국방혁신기술보안협회

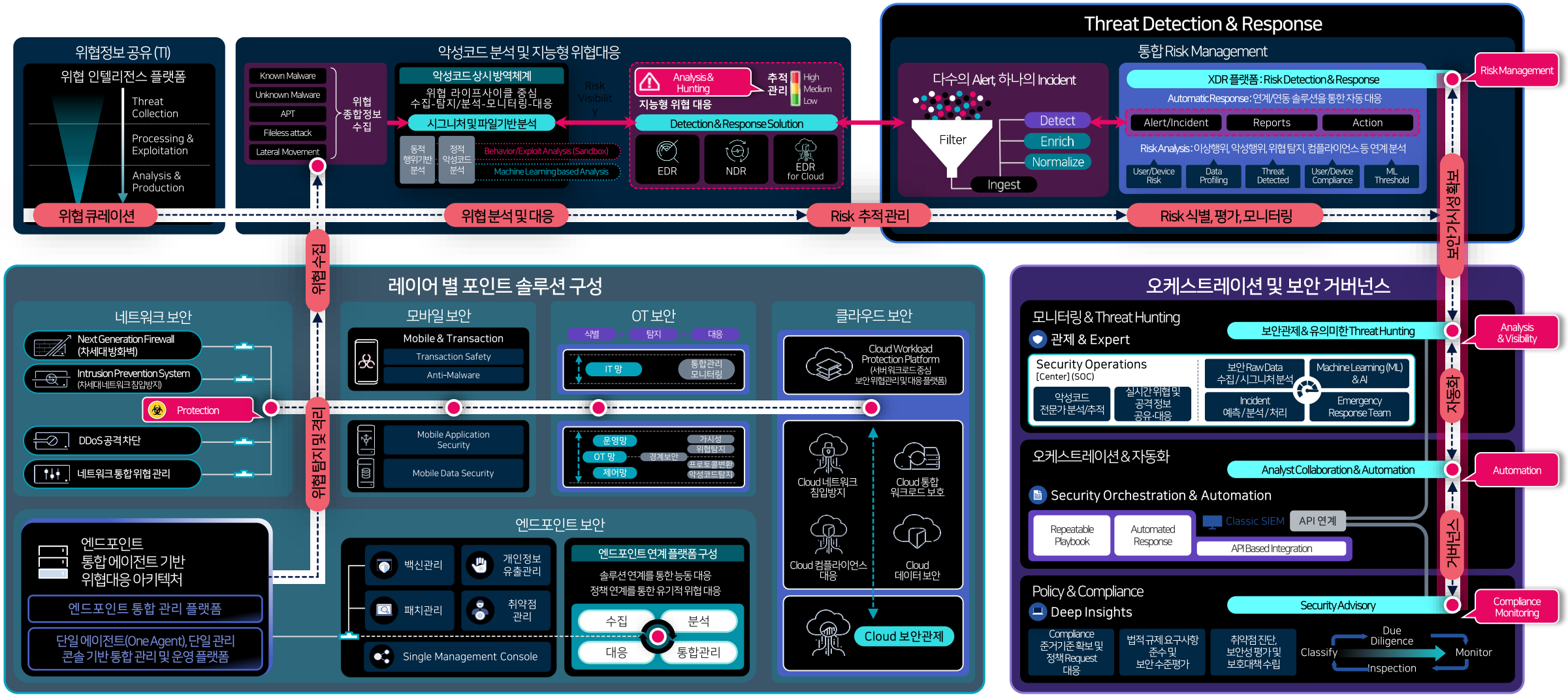
AhnLab 주요 제품 소개 (TIP/EDR/SOAR/XDR)

AhnLab

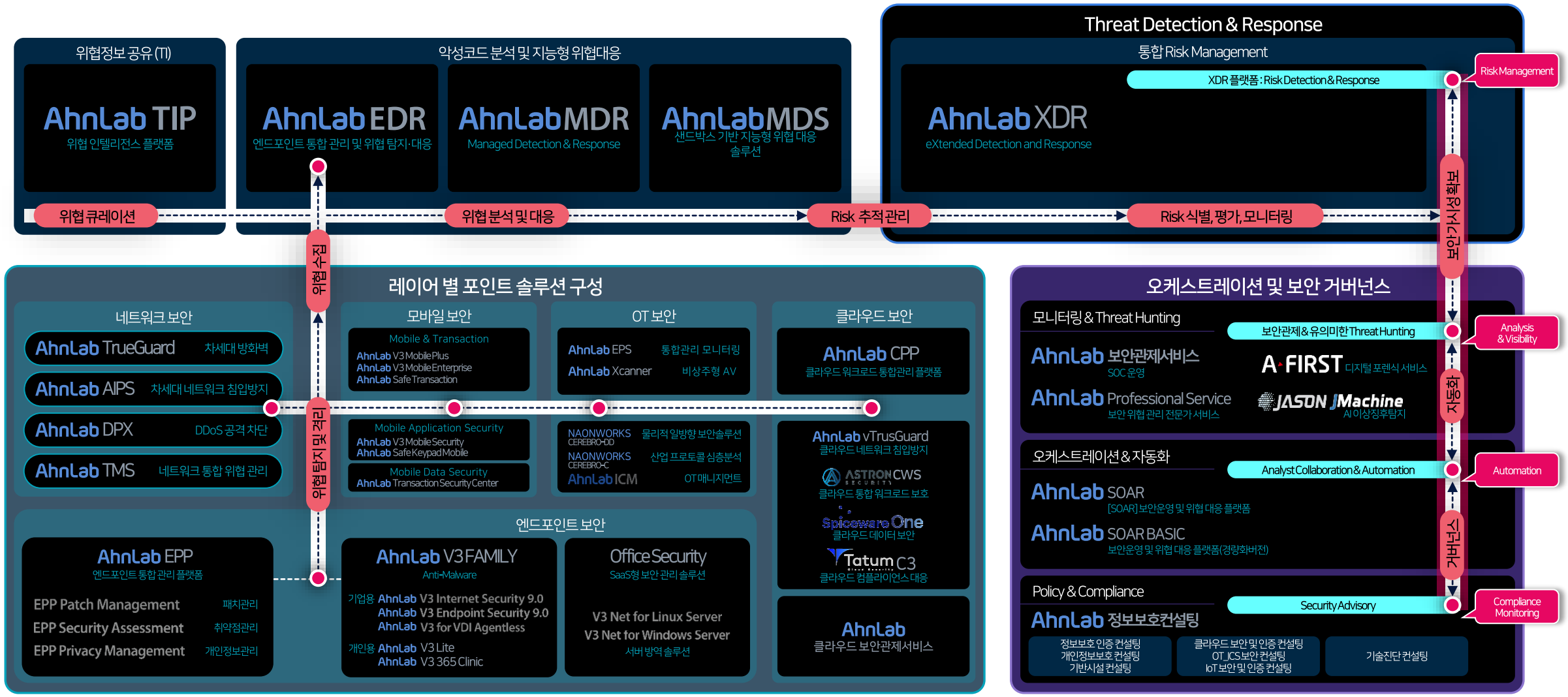
AhnLab 솔루션/서비스 맵

AhnLab

AhnLab이 그리는 보안 아키텍처



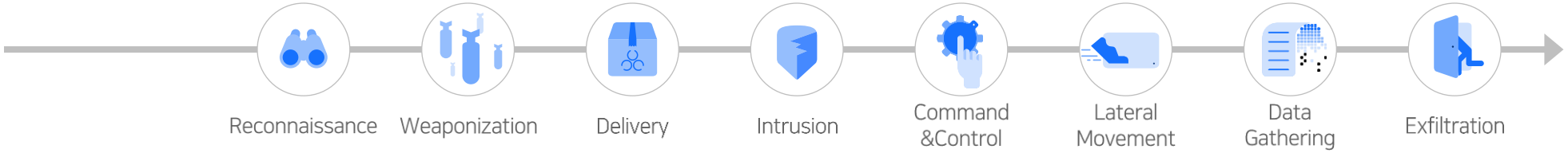
AhnLab 보안 솔루션/서비스 매핑



AhnLab TIP 소개

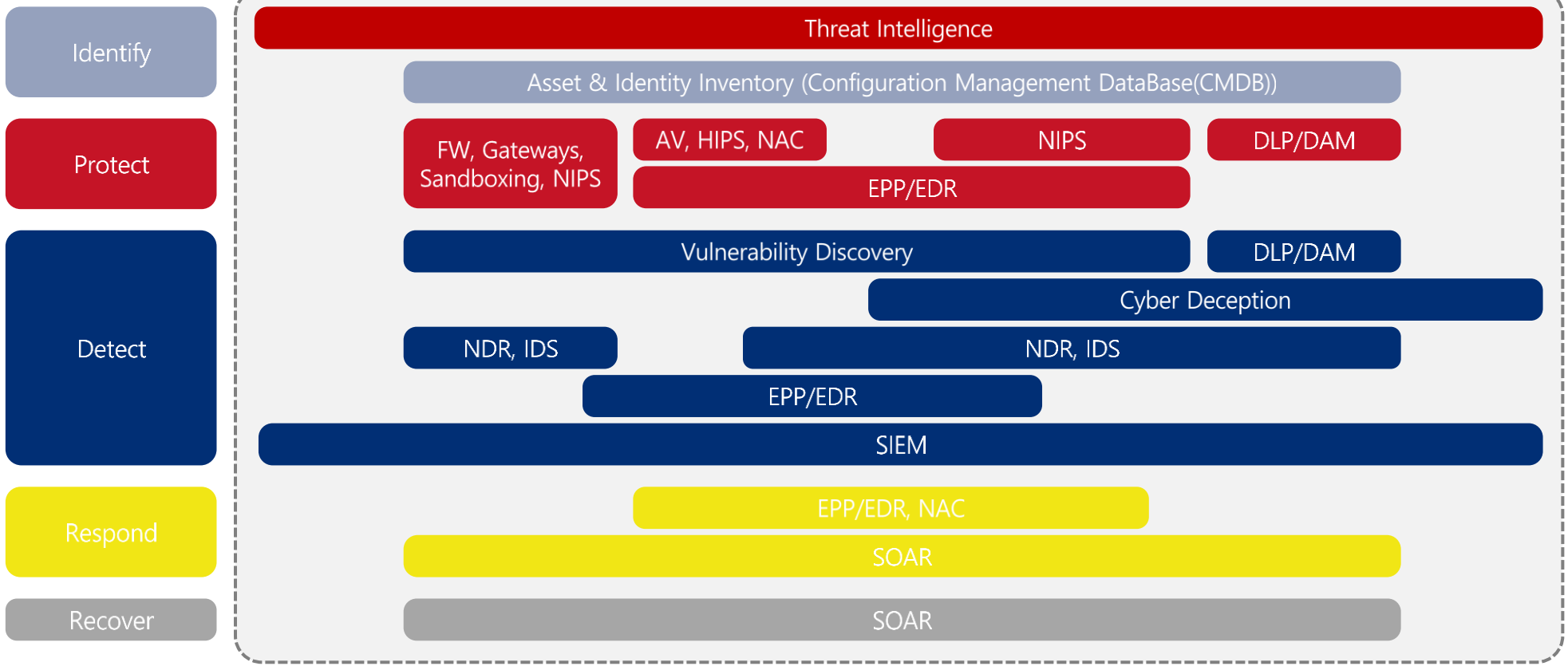
AhnLab

사이버 공격 절차(Cyber Kill Chain)에 따른 식별 및 차단 솔루션



NIST
Cyber Security Framework

TOOLS FOR CYBER DEFENSE PLATFORM

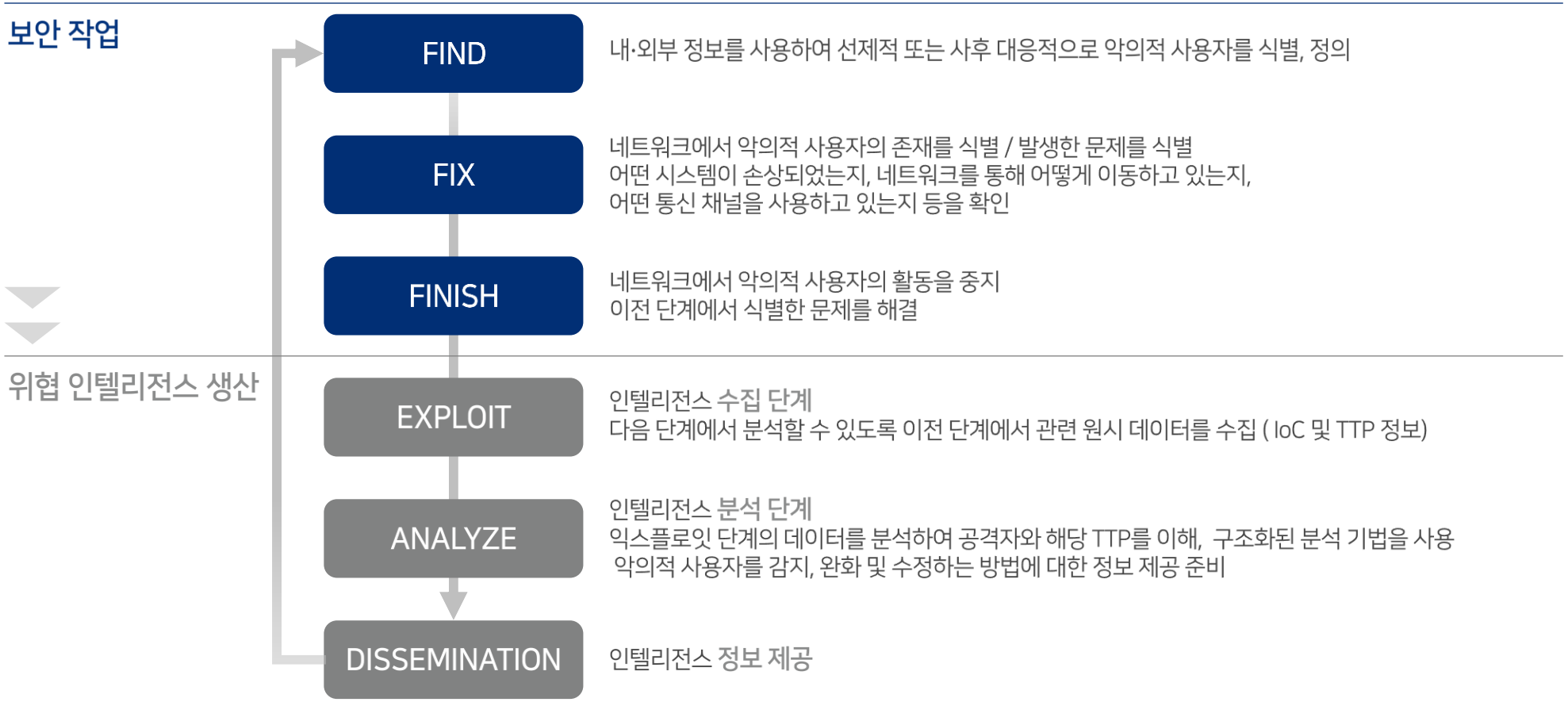


출처 : https://www.terreactive.ch/en/node/164

미군 정보 작전 사이클 – F3EAD (사이버 위협 대응 관점)

서구권 군대에서 사용되는 특수 작전 사이클 (미국 특수 작전 부대가 개발 한 F3EAD 사이클)

- 타겟을 찾고(Find) 확정 짓고(Fix) 끝장내고(Finish) 비평하고(Exploit) 분석하고(Analyze) 배포(Dissemination)하는 일련의 사이클을 뜻합니다.
- 주로 드론 타격과 특수부대 작전을 통한 요인 암살을 위한 프로세스를 사이버 보안에도 적용하여 활용 중



미군 정보 작전 사이클 – F3EAD 기반 Threat Intelligence 개념도

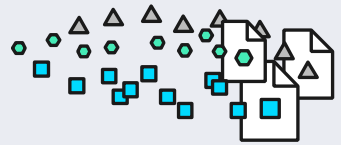
FINISH → FIX → FIND

또는 1단계와 동시 진행

① 위협 정보 수집

AhnLab
Threat Intelligence
Platform

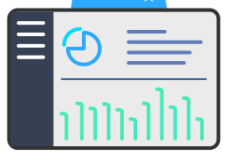
- AhnLab Telemetry (NW,EP, Mobile, etc.)
- Threat Research & Analysis Team
- CERT
- Security Partners
- Web Crawlers
- Botnet Monitoring
- Cloud Sandbox
- Open Source
- SNS, etc. .....



수집 정보를 유형별로 분류하여
체계적으로 저장

② 위협 정보 분석

TIP
Infrastructure

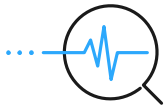


- 수집 정보의 유입 정보 분석
- 수집 정보의 평판 검증
- 수집 정보의 정적 분석
- 수집 정보의 행위 정보/동적 분석
- 통계 및 연관성 분석

- 위협 데이터셋 생성
- 침해사고 데이터 및 분석 정보 분류
- 사이버 위협 관련 실시간 이슈 정보 분류

③ 위협 정보 제공

고객사



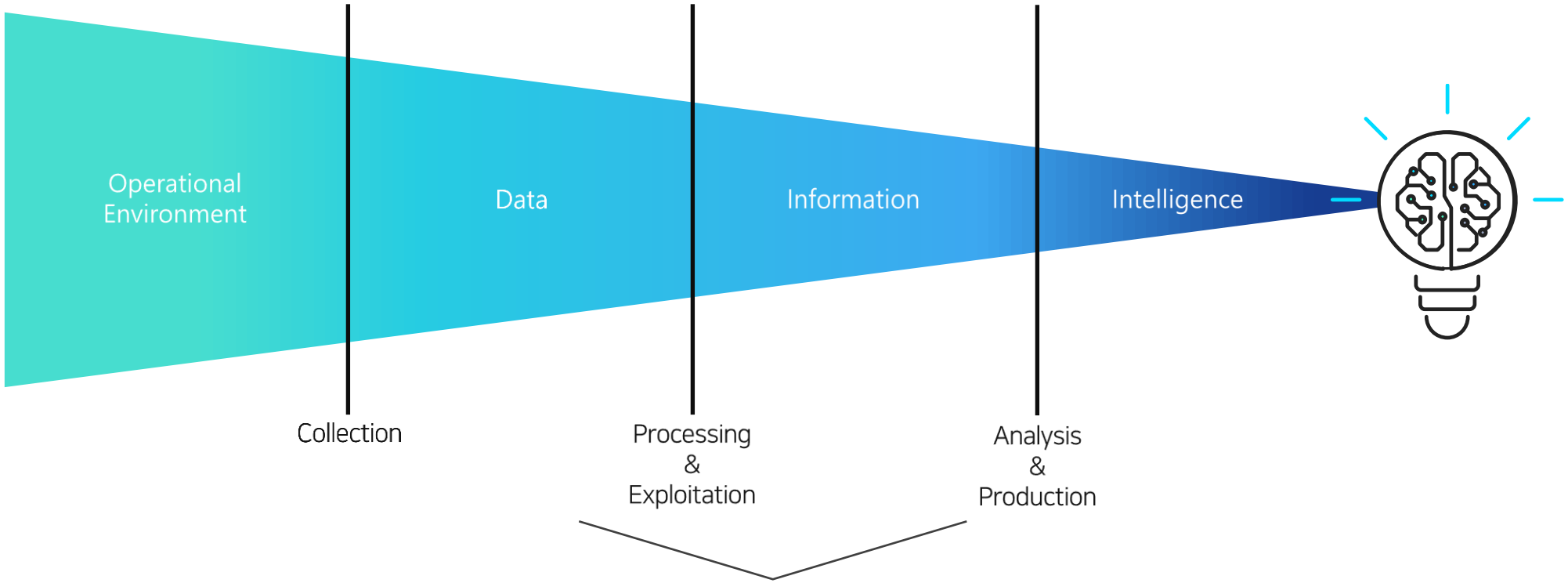
식별되지 않은 추가
위험을 예측하기 위해
의사결정자에게
제공되는 정보

임박한 위험에
대응하기 위해
상위 관리자에게
제공되는 정보

공격 및 공격 징후에
대응하기 위해 보안
실무자들에 제공되는
침해 지표와 같은 정보

정보의 수집 – Relationship of Data, Information, and Intelligence

데이터, 첩보(Information), 정보(Intelligence)의 관계 **(출처 : 미 육군 합동교범 2-0)**

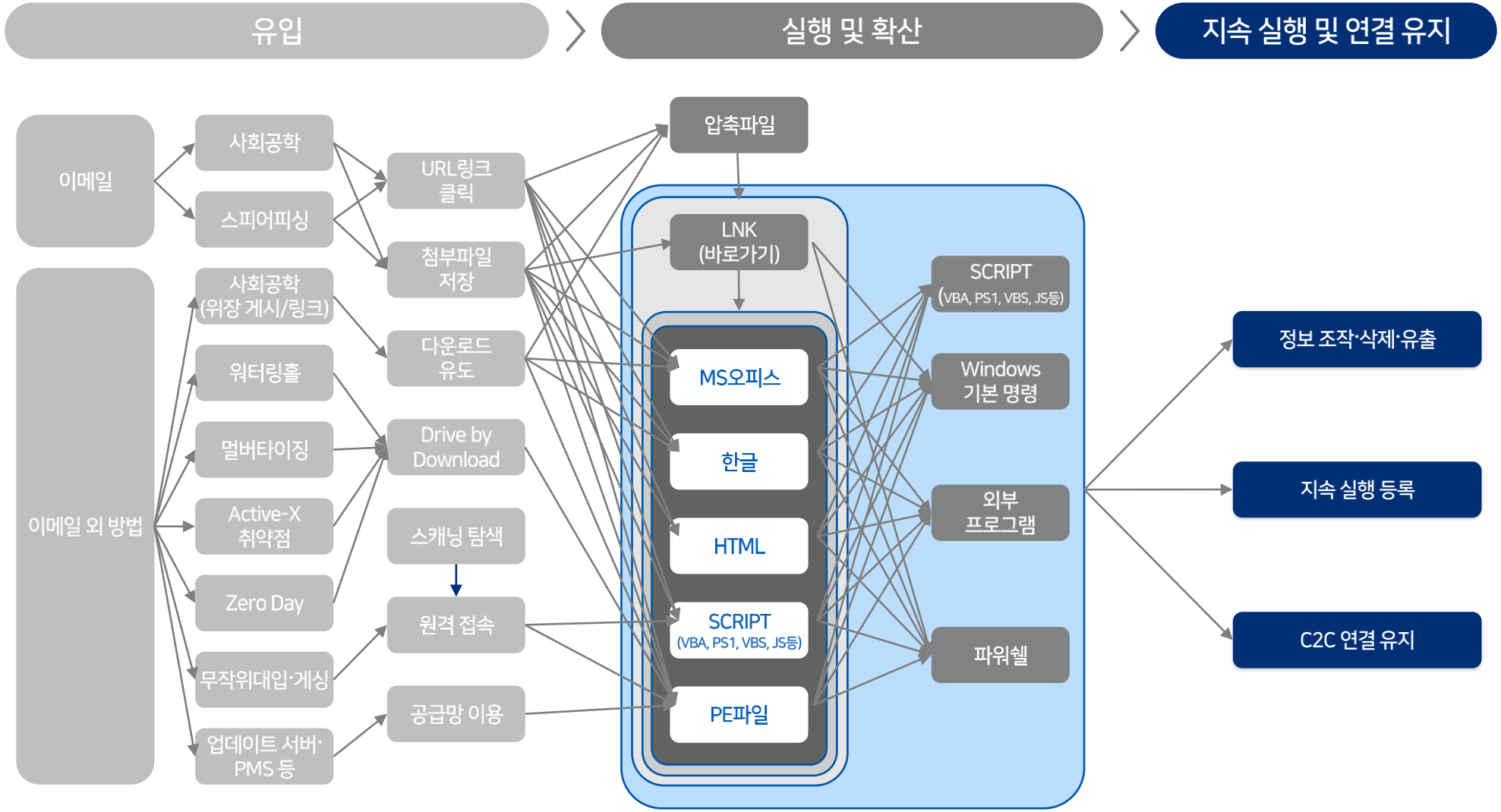


기술 Tactical
일반적인 정보

관리 Operational
정보의 조합, 공유

전략 Strategic
공격 전략, 사용된 기술, 공격 절차의 종합적인 분석

정보의 수집 – 공격 분석을 통한 공격 기법 및 침해 지표 수집



출처 : 2019 사이버 위협 인텔리전스 보고서, 금융보안원

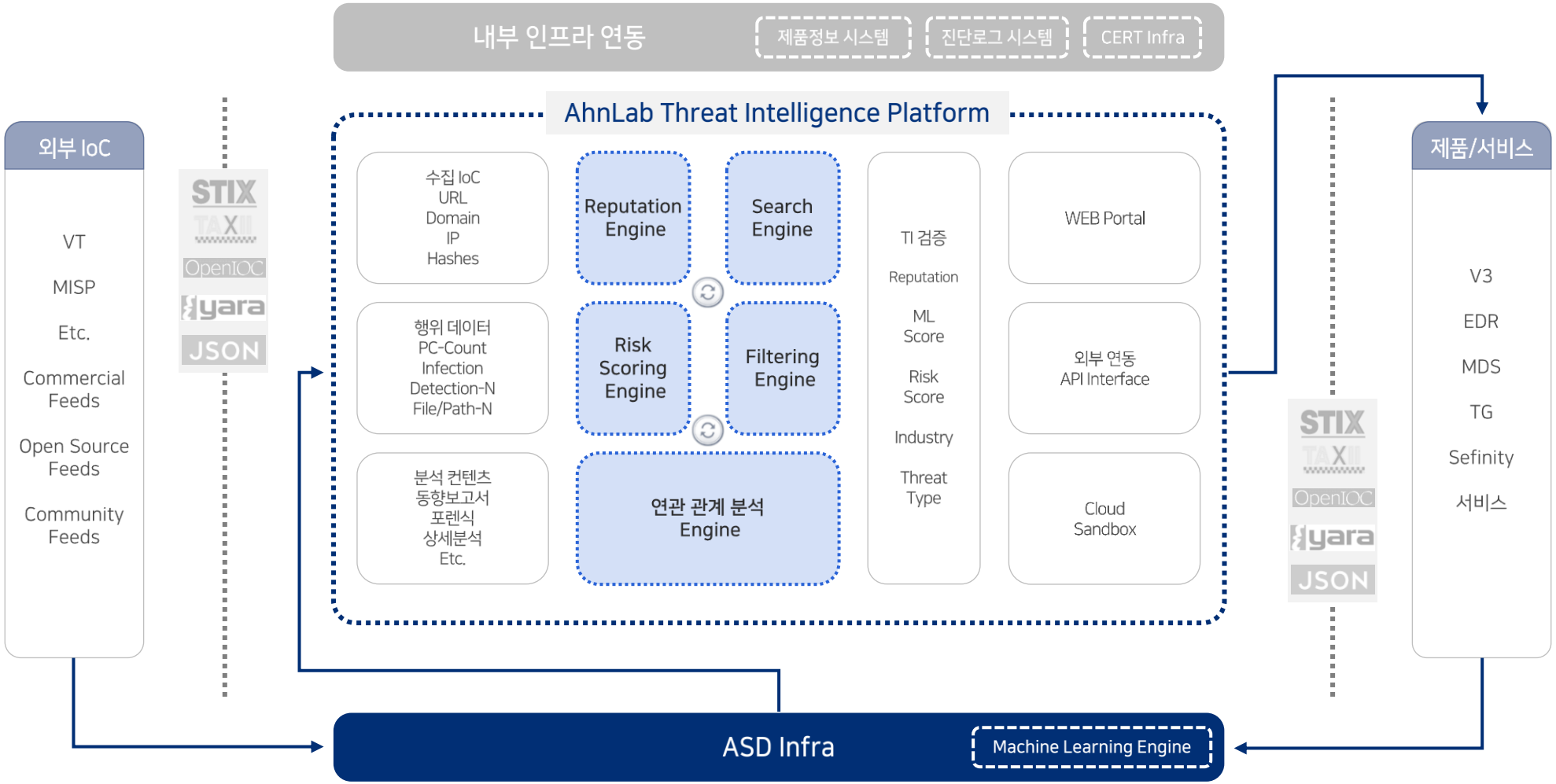
정보의 분석 - AhnLab의 Threat Contents ‘Curation’

전문 기술 및 노하우가 결합된 탁월한 시큐리티 인프라 기반의

THREAT INTELLIGENCE PLATFORM

정보의 분석 - AhnLab의 CTI 정보 제공 프로세스

정보 수집 / 데이터 분석 / 자동화



정보의 제공 – 식별 가능한 위협 정보

TIP를 통해 식별 가능한 정보

사이버 위협 또는 취약점 분석 등 악의적인 목적의 정보 수집 행위	Attack Pattern
보안통제 기능을 무력화하거나 보안 취약점을 악용한 공격 행위	Campaign
보안통제 기능의 무력화 또는 보안취약점을 악용한 공격을 통해 이용자가 정보시스템 또는 저장된 정보에 적법한 접근을 가능하게 하는 방법	Course of Action
보안 취약점 정보	Indicator
악의적인 목적의 사이버 C&C (Command & Control)	Intrusion Set
사이버 위협으로 인한 정보유출 등 침해 사고로 인해 발생 또는 발생 가능한 위해 요소	Malware
기타 사이버 보안 위협을 유발하는 요인 및 속성	Observed Data
상기에 명시된 사항들의 종합된 정보 등	Report
	Threat Actor
	Tool
	Vulnerability
	Score

위협 인텔리전스

Threat Actors - Threat Actor 특징

Threat Actor

위협 행위자, 위협 그룹, 공격 그룹, 해킹 그룹 등으로 번역

악의적인 행위를 수행하는 개인 또는 그룹

국가 지원, 사이버 범죄자, 핵티비스트, 테러리스트 등

목적 (금전 이득 혹은 정보 유출)

확실한 공격 목표

지역화

익숙한 공격 방식 유사한 악성코드와 도구 사용

동일한 버릇, 습관

지속적 공격 시도

사실상 직장인. 공무원 ? 군인 ?

방심해 종종 실수 -> 결국 사람

Threat Actors - 단서

Attack Vector

- 공격 방식
- 공격 대상, 동기 → 누구의 이익 ?
- 사용 취약점

인프라

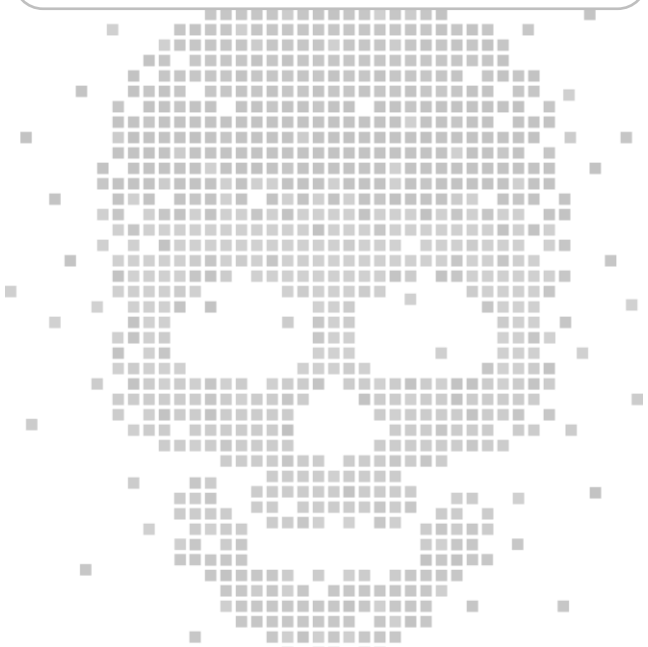
- 발신자, URL, IP
- C&C 서버 (Webshell, 운영 도구 및 방식)
- C&C 서버 운영 시간

도구

- 동일 버전 도구

악성코드

- 파일 생성 경로, 파일 이름, 레지스트리, Mutex, 파일 생성 시간, 서비스 이름
- 제작 언어, 컴파일러 버전, PDB, Rich Header
- 유사 악성 코드 (코딩 스타일), 특징적 문자열 (동일 문자, 암호 등)
- 아이콘, 속성 (버전, 이름, 언어 등), 인증서



기타

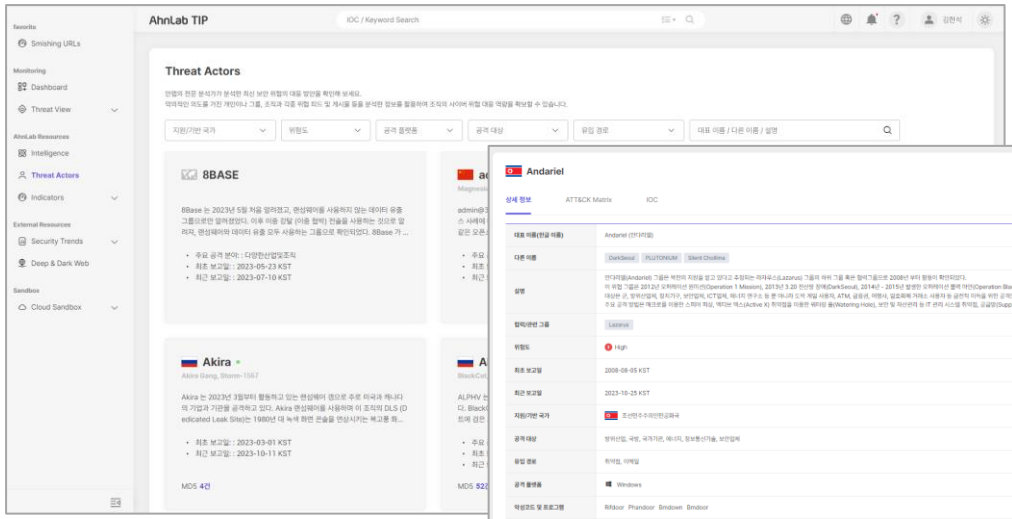
- 언어 (오타, 특정 언어 포함 경로)
- 버릇, 습관
- 실수 (실제 IP, 메일주소 노출)

Threat Actors - 정보 제공

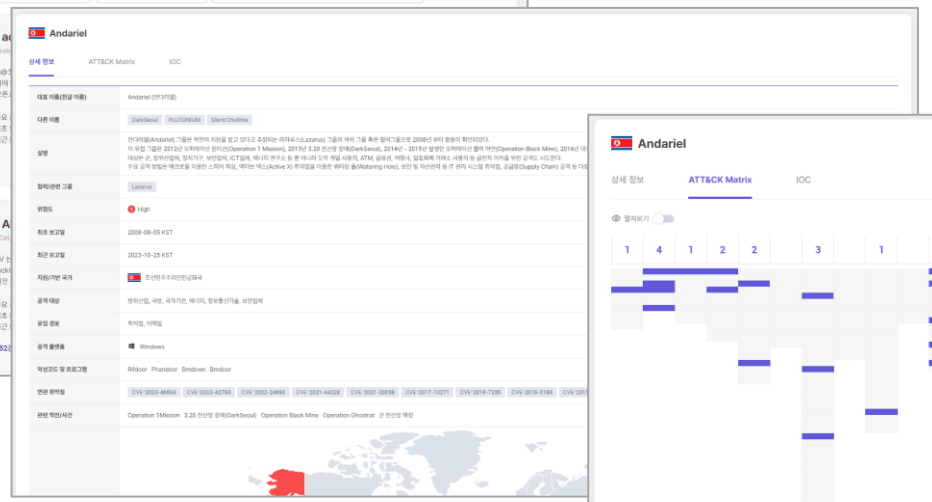
정부기관이나 기업을 대상으로 공격을 하거나, 이슈가 되는 공격 그룹을 별도로 관리해서 모니터링

Threat Actors + Motivations + Attack Trends + Threat Surface RISK + IOCs

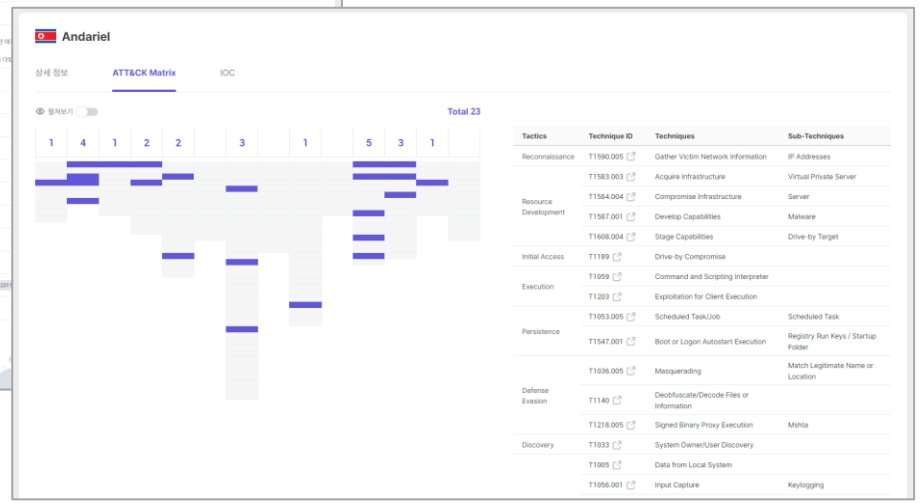
공격자 그룹



공격 그룹 정보



상세 분석 정보



ATT@CK Matrix

Use Case - Lazarus 공격 사례 (타임라인)

2023. 02. 28
안랩 TIP 포렌식 보고서

1 공공 기관 및 대학 등에 널리 사용하는 공인인증서 소프트웨어의 0-Day 취약점을 이용한 Lazarus 공격 그룹 공격 사례

안랩 TIP 선 공개

2023. 03. 13 KISA 보안공지
2023. 03. 21 KISA 보안공지

2 금융 보안 솔루션 업데이트 권고
드림시큐리티 사의 MagicLine 취약점 보안 업데이트 권고

KISA 보안 공지

2023. 03. 25
보안뉴스

3 공인 인증 솔루션 'MagicLine4NX' 취약점…북한 라자루스의 악용 흔적 발견

다수 보안매체 기사화

2023. 06. 28
국가정보원

4 국정원, '보안인증 S/W 취약점' 악용 해킹 확산 경고

국정원 보도자료

Use Case - IOC 정보를 활용한 선제적 대응

기사화 내용으로는 확인 불가한 정보

공격 대상은 누구? **Public / Education**

Lazarus 공격 그룹이 사용한 악성코드 정보는?

Lazarus

상세 정보 | ATT&CK Matrix | IOC

연관 IOC

MD5 939건 | SHA-1 2건 | SHA-256 0건 | URLs 81건 | Domains 6건 | IPs 78건

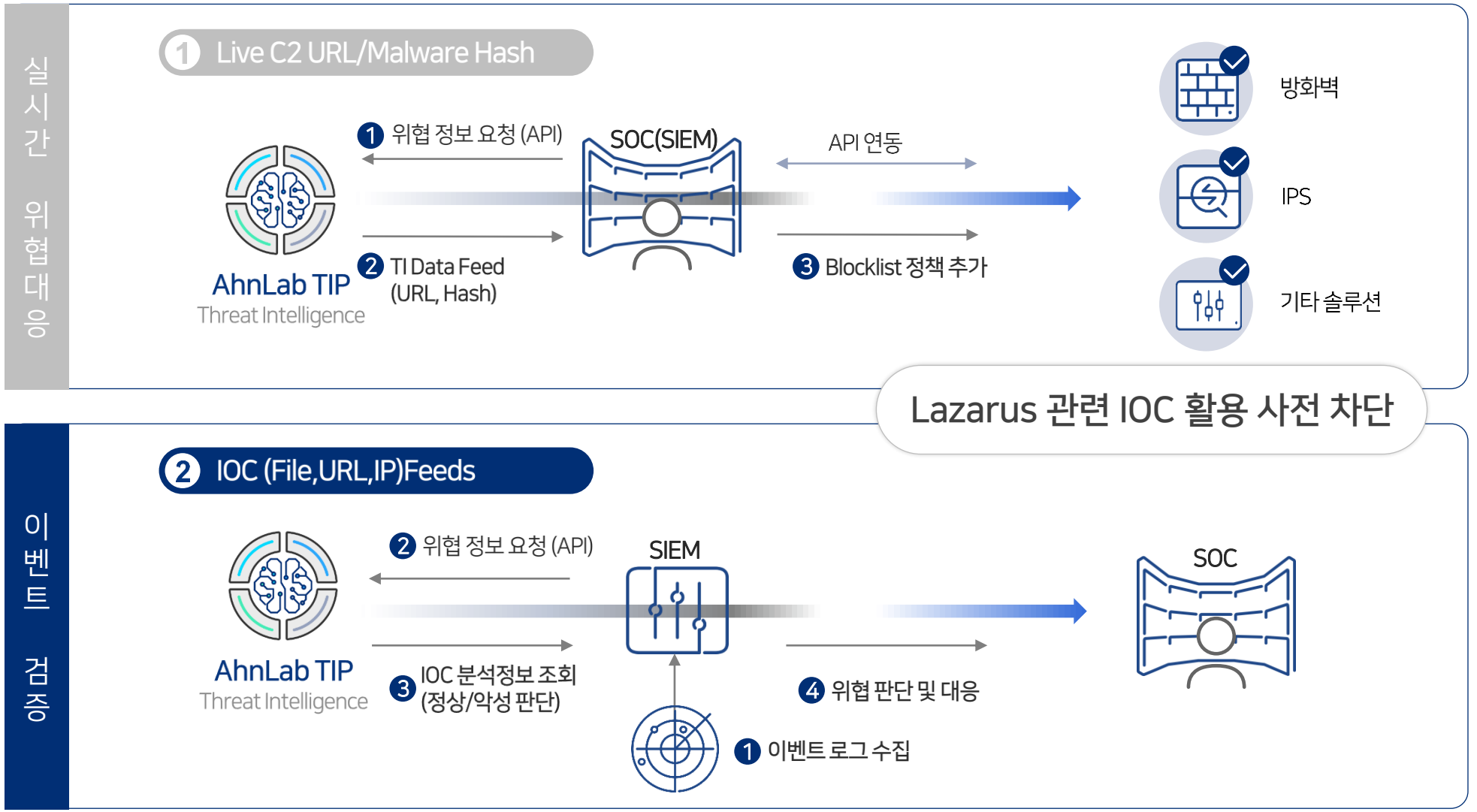
File Name	Hash(MD5)	진단명	진단 버전
java8.exe	08883d753154589a76347fda9e2799c0	Infostealer/Win.Outlook	2023.04.09.03
cryptrsa.cpl	0ade34f05a150af07e3406b719e18fb8	Trojan/Win.LazarLoader	2023.05.16.00
DevSync.cpl	1883e0ab8e2c8ee3e2dccfd7bf95fcfe	Trojan/Win.Lazardoor	2023.02.17.03
scrapkisvc.dll	19063f1f2136fd32e37371cdb2d871cd	Trojan/Win.LazarLoader	2023.05.17.00
pchealthsvc.dll	1dd5e8ff30df1ed5fc1b303c39a92e65	Trojan/Win.LazarLoader	2023.04.29.00

공격에 사용된 IP/URL 정보는?

No	IP	URL	Country
1	111.92.189.48	www.scope.co.kr	KR
2	121.78.158.46	www.studyholic.com	KR
3	121.78.246.155	dalbinews.co.kr	KR
4	183.110.224.172	ctmnews.kr	KR
5	115.68.52.47	www.artinsight.co.kr	KR
6	114.108.129.89	www.kfcjn.com	KR

Use Case - API 활용 신속한 대응 체계 구축

API 활용 범위
IOC 분석정보 조회
파일 분석 정보 조회
URL 분석 정보 조회
Domain 분석 정보 조회
IP 분석 정보 조회
TI Data Feed
File Data All Feed
URL Data All Feed
IP Data All Feed
Live C2 URL Data Feed
Smishing URL Feed
Cloud Sandbox
파일 분석 요청
URL 분석 요청
분석 상태 조회
분석 결과 조회
분석 요청 이력 조회

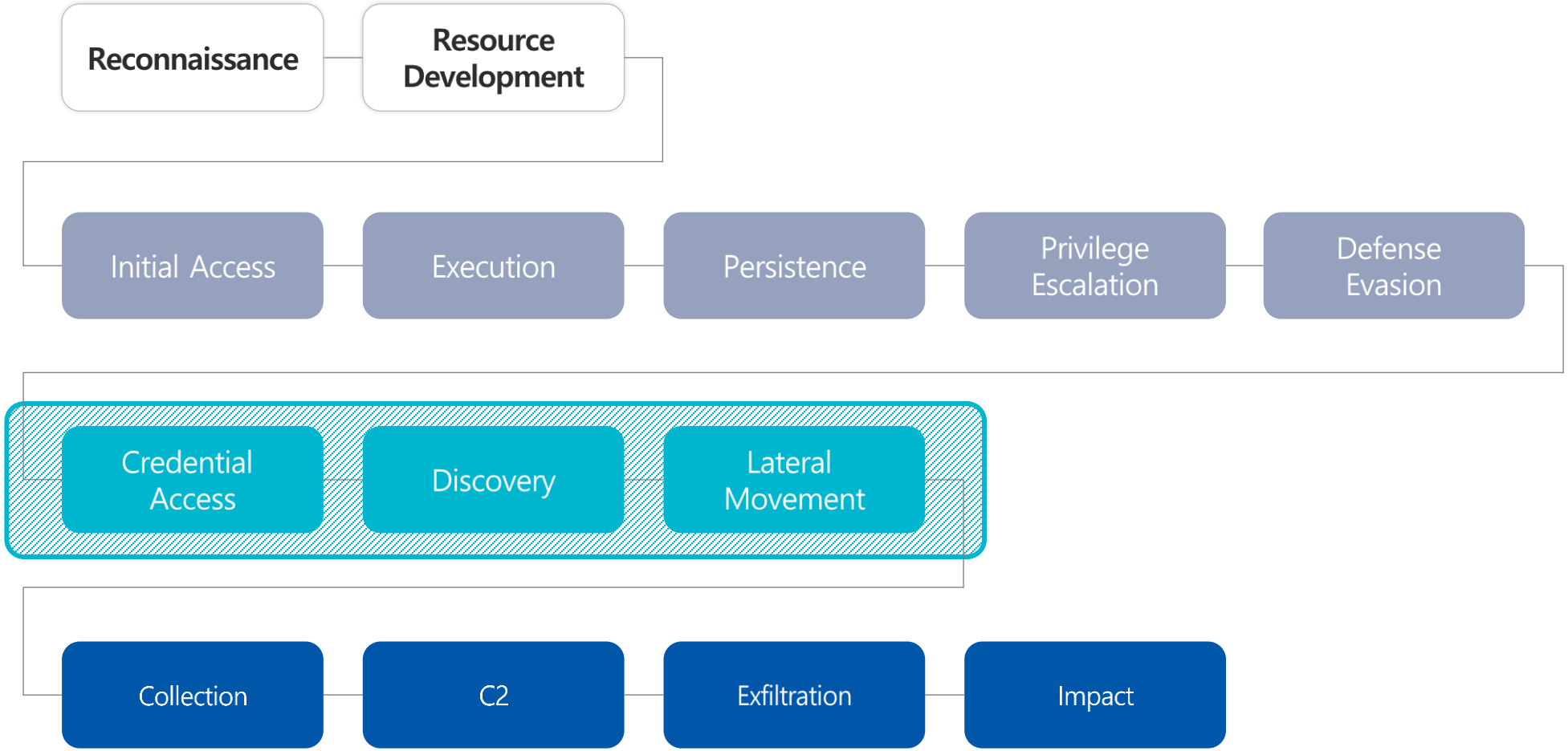


AhnLab EDR 소개

AhnLab

조직의 APT 공격 피해 단계

MITRE ATT&CK TACTICS



0 단계

피해 없음

1 단계

최초 침해 시스템 피해에 그침

2 단계

조직 전체로 피해 확산

3 단계

데이터 유출 및 랜섬웨어 감염

시사점

조직 전체로 피해가 확산되는 **Lateral Movement 단계에서 탐지 및 차단**해야 한다.

0 단계
피해 없음

- 공격자의 준비 과정

공격자의 행위 파악이 어렵다.
최근 활동중인 공격그룹의 전략(TTP)과 타깃을 파악하는 것이 필요하다.

1 단계
최초 침해 시스템 피해에 그침

- 공격자의 최초 침해 시스템
  - 설정 미흡, 소프트웨어 취약점, 사용자의 실수
- 악성 코드에 감염되는 사건들이 대부분 여기에 해당

완벽하게 막는 건 불가능하다.
하지만, 피해는 크지 않다.

2 단계
조직 전체로 피해 확산

- APT로 발전되는 단계
- 정상 행위와 악성 행위의 판별이 어려움
- 단일 보안 솔루션만으로 해결하기 어려움

하지만, 이 단계를 막아내면,
피해는 크지 않다.

3 단계
데이터 유출 및 랜섬웨어 감염

- 실질적 피해 발생

공격자가 2단계까지 성공했다면,
3단계를 막기는 어렵다.

The EDR is ...

수집(Collect)할 수 없는 대상(Object)은 분석(Analyze)할 수 없다.

분석(Analyze)하지 못하면 악성 또는 정상 여부를 확인(Confirm)할 수 없다.

악성으로 확인(Confirm)하지 못 했다면 대응(Response)도 할 수 없다.

분석(Analyze) 결과를 패턴(Pattern)화하지 못하면
동일한 위협(Known attack)을 자동 탐지(Automatic Detect)할 수 없다.

패턴(Pattern)화하는 작업 자체를 자동화(Automate)할 수 없다면
신종 위협(Unknown attack)에 실시간으로 대응(Real-time Response)할 수 없다.

- Collect
- Object
- Analyze
- Confirm
- Response
- Pattern
- Automatic Detect
- Automation of creating pattern

Endpoint Detection & Response

EDR(Endpoint Detection & Response) 정의 및 영역

EDR이란 엔드포인트 레벨에서 지속적인 모니터링과 대응을 제공하는 보안 솔루션으로,
▲보안 침해 탐지(Detect security incident) ▲엔드포인트에서의 보안 침해 억제(Contain the incident at the endpoint)
▲보안 침해 조사(Investigate security incident) ▲치료를 통한 감염 이전 상태로의 회복(Remediate endpoint to a preinfection state) 등 4가지 기능을 제공해야 한다.
EDR은 사전 또는 실행 단계에서 위협을 자동으로 차단하는 것이 아니라 적절한 엔드포인트 위협 가시성을 제공해 지능형 위협을 발견하고 조사 및 대응하는데 기여한다.

*출처: Gartner

EDR 핵심 역할

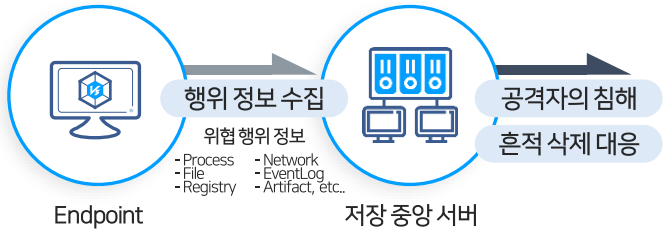
핵심역할.01

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



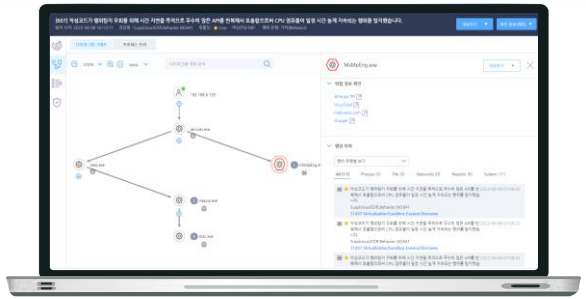
위협 행위 정보 저장

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

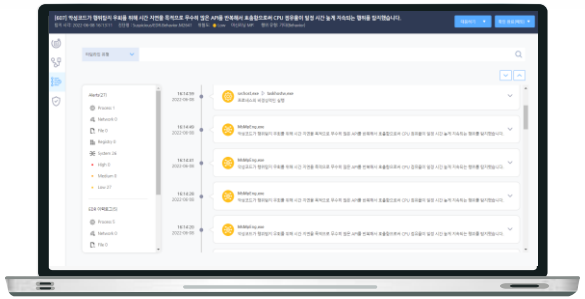
핵심역할.02

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
- Lateral Movement 위협 조기 탐지



핵심역할.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 이해제공
  - 위협 종류, 유입 경로, 행위, 연관 관계 등 상세한 정보 파악 및 대응

EDR 활용 위협 탐지·분석·대응 고도화

백신 (AV)

백신(AV)는 알려진 악성코드(파일)를 가장 빠르게 대응합니다.

#알려진 악성파일 #시그니처(DB)
#엔드포인트 보안

Sandbox (APT)

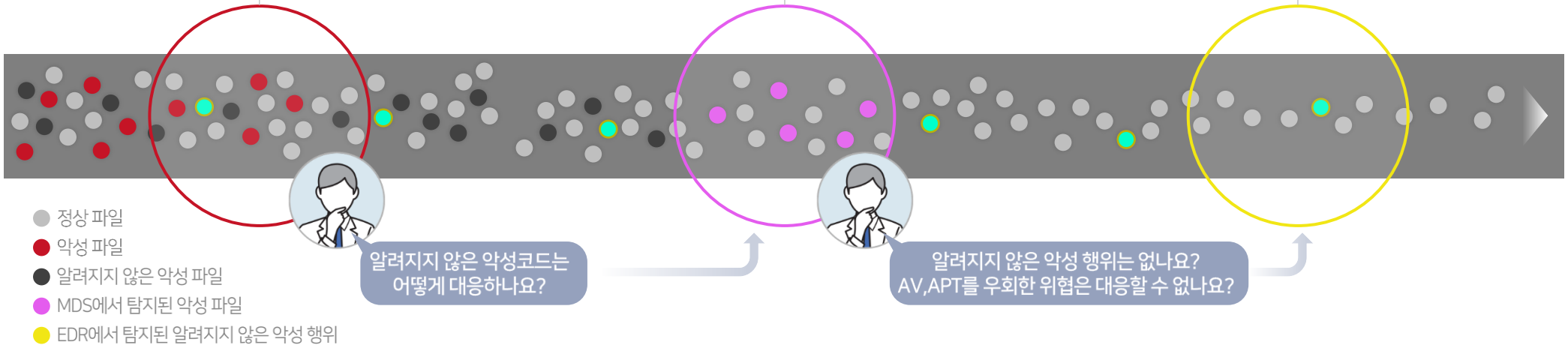
Sandbox 기반 분석 솔루션은 알려지지 않은 악성코드(파일)를 탐지하고 대응할 수 있습니다.

#알려지지 않은 악성파일
#샌드박스 #네트워크 보안

EDR

EDR은 엔드포인트에서 발생하는 모든 행위를 감시하고 저장합니다.

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



주요 특장점 – 통합 플랫폼 기반 통합 에이전트

Plug-in 방식의 라이선스 추가만으로 부담 없이 설치 가능 (병렬 구조의 분석 서버 추가 필요)

주요 특장점 – MITRE ATT&CK 평가 참여

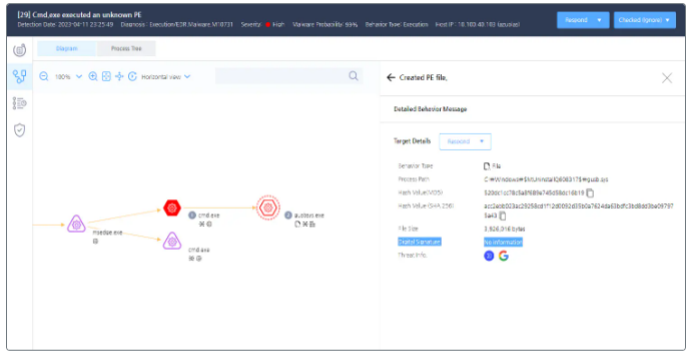
국내 EDR 벤더 유일 MITRE ATT&CK 평가 지속 참여

Round 5

1. 러시아 기반의 TURLA 공격 그룹이 사용하는 여러 공격기법 모의 수행
2. AhnLab EDR이 평가 환경에서 이뤄지는 공격들을 탐지
3. 결과 발표
4. 평가 결과를 제품에 반영해 지속적인 발전 체계 구축

AhnLab

Tactic



Data Source

Process: Process Metadata

Footnote

Due to Red Team tool leakage, the installer on azuolas filename changed from gupsys.exe to gusbsys.exe

- 고도화된 실제 위협 대상 탁월한 탐지 역량 검증

MITRE ATT&CK Evaluations – 2023년 평가 결과

SOMMA

Somma

MITRE ENGENUITY | ATT&CK® Evaluations

Detection Key

More Specific — Less Specific

AhnLab

AhnLab

Genians

EST SECURITY

평가 미참석

주요 특장점 - 국내 제조사 최대 위협 탐지 룰셋 보유

Windows 기반 1,000개 이상, Linux 기반 100개 이상의 탐지 룰셋 적용 및 지속 업데이트

유형	룰셋명	TTPs	행위 예시
Lazarus 공격 기법 EDR 룰셋	InitialAccess/EDR.Lazarus	T1190,TA0001	특정 버전 MagicLine 인젝션 행위
	SystemManipulation/EDR.Rootkit	T1014	Lazarus 그룹이 사용하는 BYOVD 드라이버 파일 생성
	SystemManipulation/EDR.Event	T1543.003,T1574.011	넷클라이언트 이상 행위
	Injection/EDR.Lazarus	T1055	특정 쉘코드 패턴
	Injection/EDR.Lazarus	T1055	Lazarus 인젝션 행위
	Fileless/EDR.Event	T1055	DLL-Sideloading (정상 파일에 PE 파일 스레드 인젝션)
	Fileless/EDR.Event	T1055	3CX 인젝션 행위
	Injection/EDR.Lazarus	T1055	MS 정상 프로세스에 인젝션 하는 행위
	InitialAccess/EDR.Lazarus	T1190,TA0001	VestCert가 파워쉘 실행하는 행위
	InitialAccess/EDR.Lazarus	T1190,TA0001	MS 정상 프로세스에 인젝션 하는 행위
	InitialAccess/EDR.Lazarus	T1190,TA0001	의심스러운 파일 생성

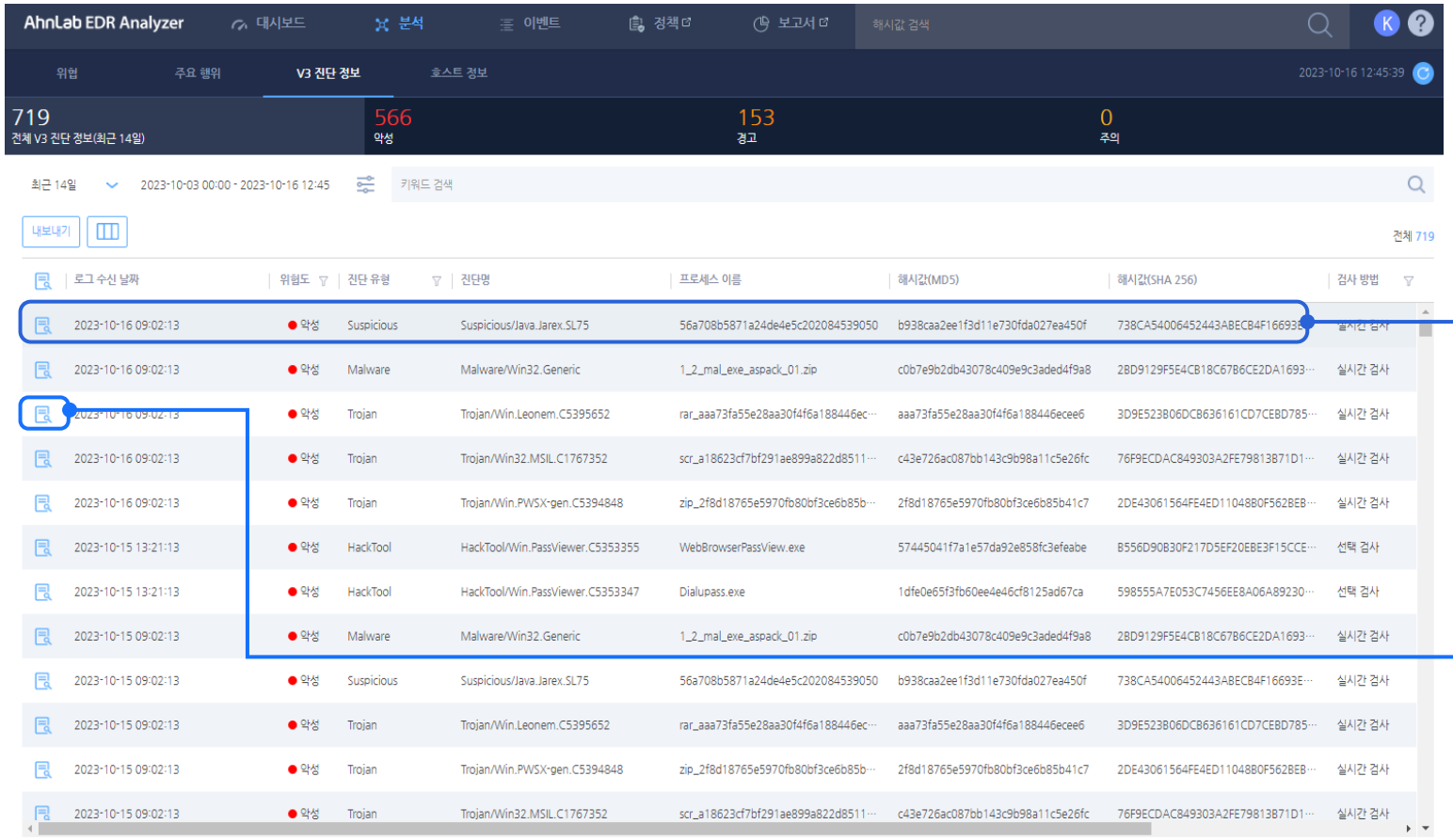
주요 특장점 – V3 연동 APT 전용 진단 룰

V3 TS 엔진의 메모리 진단과 AMSI 진단 기법으로 EDR 전용 APT 진단 룰 탐지 및 위협 구분

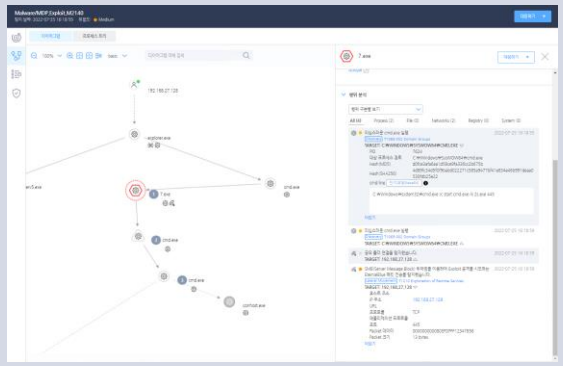
공격 그룹		탐지 포인트
Kimsuky	**Kimsuky (북한 추정)** - 타겟: 초기 국내 북한 관련 연구기관 및 에너지 기관, 금융기관 등, 2017년 이후 다른 나라 확대	✓ 워드문서 매크로 코드 탐지 ✓ VBS/JS 스크립트 파일 탐지
Lazarus	**Lazarus(Hidden Cobra), (북한 기반)** - 타겟: 국내 대기업, 금융기관, 국방부, 전 세계 방위산업/첨단산업/IT 업체 등 - 공격기법: 스피어 피싱, 공급망 공격, DDoS 공격	✓ 한글문서 내부 BAT스크립트 파일 탐지 ✓ 프로세스 메모리 코드 패턴 탐지
Andariel	**Andariel (북한 추정)** - 타겟 : 국내 금융기관, 군, 방위산업체, 정치기구, 보안업체 - 2013년 3.20 전산망 장애(DarkSeoul), 2014년 - 2015년 발생한 오퍼레이션 블랙 마인(Operation Black Mine), 2016년 대기업 전산망 해킹	✓ Beacon 백도어/Stager 탐지 ✓ 코발트 스트라이크 툴 탐지
TA505	**TA505 공격그룹 (러시아 기반)** - 타겟: 주로 금융권/에너지 업종, 일반기업으로 확대 중 - 공격기법: Dridex, Locky,Flawed Ammyy, Clop 등 랜섬웨어	✓ 메모리 내 TinyMet 다운로더 실행 탐지 ✓ 코발트 스트라이크 툴 탐지
Tonto	**Tonto 공격그룹 (중국 기반)** - 정보탈취 목적 - 타겟: 국내 및 일본, 금융기관/군사기관/방위산업/항공우주/IT업체 - 공격기법: 스피어피싱, 권한상승, 내부이동 등	✓ 악성 스크립트 탐지 ✓ 코발트 스트라이크 툴 탐지

주요 특장점 – V3 연동 알려진 악성코드 유입경로 분석

V3가 진단한 알려진 악성코드 대상 유입경로 및 프로세스 이벤트 흐름도 제공



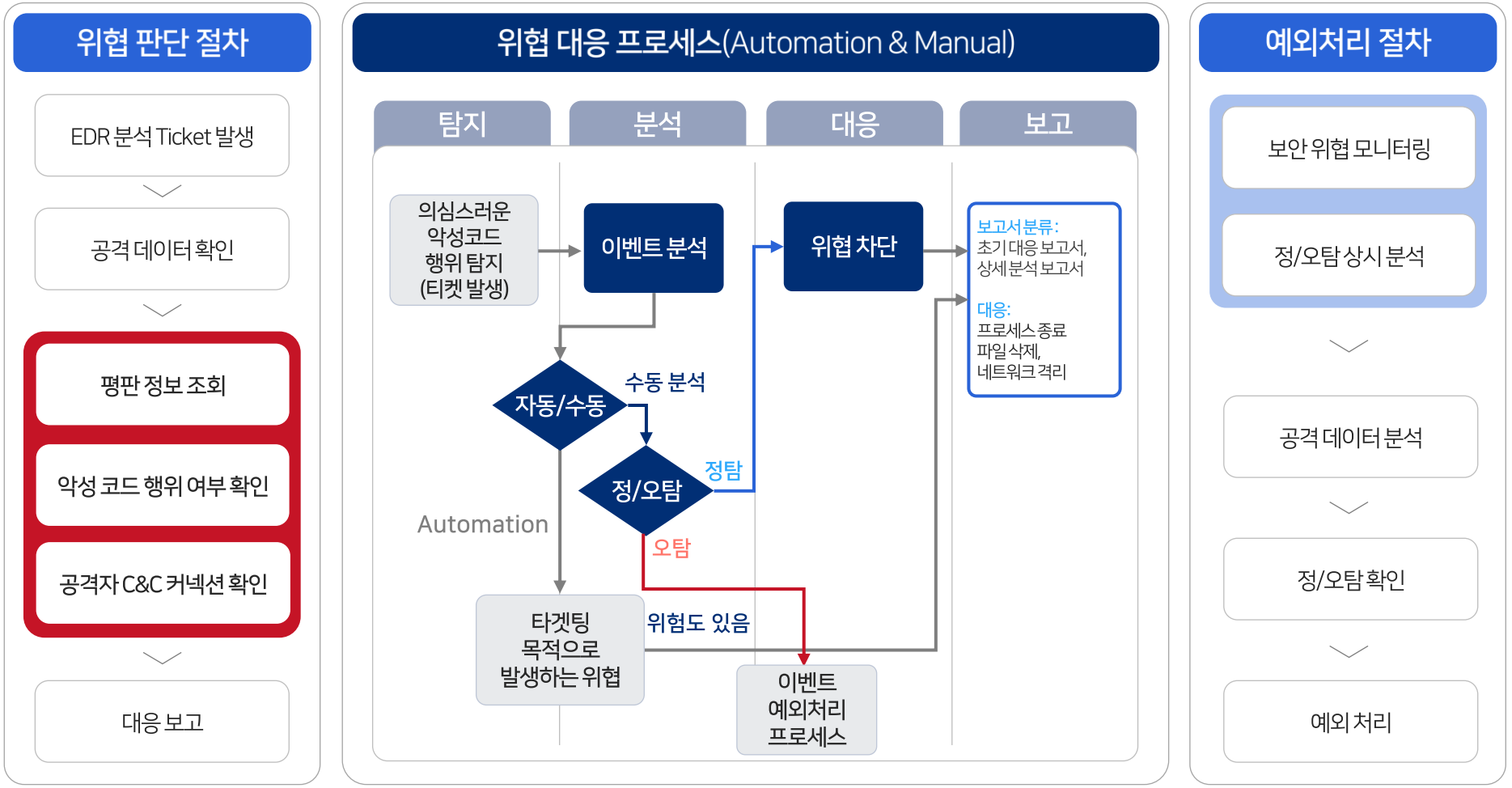
항목	내용
탐지날짜	악성코드가 탐지된 Client Time
위험도	악성 / 경고 / 주의
진단유형/진단명	악성코드 진단유형 / V3 진단명
프로세스 이름	감염된 파일 이름
Hash	감염된 파일 Hash(MD5, Sha256)
검사방법	실시간검사, 정밀검사, 예약검사, USB검사, 평판기반 실행차단, 기타검사
엔진버전	진단된 V3 엔진 버전
상태	악성코드 처리 상태 정보(삭제/프로세스 종료 등)
호스트 정보	이름, 마지막 로그인 사용자, OS, 호스트ID, 소속부서



On-Demand 분석 결과

주요 특장점 – MDR 서비스 제공 (1/2)

Online, Offline 등의 다양한 방식의 MDR 서비스 수행



주요 특장점 – MDR 서비스 제공 (2/2)

EDR에서 탐지된 위협 및 의심 행위에 대한 분석 및 대응 내역에 대한 정보 및 위협 완화 및 복구를 위한 조치 가이드도 함께 제공

MDR 초기 대응 보고서

안녕하십니까? 종합 정보보호 전문기업 AhnLab 입니다.
귀사에 대한 보안 모니터링 중 다음과 같은 위협 이벤트를 발견하여 보고 드립니다.

탐지 정보

고객사	안랩		
시나리오	Behavior/EDR.Download.M3900		
티켓 번호	R22070510112802663	위협도 등급	Low, Medium, High
발급 시간	2022-10-12 16:05:00 (+09:00)	탐지 시간	2022-10-12 16:03:58 (+09:00)
보안 시스템	EDR Server (211.233.40.134)		

상세 정보

호스트	192.168.48.128	호스트 이름	DESKTOP-VM
파일 경로	C:₩Users₩user₩Downloads₩attach		
이벤트 정보	악성코드를 다운로드하는 행위를 탐지했습니다.		
탐지 데이터	c:₩work₩xxx.exe Normal(current_hash_chkresult) C:₩Windows₩system32₩windowspowershell₩v1.0₩powershell.exe Normal (current_hash_chkresult) C:₩Windows₩system32₩bcdedit.exe Normal(current_hash_chkresult) ₩??₩C:₩Windows₩system32₩conhost.exe 0xffffffff -ForceV1 (자동 삽입 영역)		

분석가 판단

* **악성행위 :** 악성코드 다운로드, AhnLab V3 종료
  악성코드의 실행이 확인되었습니다. 악성코드의 유입 경로는 아래와 같습니다.
  -- CnC IP : 1.1.1.1
  -- URL : xxx.xxxx.com/xxx.js

  악성코드의 행위는 c:₩work₩xxx.exe를 생성하며, AhnLab V3를 무력화 합니다.
  공격자는 안티바이러스 기능을 disable하여, 원활한 공격 활동을 수행할 수 있습니다.

대응 및 권고사항

EDR 대응	Process Kill [v] 파일 수집 [v] 네트워크 격리 [v]
고객 확인 및 권고사항	* 사전 협의된 대응(프로세스 kill, 파일 삭제 등)수준으로 1차적인 긴급 대응을 수행하였으나, 파악되지 않은 잔존 위협이 존재할 가능성이 있습니다. * 사용중인 백신을 최신버전으로 업데이트 후 악성코드 검사 수행하시기 바랍니다.
안내 사항	* 대응 보고서의 경우 이벤트가 발생한 시스템에 한정됩니다. * 추가적으로 다른 PC로 전파되었을 가능성이 있기 때문에, 동일 시간대의 다른 PC의 탐지 이력을 확인하시기 바랍니다. * 전체 시스템 영향도 분석이 필요하신 경우 연계 서비스를 권고 드립니다. (침해사고 분석, 악성코드 분석, 의심시스템 진단 서비스)

MDR 대응 상세 분석 보고서

안녕하십니까? 종합 정보보호 전문기업 AhnLab 입니다.
귀사에서 발생한 위협 이벤트에 대해 상세 분석한 결과를 전달 드립니다.

탐지 정보

고객사	안랩		
시나리오	Behavior/EDR.Download.M3900		
티켓 번호	R22070510112802663	위협도 등급	Low, Medium, High
발급 시간	2022-07-13 15:25:00 (+09:00)	탐지 시간	2022-10-12 16:10:58 (+09:00)
보안 시스템	EDR Server (211.233.40.134)		

추가 상세 분석 내용

종합 의견	* 악성코드 실행 이력과, 잔존 위협, 내부 네트워크의 이동 이력이 존재함이 확인되었습니다. * 확인되지 않은 추가 위협이 존재할 가능성이 있고, 내부에 잔존 위협이 있을 가능성이 있습니다.

영역	분석 내용	조치 방법
유입 경로	http://malware.test.com/main.js	
잔존 프로세스	C:₩temp₩mal.exe	해당 프로세스를 Kill 조치 필요
잔존 파일	C:₩temp₩scan.exe C:₩temp₩httpro.exe	파일 삭제
잔존 자동 실행	이상 없음	
네트워크 현황	1.1.1.1 공격자 연결세션 유지 중	
내부 이동 현황	192.168.3.x 대역에 대한 스캐닝 이력 확인 192.168.2.1 RDP 세션 연결지속중	

분석 내용	* 기존 탐지된 악성파일 이외에 **C:₩temp₩mal.exe의 파일이 잔존해** 있음이 확인되었습니다. * 해당 파일은 Powershell.exe를 실행하여, 1.1.1.1로 파악되는 **공격자와 reverse Connection 연결에 성공**하였습니다. * 공격자의 세션이 유지되고 있기 때문에, **네트워크적인 선조치가 필요**하며, **시스템을 격리할 것을 권고** 드립니다.
권고사항	* 프로세스 kill, 파일 삭제 등 1차적인 긴급 대응을 수행하였으나, 파악되지 않은 잔존 위협이 존재할 가능성이 있습니다. * 시스템에 대한 재설치를 권고 드리며, 내부 이동 행위가 감지되었기 때문에, 사용중인 백신을 최신버전으로 업데이트 후 악성코드 검사 수행하시기 바랍니다. 추가적인 내부 흔적에 대한 조사는 **[의심 시스템 진단]** 서비스를 이용하실 것을 권고 드립니다.

AhnLab SOAR 소개

AhnLab

AhnLab SOAR 개요

Orchestration

- 다양한 솔루션과의 연동 (보안·비보안)
- Bi-directional integration (Push/Pull)
- 손쉬운 사용성

Automation

- 조직내 업무 프로세스 자동화
- Playbook 제작 지원
- 표준 대응 절차 제공

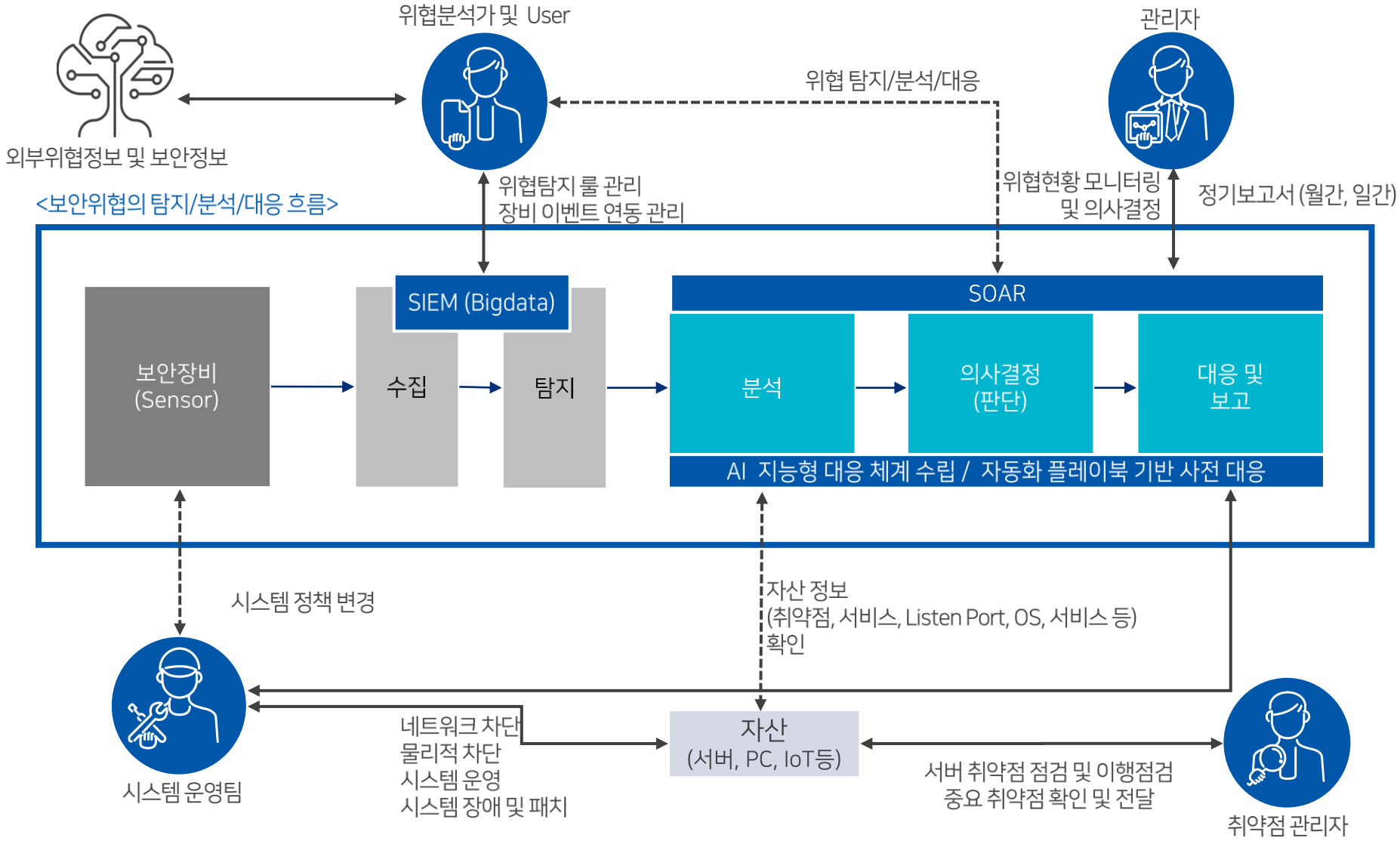
Incident Management and Collaboration

- Case Management
- 대응 전문가와 분석가 사이의 협업
- 대응 내역과 의사결정 기록 및 관리

Dashboards and Reporting

- 대응 활동에 대한 보고 지표
- 의사결정 지원

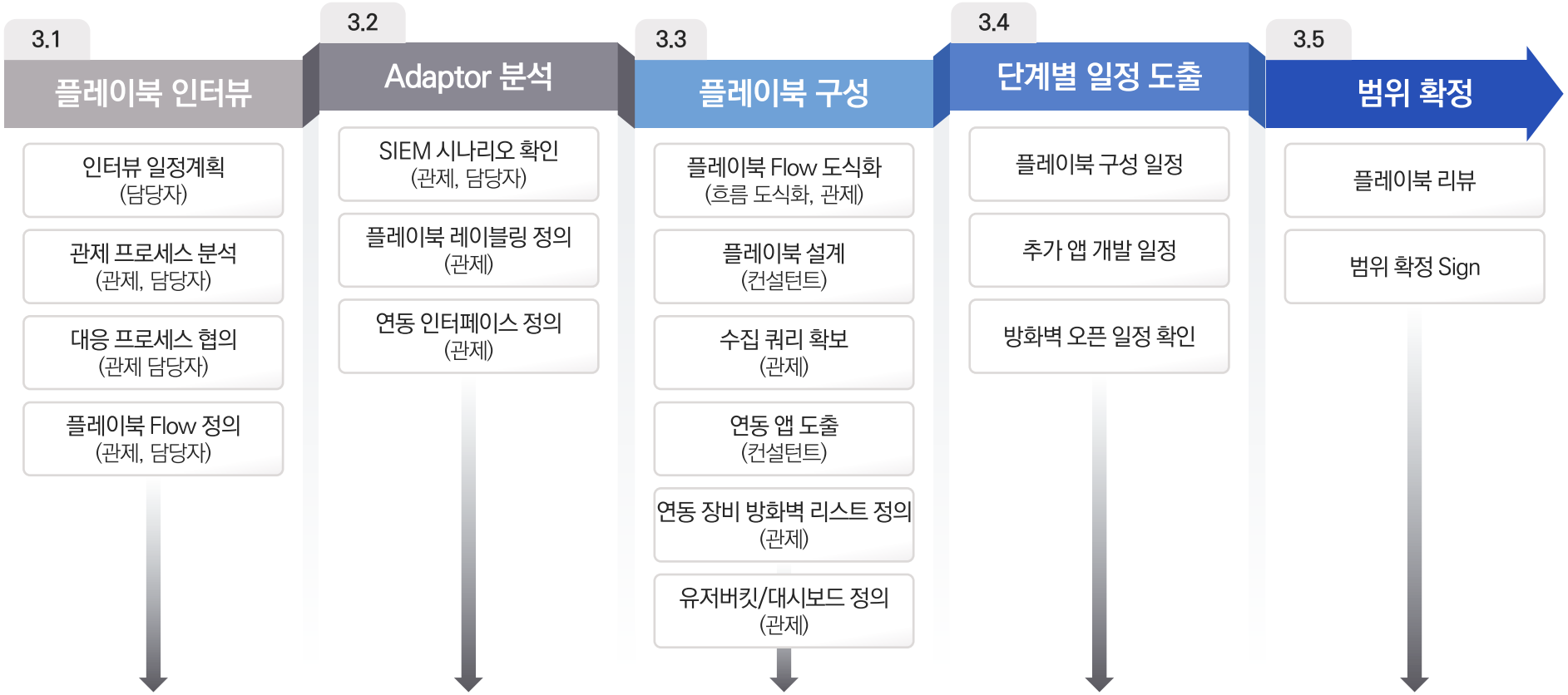
보안관제 업무의 흐름 및 이해 관계자



SOAR 구축에 특화된 방법론

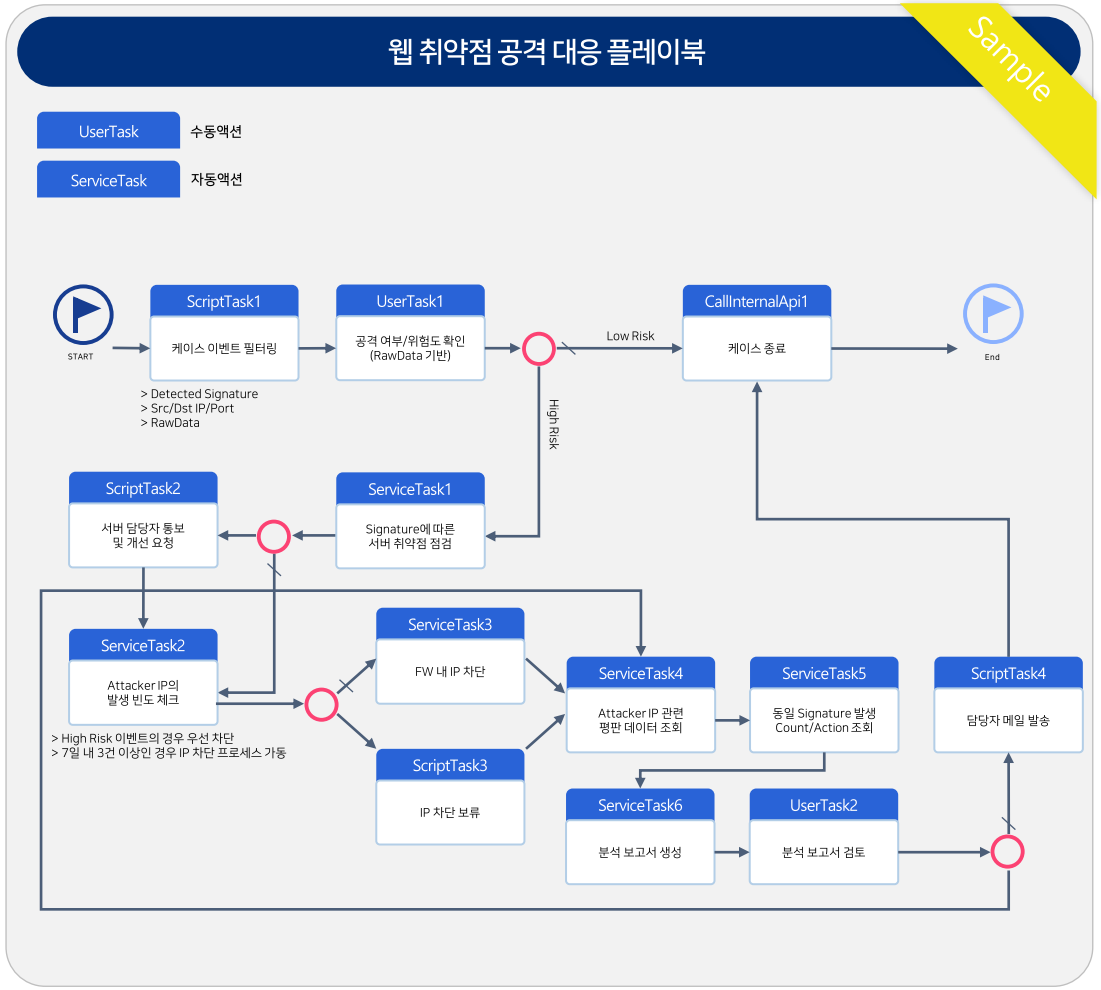
경험 – 전문가 - 조직

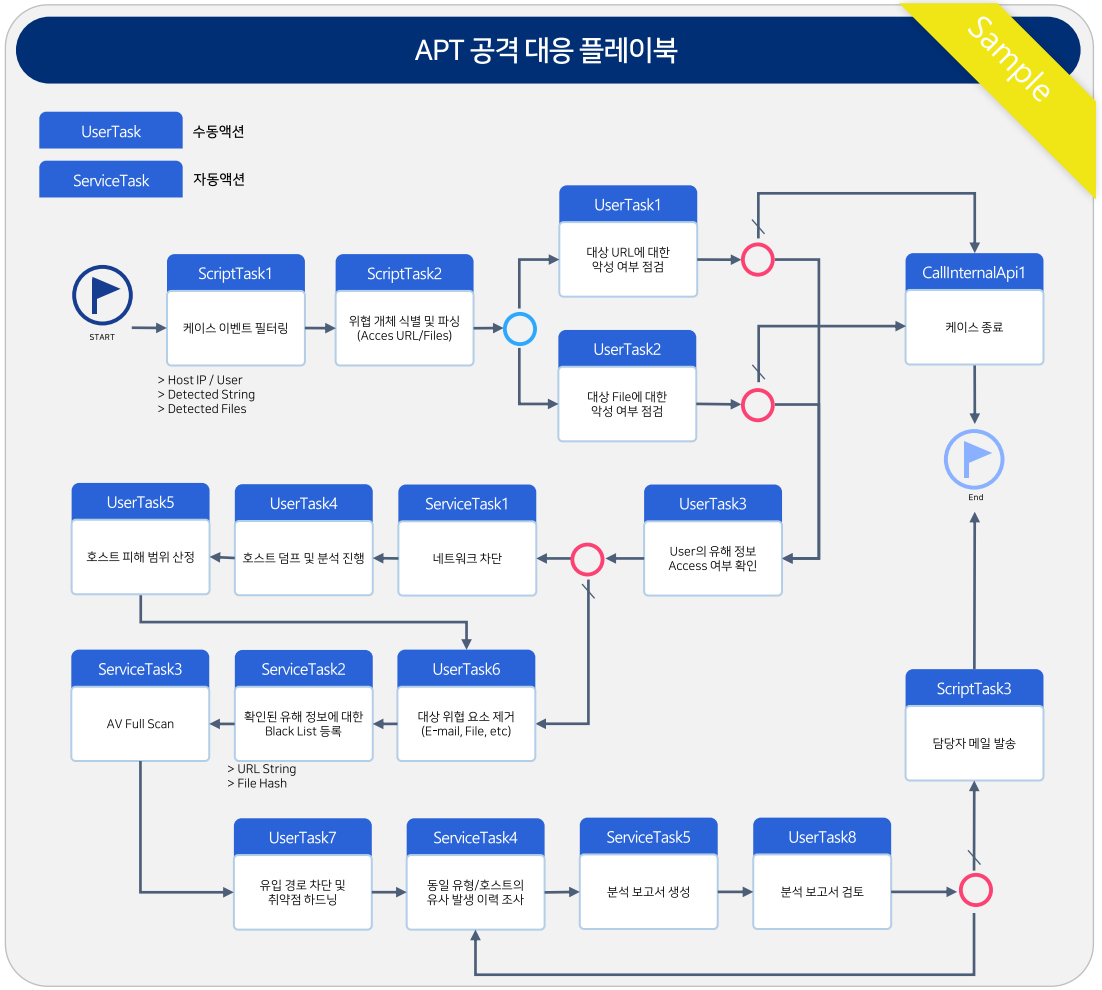
경험에 따라 담당자를 사이트를 리딩 할 수 있어야 한다. 따라서 풍부한 관제 경험과 탄탄한 조직력이 필요하다.



플레이북 대응절차 수립

제작된 플레이북을 통해 자동으로 대응 절차가 진행되며, 담당자는 조치 내역 확인 및 의사 결정을 진행



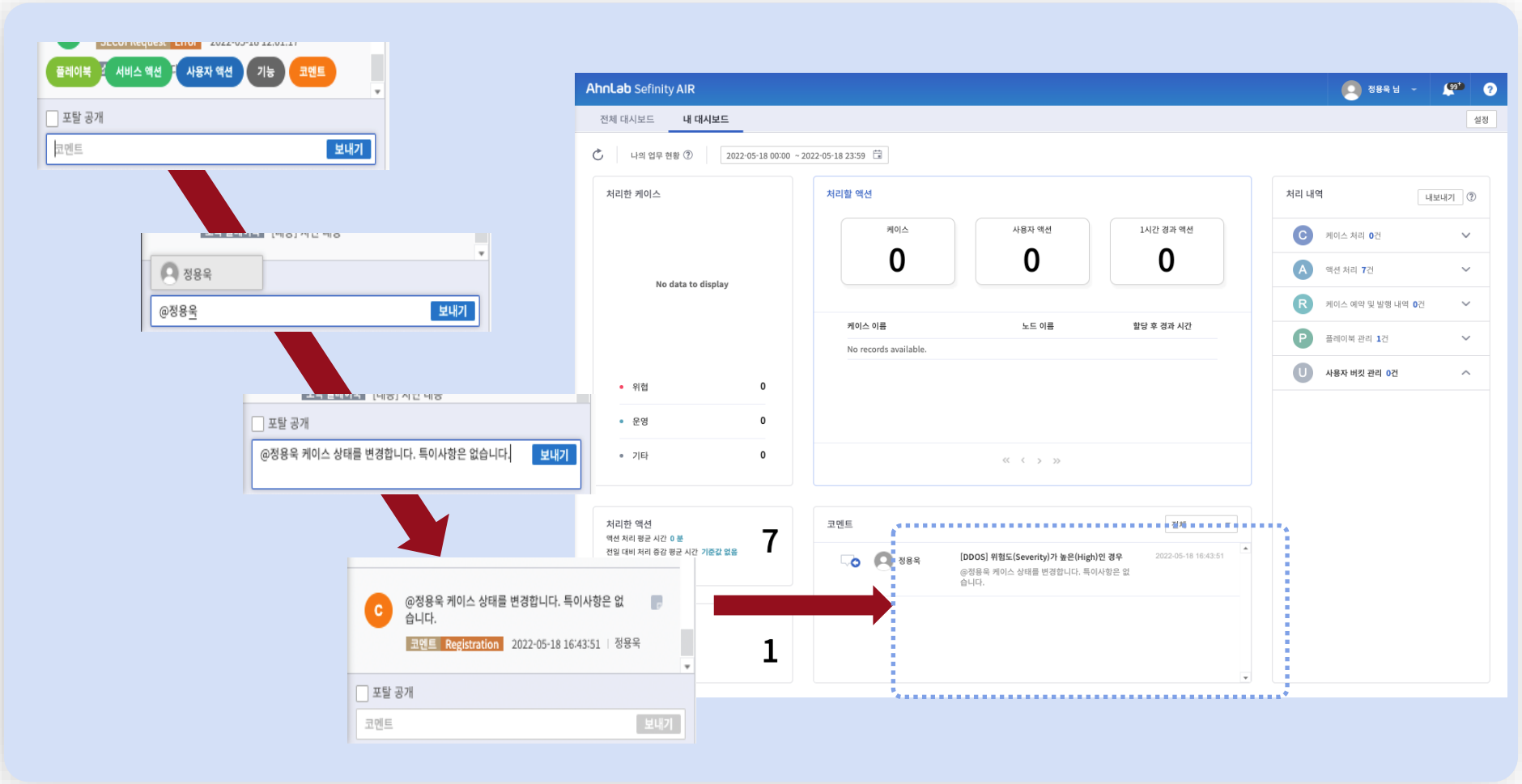


특장점 : SOC 통합 운영 환경 제공

- 사용자정의기반 SOC 종합정보 처리화면 및 사용자 정의기반 구성 가능
- 자동화 처리 결과 / 종합정보 VIEW 제공

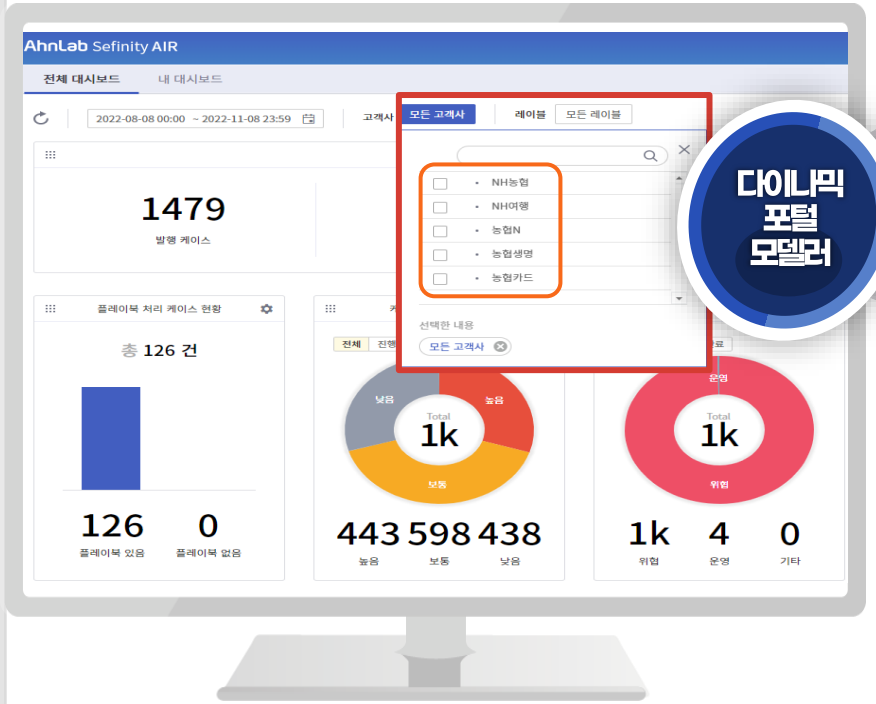
특장점 : 협업 커뮤니케이션

- 티켓별 코멘트 입력 가능하고, @(멘션) 기능을 통해 전달자를 지정할 수 있습니다.
- 자신에게 멘션이 걸린 메시지는 “내 대시보드”의 “코멘트” 위젯에서 메시지를 확인할 수 있습니다.

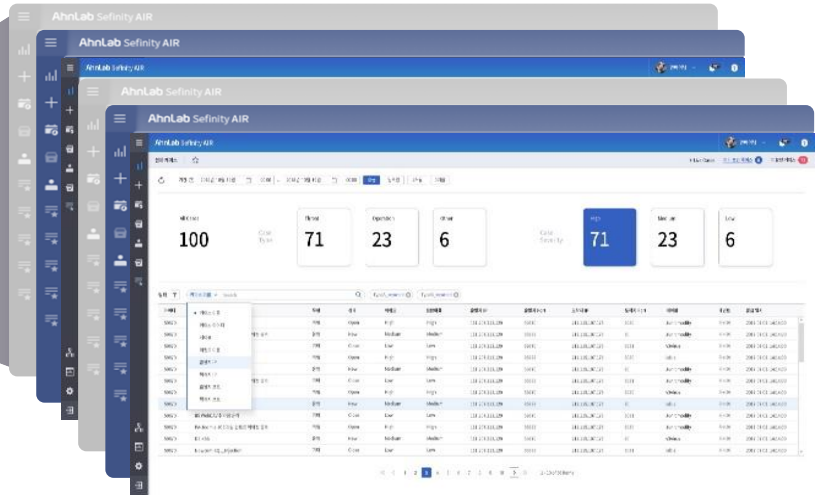


특장점 : 관제포털 플랫폼

SOC 포털 기능 보유



각 그룹사별 포털 사이트



포털 플랫폼 주요 레퍼런스

KB금융그룹 하나금융지주 에스원 HYUNDAI AutoEver

특장점 : AI 위협 분석 플랫폼 (추가 모듈)

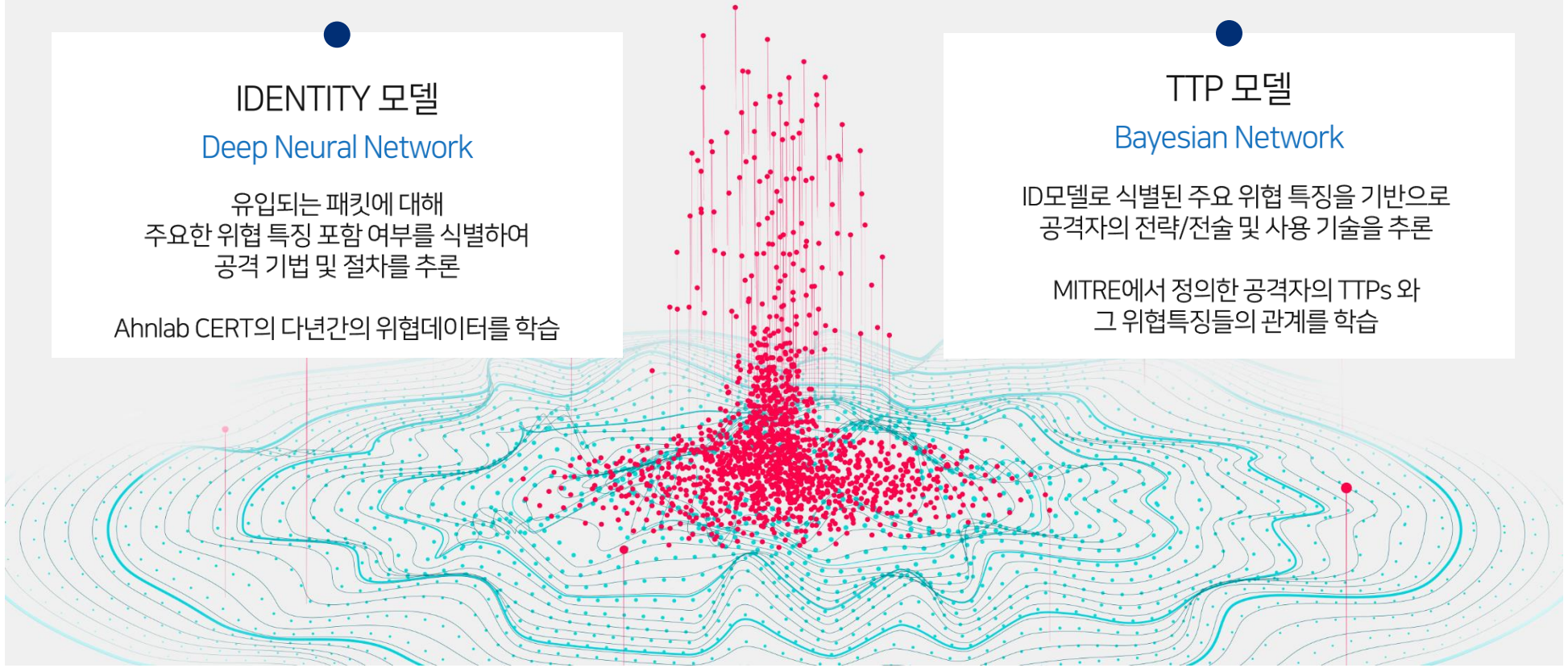
핵심 머신러닝 모델을 사용하여 Payload의 공격 전술 / 기술 / 절차를 추론

IDENTITY 모델

Deep Neural Network

유입되는 패킷에 대해
주요한 위협 특징 포함 여부를 식별하여
공격 기법 및 절차를 추론

Ahnlab CERT의 다년간의 위협데이터를 학습



TTP 모델

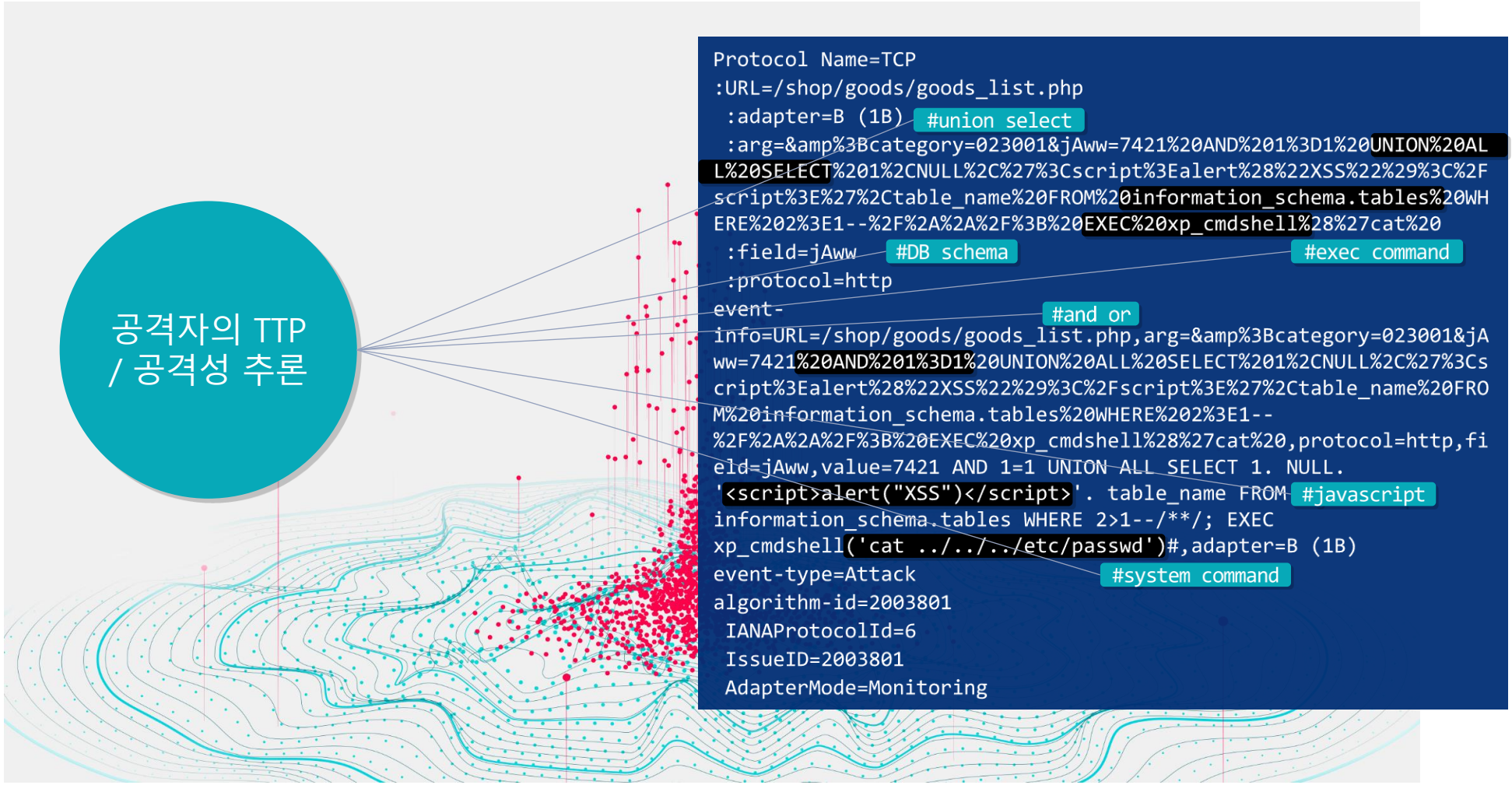
Bayesian Network

ID모델로 식별된 주요 위협 특징을 기반으로
공격자의 전략/전술 및 사용 기술을 추론

MITRE에서 정의한 공격자의 TTPs 와
그 위협특징들의 관계를 학습

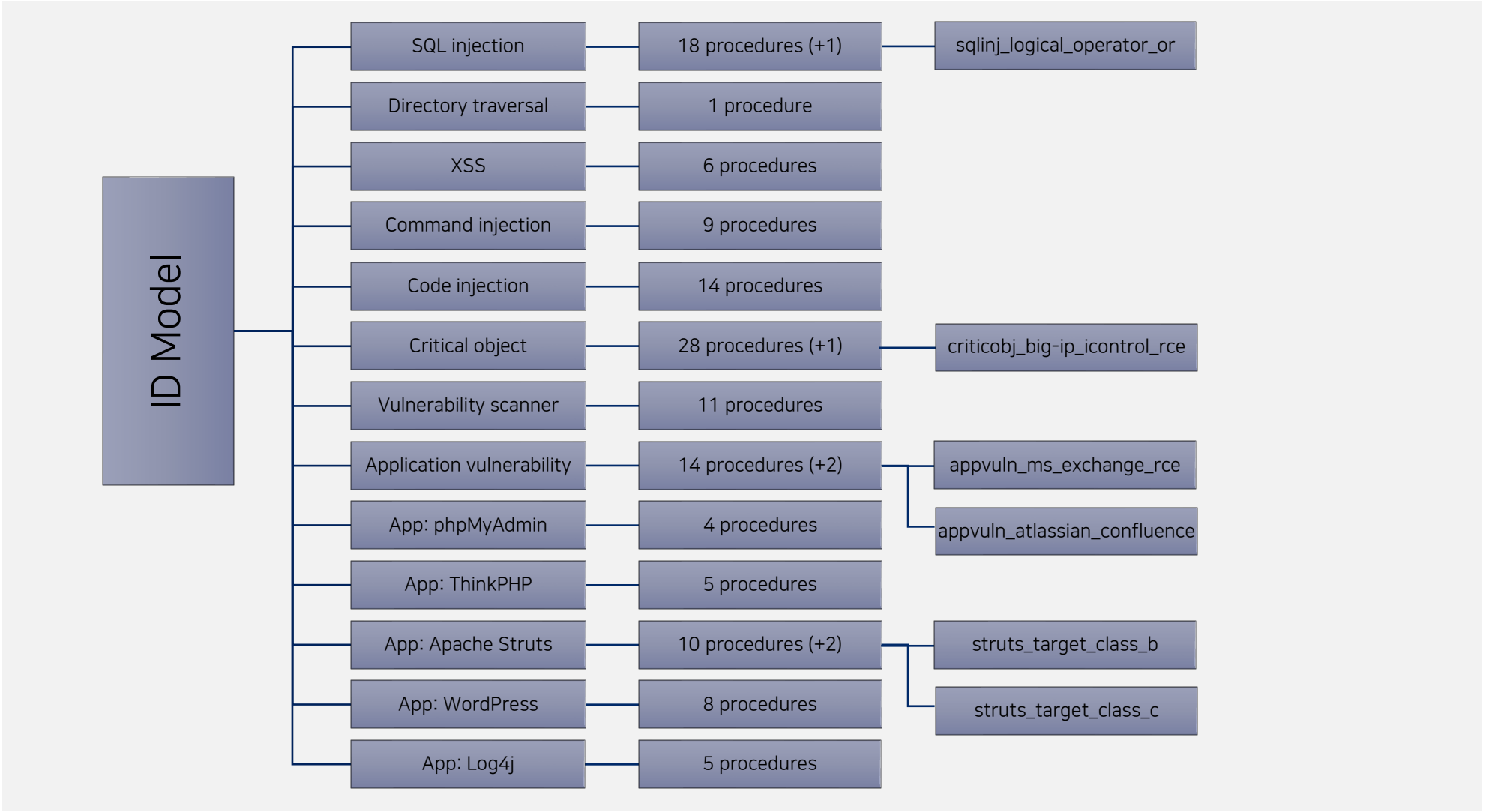
특장점 : AI 위협 분석 플랫폼 개요

AhnLab CERT에서 공격 유형별 대응 이력을 학습하여, 유입된 데이터에 대해 대응 레벨을 추천



AI 위협 분석 플랫폼 IDENTITY Model Details

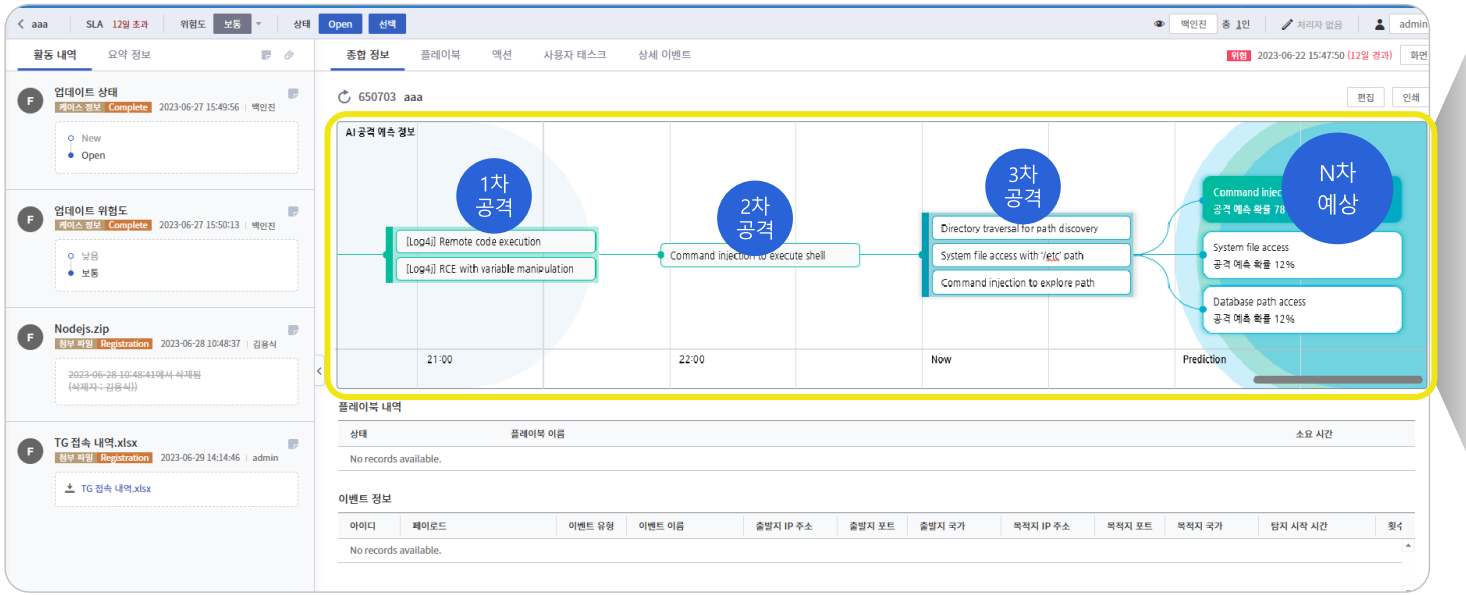
13 Techniques / 133 Procedures



AI 기능과 연동한 인텔리전스 기능 제공

AhnLab 에서 수집한 빅데이터로 만들어진 공격 체인 룰을 활용한 공격 지점 추천

사후 대응, 단편적인 대응(Case by Case)을 넘어, 상관분석을 통한 추가 공격 사전 대응
회귀분석을 통해 과거 공격과 동일/유사한 공격 시나리오에 대한 대응 정보를 제공



CA Ontology Analysis 화면

* 예시-안랩 SOAR 상관분석 UI

AhnLab XDR 소개

AhnLab

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




자산/사용자 가시성 확보	모니터링	분석/평가	확인 및 조치
• 물리적/논리적 자산 • 기업 및 개인보유 자산 • 문서 등 중요 정보 • User가 보유한 자산/사용 시간 • 계정 사용 자산/사용 시간	• 자산 변동/신규 자산 접속 • 계정 변동 사항 • 데이터의 외부 전송, 복사 • 비정상 행위 탐지 • 사용자 이상 행동 (패턴) • 위협 의심 징후	• Risk 시나리오 분석 • Context 분석 • 거버넌스/컴플라이언스 분석 • User/Asset 이상행위 분석 시간 장소 자산 사람	• 우선순위에 따른 Alert • Risk 심각도, 영향도 확인 • 가이드 및 조치 진행 • 자동/수동 조치 • Report 확인

Risk 관점의 분석 및 대응

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

A형간염검사 결과지

성명		주민번호		등록번호	
주소				검진일	2019-07-17

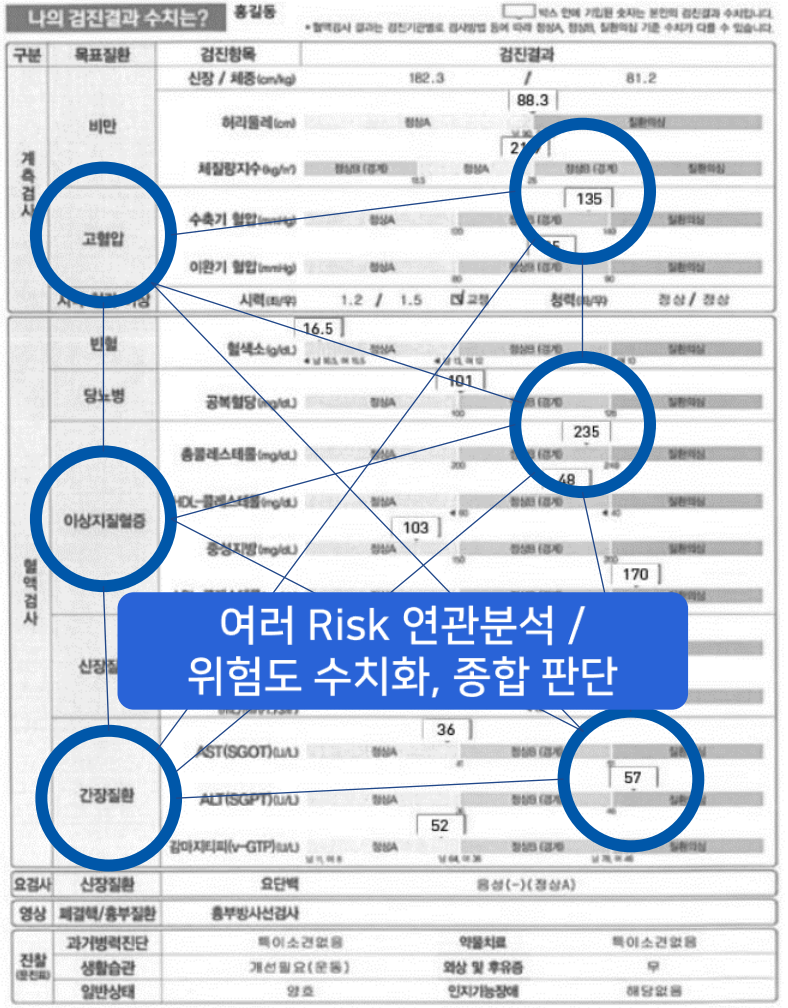
검사구분	검 사 명	결 과	판 정	단 위	참 고 치
면역혈청검사	A형간염항체(IgM)Anti-HAV	음성	정상		음성
	A형간염항체(IgG)Anti-HAV	양성	정상		음성,양성
	B형간염표면항원,일반(HBs Ag)	음성	정상		음성
	B형간염표면항체,일반(HBs Ab)	양성	정상		음성,약양성,양성
판정	정상A				
소 견	B형간염:항체양성 A형간염: 항체, 양성(있음)으로 예방접종 불필요함.				

관점의 변화

제품 관점에서 특정 영역 모니터링 → 정상/악성 여부 판단

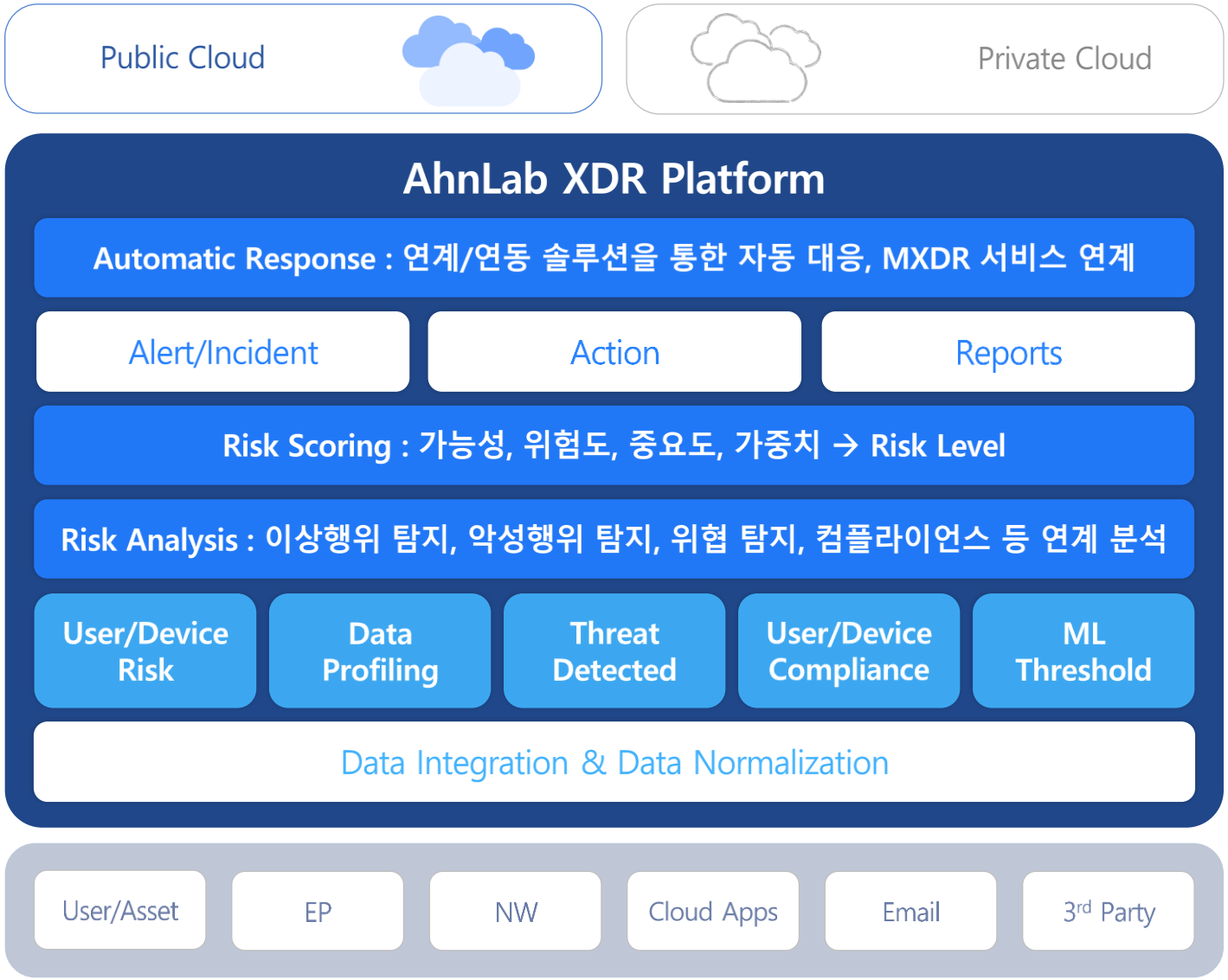
V3 = 독감 / EDR = 코로나(PCR, 역학조사)
XDR = 종합건강검진

종합적인 결과 기반 – 건강의 Risk 관리



* source : https://brunch.co.kr/@iish201403ekrr/4

AhnLab XDR



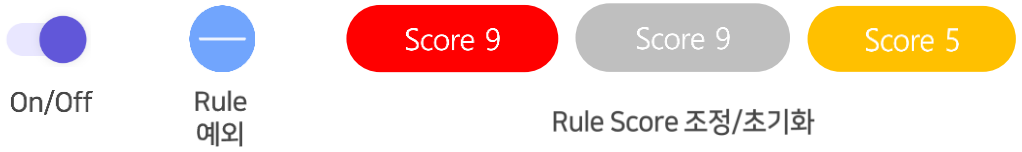
- 이기종 Data 수집, 정규화, 분석, 모니터링, 연계 대응
- ML 임계치, 내부 영향도 확인, Risk Scenario, Risk Scoring

특장점 – 시나리오 룰 실시간 업데이트

AhnLab XDR은 기존 발생했던 리스크와 최근 유행하는 리스크 시나리오를 사전 정의하여 시나리오 룰(Scenario Rule)에 실시간 반영합니다.
기업 환경에 따라 리스크 기준이 다르므로, 룰(Rule) 사용 여부를 On/Off 하거나 스코어 조정, 초기화 등을 노이즈를 최소화할 수 있습니다.

Risk Scenario

Rule Setting



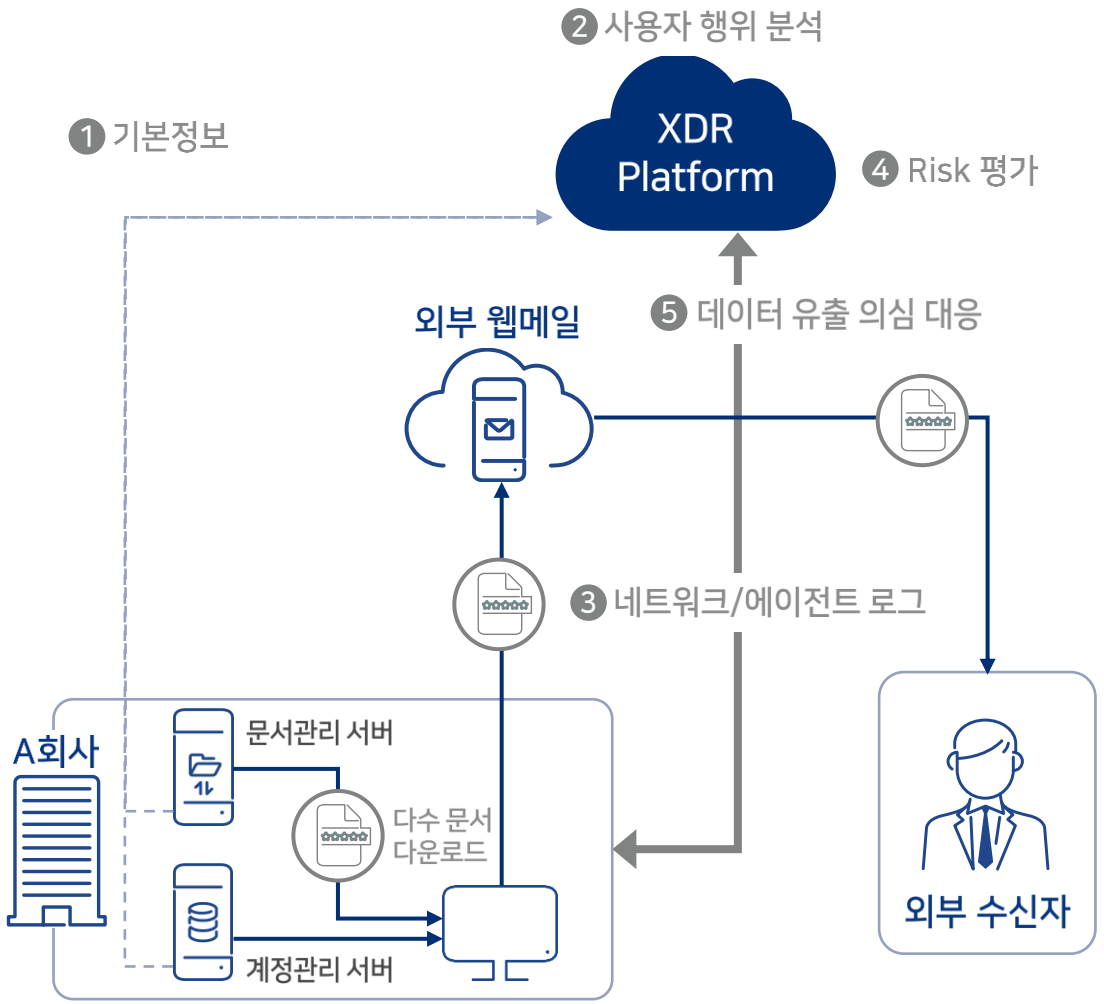
연계 규칙 / ML 엔진

- 일정 시간 내에 국가 변경 로그인 시도 탐지
- 피싱 메일 수신 탐지 및 허용되지 않은 국가 로그인 성공 탐지
- 문서 스캔 후 외부 메일을 이용한 파일 전송
- RDP를 이용한 익명 로그인 시도 탐지 / 이중 로그인 시도 탐지
- 본인의 메일 주소로 메일 발송 탐지
- 동일한 제목의 메일 대량 수신 탐지
- 임계치 이상의 SMB/NetBIOS 프로토콜 통신 시도 탐지

특장점 – 국내 실 환경에서 발생할 수 있는 Risk Scenario

안랩의 관제서비스 및 포렌식 등을 통해 오랜 시간 쌓여진 노하우 → 국내에서 발생했던 Risk + 최근 유행하는 Risk Scenario 사전 정의

시나리오 예시 : 내부자에 의한 중요자료 외부 유출



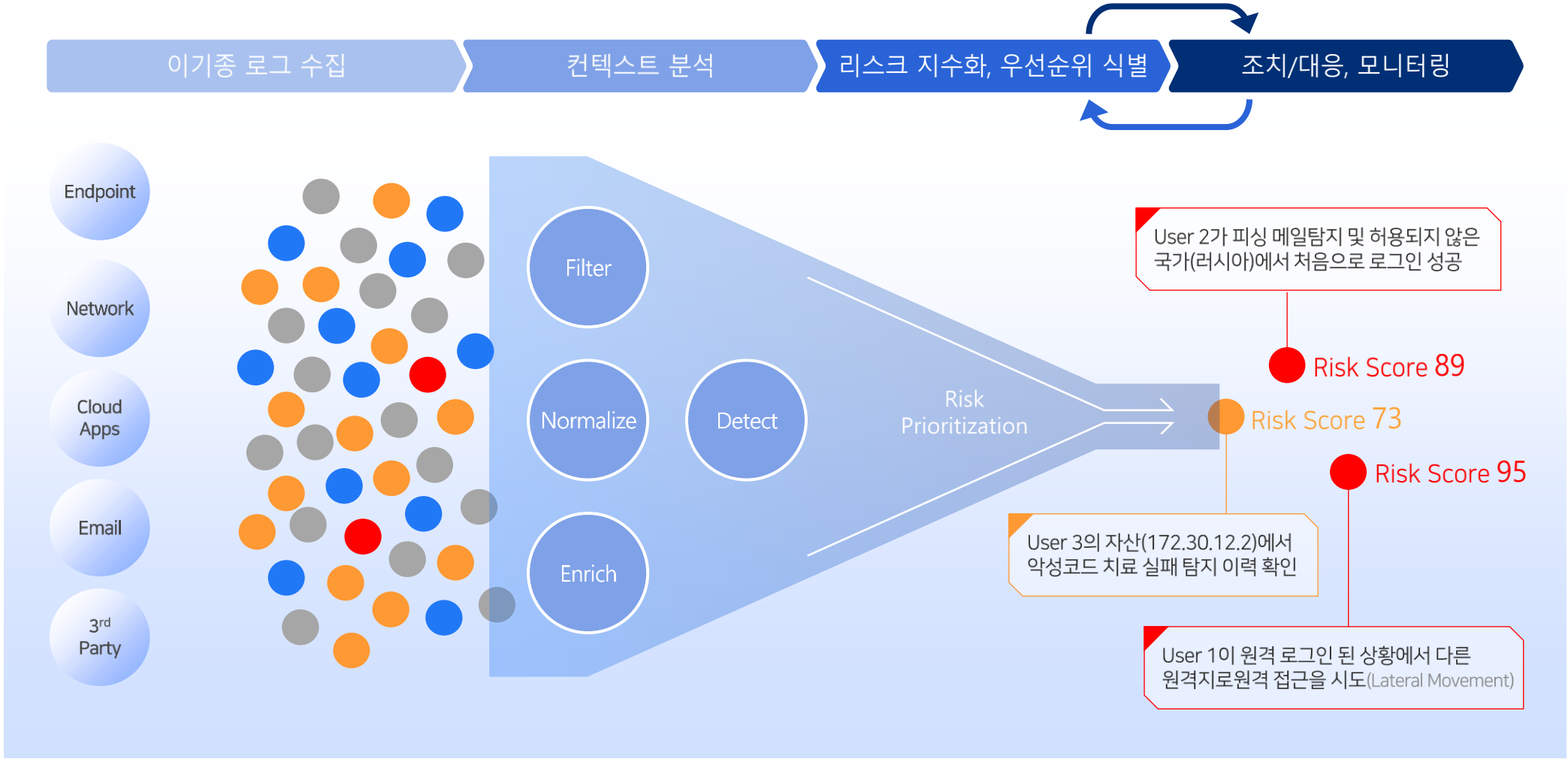
최근 1달 내 해당 User의 행동 패턴 = 임계치

- ✓ 9시 출근, 6시 퇴근
- ✓ 1시간 내 10개 미만의 파일 다운로드
- ✓ 작업 파일을 사내 서버로 업로드함. 1달 이내 300MB 미만
- ✓ 외부 메일 사용하지 않음
- ✓ 외부 메일 첨부 용량이 1달 이내 10MB 미만

수집정보	행동	타임라인
계정	내 계정으로 정상 로그인	AM 9:00
시간/위치	저녁 9시 근무중, 회사	
접속시스템	내부 문서관리 시스템 (예: Docs) 접속	PM 9:00
다운로드 이력	다수 프로젝트 파일 다운로드(200 files)	PM 9:01 – 9:30
파일 압축 이력	다수 프로젝트 파일을 압축	PM 9:31
외부시스템접속	외부 웹 메일 접속	PM 9:35
대용량 첨부 이력	메일에 대용량 파일 첨부	PM 9:36
None	AhnLab XDR 데이터 유출 의심 탐지/차단	PM 9:37
None	보안팀 출근, XDR 대시보드 확인	다음날 AM 10:00

특장점 – 리스크 우선순위 제공

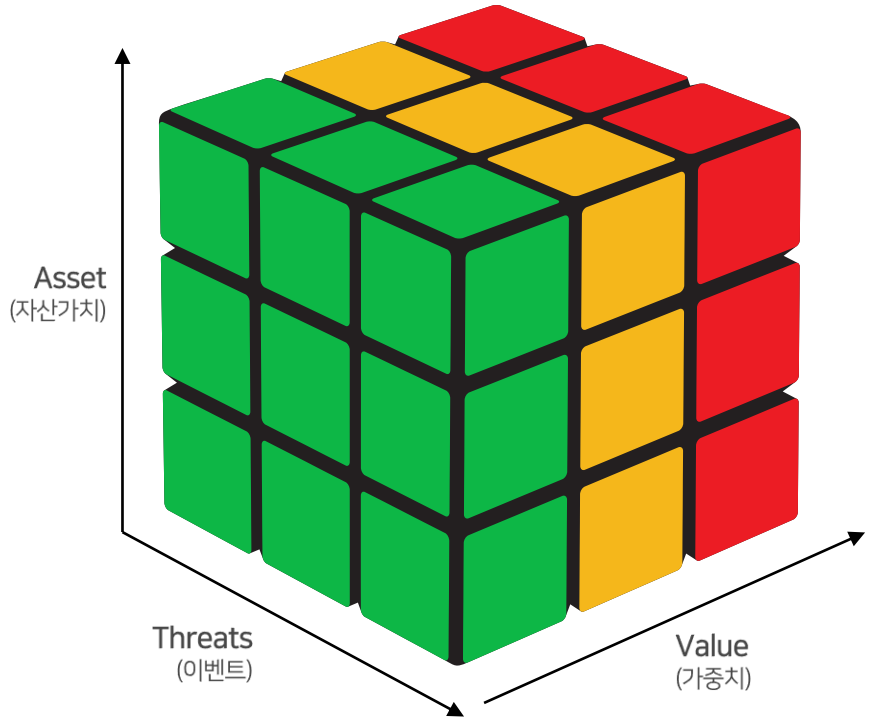
AhnLab XDR은 다양한 영역의 이기종 보안 로그를 연계 분석하여 위험도가 높은 리스크를 선별합니다.
최종 확인된 리스크에 대해 보안 담당자에게 조치 우선순위를 제공하여, 실제 위협으로 발전할 가능성이 있는 리스크를 대응 및 관리할 수 있도록 합니다.



특장점 – 리스크 지수화(Risk Score)

AhnLab XDR은 독자적인 지수(Score) 산출 방식에 기반하여 리스크 우선순위를 제공합니다.
리스크(위험)는 가능성(Likelihood, 확률)을 의미하며, 위협이 자산의 취약점을 이용하여 부정적 영향을 미칠 가능성을 뜻합니다.
지수는 이해하기 쉽도록 최대 100점까지 표기하여 사용자들이 리스크를 직관적으로 파악할 수 있도록 합니다.

Risk Score (부피) = Likelihood * Impact



Square | Sum | Root

Risk Level (LV)	Risk Score Range
Low	• Risk Score : 1 ~ 13 • User/Device : 1 ~ 100 • Dashboard : 1 ~ 100
Medium	
High	
Critical	

분류	Medium	High	Likelihood
Rule Score	4	8	x2 → x10

분류	Likelihood	Impact	Risk Score
Risk 1	25	2등급	6 (Medium)
Risk 2	25	5등급	7 (High)

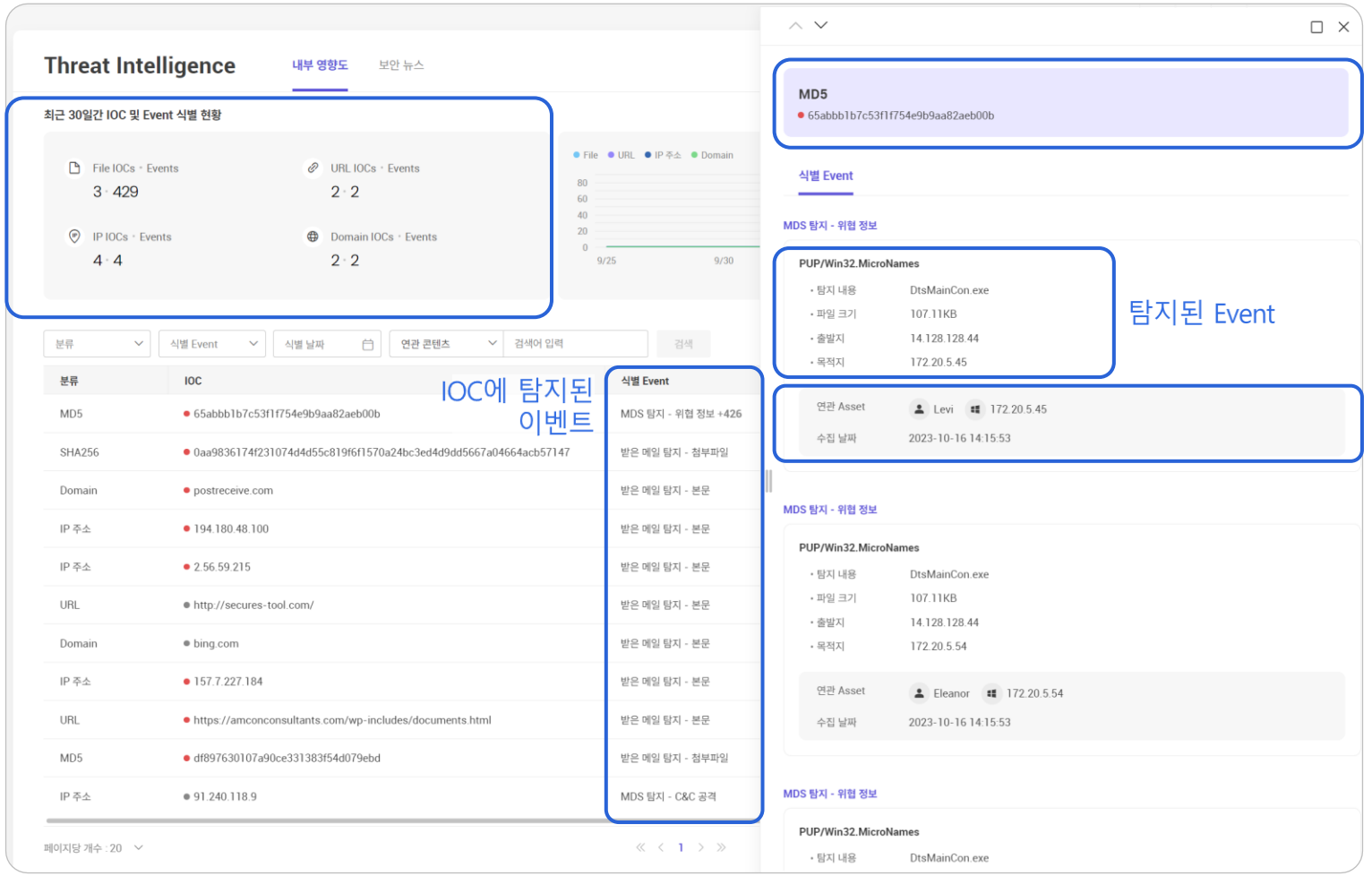
특장점 – No Agent & Data Hub

AhnLab XDR은 별도 에이전트(Agent) 설치 없이 기존 운영 중인 EPP/EDR 에이전트와 연계하여 데이터를 수집해 대응할 수 있습니다.
또한, 기업 내 자산의 보안성과 효율성을 고려해 'AhnLab XDR Data Hub'를 활용하여 수집된 로그를 필터링하고 XDR 플랫폼으로 전송합니다.

특장점 – 위협 인텔리전스 연동: 내부 영향도 파악

AhnLab TIP(Threat Intelligence Platform)와 연동하여 최근 30일 동안 확인된 IOC 정보를 기반으로 내부 자산 영향도를 확인

IOC별 탐지된 이벤트 건 수 현황 정보



국방 정보보호체계 구축 현황

AhnLab

국방 정보보호체계 구축 현황 - 1

1. 각 군 현황

각군	인터넷망	내부망	전장망	비고
육군	A	A(70%), S(30%)	A(5%), S(5%) F(20%), X(70%)	ATCIS
해군	A(60%), S(40%)	A(70%), S(30%)	A	KNCCS
공군	A	A	A	AFCCS
해병	S	S	A	KNCCS

2. 국직 현황

국직	구분	비고
국방부	지능형플랫폼 정보보호체계	NIA 시범사업
국방통합데이터센터	SDDC기반 차세대 국방 클라우드 데이터센터 정보보호체계	인터넷망, 내부망
국군사이버작전사령부	전군바이러스백신체계	20년 ~ 현재
국방전산정보원	인터넷망, 서버팜, 내부망 정보보호체계	
국군방첩사령부	인터넷망, 전용망, 업무망 정보보호체계	부처별 상이
국군지휘통신사령부	국방광대역통합망(M-BcN) 임대회선 침입방지체계	
국통사	인터넷망, 전용망, 업무망	

참고자료 – 한국군 합동지취통제체계

국방 정보보호체계 구축 현황 - 2

1. NCW – C4I 체계 현황

NCW (Network Centric Warfare) – C4I	비고
KJCCS (합동지휘통제체계) – 침입차단 및 방지체계	
AKJCCS (연합지휘통제체계) - 침입차단 및 방지체계	
TICN (전술정보통신체계) – 쉘터별 침입차단체계	
MIMS (군사정보통합관리체계) – 정보보호체계	
차기 군위성 고정 다대역 – 침입차단체계	
다출처영상융합체계(기본형)체계 – 정보보호체계	
KTMO-CELL (탄도탄작전통제소 성능개량 체계개발) – 정보보호체계	
JTDLS (합동전술데이터링크체계) – 정보보호체계	
LINK-22 (연합해상전술데이터링크) –침입차단체계	구축중
MIMS-C (연합군사정보처리체계) – 정보보호체계	
MCRC (중앙 방공 통제소) – 정보호호체계	구축중
MOSCOS (해상작전위성통신체계-II) – 침입차단체계	

국방 정보보호체계 구축 현황 - 3

1. 신기술 구축 현황

구분	대상	사업명	구축범위
AI	국방통합데이터센터	SDDC기반 차세대 국방 클라우드 데이터센터 구축사업	이상징후탐지체계
양자암호화	육군 (9사단)	스마트부대 구축사업	정찰 감시 드론 <-> 통제 센터
	해군 (2함대)	5G(특화망) 융합서비스 공공부문 선도 적용	비행대대 <-> 통제 센터
	공군 (20비)	공군 작전지원차량 양자암호체계 구축	작전차량 <-> 통제 센터
관제자동화 (SOAR)	육군본부	사이버작전 상황공유체계 구축사업	인터넷망, 내부망, 전장망, 교육망
사이버위협 정보 수집 (TIP)	육군본부	사이버작전 상황공유체계 구축사업	인터넷망

* 육군본부 '사이버작전 상황공유체계사업'은 사이버 전장관리체계 탐색개발과 유사 사업 형태

2. 보안 컨설팅 (취약점 진단) 현황

체계	대상	비고
22년 방산업체 사이버보안 취약점 진단사업	86개사 (방산업체 85개사 + 非방산업체 1개사)	방위사업청 발주
23년 방산업체 사이버보안 취약점 진단사업	65개사 (방산업체 37개사 + 非방산업체 28개사)	방위사업청 발주

* 24년 사이버보안 취약점 진단사업 공고中 – 당사 참여 준비중

More security, More freedom

Q&A

AhnLab