보안 관제와 침해 대응

보안 관제

보안 관제

- 보안 관제란?
  - 조직의 중요 정보 자원을 보안 공격으로부터 보호하기 위한 일련의 활동
    - 좁게는 모니터링, 넓게는 보안 공격을 분석하여 대응 및 예방까지 수행하는 통제활동
  - 보안 관제 모니터링 팀, 침해 사고 대응 팀, 정보 공유 분석 센터로 구성
    - 보안 관제 모니터링 팀: 탐지 및 예방
      - 365일 24시간 모니터링
    - 침해 사고 대응 팀: 대응 및 예방
      - 이상 트래픽이나 이벤트 등에 대해 상세 분석, 대응 조치 수행
    - 정보 공유 분석 센터: 공유 및 개선
      - 사이버테러 취약점과 침해 요인, 대응 방안에 관한 정보 제공, 침해 사고 분석
        - 금융 ISAC, 통신 ISAC
  - 정보, 정보 보호, 통합 보안 관제의 3가지 시스템으로 구성
    - 정보: 보안 관제의 대상
      - 윈도우, Linux/Unix 서버, DBMS, 네트워크 장비 등
    - 정보 보호: 침입 탐지 및 대응을 위한 정보 제공
      - IDS/IPS, 방화벽, NAC, DLP 등
    - 통합 보안 관제: 침입 탐지 정보의 수집 및 처리
      - SIEM / ESM 등

보안 관제

- SIEM(Security Information and Event Management)
  - SIM(보안 정보 관리) + SEM(보안 이벤트 관리) 통합
  - 여러 원본에서 이벤트 로그 데이터를 수집하고 실시간 분석을 바탕으로 정상적인 범위를 벗어나는 활동을 식별하여 적절한 조치
  - 인공 지능으로 위협 탐지 및 대응을 보다 빠르고 스마트하게 만듦

	ESM	SIEM
주요 목적	보안 위협 발생 시 대응 및 시스템 가용성 관리	지능화, 고도화, 신종 보안위협의 대응 (APT 공격 등)대용량 데이터의 심층분석
탐지방법	IP, 포트기반 탐지단순 패턴 및 알려진 공격에 대한 분석 및 대응	패킷의 문맥 및 프로토콜 레벨의 분석 및 탐지알려지지 않은 공격의 탐지 및 장기간 범위 데이터 분석
성능	오탐지 과탐지가 상대적으로 많음. 이벤트 기반 분석의 한계점	탐지 정확도가 비교적 높음

보안 관제

- 보안 관제의 수행 원칙
  - 무중단의 원칙
    - 24시간 365일 서비스 제공
  - 전문성의 원칙
    - 통합 보안 관제 시스템 등에 대한 지식 뿐 아니라 네트워크 등의 이론에 대해서도 전문 지식 및 노하우 필요
  - 정보 공유의 원칙
    - 어느 한 보안 관제 조직에서 보안 공격을 사전에 미리 탐지하여 차단했다면 이러한 탐지 및 차단 정보가 다른 보안 관제 조직에도 공유되어야 함

보안 관제

- 보안 관제의 유형
  - 직접 관제
    - 내부에 직접 보안 관제 시스템을 구축, 자체 인력
      - 전문성이 떨어질 수 있음
  - 파견 관제
    - 조직 내부에 보안 관제 시스템을 두고 운영하나, 관련 업체로부터 파견 받아 운영
      - 인력 관리 부담, 높은 비용
  - 원격 관제
    - 전문 관제 업체가 보유한 조직 외부의 보안 관제 시스템 사용
      - 보안 사고 발생 시 즉각적인 대응이 어려움
  - 클라우드 관제
    - 조직의 IT환경이 클라우드에 있는 경우에 대한 관제
      - 서버와 데이터베이스 등이 AWS(Amazon) 혹은 Azure(MS) 환경에 있는 경우

보안 관제

- 탐지 규칙
  - 특정 악성코드 또는 보안 공격이 네트워크로 유입되는 것을 탐지하기 위해 개발한 시그니처(signature)
    - 시그니처: 특정 악성코드 혹은 취약점 등을 식별할 수 있는 문자열
  - 탐지 규칙의 구조
    - 헤더: 패턴이 발견되었을 때의 대응 동작과 탐지 조건을 적용할 프로토콜, 출발지/목적지 및 방향 등의 정보 설정
    - 옵션: '탐지 조건'에서 실제 어떤 문자열을 찾으면 될지 시그니처에 해당되는 문자열 정의

Rule Header							Option
Action	Protocol	SrcIP	SrcPort	->	DstIP	DstPort	Option

보안 관제

▪ 탐지 규칙의 헤더와 옵션

Action 유형

명령어	내용
alert	경고 발생 및 로그 기록
log	로그 기록
pass	패켓 무시
drop	패켓 차단 및 로그 기록 (IPS 기능으로 사용됨, 단 인라인 구조가 되어야 한다.)
reject	패켓 차단 및 로그 기록(TCP - TCP RST 응답, UDP - ICMP Unreachable 응답)
sdrop	패켓 차단 및 로그 기록 없음

일반 옵션

명령어	내용	형식
msg	경고 이벤트 메세지	msg:"ICMP Ping test";
sid	룰 식별자 (3000000번 이상 권장)	sid:3000001;
rev	룰 버전, 수정될 경우 1씩 증가	rev:1;
priority	우선 순위 (값이 작을수록 먼저 매칭) 범위 : 1~10)	priority:1;
classtype	스노트 룰 분류	classtype:분류이름;
reference	취약점 참고 배포 URL 정보	reference: 이름 http://~;

Protocol 유형

유형	내용
tcp	TCP 탐지
udp	UDP 탐지
ip	IP 전체 탐지
icmp	ICMP 메세지 탐지
any	전체

방향 지정

형식	내용
->	요청 패켓 탐지 (응답패켓 탐지는 SrcIP/DstIP 반대로 설정)
<>	요청/응답 패켓 둘다 탐지

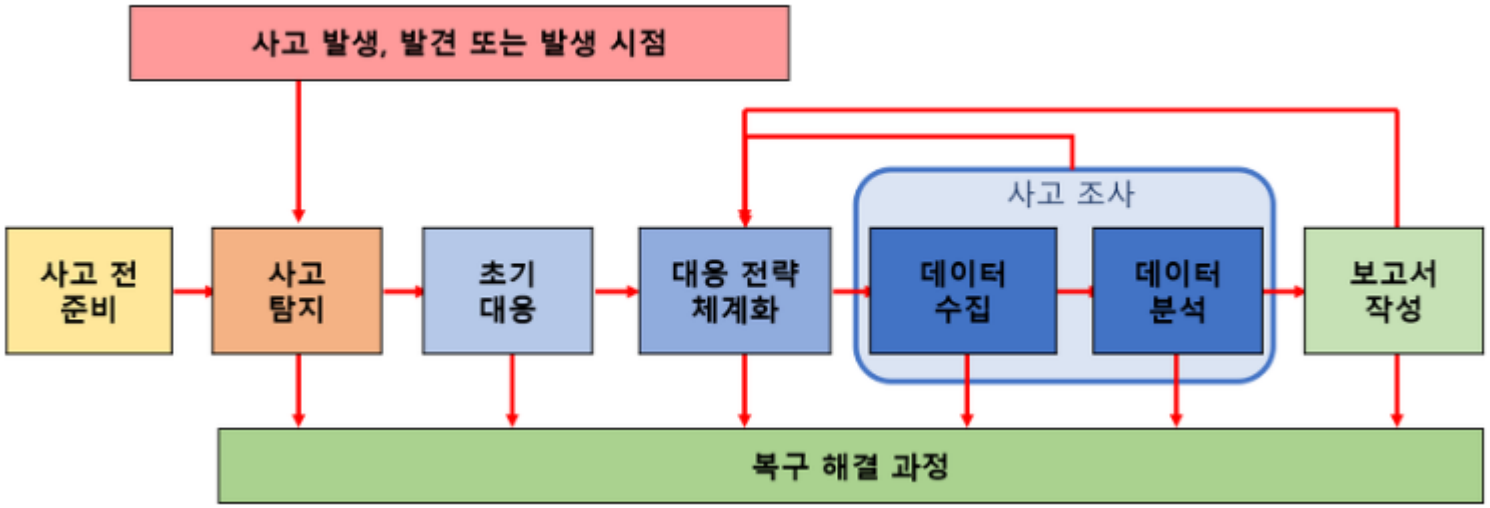
페이로드 탐색 옵션

명령어	내용	예제
content	문자/숫자 탐지	content: "xxx"; content: "|16진수 16진수|";
nocase	대소문자 구분 없이 탐지	content: "xxx"; nocase;
offset	지정한 바이트번째 부터 탐지(0번째 부터 시작)	offset:3;
depth	지정한 바이트까지 탐지(0번째 부터 시작)	depth:3;
distance	content 매칭 후 지정 위치 이후 다른 content 탐색	content:"xxx"; content:"yyy"; distance:5;
within	content 매칭 후 지정 위치 안에 다른 content 탐색	content:"xxx"; content:"yyy"; within:5;
pcre	정규화 표기, '/'는 시작과 끝에 표기, 16진수는 앞에 ₩x	pcre:"/(http|ftp) Traffic/"

침해 대응

침해 대응

- 침해 대응의 절차



침해 대응

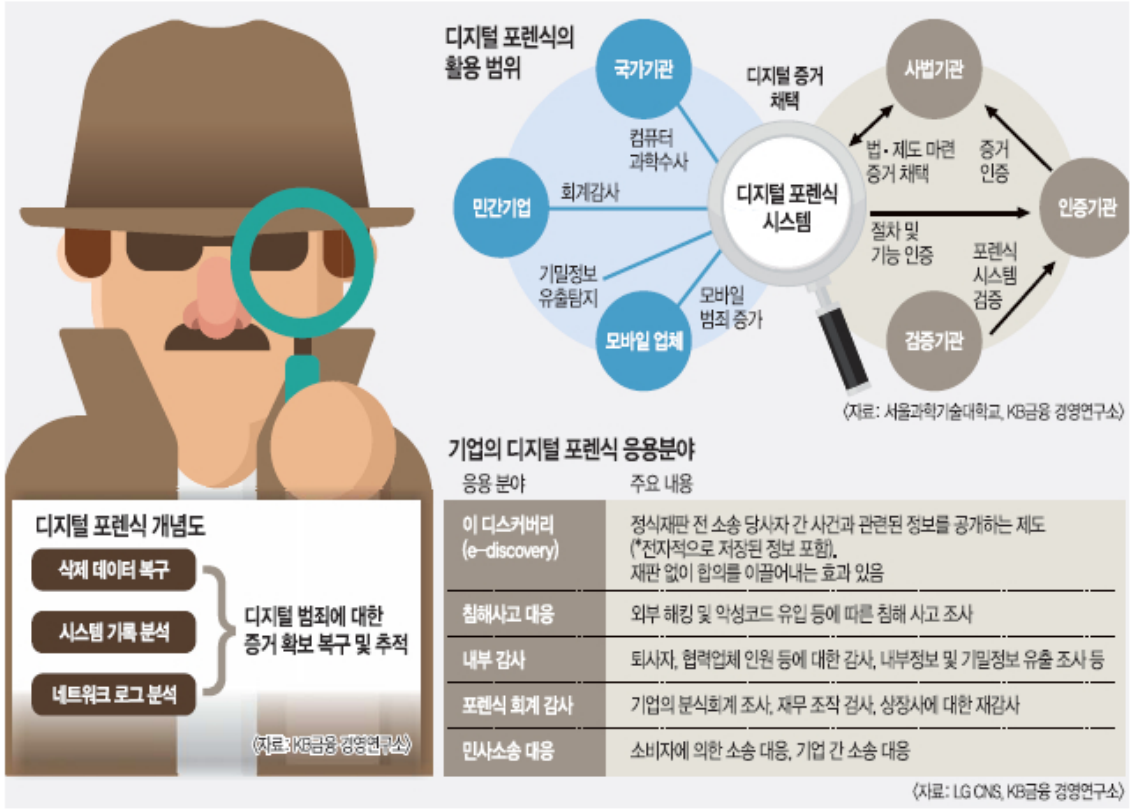
- 사전 준비
  - 조직적인 침해 대응 체계 구축
- 사고 탐지
  - ESM 및 SIEM 등의 통합 보안 관제 시스템
- 초기 대응
  - 침해 대응팀이 초기 보고 사항들을 인수/인계 받는 것으로 시작
  - 침해 사고로 인한 손실 최소화, 추가적인 손상을 막기 위해 해당 시스템의 네트워크 단절 또는 방화벽 설정 등을 변경
  - 충분한 정보를 확보하고 검토
- 대응 전략의 수립
  - 수집된 자료를 기반으로 가장 적절한 대응 전략 수립

침해 대응

- 사고 조사
  - 초기 대응으로 처리가 어려운 경우 정밀 분석(디지털 포렌식)
- 보고서 작성
  - 조사된 결과를 조직의 상급자 및 외부에 보고하기 위한 보고서 작성
- 복구 및 해결
  - 악성코드 제거, 시스템의 서비스가 가능하도록 복구
    - 운영체제 및 백신 등의 보안 패치

침해 대응

- 디지털 포렌식
  - 디지털 기기에 저장된 전자적 증거물을 사법기관에 제출하기 위해 데이터를 수집 및 분석하여 보고서를 작성하는 일련의 작업
  - 디지털 법의학이라고도 함



침해 대응

- 디지털 포렌식의 원칙
  - 정당성의 원칙
    - 획득한 증거 자료가 적법한 절차를 거쳐서 정당하게 획득되어야 한다.
      - 위법한 방법으로 수집된 증거는 법적 효력 상실
  - 무결성의 원칙
    - 수집 증거가 결함이 없이 위 · 변조되지 않았음을 증명할 수 있어야 한다.
      - 수집 당시 자료의 해시 값과 법정 제출 시점 자료의 해시 값 일치여부 확인
  - 연계보관성의 원칙
    - 증거가 획득된 다음 증거가 이송, 분석, 보관, 법정 제출이라는 일련의 과정 및 각 과정마다 담당자가 명확해야 하며 이에 대한 추적이 가능해야 한다.
      - 무결성의 원칙과 밑접한 관련, 무결성이 깨졌다면 연계보관성을 통해 문제 확인
  - 재현의 원칙
    - 동일한 조건과 동일한 상황이라면 디지털 포렌식의 분석 결과는 항상 같은 결과가 나와야 한다.
  - 신속성의 원칙
    - 디지털 포렌식 수행의 전 과정은 지체없이 신속하게 진행되어야 한다.

침해 대응

- 디지털 포렌식 유형

종류	설명
디스크	비휘발성 저장매체(하드디스크, SSD, USB, CD 등)를 대상으로 증거 획득 및 분석
라이브	휘발성 데이터를 대상으로 증거 획득 및 분석
네트워크	네트워크로 전송되는 데이터를 대상으로 증거 획득 및 분석
이메일	이메일 데이터로부터 송·수신자, 보낸·받은 시간, 내용 등의 증거 획득 및 분석
웹	웹 브라우저를 통한 쿠키, 히스토리, 임시파일, 설정 정보 등을 통해 사용 흔적 분석
모바일/임베디드	휴대폰, 스마트폰, PDA, 네비게이션, 라우터 등의 모바일 기기를 대상으로 증거 획득 및 분석
멀티미디어	디지털 비디오, 오디오, 이미지 등의 멀티미디어 데이터에서 증거 획득 및 분석
소스코드	프로그램 실행 코드와 소스 코드의 상관관계 분석, 악성코드 분석
데이터베이스	방대한 데이터베이스로부터 유효한 증거 획득 및 분석
안티, 안티안티	데이터 완전 삭제, 암호화, 스테가노그래피

침해 대응

- 디지털 포렌식의 과정


Any Questions?