NIST Computer Security Incident Handling Guide Summary

Chapter 4. Coordination and Information Sharing

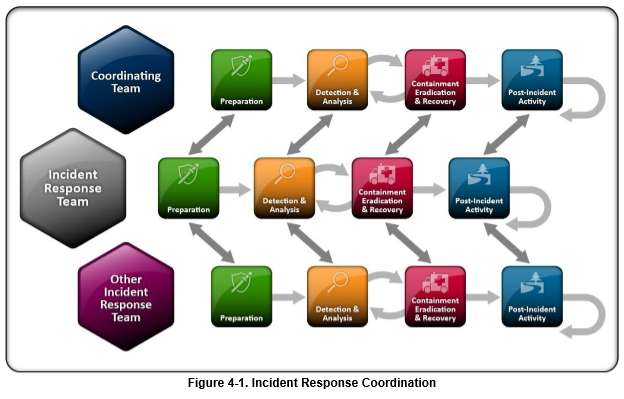
BoB7기 취약점분석 정성조

조직끼리 위협, 공격 및 취약점 정보를 공유함으로써 다른 조직에 대한 동일한 위협과 공격을 다루는데 기여할 수 있다.

또한 취약점 정보만이 기여에 영향을 미치는 것이 아니며 단일 조직에서 사용할 수 없는 기술을 사용하여 사건에 대응할 수 있는 능력도 기여에 영향을 미친다. ( 효과적으로 아웃소싱 )

# 조정

조직간의 정보 공유는 상호 작용이 이루어져야만 가능하다. 이를 위해 사고 대응 팀은 사건이 일어난 후 행동 지침을 조정해야 한다.



# 조정 관계

* 사고 대응 팀의 기술적인 부분을 담당하는 팀원은 파트너 조직의 동료와 협력할 수 있다.
* 또는 ISACs와 협력할 수 있다.
* 팀과 팀(Team-to-team): 사고 처리 단계의 모든 단계에서 협력한다.
* 팀과 조정팀(Team-to-coordinating team): 조직의 팀과 조정팀(ISAcs), 보고 수준을 충족하다는 기대를 할 수 있다.
* 조정팀과 조정팀(Coordinating team-to-coordinating team): US-CERT와 ISACs. 사건 조정 지침을 공유한다.

# 합의 사항 및 보고 사항 공유

* 외부 조직과 정보를 공유하기 전 법률 부서와 상담해야 한다.

# 정보 공유 기술

* 조직은 장애가 완전히 해결될 때까지 기다렸다가 다른 조직과 세부 정보를 공유해야 한다.

# 광고 Hoc

* 정보 공유 메커니즘은 직원과 개별 직원의 연결에 의존한다.
* 정보 공유 프로세스가 항상 동작하긴 힘들다. 연락 직원이 그만둘 수 있기 때문이다.

조직은 파트너 조직과의 공식적인 계약을 통해 정보 공유 전략을 공식화해야 한다.

# 부분적 자동화

* 모든 정보 공유의 자동화는 불가능하며 신뢰 고려 사항으로 인해 바람직하지도 않다.
* 조직이 공유할 정보의 유형을 이해한 후 모델을 기계적으로 가공하여 구축한다.
* 가능한 경우 데이터 교환 표준을 사용하여 공유해야 하는 정보를 나타낸다.
* 기술적 전송 메커니즘에 대해 합의하기 위해 파트너 조직과 협력해야 한다.

# 보안 고려 사항

* 누가 어떤 사고 정보를 볼 수 있는지 결정한다.

# 세분화된 정보 공유

* 조직은 정보를 공유할 때의 단점과 장점 사이에서 균형을 유지해야 한다.
* 사건 정보는 영향과 기술로 나눌 수 있다.

# 비즈니스 영향 정보

* 조정 팀은 보고 조직에 제공할 자원의 정도를 결정하기 위해 재무 영향 등의 정보가 필요할 수 있다.

조정 팀은 조직의 보고 수준을 요구할 수 있다.

대부분의 경우 사고 대응 팀은 명확한 가치 제안이나 보고 요구 사항이 없는 한 외부 조직과 비즈니스 영향 정보를 공유하지 않아야 한다.

# 기술 정보

* 공격 호스트의 호스트 이름, IP 주소, 멀웨어 샘플 등

조직은 수용한 지표 데이터에 내부 지표를 공유하여 추가적인 가치를 얻을 수 있다.

또한 아직 인식하지 못한 사건을 해결하기 위해 외부 지표 데이터를 사용할 수도 있다.

조직은 가능한 한 많은 정보를 공유해야 한다.

기술 지표 데이터는 조직이 실제 사고를 식별할 수 있는 경우 유용하다.

# 권고 사항

* 사고 발생 전 외부 당사자와 사건 조정 계획
* 조정 작업을 시작하기 전 법무 부서와 상의
* 사건 대응 단계 전체에 걸쳐 정보 공유
* 정보 공유 프로세스를 최대한 자동화
* 정보 공유의 장점과 단점의 균형화
* 가능한 한 많은 정보의 공유