SIEM 및 SOAR 플랫폼 구현하기: 경영진 지침

ASD는 이 간행물에 기여한 파트너들에게 감사의 말씀을 전합니다.

소개

본 보안가이드는:

- 보안 정보 및 이벤트 관리(SIEM) 및 보안 오케스트레이션, 자동화 및 대응(SOAR) 플랫폼의 가치를 설명합니다.
- 이러한 플랫폼의 작동 방식을 설명합니다.
- 도전 과제를 간략하게 설명합니다.
- 구현하기 위해 필요한 고수준의 권장 사항을 제공합니다.

주로 조직의 경영진 수준의 의사 결정권자를 대상으로 하지만 SIEM/SOAR의 구현 여부와 방법을 고려하는 모든 조직에서 사용할 수 있습니다.

이 문서는 SIEM/SOAR 플랫폼에 대한 세 가지 가이드라인 중 첫번째 지침입니다:

SIEM 및 SOAR 플랫폼 구현하기: 경영진 지침

이 문서는 경영진을 대상으로 작성되었습니다. SIEM/SOAR 플랫폼을 정의하고, 그 장점과 과제를 간략하게 설명하며, 경영진과 관련된 구현에 대한 광범위한 권장 사항을 제공합니다.

SIEM 및 SOAR 플랫폼 구현하기: 실무자 지침

이 문서는 사이버 보안 실무자를 대상으로 합니다. 기술적인 세부 사항에서는 SIEM/SOAR 플랫폼을 정의하고, 장점과 과제를 간략하게 설명하며, 구현을 위한 모범 사례를 제공합니다.

SIEM 수집을 위한 우선 순위 로그: 실무자 지침

이 문서는 사이버 보안 실무자를 위한 것으로, SIEM 수집을 위해 우선순위를 정해야 하는 로그에 대한 자세한 기술 지침을 제공합니다. 엔드포인트 탐지 및 대응 도구, Windows/Linux 운영 체제, 클라우드 및 네트워크 장치를 포함한 로그 소스를 다룹니다.

이 지침은 로깅 전략 개발에 대한 높은 수준의 권장 사항을 제공하는 '이벤트 로깅 및 위협 탐지 모범사례(Best practices for event logging and threat detection)'와 함께 읽어야 합니다.

1. SIEM 및 SOAR 플랫폼의 가치는 무엇인가요?

SIEM 및 SOAR 플랫폼은 조직의 로깅 및 가시성 전략의 구성 요소가 될 수 있습니다. 가시성은 악의적인 사이버 활동을 탐지하기 위한 기본이며 효과적이고 전방위적인 사이버 보안 전략에 매우 중요합니다.

이러한 플랫폼을 도입시 거둘 수 있는 효과는:

- 흩어져 있는 중요하고 검증된 이벤트 데이터를 수집, 중앙 집중화 및 분석하여 조직 네트워크에서 일어나는 일에 대한 **전반적인 가시성을 향상**
- 의심스러운 활동에 대한 신속한 경고를 생성하여 사이버 보안 이벤트 및 사고에 대한 조직의 **탐지 기능을 강화**
- 악의적인 공격자가 네트워크에 대한 액세스를 유지하기 위해 특정 데이터를 수정/삭제하는 것을 방지하여 이벤트 및 사고 탐지를 강화
- 알림을 통해 적시에 개입을 유도하고 사고 대응자가 발생한 상황을 기록하는 데이터에 액세스할 수 있도록 하여 사이버 보안 이벤트 및 사고에 대한 조직의 **대응력을 강화**
- SOAR의 경우 특정 대응 조치를 자동화하여 이벤트 및 사고 대응을 강화하고 대응 시간을 단축하여 보안 팀이 더 복잡한 문제에 집중할 수 있게 업무 효율화
- 로그 데이터를 수집하고 중앙 집중화해야 하는 호주 신호국의 필수 8가지 성숙도 모델과 사이버보안 및 인프라 보안 기관(CISA)의 사이버보안 성과 목표(CPG)를 이행하는 데 도움

따라서 이러한 플랫폼은 조직의 시스템과 서비스가 지속적으로 운영되고, 무단 액세스 및 도난으로부터 데이터를 보호할 수 있게 합니다.

그러나 이러한 이점은 SIEM/SOAR가 제대로 구현된 경우에만 얻을 수 있습니다(섹션 3 참조).

2. 이러한 플랫폼은 어떻게 작동하나요?

단일 조직의 네트워크는 여러 디바이스, 애플리케이션, 운영 체제 및 클라우드 서비스를 포함하는 매우 복잡한 구조일 수 있습니다. 네트워크 내의 이러한 각 소스는 로그 데이터 또는 소스 내에서 발생하는 특정 정보(예: 디바이스에서의 사용자 활동)를 생성할 수도 있습니다.

SIEM은 로그 데이터를 **수집, 중앙 집중화 및 분석**하는 소프트웨어 플랫폼의 일종입니다.

SIEM은 네트워크 전체에서 복잡하고 분산된 로그 데이터를 수집하고 이를 보고서 및 대시보드 형태로 간소화합니다. 또한 SIEM은 규칙과 필터를 적용, 이 데이터를 분석하여 사이버 보안 이벤트 또는 사고를 발생시킬 수 있는 비정상적인 네트워크 활동을 탐지합니다. 많은 SIEM 제품은 외부 소스의 최신 사이버 위협 인텔리전스를 통합하여 이러한 분석을 강화합니다. 잠재적인 이벤트나 인시던트를 감지하면 SIEM은 경고를 생성하여 조직의 보안 팀에 필요에 따라 조사하고 대응하도록 유도합니다.

SOAR는 로그 데이터의 수집, 중앙 집중화, 분석을 기반으로 구축되는 소프트웨어 플랫폼의 일종입니다. 일부 SOAR 플랫폼은 이러한 기능을 자체적으로 수행하기도 하고, 기존 SIEM과 통합하여 로그 수집, 중앙 집중화 및 분석을 활용하는 플랫폼도 있습니다.

어느 쪽이든 SOAR는 탐지된 사이버 보안 이벤트 및 인시던트에 대한 **대응의 일부를 자동화**합니다. 네트워크에서 이벤트의 원인을 격리하는 등 특정 이벤트가 발생할 때 취해야 할 특정 조치를 설정하는 사전 정의된 '플레이북'을 적용하여 이를 수행합니다. 이러한 자동화된 조치는 보안담당자를 대체하는 것이 아니라 업무를 지원하는 것입니다.

3. 이러한 플랫폼을 구현하는 데 있어 주요 과제는 무엇인가요?

SIEM이나 SOAR 모두 '한 번 설정하고 잊어버리는' 도구가 아닙니다. 두 플랫폼 중 하나를 구현하려면 집중적이고 지속적인 고도로 숙련된 인력이 필요한 프로세스입니다. 이러한 인력은 두 가지 주요 기술적 과제에 직면합니다.

첫 번째는 사이버 보안 이벤트 및 인시던트가 발생할 때 SIEM이 경보를 생성하고, 반대로 이벤트/인시던트가 발생하지 않을 때는 경보를 생성하지 않도록 하는 것입니다. 이를 위해 담당자는 SIEM이 수집할 로그 데이터의 올바른 유형과 양, 그리고 해당 데이터에 적용할 올바른 규칙과 필터를 구성해야 합니다. 여기에는 알림을 유발할 수 있는 관심 이벤트를 정의하는 위협 모델을 개발하는 것도 포함됩니다. 정확한 알림이 이루어지지 않으면 보안팀은 SIEM의 잘못된 알림으로 인해 운영상의 어려움을 겪거나 알림이 없어 실제 이벤트/인시던트를 놓칠 수 있습니다.

두 번째 핵심 기술적 과제는 SOAR가 실제 사이버 보안 사고에 대해서만 적절한 조치를 취하고, 일상적인 네트워크 활동에 대해서는 조치를 취하지 않음으로써 대응 활동을 방해하지 않도록 하는 것입니다. 정확한 조치가 이루어지지 않으면 SOAR로 인해 서비스 제공이 심각하게 중단될 수 있습니다.

이러한 기술적 과제를 해결하려면 담당자는 사내 네트워크와 조직에 맞게 SIEM/SOAR를 신중하게 구성해야 합니다. 그런 다음 네트워크, 기술, 사이버 위협 환경이 계속 변화함에 따라 이를 지속적으로 조정하고 그 효과를 테스트해야 합니다. 이러한 지속적인 작업은 내부적으로, 또는 외부 서비스 제공업체를 통해, 혹은 이 두 가지를 조합하여 수행할 수 있습니다.

따라서 SIEM/SOAR를 제대로 구현하려면 상당한 비용이 소요됩니다. 이러한 비용에는 초기 및 지속적으로 발생하는 다음과 같은 항목들이 포함될 수 있습니다:

- 플랫폼의 라이선스 및 데이터 사용 비용
- SIEM 및 SOAR 구현에 필요한 전문 기술을 갖춘 직원을 고용하고 유지하는 데 드는 비용
- 기술, 네트워크, 위협 환경이 변화함에 따라 기존 직원 숙련도를 높이는데 드는 비용과 플랫폼을 유지 관리하는데 필요한 지속적인 교육 비용
- 서비스 비용(구현이 아웃소싱된 경우)

그러나 사이버 보안 사고를 감지하지 못하거나 적절히 대응하지 못하면 막대한 비용이 발생할 수 있습니다. 또한 시스템이 오프라인 상태가 되고, 서비스 제공이 중단되며, 데이터가 유출되거나 파괴되고, 대외적인 신뢰도가 떨어질 수도 있습니다. 조직의 구현 범위를 정의하는 방법에 대한 자세한 내용은 'SIEM 및 SOAR 플랫폼 구현-실무자 지침편'(Implementing SIEM and SOAR platforms: Practitioner guidance)을 참조하세요.

4. 구현을 위한 권장 사항

다음은 SIEM/SOAR 구현 여부와 방법을 고려 중인 경영진을 위한 높은 수준의 전략적 권장 사항입니다. 이러한 플랫폼은 로그 데이터를 수집 및 중앙 집중화하고 사고 탐지를 강화할 수 있는 기술의 한 형태일 뿐이며, 로그 관리 도구와 같은 다른 옵션도 있다는 점에 유의해야 합니다.

a. 플랫폼을 자체 구축할 필요성과 가능성을 고려하기

조직에서 민감한 정보를 관리하거나 중요한 서비스를 제공하는 경우 사내에서 플랫폼을 구현해야 할 수도 있습니다.

SIEM/SOAR를 사내에서 구현할 때의 주요 이점은 내부 직원들이 조직 고유의 네트워크와 비즈니스 프로세스에 대한 깊은 이해를 가지고 있으며, 비정상적인 행동에 대해 사용자에게 직접 문의하거나 즉각적인 인시던트 대응을 시작할 수 있는 권한이 있다는 점입니다. 반면 아웃소싱을 사용하면 가시성 부족, 업무 중복, 커뮤니케이션의 어려움이 발생할 수 있습니다.

그러나 내부 구현 역량을 개발하고 유지하는 것은 자원이 많이 들고, 관련 기술 인력에 대한 수요가 높기 때문에 어려운 과제가 될 수 있습니다. 경영진은 여러 인력이 SIEM/SOAR 구현을 위해 전담으로 투입되어야 할 것을 예상해야 하며, 이러한 플랫폼을 운영하는 과정에서는 오랜 기간 동안 스트레스가 높은 업무를 수행해야 할 수도 있습니다.

조직에서 구현의 일부 또는 전부를 아웃소싱하는 경우, 다음과 같은 사항을 고려할 것을 권장합니다:

- 연중무휴 24시간 고품질 모니터링 및 사고 대응 서비스 제공
- 사이버 보안 태세가 양호한 것으로 알려져 있는지
- 외국 데이터 저장소 요구 사항에 제약을 받는지
- 외국에 소재하거나 외국에 지사를 두고 있는지

또한 다음과 관련된 계약 조항에도 특별한 주의를 기울여야 합니다:

- 서비스의 효과를 검증하고 보장하는 방법
- 서비스 제공업체가 조직에 적용되는 법률, 규제 및 내부 요구 사항을 준수하는지 확인하는 방법
- 서비스 제공업체의 기술 수준
- 제공될 서비스의 내용(표준 적용, 교육 및 최종 사용자 피드백 포함)
- 서비스 제공업체가 조직에 제공할 가시성의 수준
- 사이버 보안 사고의 탐지 및 대응에 대한 책임과 법적 의무를 분담

b. 다양한 제품 간의 잠재적인 숨겨진 비용을 주의 깊게 살펴보기

작성 기관은 다양한 SIEM/SOAR 제품과 관련된 비용을 신중하게 검토할 것을 권장합니다. 플랫폼의 가시성과 탐지 성능을 향상시키기 위해 시간이 지남에 따라 SIEM에 수집되는 로그 데이터의 양을 늘리는 것이 일반적입니다. 대부분의 SIEM 가격 모델은 SIEM이 수집하는 데이터의 양을 기준으로 합니다. 일부 제품은 사전 구매한 양에 따라 수집 한도를 제한합니다. 그렇지 않은 제품의 경우, 수집을 신중하게 관리하지 않으면 조직에서 매우 큰 비용이 발생할 수 있으므로 주의해야 합니다.

'SIEM 및 SOAR 플랫폼 구현-실무자 지침편'(Implementing SIEM and SOAR platforms: Practitioner guidance)는 이러한 플랫폼을 통해 로그를 수집, 중앙 집중화 및 분석하는 데 드는 비용을 절감하는 방법과 조직에 맞는 구현 범위를 정의하는 방법에 대해 추가로 안내하고 있습니다. 또한 '이벤트 로깅 및 위협 탐지 모범사례(Best practices for event logging and threat detection)' 도 참고하시기 바랍니다.

c. 교육비용을 포함한 지속적인 구현 비용에 대한 계획 세우기

위에서 설명한 바와 같이 SIEM/SOAR를 제대로 구현하려면 상당한 초기 비용과 지속적인 비용이 소요됩니다. 조직은 공급업체 설명서를 참조하여 대체 로깅 옵션으로 이러한 비용을 줄일 수 있는지 확인해야 합니다. 자체적인 내부 역량을 개발하는 조직의 경우에는 상당한 노력과 자금을 투입하여 지속적으로 직원을 교육할 것을 권장합니다.

d. SOAR 구현을 고려하기 전에 SIEM을 올바르게 구현하기

일반적으로 SOAR을 구현하기 전에 SIEM을 올바르게 구현하고 사이버 보안 이벤트 및 인시던트를 정확하게 알려주는지 확인해야 합니다.

e. 플랫폼의 성능 테스트 확인

네트워크, 기술 및 사이버 위협 환경의 지속적인 변화가 성능에 영향을 미치므로 플랫폼이 사이버 보안 이벤트 및 인시던트를 효과적으로 알려주는지 테스트하는 내부 프로세스와 절차를 수립하는 것이 필수적입니다.

성숙한 SIEM/SOAR 기능이 구축된 후에는 침투 테스트와 같은 외부 전문 서비스 기능을 사용하여 성능을 테스트할 것을 권장합니다. 작성 기관은 조직의 요구 사항에 가장 적합한 다양한 SIEM/SOAR 공급업체를 조사할 것을 권장합니다.

면책 조항

이 가이드의 자료는 일반적인 성격의 것으로, 법적 조언으로 간주되거나 혹은 특정 상황이나 긴급 상황에서 의존해서는 안 됩니다. 중요한 사안에 대해서는 자신의 상황에 맞는 적절한 독립적인 보안전문가의 조언을 구해야 합니다.

호주 연방은 본 가이드에 포함된 정보에 의존한 결과로 발생한 어떠한 손해, 손실 또는 비용에 대해서도 책임을 지지 않습니다.

For more information, or to report a cyber security incident, contact us:
cyber.gov.au | 1300 CYBER1 (1300 292 371)