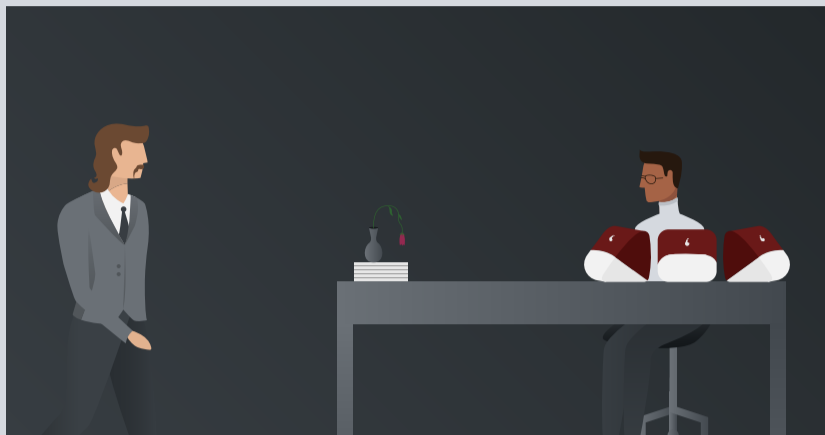


서로 다른 SIEM을 사용하는 보안관제센터(SOC) 이야기

운영의 성패는 적절한 SIEM 선택 여부에 따라 결정됩니다. 기존 SIEM을 그대로 활용하여 날로 진보하는 위협에 대응한다면 기업 보안에 있어 불확실성의 시대를 조래할 수 있습니다. 위협에 직접적으로 대응하는 자세대 지능형 SIEM 플랫폼인 IBM Security QRadar로 지혜의 시대를 열어보십시오.

기존 SIEM을 사용하는 SOC의 경우



데이터 소스
가져오기는
잘 되고 있나요?

아니요. 데이터를
SIEM으로 가져올 수
없습니다. 구문 분석이나
정규화를 수행할 수
없어 무용지물입니다.

그러니까 데이터는 있는데
애플리케이션 트래픽, 레이어 7,
액세스 로그를 확인할 수 없단
말이죠?

네. 플로우 데이터도 못 가져옵니다.
로그로 전환하면 모든 것이 너무 커져서
확인 가능한 건 이게 전부입니다.

그렇다면 왜 그런지 알아보죠.
작업에 진척이 없었다고 보고를
하기 전에 지원부서에 연락을
해봐야겠네요.

한편 지원부서에서는

전체 환경에 대한
가시성을 확보하지
못했다고 하셨죠?

전혀요. 지원도 받을
수 없어요. 솔직히
말하자면 SIEM이
아니라 골칫거리네요.

한편 차세대 SIEM을 사용하는 SOC의 경우

QRadar 배포 및 구성은 어떻게 되고 있나요?

끝났습니다! 8시간도 안 걸렸어요. 그리고 이미 15만개 이상의 에셋을 찾아냈습니다.

좋아요. 하지만 사용자와 엔터티 행동에 대한 동향까지는 아직 파악할 수 없겠지요?

가능합니다. IBM AppExchange로 쉽게 해결했어요.

좋아요. 이 작업 때문에 지원 업무 시간을 다 쓰진 않았으면 좋겠군요.

그렇 리가요. IBM은 수백 개의 비디오, 문서, 심지어 다른 사용자의 조언을 얻을 수 있는 커뮤니티까지 갖춘 온라인 공간을 제공하거든요.

이제 환경 전체에 대한 가시성이 확보된 건가요?

그럼요. 조직 안팎을 속속들이 알 수 있어요. 기대했던 결과입니다.

IBM Security QRadar는 10년 이상 Gartner SIEM 부문 Magic Quadrant 리더로 선정되었거든요.

QRadar는 빨리 배포할 수 있고 노이즈를 더 신속하게 제거할 수 있어요. 비즈니스에 대한 진짜 위협을 재빨리 탐지해서 대응할 수 있는 거죠.

* 해당 고객사례는 예시 목적으로 제공된 것입니다. 실제 성능 결과는 특정 구성 및 운영 조건에 따라 달라질 수 있습니다.

IBM Security QRadar로 최적의 운영 환경을 경험하세요.
지금 차세대 SIEM의 장점에 대해 자세히 알아보세요.

업그레이드