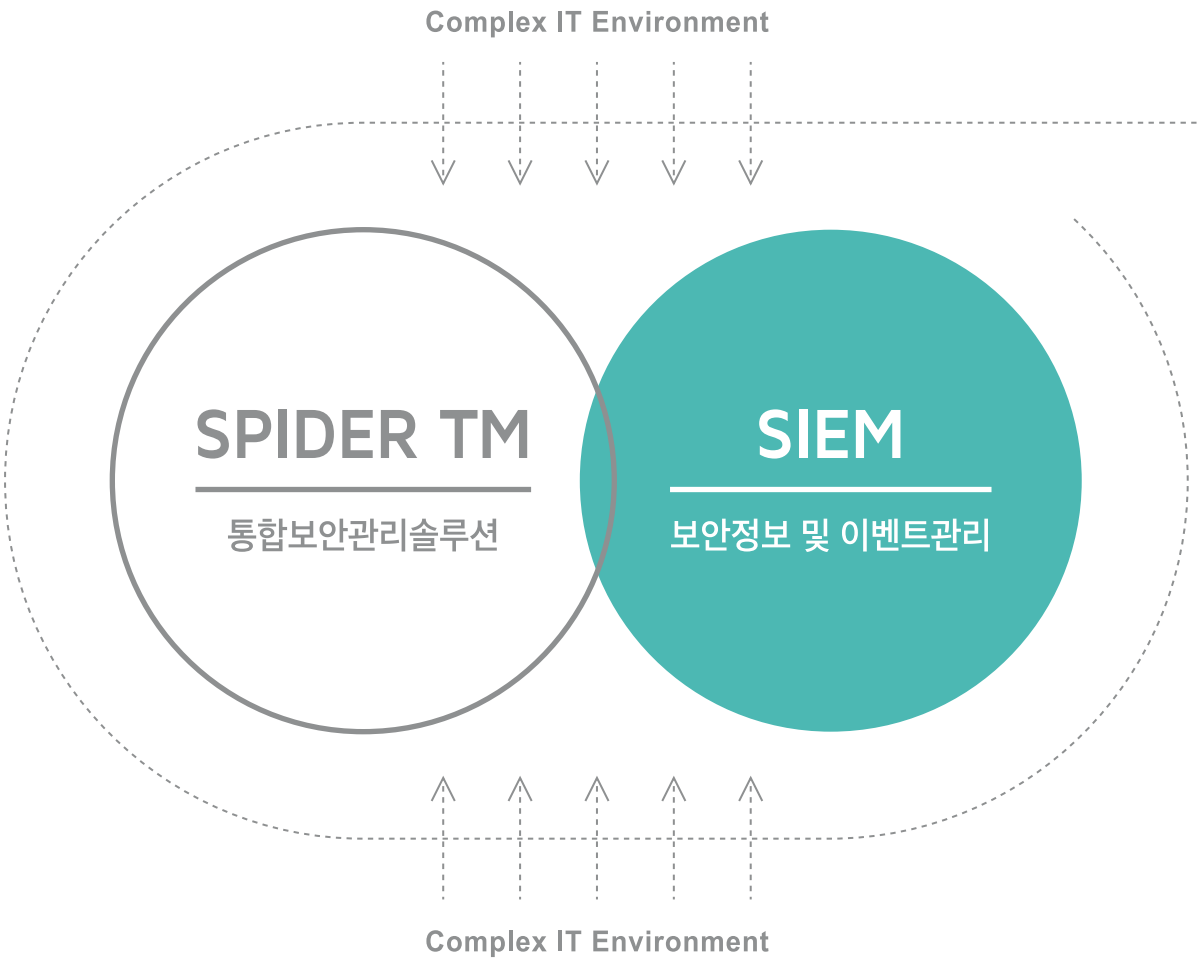
SPiDER TM

Security Information
& Event Management

# SPiDERTM

IGLOOSECURITY

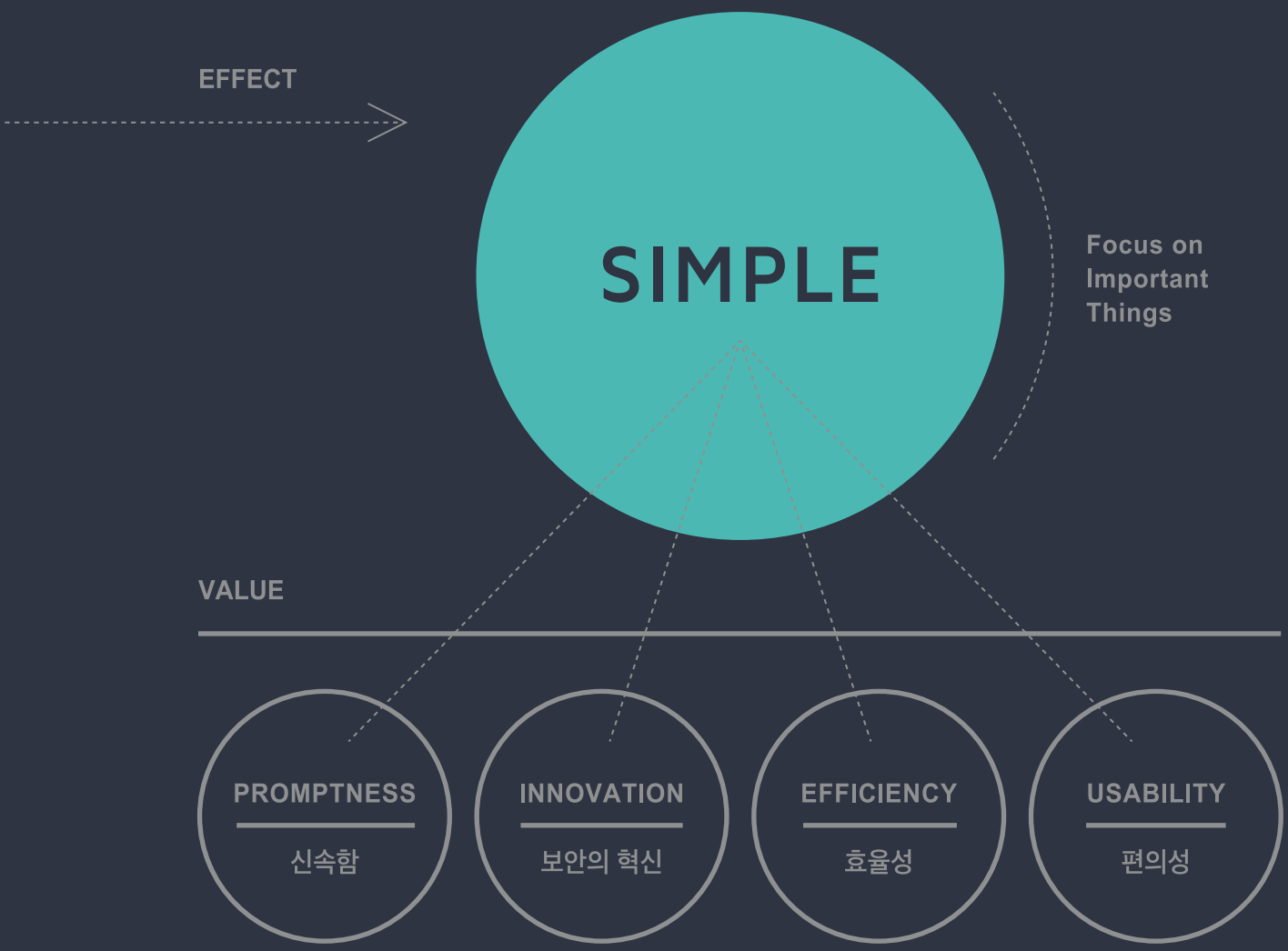
# 점점 더 **복잡해지는** [ **IT환경** ] 해답은 없을까?




## 다양한 보안 솔루션을 잘 활용한다는 것은 너무 어렵습니다.

지능적인 보안 위협, 방대한 IT 인프라, 수많은 보안 솔루션, 폭발적인 데이터 증가, 복잡한 컴플라이언스, 강화된 법 규제, 부족한 보안 전문가, 비용 증가...
IT 환경은 점점 더 복잡해 지고 있으며, 그 틈새를 파고드는 해커의 위협을 모두 다 막아내기 위해 기업들은 특정 기능을 제공하는 보안 솔루션을 하나 둘 추가로 도입하고 있습니다. 그리고 기업들은 깨닫게 됩니다. 과감한 투자로 수많은 보안 솔루션을 도입했지만, 도입한 보안 솔루션을 잘 활용한다는 것이 너무 어렵다는 사실을.

# [SIMPLE]에 그 답이 있습니다.




## 최대한 편안하게, 그러나 중요한 것은 놓치면 안됩니다.

사람들은 최대한 복잡하고 그럴 듯 하게 만들기 위해 중요한 것은 놓치고 있습니다. 최대한 간단하게 만드는 것, 그것을 통해 우리는 정말 중요한 문제에 집중할 수 있습니다. [SIMPLE]은 점점 더 복잡해는 정보보호 환경의 복잡성을 대폭 감소시킬 뿐만 아니라, 혁신, 신속함, 효율성 그리고 편의성이라는 놀라운 혜택들을 제공합니다.

# SIEM이 SIMPLE 해지는 방법

SPiDER TM은 SIEM이 'Simple' 해지기 위한 조건으로
Knowledge, Experience, Visibility를 제안합니다.

## ‘통합보안관리’와 ‘통합로그관리’의 최적화된 결합

SPiDER TM은 통합보안관제와 로그관리 및 분석 기능이 결합된 차세대 통합보안관리솔루션으로
1) 실시간 보안관제와 로그관리 및 대용량 로그 분석
2) 자체 보안관제센터의 관제 노하우 기반
3) 보안위협정보의 지속적인 업데이트 제공
4) 국내 최대 지원조직을 보유하고 있습니다.

## 최초 탐지부터 분석 대응까지 일원화된 보안관제 환경 제공

SPiDER TM은 다양한 이기종 로그를 수집하여 위협에 대한 실시간 탐지, 탐지된 이벤트에 대한 상세한 분석뿐만 아니라 해당 공격자의 IP와 K-CENTER와의 연계를 통한 위협 여부 판단, 침해 사고 처리 프로세스를 통한 사고 이력관리까지 보안관제 업무에 최적화된 기능을 제공합니다.

## 다차원 시나리오 분석을 통한 상관관계 분석 기능 제공

기존 ESM이 관제를 위해 단편적인 분석 기능만 제공했다면, SPiDER TM은 다차원 시나리오 분석을 수행해 APT 공격뿐만 아니라 내부정보유출 등 다양한 위협상황을 신속히 대처합니다. 또한, 침해 유형별 분석 규칙을 간단한 스크립트를 사용해 사용자가 직접 정의할 수 있고 실시간 또는 과거 데이터 분석 모니터링 기능을 바탕으로 새로운 공격패턴을 과거 데이터에 적용한 Time-Line 분석 기능을 제공합니다.

## BIG DATA를 처리할 수 있는 고속 파일 DB 사용

SPiDER TM은 대용량 로그를 효과적으로 처리하기 위해 고속 파일을 사용합니다. 이를 통해 수집 속도와 검색 속도가 대폭 향상되었습니다
또한, 로그수집 시 검색과 분석을 위한 실시간 인덱싱 기능을 제공하고, 실시간 압축 기능을 통해 디스크의 가용성을 보장합니다.

## 침해사고 처리 프로세스 기능을 통한 즉각적인 사고 대응 및 관리

침해사고 처리 프로세스 기능을 통해 침해사고에 즉각적인 대응 및 처리에 따른 불필요한 시간을 절약할 수 있도록 지원합니다. 이를 통해 정보보호 운영인력은 1) 자동화된 침해사고 처리 절차로 인해 효율적인 관제 업무를 수행합니다. 2) 사고에 대한 DB화 및 이력 관리를 통해 다양한 데이터 추출이 가능합니다.

## K-CENTER를 통한 위협정보 관리 체계 마련

보여주는 인텔리전스는 많이 있습니다. 하지만 실행 가능한 인텔리전스는 많지 않습니다. SPiDER TM과 연동되는 위협정보관리체계 K-CENTER는 위협관리 시스템에 서비스와 노하우가 결합된 위협관리정보체계로 API 방식과 파일 다운로드 기능을 이용하여 SPiDER TM에 위협정보를 제공합니다. 이러한 정보를 통해 정보보안인력은 최신 보안 동향 및 트렌드를 파악하고 자신의 사이트에 적합한 Rule을 만들 수 있습니다.

SPiDER TM은
클릭 몇 번으로 보안담당자가
원하는 정보를 제공합니다.

# SIMPLE

## 통합보안관리 시장점유율

# 18년간 1위


## 이글루시큐리티의 대표 솔루션 SPiDER TM

첫 출시 이후 지난 18년간 통합보안관리 시장점유율 1위를 지켜온 **SPiDER TM은 '보안'의 본질을 가장 잘 이해하는 이글루시큐리티의 대표 솔루션**입니다. 이글루시큐리티 통합보안관리솔루션 **SPiDER TM이 제공하는'Simple'의 혜택이 귀사가 안고 있는 보안 문제들**을 효과적으로 해결해 줄 것 입니다.

일본 정보보안 기업
SSK (서비스&시큐리티 주식회사)
카미야마(神山) 보안사업 이사

"SPiDER TM을  보안관제센터(SOC)의 통합보안관리솔루션으로 선정한 이유는 한국에서 충분한 검증을 거친 제품이며, 이글루시큐리티가 보안관제 서비스 분야에서 높은 경쟁력을 가지고 있기 때문이다.

SPiDER TM을  사용할수록 이 제품에 대해 감탄하게 되었다. 그 배경에는 무엇보다  제품의 높은 완성도와 뛰어난 성능 그리고 다른 제품이 제공해 주지 못하는 차별화 된 교육 프로그램이 있었다.

특히 SPiDER TM의 놀라운 편의성은 이글루시큐리티의 관제 노하우에 기반한 것으로 보안관제센터 운영에 최적화된  환경을 제공한다.  보안관제센터를 구축하는 모든 기업 및 기관에 SPiDER TM 도입을 적극 추천한다.

We Know Security

IGLOOSECURITY

서울특별시 송파구 정의로8길 7 한스빌딩 6층 TEL : 02-3452-8814 FAX : 02-3452-8815 www.igloosec.co.kr