



Do You Need A Better Defense Strategy?

SIEM 솔루션 업그레이드 전 고려해야 할 5가지 질문

Because DIY Security Isn't Good Enough

IT 보안팀은 조직을 사이버 공격으로부터 보호해야 하며 ISO 27001, PCI DSS 또는 GDPR과 같은 내부 및 규정준수 요구사항을 처리해야 합니다. 이는 많은 워크로드를 필요로 합니다. 기본 로그 관리 혹은 엑셀로 하나하나 관리를 하다 보면, 크리티컬한 사고를 발견하지 못하고 놓칠 수 있습니다.

공격은 점점 진화하고 규제환경이 지속적으로 변화하기 때문에, 기존의 기본 틀로만 이에 대응할 수는 없습니다. 이제 SIEM으로 업그레이드가 필요한 시점입니다. 이 문서를 통해 조직에 가장 적합한 솔루션을 결정하는 데 도움이 되는 5가지 핵심 질문을 살펴보시기 바랍니다.

SIEM(Security Information and Event Management) 솔루션은 자동 수집, 로그 분석 및 정규화 그 이상을 제공합니다. 고급 상관 관계 분석을 통해 위협을 자동으로 탐지하고 심각도를 평가하고 오탐을 필터링하여 중요한 이벤트에 대해 경고합니다. 내장된 자동화 및 인텔리전스 기능을 통해 조직을 보호하는 것과 동시에 대응 및 복구에 집중할 수 있습니다.



기업 보안팀에서는 평균
200,000개 보안 이벤트를
매일 마주합니다.

What is a Modern SIEM?

Advanced Analytics for Incident Identification

고도화된 데이터
수집/저장/분석기능
(Cloud/On-prem)

취약점 데이터 및
위협 인텔리전스
실시간 상관분석

자동 탐지 및
고위험 위협에 대한
우선순위화

사용자 행위 분석
및 이상행위 탐지

자산 및 서비스
사용자 프로파일링
자동화



보안사고 및 고위험 사용자에 대한 우선순위화

1

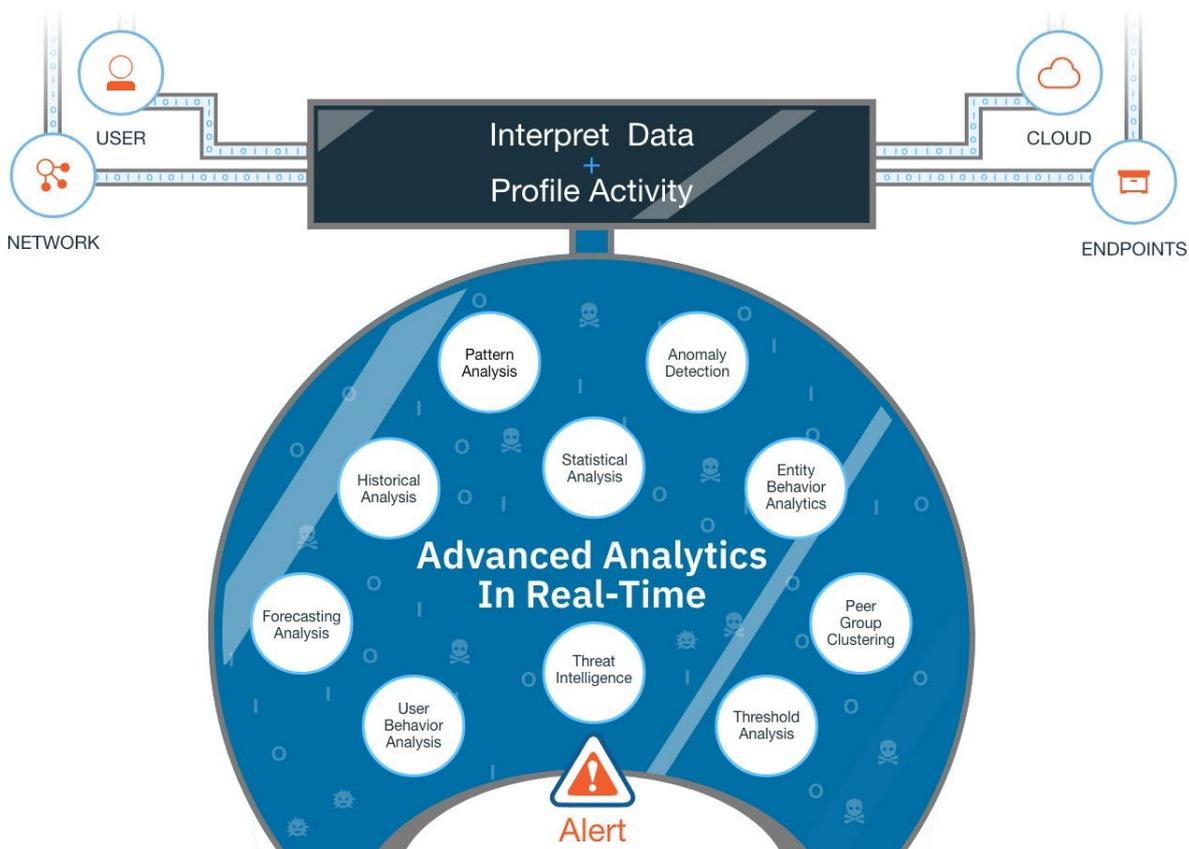
모든 보안 관련 데이터를 실시간으로 관리할 수 있는가

엑셀 시트를 사용하여 로그를 검색하고 관리하는 경우 실시간 변경 사항이 누락될 가능성이 높으며 최신화를 위해 상당한 시간과 노력을 들여야 합니다. 중앙 집중화된 최신 SIEM을 통해 로그 수집, 정규화 및 분석을 자동화할 수 있습니다. 더불어 로그 외에도 더 깊은 네트워크 수준의 통찰력을 제공합니다.



네트워크 플로우 정보는 해커가 숨길 수 없는 공격의 흔적을 찾게 도와줍니다.

시스템 로그 외에도 최신 SIEM은 네트워크 플로우, 엔드포인트 데이터, 클라우드 사용 및 사용자 행위를 분석합니다. 이러한 다양한 활동 측면을 상관 분석하여 사용자 환경에서 일어나는 일을 완벽하게 파악하고 정상적인 활동의 기준을 식별할 수 있습니다. 이를 바탕으로 위협으로 인지되는 수준을 자동으로 식별합니다.



2

정보보호 프로그램이 사회 공학적인 위협 요소를 고려하는가

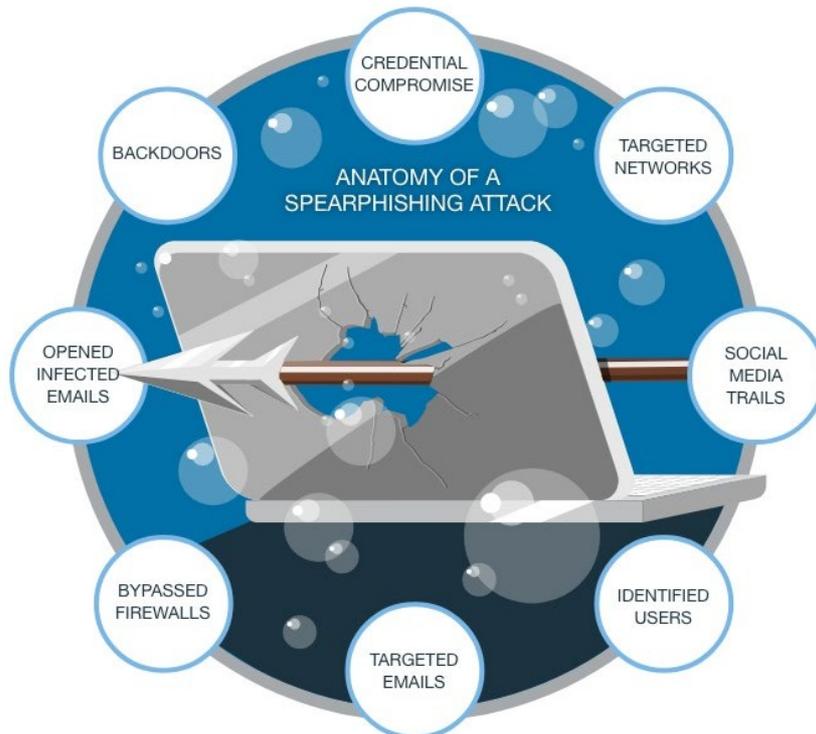
때로는 사용자를 속여서 악성 링크를 클릭하도록 유도하는 경우가 있습니다. 사회 공학적인 요소를 이해하는데 도움이 되는 해결책을 가지고 계신가요?



전체 공격 중 60%는
우연한 실수로 인해
혹은 악의적으로
내부자에 의해
발생합니다.

공격의 대상이 된 사용자 혹은 악의적인 사용자는 다른 사용자와 다른 행동을 보입니다. 이 이상행위를 일찍 발견하면 피해 예방에 도움이 됩니다. 이를 위해 조직의 사용자의 정상적인 활동 범위를 이해하고 해당 기준을 사용하여 위협이 되는 예외를 식별해야 합니다. 사용자 행동 분석 러닝머신을 활용하면 전사적으로 이상 징후 탐지에 도움이 될 수 있습니다.

SIEM의 일부인 UBA(User Behavior Analytics)를 통해 비정상적인 사용자 활동을 발견할 수 있으며, 가장 위험한 사용자를 우선순위화하여 식별할 수 있습니다.



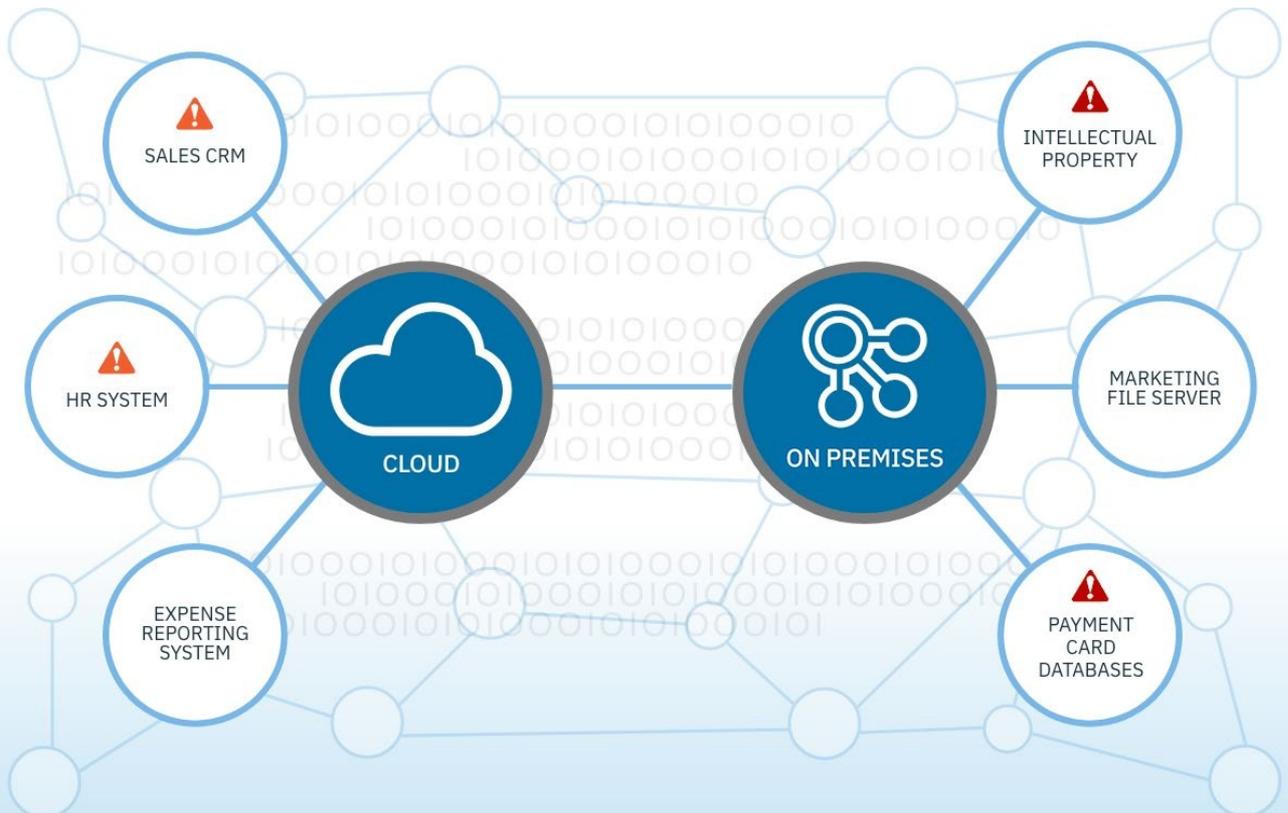
3

중요데이터 및 자산에 대한 위협을 우선순위화할 수 있는가

마케팅에서 사용하는 파일 서버와 PCI 환경 데이터베이스는 위협에 노출되면 큰 보안 사고를 야기할 수 있습니다. 자산의 중요도를 이해하고 비즈니스 위협 정도를 기반으로 위협에 대해 우선순위를 자동으로 지정하여 위협을 알려주는 솔루션이 필요합니다.

좋은 보안 솔루션은 네트워크에 대한 이해를 제공해야 합니다. 이는 담당자에게 가장 민감한 자산이 무엇이며 어느 네트워크 계층 및 클라우드 서비스에 존재하는지를 정의하는 것을 도와줍니다. 또한 해당 고유환경에 맞는 강력한 분석을 기반으로 합니다.

“ 데이터 유출 발견까지 **191**일이 소요되며 복구에는 추가로 **66**일이 소요됩니다.



4

시스템이 생산성 향상을 위해 프로세스를 자동화할 수 있는가

대부분의 보안 팀은 인력 부족과 전문성의 부족으로 어려움을 겪고 있습니다. 좋은 SIEM 솔루션은 수동 프로세스를 최소화할 수 있도록 AI 및 자동화를 제공합니다. 최신 SIEM을 도입하여 추가인력을 투입하지 않고도 생산성을 높일 수 있습니다.

이상적인 SIEM 솔루션은 위협 탐지, 우선 순위 지정 및 사고조사 프로세스 자동화를 지원합니다. 사고대응 및 복구 프로세스를 가속화하는 케이스 관리를 할 수 있도록 검증된 타시스템과의 연동을 제공합니다.

“ **70%**의 사이버 보안 전문가들은 기술 부족이 조직에 영향을 준다고 인지합니다.

“ **2020년까지 150만 건의 사이버 보안 전문가 부족 현상이 발생할 것입니다. 최근 2년에 100만 건이 증가했습니다.**

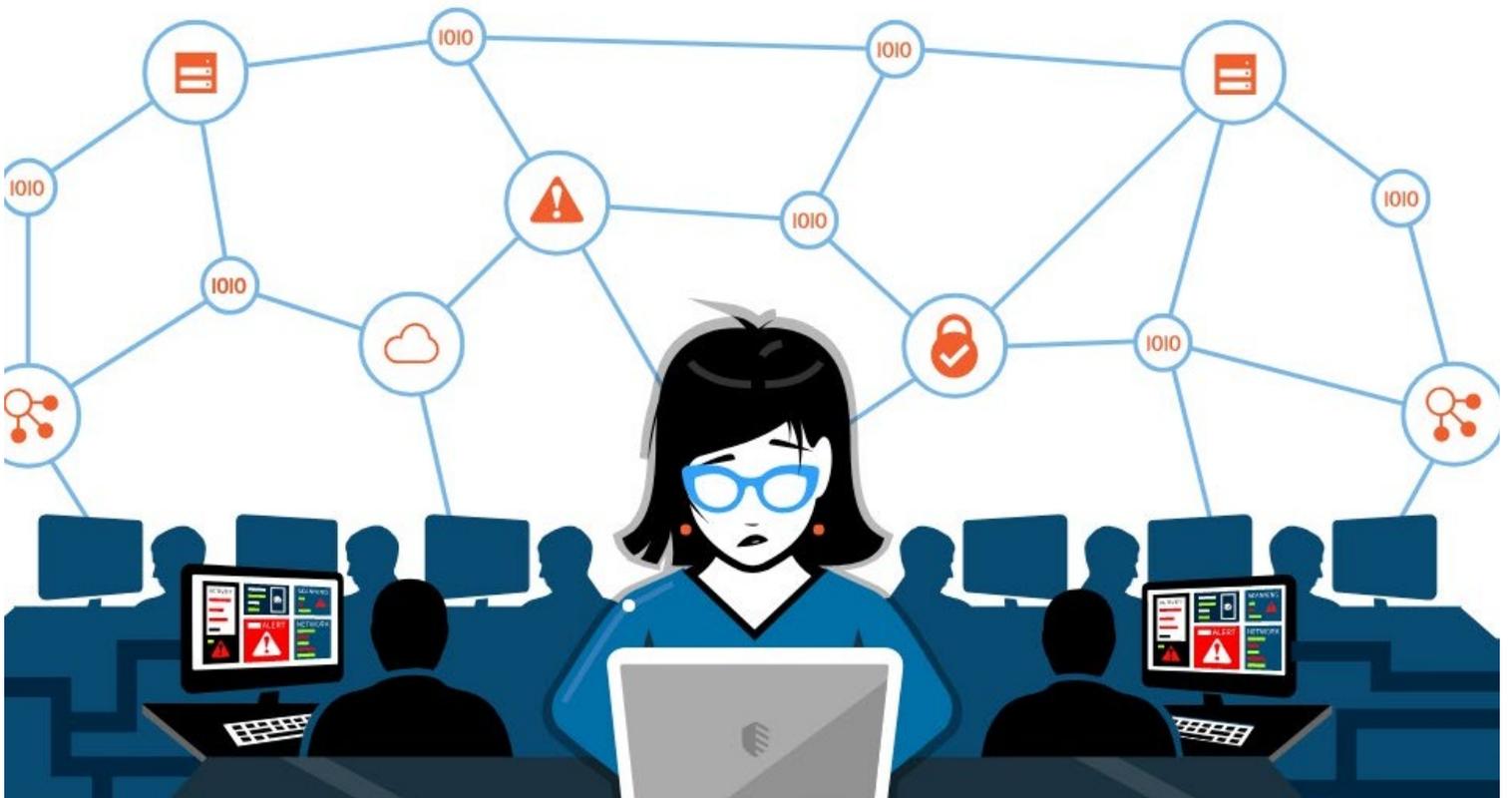
5

귀사의 환경에 적용 및 통합하는 것이 얼마나 쉬운가

어떤 설치 방식을 지원하는지 확인해야 합니다. 하드웨어, 소프트웨어 또는 SaaS 솔루션, 어떤 방식을 선호하든 좋은 SIEM은 사용자의 요구를 충족할 수 있을 만큼 유연해야 합니다. 더불어 SIEM을 통해 가치를 얻으려면 데이터를 연동해야 합니다. 온 프레미스, SaaS 애플리케이션, 퍼블릭 클라우드 환경을 비롯하여 모든 환경에서 작동하는지 확인하십시오.

연동이 용이한지 검토해야 합니다. 로그소스뿐 아니라 위협 인텔리전스 피드, 취약점 스캐너, 사고 대응 플랫폼 및 유스 케이스 관리 시스템 등과 같이 SIEM의 완전성을 위해 필요한 보안 솔루션과의 통합을 지원하는지 고려하십시오. 앱 통합을 위한 개방형 에코시스템은 변화하는 위협 및 위협에 대한 최신 정보를 신속하게 제공하고 사고에 신속대응할 수 있도록 지원합니다.

“ 네트워크 보호를 위해 기업은 평균 **75개**의 보안 제품을 사용합니다. 이를 통합하여 볼 수 있어야 합니다.



갈수록 진화하는 사이버 범죄 — 귀사는 대비하고 있습니까?

최신 SIEM 솔루션은 기본 로그 관리 툴과 수작업 프로세스보다 훨씬 많은 작업을 처리합니다. 하루에 20만 건의 보안 위협이 발생하므로 번개처럼 빠르게 기업을 보호해야 합니다. 훌륭한 SIEM은 피싱 공격, 악성 코드, 자격 위조, 데이터 유출과 같은 위협과 다른 신종 위협에 대해서도 탐지할 수 있어야 합니다. 피해가 시작되기 전에 준비해야 합니다. 모든 SIEM 솔루션이 다 똑같은 것은 아닙니다.

Look for a Solution That:



다양한 위협에 대한
고급 보안 분석 기능 제공



중요 항목 식별을 위한
위협/알람의 우선순위
자동 지정



기존 시스템과의 즉각적인
통합/연동 제공



단일 플랫폼에
보안 데이터 통합력
통합 제공



배포 스케일에 대한 확장성
- 소규모부터 대규모까지!



유연한 도입 방식
- On-Premise
- SaaS
- Public Cloud

About IBM QRadar

IBM QRadar Security Intelligence Platform은 단일 인터페이스에서 로그 관리, 고급 분석, 네트워크 분석, 취약점 관리, 사용자 행동 분석, 위협 인텔리전스 및 AI 기반 위협 조사를 통합하는 포괄적인 보안 분석 솔루션입니다.

모든 솔루션 구성 요소를 통합하여 운영 가능하며 고객이 원하는 만큼의 규모로 시작할 수 있으며 쉽게 확장, 축소 가능합니다. 고객 환경에 맞는 500개 이상의 미리 정의된 탐지 룰을 통해 고객은 쉽게 위협을 모니터링하고 사고에 대응할 수 있습니다.

IBM Security App Exchange를 통해 신속하고 쉽게 새로운 기능을 추가할 수 있습니다.

더 알아보기

www.ibm.com/kr-ko/security/security-intelligence



References

[Investigating Threats with Watson for Cyber Security](#), IBM

[The IBM X-Force 2016 Cyber Security Intelligence Index](#), IBM

[Ponemon Institute's 2017 Cost of Data Breach Study: Global Overview](#), IBM

[Cybersecurity skills shortage creating recruitment chaos](#), CSO

[Cybersecurity labor crunch to hit 1.5 million unfilled jobs by 2021](#),

[Defense in depth: Stop spending, start consolidating](#), CSO



IBM Security