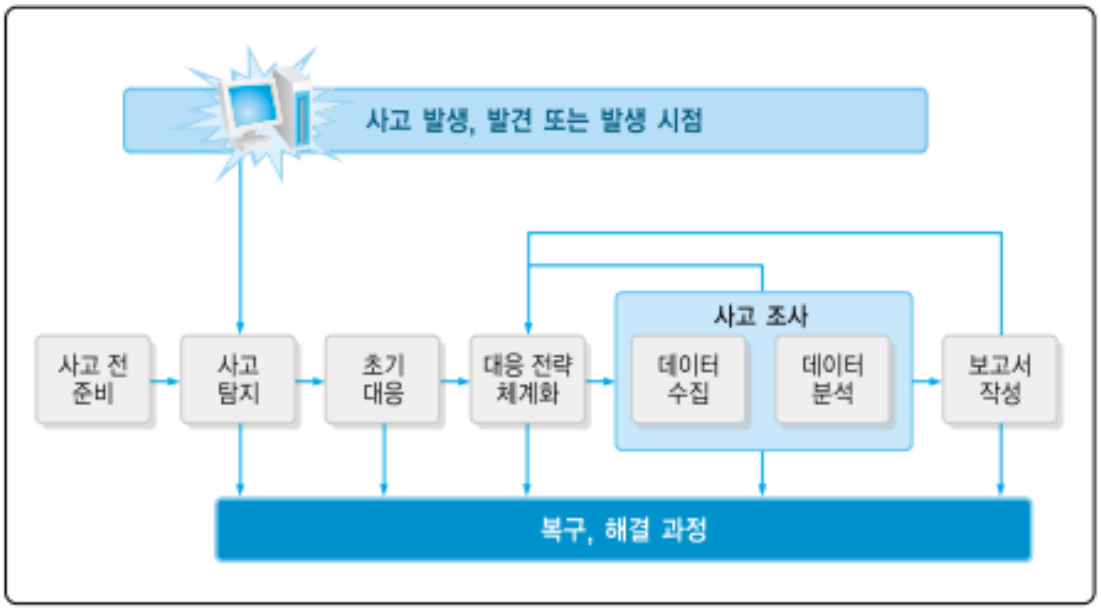
보안관제 서비스 및 업무 프로세스

공공기관

아래는 KISA에서 배포한 침해사고 분석 절차 가이드라인에 첨부되어 있는 그림.



〈그림 2-1〉 사고 대응 7단계

KISA는 사고 대응 절차를 사고 전 준비, 사고 탐지, 초기 대응, 대응 전략 체계화, 사고 조사, 보고서 작성, 복구 및 해결 과정, 7단계로 구분한다.

1. 사고 전 준비 과정: 사고가 발생하기 전 침해사고 대응팀과 조직적인 대응을 준비. 보안 사고가 언제 발생할지 알 수 없기 때문에 언제든 대응 가능하도록 행동 방안을 구축하고, 사고 대응을 위한 기술, 도구 등을 준비해두어야 한다.

2. 사고 탐지: 정보보호 및 네트워크 장비에 의한 이상 징후 탐지. 관리자에 의한 침해 사고의 식별. IDS, IPS 등 장비가 사고를 탐지하기 위해 사용되며 사고 징후로는 여러 번의 로그인 실패, 로그 파일이나 내용의 삭제와 같은 비정상적인 행위. 사고가 탐지될 시 탐지된 정보들을 기록하여 보고해야 한다.

3. 초기 대응: 초기 조사 수행, 사고 정황에 대한 기본적인 세부사항 기록, 사고 대응팀 신고 및 소집, 침해사고 관련 부서에 통지. 사건 데이터를 분석해서 정오탐 여부를 판단하여 공격 유형을 구분하고 대응책을 구상한다.

4. 대응 전략 체계화: 최적의 전략을 결정하고 관리자 승인을 획득, 초기 조사 결과를 참고하여 소송이 필요한 사항인지를 결정하여 사고 조사 과정에 수사기관 공조 여부를 판단. 침해당한 정보가 얼마나 중요한지, 공격자는 누구인지, 어느 정도의 경제적 피해가 있었는지 등을 고려하여

대응 전략을 수립한다. 이때 초기 대응 때 얻은 사건 데이터를 사용한다.

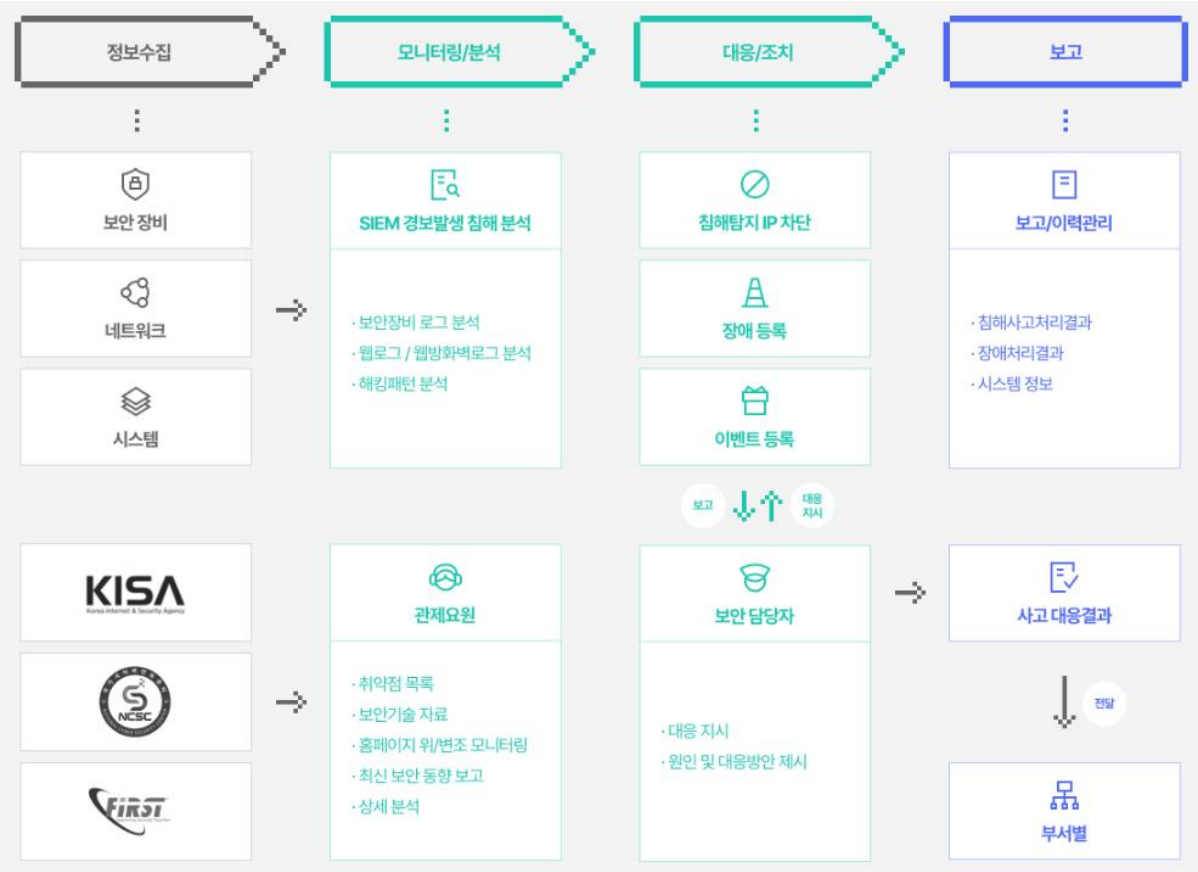
5. 사고 조사: 데이터 수집 및 분석을 통하여 수행. 언제, 누가, 어떻게 사고가 일어났는지, 피해 확산 및 사고 재발을 어떻게 방지할 것인지를 결정. 조사는 호스트 기반과 네트워크 기반 증거로 나누어 조사해야 하며 조사 과정은 데이터 수집과 자료 분석으로 나뉜다. 호스트 기반 정보로는 시스템 날짜와 시간, 현재 동작 중인 어플리케이션, 연결된 네트워크 상황 등. 네트워크 기반 정보는 IDS, 라우터, 방화벽 로그 등.

6. 보고서 작성: 의사 결정자가 쉽게 이해할 수 있는 형태로 사고에 대한 정확한 보고서를 작성.

7. 복구 및 해결 과정: 차기 유사 공격을 식별 및 예방하기 위한 보안 정책의 수립, 절차 변경, 사건의 기록, 장기 보안 정책 수립, 기술 수정 계획수립 등을 결정.

민간

아래는 이글루 시큐리티에서 배포한 보안관제 업무 프로세스 그림.



이글루 시큐리티는 관제 업무 프로세스를 정보 수집, 모니터링/분석, 대응/조치, 보고, 4단계로 구분한다.

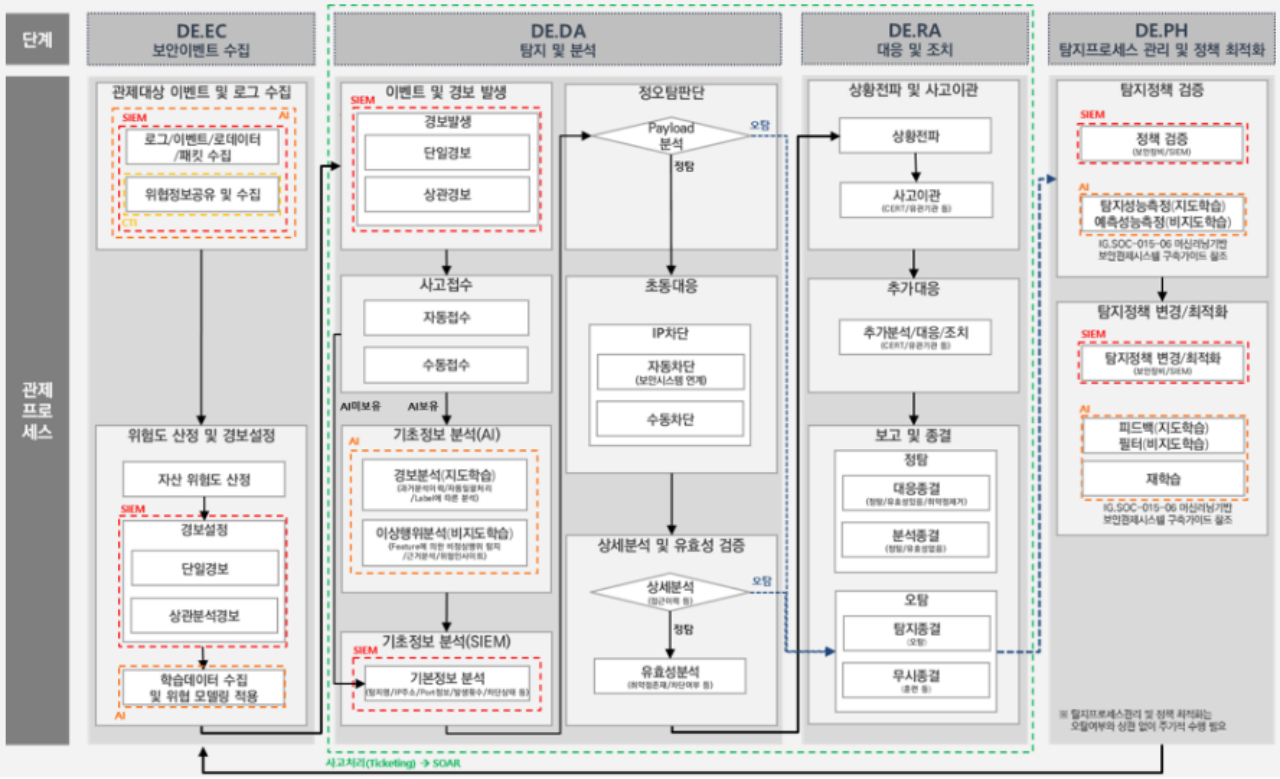
1. 정보 수집: 보안관제 대상의 보안 이벤트 및 로그를 수집하고 이에 대한 경보를 설정한다.

2. 모니터링/분석: 관제 대상 시스템에서 이벤트 및 경보가 발생했을 때 기본정보를 분석하고, 정탐 여부를 판단하고, 초동 대응 및 상세 분석을 수행한다.

3. 대응/조치: 상황전파 및 사고 이관, 필요 시 추가 대응을 수행하고 이슈가 종결 되었을 시 보고한다.

4. 보고: 평상 시 주기적인 수행 또는 오탐 발생 시 수행하게 되며, 탐지 정책을 검증하거나 변경 또는 최적화를 수행한다.

최근에는 보안 관제의 각 프로세스에 인공지능이 사용되고 있기도 하다. 아래는 이글루 시큐리티 보안관제방법론에서 제시하는 상세한 인공지능 보안관제 프로세스 그림.



관제 대상의 이벤트 로그를 수집해서 경보를 발생시키는 과정에 인공지능을 사용. 인공지능이 경보와 이상 행위를 분석해서 경보를 한번 걸러줌으로써 관제원에게 전달되는 경보의 양을 줄이는 역할을 하는 듯 하다.