하이브리드 멀티 클라우드 여정을 위한 보안 운영 전략

나병준 실장/전문위원
한국IBM 보안 사업부

Run anywhere | Gain security insights | Take action faster

IBM Security

IBM

가속화되고 있는 디지털 혁신

애플리케이션

모듈화, 컨테이너화

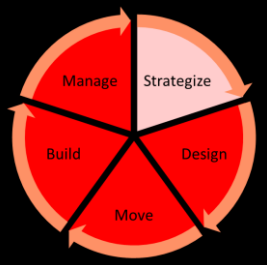
데이터

고급 분석 및 AI를 위한 공유 리소스

인프라스트럭처

하이브리드 멀티 클라우드 환경에 분산됨

한국 기업들 사이에 클라우드가 확산되고 있으며, 2023년에는 기업당 9개 이상 사용할 것으로 예상



현재

7

개의 클라우드를 한국 기업에서 사용 중(평균)

3년 후

9

개의 클라우드를 한국 기업에서 사용할 것으로 예상(평균)

출처: 2020년 IBM 기업가치 연구소 하이브리드 멀티클라우드 설문 조사(한국, n=140)
Q3. 귀사에서는 몇 개의 클라우드를 사용하십니까? 현재, 3년 후.

기존의 보안 방법이 디지털 혁신을 따라가기 힘든 이유

너무 많은 업무

- Meet with CIO and stakeholders
- Nail down third-party risk
- Manage GDPR program with privacy office
- Respond to questions from state auditors
- Update CEO for board meeting
- Update budget projections
- Write security language for vendor's contract
- Make progress on the never-ending identity project
- Review and updated project list
- Edit communication calendar
- Update risk rankings on security roadmap
- Clarify policies governing external storage devices
- Provide testing and encryption tool direction
- Provide data handling best practices
- Help with new acquisition
- Meet with senior project manager
- Send new best practices to development teams
- Review logs for fraud ongoing investigation
- Help with insider threat discovery
- Determine location of sensitive data in the cloud
- Investigate possible infection on legacy system
- Continue pen testing of new business mobile app
- Help architects understand zero-trust
- Answer security policy emails
- Format security status report for executives
- Meet with recruiter to discuss staffing
- Write test plan requirements for new products
- Meet regarding improving security of facilities

너무 많은 공급 업체

너무 심한 복잡성

너무 많은 경고

보안에 대한 현대화된, 개방형의 통합 접근 방식이 필요

고객의 보안 과제

- 클라우드 보안
- 지능형 위협
- 규정 준수와 개인정보보호
- 스킬 부족
- 모바일, 엣지, IoT/OT

IBM 솔루션

IBM **Security**

Align
비즈니스를 위한 보안 전략

Protect
디지털 사용자, 자산 및 데이터

Manage
증가하는 위협에 대한 방어

Modernize
개방형, 멀티 클라우드 플랫폼으로의 보안

IBM 차별화 포인트

- 깊은 전문성
- 개방형 플랫폼
- AI 기반 기술
- 가장 큰 생태계

보안 운영에서 필요한 사항

보안 분석 효율 향상

분석을 위한 모든 데이터 연계 구성

위협 관리 프로세스 및 추가 분석 환경 구성

반복적이고 오랜 작업 자동화

- ✓ 빠른 위협 탐지, 지속적인 위협 조사와 빠른 대응을 통한 위험 완화
- ✓ 구현된 분석 프로세스 및 보고방안을 통해 지속적인 보안 모니터링 강화
- ✓ 보안 운영 팀의 기술, 효율 및 팀 분위기 향상

IBM SOC 고도화 방안

차세대 보안 운영의 5가지 핵심사항

I
인공 지능을 활용한 Advanced 위협 분석 환경 구성

II
대응 자동화 및 워크플로우

III
산업 별/국가별 위협 정보를 활용한 대응

IV
빠른 대응을 위한 시스템 연계 및 판단 제공

V
Use Case 라이브러리를 통한 분석 방안 활용

클라우드 SOC 운영

Run anywhere | Gain security insights | Take action faster

Cloud 보안 트랜드

	클라우드 전환	자원 및 기술	관련 보안 솔루션	데이터의 폭발적 증가
경향	클라우드 업체들은 자체 보안 강화를 위한 솔루션을 제공하여 가시성 확보 및 위협 분석을 위한 방안 제공	새로운 보안 운영 방안 및 다양한 분석 방안의 증가로 인해 SOC의 업무 부담 가중	보안 솔루션 업체는 클라우드 보안을 위한 솔루션을 상호 운용 가능한 아키텍처와 활용가능한 UI를 제공	데이터 양이 기하 급수적으로 증가하여 그 안에 규정 위반으로 발생한 위험을 발견하기 어려움
운영 관점	운영 관점에서 고객은 보다 쉽게 클라우드 데이터와 자산을 보호 할 수 있는 방안을 기반으로 보안 운영 안을 평가	완벽한 탐지, 조사 및 대응을 위해 시스템을 통합하고 워크플로우를 간호화하길 원함. MSSP 서비스 활용이 증가	분산 운영 솔루션들 보다는 통합하여 운영하기 쉽고 상호 운용성이 보장되는 솔루션을 기반으로 SOC 운영을 목표	보안 데이터 레이크를 구성하여 데이터를 저장하고 저장된 데이터를 기반으로 위협을 탐지하고 추가 분석 및 컴플라이언스 요건까지 해결
SOC 운영의 어려움	클라우드 환경으로의 변호는 보안 관제 시스템의 변화를 가져오고 있고 SOC에서는 단일화해서 운영 할 수 방안을 찾고 있음	보안 관제 시장에서는 사고 관리 및 대응을 위해 SOAR을 접목하고 있으며, MSSP에서도 운영이 가능하도록 구성 지원	SOC의 원활한 운영을 위해서 더 많은 Cloud 및 On-Prem을 통합할 수 있는 플랫폼과 경험을 요구	여러 보안 업체들이 UEBA, EDR에서 데이터 저장과 조사가 가능한 방향으로 진화

다양한 클라우드 기업과 기술

IBM, amazon web services, LogRhythm, McAfee, FORTINET, paloalto NETWORKS, Symantec, splunk>, Microsoft, exabeam, Google, SECURONIX, DEMISTO A PALO ALTO NETWORKS COMPANY, FireEye

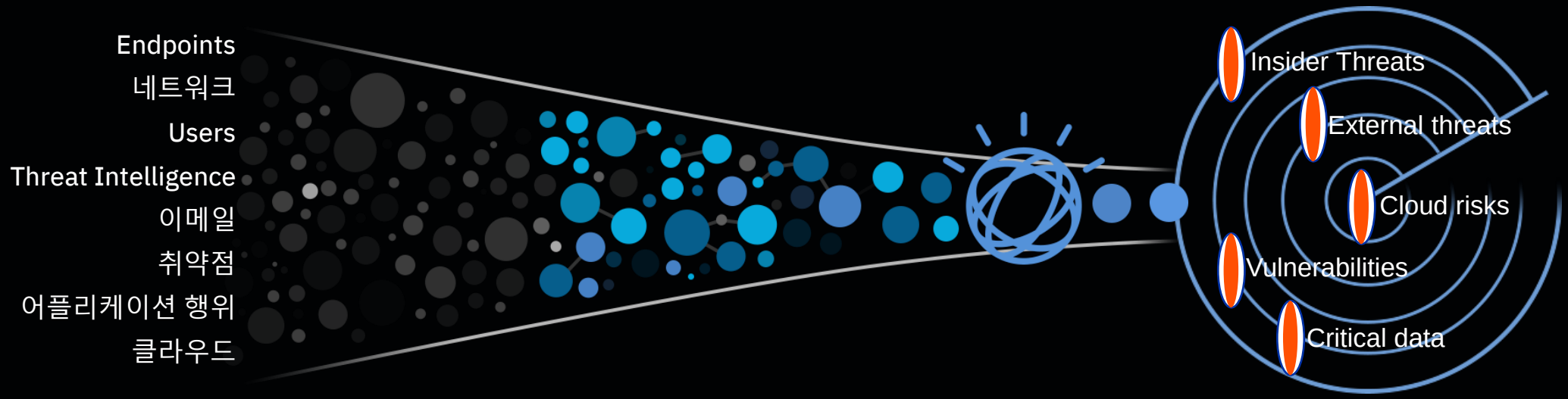
클라우드 SOC 운영을 위한 4가지 측면

가시성

탐지

조사

대응



수천억건의 이벤트

최신 위협 탐지

경보 우선 순위 및 원인 조사

보안위협을 빠르게 대응

멀티 클라우드 보안 전략

IBM Cloud 보안 전략

1. **클라우드 서비스 활용 내역과 위협 확인**
   기업 전체의 클라우드 자산을 정확히 확인(대외 서비스, 사내 운영시스템)

2. **기업용 SaaS 시스템 보호**
   O365, Salesforce 등 클라우드 어플리케이션에 대한 보안 방안 확보

3. **IaaS 와 PaaS 서비스 보호**
   클라우드 인프라를 보호하고 위협을 실시간으로 분석환경 구성

4. **클라우드의 워크로드 보안강화**
   컨테이너 레벨의 어플리케이션들을 보안 모니터링 할 수 있는 방안 확보

aws
Azure
Google Cloud Platform
IBM Cloud
Red Hat OpenShift
Red Hat Enterprise Linux
StackRox
Twistlock
A PALO ALTO NETWORKS COMPANY
aqua
Sysdig

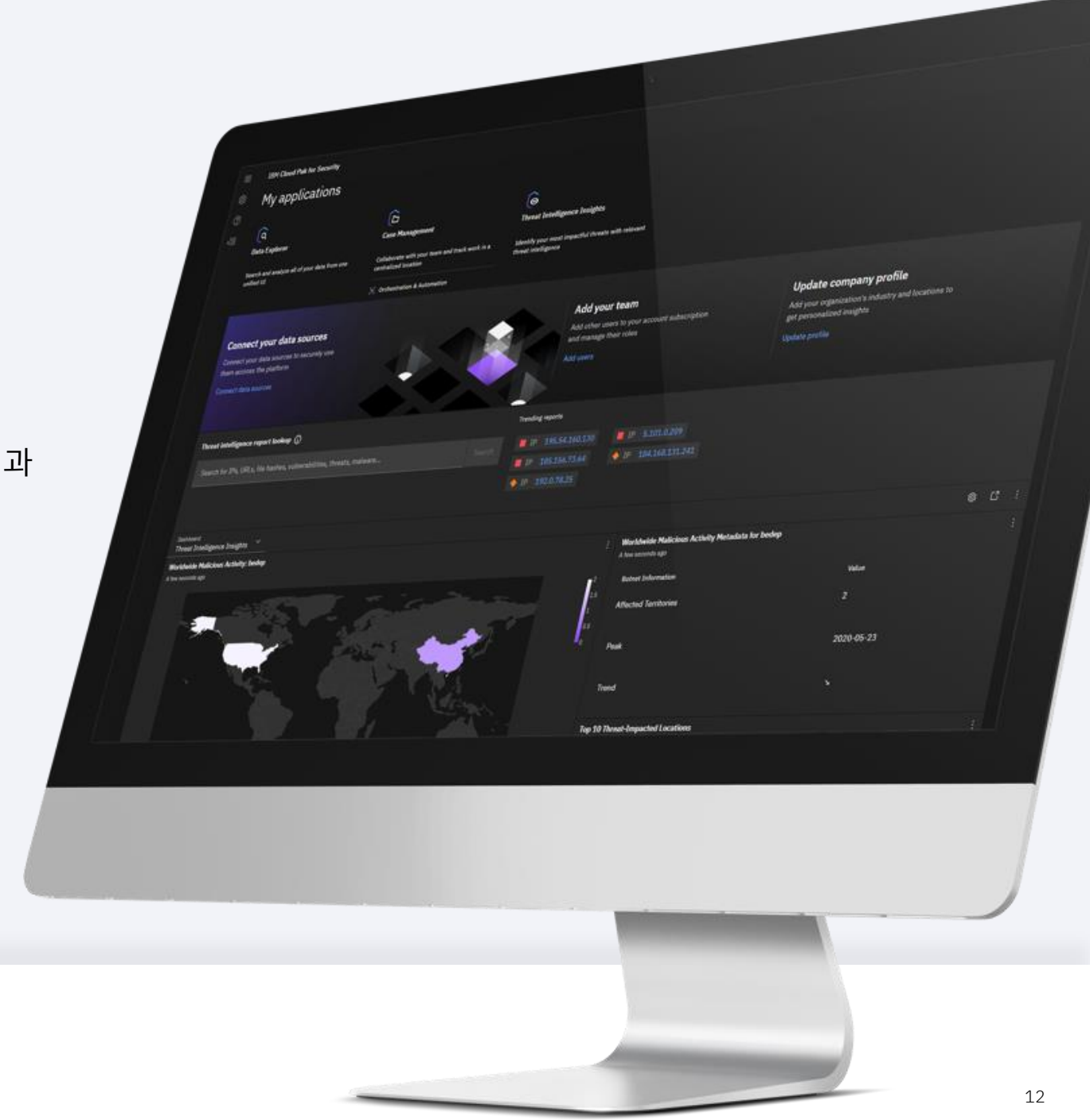
IBM Cloud Pak for Security

기존 보안 팀과 솔루션들을 보다 신속하게 통합하여 위협 및 위험에 대한 심층적인 통찰력을 생성하고, 대응조치를 조정하고, 대응을 자동화하면서, 반면에 데이터는 원위치에 그대로 두는 플랫폼입니다.

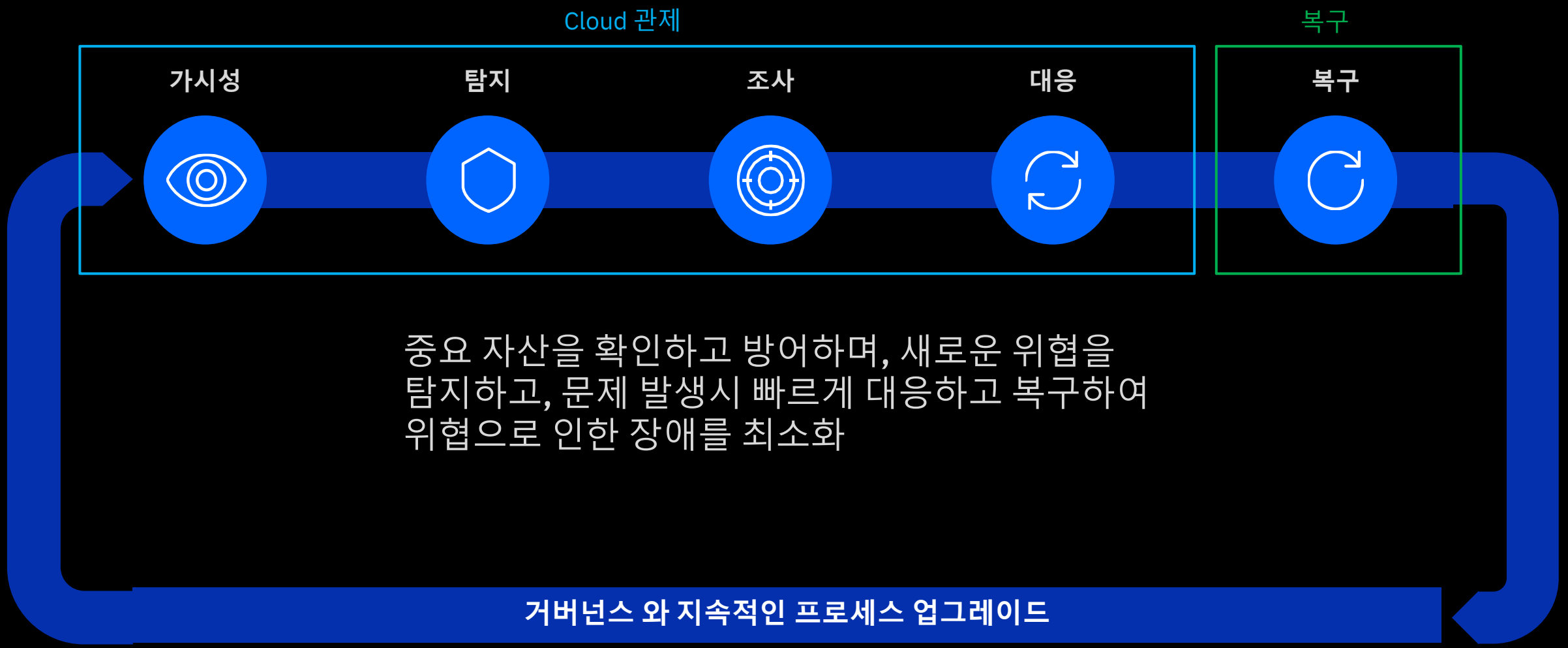
- 보안 통찰력을 확보
  IBM 및 타사의 보안 솔루션, 데이터 및 클라우드 전반에 대한 가시성과 분석을 제공하는 통합 콘솔 사용

- 더 빠른 조치
  AI 및 자동화를 통해 운영을 단순화하고 대응을 간소화하여 시간을 절약하고 위험을 낮춤

- 아키텍처 현대화(Modernization)
  유연성과 확장성을 제공하고 벤더 종속을 방지하는 개방형 멀티 클라우드 플랫폼으로 어디서나 실행 가능



IBM 클라우드 SOC 운영 프로세스



고객과 함께 가는 IBM Security

IBM Security는

100%
의 US 포춘 100대 기업을 고객사로 하고 있습니다.

95%
의 글로벌 포춘 500대 기업을 고객사로 하고 있습니다.

금융
50개 중 49개의 세계에서 가장 큰 금융 서비스 회사 및 은행이 고객입니다.

기술
15개 중 13개의 세계에서 가장 큰 기술 회사가 고객입니다.

헬스케어
15개중 14개의 세계에서 가장 큰 헬스케어 회사가 고객입니다.

통신
10개의 가장 큰 통신 회사가 고객입니다.

자동차
20개중 19개의 세계에서 가장 큰 자동차/부품 회사가 고객입니다.

항공사
10개 중 8개의 세계에서 가장 큰 항공사가 고객입니다.

IBM Security의 보안 사업 대상

14개의 분야에서 마켓 리더로 인정 받고 있습니다.

- SIEM
- Security Analytics
- Fraud Reduction Intelligence Platform
- Web Fraud Detection
- Identity Governance
- Access Management
- Identity as a Service
- Identity Management
- Risk-Based Authentication
- Data Security and Database Security
- Data Center Backup and Recovery
- Unified Endpoint Management
- Managed Security Services
- Cybersecurity Incident Response Services

고맙습니다

다음 사이트를 통해 IBM Security에 대한 소식을 듣고 도움을 받을 수 있습니다.

web.facebook.com/groups/725870507536094

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

@ibmsecurity

youtube.com/ibmsecurity