전공 용어

1. SIEM : SIEM(Security Information and Event Management) 소프트웨어는 경계부터 최종 사용자까지 전체 범위에서 로그를 수집, 저장 및 분석합니다. 종합적인 보안 보고 및 규제 준수 관리와 함께 신속한 공격 탐지, 차단 및 응답을 위해 보안 위협을 실시간으로 모니터링합니다. SIEM을 사용하는 네트워크에서 공격이 발생하면 소프트웨어가 모든 IT 구성 요소(게이트웨이, 서버, 방화벽 등)에 대한 인사이트를 제공합니다.

이점: SIEM 소프트웨어는 조직에서 네트워크에 대한 최신 보안 위협을 탐지할 수 있는 강력한 도구입니다. SIEM은 보안 이벤트의 장기적 분석과 함께 실시간 보고 기능을 통해 조직의 IT 보안에 대한 포괄적 방어 체계를 제공합니다. SIEM 소프트웨어는 네트워크 전반의 소스에서 생성되는 이벤트 레코드를 로깅합니다. 이러한 로그들은 나중에 소프트웨어에서 분석 과정을 지원하는 중요한 포렌식 도구를 IT 직원에게 제공합니다. 완벽한 로그 수집은 수많은 규제 준수 보고 요구 사항을 충족하는 데 도움이 됩니다. 구문 분석 및 표준화는 서로 다른 시스템의 로그 메시지를 공통 데이터 모델로 매핑하고 다양한 소스 형식으로 로깅된 관련 이벤트를 분석하도록 지원합니다. 상관분석 기능은 개별 시스템 또는 애플리케이션의 로그 이벤트를 연결시킴으로써 보안 위협의 탐지 및 대응 속도를 높여줍니다. SIEM 어그리게이션은 중복되는 이벤트 레코드를 통합하고 상관분석 및 집계된 이벤트 데이터를 실시간으로 보고하며 장기 요약 내용과 비교함으로써 이벤트 데이터의 양을 줄입니다.

문제 해결: 네트워크 보안 위협은 빠르게 확산되고 있을 뿐만 아니라 끊임 없이 새로운 위협이 등장하고 있습니다. 모바일 사용자, 원격지 및 네트워크 액세스 디바이스 수가 늘어남에 따라 네트워크 진입 지점도 증가할 수 밖에 없습니다.

새로운 애플리케이션과 기술은 네트워크에서 위험이 발생하고 공격을 일으키는 요인이기도 합니다. 많은 조직에서 보안 위반이 몇 개월 동안 전혀 감지되지 않을 수 있는 반면, 일부 조직에서는 악의적 활동으로부터 네트워크를 보호하기 위한 전담 IT 부서를 갖추고 있습니다. 조직의 IT 부서는 다양한 소스에서 데이터를 분석하여 네트워크에 가해지는 위협을 파악하고 이런 위협을 해결하기 위한 조치를 결정해야 합니다.

IT 직원에게는 네트워크의 모든 레이어 및 위치에서 발생하는 위협으로부터 보호하기 위한 계층형 보안 기능을 제공하는 완벽하고 포괄적인 솔루션이 필요합니다. IT 부서는 다음을 전제로 규제 준수 요구 사항도 충족해야 합니다.

* 누가 무엇을 언제 했는지 조사하고 보고서를 작성할 수 있는 책임 규명.
* 보안 제어, 비즈니스 애플리케이션 및 보호 대상 자산에 대한 가시성을 제공하는 투명성.
* 회사 내의 IT 위험에 관한 측정 지표 및 보고 기능을 제공할 수 있는 측정 가능성.

2.

5.