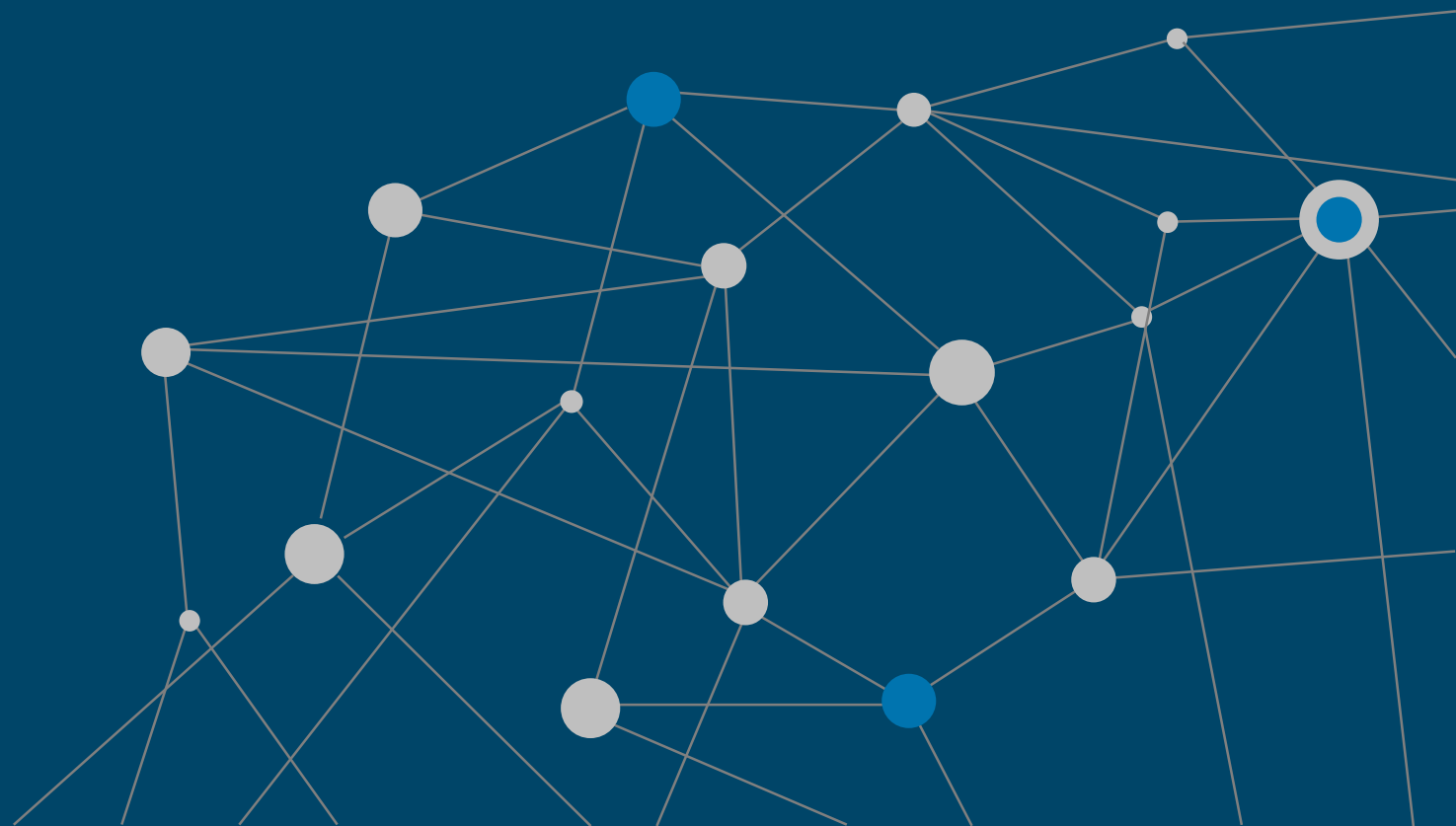
보안 강화를 위한 가시성 확보 및 자동화 대응 구현

발표자 : 김종윤 부장



비즈니스 환경의 변화

4차 산업혁명(4th Industrial Revolution), 디지털 대전환(Digital Transformation)

AI

양자 컴퓨터

로봇공학 및 자동화

Big Data

블록체인

6G 통신 기술

비즈니스 환경의 변화

AI 기술 경쟁의 가속화, 업무 방식의 변화

첨단 AI 데이터센터

텍사스 애빌린

[스타게이트 프로젝트]

미국 전역 5~10개의 데이터센터 건설

광주광역시

[지역사업 모델]

광주광역시 국가 인공지능 집적단지
29년까지 조성

- 경제적 측면 – 고용창출, 지역 경제 활성화, 부동산 가치 상승
- 기술 생태계 발전 – AI 기반 서비스 확산, 연구개발(R&D)
- 지역 브랜드 가치 상승
- 인프라 및 에너지 투자 확대

업무 방식의 변화

AI가 말하는 앞으로 5년 뒤… 업무방식의 변화

1. 원격 근무와 하이브리드 모델의 확대
2. 인공지능(AI)과 자동화의 활용 증가
3. 디지털 기술의 심화
4. 직원의 건강과 웰빙 강조
5. 글로벌화와 다양성 확대
6. 데이터 기반 의사결정의 일상화

[메타 – '오라이언']

네트워크 환경의 변화

SDN(Software-Defined Networking)

[출처 – 한국과학기술정보연구원]

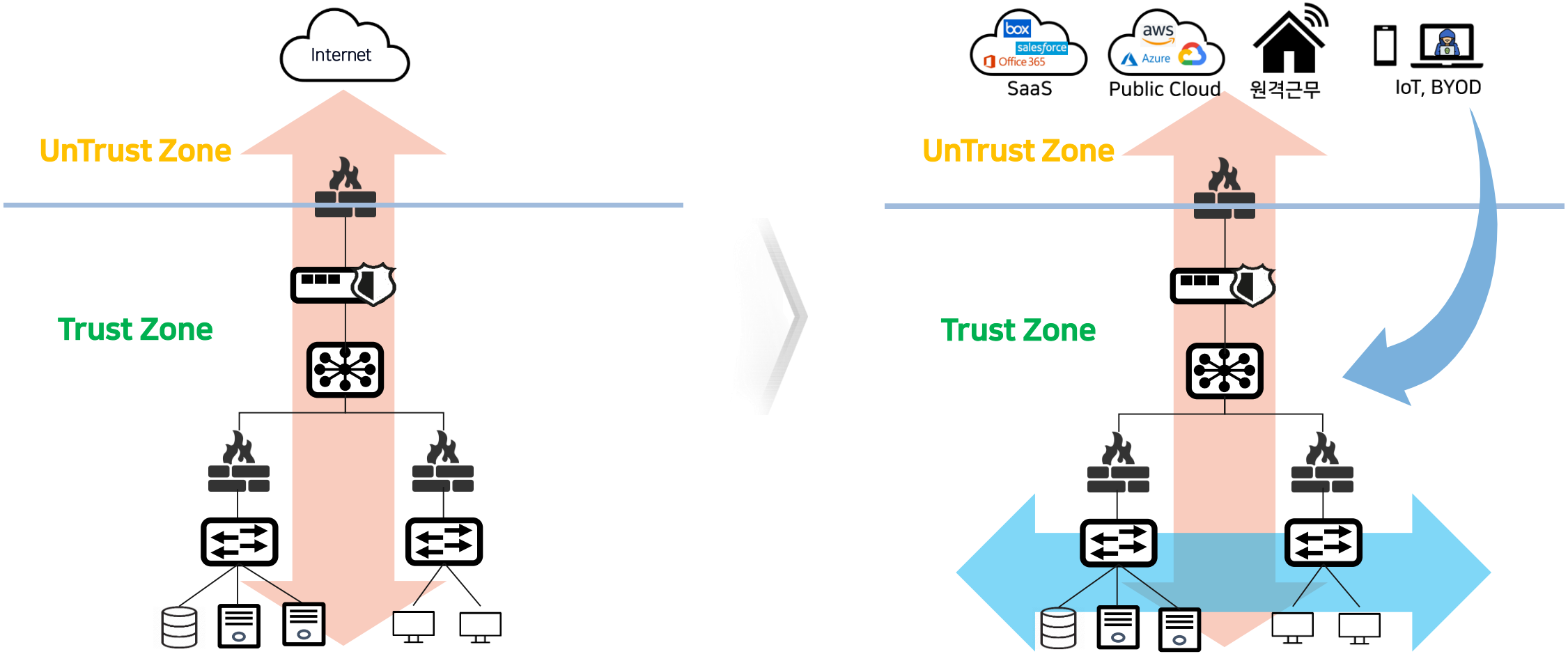
- 중앙 집중화된 제어
- 유연한 네트워크 구성
- 자동화 및 프로그래밍
- 애플리케이션 중심

데이터 전송(Data Plane) / 네트워크 제어(Control Plane)

항목	Legacy	SDN
구조	데이터+컨트롤 통합	데이터, 컨트롤 분리
관리	개별 장비 관리	중앙 소프트웨어 관리
유연성	낮음(하드웨어 의존)	높음(소프트웨어 기반)
비용	높음(전용 장비)	낮음(범용 장비)
보안	분산관리, 일관성 부족	중앙화 보안, 일관성 유지

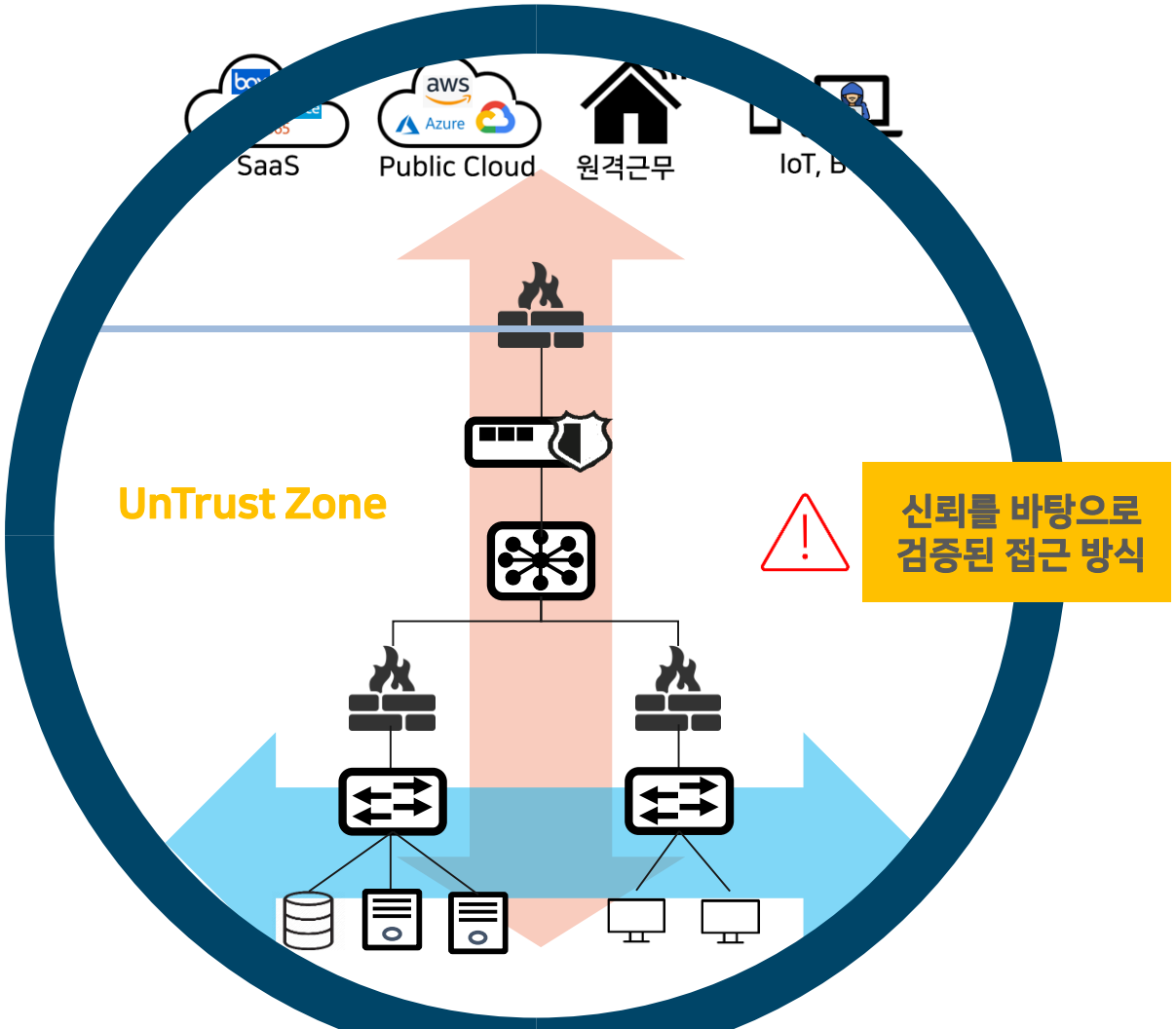
네트워크 보안 모델의 변화

경계보안 모델에서 제로트러스트 보안 모델로의 변화

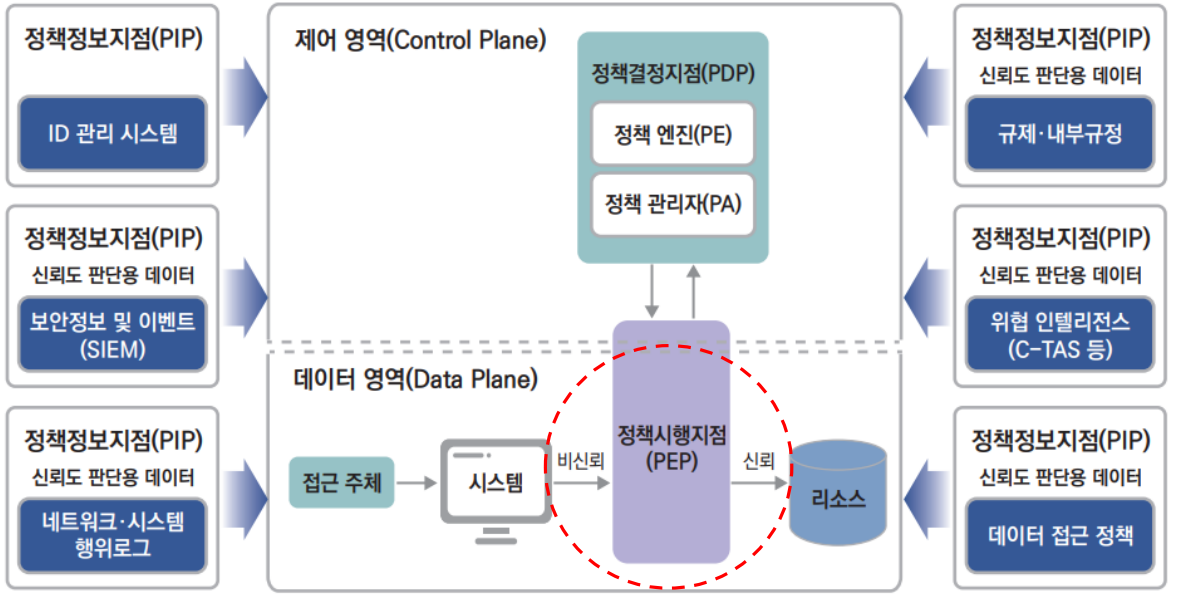


네트워크 보안 모델의 변화

경계보안 모델에서 제로트러스트 보안 모델로의 변화



[제로트러스트 아키텍처 보안 모델 및 논리 구성 요소]

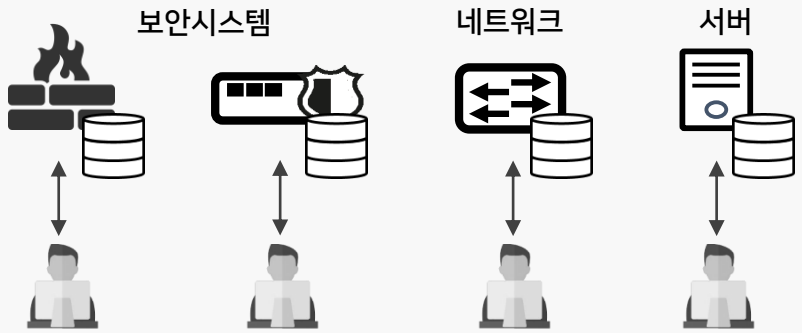


[출처 - 제로트러스트 가이드라인2.0]

보안 운영 기술의 변화

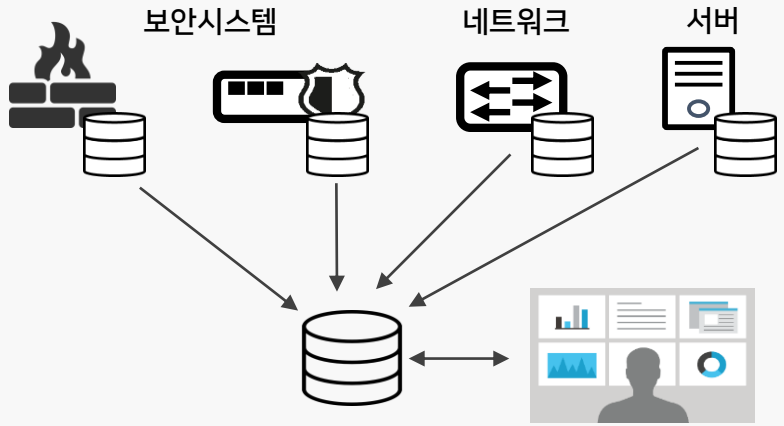
사일로화 된 운영에서 통합운영으로 변화

사일로(Silo)화 된 보안운영



- 독립적인 방식의 데이터 관리
- 팀 간 협업의 문제
- 팀 별 별도의 도구와 프로세스 사용으로 자원 낭비
- 독립적인 위협 탐지로 상호 연관성 분석이 힘듦

통합 보안운영



- 중앙화된 데이터 관리
- 팀 간의 경계가 허물어지고 하나의 목표 아래 협업
- 중복된 부분의 자원 낭비를 줄여 효율성 강화
- 모든 데이터의 상호 연관성을 분석

보안 운영 기술의 변화

대표적인 통합운영 제품 군

SIEM (Security Information and Event Management)

- IT 네트워크 전반에서 생성되는 로그와 이벤트를 중앙 집중화

로그관리 | 상관관계 분석 | 실시간 모니터링 | 규제 준수 지원 | 위협 탐지

- ☑ 오탐(False Positive)
- ☑ 평균탐지시간(Mean Time To Detect)
- ☑ 평균대응시간(Mean Time To Response)

SOAR (Security Orchestration, Automation Response)

- 다양한 보안 도구와 프로세스를 통합, 자동화하여 보안 사고에 신속히 대응

자동화된 워크플로우 | 사고 대응

- ☑ 복잡한 워크플로우
- ☑ 통합 및 플레이북 구현/유지보수의 어려움
- ☑ 능숙한 보안운영팀(전문인력)의 능력 필요

XDR (Extended Detection and Response)

- SIEM, SOAR의 기능 요소를 수용하고, 확장된 탐지 및 대응

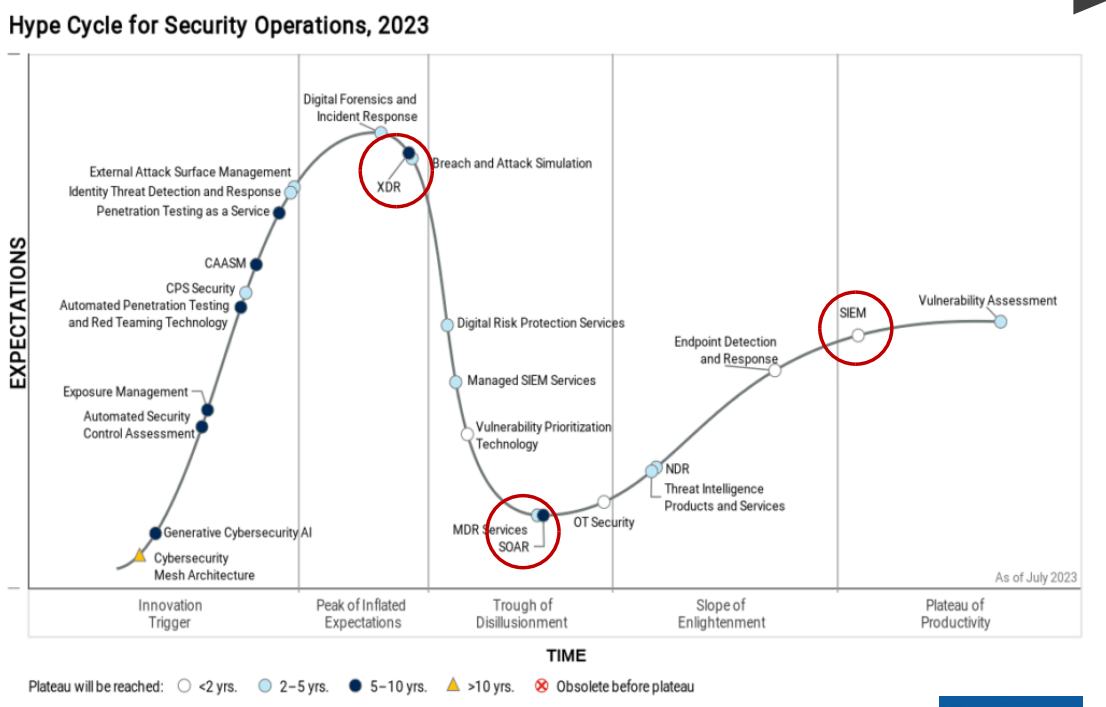
다양한 데이터 통합 | AI/ML | 통합 분석, 자동 대응

- ☑ 평균탐지시간, 평균대응시간 개선
- ☑ AI/ML의 컨텍스트 자동 분석
- ☑ 간결한 자동대응 구현

보안 운영 기술 동향

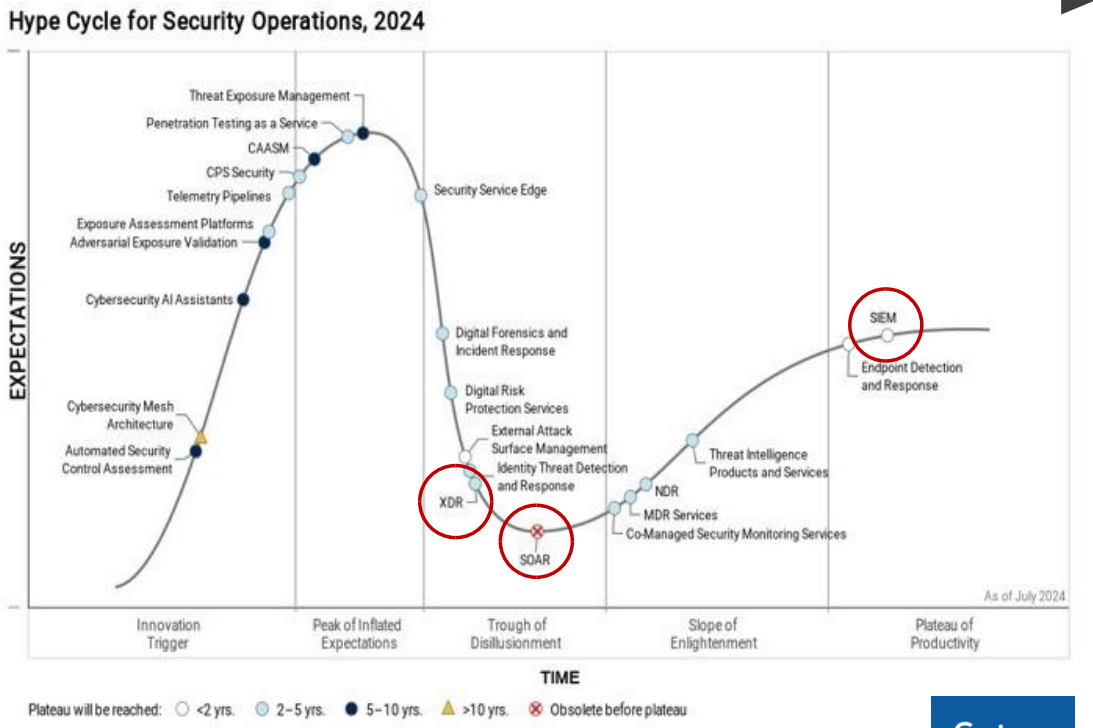
가트너의 “보안운영 Hype Cycle”

2023년 Security Operations



Gartner

2024년 Security Operations

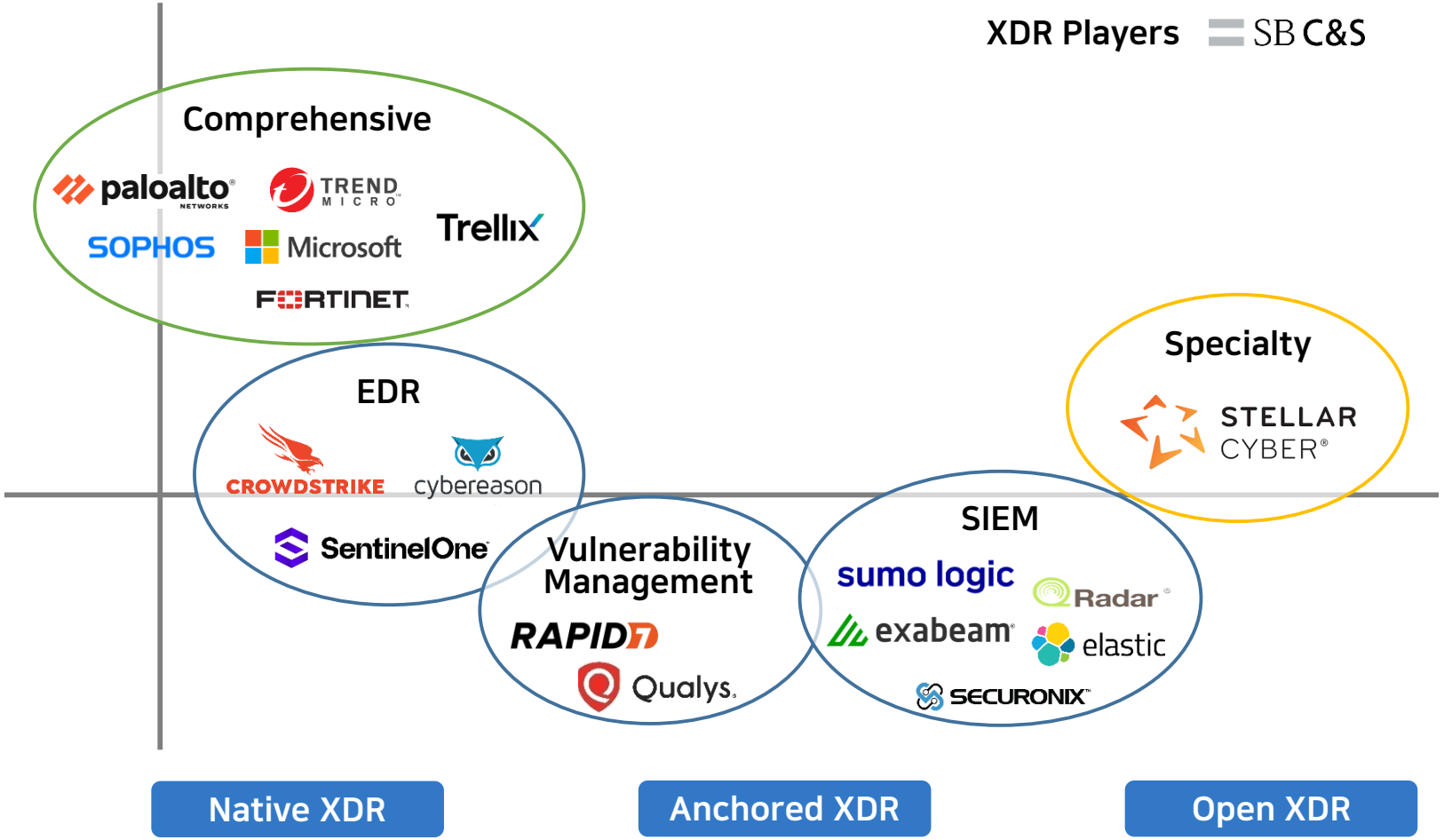


Gartner

Hype Cycle – 새로운 기술이 어떻게 발전하고 수용되는지 시간에 따른 변화를 제공하여 조직의 기술 도입 전략을 돕는 데이터를 제공

XDR(Extended Detection and Response) 분류

XDR 보안벤더의 제품 형태 분류



Native or Closed XDR

- 단일 공급업체(벤더)의 보안장비 통합 연계
- 타 제품과의 연동 및 분석에 제약 발생
- 모든 구성 요소에 대한 재구매 발생 가능

Anchored XDR

- 개방형과 폐쇄형의 중간 형태
- 원격 분석을 위해 3rd-Party와의 통합에 의존, EDR에 의존도를 보임

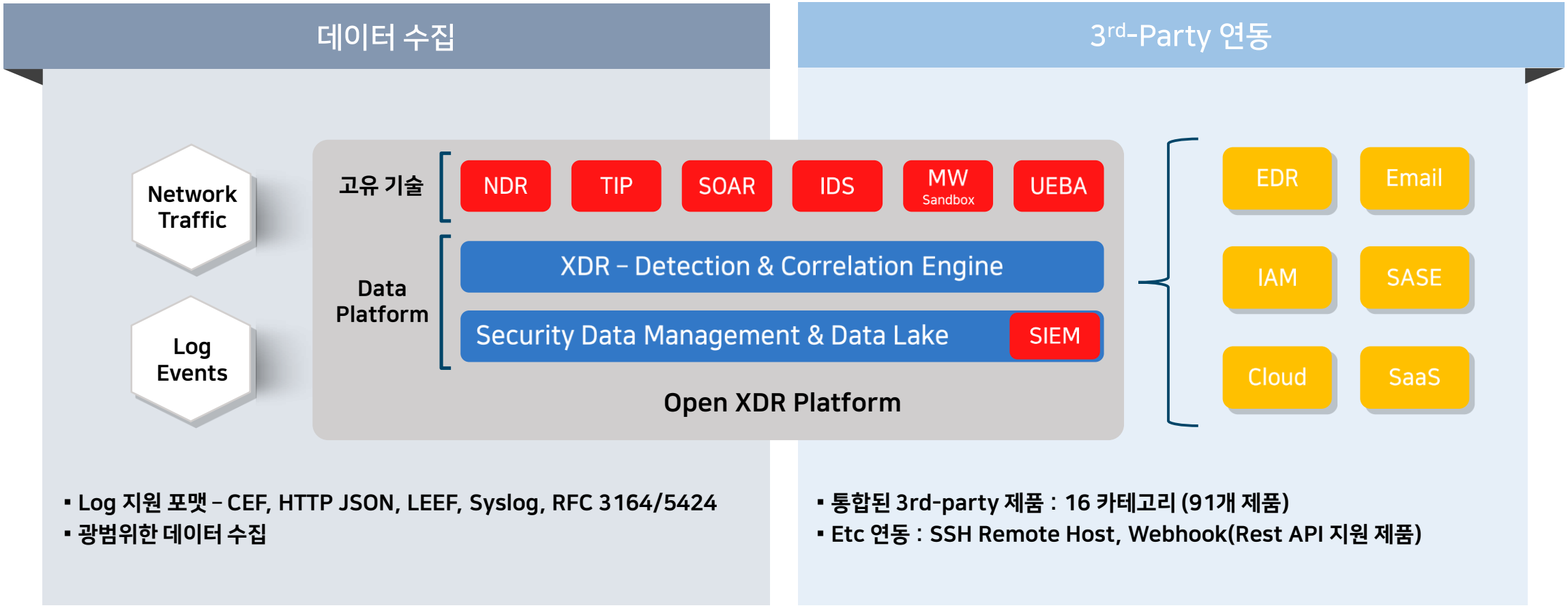
Open XDR

- 최소화된 파트너(벤더) 종속으로 기 구축된 보안제품과 연계 가능
- 기존 보안 제품(툴) 교체 없이 구축 및 활용 가능

SB C&S - 소프트뱅크 그룹의 자회사로 기업 고객을 위해 ICT제품, 클라우드 서비스 및 디지털 변환 솔루션을 제공

한드림넷 Open XDR(VIPM-USM)

통합 플랫폼 제공

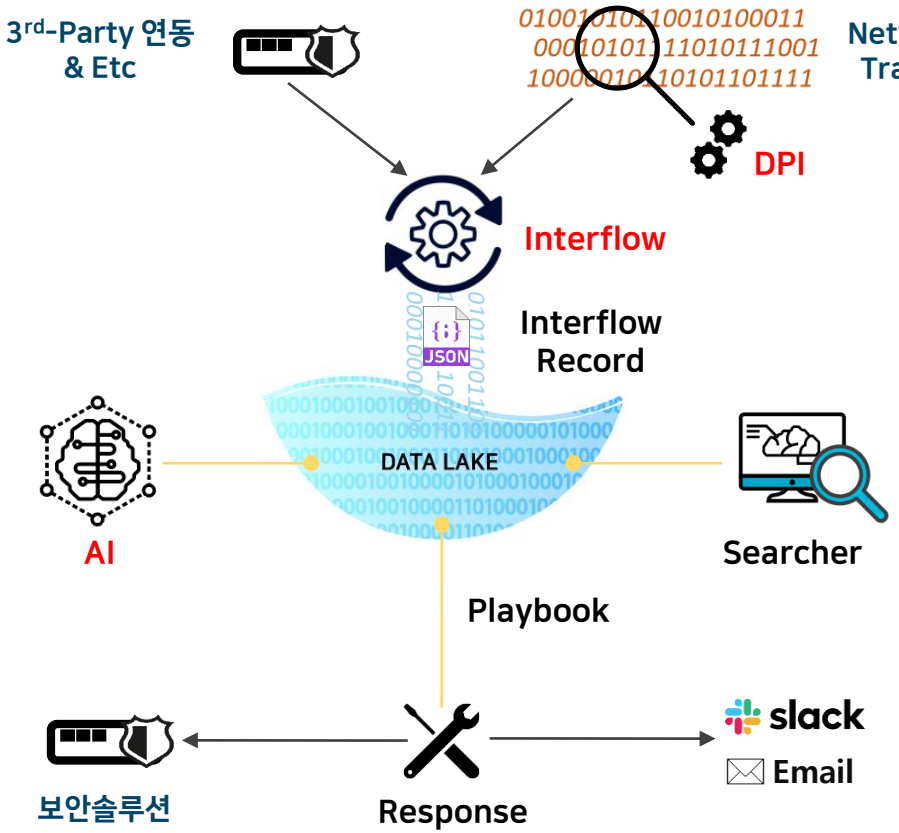


- Log 지원 포맷 – CEF, HTTP JSON, LEEF, Syslog, RFC 3164/5424
- 광범위한 데이터 수집

- 통합된 3rd-party 제품 : 16 카테고리 (91개 제품)
- Etc 연동 : SSH Remote Host, Webhook(Rest API 지원 제품)

한드림넷 Open XDR(VIPM-USM)

주요 기술 - 아키텍처



Detection AI

- 데이터 수집, 분석
- DPI(Deep Packet Inspection), TI, ML-IDS, Sandbox

- 데이터를 표준화(Metadata)
- 데이터의 압축(100:1), 보강(Location 정보 등), 저장(JSON)

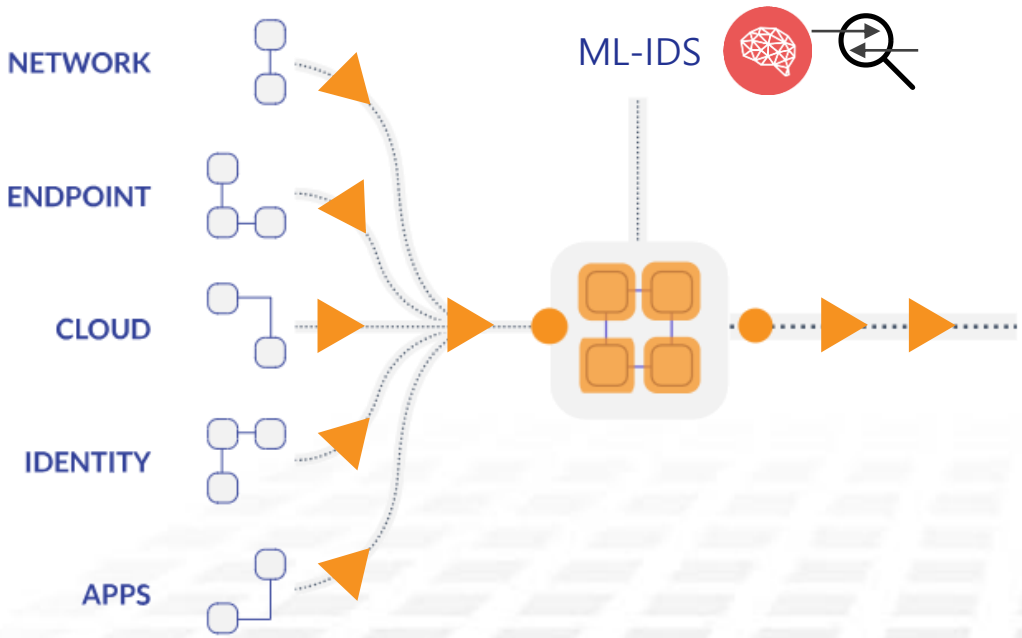
Correlation AI
Copilot AI

- Big Data(Data Lake)
- AI + 머신러닝 분석
  - 상관관계, 자산의 위협도, 위협점수+신뢰도+TI, 킬체인 분류
- 데이터 검색 및 분석(ElasticSearch)

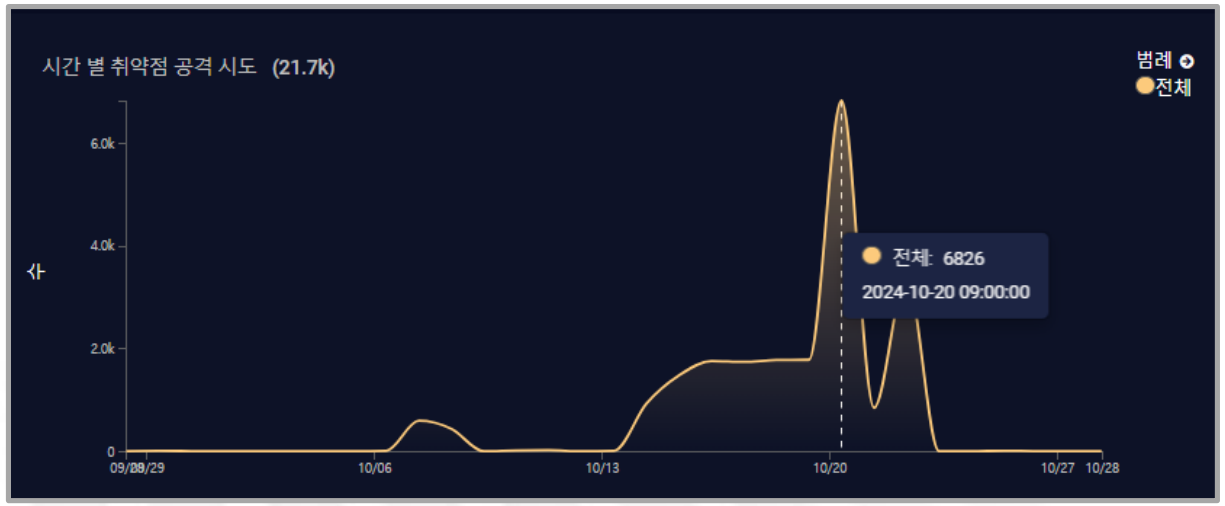
- Playbook을 통한 자동대응
- 차단 시스템 연동, Email, Messenger

한드림넷 Open XDR(VIPM-USM)

주요 기술 – 머신러닝 IDS(ML-IDS)

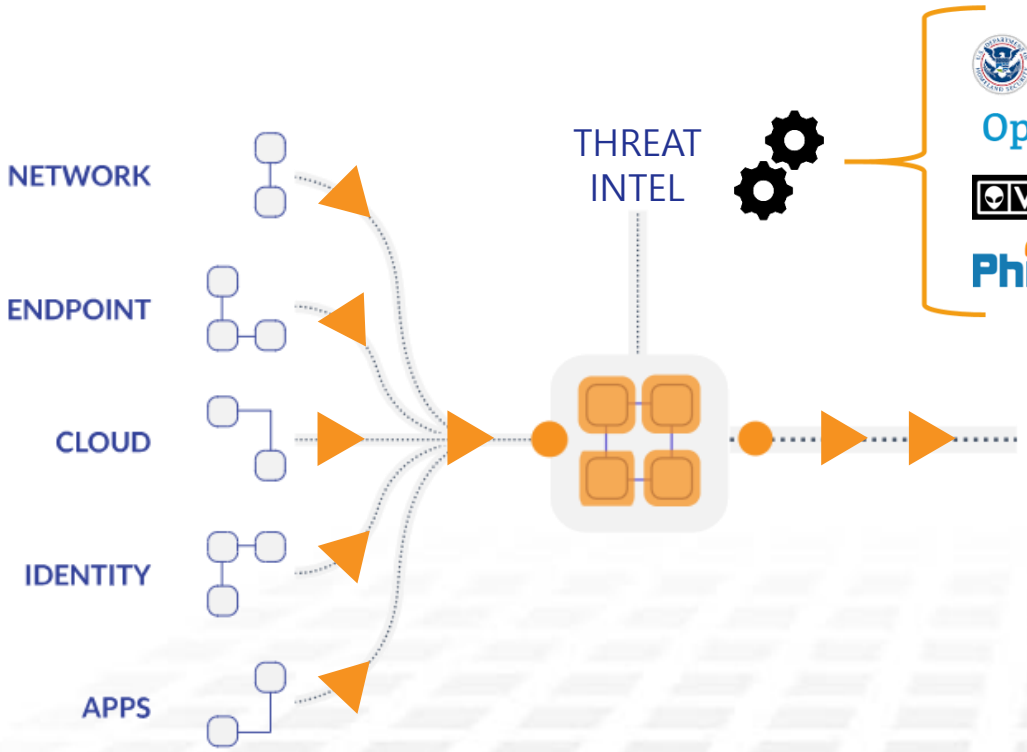


일반적인 서명 기반의 IDS와 대조적으로 ML-IDS는 서명 일치 비율을 학습하고, 해당 비율이 변경될 때 이벤트를 생성



한드림넷 Open XDR(VIPM-USM)

주요 기술 – TI(Threat Intelligence)



Homeland Security · Qualys. · OpenPhish · Microsoft · ABUSE · OVB · proofpoint. · CYBETS · PhishTank · ANOMALI

Phishing

Malware

CnC, Backdoor

Spam

Bot

P2P

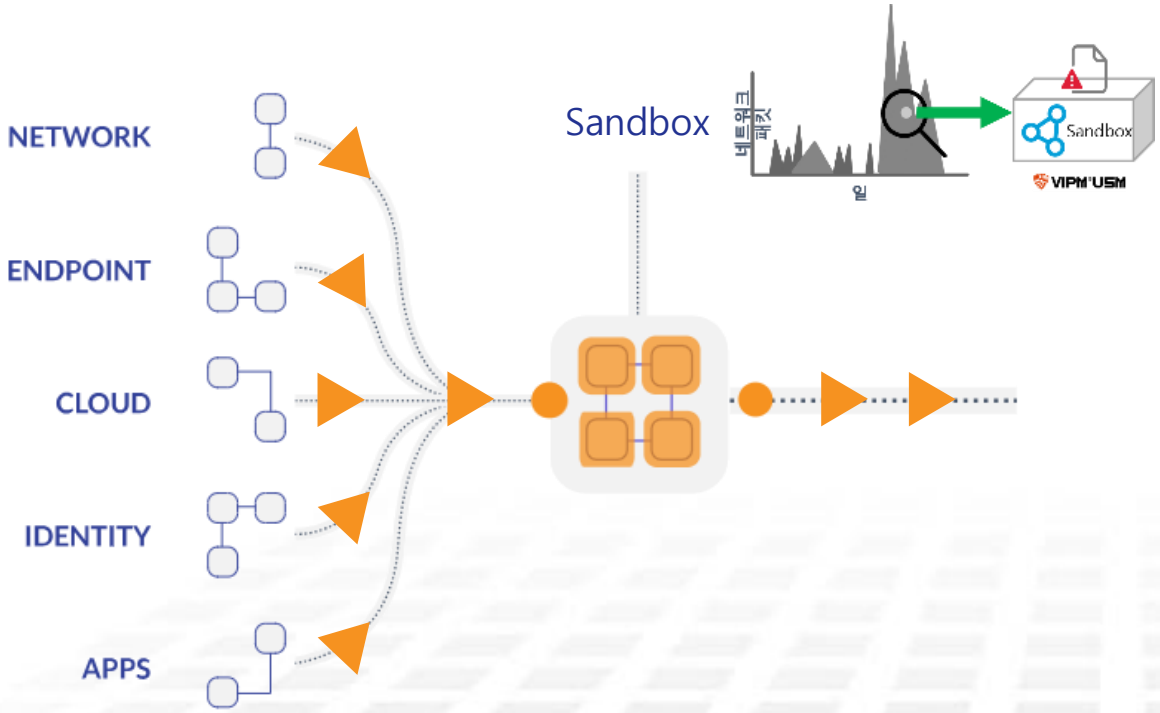
Brute Forcer

⋮

전세계 16개의 CTI(Cyber Threat Intelligence)
사들의 보안 위협정보를 받아 교차 검증 후
최신 정보를 유지

한드림넷 Open XDR(VIPM-USM)

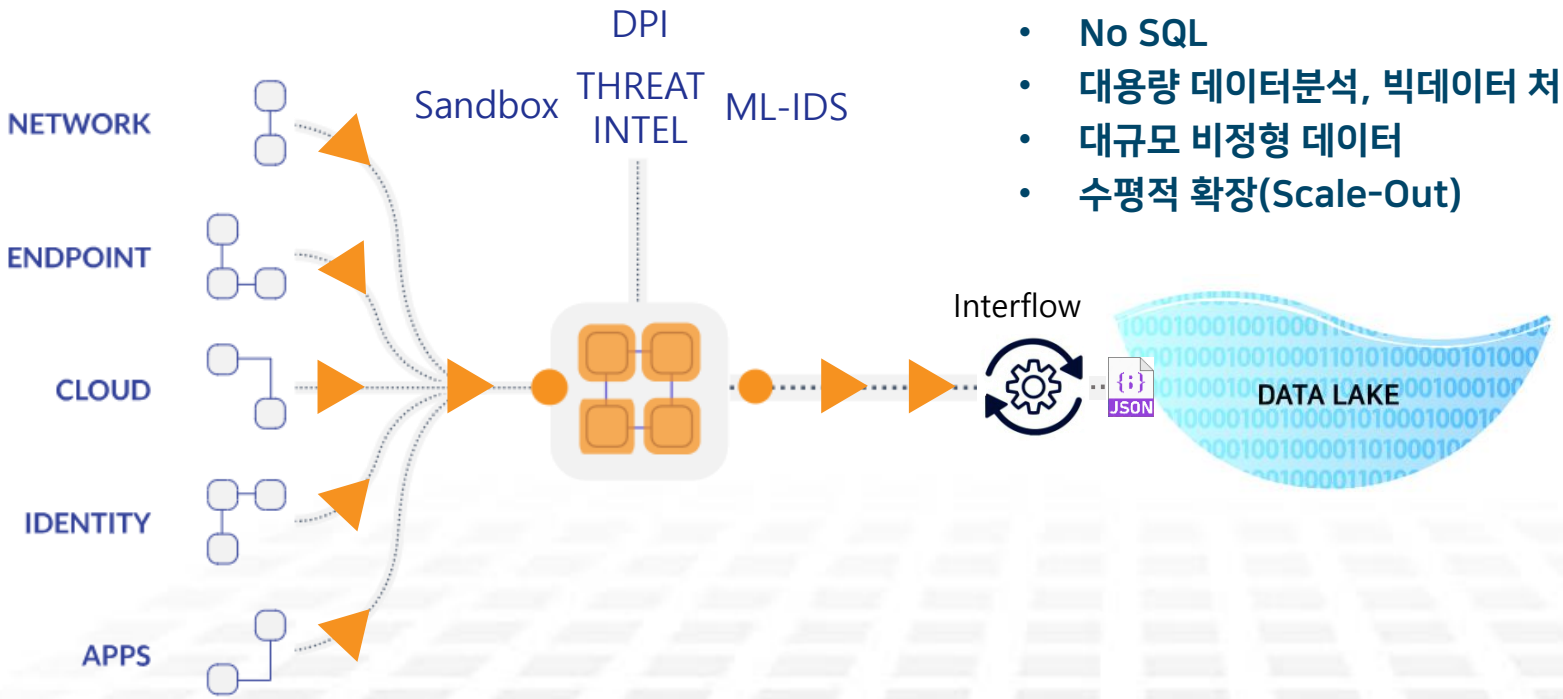
주요 기술 – 파일 분석(Sandbox)



네트워크 트래픽 내 의심스러운 파일 분석을 위해
가상환경 PC 에서 파일을 실행하여 이상 행위를 분석하는
Sandbox 기술 제공

한드림넷 Open XDR(VIPM-USM)

주요 기술 – 빅 데이터(Big Data)



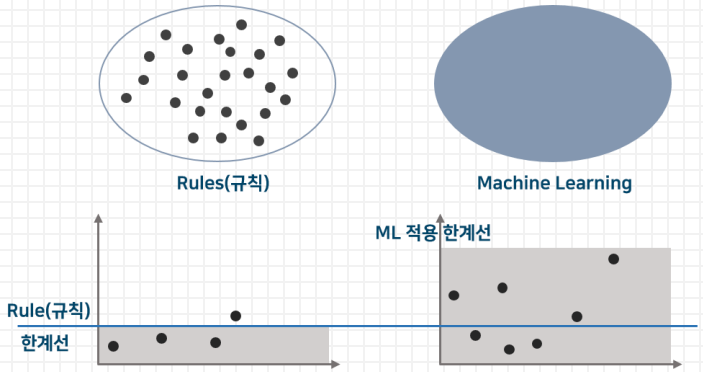
- No SQL
- 대용량 데이터분석, 빅데이터 처리
- 대규모 비정형 데이터
- 수평적 확장(Scale-Out)

JSON

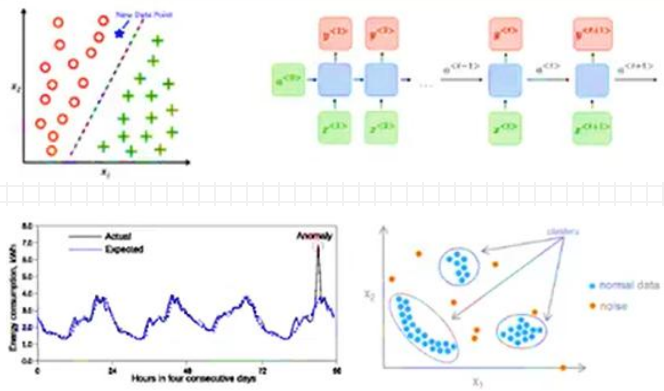
"srcip_geo_point": "37.4821,126.8954",
"srcip_host": "192.168.10.87",
"srcip_reputation": "Phishing",
"srcip_sig_id": "100.100.10.200.null",
"srcip_type": "private",
"srcip_version": "ipv4",
"srcmac": "fc:75:e6:01:5e:38",
"srcport": 48102,
"start_bucket_time": 1728886500000,
"state": "Established",
"stellar": {
"alert_time": 1728886800647,
"detection_time": 140311,
"rule_id": "sandbox_external_sa_1",
"rule_revision": 0,
"status": "New",
"task": "sandbox_external_sa"

한드림넷 Open XDR(VIPM-USM)

주요 기술 – 머신러닝/AI 분석



▪ 알려지지 않은 또는 이상 동작 탐지

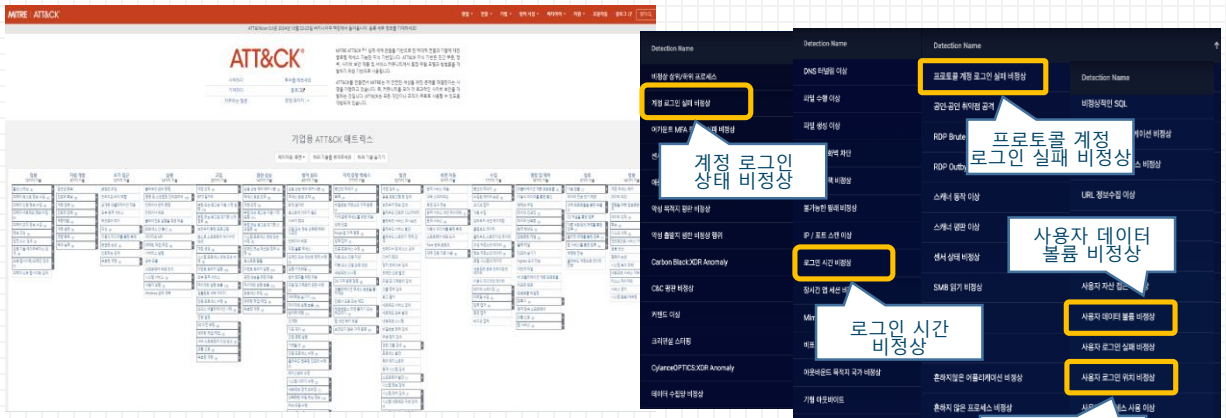


▪ 지도 학습(Supervised M/L)

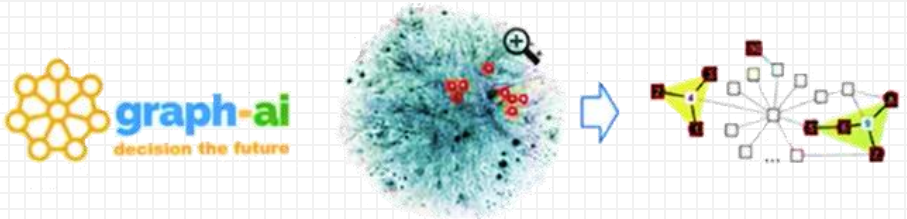
사전에 정의된 Label 및 유사도를 기준으로 학습 및 탐지 수행
(SVM, LSTM)

▪ 비지도 학습(Unsupervised M/L)

입력되는 데이터를 기준으로 학습하여 패턴을 찾고 그에 대한 비정상적 편차를 학습하여 탐지 수행
(시계열, 희귀이벤트, 그래프, 임계치, 피어 기반 시계열 분석)



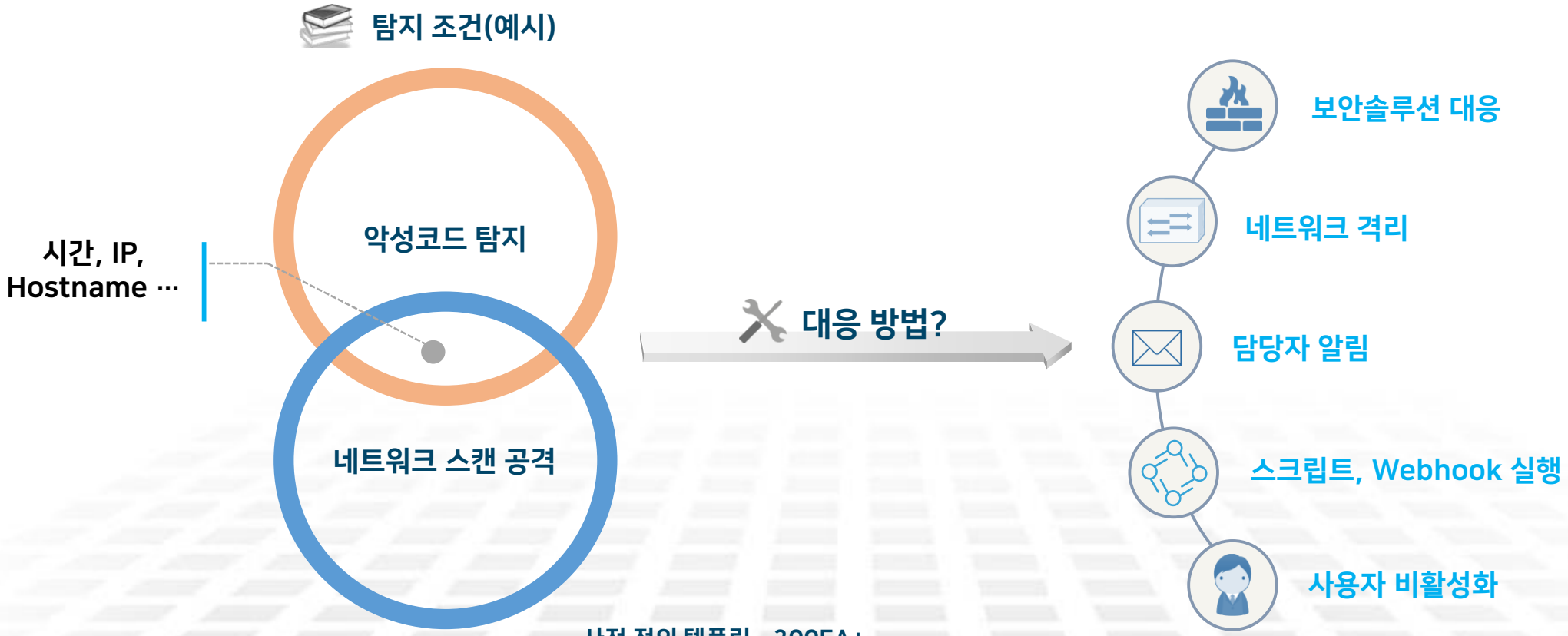
▪ 세분화된 머신러닝 탐지 모델



▪ 탐지 및 기타 데이터 신호와의 상관관계 탐지

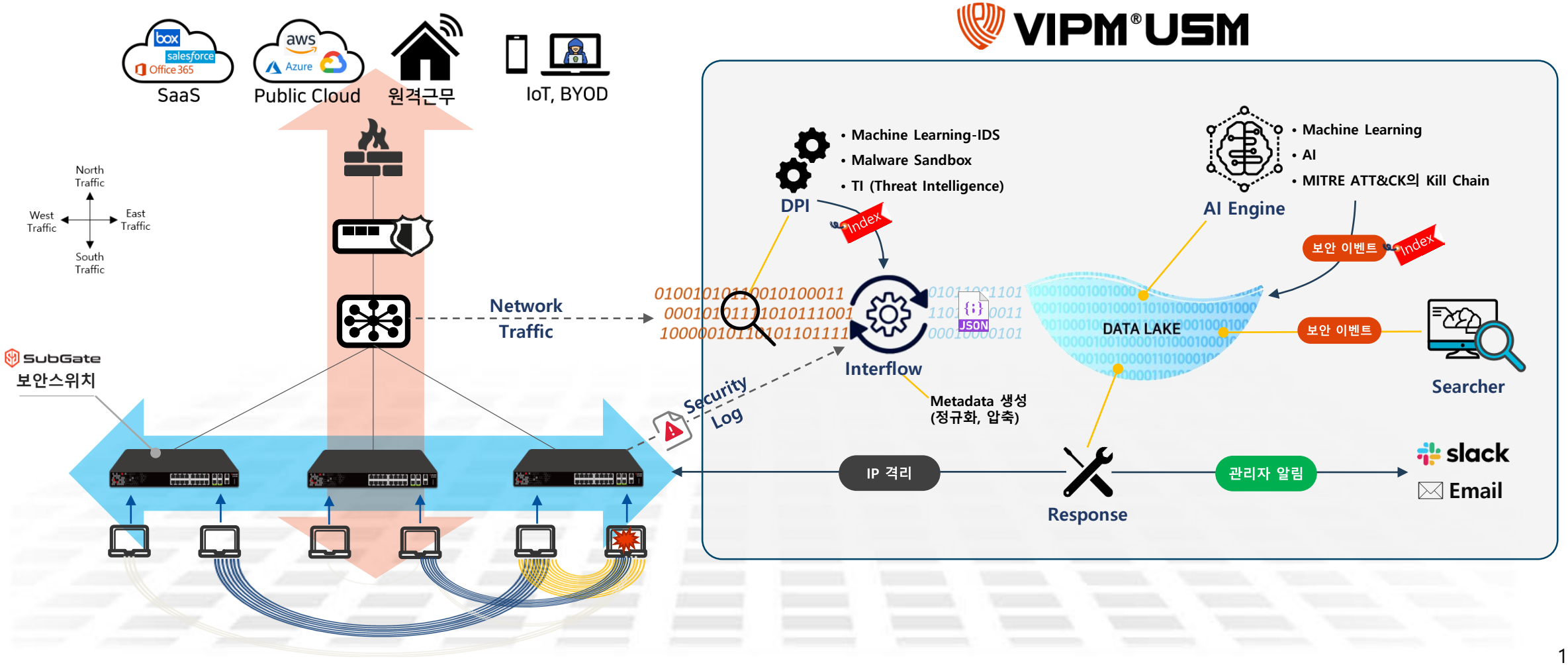
한드림넷 Open XDR(VIPM-USM)

주요 기술 – 위협 대응(Threat Response)



한드림넷 Open XDR(VIPM-USM)

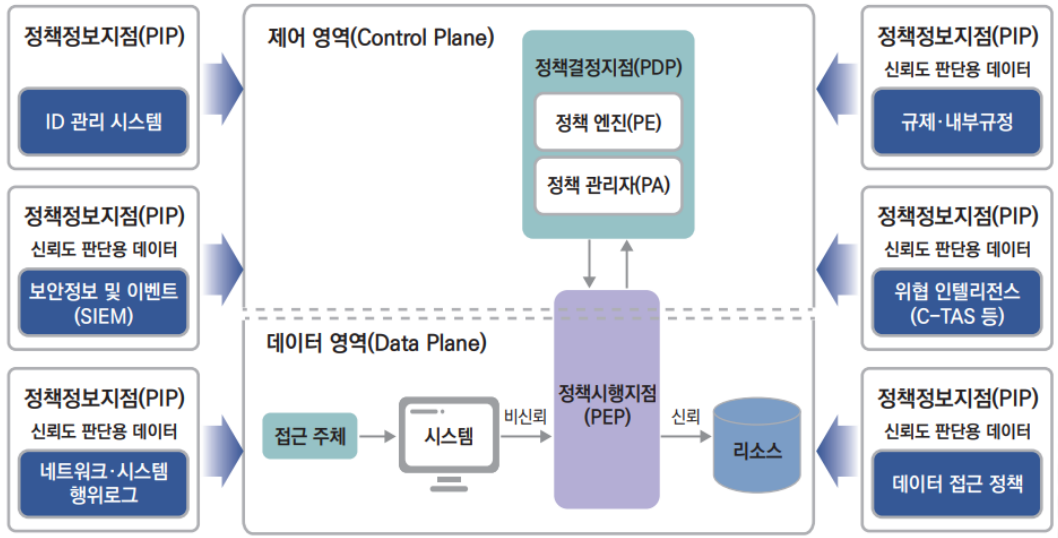
네트워크 환경의 보안 가시성 확보



한드림넷 Open XDR(VIPM-USM)

제로트러스트 보안 모델의 보안 가시성 확보

[제로트러스트 아키텍처 보안 모델 및 논리 구성 요소]



- 다중 인증(Multi-factor authentication)
- 최소한의 접근 권한(Least Privilege Access)
- 세분화(Micro-Segmentation)
- 지속적인 모니터링(Continuous Monitoring)

- Never Trust, Always Verify (절대 신뢰하지 말고, 항상 검증하라)

"성공적인 인증 후에도, 지속적인 모니터링을 통하여 신뢰성에 의심이 가는 상황이 발생하는 경우 강화된 추가 인증을 받거나 현재의 접근 세션에 대한 강제 종료 필요"

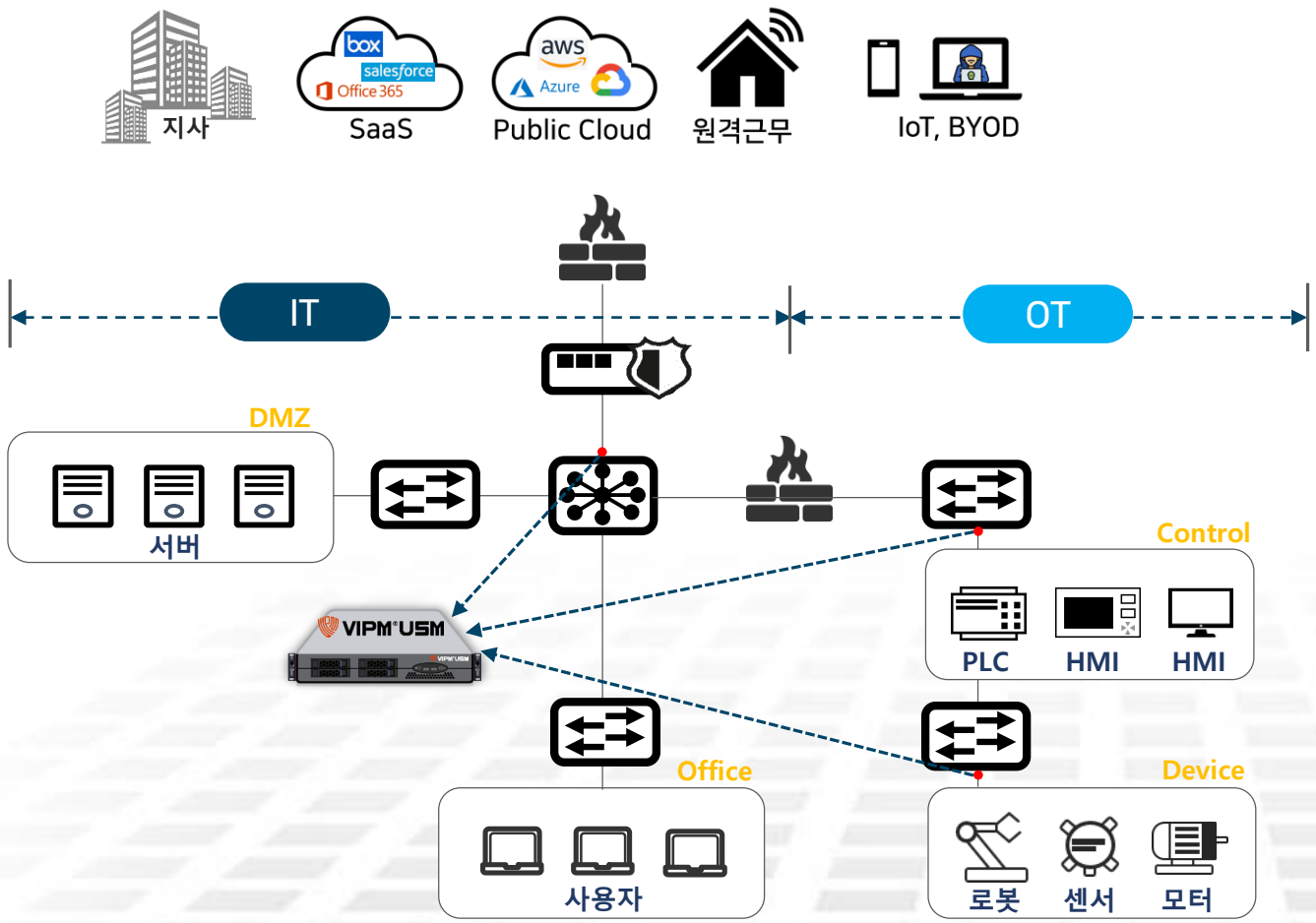
(제로트러스트 가이드라인 2.0 – 제로트러스트 아키텍처 기본 원리 중)

1. 민감한 자산 식별
2. 민감한 자산에 대한 통신 매핑
3. 마이크로 세분화 정의
4. 정책 구현
5. 지속적인 모니터링 구현

- VIPM-USM 사이버 킬체인

한드림넷 Open XDR(VIPM-USM)

IT/OT 환경의 통합 보안 가시성 확보



단일 플랫폼에서 IT/OT 환경을 통합

- 비표준 SCADA 프로토콜 감지
- SCADA 네트워크 경계 위반 감지
- 네트워크 공격 탐지(OT 서명 기반)
- 악의적, 의심스러운 파일 탐지
- 비정상적인 통신 / 포트 / 데이터 전송
- IT에서 OT로 측면 이동 인시던트 감지

AAON PRISM 2	ESK M3	Invar Systems AS/RS 제어	PI Data Archive
B&R 자동화	Ethernet/IP	iWarehouse	Process Field Net
BACnet 어플리케이션 계층	Experion product	KEYENCE 바코드 리더	Rockwell RNA
BACnet 네트워크 계층	fanuc gen	Lenel OnGuard 클라이언트	S7 Communication
BACnet 가상 링크 제어	General Electric Proficy	제조 메시지 사양(ISO 9506)	S7 Communication Plus
Bosch 시큐리티 코넥틱스	일반객체 변전소 이벤트	Mercury Security	Schneider 통합 객체 네트워크
Codesys 프로토콜	고가용성	Mettler Toledo 인터페이스 명령	SeamLess Message
일반산업 프로토콜	데이터 링크제어	Modbus	Siemens Apogee
CSP AB 이더넷	Honeywell	Modbus 원격 터미널 장치	Socomec
DeltaV	HSR/PRP 감독	Moxa (ASPP)	Toyo PLC
분산네트워크 프로토콜	IEC 60870-5-104	Omron FINS 프로토콜	Vnet/IP
DLMS/COSEM(IP기반)	IEC 61850 샘플링 값	OPC 통합 아키텍처	Yokogowa
DLMS/COSEM(IP 래퍼 기반)	IEEE C37.118 동기위상기	병렬 이중화 보호	
Dr Schenk	제어센터 간 통신	PC-cubed	
EquipCommand 프로토콜	Intermec SmartSystem	PI AF	

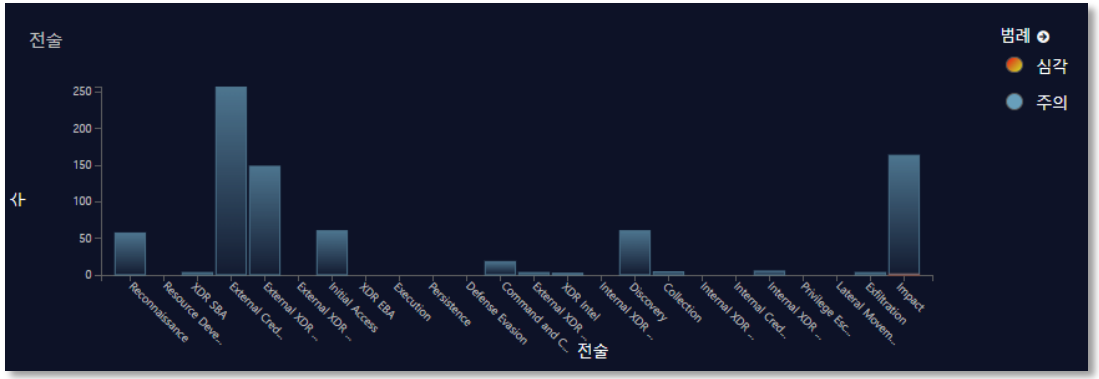
한드림넷 Open XDR(VIPM-USM)

주요 제공 화면

사이버 공격 단계

- 록히드마틴의 사이버 킬체인 7단계를 보강하여, 5단계 로 AI 경보 처리의 용이성, 분석의 효율성을 강화

사이버 공격의 기술/전술

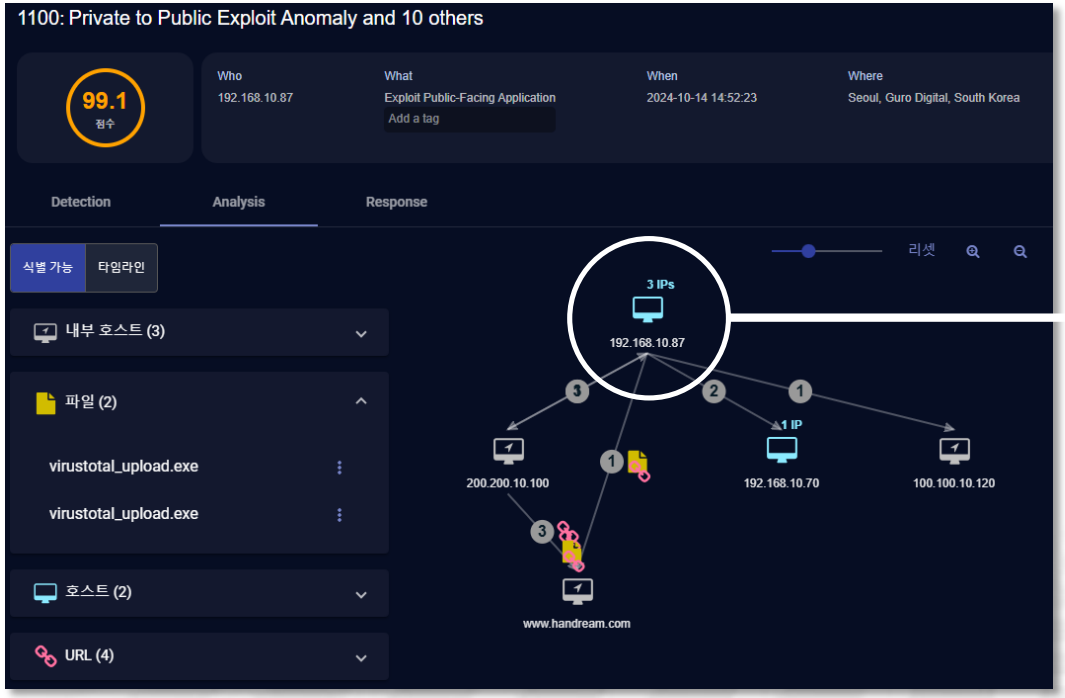


- MITRE ATT&CK Framework 기반의 위협 기술/전술을 세분화하여 제공

한드림넷 Open XDR(VIPM-USM)

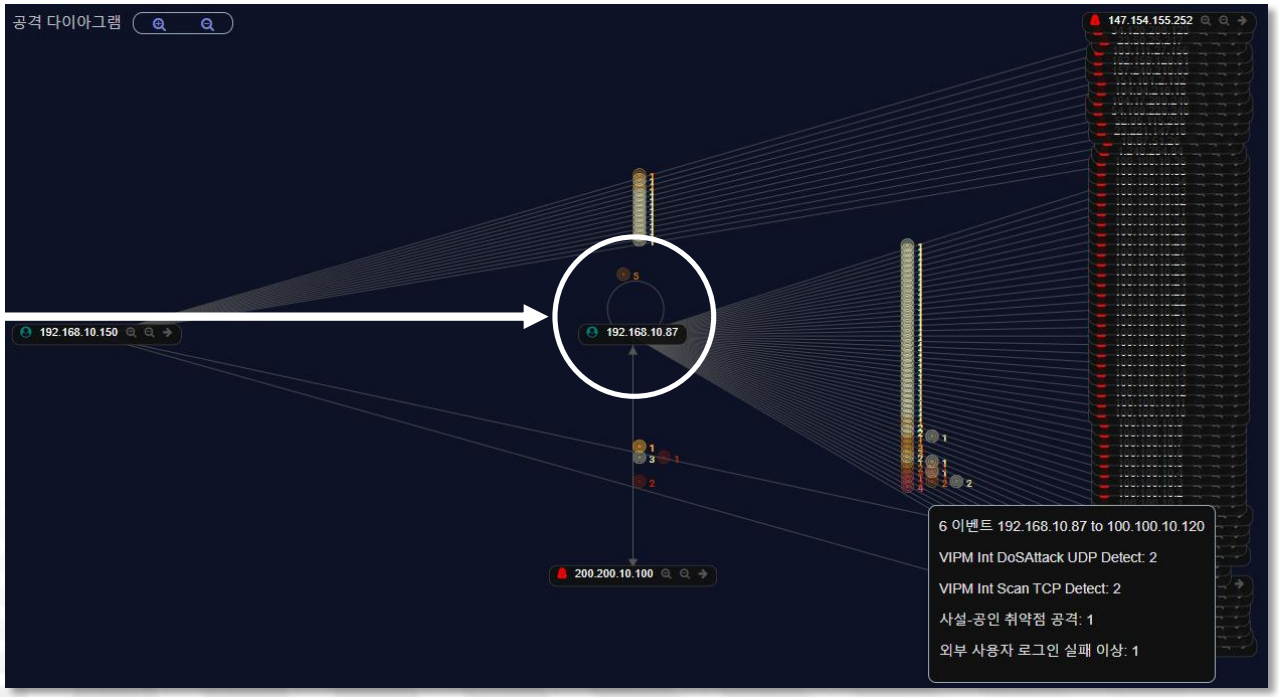
주요 제공 화면

자동 상관관계 분석



- 컨텍스트 분석으로 보안 요소의 상관관계를 제공
- 식별 가능한 증거 및 사건을 타임라인 별로 제공

위협 헌팅



- 위협요소를 중심으로 복잡한 공격 정보를 한눈에 파악 할 수 있는 공격 다이아그램 제공

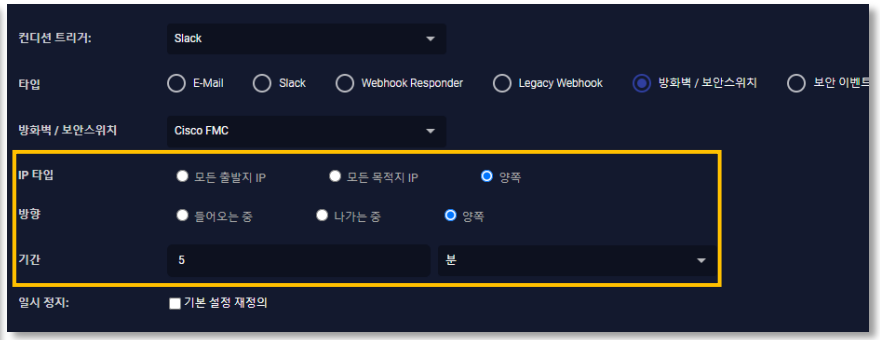
한드림넷 Open XDR(VIPM-USM)

주요 제공 화면

3rd-Party 통합

카테고리	제품 수	카테고리	제품 수
Cloud Security	2	NDR	1
Database	2	PaaS	7
DNS Security	2	Password 관리	1
Email	5	SaaS	8
Endpoint Security	30	SASE	2
Firewall	13	Security Switch	1
Honeypot	1	Vulnerability Scanner	9
IdP	5	Web Security	7

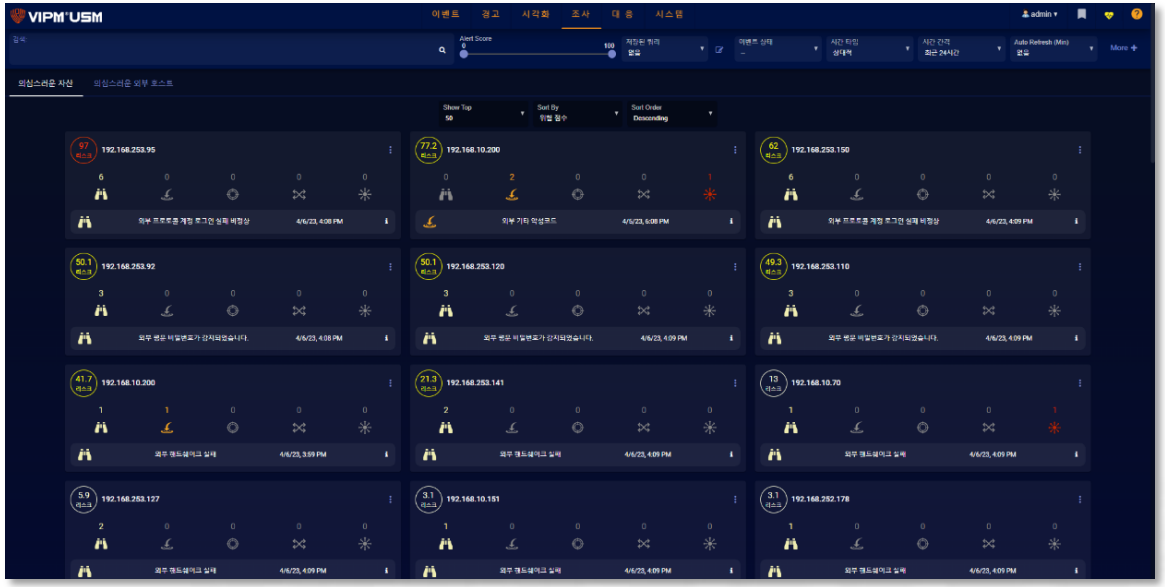
위협 대응



한드림넷 Open XDR(VIPM-USM)

주요 제공 화면

자산 파노라마 뷰



- 보안 Risk가 높은 내부 자산에 대한 파노라마 뷰
- 의심스러운 외부 Hosts 에 대한 파노라마 뷰

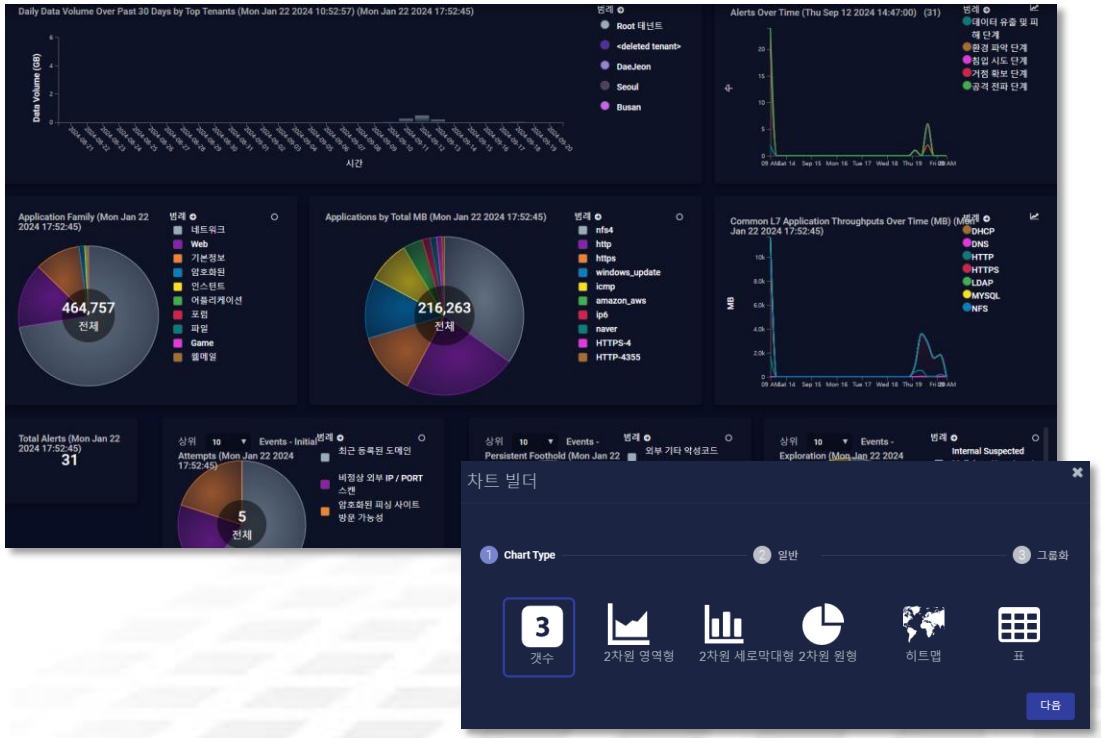
네트워크 가시성

- 네트워크, 서버, 데이터베이스, 어플리케이션, HTTP, DNS, 터널 어플리케이션 대한 시각화 뷰

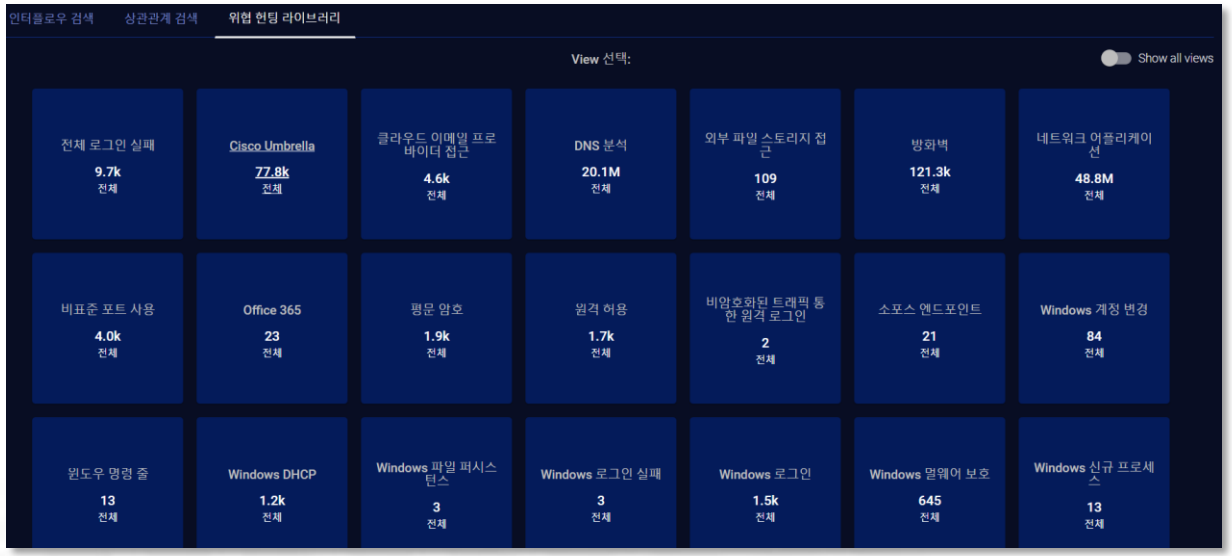
한드림넷 Open XDR(VIPM-USM)

주요 제공 화면

사용자 정의 대시보드 생성



위협 헌팅 라이브러리



- 위협 헌팅이 된 정보를 라이브러리화 하여 제공

한드림넷 Open XDR(VIPM-USM)

기대효과

▪ 전체 공격 표면 보호

즉시 사용 가능한 위협 탐지 기능을 통해 온프레미스, 클라우드, IT/OT 환경에 대한 위협을 식별합니다.

▪ SecOps 성능 향상

MTTD(평균 탐지 시간) 8배 이상, MTTR(평균 대응 시간)을 20배 이상 개선합니다. AI를 통해 보안운영 업무 효율성을 극대화 시킵니다.

▪ 비용의 절감

DPI, Sandbox, TI, SOAR 기능을 별도 구매 없이, 기본 제공하고, 타 보안 솔루션의 이벤트 통합 옵션으로 보안운영 투자 전략에 있어 비용 절감 효과를 제공합니다.

감사합니다.

발표자 : 김종윤 부장 (jykim@handream.net)