



## 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 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 솔루션을 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 끊임없이 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?



# 원격보안관제 서비스 카탈로그

핵심 서비스	구축 서비스	리포팅 서비스	부가 서비스	인텔리전스 서비스
Threat Monitoring 24 x 7	Log Source Integration	Threat Intelligence Analysis – AI based	Executive Reporting	Global forensics Investigation
Threat Triage	Flow Source Integration	Security Intelligence Bulletins	Compliance Reporting (PCI / ISO27001)	Vulnerability Scanning
Threat Response	Use Case Design	Threat Hunting	Weekly KPI / KRI reporting	시큐아이 firewall management service
				시큐아이 DDOS service
				Penetration testing service



Premium (and all the services below)



Enterprise



Standard



# IBM 시큐아이 원격보안관제서비스(SOC)

## 지난 4년 연속 매니지드 보안 서비스 분야에서의 리더 자리매김

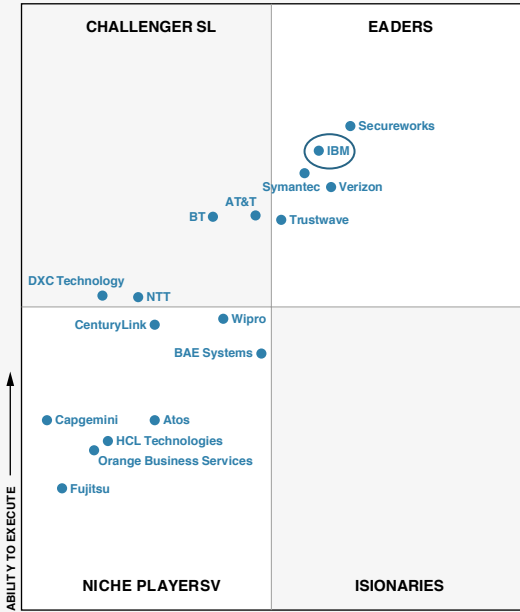
Watson 기반의 자동 채팅 기능과 보안관제서비스(SOC) 분석가 예약 시스템과 같은 새로운 기능을 탑재한 완벽한 기능의 포털. 이 포털은 QRadar 관리 콘솔을 활용하여 로그관리, 검색 및 보고 기능 제공

## SIEM(Security Intelligence Event Management)분야에서의 리더 자리매김

IBM SIEM(보안 인텔리전스 이벤트 관리)의 대표 오퍼링인 QRadar는 온 프레미스 및 IaaS의 하이브리드 모니터링 옵션을 포함하여 다양한 환경을 지원할 수 있는 유연한 아키텍처 제공

**Magic Quadrant for Managed Security Services(MSS), Worldwide - 2018**

Figure 1. Magic Quadrant for managed Security Services, Worldwide



COMPLETENESS OF VISION → As of December 2017 © Gartner, Inc  
Source: Gartner (February 2018)

**Magic Quadrant for SIEM - 2017**

Figure 1. Magic Quadrant for Security Information and Event Management



COMPLETENESS OF VISION → As of December 2017 © Gartner, Inc  
Source: Gartner (December 2017)



IBM 시큐아이  
원격보안관제센터(SOC)와  
함께라면 안전합니다.





© Copyright IBM Corporation 2018

한국아이비엠주식회사

(07326) 서울시 영등포구 국제금융로10 서울국제금융센터

Three IFC

전화번호 : (02) 3781-7114

[www.ibm.com/kr](http://www.ibm.com/kr)

2018년 8월

Printed in Korea

All Rights Reserved

IBM, IBM 로고, [ibm.com](http://ibm.com)은 미국 및/또는 다른 국가에서 IBM Corporation의 상표 또는 등록 상표입니다. 상기 및 기타 IBM 상표로 등록된 용어가 본 문서에 처음 나올 때 상표 기호(® 또는 ™)와 함께 표시되었을 경우, 이러한 기호는 본 문서가 출판된 시점에 IBM이 소유한 미국 등록 상표이거나 관습법에 의해 인정되는 상표임을 나타냅니다.

해당 상표는 미국 외의 다른 국가에서도 등록 상표이거나 관습법적인 상표일 수 있습니다. IBM의 최신 상표 목록은 [ibm.com/legal/copytrade.shtml](http://ibm.com/legal/copytrade.shtml) 웹 페이지의 "저작권 및 상표 정보" 부분에서 확인할 수 있습니다.

기타 다른 회사, 제품 및 서비스 이름은 다른 회사의 상표 또는 서비스 표시일 수 있습니다.

이 문서에는 IBM 제품과 서비스를 참조한 경우에도 IBM이 비즈니스를 수행하고 있는 모든 국가에서 해당 제품과 서비스를 제공함을 의미하는 것은 아닙니다.