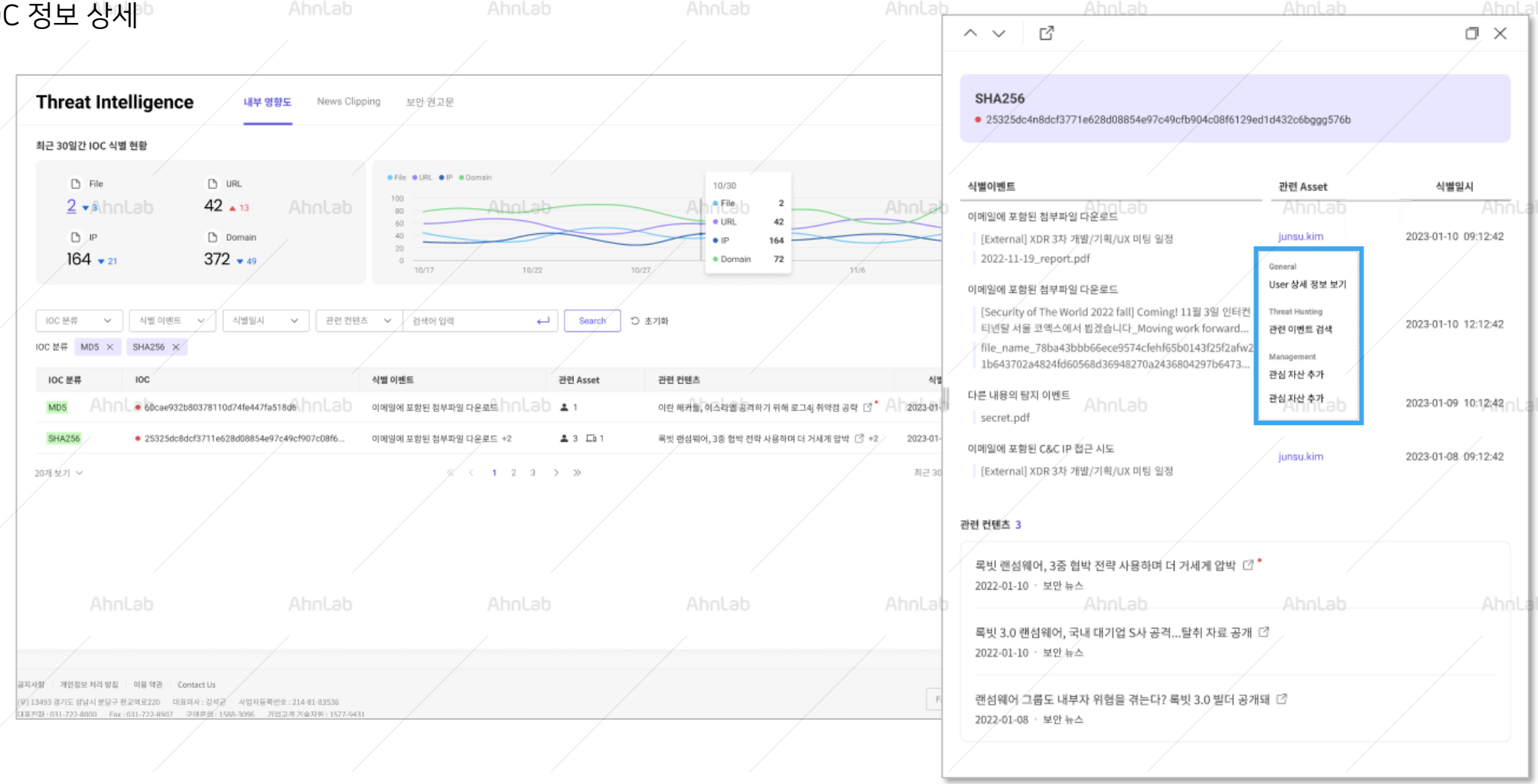
산업군에 따라 위협의 유형도 다르고, 사용자의 패턴도 상이함

내가 속한 업계의 Risk 수준을 확인하고, 공유된 정보를 참고하여 보안 수준을 강화

AhnLab XDR : Threat Intelligence 연계

Threat Intelligence – 내부 영향도 확인

식별 IOC 정보 상세



AhnLab XDR

Public / Private Cloud

On-Premise

Cloud Platform

- 다양한 환경 고려
- 이식성 지원
- 산업군 보안 수준 확인
- 시나리오 공유
- 다양한 서비스 제공

User/Asset Based

- 명확한 Risk 현황 파악
- 신속한 조치
- 이상행위 탐지
- 개별 AI 학습

Open Platform

- Alliance
- Data Connector

AhnLab XDR Platform

Automatic Response : 연계/연동 솔루션을 통한 자동 대응

Alert/Incident | Reports | Action

Risk Scoring : 가능성, 위험도, 중요도, 가중치

Risk Analysis : 이상행위 탐지, 악성행위 탐지, 위협 탐지, 컴플라이언스 등 연계 분석

User/Device Risk | Data Profiling | Threat Detected | User/Device Compliance | ML Threshold

Data Integration & Data Normalization

User/Asset | EP | NW | Cloud Apps | Email | 3rd Party

Service

TIP

MDR

SOC

XDR Alliance

More security, More freedom

AhnLab