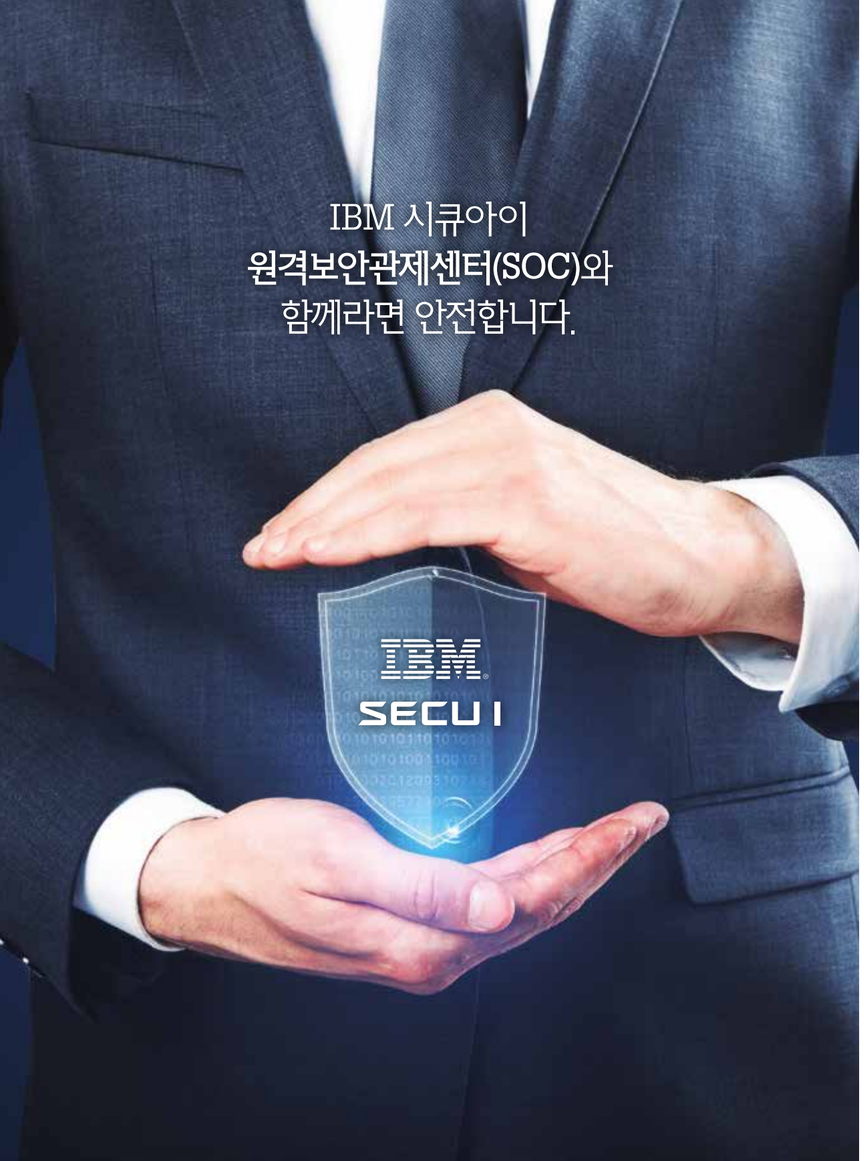





한국아이비엠주식회사
(07326) 서울시 영등포구 국제금융로10 서울국제금융센터
Three IFC

전화번호 : (02) 3781-7114
**www.ibm.com/kr**

2018년 8월

Printed in Korea



# IBM 시큐아이
# 원격보안관제서비스(SOC)

IBM은 글로벌하게 보안관제센터를 구축하고 운영해온 경험과 검증된 솔루션을 기반으로, 시큐아이가 보유한 국내 보안관제센터 운영 노하우를 접목하여 Watson 기반의 비용 효율적인 고객의 보안 요건에 최적화된 원격보안관제센터(SOC)를 공동으로 운영하고자 사업을 추진하게 되었습니다.

# IBM 시큐아이
# 원격보안관제센터(SOC) 설립 배경

## 보안 패러다임의 **변화**

보안 인텔리전스 → 인공지능 보안 + 클라우드 환경에서의 보안 서비스 가능


보안 패러다임의 변화에 따라, 인공지능 보안 시대의 시작, 모든 고객들이 클라우드로 인프라를 전환하면서 보다 철저하고 신속한 대응이 중요합니다. IBM은 글로벌 자산을 이용하여 원격관제를 통해 임팩트있게 새로운 패러다임을 이끌어 가고자 합니다.

IBM은 관제센터에 대한 **구축 경험 및 글로벌 솔루션**을 기반으로, 시큐아이의 국내 보안관제 운영 노하우를 접목하여 2018년 8월 17일, **IBM 보안사업부와 보안 전문기업 시큐아이와의 원격보안관제센터(SOC) 공동 운영 사업** 추진

*** 왜 원격보안관제서비스(SOC)가 필요한가?**

다양한 채널에서 들어오는 보안 위협에 대해 상시 대응 가능, 외부 동향을 쉽게 파악하여 전체적 시각에서 서비스를 제공하는 컨트롤 타워 역할이 필요



# 대상 고객 및 **기대효과**

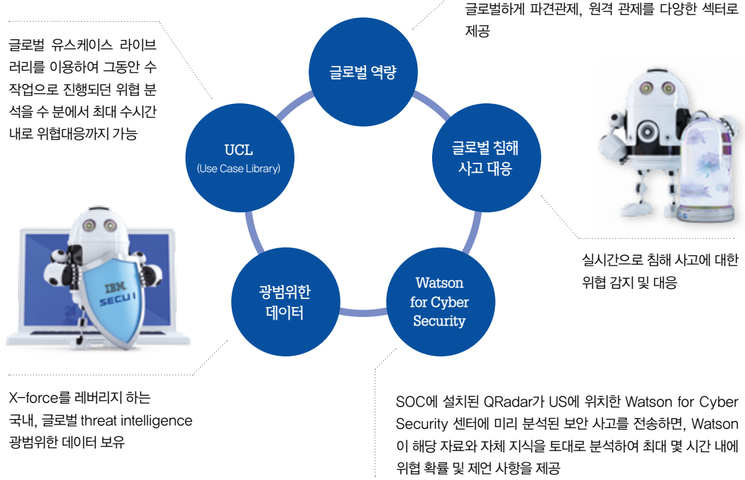
**어떠한 고객에게 원격보안관제(SOC)가 꼭 필요할까요?**

- 기업의 전사 보안을 운영 및 관리함에 있어서 효율적이고 효과적인 보안 역량을 필요로 하는 경우
- 보안 전문성 강화를 위해 보안 관제센터가 필요한 경우
- 외부 전문 보안인력을 통해 집중된 보안 운영이 필요한 경우

**원격보안관제(SOC)를 통해 기대할 수 있는 효과는?**

- 외부적인 보안 동향에 대해 쉽게 상시 파악 가능
- 기업의 보안 현황을 끊김없이 관리/통제 및 개선
- 보안 인텔리전스, 보안 통합, 리포팅 개선
- 시기적절한(신속한) 사건 대응 구현
- 숙련된 보안 관리 인력 및 경험으로 인력 부족 해소

# Why IBM 시큐아이 **원격보안관제센터(SOC)**인가?




글로벌 유스케이스 라이브러리를 이용하여 그동안 수작업으로 진행되던 위협 분석을 수 분에서 최대 수시간 내로 위협대응까지 가능

글로벌하게 파견관제, 원격 관제를 다양한 섹터로 제공



실시간으로 침해 사고에 대한 위협 감지 및 대응



X-force를 레버리지 하는 국내, 글로벌 threat intelligence 광범위한 데이터 보유

SOC에 설치된 QRadar가 US에 위치한 Watson for Cyber Security 센터에 미리 분석된 보안 사고를 전송하면, Watson이 해당 자료와 자체 지식을 토대로 분석하여 최대 몇 시간 내에 위협 확률 및 제언 사항을 제공



# **SOC** Service Type

SOC의 서비스 형태는 Standard, Enterprise, Premium으로 나뉘며 각 서비스 별 제공 서비스를 정의합니다.

| Service Type | Service Description |
|---|---|
| Standard SOC | • Monitoring<br>• 24x365 security monitoring |
| | • AI – based security intelligence and analytics<br>• Comprehensive threat intelligence database based on domestic and global intelligence |
| | • Monthly KPI / KRI reporting |
| Enterprise SOC | • Endpoint security deployment / File integrity monitoring for critical servers (initial trial) |
| | • Vulnerability Management |
| | • 시큐아이 IPS / IDS solution service (policy management and firewall traffic monitoring) |
| Premium SOC | • Penetration testing service |
| | • Weekly SLA reporting review |
| | • 시큐아이 DDOS solution service |
| | • Monthly global threat review |