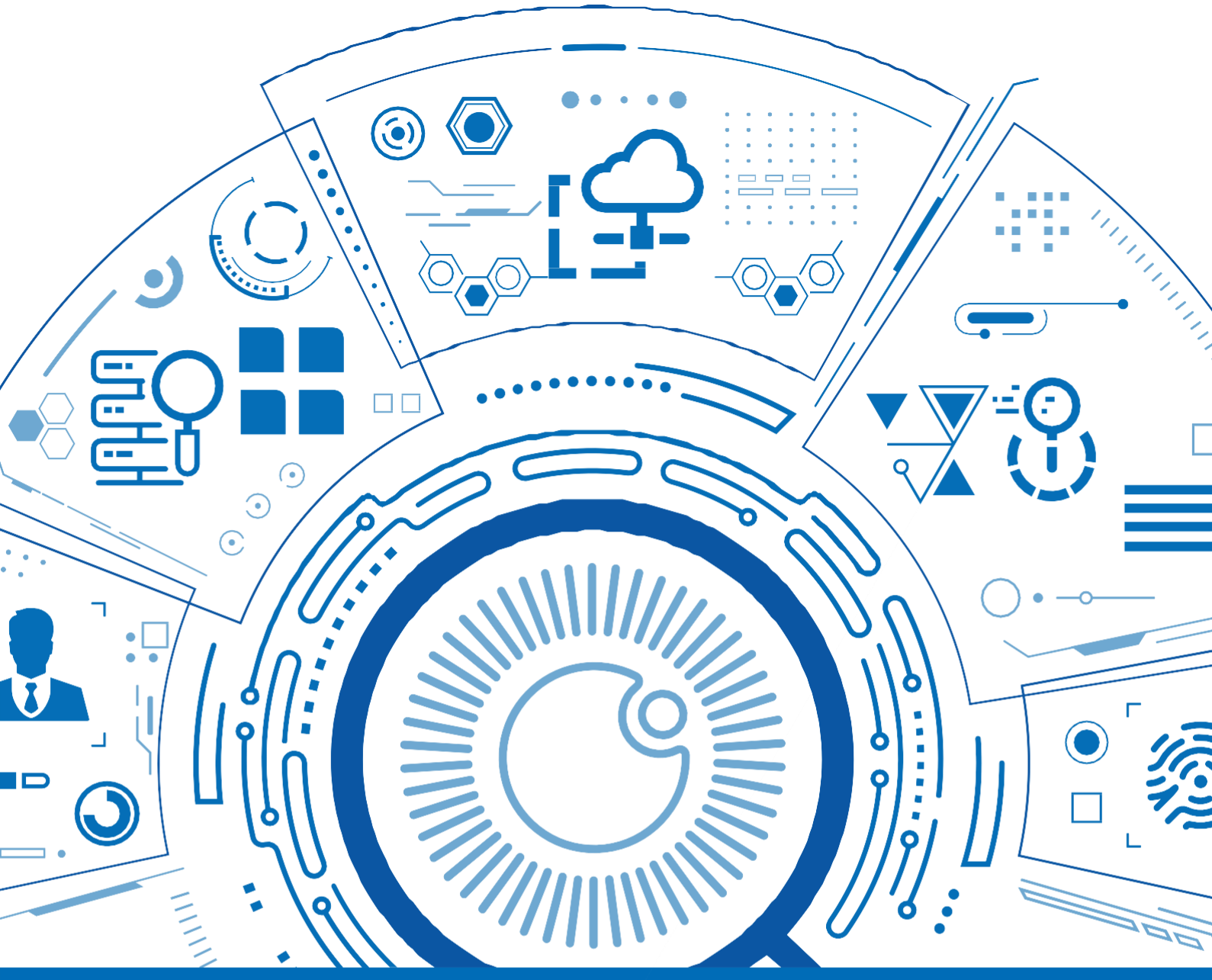
# SIEM 및 SOAR 플랫폼 구현: 실무자 지침



Australian Government

Australian Signals Directorate





National Cyber Security Centre

a part of GCHQ

Communications Security Establishment

Centre de la sécurité des télécommunications

Canadian Centre for Cyber Security

Centre canadien pour la cybersécurité

Te Tira Tiaki

Government Communications Security Bureau

National Cyber Security Centre

PART OF THE GCSB

NISC

内閣サイバーセキュリティセンター

National center of Incident readiness and Strategy for Cybersecurity

JPCERT CC®



National Cyber and Information Security Agency

NÚKIB

ASD는 이 간행물에 기여한 파트너들에게 감사의 말씀을 전합니다.

# 목차

# 소개

이 문서는 사이버 보안 실무자를 위한 보안 정보 및 이벤트 관리(SIEM) 및 보안 오케스트레이션, 자동화 및 대응(SOAR) 플랫폼에 대한 높은 수준의 지침을 제공합니다. 이 지침은 주로 정부 및 기업 내 실무자를 대상으로 하지만 중요 인프라 조직뿐만 아니라 SIEM/SOAR 플랫폼에 관심이 있거나 현재 사용 중인 모든 조직의 실무자들도 사용할 수 있습니다.

본 가이드는 네 가지 섹션으로 구성되어 있습니다:

- SIEM 및 SOAR 플랫폼 정의
- 사이버 보안 태세에 기여할 수 있는 잠재적인 이점에 대한 설명
- 이점을 실현하기 위해 플랫폼을 적절히 구현하는데 수반되는 과제를 제시
- SIEM/SOAR 구현의 각 단계(조달, 구축 및 유지 관리)에서 실무자가 참조할 수 있는 모범 사례 원칙을 제공

이 문서의 권장 사항은 일반적인 조언으로 간주해야 하며, 각 조직은 로그의 수집, 중앙 집중화 및 분석을 특정 환경과 위험 프로필에 맞게 조정해야 합니다.
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.

용어에 대한 참고 사항: 아래에서 설명하는 것처럼 모든 SIEM 플랫폼은 로그 수집, 중앙 집중화 및 분석을 수행합니다. 일부 SOAR 플랫폼에는 SIEM이 내장되어 있어 이러한 기능을 자체적으로 수행할 수 있습니다. 다른 많은 SOAR 플랫폼은 별도의 SIEM과 통합되어 SIEM의 로그 수집, 중앙 집중화, 분석 기능을 활용합니다. 그러나 자동화된 대응 기능을 수행하는 플랫폼은 SOAR 플랫폼뿐입니다. 이 가이드에서 SIEM에 대한 언급은 특히 로그 수집, 중앙 집중화 및 분석 기능을 의미합니다. 조직에서 SIEM이 내장된 SOAR를 사용하는 경우에는 다음과 같습니다.
콘텐츠는 SOAR의 로그 수집, 중앙 집중화 및 분석과 관련이 있습니다. SIEM/SOAR 플랫폼에 대한 언급은 두 플랫폼 모두에 적용되는 지침에 관한 것입니다. SOAR에 대한 언급은 특히 SOAR 플랫폼만이 수행할 수 있는 자동화된 대응 기능에 관한 것입니다.

# 1. SIEM 및 SOAR 플랫폼 정의

## SIEM 플랫폼이란 무엇인가요?

SIEM은 사이버 보안을 목적으로 네트워크 또는 시스템 내의 소스에서 로그 데이터를 수집, 중앙 집중화, 분석하는 소프트웨어 플랫폼 또는 어플라이언스의 일종입니다. 이러한 목적을 위해 제대로 구현된 SIEM 플랫폼은 네트워크에 흩어져 있는 중요한 로그 데이터의 수집과 중앙 집중화를 자동화하여 보안팀이 보다 쉽게 탐색할 수 있게 해줍니다. 다른 로그 수집 및 중앙 집중화 도구와 달리 잘 구성된 SIEM은 사전 정의된 평상시 네트워크 활동 기준, 규칙 및 필터를 적용하여 로그 데이터를 분석하고 상호 연관성을 파악합니다. 이러한 분석을 통해 SIEM 플랫폼은 사이버 보안 이벤트나 인시던트를 나타낼 수 있는 네트워크의 비정상적인 활동을 탐지할 수 있습니다. 대부분의 SIEM 제품은 최신 위협 인텔리전스를 통합하여 분석을 강화합니다.

SIEM 플랫폼은 쿼리 언어를 사용하여 로그 데이터를 검색하고 분석합니다. 일반적으로 사용되는 쿼리 언어는 SIEM 제품마다 다릅니다.1 쿼리는 주기적으로 또는 필요에 따라(예: 비정상적인 활동을 조사하거나 사고 발생 후 포렌식 분석을 수행하기 위해) 실행되며 대시보드, 보고서 또는 알림의 형태로 정보를 반환합니다.

## SOAR 플랫폼이란 무엇인가요?

SOAR는 네트워크에서 탐지된 비정상적인 활동에 대한 대응을 자동화하는 소프트웨어 플랫폼입니다. 이 플랫폼은 사고 대응과 비즈니스 연속성 계획을 결합하여 특정 보안 이벤트 발생 시 취해야 할 몇 가지 조치를 지시하는 사전 정의된 '플레이북'을 적용하여 대응을 자동화합니다. 이러한 자동화된 조치는 인시던트 대응자를 대체하지는 않지만 비정상적인 활동에 대한 대응을 간소화할 수 있습니다. 2

일부 SOAR 플랫폼은 SIEM 플랫폼과 통합하여 로그 데이터의 수집, 중앙 집중화, 분석을 활용하도록 설계되었습니다. 다른 플랫폼은 자체적으로 로그 수집, 중앙 집중화, 분석을 수행합니다. 또한 방화벽, 엔드포인트 보안 솔루션, 취약성 스캐너 등 다른 보안 도구와 통합할 수도 있습니다.

---

1 서로 다른 쿼리 언어 간의 격차를 해소하는 한 가지 방법은 탐지 규칙을 SIEM 플랫폼별 쿼리 언어로 텍스트로 표시하고 구현할 수 있는 YAML(또 다른 마크업 언어) 기반 형식인 시그마를 사용하는 것일 수 있습니다. 참조: https://github.com/SigmaHQ/sigma.

2 SIEM과 SOAR는 탐지 기술의 한 형태일 뿐이라는 점에 유의하세요. canary 기술과 같은 다른 형태는 여기서는 논의되지 않습니다.

# 2. SIEM 및 SOAR 플랫폼 잠재적 이점

자동화를 통해 SIEM/SOAR 플랫폼은 보안팀의 네트워크 가시성과 사이버 보안 이벤트 및 인시던트를 탐지하고 대응하는 능력을 강력하게 향상시킬 수 있습니다. 그러나 이러한 각 이점은 SIEM/SOAR 가 제대로 구현된 경우에만 제공됩니다. (섹션 3 참조)

궁극적으로 네트워크 가시성과 사이버 보안 이벤트 및 사고의 탐지 & 대응을 강화하면 네트워크에 저장된 정보의 보안성과 무결성이 향상됩니다. 제대로 구현되고 지속적으로 유지 관리되는 SIEM/SOAR 플랫폼은 시스템의 중단, 민감 데이터의 탈취 또는 변조, 중요 네트워크에 대한 제어권 상실을 방지하는 데 도움이 될 수 있습니다.

탐지 및 대응 시간을 간소화함으로써, 제대로 구현된 SIEM/SOAR 플랫폼은 비용이 많이 드는 사이버 보안 사고를 예방하고 네트워크에서 공격자를 제거하는 데 드는 고비용 절차를 피할 수 있도록 돕습니다. 이러한 잠재적인 사고 기반 비용은 SIEM/SOAR 플랫폼을 제대로 구현하는 데 드는 비용보다 훨씬 더 클 수 있습니다.

## 가시성 향상

로그 수집 및 중앙 집중화를 자동화하고, 이 데이터를 분석하고, 대시보드와 보고서로 분석 결과를 제시함으로써 SIEM은 보안 팀이 네트워크 전반에서 무슨 일이 벌어지고 있는지를 보다 더 쉽게 파악하고 해석할 수 있게 해줍니다. 이러한 정보는 매우 복잡하고 분산되어 있을 수 있습니다.

중앙 집중식 로그 솔루션 또는 SIEM 플랫폼을 구현할 때 또 다른 장점은, 의심스러운 이벤트를 조사하는 동안 이벤트 데이터를 보다 쉽게 접근할 수 있다는 것입니다. 이는 각 시스템에 로그인하여 수동으로 로그를 수집할 필요를 없애줍니다.

로그 데이터를 수집하고 중앙 집중화하는 것은 모든 조직이 호주신호국(ASD)의 필수 8가지 성숙도 모델과 사이버보안 인프라 보안 기관(CISA)의 사이버보안 성능 목표(CPG)를 이행하는 데에도 매우 중요합니다. 규정 준수 요건이 로그를 수집하고 중앙 집중화하는 도구를 구현하는 주요 목적이라면 SIEM/SOAR 플랫폼이 가장 적절하거나 비용 효율적인 선택은 아닐 수 있습니다. 이 경우에는 다른 도구를 사용할 수도 있습니다. 예를 들어, CISA의 Logging Made Easy(LME)는 로그 수집을 중앙 집중화하는 무료 오픈 소스 플랫폼입니다. LME는 로그 관리 및 위협 탐지 시스템이 필요한 중소규모 조직을 위한 것으로, CISA의 LME GitHub 페이지에서 직접 다운로드할 수 있습니다.

# 탐지 기능 향상

또한 잘 구성되고 지속적으로 유지 관리되는 SIEM 플랫폼은 네트워크에서 비정상적인 활동에 대한 신속한 경고를 생성하여 보안팀에 추가 조사를 촉구함으로써 사이버 보안 이벤트 및 인시던트의 탐지 기능을 향상시킵니다. 이상 징후 탐지와 같은 일부 탐지는 효과적으로 작동하려면 많은 양의 데이터가 필요하지만, 잘 유지 관리된 SIEM 플랫폼은 탐지가 오탐지인지 여부를 판단하는 데 도움이 됩니다.

로그 수집을 자동화하고 중앙 집중식 로그의 무결성을 확보하면 일부 악의적인 사이버 공격자가 네트워크 또는 시스템 접속을 유지하기 위해 사용하는 전술인 '무단 수정 및 삭제'로부터 로그를 보호하여 탐지가 향상됩니다.3 또한 조직은 커뮤니티 또는 공급업체의 공통 탐지 룰을 사용할 수 있는 SIEM 플랫폼을 사용하여 로그 이벤트 표준화 수준을 향상시켜야 합니다. 공통 탐지 규칙을 사용하면 이벤트를 탐지하는 기능이 향상되고 이러한 규칙을 배포하는 데 필요한 시간이 단축됩니다.

# 대응력 향상

SIEM/SOAR 플랫폼은 사이버 보안 이벤트 및 사고에 대한 대응 능력도 향상시킬 수 있습니다. SIEM 플랫폼은 비정상적인 활동에 대한 신속한 알림을 생성함으로써 다음과 같은 기능을 제공합니다.

조직은 이벤트가 인시던트로 확대되기 전에 개입하거나 인시던트가 발생한 경우 신속하게 조치하여 피해를 제한할 수 있습니다.

SIEM 플랫폼의 효과적인 로그 수집, 중앙 집중화, 알림 기능은 사고 대응자에게 필요한 데이터를 제공하여, 무엇이 발생했는지 분석하고 어떤 조치가 필요한지를 판단할 수 있게 합니다. 로그 중앙 집중화는 악의적인 사이버 공격자가 자신의 흔적을 숨기기 위해 이벤트 로그를 수정하거나 삭제하려고 시도하는 경우 매우 중요한 단서가 될 수 있습니다.4

SOAR의 자동화된 대응 기능은 사이버 보안 이벤트 및 사고에 대한 전반적인 대응을 더욱 효과적으로 만들 수 있습니다. SOAR 플랫폼이 사고 대응 담당자를 대체할 수는 없지만, 특정 이벤트 및 사고 대응과 관련된 일부 작업을 자동화함으로써 직원이 이벤트 또는 사고로 인해 발생한 더 복잡하고 가치 있는 문제에 집중할 수 있도록 할 수 있습니다. 또한 SOAR 플랫폼이 대응을 자동화함으로써, 자동화된 공격 기법을 사용하는 악의적 사이버 행위자들과 속도 면에서 경쟁할 수 있는 기반도 마련해 줍니다.

3 Living Off the Land Techniques 식별 및 완화하기| Cyber.gov.au 를 참조하세요.

4 이 기법은 Volt Typhoon campaign에서 관찰되었습니다. 자세한 내용을 확인하세요, 참조: 중국 국가 배후 사이버 활동| Cyber.gov.au.

## 사용 사례: LOTL 위협 탐지 및 대응

악의적인 사이버 공격자들은 종종 운영 체제나 환경의 합법적인 도구와 기능을 활용하여 목적을 달성합니다. LOTL(Living off the Land)로 알려진 이 기법은 탐지 및 방어가 어려울 수 있습니다. 그러나 잘 구현된 SIEM 또는 SOAR 플랫폼은 다음과 같은 방식으로 위협 헌팅 기능을 향상시켜 LOTL 전술, 기술 및 절차(TTP)를 성공적으로 탐지할 수 있습니다:

- 네트워크 디바이스, 엔드포인트 및 기타 시스템에서 로그를 수집하고 중앙 집중화하면 로그 무결성을 유지하는 데 도움이 되고, LOTL TTP를 사용하는 악의적인 사이버 공격자가 네트워크 접속을 유지하기 위해 로그를 수정/삭제하는 것을 방지하며, 환경 내의 모든 활동에 대한 전체적인 관점을 제공할 수 있습니다.
- 수집된 로그를 분석하는 규칙을 구현하면 탐지하는 데 큰 도움이 됩니다:
  - LOTL 스크립팅 작업
  - 명령어나 도구의 실행
  - 환경에서 비정상으로 간주되는 시스템 접근 시도
- SIEM에서 정상적인 사용자 및 애플리케이션 동작을 기준선(Baseline)으로 삼으면 플랫폼이 기준선과의 편차를 분석하여 잠재적인 악의적 활동을 식별할 수 있습니다. SOAR의 머신 러닝 모델을 활용하면 행동 분석을 통해 비정상적인 패턴(도구 실행 빈도 변화, 권한 상승 시도 등)을 탐지하는 대응 역량을 크게 향상시킬 수 있습니다.
- SIEM 또는 SOAR는 위협 인텔리전스 정보를 수집하여 LOTL TTP에 대한 최신 대응을 가능하게 해야 합니다. 로그, 행동 지표, 위협 인텔리전스 피드를 결합하여 상관분석을 수행하면, 사용자 및 시스템의 활동이 합법적인지 악의적인지 판단할 수 있습니다.
- SOAR의 자동화 및 대응 기능은 플레이북을 활용하여 의심되거나 이상행위로 인해 발생할 수 있는 피해를 제한할 수 있습니다. 자동화된 대응 기능의 예로는 시스템 격리, 네트워크 트래픽 분리 또는 차단, 자격증명 해지 등이 있습니다.
- 엔드포인트 탐지 및 대응(EDR) 툴과 같은 다른 기술과 통합된 SIEM 또는 SOAR 플랫폼은 툴, 스크립트 또는 기타 합법적인 툴을 식별하고 차단하여 LOTL 공격에 대한 전반적인 대응력을 향상시킬 수 있습니다.
- LOTL 활동은 식별 및 예방이 어렵기 때문에 시스템이 침해되고 악의적인 사이버 공격자가 의도한 목표를 성공적으로 달성하는 경우가 많습니다. SIEM/SOAR 플랫폼을 구현하면 조직의 LOTL 기법에 대한 탐지, 대응, 복구 능력이 크게 향상됩니다.

# 3. SIEM 및 SOAR 플랫폼 구현의 과제

이 섹션에서는 SIEM/SOAR 플랫폼 도입 여부를 고려 중인 실무자를 위해 몇 가지 주요 과제를 설명합니다. 두 플랫폼 모두 '한 번 설정하고 잊어버리는' 도구가 아닙니다. 이러한 플랫폼은 숙련된 인력이 제대로 구현하고 지속적으로 유지 관리해야만 가시성, 탐지 및 대응 기능을 향상시킬 수 있습니다. 모든 SIEM 플랫폼의 핵심 과제는 로그 소스에서 데이터를 올바르게 수집하고 효과적인 탐지 메커니즘을 구성하는 것입니다. SOAR 플랫폼의 핵심 과제는 특정 이벤트에 대한 효과적인 자동화된 대응 프로세스를 정교하게 조정하는 것입니다.

## 수집된 데이터의 정규화

SIEM은 네트워크 또는 시스템 내의 다양한 소스에서 데이터를 수집, 처리, 분석합니다. 이러한 다양한 소스에는 방화벽, 침입 탐지/방지 시스템(IDS/IPS), 엔드포인트, 애플리케이션 등이 포함될 수 있습니다. 각 소스마다 로그 형식이 다를 수 있기 때문에 로그 분석에 어려움이 있습니다. 조직은 SIEM을 효과적으로 구현하기 위해 다음과 같은 문제를 해결해야 합니다:

- 비정형 로그와 정형 로그 모두에서 데이터를 정확히 파싱 및 추출
- 수집된 모든 로그에서 용어의 표준화(예: "src_ip" 및 "sourceAddress")
- 다른 시간대에 수집된 로그에 대한 시간 동기화를 설정

## 환경 전반의 수집 범위

로그 데이터 수집은 조직 환경의 범위와 위험 평가 우선순위도 고려해야 합니다. 예를 들어, 조직에서 12개의 AD(Active Directory) 서버 중 10개에만 로그/데이터 복제 메커니즘을 배포한 경우, SIEM 플랫폼은 나머지 2개 AD 서버에서 발생하는 이벤트를 수집하지 못하므로 해당 영역에 '사각지대'가 발생합니다.

반대로, 조직이 위험 평가 프로세스를 통해 SIEM 플랫폼이 조직의 데스크톱 플랫폼 중 특정 비율의 데스크톱 활동만 수집하도록 수용하는 경우, 이 같은 데스크탑 활동을 대표하는 샘플링 방식을 선택할 수 있습니다.

### 로그 중앙 집중화 대 로그 분석

SIEM 플랫폼을 주로 로그 중앙 집중화 도구로 사용하는 경우 대량의 로그 소비가 발생할 가능성이 높습니다. SIEM을 이러한 목적으로 사용해서는 안 됩니다. 규정 준수나 감사를 위한 로그 중앙 집중화가 주된 목적이라면 조직은 보다 적합한 다른 도구를 사용할 수 있습니다. 데이터 레이크 및 대체 저장 메커니즘을 활용하여 보안이벤트, 위협 또는 인시던트를 식별하는 데 직접적인 가치를 제공하지 않는 로그를 별도로 중앙화하는 것이 바람직합니다.

이러한 방식이 경제적이며 보안팀은 SIEM을 통해 필요한 로그만 선별 수집할 수 있도록 지원하여 불필요한 로그 필터링 작업을 줄일 수 있습니다.

또한 SIEM 플랫폼을 모든 로그의 중앙 저장소로 취급할 경우 보안 목적에 특화된 로그 분석의 효과는 오히려 저하될 수 있습니다. (자세한 내용은 아래 참조)

# 효과적인 로그 분석 달성

효과적인 로그 분석을 구현하려면, SIEM 플랫폼을 조직의 고유한 IT 환경과 비즈니스 요구 사항에 맞게 신중하게 구성되어야 합니다. 분석이 효과적으로 수행되려면 SIEM은 다음 두가지를 모두 충족해야 합니다:

- True Positive: 실제 이벤트 또는 사고 발생시 경고를 생성함
- True Negative: 이벤트나 사고가 없을 때는 경고를 생성하지 않음

이를 위해서는 SIEM이 적절한 유형과 양의 로그 데이터를 수집 및 중앙화하고, 이에 맞는 규칙과 필터가 설정되어야 하며, 이러한 작업은 전문인력에 의해 지속적으로 수행되어야 합니다. 이러한 구성과 조정은 단발성 작업이 아니라, 환경 변화, 플랫폼 기능 업데이트, 위협 지형 변화 등에 따라 지속적으로 유지·조정되어야 하는 장기적인 과업입니다.

반면, 수집되는 데이터가 불완전하거나 일관되지 않거나, 적용된 규칙 및 필터가 과도하게 둔감할 경우, False Negative(실제 이벤트나 사고가 발생했음에도 경고가 생성되지 않음)가 발생할 수 있습니다. 이는 탐지 및 대응 측면에서 심각한 리스크를 야기할 수 있으며, 보안 팀이 SIEM 경고에 과도하게 의존할 경우 문제가 더욱 심화됩니다.

또한, SIEM이 과도한 양의 로그를 수집하고, 과도하게 민감한 규칙 및 필터를 적용할 경우, False Positive(실제 이벤트가 아님에도 경고가 생성됨)가 빈번하게 발생할 수 있습니다. 이러한 과다 경고는 보안 팀에 '알림 피로(Alert Fatigue)'를 유발해 실제 이벤트에 대한 대응이 지연되거나 누락될 위험을 증가시킵니다.

이러한 불균형은 실제로 흔히 발생하는 문제로, 많은 보안 팀이 로그 데이터를 과다하게 수집하고 중앙화하려는 경향을 보이기 때문입니다. 이는 결과적으로 효과적인 규칙 및 필터의 개발을 어렵게 만듭니다.

SIEM이 효과적인 로그 분석을 수행하도록 구성되지 않은 경우, 해당 SIEM과 연동된 SOAR 플랫폼의 기능 또한 저하될 수 있으며, 이는 중대한 운영상 영향을 초래할 수 있습니다.

자세한 로그 수집 우선순위에 대한 실무자 가이드는 본 시리즈의 관련 문서인 'SIEM 및 SOAR 플랫폼 구현-실무자 지침편'(Implementing SIEM and SOAR platforms: Practitioner guidance)를 참고하시기 바랍니다.

# 대응 자동화의 위험

SOAR 플랫폼 역시 조직의 고유한 환경에 맞게 신중하게 구성되어야 하며, 이를 위해 다양한 전문 기술 인력이 필요합니다. 여기에는 다음과 같은 역할이 요구됩니다:

- 보안 전문가: 어떤 대응 절차를 자동화할지 식별
- 플랫폼 엔지니어: 자동화 로직 설계
- 개발자: 자동화된 대응이 자체 개발 시스템 또는 서비스에 어떤 영향을 미칠지 판단
- 법무/준법/리스크/컴플라이언스 전문가: 자동화 대응과 관련된 법적·규제적 리스크 평가

SOAR의 자동화 대응 기능이 제대로 구성되지 않고 유지관리되지 않는 경우, 일반 사용자나 시스템의 정상적인 행동을 보안 이벤트로 잘못 인식하고 자동으로 격리·차단 조치를 취할 수 있습니다. 이로 인해 서비스 제공에 다양한 수준의 지장이 발생할 수 있습니다.

또한, 조직 내 구성원이 자동화된 대응 기능에 대한 신뢰가 부족하거나, SOAR를 장기적으로 운영할 전문성과 자신감이 부족한 경우, 고비용으로 도입한 SOAR가 방치될 가능성도 존재합니다.

이러한 이유로 SOAR 플랫폼은 일반적으로 미성숙한 환경, 즉 기존 SIEM이 없거나 SIEM 기능이 초기단계에 있거나 숙련된 보안 팀이 부족한 환경에는 적합하지 않습니다. 일반적으로 SIEM 플랫폼을 올바르게 구현하고 효과적인 로그 분석을 달성하는 데 투자하는 것이 SOAR를 구현하는 것보다 우선 순위가 높습니다.

# 자원 소모

SIEM/SOAR 플랫폼을 올바르게 구현하려면 상당한 비용이 지속적으로 발생합니다. 여기에는 다음이 포함될 수 있습니다:

- 플랫폼의 선불 및 지속적인 라이선스 또는 데이터 사용 비용
- SIEM/SOAR 구현하는데 필요한 전문 기술을 갖춘 직원을 고용하고 유지하는 데 드는 비용
- 기존 인력 역량 강화에 드는 초기 교육 비용
- 기술, 환경 및 위협이 계속 변화함에 따라 직원들이 플랫폼을 유지하고 시간이 지남에 따라 플랫폼을 성숙시킬 수 있도록 직원 교육에 지속적으로 투자하는 데 드는 정기 교육비용
- 거버넌스 및 플랫폼 유지 관리와 관련된 지속적인 비용
- 조직이 구축을 아웃소싱하는 경우 도입 및 개선 작업에 대한 서비스, 유지관리 비용,

구성 및 유지 관리를 아웃소싱하는 데는 많은 비용이 들 수 있습니다. 민감한 정보를 관리하거나 중요하거나 고유한 서비스를 제공하는 조직의 경우 규제 준수 및 안정적 서비스 제공 측면에서 사내 역량을 개발하는 것이 더욱 적합합니다.

내부 직원은 네트워크에 대한 이해도가 높기 때문에 네트워크에서 비정상적이거나 의심스러운 활동을 식별하는 데 매우 유용할 수 있습니다. 외부 서비스 제공업체가 쉽게 식별할 수 있는 '항상 비정상적인' 활동이 있는 반면, 환경에 대한 심층적인 지식이 없으면 미묘한 활동은 눈에 띄지 않을 수 있습니다.

또한 보안팀은 내부자 위협을 방지하거나 자격 증명 도용을 조사하기 위해 네트워크에서 사용자의 행동에 대해 직접 문의하고 조사할 수 있는 권한이 있어야 합니다. 이를 통해 내부자 위협 및 자격 증명 도난 사고를 선제적으로 탐지할 수 있습니다.

반면 외부 위탁시에는 가시성 부족, 작업 중복 및 커뮤니케이션 오류 등을 초래할 수 있습니다. 아웃소싱을 선택하는 경우 조직의 요구 사항에 가장 적합한 다양한 SIEM/SOAR 공급업체를 조사할 것을 권장합니다.

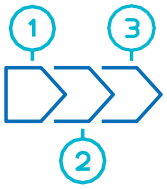
SIEM/SOAR 플랫폼의 구성 및 유지 관리를 아웃소싱하지 않고 내부에서 수행하려는 조직은 복수의 전담 인력을 상시배치 할 수 있어야 합니다. 또한 SIEM을 운영하려면 장기간에 걸쳐 스트레스가 많은 작업을 수행해야 하므로 이에 대한 인적 지원 체계도 병행되어야 함을 유념해야 합니다.

# 4. SIEM/SOAR 구현을 위한 모범 사례 원칙

이 섹션에서는 SIEM/SOAR 플랫폼을 구현하는 각 단계(조달, 구축 및 유지 관리)에서 실무자가 참조할 수 있는 11가지 모범 사례 원칙을 제공합니다.

## 조달

1. 조직의 SIEM/SOAR 구현 범위를 명확히 정의하십시오.
2. 데이터 레이크 아키텍처를 갖춘 SIEM 제품을 고려해 보십시오.
3. 여러 소스의 데이터를 상관 분석할 수 있는 SIEM 제품을 고려해 보십시오.
4. 다양한 제품의 숨겨진 비용(라이선스, 스토리지 등)을 찾아보십시오.
5. 기술뿐 아니라 교육에도 투자하십시오.




## 수립

6. 네트워크에서 일상적인 업무 활동의 기준선을 설정하십시오.
7. 로그 수집에 대한 표준지침을 개발하십시오.
8. SIEM을 조직의 엔터프라이즈 아키텍처에 통합하십시오.

## 유지관리

9. 위협 탐지 성능을 지속적으로 평가하십시오.
10. 사전 처리를 통해 불필요한 로그 수집을 줄이십시오.
11. SIEM/SOAR의 성능을 테스트하십시오.

# 조달 원칙

다양한 SIEM/SOAR 제품 중에서 선택할 때, 실무자는 사용 가능한 리소스에 따라 조달 단계에서 다음 원칙을 참고해야 합니다.

## 1. 조직의 구현 범위를 명확히 정의하기

SIEM/SOAR 플랫폼에 투자하기 전에 조직은 플랫폼 구현을 위한 개념 증명(POC)을 개발해야 합니다. 조직마다 SIEM/SOAR 플랫폼 구현을 위한 POC의 정의가 다를 수 있습니다. 하지만 철저한 POC를 통해 조직은 구현 중에 예기치 않은 문제나 지연으로부터 조직을 보호하는데 도움이 됩니다.

먼저, 조직은 SIEM/SOAR 구현을 위한 POC의 범위를 파악해야 합니다. POC는 특정 비즈니스 영역 또는 주요 위험 또는 위협 모델을 해결하는 데 초점을 맞출 수 있습니다. 또한 사용 가능한 공급업체가 이러한 주요 기술 및 운영 요구 사항을 충족하는지 또는 초과하는지 여부도 고려해야 합니다. 처음에 범위를 올바르게 파악하면 전사적으로 작동 가능한, 종단간(end-to-end) POC를 성공적으로 수행할 수 있습니다.

책임 있는 시스템 운영자를 파악하는 것은 아래 나열된 질문에 답하는 데 필수적입니다. 인증 기관은 플랫폼 유지 관리를 담당하는 팀의 일원이 시스템 운영자가 될 것을 권장합니다. 또한 시스템 운영자는 거버넌스 또는 기술 변경을 감독하고 승인하는 거버넌스 역할도 담당합니다. (원칙 8 참조)

SIEM/SOAR 플랫폼 구현을 위한 POC를 설계할 때 검토해야 할 주요 질문들:

- SIEM/SOAR 구현의 주요 목적은 무엇인가?
- 구현 과정 및 결과와 관련된 이해관계자는 누구인가?
- 구현을 통해 어떤 리스크, 위협 및 사용 사례를 해결할 것인가?
- 어떤 데이터 소스를 우선적으로 수집할 것인가?
- SSO, API 연계, 기존 보안 도구 등 외부 시스템과의 통합**이 구현에 장애가 될 가능성은 없는가?
- 플랫폼을 온프레미스(On-premise)로 구축할 것인가, 아니면 SaaS(Software as a Service)로 도입할 것인가?
- 온프레미스, 하이브리드, 클라우드 또는 멀티 클라우드 아키텍처와 어떤 통합이 필요한가?
- 플랫폼의 지속적인 유지 관리를 포함한 구현은 어느 팀에서 담당하나?
- 플랫폼을 운영할 보안 분석가 및 엔지니어를 포함한 인적 자원이 몇 주 동안 구현 작업에 투입 가능한가?
- 가용 인력이 구현에서 맡은 역할에 맞는 충분한 전문성을 갖추고 있나?
- 공급업체의 지원이 충분한지, 혹은 다른 전문 서비스 업체의 추가 지원은 가능한지?
- 최종 구현에 대한 책임자는 누구인가?
- 조직에 기존 사고 대응 프로세스(IR 프로세스)가 마련되어 있는가?

위의 질문 외에도 시스템 운영자는 SIEM 플랫폼 구현을 위한 POC가 다음을 충족하는지 확인해야 합니다:

- 조직 특화된 로그 수집 요건을 반영하고, 필요한 이벤트를 기록하도록 최종 장치(end device)를 설정하며, 포워더(forwarder) 가 해당 로그를 탐지하도록 구성되었는지 확인할 것
- 보안을 최우선으로 고려하고, 로그 수집은 보안 피드(security feeds)에 한정할 것.
- 잠재적 이벤트 및 인시던트에 관련된 검색(query) 및 앱 실행이 이뤄질 것.

새로운 로그 소스는 기존 로그 소스가 다음 사항을 기준으로 감사된 이후에만 추가할 것:

- POC의 성공 여부를 판단하기 위한 평가 절차를 포함해야 합니다. 이 절차는 플랫폼을 실제로 운영하거나 사용하는 보안 분석가 및 엔지니어, 또는 최종 사용자들의 피드백이 평가에 반영될 수 있도록 구성되어야 합니다. 최종 사용자 피드백의 요소는 다음과 같은 항목을 포함해야 합니다: 사용자 인터페이스(UI), 조사 및 분석 워크플로우, 자동화 기능 등의 사용 경험.

인증 기관은 SIEM을 구현하는 조직이 초기 라이선스 및 스토리지/컴퓨팅 요구 사항에 대해 다음 데이터 수집 표를 고려할 것을 권장합니다:

| 조직 인력 배치 | 최소 | 제안사항 |
|---|---|---|
| <50(최소한의 조직) | 50GB | 200GB |
| 50-400(소규모 조직) | 150GB | 300GB |
| 400-2000(중간 규모 조직) | 250GB | 600GB |
| 2000-5000(중규모/대규모 조직) | 500GB | 1.5TB |
| >5000(대규모/포트폴리오 조직) | 1TB | 2.5TB |

## 2. 데이터 레이크 아키텍처를 갖춘 SIEM 제품 고려하기

여러 SIEM 제품 중에서 선택할 때는 데이터 레이크(data lake) 아키텍처를 내장했거나 내장 가능한 제품을 고려할 것을 권장합니다. SIEM 제품마다 아키텍처 패턴은 상이하며, 아키텍처는 데이터 전파 방식, 로그 중앙화 방식, 정보 접근 권한 제한 방식을 결정하여 해당 SIEM의 활용 가능성을 좌우하게 됩니다.

SIEM 내의 데이터 레이크 아키텍처에는 모든 보안 관련 로그가 로그 리포지토리에 복제되어 있습니다. SIEM은 자체 피드를 수신하는 대신 이 리포지토리에서 분석용 로그를 가져옵니다. 로그 리포지토리는 데이터의 무결성과 기밀성을 유지하기 위해 적절하게 보안이 유지되어야 합니다. 조직은 로그 보호를 개선하기 위해 로그 리포지토리와 SIEM 플랫폼을 분리된 모니터링 영역(예: 로그 트래픽만 허용하는 영역)에서 호스팅하는 것도 고려할 수 있습니다. 그러나 SOAR 플랫폼을 분리된 모니터링 영역에서 호스팅하면 대응 조치(remediation action) 수행에 제약이 생길 수 있습니다.

데이터 레이크 아키텍처에 대한 자세한 정보를 포함하여 일반적인 SIEM 아키텍처 패턴에 대한 설명은 부록A를 참조하세요.

## 3. 여러 소스의 데이터를 상호 연관시킬 수 있는 SIEM 제품을 고려하기

저작 기관들은 또한 다양한 출처의 로그 데이터를 분석하고 상관 분석할 수 있는 SIEM 플랫폼을 고려할 것을 권장합니다. 이러한 출처에는 기존 레거시 IT 시스템뿐만 아니라 클라우드 환경도 포함되며, 조직 내 다양한 네트워크 환경에서 생성되는 데이터를 아우릅니다.

조직은 사이버 위협 인텔리전스(Cyber Threat Intelligence) 피드와 같은 외부 데이터 소스를 분석에 통합할 수 있는 기능과 보안 매개변수를 갖춘 SIEM을 우선적으로 고려해야 합니다.

또한, 선택한 SIEM 플랫폼이 예상되는 워크로드를 안정적으로 처리할 수 있는지, 그리고 기존 보안 운영 체계에 원활하게 통합될 수 있는지도 반드시 확인해야 합니다.

※ 참고: 모든 로그를 SIEM 플랫폼에 수집하는 것은 비용 부담이 클 수 있으므로, 로그 관리 및 통합에 따른 비용도 고려해야 합니다. 저작 기관은 SIEM 수집을 위한 우선 로그: 실무 가이드(Priority logs for SIEM ingestion: Practitioner guidance) 문서에서 로그 수집 대상 선정에 대한 추가 지침을 제공하고 있습니다. 이 가이드는 위협 중심(threat-led) 접근 방식을 기반으로, 보안성과 비용의 균형을 고려해 선택적으로 로그를 수집할 것을 권장합니다. 예를 들어, 동일한 이벤트 ID 및 로그를 활용하는 EDR(Alert 기반 엔드포인트 탐지 및 대응) 경보는 우선 수집 대상으로 권장됩니다.

## 4. 다양한 제품의 숨겨진 비용 찾기

SIEM 및/또는 SOAR 플랫폼 도입을 고려하는 모든 조직은 초기 비용뿐만 아니라 지속적인 운영 비용까지 포함한 총소유비용(TCO, Total Cost of Ownership)을 사전에 충분히 계획해야 하며, 일부 제품 및 서비스에 포함된 숨은 비용(위의 '자원 소모' 항목 참조)도 꼼꼼히 확인해야 합니다. 이러한 플랫폼 중 일부는 동일한 공급업체에서 만든 다른 제품과 통합되도록 설계되어 있어 전체 보안 기능을 사용하려면 다른 제품을 구매해야 합니다. 단일 공급업체의 IT 제품이 집중되어 있으면 단일 장애 지점(Single Point of Failure)이 발생할 수 있으며, 그 결과 해결에 많은 비용이 소요될 수 있습니다. 또한 선택한 플랫폼이 공급업체의 제품군 외부에 있는 제품의 로그를 통합하는 데 어려움을 겪는다면 환경에 대한 완전한 가시성을 확보하기 어려울 수 있습니다. 이는 여러 공급업체의 제품과 레거시 IT가 포함된 네트워크의 경우 중요한 문제입니다. 결국, 잘못된 제품 선택으로 인해 조직은 다른 공급업체로 전환해야 할 수 있으며, 이는 매우 큰 비용을 초래할 수 있습니다.

부 제품은 경쟁력 있는 라이선스 가격을 제시하지만, 실제 구축 또는 타 벤더로부터의 마이그레이션 비용이 매우 높아 실질적인 비용 부담이 더 커질 수 있습니다. 일반적으로 SIEM 라이선스 비용은 전체 도입 비용의 일부에 불과합니다.

대부분의 SIEM은 로그 수집량 기준 과금 모델을 따릅니다. 일부 라이선스는 일정량의 로그를 무료로 제공하지만, 다른 경우는 사전에 구매한 로그량에 따라 수집이 제한되며, 로그 수집량에 제한이 없는 라이선스의 경우에는 수집량이 많아질수록 과도한 비용이 발생할 수 있습니다. 이러한 경우, 조직은 수집을 신중하게 관리하지 않으면 매우 큰 비용이 발생할 수 있다는 점을 염두에 두어야 합니다. 특히 일부 SIEM 플랫폼의 기본 설정 또는 권장 설정은 로그 수집량을 증가시키는 경향이 있어, 이에 대한 주의가 필요합니다.

또한, SIEM/SOAR 플랫폼의 구축 및 유지관리 작업을 외부 업체(예: MSP, 외부 계약사)에 아웃소싱할 경우에도 단일 실패 지점 및 추가 비용 발생 위험이 존재합니다. 아웃소싱 시에는 다음 사항들을 사전에 고려해야 합니다:

"데이터 저장 및 분석의 지리적 위치, 해당 위치에 적용되는 규제 요건, 외부 업체가 보안 인력 교육이나 쿼리 실행 등 추가 서비스 비용을 청구하는지 여부"

이와 같은 요소들을 종합적으로 고려하여 도입 여부 및 벤더 선정 결정을 내려야 합니다.

하지만 조직이 초기 SIEM/SOAR 플랫폼을 신중하게 선택하거나 새로운 벤더로 전환할 때 충분한 검토를 거친다면, 이는 장기적인 보안 투자로 이어지며 예기치 못한 비용을 상쇄할 수 있는 가치를 제공하게 됩니다.

### 5. 기술뿐 아니라 교육에 투자하기

SIEM/SOAR 플랫폼을 통해 가시성, 탐지 및 대응을 향상시키려면 특히 숙련되고 헌신적인 인력이 필요합니다. 섹션 3에서 설명한 것처럼 일부 조직에서는 플랫폼의 구축 및 유지 관리를 아웃소싱하는 것이 적합하지 않을 수 있습니다. 이는 현재 직원의 스킬을 향상시키고 멘토링할 수 있는 좋은 기회입니다.

SIEM/SOAR 플랫폼을 조달하고 사내 역량을 개발하려는 모든 조직은 플랫폼 구현을 위한 직원 교육에 상당한 자원을 투입할 계획을 세워야 합니다. 즉, 플랫폼을 구축하고 유지 관리할 수 있는 기술을 갖출 수 있도록 직원 교육에 선행 투자를 해야 합니다. 또한 조직은 기술, 환경 및 위협이 지속적으로 변화함에 따라 직원들이 자신의 기술을 검증하고 플랫폼을 유지 및 성숙시킬 수 있도록 지속적으로 교육 비용을 지불해야 합니다.

기본 교육 주제에는 다음이 포함되어야 합니다:

- 플랫폼 유형과 같은 SIEM 기본 사항
- 로깅 기본 사항
- 로그 조작 및 필터링
- 쿼리 및 검색
- 로그 분석 및 조사
- 공격 프레임워크 및 전술, 기법, 절차(TTP)(예: MITRE ATT&CK5)
- 알림 및 보고
- 대시보드 구축
- SIEM 데이터 피드 및 인덱스의 상태를 유지합니다.

## 수립 원칙

작성 기관은 실무자가 SIEM/SOAR 플랫폼의 구축 단계에서 다음 원칙을 참조하여 조직의 고유한 환경에 맞게 플랫폼을 초기에 구성하고 구현을 위한 표준 및 프로세스를 만들 것을 권장합니다.

### 6. 네트워크에서 평소와 같은 비즈니스 활동의 기준선 설정하기

로그 데이터를 수집, 중앙 집중화 및 분석하기 위해 SIEM을 배포하기 전에 보안팀은 네트워크의 일상적인 업무(BAU) 활동의 기준선을 설정해야 합니다. 기준선을 설정하려면 설치된 도구와 소프트웨어, 계정 동작, 네트워크 트래픽, 서비스 메시, 시스템 상호 통신 내역을 점검해야 합니다. SIEM은 정상적인 네트워크 활동의 정확한 기준선이 설정되어야만 보안팀에 사이버 보안 이벤트 및 인시던트를 효과적으로 알릴 수 있습니다.

기준선은 하루아침에 만들어지지 않습니다. 오히려 조직의 복잡성에 따라 최소 몇 주에 걸쳐 로그를 수집하고, 쿼리를 개발하고, 비정상적인 사용자 활동을 조사하고, 알림을 필터링 및 조정하여 보안팀이 일상업무 패턴에 대한 감을 잡을 때까지 개발됩니다. 기준선을 설정하는 동안 시스템이 이미 손상된 경우 악의적인 활동이 정상으로 받아들여질 위험이 큽니다. 작성 기관은 다음과 같은 기간 동안 베이스라인을 통해 해당 업무 활동이 실제로 정상인지 여부를 철저하게 검증할 것을 권장합니다.

---

5 MITRE 및 MITRE ATT&CK는 MITRE Corporation의 상표입니다.

일단 기준선이 설정되면 네트워크의 변화를 반영하기 위해 지속적으로 유지 관리해야 합니다. 보안팀은 네트워크에서 폐기되거나 추가되는 자산과 사용자 행동 패턴의 변화를 알고 있어야 합니다. 예를 들어, 쿼리 실패 시 리포트가 생성되지 않는 경우가 종종 있습니다. 이를 "탐지할 사건이 없음"으로 잘못 해석할 수 있습니다. 실제로는 기준선이 현실을 반영하지 못해 SIEM이 이벤트를 식별하지 못하는 것일 수 있습니다.

작성 기관은 기준선을 정기적으로 검토하고 엔터프라이즈 아키텍처 프로세스를 통해 임시 수정(ad hoc amendment)할 수 있는 내부 프로세스를 수립할 것을 권장합니다. (원칙 8 참조)

조직은 베이스라인 원칙 외에도 베이스라인을 검증하고 TTP와 같은 다른 헌팅 기법을 도입하는 위협 헌팅 프레임워크를 구축할 수 있습니다. 위협 헌팅은 기준선이 모든 악성 행위를 누락하는지 테스트하고 새로운 공격 방법이 조직의 환경에 영향을 미칠 수 있는지 여부를 판단하는 한 가지 방법입니다. 조직의 위협 헌팅 프레임워크에는 위협 인텔리전스가 포함되어야 하며, 이를 통해 최신 침해지표와 공격자 TTP를 모사하고 탐지하는 것이 바람직합니다.

## 7. 로그 수집에 대한 표준 개발하기[6]

SIEM 시스템 운영자는 애플리케이션 및 시스템에 대한 사전 정의된 기준 로그 수집 요구사항을 보유해야 합니다. 또한, 필요 시 추가 로그 수집을 활성화하거나 비활성화할 수 있도록 해당 기준에서 벗어나는 사항에 대한 승인 절차를 마련해야 합니다. 과도한 수준의 로그 수집은 장비 성능 저하, 로그 저장소 및 SIEM 성능 저하, 네트워크 트래픽 증가를 유발할 수 있습니다. 이에 따라, 조직은 이러한 영향 최소화를 위해 벤더 문서를 참고하여 대체 로그 옵션을 검토해야 합니다.

시스템에서 로그가 생성되지 않는 상황은 조직 입장에서 위험 신호로 간주되어야 합니다. 조직은 시스템이 로그 및 텔레메트리를 생성하지 않게 되었을 때 이를 식별할 수 있는 프로세스를 갖추어야 하며, SIEM 플랫폼은 실시간 및 이력 로그뿐만 아니라, 기타 텔레메트리 데이터에 대해서도 침해 지표(IOC)와 일치하는 항목을 분석할 수 있도록 구성되어야 합니다.

조직은 로그 보존 및 아카이빙 정책을 구현해야 합니다. 로그를 보존해야 하는 기간은 조직의 다양한 특수 요인에 따라 달라지며, 보존하는 동안에는 항상 접근 가능한 상태로 유지되어야 합니다. 보안 측면에서 보존 기간은 조직의 위협 탐지 평균 시간(MTTD)을 고려해야 하며, 위협을 빠르게 탐지할 수 있다면 짧은 보존 기간도 가능할 수 있습니다.

또한, 사이버 보안 사고 조사 지원을 위해 로그가 충분 기간 동안 유지되어야 하며, 보존 정책에는 가치가 없어진 로그나 보존 기간이 지난 로그에 대해 삭제/정리/폐기하는 방식도 포함되어야 합니다. 이와 함께, 조직은 법적/규제적 로그 보존 요구사항이 적용될 수 있으므로 관련 내용을 함께 반영해야 합니다.

작성 기관은 각 조직의 위험 프로파일 및 규제 요건에 맞게 보존 기간을 맞춤화할 것을 권장합니다. 탐지 기능이 새롭게 도입되는 조직의 경우, 다음과 같은 기준을 참고할 수 있습니다:

관리자 및 보안 관련 이벤트 로그: 최소 1년 보존

기타 정보성 로그(이벤트 문맥 파악용): 최소 90일 보존

조직은 또한 네트워크 방어자가 보안 사고를 정확히 식별할 수 있도록, 고품질·고신뢰성의 사이버 보안 이벤트를 중심으로 이벤트 로그 수집 정책을 수립하는 것이 바람직합니다. 유용한 이벤트 로그는 보안 담당자가 이상 징후를 평가하고, 오탐(false positive)과 실제 위협(true positive)을 명확히 구분하는 데 도움을 줍니다.

로그 수집 전략에 대한 자세한 내용은 다음을 참조하세요.
Priority logs for SIEM ingestion - Practitioner guidance | Cyber.gov.au

6 https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and_administration/gateway-hardening/gateway-security-guidance-package-gateway-operations-manag

### 8. SIEM을 조직의 엔터프라이즈 아키텍처에 통합하기

SIEM 시스템 운영자는 네트워크의 모든 신규 데이터 소스 및 변경된 데이터 소스에 대해 계속 인지하여 SIEM이 모든 관련 로그 데이터를 효과적으로 수집할 수 있도록 해야 합니다. 따라서 시스템 운영자는 조직의 엔터프라이즈 아키텍처 그룹 및 변경 제어 위원회의 상시 구성원으로 참여해야 합니다. 또한 SIEM 구현을 담당하는 팀은 IT 관리자와 정기적으로 협업을 유지하여 IT 시스템이 최적으로 조정되도록 해야 합니다.

최적의 튜닝에는 자산 관리(예: SIEM이 새로운 자산에 대한 가시성을 확보하는 것) 및 행동 모니터링(예: 더 이상 네트워크에 액세스할 수 없거나 네트워크의 특정 부분에 액세스해서는 안 되는 사용자의 활동을 SIEM이 경고하도록 하는 것)이 포함될 수 있습니다.

또한, 준법(컴플라이언스) 목적으로 특정 로그 수집을 결정한 IT 관리자의 판단은 SIEM의 기능에 영향을 줄 수 있습니다. SIEM이 수집하는 로그의 품질이 낮을수록, SIEM의 분석 결과도 덜 유용하게 됩니다. 보안 팀은 또한 SIEM의 가시성에 영향을 줄 수 있는 주요 인프라 변경 결정(예: 클라우드 도입)에 대해 사전 인지하고 의견을 제시할 수 있어야 합니다.

보안 팀이 개발자와 함께 협업하여, 신규 시스템 또는 제품이 유용한 보안 로그를 생성하도록 설계하는 것이 중요합니다. 이러한 준비는 보안 사고 발생 시 로그 접근 및 분석 시간을 단축하는 데 도움이 됩니다.

또한 조직은, 새로 도입된 시스템의 모든 로그를 SIEM에 자동으로 전송하는 것이 항상 적절하다고 가정해서는 안 됩니다. 신규 시스템과 그로부터 생성되는 로그 데이터는 비정상 네트워크 활동 식별에 기여할 수 있는 가치 여부를 분석한 후 SIEM에 연동 여부를 결정해야 합니다. 예를 들어, 신규 애플리케이션이 기존 그룹 정책을 통해 인증 메커니즘을 사용하는 경우, 해당 인증 이벤트는 이미 SIEM으로 전송되고 있을 수 있습니다.

## 유지 관리 원칙

실무자는 SIEM/SOAR 플랫폼 수명의 유지 관리 단계에서 다음 원칙을 참조하여 플랫폼을 지속적으로 조정하고 시간이 지남에 따라 탐지 및 대응 기능을 성숙시켜야 합니다.

### 9. 위협 탐지를 지속적으로 평가하기

SIEM 플랫폼이 배포된 이후, 조직은 해당 플랫폼의 경보(alert) 메커니즘을 정기적으로 점검 및 튜닝하는 절차를 수립해야 합니다. 저작 기관의 기존 권고에 따라, 조직은 MITRE ATT&CK 단계와 연계된 표준화된 경보 명명 규칙(naming convention)을 적용하는 방안을 검토해야 하며, 이를 통해 보안 사고 대응 및 분류 속도를 높일 수 있습니다. 모든 경보 규칙(alert rule)은 조직의 위협 모델(threat model) 및 위험 프로파일(risk profile)을 반영해야 하며, 이에 따라 지속적으로 조정(tuning)되어야 합니다.

위협 모델이 변화하면, 이에 따라 탐지 역량(detection capabilities) 또한 조정되어야 합니다. 예를 들어, 조직의 주요 업무 프로세스가 기존 레거시 시스템에서 지원되는 최신 플랫폼으로 이전되는 경우, 해당 변경 사항이 SIEM 설정에 반영되어야 합니다. 위협 탐지 역량을 평가하는 과정에서, 기존의 불필요한 경보 규칙을 폐기하거나, 새로운 경보 규칙을 테스트해야 할 필요성이 제기될 수 있습니다. 이러한 탐지 규칙은 위협 모델이 요구하는 새로운 보안 요구사항을 충실히 반영해야 합니다.

또한, 조직은 사용 사례 분석(use case analysis)을 위해 MaGMa(Management, Growth and Metrics assessment)와 같은 보다 체계적인 평가 프레임워크의 도입을 검토할 수도 있습니다.

---

7 https://www.betaalvereniging.nl/wp-content/uploads/FI-ISAC-use-case-framework-verkorte-versie.pdf

## 10. 사전 처리를 통한 불필요한 로그 수집 감소시키기

앞서 설명한 바와 같이 과도한 로그 수집은 SIEM을 구현할 때 흔히 발생하는 문제입니다. 너무 많은 로그를 수집하면 비용이 많이 들고, 오탐 경보가 발생할 수 있으며, 플랫폼의 데이터 처리 용량에 부담을 주어 성능이 지연되거나 저하될 수 있습니다. 보안 분석에 필수적인 정보에 초점을 맞춘 사용자 정의 파싱 규칙을 구현하면, 로그에서 필요한 필드만 추출하여 수집되는 데이터의 양을 줄이는 데 도움이 됩니다.

조직은 이러한 문제 발생 가능성을 줄이기 위해, 로그가 SIEM에 수집되기 전에 사전 처리(pre-processing)하는 절차를 적용해야 합니다. 사전 처리는 다음 세 가지 지점 중 하나에서 수행될 수 있습니다:

원본/호스트(Source/Host), 포워더/복제기(Forwarder/Replication), SIEM 수집 지점(SIEM Ingestion)

각 지점에 대한 자세한 설명은 부록 B를 참조하세요.

## 11. SIEM/SOAR의 성능을 테스트하기

조직은 SIEM 및/또는 SOAR 플랫폼의 성능을 테스트하기 위한 연습 시나리오를 수행해야 합니다. 이러한 테스트는 내부 보안팀이 수행하거나, 모의 해킹(Penetration Test) 업체 등 외부 서비스 제공자가 수행할 수 있습니다.

SIEM 성능을 향상시키기 위해서는, 로그 수집 및 처리 파이프라인 상의 병목 현상(bottleneck)이 없는지 확인하는 것이 필수적입니다. 이러한 플랫폼을 테스트해야만, 보안팀은 다음 사항을 확신할 수 있습니다:

필요한 로그가 실제로 생성되고 있는지, 해당 로그가 SIEM에 수집되고 있는지, SIEM이 정확한 탐지 결과(True Positive/True Negative)를 제공하는지, SOAR가 경보(alert)에 따라 적절히 조치하고 있는지

조직은 비즈니스 목표의 변화 및 신규 위협에 대응하기 위해, 플랫폼 성능을 지속적으로 평가해야 합니다.

또한 조직은 시간 경과에 따른 탐지력 향상 추적을 위해, 잘 알려진 TTP(전술·기술·절차)를 활용한 정기 테스트를 계획해야 하며, 신규 공격 벡터에 대한 임시 테스트(ad hoc)와의 균형도 맞춰야 합니다.

테스트의 주요 영역은 다음과 같습니다:

- Active Directory 및 PowerShell 변경 탐지
- LSASS.exe 덤프와 같은 일반적인 공격 기술
- Golden Ticket, Living Off the Land, DCSync 활동 감지
- 명령 및 제어(C2) 활동/의심스러운 도메인으로의 비정상적인 트래픽 탐지
- 네트워크 내부에서 네트워크 스캐닝/정찰 활동 탐지

이러한 공격과 Active Directory 변경 모니터링의 중요성에 대한 자세한 내용은 다음을 참조하세요.

Detecting and Mitigating Active Directory Compromises를 참조하세요.

# 부록 A: SIEM 아키텍처 패턴

다음 접근 방식은 SIEM 플랫폼의 일반적인 아키텍처입니다. 다음 예에서 '로그 리포지토리(Log Repository)'는 데이터 레이크 또는 S3 버킷과 같이 로그를 중앙 집중화하기 위한 일반화된 위치를 의미합니다. '소스(Source)'는 환경 내의 데이터 소스를 의미합니다. '현재(Current)'는 최근 로그의 저장소 또는 피드를 의미하며, '이전(Old)'은 이전 로그의 저장소 또는 피드를 의미합니다.

로그 리포지토리에는 아래 그림과 같이 여러 가지 용도가 있습니다. 일반적으로 로그의 원본 또는 복제된 사본을 로그 리포지토리로 보내는 것은 조사에 매우 중요합니다. 그 이유는 다음과 같습니다. SIEM 또는 기타 로그 처리 도구를 통한 가공과정에서 로그 무결성을 손상시킬 수 있으며, 원본 데이터 소스는 제한된 기간 이후에는 삭제될 수 있기 때문입니다.

## 1. 데이터 레이크 또는 리포지토리 우선 접근 방식

작성 기관에서 권장하는 접근 방식은 데이터 소스에서 SIEM으로 직접 로그를 전송하는 대신 로그 저장소로 먼저 로그를 전송하는 것입니다. 이 아키텍처(아래 그림)에서는 모든 로그가 로그 리포지토리로 복제되며, SIEM은 자체 피드를 수신하는 대신 현재 리포지토리에서 검색 및 처리를 위해 최근 로그를 가져옵니다.

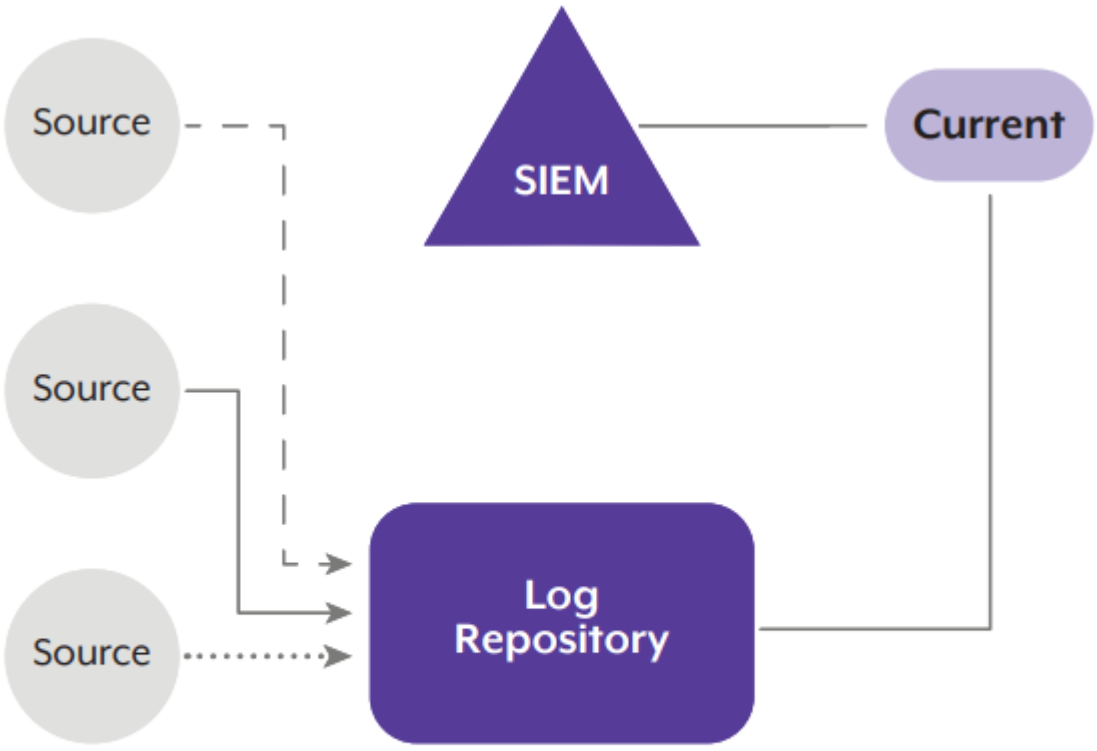



Figure 1. Data lake or repository-first approach visualisation

## 2. 로그 리포지토리와 SIEM 간의 이중 로그 복제

다음 아키텍처 예제에서는 모든 데이터 소스가 로그를 복제하여 SIEM과 로그 리포지토리 모두에 전달합니다. SIEM으로 수집된 로그의 관리는 현재 및 이전 리포지토리를 사용하여 이루어지며, 이 리포지토리 자체는 SIEM을 통해 관리됩니다. 이 관리에는 기본 로그 리포지토리와 무관하게 보존 및 폐기를 위한 모든 활동이 포함됩니다. 이 아키텍처는 수집을 위해 식별된 모든 데이터 소스가 SIEM 보안 요구사항과 관련이 있다고 판단되고 피드의 유틸리티가 데이터 볼륨 관리를 지원하는 경우에 사용할 수 있습니다. 또는 이 아키텍처는 비즈니스상의 이유로 데이터 레이크 우선 접근 방식으로 쉽게 재설계할 수 없는 기존 SIEM을 보유한 조직에 유용할 수 있습니다.

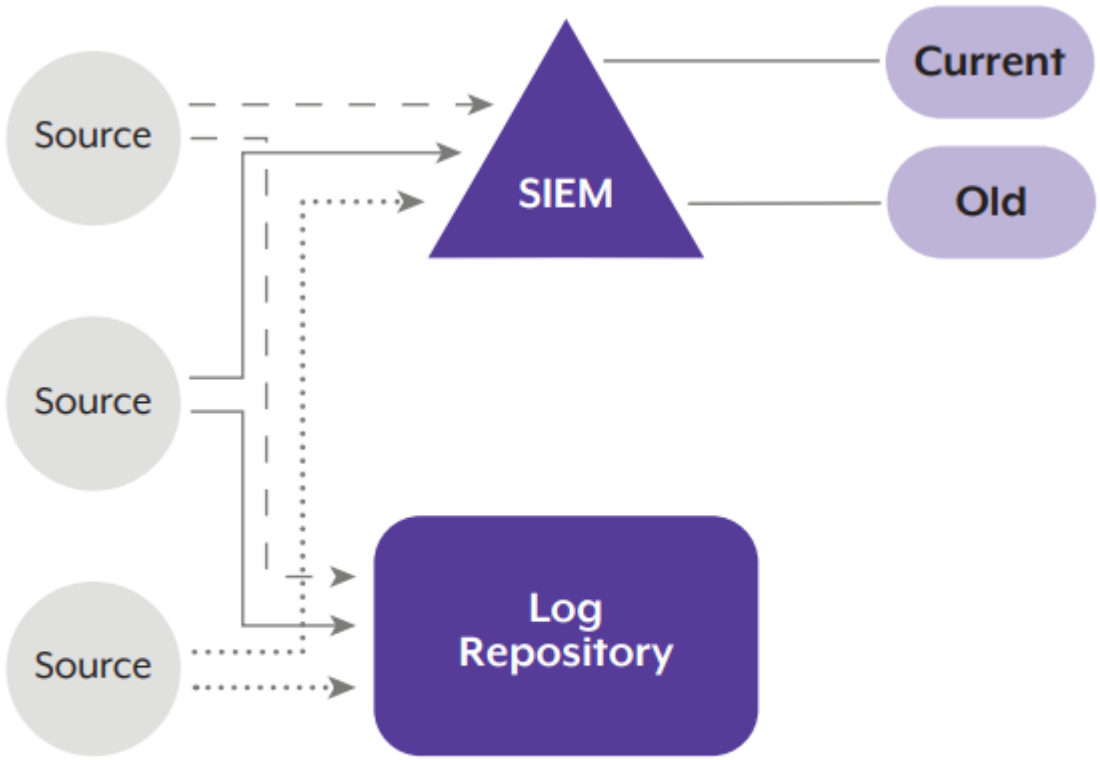



Figure 2. Dual log replication between log repository and SIEM visualisation

## 3. 요구 사항에 따른 독립적인 로그 피드

이 예에서는 일부 데이터 소스가 로그 리포지토리에만 특정 로그를 저장하도록 구성되는 반면, 다른 데이터 소스는 로그 리포지토리와 SIEM 모두에 대한 로그를 계속 복제한다는 점을 제외하면 앞서 예시에서 언급한 것과 유사합니다. 이 아키텍처는 보안 정보를 포함하지 않을 수 있는 로그를 저장해야 하는 거버넌스 또는 로그 아카이빙 요구 사항이 번거로운 조직에 유용할 수 있습니다.

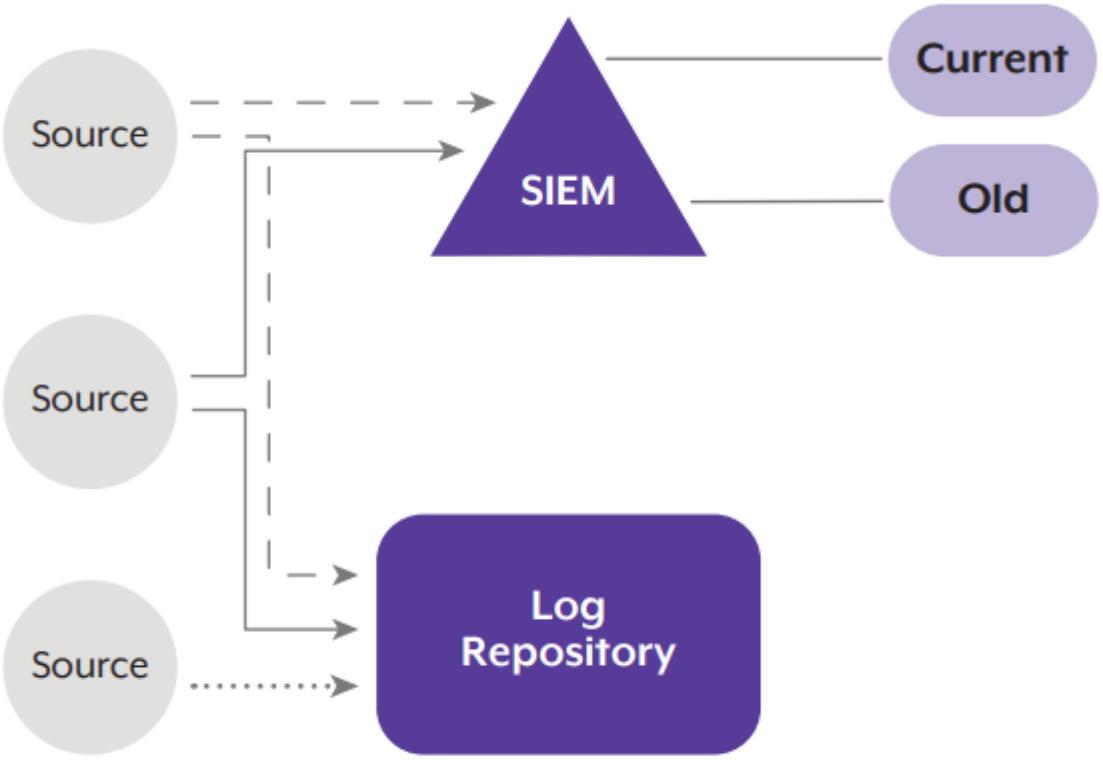



Figure 3. Independent log feeds based on requirements visualisation

## 4. SIEM 우선 아키텍처

다음과 같은 SIEM 우선 아키텍처가 사용되기도 하지만, 작성 기관에서는 이를 권장하지 않습니다. SIEM 우선 접근 방식에서는 로그를 먼저 수집하고 SIEM에서 중앙 집중화한 다음 로그 리포지토리로 복제합니다. 이 접근 방식은 처리 성능 관점에서 비효율적일 수 있습니다. 또한 문제가 발생하면 SIEM 처리로 인해 로그의 무결성이 위험해질 수 있습니다. 로그 리포지토리에는 원본이 아닌 처리된 로그만 포함되기 때문에 사고 조사에 문제가 될 수 있습니다.

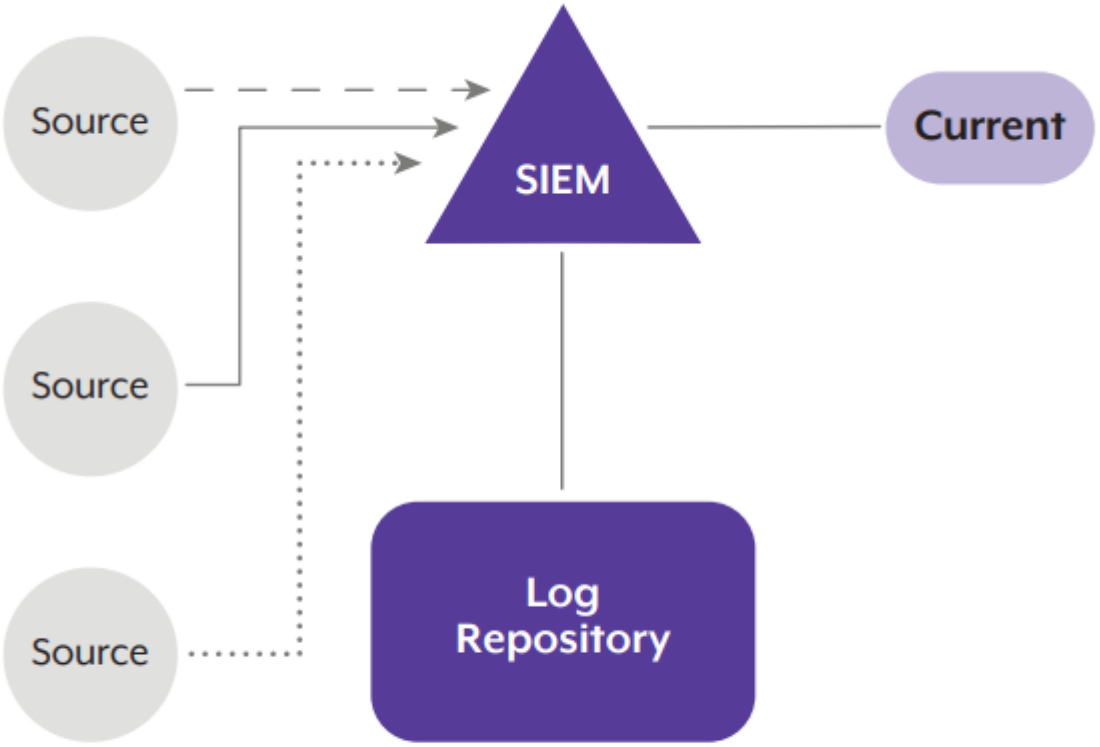



Figure 4. SIEM-first architecture

## 5. 개인 식별 정보 보호

직원의 개인 식별 정보(PII) 보호에 대한 특정 요구 사항이 있는 조직의 경우, 다음 다이어그램은 SIEM 사용자의 액세스를 제한하도록 SIEM을 설계할 수 있는 방법을 보여줍니다. 표준 역할 기반 액세스 제어(RBAC)를 적용하는 것 외에도 SIEM의 데이터를 세그먼트 방식으로 구성하고 색인화하여 데이터 소스에 대한 SIEM 사용자 액세스를 제한할 수 있습니다. 아래 다이어그램에서 사용자 A는 제한된 로그에 대한 액세스 권한만 가지고 있고 사용자 B는 전체 로그에 대한 액세스 권한을 가지고 있습니다.

일부 SIEM 플랫폼은 이러한 아키텍처를 기본적으로 지원하며, 로그 소스를 SIEM 플랫폼 내의 개별 위치에 존재하는 특정 데이터 하위 집합으로 수집할 수 있도록 합니다. 이러한 하위 집합은 다양한 형태의 제한적 접근 제어 메커니즘을 통해 사용자의 데이터 접근을 세분화하여 제어할 수 있도록 구성할 수 있습니다.

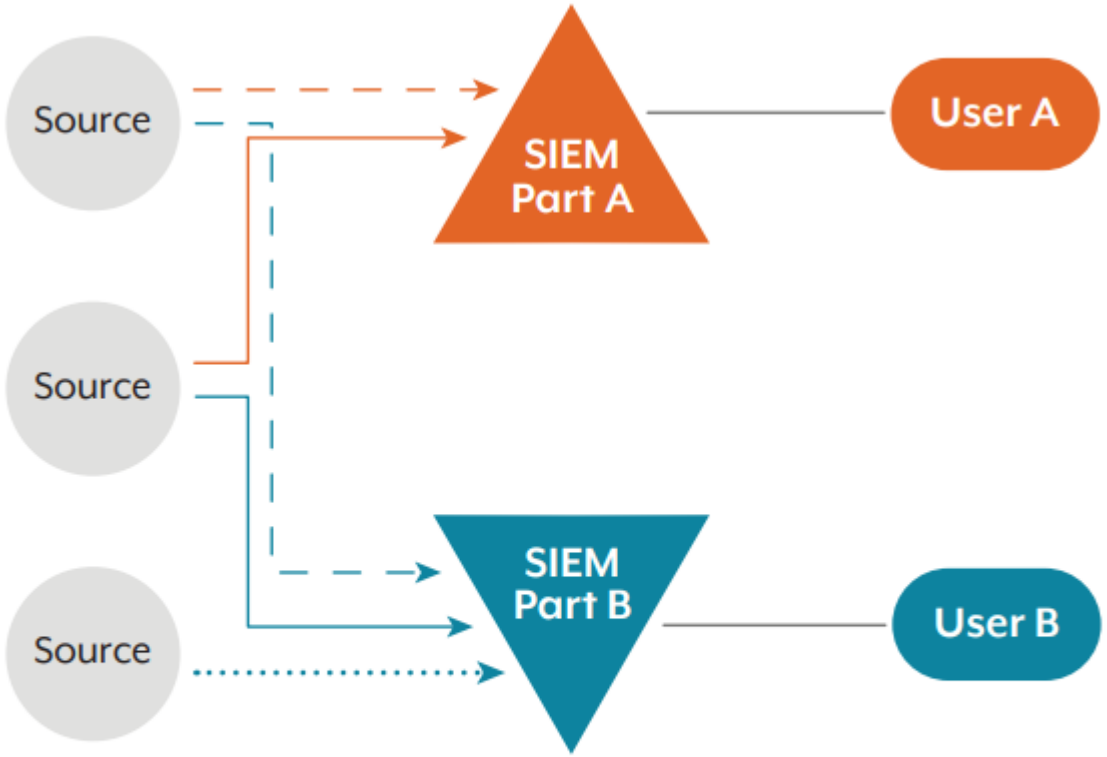



Figure 5. Protecting Personal Identifying Information (PII)

# 부록 B: 사전 처리 방법

SIEM이 중앙 집중식 로깅 솔루션이 아닌 소스에서 직접 가져오는 경우, 사전 처리는 로그 수집 및 중앙 집중화의 다음 단계로 전달되는 데이터의 양을 줄여줍니다. 사전 처리를 통해 불필요한 정보를 제거하여 포워더의 부담을 줄이고, 스토리지를 최적화하고, 표준화를 달성하고, SIEM 분석을 개선할 수 있습니다. 전처리를 위한 몇 가지 방법이 아래에 설명되어 있습니다.

## 1. 소스 로그 분리

이 방법에서는 데이터 소스(또는 호스트 장치)가 특정 기능에 따라 로그를 생성하고 여러 유형으로 분리하도록 구성됩니다. 그 중에서 특정 유형의 로그(아래 다이어그램에서 Log1)만이 '복제(replication)' 방식(예: 포워더)을 사용하여 SIEM으로 전달되며, 이는 로그 리포지토리를 통하거나 SIEM 및 로그 리포지토리와 병행하여 처리될 수 있습니다.

반면에, 원치 않는 로그(Log2, Log3)는 로그 보존 정책에서 명시한 기간 동안만 데이터 소스에 남아 있게 됩니다.

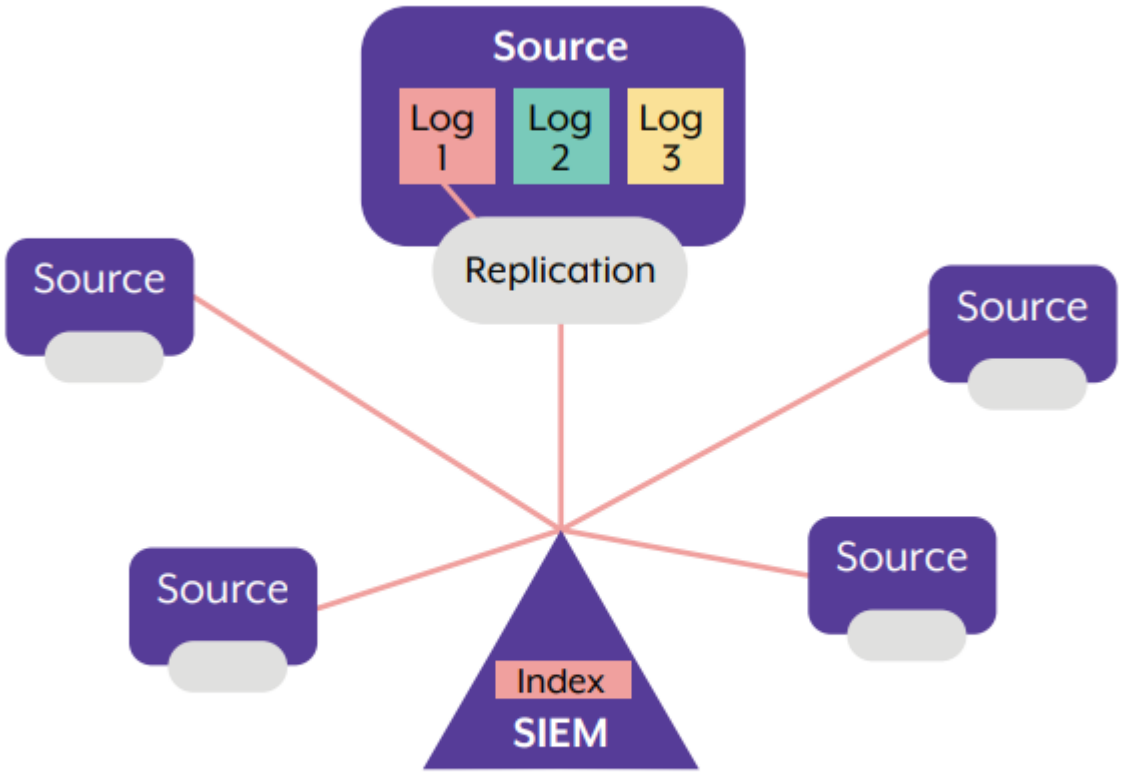



Figure 6. Separation of logs at the source

# 2. 복제 지점 사전 처리

이 예에서는 데이터 소스(또는 호스트 장치)가 특정 기능에 따라 로그를 생성하고 여러 유형으로 분리하도록 구성되었습니다. 이전 예제와 달리 세 가지 로그 유형가 포워더 또는 복제 지점과 상호 작용합니다. 로그 1과 로그 2는 SIEM 및 로그 리포지토리를 가리킵니다.

복제/포워더는 로그 유형 1과 2를 전달하는 것 외에도 다른 로그 소스(예: 로그 유형 3)를 수집하여 SIEM과는 다른 보조 위치로 복제하는 데 사용됩니다. 로그 유형 3 항목은 전용 스토리지 영역 또는 데이터 레이크로 복제됩니다.

이 사전 처리 방법은 조사를 위한 중요한 정보 소스인 PowerShell 로그에 일반적으로 사용되지만, 크기와 형식으로 인해 SIEM에 수집 부담을 일으킬 수 있습니다.

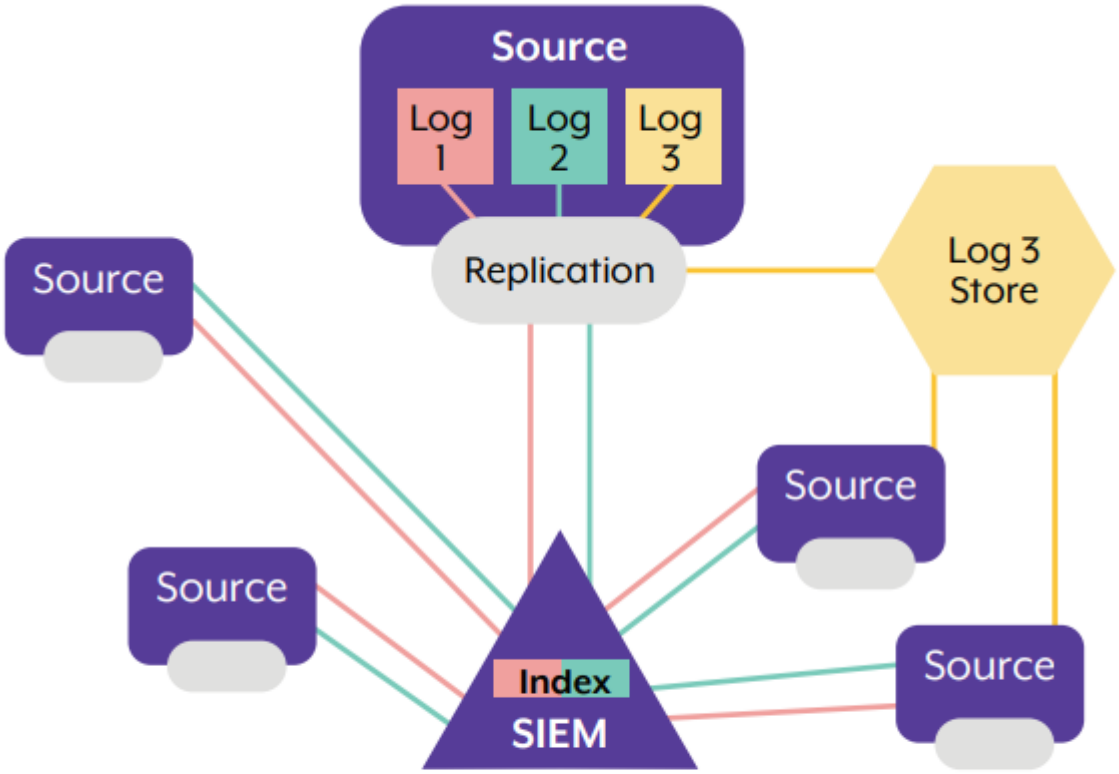



Figure 7. Pre-processing by the replication mechanism

# 3. SIEM 수집

이 예에서는 세 개의 로그 소스(Log 1, Log 2, Log 3)가 모두 데이터 소스에서 SIEM으로 복제되어 처리됩니다. 원치 않는 로그 소스가 소스에 남아 있거나 다른 리포지토리로 전송되는 이전 예제와 달리, 모든 로그가 SIEM으로 복제됩니다.

SIEM은 이러한 로그 유형 중 하나(예: 로그 유형 2)에 대해서만 경고하도록 구성할 수 있으며, 나머지 로그 유형(예: 로그 유형 1 및 3)은 '콜드 스토리지'라는 스토리지 메커니즘에 보관합니다. SIEM 쿼리에 다른 로그 유형의 추가 로그 정보가 필요한 경우, SIEM은 콜드 스토리지에서 파일 또는 이벤트를 다시 SIEM으로 검색하여 처리합니다.

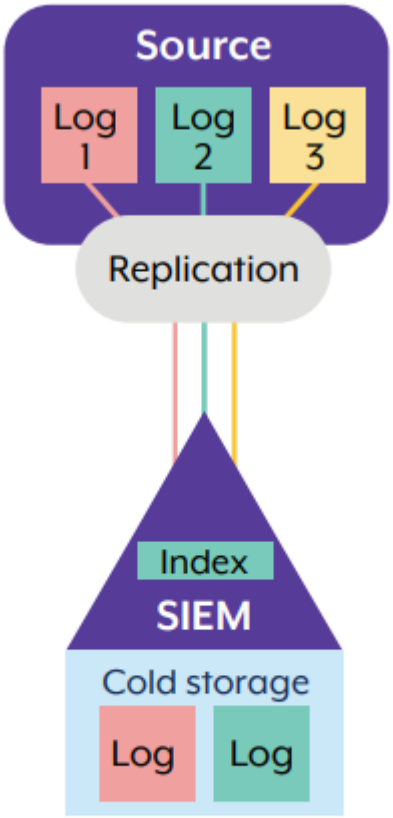



Figure 8. At SIEM separation

**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)