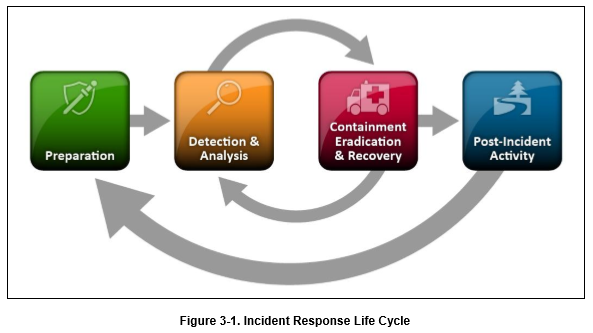
NIST Computer Security Incident Handling Guide Summary

Chapter 3. Handling an Incident

BoB7기 취약점분석 정성조



준비 단계에는 사건 대응 팀을 구성하고 교육하며 필요한 툴과 자원을 확보하는 것이 포함된다.

탐지&분석단계와 회복 단계는 순환되며 추가 호스트가 감염되었는지 확인한다.

적절한 처리 후 자세한 보고서를 발행한다.

# 준비

사전 준비가 상당히 중요하다.

사고 대응 팀은 일반적으로 사고 예방에 대한 책임이 없지만, 사고 대응 프로그램의 성공에는 필수적이다.

# 사고 처리 준비

조직은 하나의 메커니즘에 장애가 발생할 경우 별도의 메커니즘을 가져야 ㅎ나다.

* 법 집행기관 및 기타 사고 대응 팀과 같은 조직 내부 및 외부 팀의 연락처
* 온라인 양식과 같은 사고 보고 메커니즘 (하나 이상)
* 사고 정보, 문제 추적 시스템
* 연방 기관의 경우 FIPS인증 암호화 알고리즘 2를 사용해야 한다.
* 중앙 커뮤니케이션 및 조정을 위한 War-room
* 민감한 소재 확보를 위한 안전한 보관 시설
* 이동식 미디어 비우기

# 장애 분석 자원

* 포트 목록
* 기술적인 문서
* 중요 자산 목록
* **중요 파일의 암호화 해시**
* 분석, 검증 및 제거 시간 단축 소프트웨어
* 복구를 위해 새로 설치된 OS에 액세스

많은 사고 대응팀은 조사 중에 필요한 자료가 들어있는 휴대용 케이스인 점프 키트를 만든다.

점프 키트: 패킷 스니퍼, 디지털 포렌식 등을 할 수 있는 노트북 (필수적)

# 사고 예방

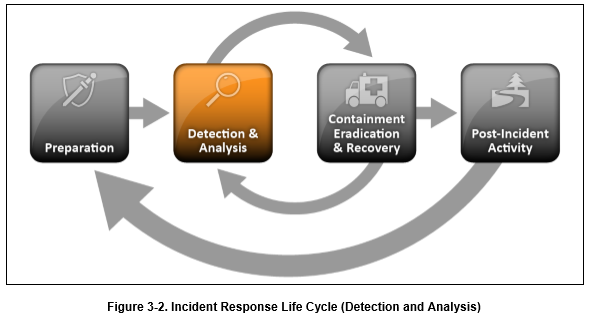
사건 발생 횟수를 낮게 유지하는 것은 조직의 비즈니스 프로세스를 보호하는 데 매우 중요하다.

* 위험 평가. 각 위험을 이해해야 하고, 우선 순위를 정하고 합리적인 위험 수준까지 도달할 때가지 완화시켜야 한다.
* 호스트 보안. 사용자는 승인된 권한에만 접근할 수 있다. 지속적으로 모니터링 되어야 함.

SCAP(Security Content Automation Protocol): 28개의 운영 체제 및 애플리케이션 구성 사용 호스트를 일관되고 효과적으로 보호하는 데 도움을 주는 가이드

* 네트워크 보안. 명시적으로 허용되지 않는 모든 활동을 거부해야함. (include VPN)
* 사용자 인식 및 교육

# 보호 및 분석



# 공격 벡터

조직은 일반적으로 모든 문제를 처리할 수 있도록 준비해야 하지만 **일반적인 공격 벡터를 사용하는 사고를 처리할 수 있도록 준비해야 한다.**

* 외부/탈착식 미디어: 이동식 미디어 또는 주변 장치에서 실행된 공격
* 소모(attrition): DDos 공격과 같은 액세스 손상 또는 거부 공격
* 웹: XSS와 같은 웹 기반 응용 프로그램에서 실행되는 공격 (lead to malware)
* e-메일: 악의적인 링크, 첨부 문서를 통한 공격
* Impersonation(위장): 입력을 위장하는 것이다. Spoofing, MITM, SQL injection
* 부적절한 사용: 권한 있는 사용자의 실수로 인한 민감한 데이터 손실 혹은 시스템 개방
* 장비 분실 또는 도난
* 기타

# 사고 징후

사고 대응의 가장 어려운 부분은 위험을 정확하게 탐지하고 평가하는 것이다.

* 자동 탐지: 네트워크 기반 및 호스트 기반 IDS/PS, 로그 분석기
* 잠재적인 사고 징후의 양은 높다(조직에서 매일 수천 또는 수백만개의 침입 감지 센서 알람을 수신하는 것은 드문 일이 아니다.)
* 사건의 징후는 전조(precursor)와 지표(Indicator)라는 두 가지 범주 중 하나로 나뉜다. 전조는 “어떤 사건이 일어날 수 있다는 징후”이고 지표는 사건이 발생했거나 현재 발생하고 있다는 표시이다.
* 스캔 탐지 웹 서버 로그 항목
* 새로운 공격에 대한 공지
* 네트워크 침입 탐지 센서
* 안티 바이러스 소프트웨어. 호스트가 멀웨어에 감염된 것을 탐지
* 익숙하지 않은 원격 시스템에서 여러 번 실패한 로그인 시도 기록
* 일반적인 네트워크 트래픽 흐름과 비정상적인 차이 발견

# 전조와 지표의 출처

* IDPs: 의심스러운 이벤트를 식별하고 공격이 탐지된 날짜와 시간, 공격 유형, 소스 등 관련 데이터를 기록한다.
* SIEM(Security Information and Event Management): 로그 데이터 분석을 기반으로 경고를 생성, 예방
* 안티 스팸 및 안티 바이러스 소프트웨어: 다양한 형태의 멀웨어를 탐지하고 알림을 생성하며 멀웨어가 호스트를 감염시키지 못하도록 방지한다. (백신)
* 파일 무결성 검사 소프트웨어: 해시 알고리즘을 사용하여 체크섬을 얻고 이를 통해 무결성을 검사한다.
* 타사 모니터링 서비스
* 운영 체제, 서비스 및 애플리케이션 로그
* 네트워크 디바이스 로그
* 네트워크 흐름: 악성 프로그램, 데이터 유출 및 기타 악의적인 행위로 인해 발생하는 비정상적인 네트워크 활동을 찾음
* 새로운 취약점 및 공격의 정보: NVD(National Vulnerability Database), US-CERT33및 CERT.CC와 같은 32개 조직의 주기적인 위협 업데이트 정보
* 조직 내 사람: 조직 내의 사용자, 시스템 관리자, 네트워크 관리자, 보안 담당자 등이 사고 징후를 보고할 수 있다. 이런 모든 보고서를 검증하는 것이 중요하다.
* 다른 조직에서 온 사람: 외부 발생 사건 보고는 심각하게 받아들여야 한다.

# 사고 분석

모든 전조나 지표가 정확하다고 보장된다면 사고 감지와 분석은 쉽지만 그렇지 않다. 이 중에서 실제 보안 사건을 찾는 것은 어려운 일일 수 있다.

* 프로파일 네트워크 및 시스템: 프로파일링은 예측된 활동의 특성을 측정하여 변화를 보다 쉽게 식별할 수 있도록 하는 것이다.
* 정상 동작을 이해한다.: 비정상적인 상황을 인지하기 위해서.
* 로그 보존 정책 생성: 방화벽, IDPS 및 응용 프로그램 로그와 같은 여러 위치에서 사건에 대한 정보를 기록할 수 있다.
* 이벤트 상관 관계 수행: 로그만으로는 공격 성공 여부를 알 수 없기 때문에 여러 지표의 출처 간 사건을 연결하는 것은 발생 여부 검증에 매우 유용하다.
* 모든 호스트 클럭을 동기화된 상태로 유지한다.: 로그에 일관된 타임 스탬프를 기록하기 위하여
* 정보의 기술 자료 유지 및 사용
* 연구를 위한 인터넷 검색 엔진 사용
* 패킷 스니퍼를 통한 추가 데이터 수집
* 데이터 필터링: 단순히 모든 지표를 검토하고 분석할 시간은 충분하지 않기 때문에 최소한 가장 의심스러운 활동을 조사해야 한다.

# 사고 기록

사고가 발생한 것으로 의심되는 사고는 관련 내용을 즉시 기록해야 한다. 노트북, 오디오 레코더, 디지털 카메라도 이러한 용도로 사용될 수 있다.

사고 대응 팀은 사고 상황에 대한 기록과 기타 관련 정보를 유지해야 한다. 문제 추적 시스템과 같은 애플리케이션 또는 데이터베이스를 사용하면 사고를 적시에 처리하고 해결할 수 있다.

# 문제 추적 시스템은 포함해야 한다.

* 사고의 현재 상태
* 사고 요약
* 사고 관련 지표
* 관련된 다른 사건
* 이 사건에 대한 모든 사고 취급자의 조치
* 적용될 수 있는 보관 체인의 사용
* 사고와 관련된 영향 평가
* 사건 조사 중 수집된 증거 목록
* 사고 핸들러의 의견, 다음에 수행해야 할 단계

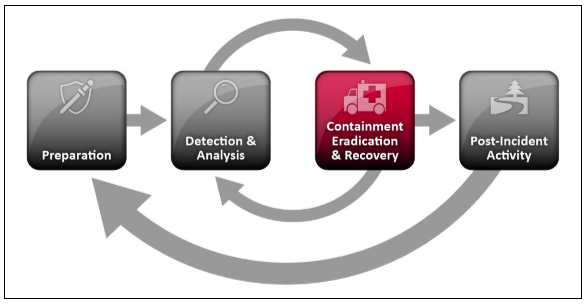
# 사건 우선 순위

* 기능 영향: 사건이 조직의 기능에 영향을 끼침
* 정보 영향: 사건이 조직 정보의 기밀성, 무결성 및 가용성에 영향을 끼침
* 복구 가능성: 경우에 따라 장애로부터 복구할 수 없음

# 사고 통보

* 일반적으로 CIO, 정보 보안 책임자, 지역 정보 보안 요원, 조직 내 기타 사고 대응 팀, 시스템 소유자, 공무, 법무부, US-CERT 등에게 알림
* 통보 방법: E-mail, 웹 사이트, 전화 통화, 직접, 음성 사서함

# 회복



# 격납 전략 선택

조직은 의사 결정의 용이성을 위해 기준을 명확하게 문서화하여 각 주요 사건 유형에 대해 별도의 봉쇄 전략을 수립해야 함.

# 전략을 결정하기 위한 기준

* 자원의 잠재적 손상 및 도난
* 증거 보존의 필요성
* 서비스 가용성
* 전략 구현에 필요한 시간 및 자원
* 전략의 효과 (부분 억제, 완전 억제)
* 기간 ( 몇 시간 내에 해결되야 하나? )

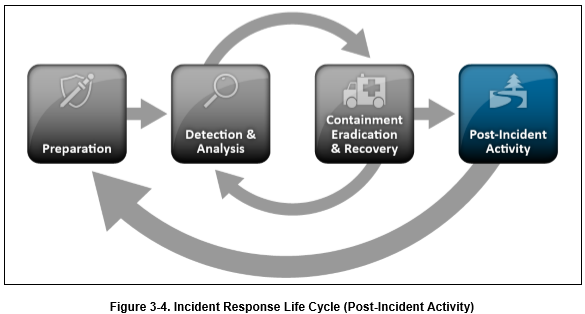
# 근거 수집 및 취급

* 식별 정보 로그 보관 (컴퓨터 일련 번호, 모델 번호, MAC 등)
* 개인의 이름, 직함 및 전화 번호 보관
* 발생 시간 및 날짜 보관
* 증거가 저장된 위치 로그 보관

# 공격 호스트 식별

* 공격 호스트의 IP주소: 동적 주소 할당을 고려해야 함
* 검색 엔진을 통해 공격 호스트 검색
* 사고 데이터베이스 사용
* 가능한 공격자 통신 채널 모니터링

# 사건 후 활동



# 교훈 습득

* 얼마나 잘 처리했는가? ( 절차, 시간 준수 )
* 유사한 사고가 발생했을 때 어떻게 대처할 것인가
* 다른 조직과의 정보 공유가 어떻게 개선될 수 있는가
* 향후 문제를 탐지, 분석하기 위해 필요한 추가 툴 혹은 자원은 무엇인가

# 수집된 사고 데이터의 사용

* 각 사건에 관한 객관적인 데이터를 생성해야 함
* 사고 데이터를 다른 조직과 공유해야 함
* 실행 가능한 데이터를 수집하는데 초점을 맞춰야 함

# 각 사건의 주관적 평가

사고 대응 팀 구성원들은 다른 팀원들과 팀 전체의 성과 뿐 아니라 자신의 성과를 평가해야 한다.

# 평가 항목

* 장애 대응 정책, 계획 및 절차
* 툴 및 리소스
* 팀 모델 및 구조
* 사고 처리 교육
* 사고 문서 및 보고서
* 성공 척도

# 증거 보유

조직은 증거 보존 기간 정책을 수립해야 한다.

* GRS: 사고 처리 기록을 3년간 보관해야 한다
* 디스크에 수천개의 이메일이 포함된 경우 조직은 반드시 필요하지 않다면 3년 이상 보관하지 않아도 된다. ( 주관적 평가 )