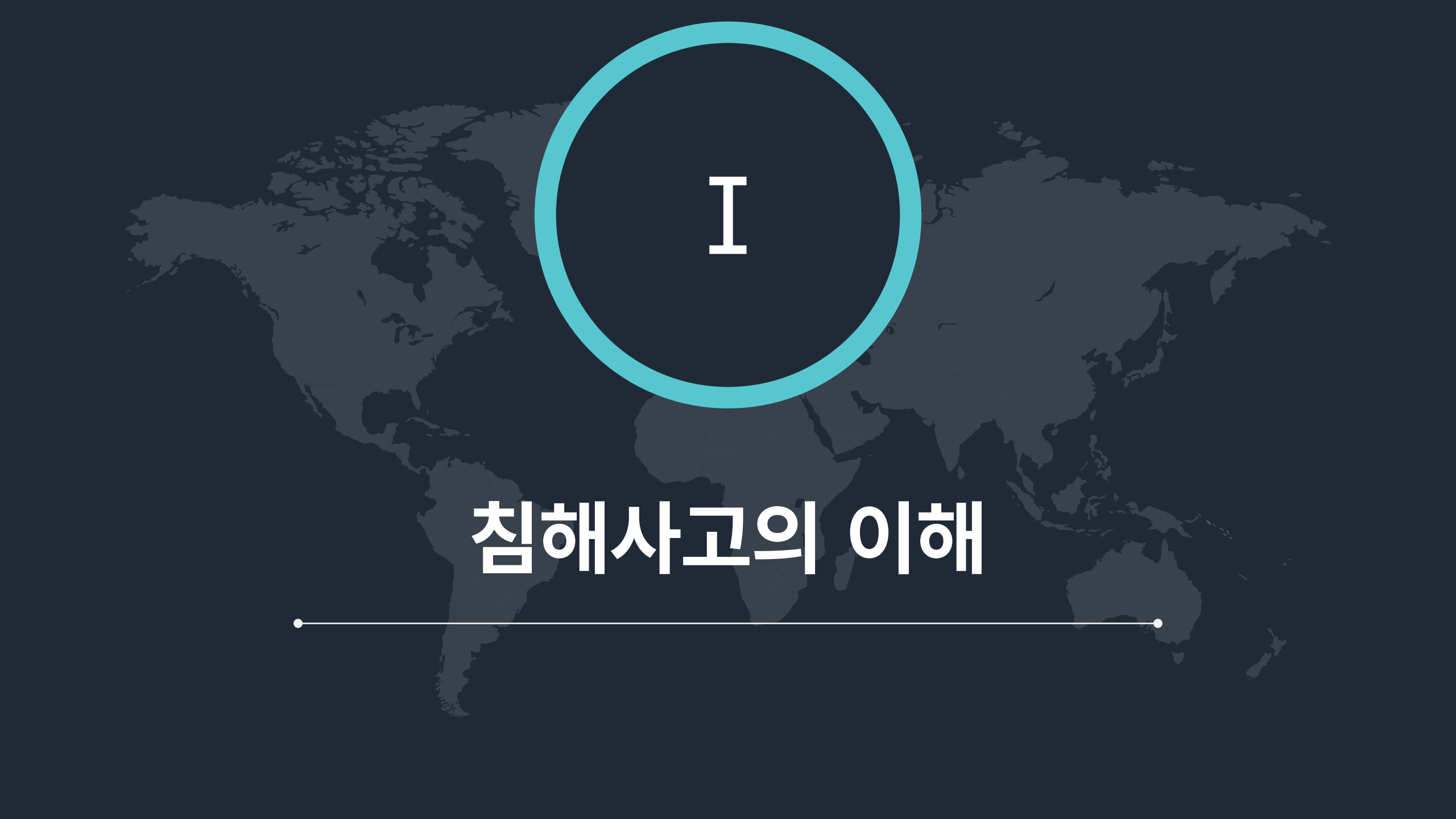
CHAPTER 05

침해사고 대응

이현호 hyeonholee@korea.com

목차



I

침해사고의 이해

I 침해사고의 이해

1 컴퓨터 침해사고와 CERT

- **CERT (Computer Emergency Response Team)**
  - 침해사고를 대응하고 보안사고를 대비하는 역할을 하는 비상대응조직
  - 1988년 11월 22일, 미국 전역의 컴퓨터가 모리스 웜에 의해 멎어버린 사건 이후
    미 정부가 적극적으로 침해사고의 대응책을 마련
  - 미 국방부 고등연구 계획국(Defense Advanced Research Projects Agency, DARPA)은
    컴퓨터와 관련한 침해사고에 적절히 대응하고자,
    카네기멜런대학 내의 소프트웨어공학연구소에 CERT를 설립

1 컴퓨터 침해사고와 CERT

- **CERT에 필요한 구성원**

시스템 운영 전문가	대외 언론 및 외부기관 대응 전문가	법률팀	인사팀

침해사고가 발생한 시스템을 효율적으로 복구하기 위해 서비스와 시스템의 관계를 명확하게 이해하고 조치를 취함

1 컴퓨터 침해사고와 CERT

- **CERT에 필요한 구성원**

시스템 운영 전문가	**대외 언론 및 외부기관 대응 전문가**	법률팀	인사팀
침해사고를 이해하고 언론 및 사이버안전국, 경찰에 적절한 방법으로 대응			

1 컴퓨터 침해사고와 CERT

- **CERT에 필요한 구성원**

시스템 운영 전문가	대외 언론 및 외부기관 대응 전문가	**법률팀**	인사팀

침해사고 대응 과정에서 법적인 문제가 발생했을 때 판단을 내리고 법적인 후속 절차를 밟음

1 컴퓨터 침해사고와 CERT

- **CERT에 필요한 구성원**

시스템 운영 전문가	대외 언론 및 외부기관 대응 전문가	법률팀	**인사팀**

조직 내 구성원의 권리와 책임을 파악하고 침해사고 대응 과정에서 적절한 조직원을 찾도록 지원

II

침해사고 대응 절차

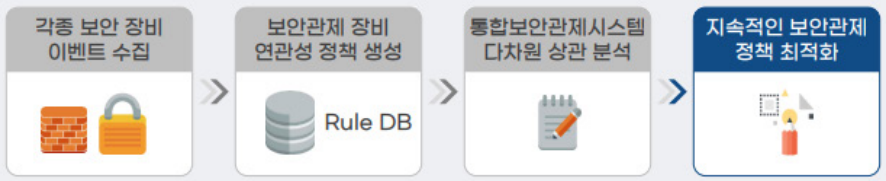
II 침해사고 대응 절차

1 실무 관점의 침해사고 대응 개요

정보 수집

정보수집 → 탐지분석 → 대응/조치 → 보고/사후처리

항목	수행업무	수행인력	대상 시스템
연동대상 보안시스템 로그 수집	• 네트워크 보안시스템 로그 수집 여부 확인	보안관제	FW, IPS, WAF, DDoS 등
최신 위협 동향 정보 수집	• 각종 위협정보 수집	보안관제	CTI, KRCERT, C-TAS



❖ 최신 위협 정보 수집


수집정보


국내/외 보안정보


FIRST 공식사이트

탐지/분석

정보수집 → 탐지분석 → 대응/조치 → 보고/사후처리

항목	수행업무	수행인력	대상 시스템
이벤트 탐지 분석	• 수집된 로그를 기반으로 탐지된 이벤트에 대한 공격 유효성 분석	보안관제	SIEM
통계성 탐지 분석	• 네트워크 트래픽 유입량 및 임계치 설정에 따른 공격 탐지 및 분석	보안관제	SIEM
위협 정보 공격 탐지	• 유관기관 및 최신 위협 정보를 토대로 공격 탐지 및 분석	보안관제	SIEM

1단계	2단계	3단계	4단계
사이버 위협 초동 분석	침해사고 정밀 분석	침해사고 대응 방안 마련	침해사고 보고 절차 마련
• 보안관제의 초동 대응 및 분석접수 • 기본 공격 정보로 위협 및 성공여부 등 1차 상황 보고 • 필요 시, 긴급차단 대응	• 취약점 및 피해 유무 에 따른 정밀분석 수행 • 상세정보(시스템로그, 덤프 등) 수집 및 분석 • 피해규모 조사 등	• 침해사고 재발방지 방안 제시 • 사전예방을 위한 보호대책 제시	• 침해사고 타임테이블 정리 및 피해상황 정리 절차 마련 • 내/외부용 침해사고 보고 절차 마련

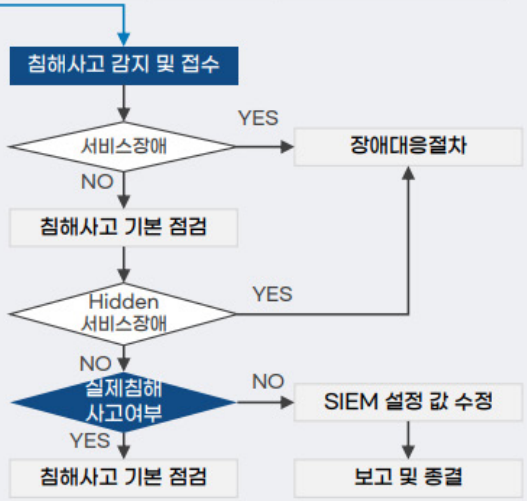
II 침해사고 대응 절차

1 실무 관점의 침해사고 대응 개요

대응 조치

정보수집 → 탐지분석 → **대응/조치** → 보고/사후처리

항목	수행업무	수행인력	대상 시스템
초동 대응	• 수집된 로그를 기반으로 탐지된 이벤트에 대한 공격 유효성 분석	보안관제	SIEM
대응	• 네트워크 트래픽 유입량 및 임계치 설정에 따른 공격 탐지 및 분석	보안관제	FW, IPS, APT 등
분석	• 유관기관 및 최신 위협 정보를 토대로 공격 탐지 및 분석	보안관제	SIEM



보고/사후처리

정보수집 → 탐지분석 → 대응/조치 → **보고/사후처리**

항목	수행업무	수행인력	대상 시스템
시스템 복구	• 피해 확산 방지, 악성코드 제거, 시스템 복원	보안관제	피해 시스템
재발 방지	• 공격에 이용된 취약점 보유 여부 점검	보안관제	피해 시스템
보고	• 공격시간, 방법, 피해유무, 대응방안 등 보고	보안관제	-

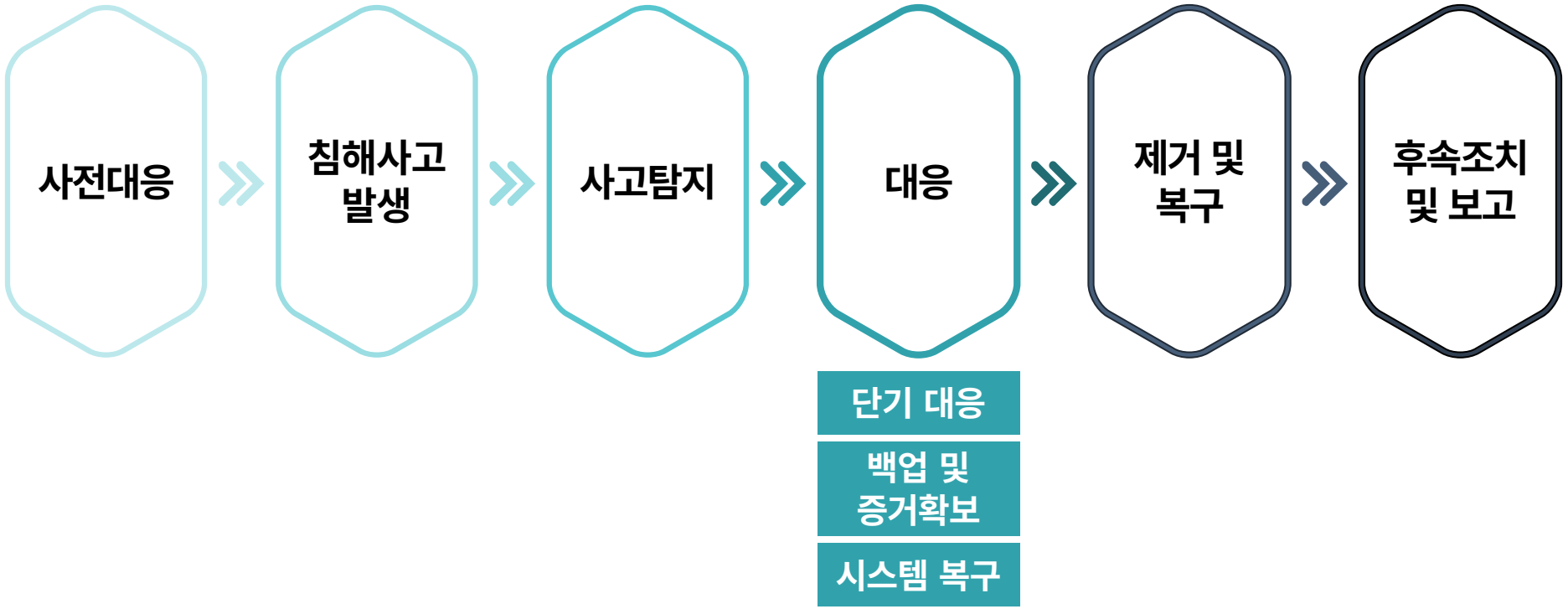
01 피해확산 방지
- 확인된 공격 IP 및 패턴에 대한 타 시스템 분석
- 각 장비별 보안설정 확인
- 최신 보안패치 설치 등 피해원인 제거 및 복구

02 재발방지 보안대책 마련
- 유사 침해시도를 탐지/방지할 수 있는 탐지패턴 개발 및 적용
- 업데이트 / 패치 필요 보안장비에 대한 권고
- 피해내역에 대한 평가 / 보안인식 교육

03 보고 및 철저한 이력관리
- 조치결과에 대해 보안담당자에게 보고
- 철저한 이력관리를 통해 사후 방지 철저

2 침해사고 대응 절차

- 컴퓨터와 관련한 침해사고에 적절히 대응하기 위해 만든 CERT(Computer Emergency Response Team)의 침해 대응 절차



2 침해사고 대응 절차

▪ 사전 대응

등급	상황	대응
1등급	• 분산 서비스 거부 공격을 당하고 있어 정상적인 동작이 불가능 • 침입자에 의해 서버의 중요 파일이 삭제 중 • 트로이 목마 등의 악성 프로그램이 실행되어 정상적인 접근 제어를 실시해도 다른 경로를 통해 침입자의 지속적인 공격 시도 탐지 • 침임자의 공격에 대한 대응 수단이 없는 상황	• 침해사고 발생 상황이라고 판단되면 시스템 담당자가 CERT팀의 팀장에게 즉시 보고 • 단, 긴급 상황에서는 피해를 최소화하기 위해 네트워크의 인터페이스 단절, 전원 공급 중단 등의 조치를 먼저 수행할 수 있음

2 침해사고 대응 절차

▪ 사전 대응

등급	상황
2등급	• 비인가자에 의해 관리자 명령이 실행 중 • 시스템 자원을 불법적으로 사용하는 프로그램이 실행 중 • 일반 사용자의 홈 디렉터리에 시스템 파일 발견 • 일반적이지 않은 숨김 속성의 파일 또는 디렉터리 검출 • 시스템 담당자가 알지 못하는 사용자가 추가되거나 사용자 권한이 임의로 변경
3등급	• 외부 또는 내부로부터의 계속적인 취약점 수집(Scanning) 행위 탐지 • 외부 또는 내부로부터의 계속적인 불법적 접근 시도 탐지 • 외부 또는 내부로부터의 비정상 패킷의 전송량이 증가 • 확산 속도가 빠른 바이러스 경보 인지

2 침해사고 대응 절차

▪ 사전 대응

등급	대응
2등급 · 3등급	• 시스템 담당자가 비인가 접근 시도 및 정보 수집 행위를 발견하면 CERT 팀과 함께 해당 단말기 또는 IP를 조사하여 소속 네트워크 및 조직 파악 • 내부 시스템에서 침입 시도가 발생한 경우에는 시스템 위치를 확인하여 책임자와 접속 경위 등을 조사 • 외부 네트워크로부터 침입 시도가 발생한 경우에는 해당 조직의 시스템 담당자 또는 보안 담당자에게 해당 IP로부터 불법적인 접근 시도가 발생하였음을 통보하고 협조 요청 • 침입 시도에 대한 적절한 조치가 수행되지 않고, 그 위협이 심각한 경우에는 정보수사기관(검찰, 경찰) 및 대외 유관기관(한국인터넷진흥원 등)에 수사 또는 조사를 의뢰 • 침입 시도에 대한 대응이 종료된 이후에는 CERT 팀의 팀장이 침입 시도 방법, 침입 시도 대응책 등이 포함된 '침입 시도 대응 보고서'를 작성하여 관련 담당자에게 이메일 또는 문서로 공지

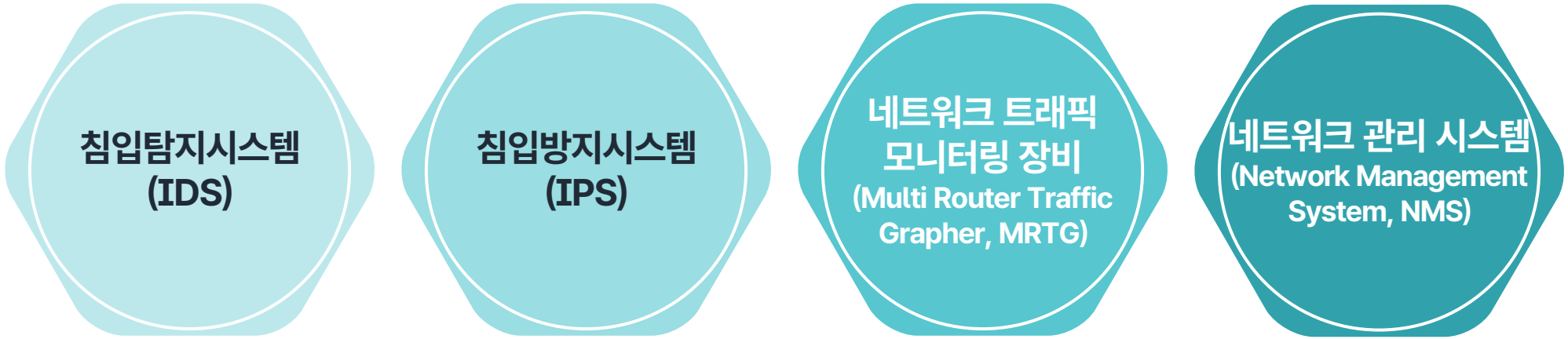
2 침해사고 대응 절차

▪ 사고 탐지

- 침해사고 식별 과정에서 확인해야 할 사항

2 침해사고 대응 절차

- **사고 탐지**
  - 침해사고 발생을 실시간으로 식별하는 과정에 쓰이는 시스템



2 침해사고 대응 절차

- **대응**
  - 침해사고로 인한 손상을 최소화하고 추가적인 손상을 막기 위한 것으로 크게 세 단계에 따라 수행됨

2 침해사고 대응 절차

- 대응

단기대응	백업 및 증거 확보	시스템 복구
• 기본적으로 손상을 최소화하기 위한 단계 • 침해사고가 발생한 시스템이나 네트워크를 식별하고 통제될 수 있는 경우에는 해당 시스템이나 네트워크의 연결을 해제하거나 차단	• 침해사고 발생 후 후속 처리를 위해 침해사고 발생 시스템을 초기화하기 전에 백업 • 포렌식 절차에 따라 시스템의 이미지를 획득하는 과정	• 시스템에 백도어 등의 악성코드를 제거 • 시스템 계정 및 패스워드를 재설정하고 보안 패치 적용 • 다시 서비스가 가능하도록 네트워크에 연결

2 침해사고 대응 절차

▪ 제거 및 복구

- 최초 침해사고 발생을 식별한 시스템 및 네트워크 이외에 추가로 침해사고가 발생한 곳이 있는지 모두 확인하고 조치하는 단계
  - **서비스를 완전하게 복구하는 과정에서 보안 툴을 설치하고 로그 설정을 강화하여 침해사고가 다시 발생하는지 여부를 모니터링하는 것이 중요함**
  - 발생한 침해사고의 유형에 따라 시스템과 네트워크를 어떤 방식과 주기로 모니터링할지 결정한 뒤 완전한 복구를 진행해야 함
  - **제거와 복구가 매우 중요한 침해사고 유형은 랜섬웨어(Ransomware)에 의한 것**
    - 체계적인 백업 시스템으로 침해사고로 인한 데이터 손실을 막는 것이 중요
  - 모든 조치가 완료된 상황에서 서비스를 완전하게 복구

2 침해사고 대응 절차

▪ 후속 조치 및 보고

- 침해사고 식별과 대응 과정은 정해진 기록 문서에 따라 작성
- 작성된 문서와 포렌식 과정에서 획득한 자료를 기반으로 침해사고에 대한 보고서를 작성
- 침해사고의 원인을 확인하고 그 대응책을 마련해야 함

OOO 침해사고 보고

작성자 : OOO
작성일 : 2025-00-00

(1) 침해사고 발생 일지 : 시간대별로 발생 사실 및 확인 사실을 기록한다.
(2) 사고 원인 : 침해사고가 발생한 원인을 기술한다.
(3) 초기 대처 : 침해사고 시 현황과 그에 따른 대응 내용을 기술 한다.
(4) 복구 현황 : 보고서 작성 시점의 복구 현황을 기술한다.
(5) 대처 오류 및 해결 방안 : 사고 대응 과정에서 잘못한 점과 그에 대한 해결 방안을 강구하여 기술한다.

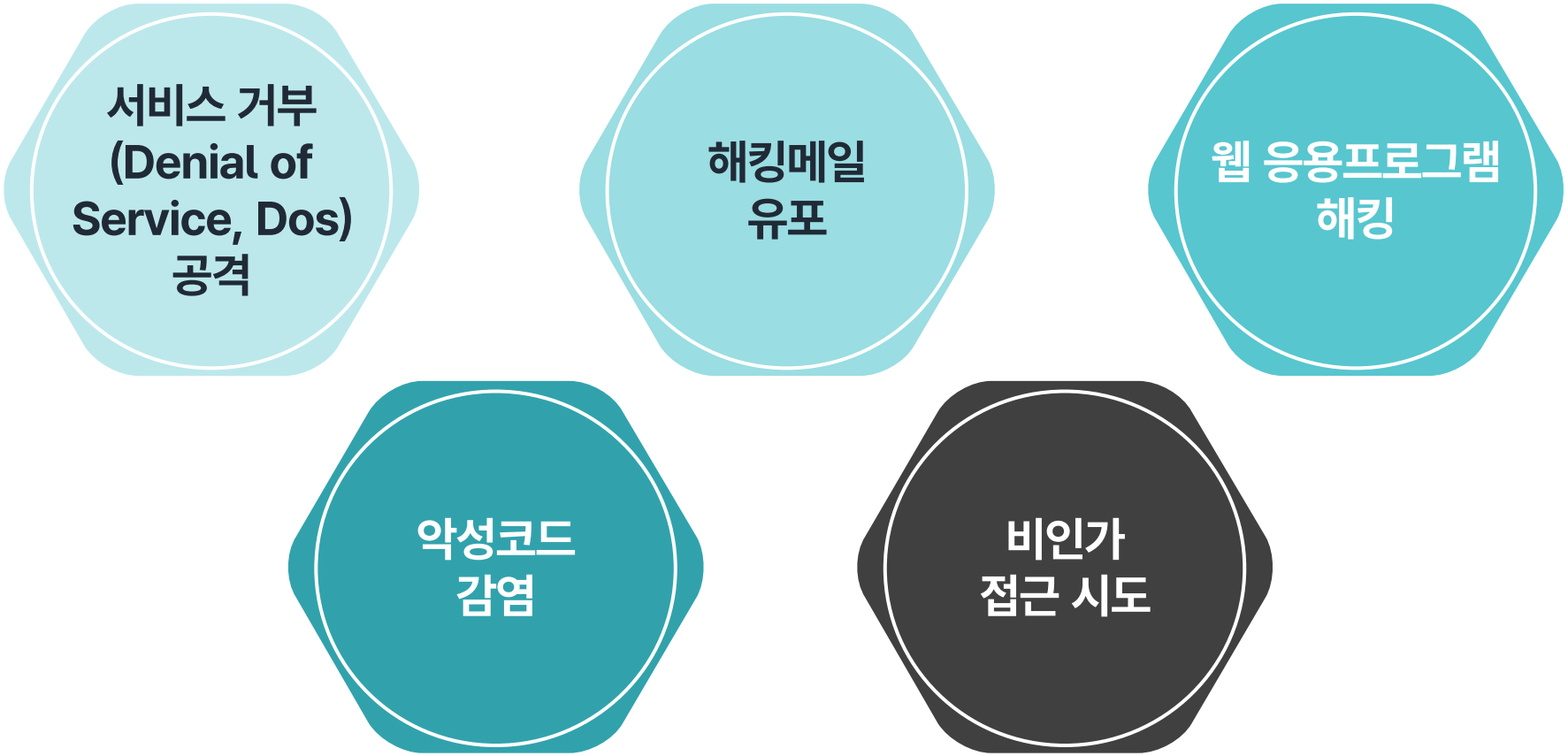
III

침해사고 유형별 대응

III 침해사고 유형별 대응

1 주요 침해사고 유형

- 다양한 해킹 공격 기법들이 있으나 보안관제 관점에서 대응 방책을 고려하여 5가지로 분류



2 서비스 거부(Denial of Service, DoS) 공격

서비스 거부 공격

- 정보통신망 및 정보시스템을 대상으로 대량의 트래픽을 유발시켜 정상적인 서비스를 방해하거나 마비시키는 공격
- 다수의 좀비 PC들을 봇넷(Bot Net)으로 구축하여 대규모로 이루어지는 서비스 거부 공격을 특히 **분산 서비스 거부**(Distributed DoS, DDoS) 공격으로 구분
  - 최근의 서비스 거부 공격은 봇넷 구축 및 공격 자동화를 통해 DDoS화

대표적인 공격 사례

- 7.7 DDos 공격(2009년)
- 3.3 / 3.4 DDos 공격(2011년)
- 320사이버테러(2013년)
- 625사이버테러(2015년)

2 서비스 거부(Denial of Service, DoS) 공격

▪ 서비스 거부(DoS) 공격 수법

통신량 한계 초과 공격	네트워크에 대량의 패킷을 전송하여 **네트워크 대역폭의 처리 한계를 초과**시키는 공격 수법
접속처리 한계 초과 공격	TCP 프로토콜의 통신 특성을 악용하여 **대상 시스템의 자원을 고갈시켜 정상적인 처리를 방해**하는 공격 수법
웹 서버 부하 가중 공격	짧은 시간 동안 반복적으로 웹 페이지를 요청하여 **웹 서버에 과부하를 유발**시키는 공격 수법
웹 응용프로그램 부하 가중 공격	웹 응용프로그램의 보안 약점을 이용하여 **웹 서버 또는 DB 서버에 부하를 가중**시키는 공격 수법

2 서비스 거부(Denial of Service, DoS) 공격

▪ 서비스 거부(DoS) 공격 대응 방책

정상적인 트래픽	비정상적인 트래픽
• 인터넷 서비스 공급자(ISP)에 **대역폭 증설, 해외 트래픽 차단** 등 요청 • QoS(Quality of Service) 정책을 통해 **유입 트래픽량 조절** • **DDoS 사이버 대피소, 싱크홀** 등의 서비스 활용 • 최악의 경우 **서비스 일시 중지**	• 정보보호체계 중 DDoS 대응장비, IPS(침입방지시스템)는 **비정상적인 트래픽에 대한 차단** 가능 • 비정상적인 트래픽을 유발시키는 **공격지 IP, 대역 등 차단** • 패킷 덤프를 통해 패턴 추출 후 발견되는 패턴에 대해 **정보보호체계에 정책 적용**

3 해킹메일 유포

해킹메일 유포

- 정보통신망 및 정보시스템에 대한 공격이 불비한 경우 **사용자 개인을 공격 대상으로 하여 해킹메일을 유포**하는 공격 수법
- 지인으로 위장하거나 권력기관 등을 사칭하는 **사회공학적 방법을 이용**하여 정교하게 이루어지는 경향
- 사용자 PC에 침투한 후 **내부 정보통신망 및 정보시스템까지도 해킹**하는 후속 공격도 가능

대표적인 공격 사례

- 네이버, 카카오 등 포털 사이트 안내메일 사칭(피싱형)
- 외교연구원, 국회의원실 등 안보 관련 기관 사칭(첨부파일형 악성코드)
- 세금 체납, 저작권 침해 안내메일 사칭(첨부파일형 악성코드)

3 해킹메일 유포

▪ 해킹메일 유포 수법

첨부파일형 악성코드	• **MS오피스, 아래한글, PDF 등 문서편집기** 내 임의코드 실행 가능 보안 취약점이나 매크로 기능 악용 • 악성코드를 은닉한 첨부파일을 발송하여 수신자가 **첨부파일을 열람하면 악성코드에 감염**되도록 유도하는 수법
자동감염형 악성코드	• **웹 브라우저, ActiveX, 기타 플러그인** 등의 취약점 악용 • 첨부파일을 열어보지 않고 **메일 본문만 열람했음에도 악성코드에 감염**되도록 유도하는 수법 * 단, 운영체제 보안기능이 강화되면서 줄어드는 추세
피싱형	• **메일 본문 내 링크 클릭 시 공격자가 구축한 피싱 사이트로 연결**되도록 하여 계정 정보, 금융 정보 등의 입력을 유도하는 수법

3 해킹메일 유포

▪ 해킹메일 유포 대응 방책

조직 내 메일서버	조직 외 메일서버	사용자 교육
• **스팸메일 차단시스템** 등 정보보호체계를 도입하여 해킹메일 유입 통제/차단 • 의심스러운 메일에 대한 **신고 프로세스** 운용	• 사용자 PC 등 단말기에 **안티 바이러스** 등 정보보호체계 도입·운용 • 해킹메일 열람 여부를 탐지하기 위해 **IPS(침입차단시스템) 등 정보보호 체계**에 정책 적용	• 사용자에 대한 **지속적인 교육 및 홍보** 캠페인

4 웹 응용프로그램 해킹

웹 응용프로그램 해킹

- 응용프로그램의 기능상 허점, 보안 약점 등을 악용하여 웹 응용프로그램을 변조하거나 악성 파일을 탑재하거나 정보를 절취하는 공격 수법
- 웹 응용프로그램은 사용자가 자료를 입력/변경/삭제할 여지를 제공하고 있어 사용자가 악의적인 목적으로 악성 파일을 웹 서버에 탑재할 수 있는 여지
- 웹 응용프로그램의 복잡도가 증가하면서 보안 약점이 내재되어 있을 가능성 증가
  - 소프트웨어 개발 보안을 적용하고 자동화된 취약점 진단 도구로 확인하더라도 발견하지 못하고 놓치는 보안 약점이 존재할 가능성 증가

침해사고 유형별 대응

4 웹 응용프로그램 해킹

- **대표적인 공격 사례**
  - 2005년, 한국 MSN 뉴스사이트 해킹(악성코드 유포지 악용)
  - 2013년, 청와대 홈페이지 변조(웹 변조)
  - 2014년, KT 홈페이지 개인정보 유출(정보 절취)

4 웹 응용프로그램 해킹

▪ 웹 응용프로그램 해킹 수법

웹 변조	**특정 웹 페이지를 삽입**하거나 **기존의 내용을 변조**하는 공격 수법 * 과거에는 단순 과시를 위한 이미지 삽입 등 단순 변조가 많았으나 **악성코드 유포지 악용과 결합되는 방식으로 발전**하는 추세
악성코드 유포지 악용	다수가 접속하는 웹 사이트에 **악성코드 다운로드를 유도하는 다른 페이지나 스크립트를 삽입**하는 공격 수법
명령제어 경유지 악용	공격자가 자신의 위치를 은폐하기 위한 의도로 **봇넷에서 절취한 자료를 임시 보관하거나 봇넷을 제어하기 위한 명령제어 경유지로 악용**하는 공격 수법
정보절취	웹 응용프로그램이 구동되는 웹 서버 또는 웹 서버에 연결된 다른 서버에 보관되어 있는 **개인정보 등 비공개 자료를 절취**하는 공격 수법

4 웹 응용프로그램 해킹

▪ 웹 응용프로그램 해킹 대응 방책

설계 · 개발 단계	운영 단계
• 설계보안, 개발보안 등 **보안공학** (Security Engineering) 및 **위험관리 방법론** 적용 • 운영 전 **취약점 진단, 모의침투 테스트** 등을 통해 잠재적인 보안 약점 제거	• 공격자가 자주 사용하는 **웹 해킹 패턴을 IPS(침입방지시스템), 웹 방화벽** 등 정보보호체계에 정책 적용 • 웹 응용프로그램이 구동되는 **서버 내 보안OS, 웹 쉘 탐지 솔루션, 웹 변조 탐지 솔루션** 등 도입·운영

5 악성코드 감염

악성코드 감염

- **원격 명령제어, 정보 절취, 시스템 파괴** 등을 목적으로 악성코드를 감염시키는 공격 수법
- 악성코드 **유형** : 웜, 바이러스, 트로이목마, 스파이웨어, 애드웨어, 랜섬웨어 등

5 악성코드 감염

▪ 악성코드 감염 대응 방책

악성코드 다운로드 시	악성코드 실행 시	악성코드 실행 이후
알려진 **악성코드의 주요 패턴을 IPS(침입방지시스템)** 등 정보보호체계에 정책 적용	사용자 PC 등 단말기에 **안티 바이러스** 등 정보보호체계 도입·운용	**외부의 명령제어 서버와 통신**하는 패턴을 IPS(침입방지시스템) 등 정보보호체계에 정책 적용

6 비인가 접근 시도

비인가 접근 시도

- 실제 공격은 아니지만, 공격 등을 수행하기 전에 **정보통신망 및 정보시스템의 취약점을 수집**하기 위한 시도
- 비인가 접근 시도 **유형** : 네트워크 포트 스캐닝, 웹 응용프로그램 디렉토리 구조, 스캐닝 등

▪ 비인가 접근 시도 대응 방책

단순 스캐닝은 차단하지 않음	접근 차단 조치
과도한 차단 시 **서비스 가용성 저하** 우려	지나친 비정상적인 스캐닝 활동 등 식별 시 **해당 IP, 대역 등 차단**

IV

보안관제 문서 산출물 작성

보안관제 문서 산출물 작성

1 보안관제사의 업무 미리보기

출처 캐치가한다 - 청년친화강소기업 윈스편, 캐치TV(2020.06.23), https://www.youtube.com/watch?v=QMmgcfye-lY

IV 보안관제 문서 산출물 작성

1 보안관제사의 업무 미리보기

보안관제서비스 전문기업 윈스의 사례

자체 개발 보안관제시스템

- 다양한 가시화 및 시각화 기능을 제공하는 보안관제시스템 활용
- 실시간 모니터링 수행

출처 캐치가한다 - 청년친화강소기업 윈스편, 캐치TV(2020.06.23), https://www.youtube.com/watch?v=QMmgcfye-lY

보안관제 문서 산출물 작성

1 보안관제사의 업무 미리보기

보안관제서비스 전문기업 윈스의 사례

침해시도/침해사고 및
사이버보안 이벤트 발생

공격자 IP 식별 및
탐지/차단 규칙에 적용

오탐의 경우
탐지/차단 규칙에서 해제

관련 내용 정리하여
보고서 작성

출처 캐치가한다 - 청년친화강소기업 윈스편, 캐치TV(2020.06.23), https://www.youtube.com/watch?v=QMmgcfye-lY

보안관제 문서 산출물 작성

1 보안관제사의 업무 미리보기

보안관제서비스 전문기업 윈스의 사례

보안관제사의 업무는
각 보안관제 조직의 특성을 고려한 업무 프로세스에 의해 이루어짐

- **보안관제사는 업무 프로세스에 따라 보안관제 업무를 수행하고 업무 간 각종 산출물을 조직에서 정한 문서 형태로 작성**

2 문서 산출물의 이해

- 정보보안 경영시스템(Information Security Management Systems, ISMS)에 대한 ISO/IEC 국제 표준에서는 **'문서화된 정보'로 유지**하여야 함을 규정

- *The scope shall be available as documented information.*

. . .

- *The organization shall retain documented information about the information security risk assessment process.*

. . .

- *The organization shall retain documented information about the information security risk treatment process.*

. . .

- *The organization shall retain documented information of the results of the information security risk assessments.*

. . .

ISO/IEC 27001(정보보안 경영시스템에 대한 국제 표준)

출처 ISO/IEC 27001:2022 본문 중 일부, ISO/IEC 27001:2022, https://www.iso.org/standard/27001

보안관제 문서 산출물 작성

2 문서 산출물의 이해

문서 산출물 = **문서화**된 정보

- **조직 내·외부의 이해관계자 간 의사소통**을 위해 활용 가능한 문서화된 정보
- **경영진 등이 중요한 의사결정**을 위해 활용 가능한 문서화된 정보
- 업무의 성과측정을 위해 **업무 내역을 측정 가능한 형태로 가시화**하는 문서화된 정보

24시간 365일 지속되는 보안관제 업무에서도 **문서 산출물을 생성·유지**하는 것이 중요

3 보안관제 문서 산출물

보안관제 문서 산출물

보안관제 업무 간 발생되는 문서화된 정보

3 보안관제 문서 산출물

▪ 주요 산출물 유형

티켓 처리	• 요청서, 확인/내역서 등 티켓의 처리 과정에 따라 생산되는 문서
전파문	• 상황전파문, 보안권고문 등
보고서	• 정기(일일/주간/월간) 보고서 • 침해시도/침해사고 보고서 • 사이버위협정보(CTI) 보고서 • 성과분석 보고서 • 기타 조직에서 정하는 유형의 보고서
통계	• 전자적 방식에 의해 집계·산출된 내역을 정리한 문서

4 티켓 처리

티켓(Ticket)

어떤 이벤트가 발생했을 때 발생된 이벤트와 관련한 **전 작업 주기를 관리하기 위한 단위**

침해시도/ 침해사고	• **침해시도/침해사고가 발생**되면 해당 이벤트에 대한 티켓을 자동으로 생성/발행하고 모든 조치가 완료되면 종결 처리
이관 요청	• **타 조직 또는 부서 간 이벤트의 이관을 요청**할 때 티켓을 생성/발행하고 모든 조치가 완료되면 종결 처리
기술지원 요청	• **조직 내 구성원이 기술지원을 요청**할 때 티켓을 생성/발행하고 모든 조치가 완료되면 종결 처리

보안관제 문서 산출물 작성

4 티켓 처리

수많은 티켓을 효율적으로 관리하기 위해
전자적 처리를 위한 티켓처리시스템을
도입·운영하더라도 **각 티켓에 대한 문서 산출물을 내보내는 기능은 구비**

4 티켓 처리

- **예시) 침해시도/침해사고 정보 이관**

① 보안관제팀에서 침해시도/침해사고를 탐지

② 보안관제팀 및 기술지원팀에 의한 초기 분석 결과, 법령에 따라 유관기관에 이관해야 하는 사이버공격 유형으로 확인

③ '침해시도/침해사고 정보 이관 요청서' 작성

- 대부분 이관 대상 조직에서 정하고 있는 서식 적용

④ 작성된 '침해시도/침해사고 정보 이관 요청서'를 이관 대상 조직에 전달

- 공문서, 전자문서(문서24), 이메일 등 이관 대상 조직에서 정하고 있는 방식 적용

⑤ 이관 대상 조직에서 문서를 접수한 후 '접수확인서' 회신

- 정상 접수의 경우 최종 처리 후 '처리결과서'로 갈음하고 접수되지 않은 경우에 한하여 반송 가능

⑥ 이관 대상 조직에서 최종 처리 후 '처리결과서' 회신

4 티켓 처리

▪ 예시) 침해시도/침해사고 정보 이관

- 주요 포함 항목

탐지 정보	• 조직명, 담당자, 탐지된 이벤트명, 탐지방법, 발생 일시, 이관 요청 일시, 연락처
침해시도/ 침해사고 정보	• 출발지 IP, 출발지 포트, 목적지 IP, 목적지 포트, 경유 IP, 발생 건수(건/분), 침해시도/침해사고 유형, 주요 내용

보안관제 문서 산출물 작성

5 전파문

전파문

상황을 알리거나 **보안 패치/업데이트** 등 **보안조치를 권고**하는 등의 목적으로 작성하는 문서

보안관제 문서 산출물 작성

5 전파문

상황전파문	상황해제문	보안권고문	사이버위기경보 발령문
위계를 갖춘 보안운영센터의 경우 상위 보안운영센터에서 하위 보안운영센터에 상황을 공유하고 조치를 지시하는 상황전파문 발송 예 국가 보안운영센터 (국가정보원) ↓ 단위 보안운영센터 (국방사이버지휘통제센터 / 사이버작전사령부)	상황전파문이 더 이상 유효하지 않은 경우 조치 해제를 지시하는 상황해제문 발송	조직 내 업무 시스템의 공지사항에 알려진 보안 취약점에 대해 보안 패치/업데이트 등 보안조치를 권고하는 보안권고문 게시	국가사이버안보센터 등 법령에서 정한 사이버위기경보 발령권자에 의한 사이버위기경보 상향 또는 하향에 대한 발령문 게시

보안관제 문서 산출물 작성

5 전파문

- 예시) 상황전파문(한국인터넷진흥원 C-TAS)

IP

2024-04-11 상황전파문

등록일 2024.04.11 위협정보수 7

CSV

JSON

발생일시	위협정보	국가코드
2024.04.11 20:10	61.223.129.92	TW
2024.04.11 20:10	114.47.89.149	TW
2024.04.11 20:10	43.255.118.51	HK
2024.04.11 20:10	43.255.118.52	HK
2024.04.11 20:10	111.253.224.242	TW
2024.04.11 20:10	43.255.118.50	HK

보안관제 문서 산출물 작성

5 전파문

- 예시) 사이버위기경보 발령문(국가사이버안보센터)

[주의 경보발령] 국가공공기관 사이버위기 '주의' 경보 상향발령

작성일 : 2017.03.09

□ 내용

o 국가사이버안전센터는 최근 복잡한 주변정세에 편승한 국내 기관 및 단체 대상의 해킹시도 증가 및 한미 연합 훈련 기간 중 북한에 의한 사이버공격 가능성 고조 등에 적극 대응하기 위해 3.9(목) 18:00부 사이버위기 '주의' 경보를 발령

□ 발령 취지

o 각급기관 보안활동 강화 및 국가 정보통신기반시설 전반에 보안 태세 강화 필요

□ 대응 요령

o 각급기관은 위기대응 실무매뉴얼에 따라 사이버위기'주의'경보단계 대응활동 수행(국정원 홈페이지 → 사이버위기경보 → 경보단계 참고)

o 각급기관 및 보안관제센터는 근무보강 등 비상근무태세 유지

보안관제 문서 산출물 작성

6 보고서

보고서

조직 내에서 **보고 목적**으로 생산하는 문서

정기(일일/주간/월간) 보고서	• 보안관제 업무에 대한 일상적인 보고서
침해시도/ 침해사고 보고서	• 침해시도/침해사고 발생에 따른 대응 및 조치 경과를 보고하는 문서
사이버위협정보 (CTI) 보고서	• 사이버위협정보의 수집 및 분석에 따른 정보판단을 위한 보고서
성과분석 보고서	• 연감/연차보고서와 같이 단위 기간(분기/반기/연)에 대한 업무성과를 분석한 보고서
기타	• 기타 조직에서 정하는 유형의 보고서

6 보고서

▪ 예시) 정기(일일/주간/월간) 보고서

- 주요 포함 항목
  - 기본 정보 : 근무일자, 보고일자, 근무자(소속/업무/성명)
  - 결재선
  - 환경 정보 : 사이버위기경보 단계, 대내·외 주요 동향 등
  - 일일/주간/월간 보안관제 건수
    * 사이버위협 대응, 보안권고 및 위기경보 전파, 상황전파문(유해 IP/URL 차단 등), 탐지/차단 규칙 등 정책 변경, 기타
  - 보안관제 주요 내용
    * 보안권고 및 위기경보 전파, 상황전파문, 정책 변경, 기타 특이사항
  - 공격유형별 대응현황
    * 유형(시스템 취약점, 웹 취약점, 비인가 접근, 서비스 거부, 웜/바이러스, 정보수집, 합계)별 전일 탐지, 금일 탐지, 전일 대응, 금일 대응 내역을 수록한 표

6 보고서

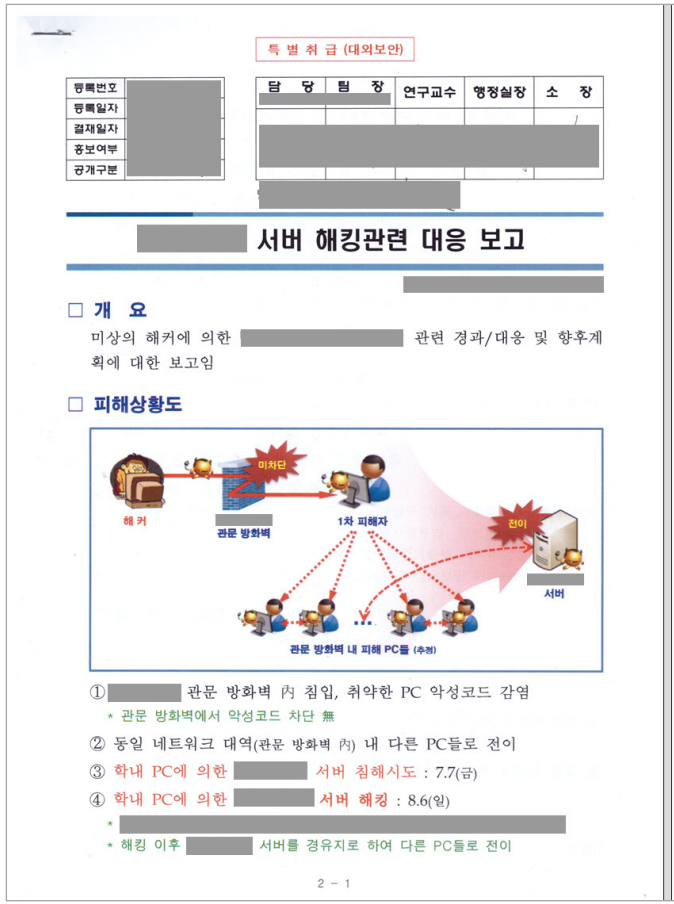
▪ 예시) 침해시도/침해사고 대응 보고서

- 주요 포함 항목
  - 보고서 제목, 보고 일시, 담당자, 결재선
  - 개요 : 보고 문건에 대한 개요(2~3줄 이내)
  - 환경 정보 : 사이버위기경보 단계, 대내·외 주요 동향 등
  - 피해상황도 : 피해상황에 대한 요약 그림 및 설명
  - 경과 및 조치사항
    * 사건에 대한 경과 및 조치사항을 시간 순으로 나열
  - 사고 원인 : 조사/분석을 마친 경우 사고 원인에 대한 설명
  - 후속조치 계획 : 보고 이후 후속조치에 대한 계획을 설명

보안관제 문서 산출물 작성

6 보고서

- 예시) 침해시도/침해사고 대응 보고서



특 별 취 급 (대외보안)

등록번호	[redacted]
등록일자	
결재일자	
홍보여부	
공개구분	

담 당	팀 장	연구교수	행정실장	소 장
[redacted]				

[redacted] 서버 해킹관련 대응 보고

□ 개 요

미상의 해커에 의한 [redacted] 관련 경과/대응 및 향후계획에 대한 보고임

□ 피해상황도

① [redacted] 관문 방화벽 內 침입, 취약한 PC 악성코드 감염
* 관문 방화벽에서 악성코드 차단 無
② 동일 네트워크 대역(관문 방화벽 內) 내 다른 PC들로 전이
③ 학내 PC에 의한 [redacted] 서버 침해시도 : 7.7(금)
④ 학내 PC에 의한 [redacted] 서버 해킹 : 8.6(일)
* [redacted]
* 해킹 이후 [redacted] 서버를 경유지로 하여 다른 PC들로 전이

2 - 1

특 별 취 급 (대외보안)

□ 경과사항

○ [redacted]로 침해사고 통보(국가정보원 NCSC 이관) : 8.24(목)
* [redacted]
○ [redacted] 취약점 진단 진행 : 8.25(금) ~ 8.31(목)
○ [redacted] : 9.1(금) 17:30
○ [redacted] 취약점 진단 진행 : 9.4(월) ~ 9.6(수)
○ 사고 서버 백업 및 디스크 이미지 확보 : 9.7(목) ~ 9.8(금)
○ 사고 서버 [redacted] 작업 : 9.8(금) ~ 9.11(월)
* [redacted] 수행 예정

□ 사고원인

○ [redacted] 존재
* [redacted]
○ 서버 등 정보체계 비밀번호 취약성 존재
○ 보안 관련 위협 동향 및 정보 숙지 미흡
○ 관련 법령 · 규정의 숙지 및 이행 미흡

[redacted]

□ 향후계획 / 결언

○ 피해 서버 복구 및 재운영 준비
* 재운영 전 취약점 점검 [redacted]
○ [redacted]
* [redacted]
* [redacted]
○ 무분별한 정보체계(홈페이지, NAS 등) 도입 지양 : 도입 시 보안성 검토 必

//끝//

2 - 2

보안관제 문서 산출물 작성

7 보안관제 문서 산출물의 중요성

- 정보보안 국제표준에서 정하고 있는 기본원칙(문서화된 정보의 유지) 준수
- 관계법령, 규정, 지침에서 정하고 있는 규제적 요건 충족
- 단편적인 로그만으로는 이해하기 어려운 맥락적 정보 제공
- 보안사고 발생 시 책임추적성(Accountability)을 위해 필요한 감사증적(Audit Trail)
- 유효한 법정 증거로 채택 가능

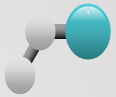
요약 정리

- 지금까지 학습한 내용을 정리해보겠습니다.

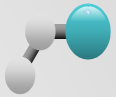
요약정리

- **침해사고의 이해**
  - **CERT(Computer Emergency Response Team)**
    - 침해사고를 대응하고 보안사고를 대비하는 역할을 하는 비상대응조직
    - **필요 구성원 :** 시스템 운영 전문가, 대외 언론 및 외부기관 대응 전문가, 법률팀, 인사팀
- **침해사고 대응 절차**
  - **사전대응 → 침해사고 발생 → 사고탐지 → 대응 → 제거 및 복구 → 후속조치 및 보고**
    - **사전대응 :** 등급 및 상황을 고려한 대응
    - **사고탐지 :** 사고 발생시점, 사고 발견자 및 보고자, 발견 경위, 발생 범위 및 손해 내용 등에 대한 확인
    - **대응 :** 침해사고로 인한 손상을 최소화하고 추가적인 손상을 막기 위해 세 단계에 따라 수행
      - 단기대응 → 백업 및 증거 확보 → 시스템 복구
    - **제거 및 복구 :** 추가적인 침해사고를 확인하여 조치하고, 모든 조치가 완료된 상황에서 완전한 복구
    - **후속조치 및 복구 :** 문서를 작성하고 원인을 확인하여 대응책 마련

요약정리



- **침해사고 유형별 대응**
  - **서비스 거부(Denial of Service, DoS) 공격**
    - 대량의 트래픽을 유발시켜 정상적인 서비스를 방해하거나 마비시키는 공격
  - **해킹메일 유포**
    - 개인을 공격 대상으로 하여 해킹메일을 유포하는 공격 수법
  - **웹 응용프로그램 해킹**
    - 웹 응용프로그램을 변조하거나 악성 파일을 탑재하거나 정보를 절취하는 공격 수법
  - **악성코드 감염**
    - 원격 명령제어, 정보절취, 시스템 파괴 등을 목적으로 악성코드를 감염시키는 공격 수법
  - **비인가 접근 시도**
    - 실제 공격은 아니지만, 공격 등을 수행하기 전에 정보통신망 및 정보시스템의 취약점을 수집하기 위한 시도



보안관제 문서 산출물 작성

보안관제 문서 산출물

- 보안관제 업무 간 발생되는 문서화 된 정보
  - 24시간 365일 지속되는 보안관제 업무에서도 문서 산출물을 생성 · 유지하는 것이 중요
  - 특히, 정보보안 경영시스템 국제 표준에서는 문서화 된 정보(documented information)의 유지에 대해 규정
- 조직 내 · 외부의 이해관계자 간 의사소통 및 경영진 등의 중요한 의사결정에 활용 가능
- 업무의 성과측정을 위해 업무 내역을 측정 가능한 형태로 가시화

주요 유형

- **티켓(Ticket) 처리 :** 요청서, 확인/내역서 등 티켓의 처리 과정에 따라 생산되는 문서
- **전파문 :** 상황을 알리거나 보안 패치/업데이트 등 보안조치를 권고하는 등의 목적으로 작성하는 문서
- **보고서 :** 조직 내에서 보고 목적으로 생산하는 문서
- **통계 :** 전자적 방식에 의해 집계 · 산출된 내역을 정리한 문서

참고문헌

- 정보통신기반보호법 (법률)
- 정보통신망 이용촉진 및 정보보호 등에 관한 법률 (법률)
- 사이버안보 업무규정 (대통령령)
- 국가사이버안전관리규정 (대통령훈령)
- 국가 정보보안 기본지침 (국가정보원 지침)
- 보안관제학, 2014, 안성진 등 공저, 이한미디어
- 2023 국가정보보호백서, 2023, 국가정보원 등 관계기관 합동
- 국가사이버안보센터 웹 사이트, http://www.ncsc.go.kr
- 한국인터넷진흥원 웹 사이트, http://www.kisa.or.kr
- KISA 보호나라 & KrCERT/CC 웹 사이트, http://www.krcert.or.kr
- 캐치가 한다 - 청년친화강소기업 윈스편, 캐치TV, 2020.06.23, https://www.youtube.com/watch?v=QMmgcfye-lY

수고하셨습니다