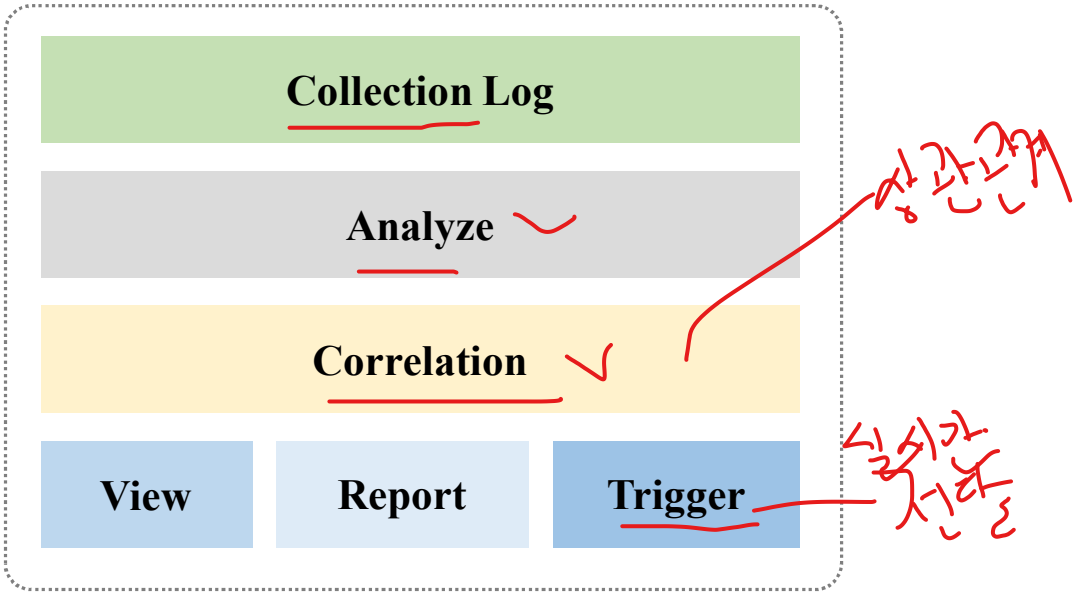
SIEM(Security Information & Event Management)

- 보안 관련 정보를 관리하는 보안도구
- SIEM의 주요기능
  - 다양한 이기종 장비에서 발생하는 로그를 통합 수집하고 분석
  - 로그 분석을 통해 각종 공격과 정책 위반을 탐지와 경고
    - ❶ SIEM 탐지기법 : 시그니처 탐지기반과 이상행위 탐지기법 모두 활용
    - ❷ 정책 위반을 탐지하면 곧 경고를 생성하고 보안 담당자에 통보
      * 보안 이상 징후가 발생하는 즉시 탐지하는 실시간 대응이 어려움
    - ❸ 경고를 발생시키는 정책은 기업이나 기관의 관심사안에 따라 다름
    - ❹ 경고는 중요도를 부여할 수 있어야 하며 중요도에 따라 향후 상세 분석 여부 결정
  - 보고서 생성(로그를 보고서로 변환)

    (예) 얼마나 많은 접속이 발생했는가? 가장 많은 접속을 일으키는 어떤 것인가?

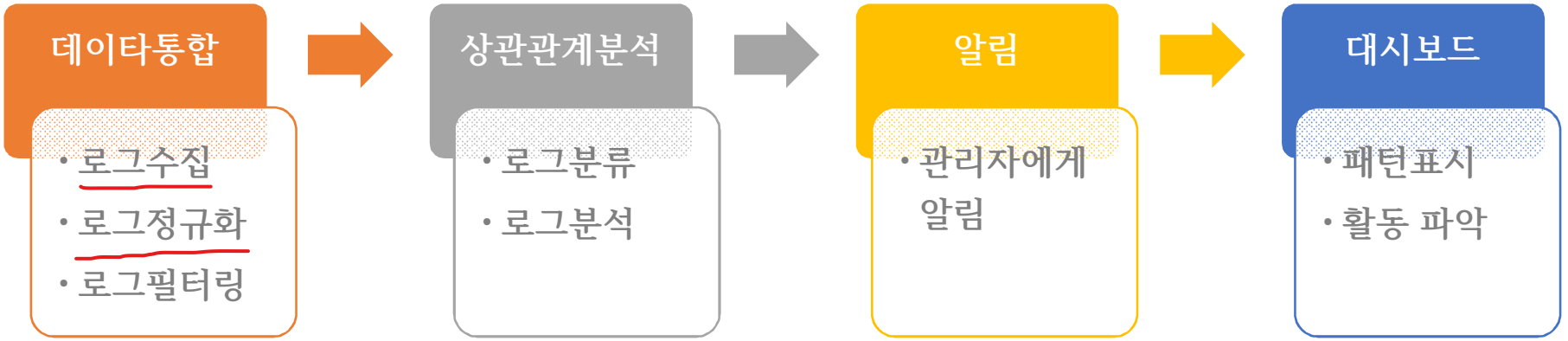
SIEM 동작 방식

Infrastructure Log



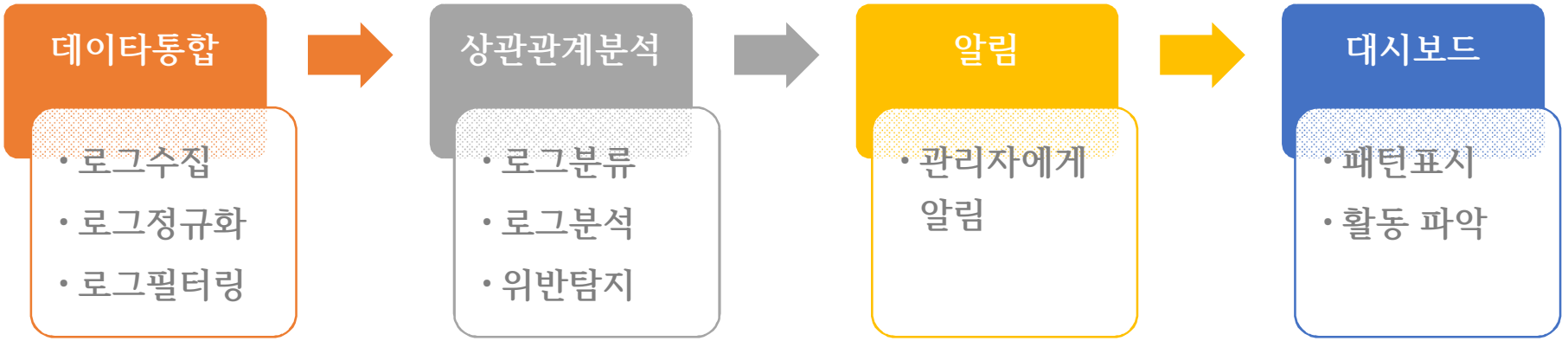
SIEM(Security Information & Event Management)

SIEM 개략적 처리 프로세스



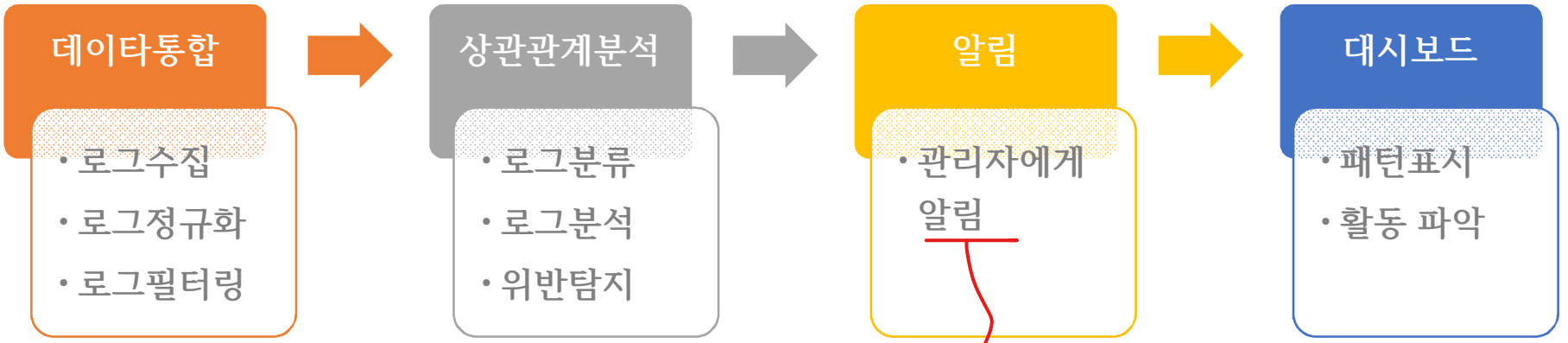
- **로그수집(collection)**
  - 관제 대상의 Agent, SNMP, Syslog 서버로부터 로그 수집

- **로그정규화(normalization)와 필터링(filtering)**
  - 로그 형식을 표준 형식으로 변환
  - 수집한 이벤트나 플로우 데이터를 데이터베이스에 저장하려면 일정한 형태로 변환 필요
  - 업체에 따라 자동 정규화 또는 수동 정규화 방법 사용
  - 정규화 과정에서 불필요한 데이타 필터링 수행



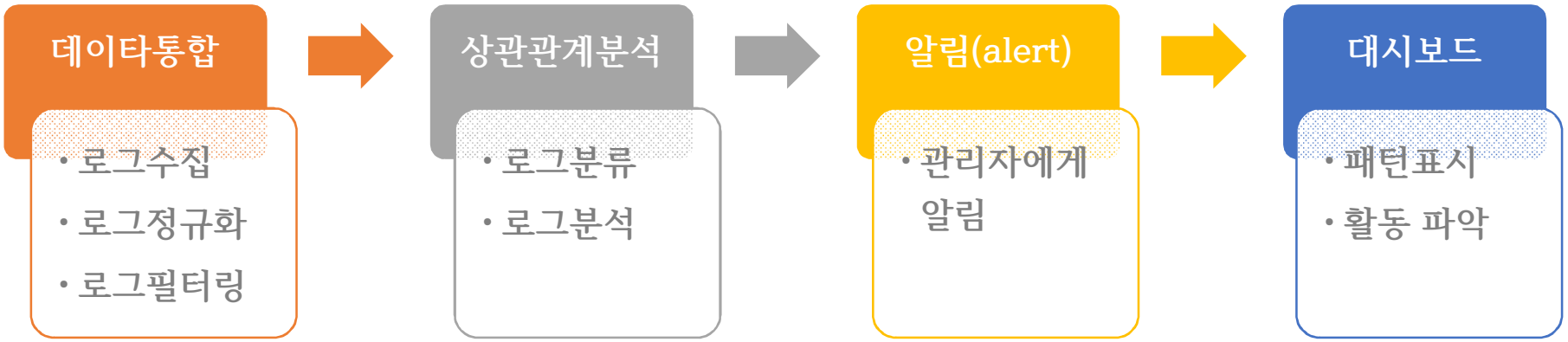
상관관계분석(Correlation)

- 동기종 또는 이기종의 여러 보안 솔루션에서 발생하는 로그 패턴간에 연관성 분석
- 로그들간에 상호연관 분석을 함으로써 실시간 보안 위협을 파악하고 대응



위험 탐지

- 로그를 분석해서 보호 대상의 전산 환경에 발생하는 문제와 공격과 정책의 위반 탐지
- 탐지는 설정한 규칙이나 조건에 맞을 때 발생
- 탐지 규칙은 임계값을 초과하거나 통계 기반의 사용자 행위를 분석하는 방법이 있음



- 알림(Alert, 경고)

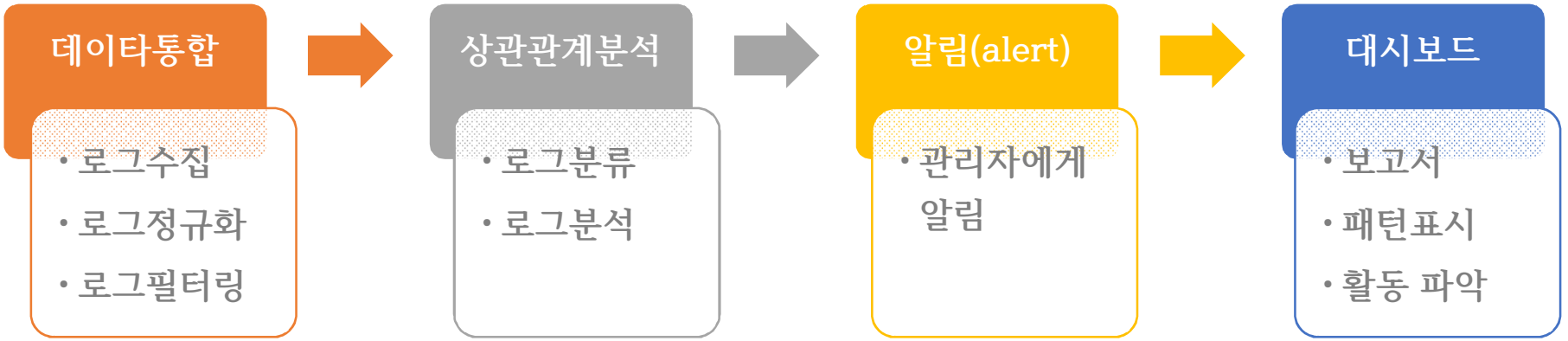
  - 경고란 보안 담당자의 검토가 필요하다는 의미

  - 정책 위반을 탐지하면 곧 경고가 생성하고 보안 담당자에게 통보

  - 경고를 발생시키는 정책은 운영하는 기업이나 기관의 관심 사안에 따라 다름

  - 경고는 중요도를 부여 할 수 있어야 함

  - 중요도는 해당 경고를 향후 상세 분석을 할 것인지를 결정하는 기준으로 사용



- 대시보드 (또는 보고서)

  -로그는 보고서 또는 대시보드로 변환 될 수 있음

  - 얼마나 많은 접속이 발생했는가?
  - 가장 많은 접속을 일으키는 호스는 어떤 것인가?
  - 가장 많은 데이터를 인터넷으로 전송한 호스트는 무엇인가?
  - 해당 호스트를 사용하는 사용자는 누구인가?

SIEM 상세 처리 프로세스