침해사고 대응 분석

정보보호연구실 조대인

디지털 포렌식

- 증거수집
- 침해사고 대응

- 기업 관점에서는 침해사고 대응에 더욱 초점

침해사고 대응이란?

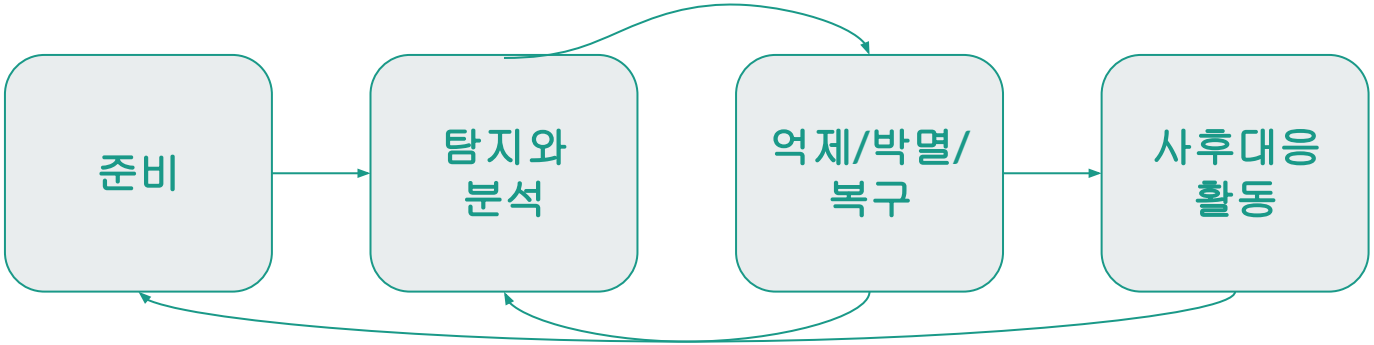
- 침해사고 -> 보안에 위협이 될 수 있는 모든 사고

  침해사고 대응 - 사전 탐지, 사후 대처

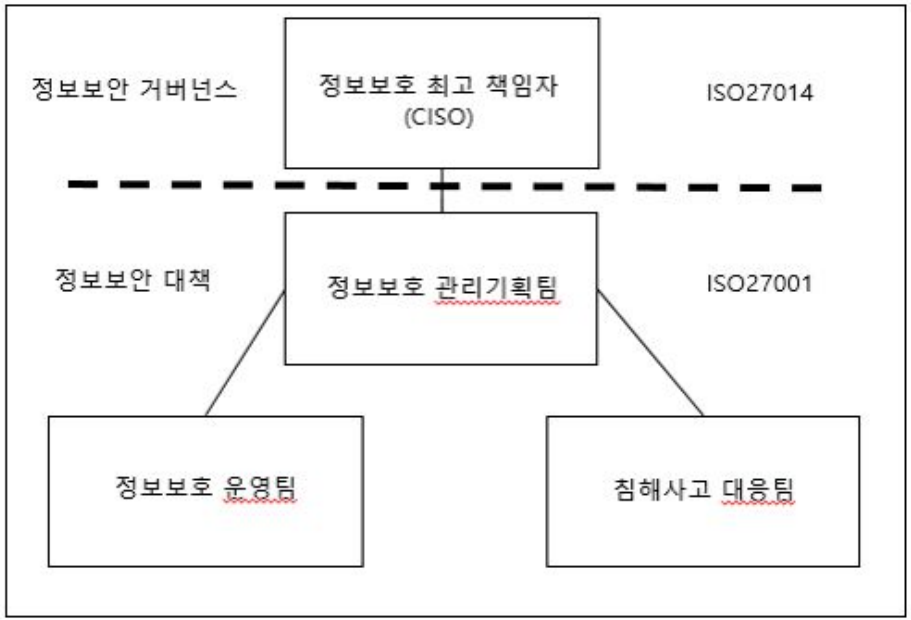
침해사고 대응의 과정

준비, 대응, 개선

침해사고 대응 프로세스



보안 거버넌스의 이해


정보보안 거버넌스
정보보호 최고 책임자
(CISO)
ISO27014
정보보안 대책
정보보호 관리기획팀
ISO27001
정보보호 운영팀
침해사고 대응팀

법의 이해

- 정보통신망법(민간, 공공 부문) - 정보 통신 서비스 제공자
- 개인정보보호법(민간 부문)
- 신용정보법(민간 부문) - 금융기관
- 전자금융거래법(민간 부문) - 금융기관

법의 적용

- 법에서는 판례를 매우 중시
  - 판례를 알아두는 것이 매우 중요하게 작용

대응 프로세스 진단

- Red, Blue Team
- CALDERA

인증기관

- 인증의 이점
  - 대외적으로 보안 수준을 판별할 수 있게됨

KISA ISMS-P, CSAP(클라우드 서비스 보안 인증 제도)

ISO 27001

보안 컨설팅을 희망한다면

- 여러가지 인증 제도
- ISO 27000 series 확인
- 보안 거버넌스에 관해 자세한 조사
- 사내 보안 팀 구조를 파악해 보는 것
- 취약점 분석(모의해킹, 웹 진단) 등 직접 해보는 것도 필요

CTF란?

Capture the flag의 약자로 취약점을 찾아내 flag를 획득하는 방식의 대회

Jeopardy(제퍼디)

Attack and Defence

CTF를 준비하는 방법

1. 기타 워게임 사이트에서 문제를 풀어본다
2. 인프런, Dreamhack 등에서 강의를 유심히 본다
3. 팀구성을 하여 각자 분야에 맞는 문제를 풀어본다
4. 암호는 기본이다.

기타 대외활동

- Best of the Best
- 사이버보안 동아리 연합
- Team H4C
- K-Shield 주니어
- 이외 여러 경진대회
    - 이보다 중요한건 결국 개인 실력을 기르는 것이다.