IGLOO

클라우드 환경에서의

보안관제 운영 방안

SECURITY &
INTELLIGENCE

IGLOO

클라우드 환경에서의 보안관제 운영 방안

보안관제에 지능을 더하다

SECURITY &
INTELLIGENCE

보안 이슈는 기술적 이슈보다 더 복잡합니다

2022년까지, 전 세계적으로 약 2백만 명의 사이버 보안 인력이 부족할 것으로 전망

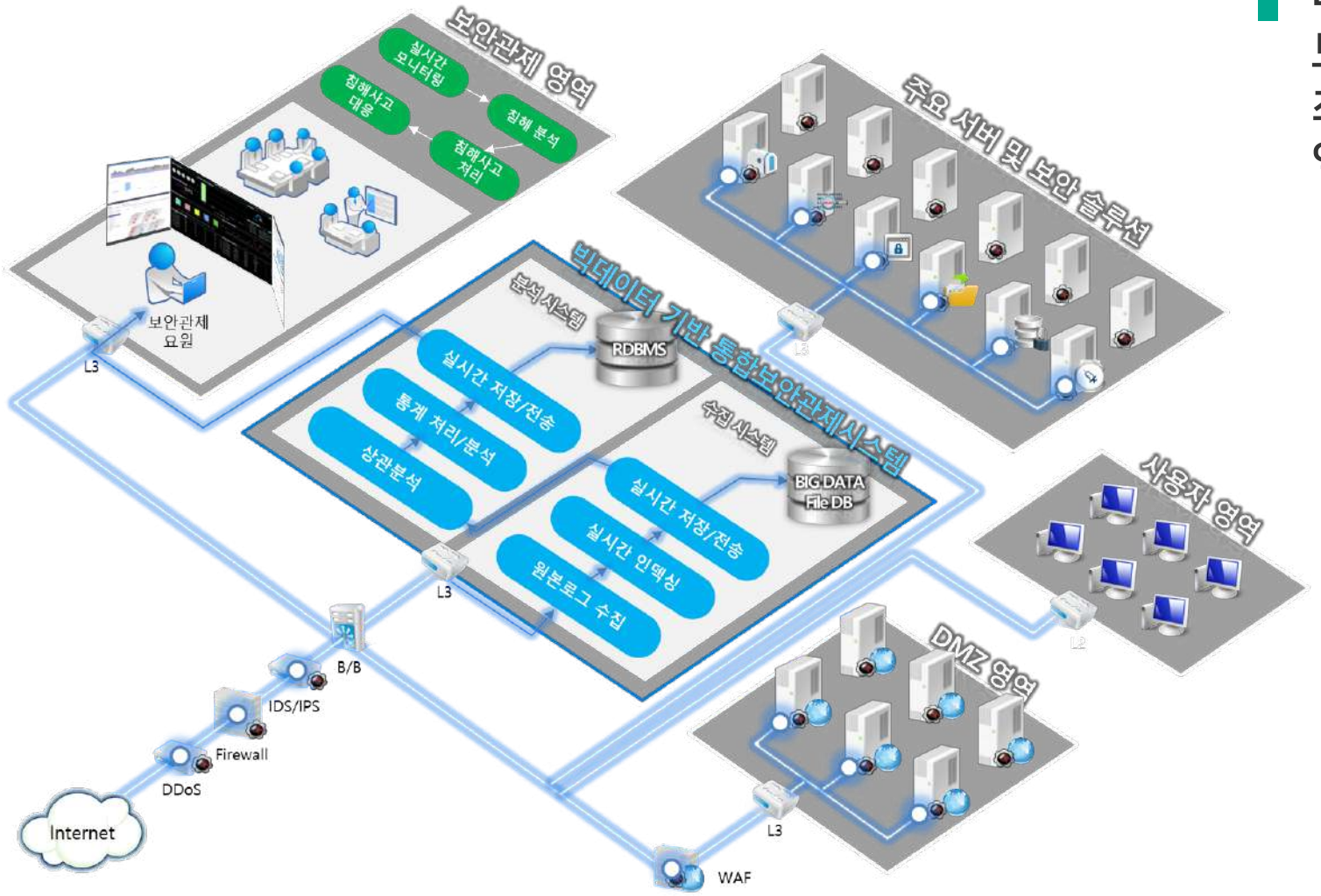
- 새로운 보안위협들에 대한 적절한 대응 부족
- 더욱 더 복잡해지는 많은 보안 경고에 업무 가중
- 숙련된 기술 보유한 SOC 전문인력은 현저히 부족
- SOC 운영모델의 지속적이고 체계적인 관리 부족

SOC는 빅데이터를 거쳐 지능형 보안관제로 진화하고 있습니다

보안관제는 보안위협, 보안기술

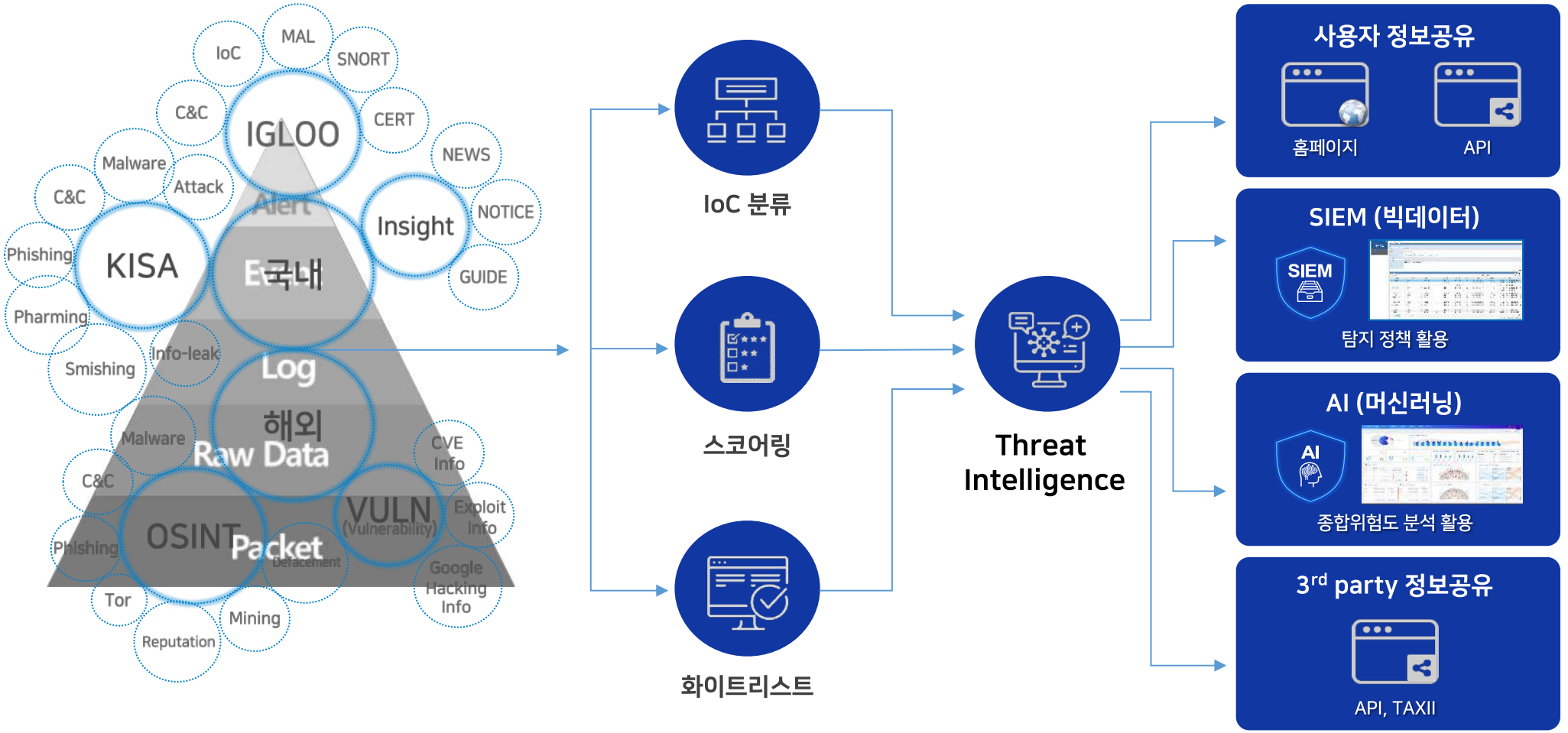
1세대 단위 보안관제	2세대 통합 보안관제	3세대 빅데이터 보안관제	4세대 지능형 보안관제
- 방화벽, 침입탐지시스템 등 네트워크 기반의 보안장비를 이용한 초기 구축단계 - 보안 인프라의 고도화 및 안정화 단계	- 정보공유분석센터(ISAC), 종합분석시스템 등이 구축 - 위협 트래픽 관리, 취약점 관리, 웹 변조 모니터링 등 관제의 범위 확대	- 보안위협의 고도화·지능화 - 대다수의 로그, 이벤트, 네트워크 패킷 연동으로 시나리오 기반 분석 확대 - 위협인텔리전스 구축/활용	- 머신러닝(ML) 기반의 정오탐 분류 및 이상행위 식별로 관제역량 향상 - **SOAR 기반의 업무절차 및 대응 자동화**
Individual Solution	ESM (Enterprise Security Management)	SIEM (Security Information and Event Management) CTI (Cyber Threat Intelligence)	AI · ML (Machine Learning) SOAR (Orchestration Automation and Response)

4세대 보안관제 - ① 빅데이터 기반 통합보안관제시스템 [SIEM]

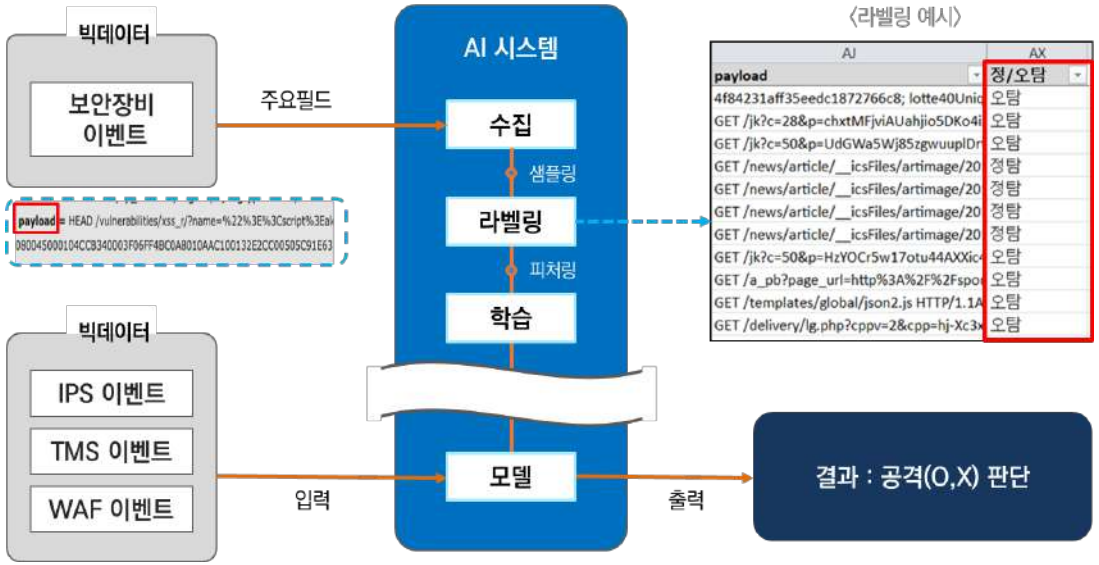


다양한 이기종 장비의 원본로그를
모두 수집하여,
최초 탐지부터 분석, 대응까지
일원화된 보안관제 환경을 제공

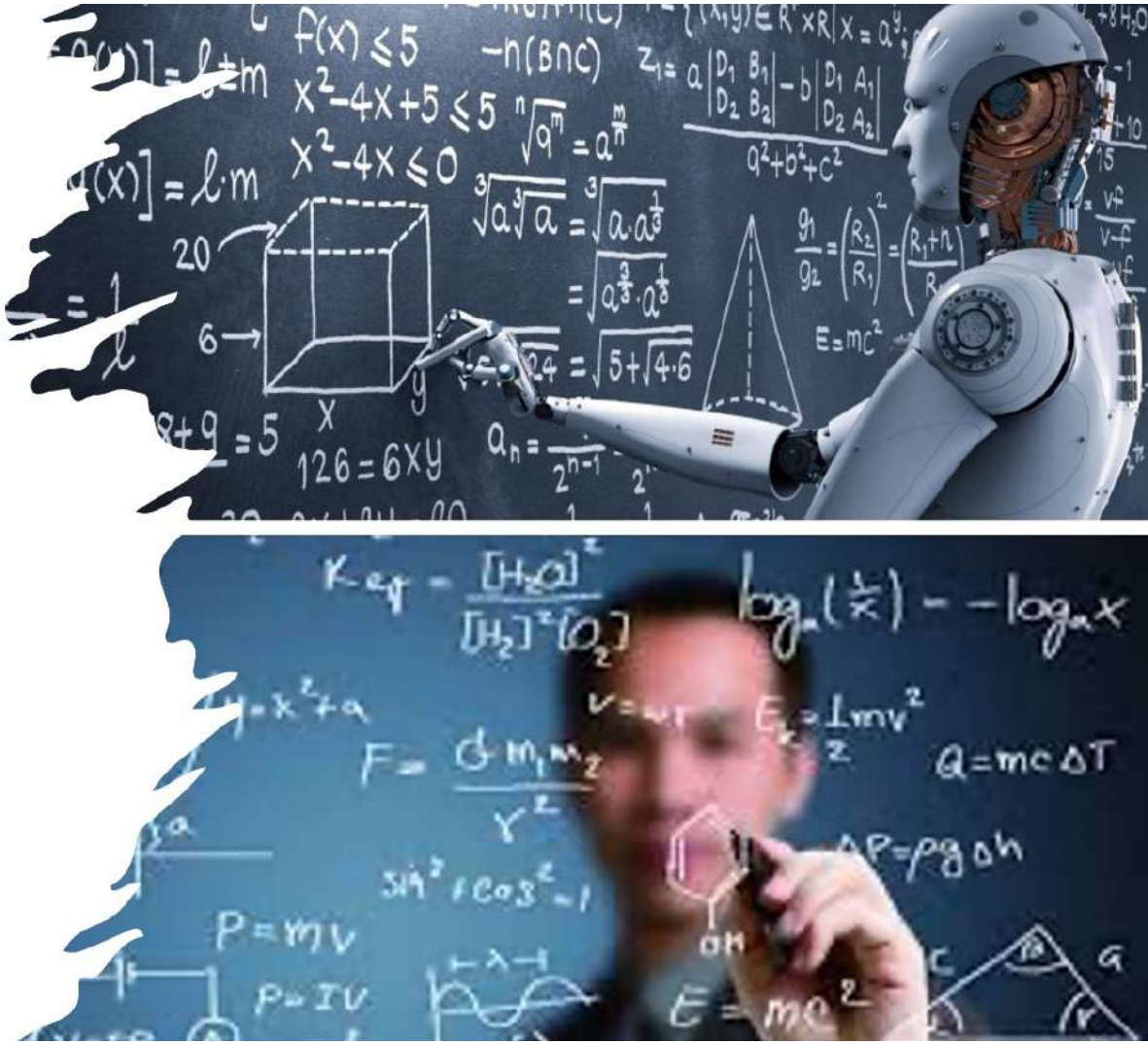
국내·외 다양한 위협데이터를 수집하여, 상호 연관 관계를 분석하는데 필요한 위협정보를 제공



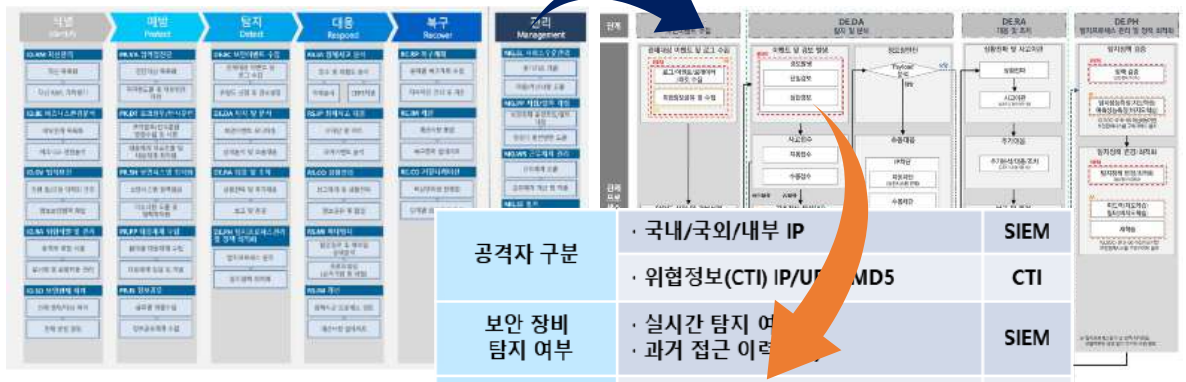
90% 이상 높은 정확도, 24X365 일관된 결과 제공



▲ 보안이벤트 분석모델 개발 및 운영 방법 (지도학습 예시)



보안관제 인력과 시스템의 협업을 통해 보안관제 업무를 자동화

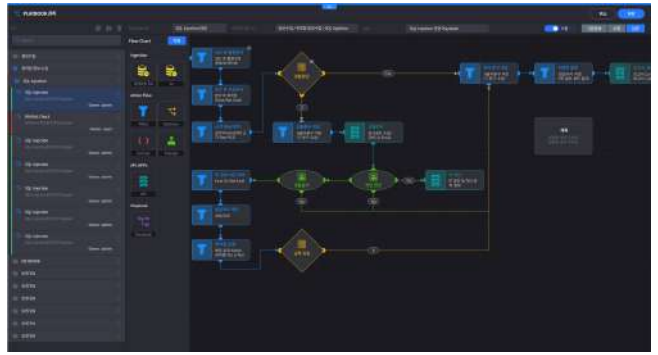


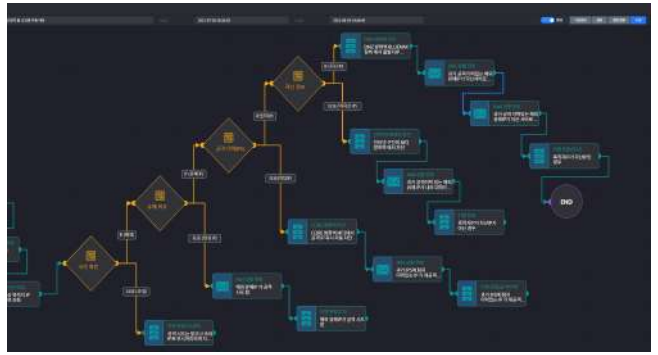
▲ 보안관제 방법론

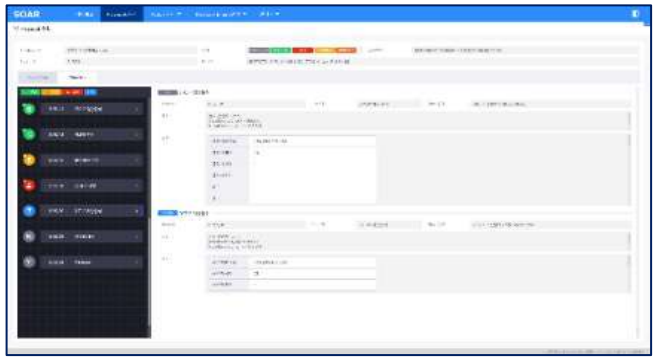
▼ 침해시도 대응절차

플레이북 컴포넌트 정의 ▶

공격자 구분	· 국내/국외/내부 IP	SIEM
	· 위협정보(CTI) IP/UR MD5	CTI
보안 장비 탐지 여부	· 실시간 탐지 여 · 과거 접근 이력	SIEM
침해대응이력	· 과거 침해 이력 확인(해당기관)	SIEM
Payload	· 탐지 패킷 (IPS/TMS) · FULL 패킷 (WAF) (웹쉘 업로드/설정값 다운로드)	SIEM
웹서버	· 자산 여부 · 서비스 여부 : 80, 443 Port	자산
	· 웹 접속 로그(Access log) 분석	SIEM
자산관리솔루션	· OS, WEB, WAS, DB 정보 (플랫폼에 맞는 공격 여부) · ASP, JSP, PHP 언어	SIEM 자산
	· 해당 Application 사용 여부 (Fckedit, PHPMyadmin, log4j) > 수동 혹은 수집된 웹로그 이력 조회 후 사용 여부 확인	자산
취약점	· 취약점 존재 여부	취약점







4세대 보안관제 - ④ 보안관제 대응자동화 플랫폼 [SOAR]

수집 Ingestion

- SIEM (경보)
- 머신러닝 기반 보안관제시스템 (학습(Training)및 예측(Prediction))
- 자산정보 취약점정보
- 위협 인텔리전스 (Threat Intelligence)
- 다수의 이기종 보안장비 및 솔루션 보안 이벤트

자동 대응

직접 대응

시스템대응 Orchestration & Automatic Response

Automation |Playbook-based Response|

정보분석 (Investigation)
- 위협지표 영향범위 및 평판조사
- 유효 취약점 공격여부
- 이전경보 발생여부
- 자산 · 사용자 정보 취합

판단 (Decision)
- 공격 유효성 판단
- 정 · 오탐 판단
- 완료 · 무시 판단
- 차단 · 격리 판단

차단 (Blocking)
- 방화벽 차단
- NAC 격리
- 서비스 차단(IPS)
- 계정 잠금

API 연동 |APPS|

DBMS Query APPS | ES Query APPS | REST API APPS | SMS/ Email APPS | IPS Block APPS | FW Block APPS

Manually Response |Function-based|

초동분석
- 위협지표 영향범위 및 평판조사
- 유효 취약점 공격여부
- 이전경보 발생여부
- 자산 · 사용자 정보 취합

초동대응
- 공격 유효성 판단
- 정 · 오탐 판단
- 완료 · 무시 판단
- 차단 · 격리 판단

조치대응
- 방화벽 차단
- NAC 격리
- 서비스 차단(IPS)
- 계정 잠금

전문가대응 Expert Response

조치 Recovery

- Incident 원인제거 (Malware, Service, Process 등)
- 보안위협(Weakness) 및 취약점(Vulnerability) 패치
- 분석결과 보고서 작성 (Reporting)

IGLOO

클라우드 환경의 보안관제 운영 방안

클라우드 보안위협, 그리고 보안관제

SECURITY &
INTELLIGENCE

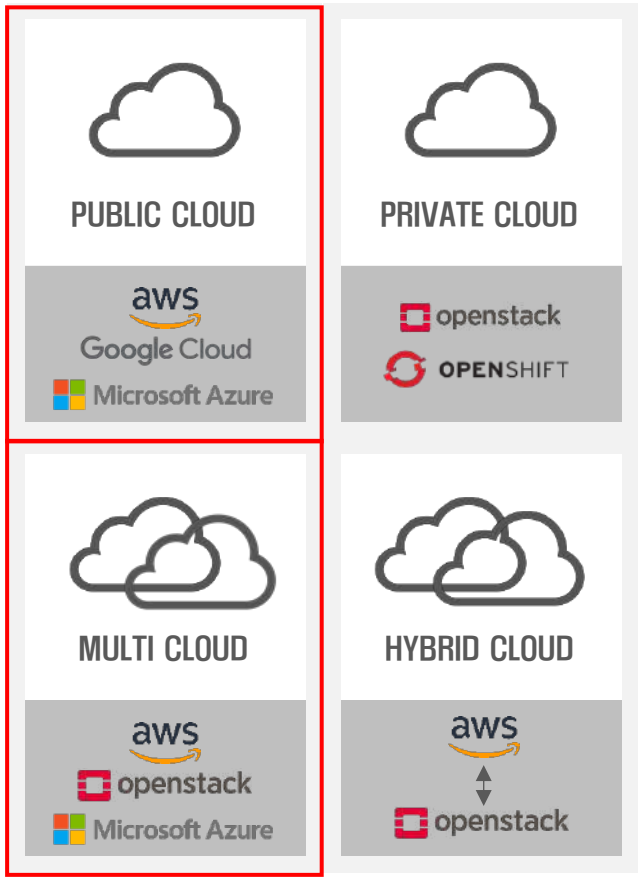
2019년부터 CSP 보안책임은 제외, 클라우드 보편화에 따라 운영보안 및 아키텍처 관점으로 변화

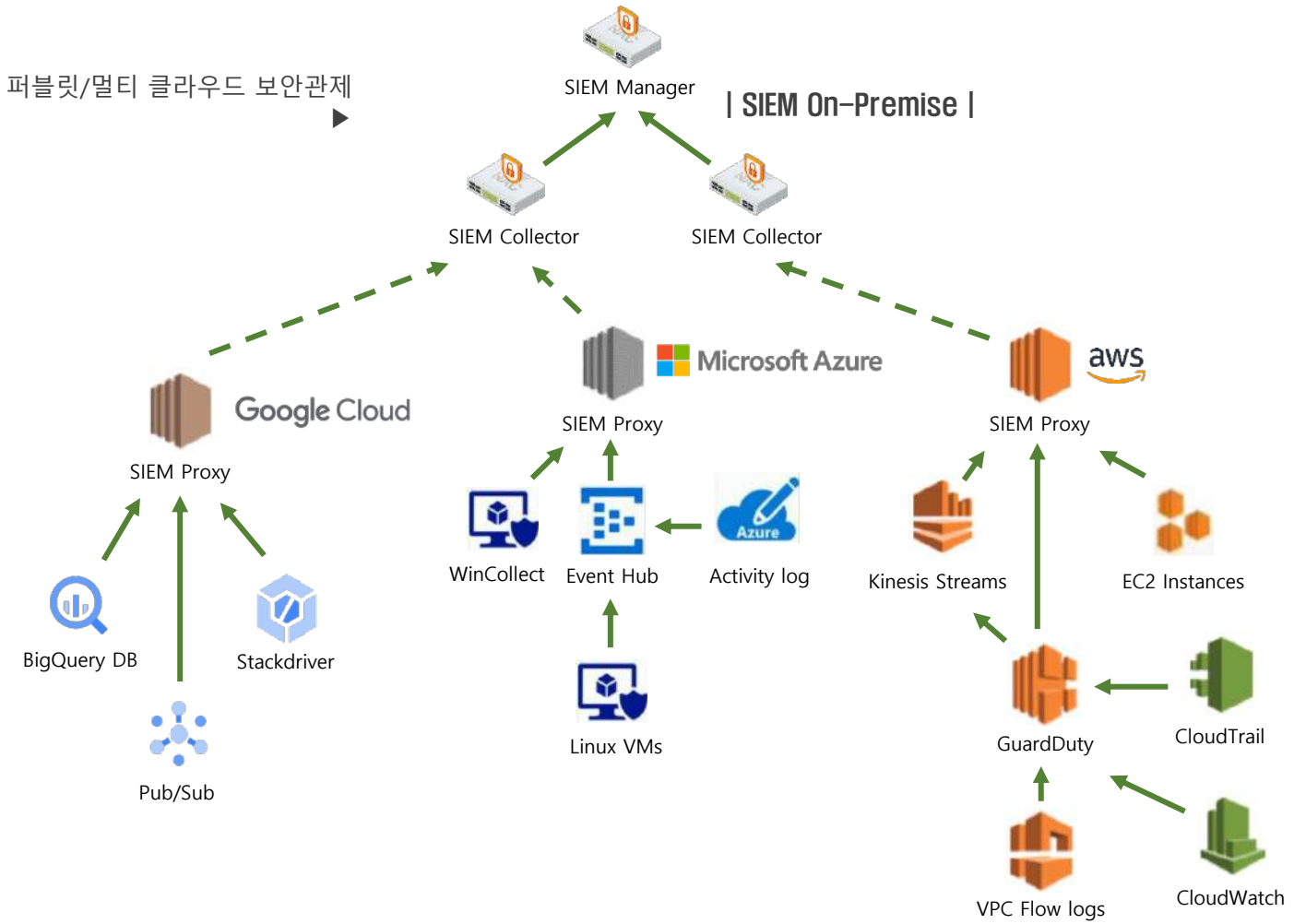
2013년	2016년	2019년	완화 방안 (2019년 기준)
Abuse and Nefarious Use of Cloud Services	Abuse and Nefarious Use of Cloud Services	**클라우드 서비스 오용/악용** (Abuse and Nefarious Use of Cloud Services)	· 서비스 오용 및 악용 모니터링
Malicious Insiders	Malicious Insiders	**내부자 위협** (Insider Threat)	· 잘못된 인증 및 접근권한 감사, 주기적인 교육
Insufficient Due Diligence	Insufficient Due Diligence	**불충분한 신분, 크리덴셜, 접근 키관리** (Insufficienet Identity, Credential, Access Key Management)	· 최소권한원칙에 따른 인증조치(이중인증,접근권한)
Insecure Interfaces and APIs	Advanced Persistent Threats	**취약한 제어영역** (Weak Control Plane)	· 클라우드 서비스 운영자 관점의 서비스 제어 방안
Shared Technology Vulnerabilities	Insufficienet Identity, Credential, Access Key Management	**잘못된 설정과 부적절한 변경관리** (Misconfiguration and Inadequate Change Control)	· 클라우드 자원의 복잡도로 인한 인프라 구성의 한계 · 잘못된 자원검사 기술 및 자동화 필요
Data Loss	Insecure Interfaces and APIs	**제한된 클라우드 사용의 가시성** (Limited Cloud Usage Visibility)	· 보안솔루션을 통한 위협 가시성 확보
Data Breaches	Shared Technology Issues	**불안전한 인터페이스 및 API** (Insecure Interfaces and APIs)	· OCCI나 CIM과 같은 OpenAPI 프레임워크 고려
Account or Service Hijacking	Data Loss	**데이터 유출** (Data Breaches)	· 잘못된 인증 및 인가로 인한 데이터 유출 대응 · 침해사고 예방 및 대응활동
Denial of Service	Data Breaches	**계정 하이재킹** (Account Hijacking)	· 계정 유출 및 도난 주의 · 심층방어기법 및 IAM관리
	Account Hijacking	**메타스트럭처와 애플리스트럭처 실패** (Metastructure and Applistructure Failure)	· 클라우드 서비스 제공자 관점의 보안방안 제시
	Denial of Service	**클라우드 아키텍처 및 전략 미흡** (Lack of Cloud Security Architecture and Strategy)	· 클라우드 기반 보안아키텍처 및 프레임워크 수립 필요 · 클라우드 기반 위협모델의 최신화
	System Vulnerabilities		

관리적 위협

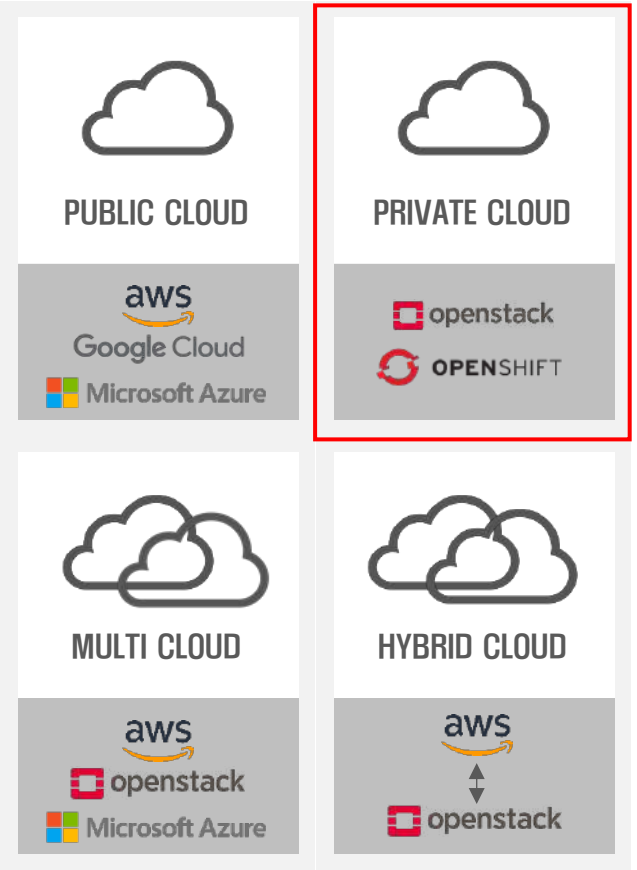
기술적 위협

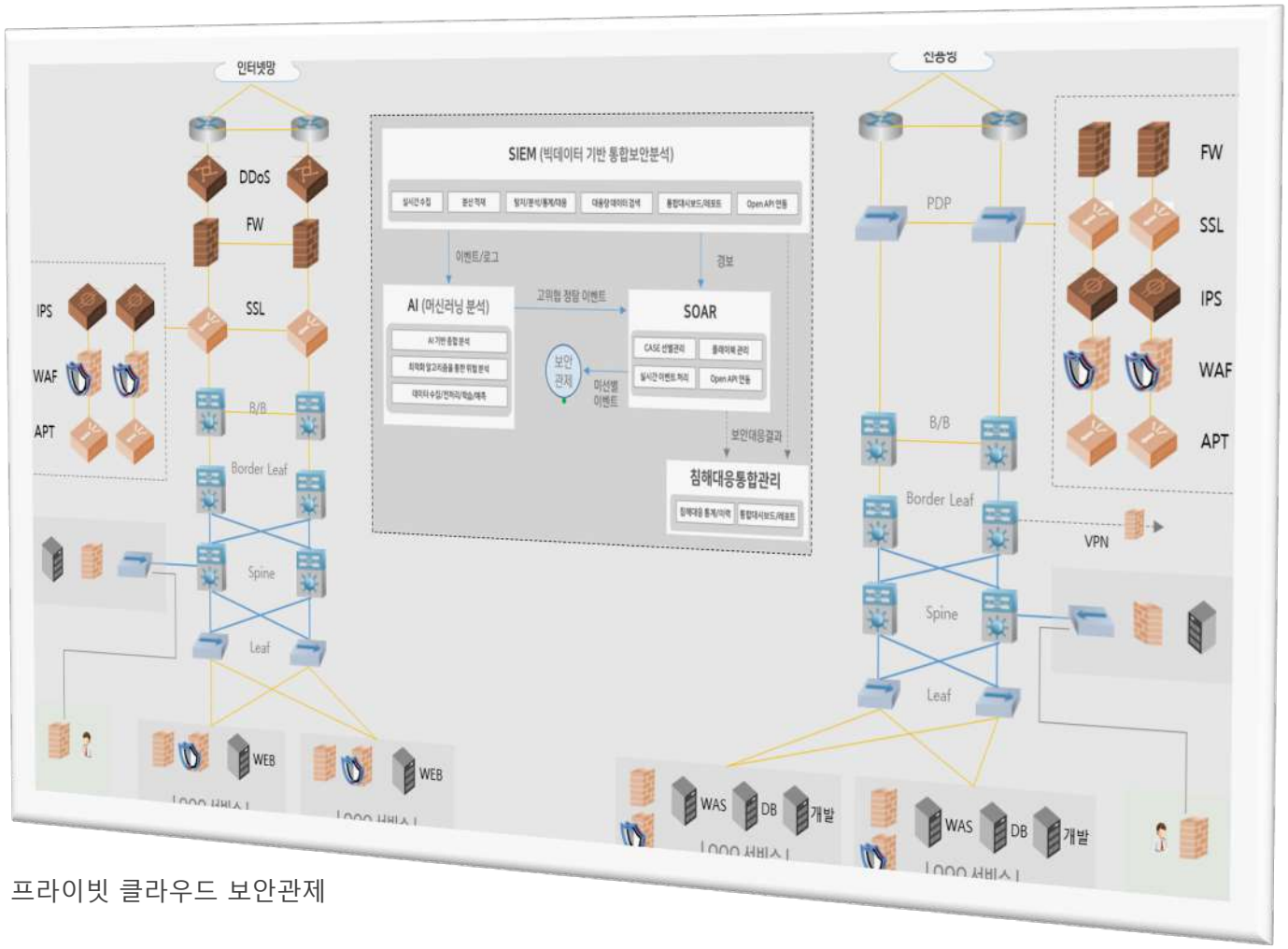
퍼블릭/멀티 클라우드는 CSP 보안서비스를 활용하여 온프레미스에서 보안관제를 수행





프라이빗 환경에서는 클라우드 가시성을 충분히 확보하는 온프레미스 보안관제 형태를 유지





▲ 프라이빗 클라우드 보안관제

프라이빗 클라우드 보안이슈 <Fortinet, 프라이빗 클라우드 보안>

프라이빗 클라우드는 조직의 보안 및 규정 준수의 성취에도 불구, 4가지 자체 보안이슈 존재

1. 퍼블릭 클라우드 제공업체와의 공동 책임 모델과 달리 보안에 대한 전적인 책임이 있음
   Full responsibility for security, unlike the shared responsibility model with public cloud providers
2. 보안 침해는 대중의 인식과 달리 퍼블릭 클라우드보다 프라이빗 클라우드에서 더 일반적임
   Security breaches are more common with private clouds than public ones, contrary to popular perception
3. 프라이빗 클라우드와 퍼블릭 클라우드 간에 워크로드를 이동하면 구성 오류 및 기타 보안 문제의 위험이 높아짐
   Shifting workloads between private clouds and public ones increase the risk of configuration errors and other security issues
4. 네트워크 안의 트래픽에 대한 동서 가시성 부족함
   A lack of east-west visibility, that is, into traffic within the network

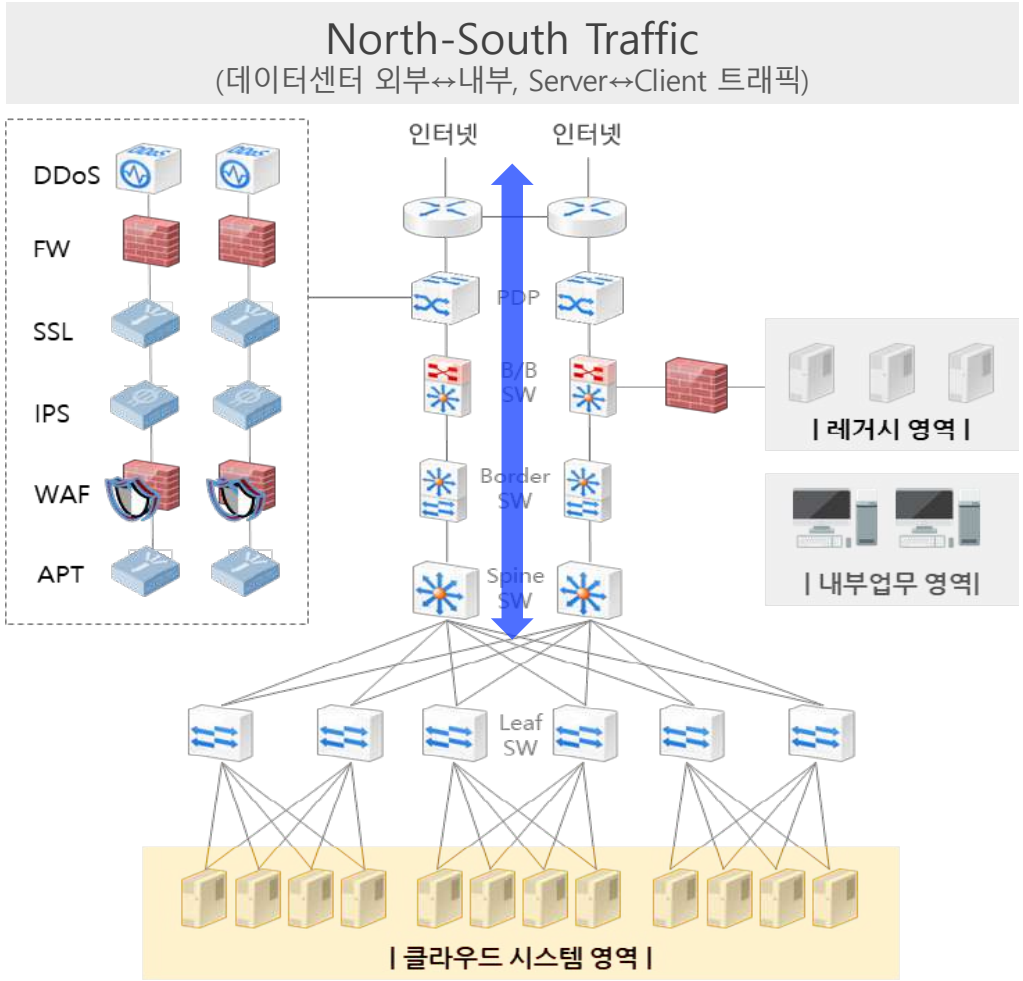
IGLOO

클라우드 환경의 보안관제 운영 방안

볼 수 없다면 대응할 수 없다

SECURITY & INTELLIGENCE

외부↔내부 종단간 트래픽은 기존 모니터링 및 대응체계로 대응



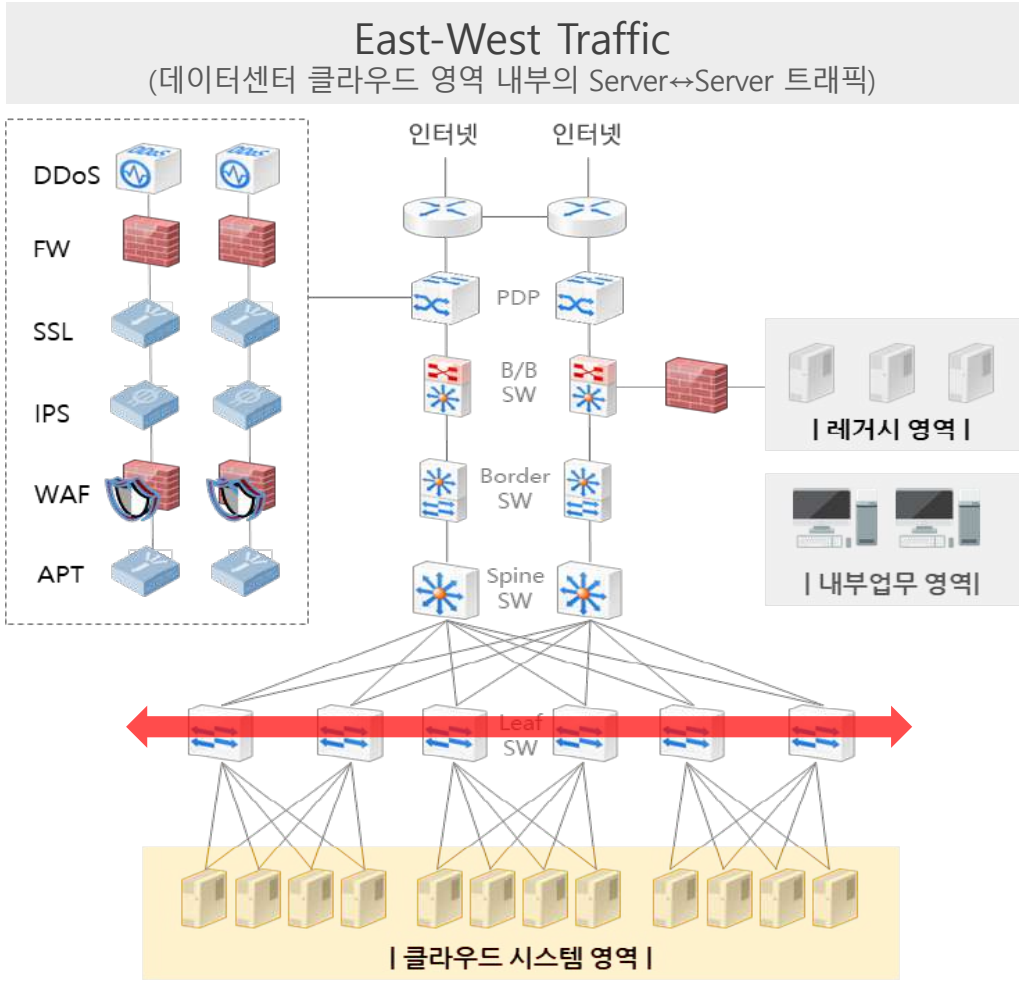
"North-South" 트래픽은

① (의미) 데이터센터와 클라이언트, 네트워크상의 데이터센터 외부와
통신되는 트래픽을 말함

② (보안) FW, IPS, Anti-DDoS 등 전통적인 네트워크 보안장비를 통해
위협행위(공격트래픽)를 대응함

보안 장비	설 명
DDoS 대응시스템	DDoS공격을 차단 (국정자원 사이버대피소 가능)
침입차단시스템(FW)	인가된 서비스外 모든 트래픽 차단
침입방지시스템(IPS)	시그니처와 룰을 기반으로 유해트래픽 차단
악성코드탐지시스템(APT)	알려지지 않은 지능화된 악성코드 탐지
웹방화벽(WAF)	웹해킹 공격트래픽 차단
홈페이지 위변조 탐지	홈페이지 위·변조 공격을 탐지 (웹쉘차단)
스팸/바이러스차단시스템	악의적 해킹 메일의 유입을 차단
유해사이트 차단시스템	악성코드 배포/경유, C2C 접근을 차단
서버보안,서버/DB 접근통제	SecureOS, 서버/DB 비인가 접근을 차단

클라우드 영역내 위협 모니터링 및 대응을 위한 전용솔루션 필요



"East-West" 트래픽은

① (의미) 데이터센터 내부에서 발생되는 트래픽으로서 보안장비를 거치지

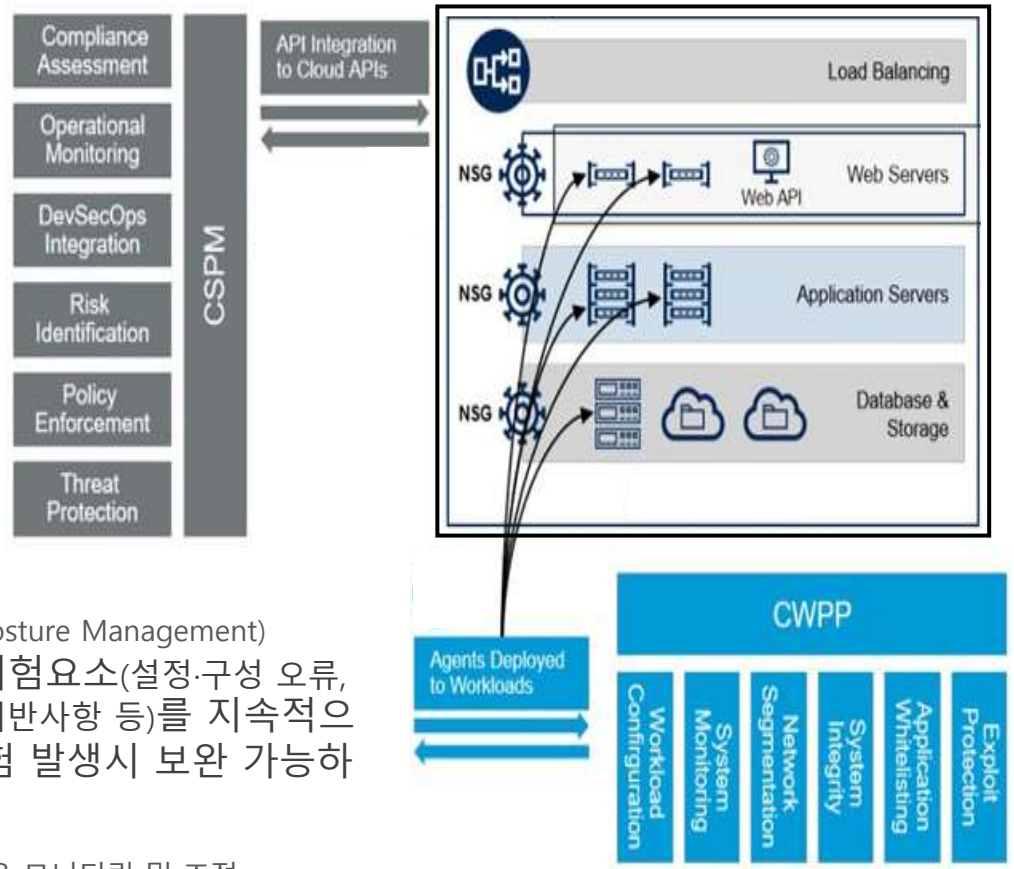
않는 서버와 서버 또는 VM과 VM간의 트래픽을 말함

② (보안) 전통적인 종단간 네트워크 보안장비로는 측면이동을 통한 위협

행위 또는 침해여부 모니터링이 불가능하기에, 네트워크 가시성 및

어플리케이션 무결성	확보, 보안감사 등을 통해 대응함
클라우드 네트워크 가시성 (Network Visibility)	클라우드 환경에서 전체 트래픽을 수집/분석, 보안위협을 식별
클라우드 워크로드 보호 (Cloud Workload Protection)	워크로드의 침해시도를 탐지하고 방어
클라우드 보안형상 관리 (Cloud Security Posture Mgt)	인프라 구성변경 및 보안정책 위반 등의 위험요소를 예방, 탐지 및 대응

클라우드 환경의 보안형상 및 워크로드 이상행위 모니터링



▲ CSPM, CWPP의 배치 및 기능적 요소 - 출처 : 가트너

CSPM (Cloud Security Posture Management)
클라우드 인프라의 위험요소(설정·구성 오류, 사용자 실수, 규제준수 위반사항 등)를 지속적으로 모니터링하여, 위험 발생시 보완 가능하도록 제시

① 서비스 구성의 보안설정을 모니터링 및 조정
위험신뢰도, 계정설정 및 암호화 등을 모니터링하여 규정 위반과
과도한 위험일 경우 자동 조정 조치

② 클라우드 운영환경 전반의 위험 가시성 제공
보안 취약점을 탐색하고 설정오류나 정책충돌 등을 방지

CWPP (Cloud Workload Protection Platform)
워크로드 보안과 취약성평가, 구성검사를 지속적으로 적용하여 침해시도를 탐지(Detect)하고 방어

① 보안 강화 및 설정/취약점 관리
워크로드 운영에 불필요한 컴포넌트 삭제, 운영 기준에 맞춰 시스템이
구성돼 있는지 검사

② ID기반 세그멘테이션과 네트워크 가시성
워크로드별 세분화된 방화벽을 구축하고 가시성을 확보, 방화벽 솔루션
자체 또는 클라우드 보안그룹 등 활용

③ 시스템 무결성 보장
VM 및 컨테이너 이미지가 마운트 되기전에 무결성을 확인하거나,
워크로드가 부팅/구동된 상태에서 시스템 파일이나 구성에 대한 무결성
을 실시간 모니터링

④ 애플리케이션 제어
제로트러스트 관점에서 화이트리스트 기반으로 애플리케이션 실행 제어

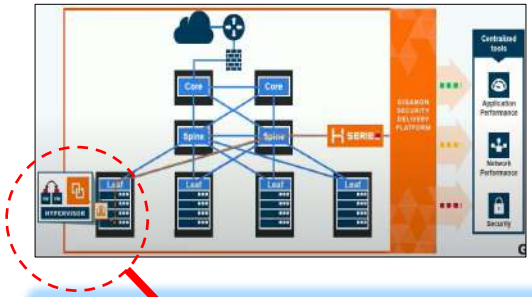
⑤ 익스플로잇 예방 및 메모리 보호
OS 및 실행이 가능한 애플리케이션의 취약점에 대응

⑥ 서버 워크로드 EDR, 행위 모니터링 및 위협 탐지/대응
네트워크 통신, 프로세스 시작 등을 모니터링해 의심 행위를 탐지/대응

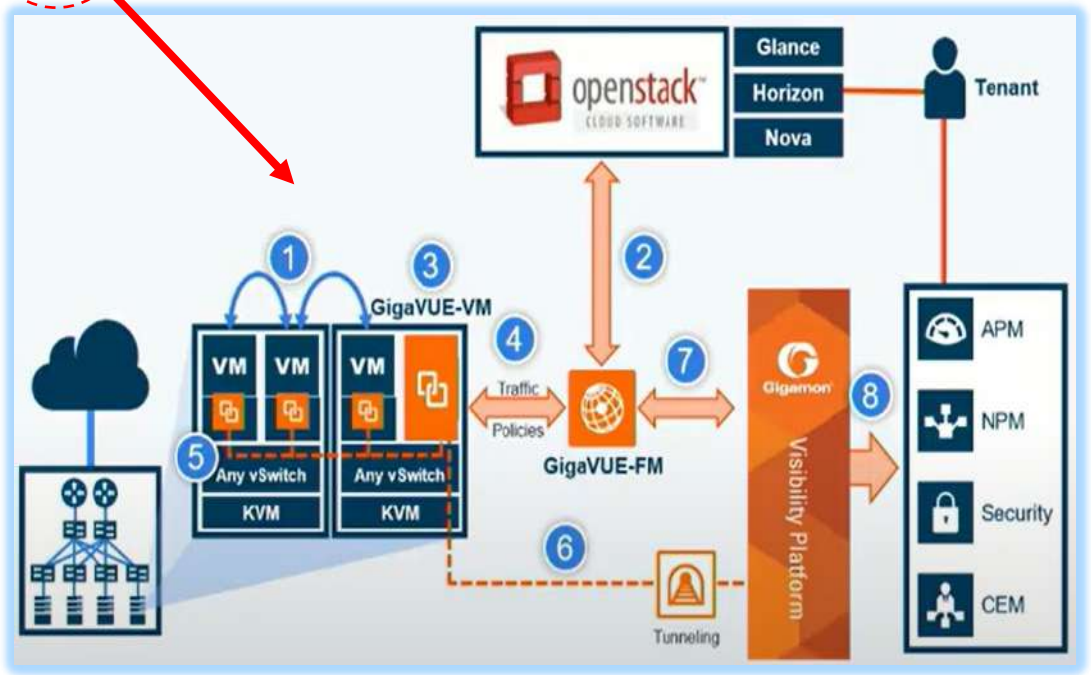
⑦ 호스트 기반 침입 방지 시스템
유입되는 네트워크 트래픽을 분석해 공격을 탐지/차단

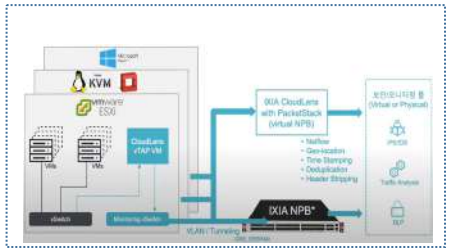
⑧ 안티 멀웨어
시그니처 기반으로 멀웨어를 탐지/차단

전용에이전트로 VM, 컨테이너 내부 트래픽을 수집, 분석용 보안툴로 전달하는 방식으로 구현

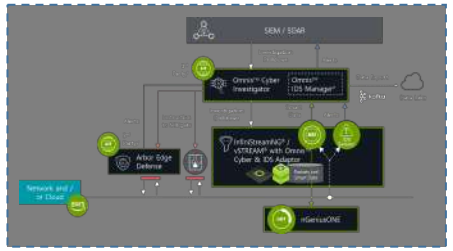


▼ 기가몬社 Gigamon Hwak 예시





▲ 키사이트社 CloudLens



▲ 넷스카웃社 nGeniusONE

① OpenStack
Horizone/Nova가 G-vTAP(Gigamon Virtual Taps)과 함께 패키지된 테넌트 VM을 설치

② GigaVUE-FM
OpenStack/Nova 컨트롤러에서 테넌트 VM을 검색

③ GigaVUE-FM
GigaVUE-VM(Virtual Visibility Node) 설치

④ GigaVUE-FM
G-vTAPs에 트래픽 정책 설정

⑤ G-vTAPs : GiagVUE-VM으로 트래픽 필터 및 복제

⑥ GigaVUE-VM
가시성 플랫폼으로 트래픽을 전송하기 전에 추가적인 필터링 및 슬라이싱

⑦ GigaVUE-FM
트래픽 전송전에 트래픽 정책 설정

⑧ Visibility Platform : 트래픽 최적화 및 보안툴 전달

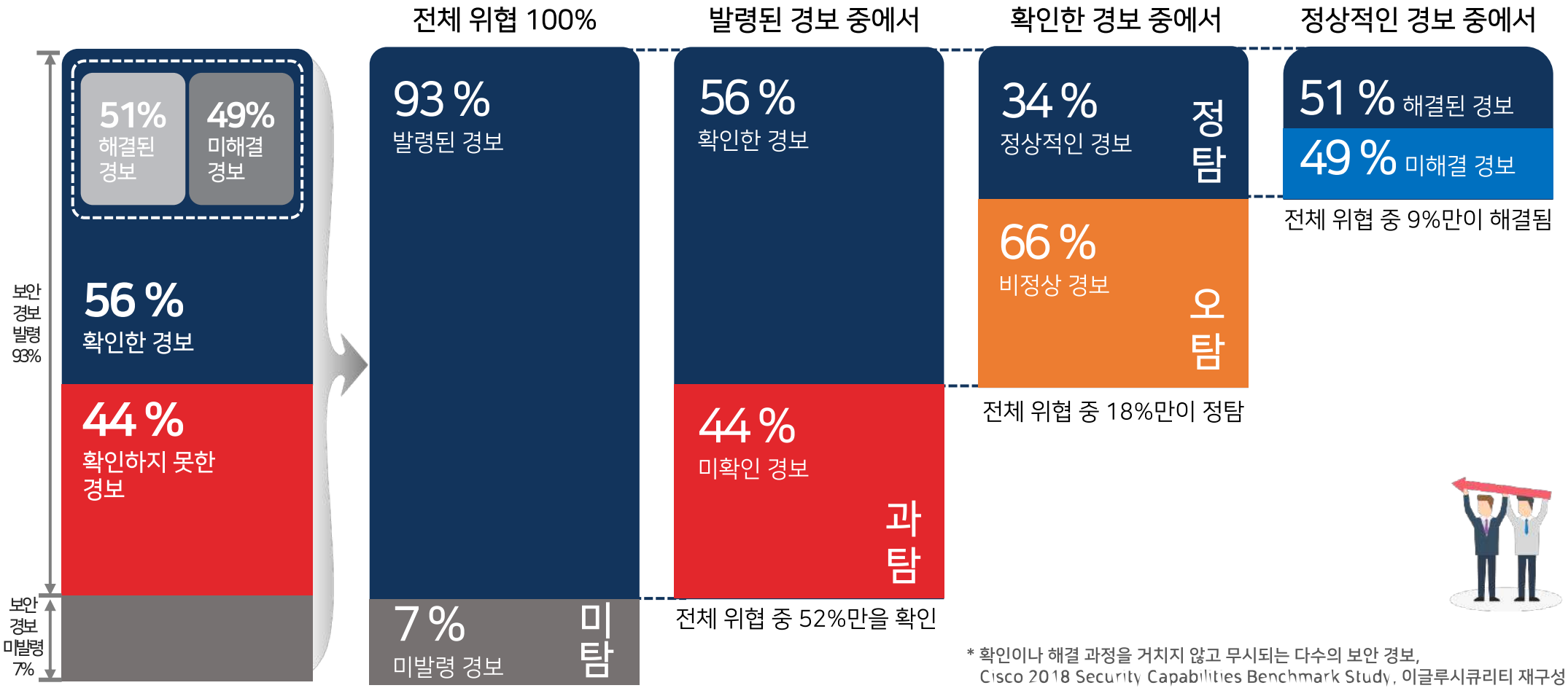
IGLOO

클라우드 환경의 보안관제 운영 방안

프라이빗 클라우드의 보안관제 운영

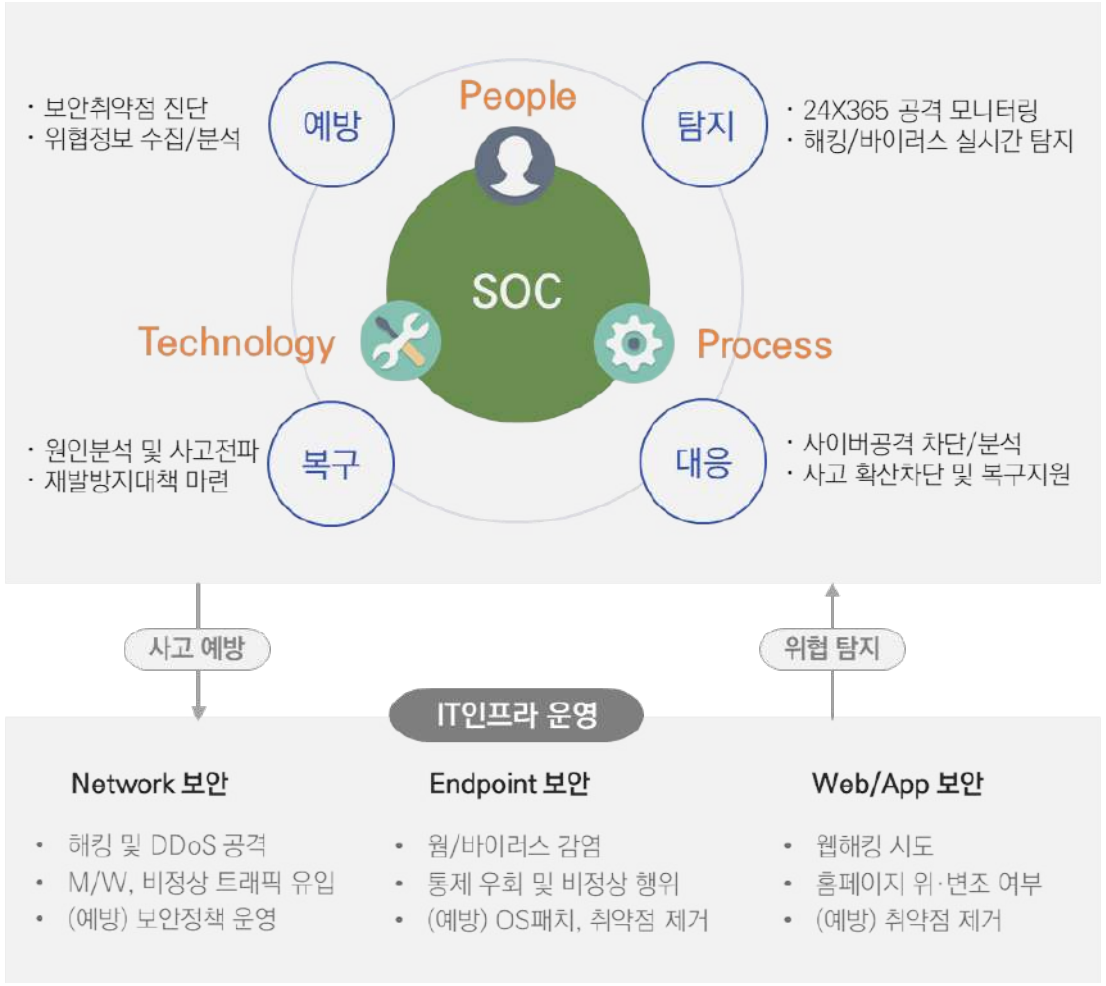
SECURITY &
INTELLIGENCE

끊임없이 발생하는 보안경보는 SOC 한계를 이미 넘어섰습니다



* 확인이나 해결 과정을 거치지 않고 무시되는 다수의 보안 경보,
Cisco 2018 Security Capabilities Benchmark Study, 이글루시큐리티 재구성

보안관제센터(SOC)는 신뢰할 수 있는 효과적이고 지속 가능한 운영방안이 필요합니다



- 최신 보안위협들에 대한 인지 및 분석 역량
- 위협 기반의 의사결정 및 효과적인 대응
- 오탐을 줄이고 실질적 위협들에 대한 빠른 대응
- 사각지대 최소화를 위한 효율적 자원의 배치

보안관제의 가시성 확보 및 대응 자동화를 통한 지능형 보안관제체계 구축

보안관제센터는 24시간 365일 네트워크·서비스 대상의 사이버공격을 모니터링 하여 **침해시도 신속히 대응할 수 있는 관리체계를 구축**

통합 관제

(보안관제영역) 보안관제, 침해대응, 보안진단, 위협분석, 보안운영 등 분야별 전담팀 운영으로 **보안관제센터 운영체계를 확립**

자동 대응

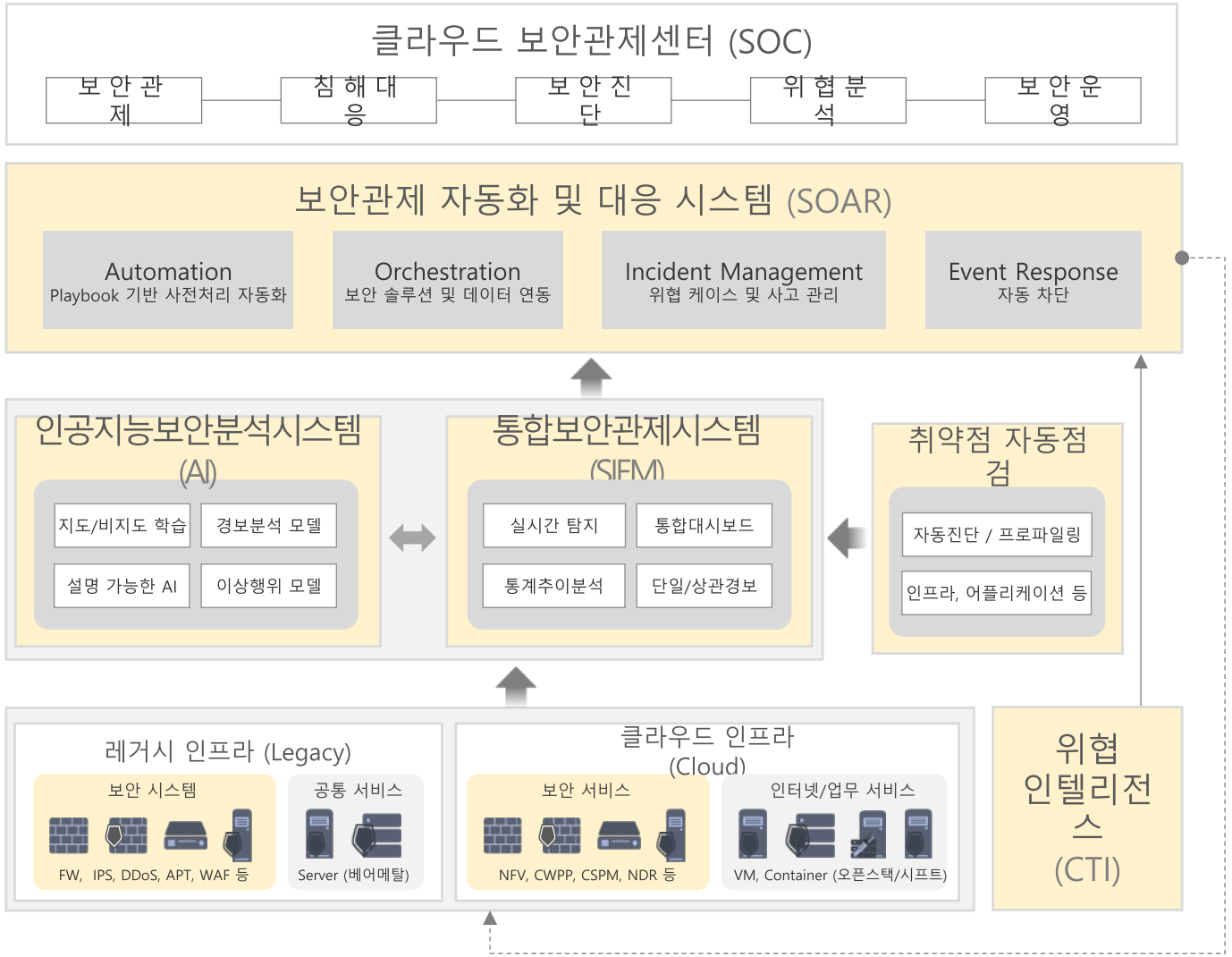
(자동대응영역) SOAR를 통해 경보이벤트의 보안장비 차단, 대응결과 이력관리 등 **단순·반복적인 대응업무를 자동화**

분석 수집

(수집분석영역) 빅데이터 수집 및 상관분석, 인공지능 분석을 통해 대량의 보안로그·이벤트에서 **유의미한 인사이트(경보이벤트)를 추출**

(운영탐지영역) 클라우드 운영환경의 가시성 확보 및 보안성 강화를 위한 전용솔루션 도입을 통해 **클라우드 보안역량을 확대**

탐지 운영



보안관제센터(SOC) 운영모델의 체계적인 관리 및 지속적인 개선

Strategy & Planning (전략수립)

Architecture & Design (아키텍처)

Build & Operating (구축/운영)

Assesment & Improve (평가/개선)

식별 (Identify)	예방 (Protect)	탐지 (Detect)	대응 (Respond)	복구 (Recover)	관리 (Management)
ID.AM 자산관리	PR.VA 취약점 진단	DE.EC 보안이벤트 수집	RS.IA 침해사고 분석	RC.RP 복구계획	MG.SL 서비스 수준관리
자산 목록화	진단대상 목록화	관제대상 이벤트 및 로그 수집	접수 및 위험도 분석	분야별 복구계획 수립	평가지표 개발
자산 R&R 가치평가	취약점 도출 및 대응방안 마련	위험도 산정 및 경보설정	자체 분석 / CERT 지원	지속적인 관리 및 개선	미흡/개선사항 도출
ID.BE 비즈니스환경분석	PR.DT 모의침투/인식훈련	DE.DA 탐지 및 분석	RS.IP 침해사고 대응	RC.IM 개선	MG.PP 지침/절차 개정
외부연계 목록화	DDoS 대응 훈련	보안 이벤트 모니터링	IP 차단 및 격리	개선사항 통합	보안관제 운영지침/절차 개정
비즈니스 영향분석	악성메일 모의훈련	상세분석 및 초동대응	과거 이벤트 분석	복구전략 업데이트	매뉴얼/가이드 개정
ID.GV 법적요건	PR.SH 보안시스템 최적화	DE.RA 대응 및 조치	RS.CO 상황전파	RC.CO 커뮤니케이션	MG.WS 근무체계관리
관련 법/규정 이해와 관리	보안시스템 정책점검	상황전파 및 추가대응	보고/비상상황 전파	비상연락망 현행화	인력구성/관리/정보보호교육
보안정책 확립	이슈사항 도출 및 정책최적화	보고 및 종결	위협공유	단계별 보고체계 점검	근무체계 도출/개선 및 적용
ID.RA 위험식별 및 관리	PR.PP 대응체계 수립	DE.PH 탐지프로세스 관리	RS.MI 확대방지		MG.SE 평가
내·외부 위협 식별	분야별 대응체계 수립	탐지프로세스 관리	침입경로 및 취약점 상세분석		평가항목 도출
문서화 및 위험허용 관리	대응체계 점검 및 개발	탐지정책 최적화	프로파일링 (공격기법 및 위협)		미흡/개선사항 도출
ID.SO 보안관제체계	PR.IS 정보공유		RS.IM 개선		MG.CE 인증
관제범위/대상 파악	글로벌 위협수집		침해사고 프로세스 검토		정보보호관리체계 인증
문서화 및 위험허용 관리	정보공유체계 수립		개선사항 업데이트		지속적인 관리 및 개선
					MG.SP SOC보호 및 시스템 운영
					정보시스템 접근제어/보안관리
					데이터 보호/물리적 보안

범례: 기능(Function) / 세부활동(Category) / 통상적 보안관제 범위

* NIST Cyber Security Framework 등 다양한 정보보호관리체계를 접목하여,
보안관제센터 업무정의 및 수준평가에 활용 가능한 IGLOO SOC Framework

IGLOO

THANK YOU

경청해주셔서 감사합니다

SECURITY &
INTELLIGENCE