악성코드 / 해킹 / 정보 유출

# 침해사고 조사 및 대응 실무 과정

5일 교육과정 커리큘럼


INSEC security

악성코드 / 해킹 / 정보 유출

# 침해사고 조사 및 대응 실무 과정 (5일)

| 교육일정 | 교육내용 | 교육시간 |
|---|---|---|
| 1일차 | **침해사고 조사 개요**<br>- 침해사고 정의<br>- 침해사고 유형 | 10:00 ~ 10:50 |
| | **침해사고 조사 절차**<br>- 침해사고 조사 준비 절차<br>- 침해사고 단계별 수집, 분석, 결과 보고 단계별 절차 | 11:00 ~ 11:50 |
| | **침해사고 사례**<br>- 국내 침해사고 사례<br>- 해외 침해사고 사례 | 13:00 ~ 13:50 |
| | **침해사고 관련 증거 데이터 수집**<br>- 데이터 수집 절차<br>- 원격 데이터 수집<br>- Off Line 데이터 수집<br>- Log Data 수집 | 14:00 ~ 14:50 |
| | **침해사고 관련 증거 데이터 수집 및 분석 도구**<br>- FTK Imager를 이용한 데이터 수집<br>- EnCase Imager를 이용한 데이터 수집<br>- AXIOM을 이용한 데이터 수집<br>- X-Ways Forensics를 이용한 데이터 수집<br>- Forensic Falcon을 이용한 하드디스크 복제 및 이미징<br>- Media Imager를 이용한 하드디스크 복제 및 이미징<br>- Forensic MagiCube Pro를 이용한 하드디스크 복제 및 이미징 | 15:00 ~ 15:50 |
| | **메모리 덤프**<br>- 메모리 덤프 개요<br>- 메모리 구조<br>- 메모리 덤프 절차 | 16:00 ~ 16:50 |
| | **메모리 덤프 및 분석 도구**<br>- Dump it을 이용한 메모리 덤프 실습<br>- FastDump Pro를 이용한 메모리 덤프 실습<br>- MAGNET PROCESS CAPTURE를 이용한 메모리 및 프로세스 덤프 실습<br>- Responder Pro를 활용한 메모리 분석<br>- MAGNET AXIOM을 이용한 메모리 분석<br>- Volatility를 이용한 메모리 분석 | 17:00 ~ 17:50 |
| | 질문 & Review | 17:50 ~ 18:00 |
| | * 교육 진행 시 사용 툴<br>EnCase, EnCase Imager, FTK Imager, MAGNET AXIOM, X-Ways Forensics<br>Forensic Falcon, Media imager, Forensic MagiCube Pro<br>Dump it, FastDump Pro, MAGNET Process Capture Responder Pro, Volatility 등 | |

* 교육 시간 및 교육 내용은 사정에 따라 변동될 수 있으니 참고 바랍니다.

상담문의 : 02-851-5687

악성코드 / 해킹 / 정보 유출

# 침해사고 조사 및 대응 실무 과정 (5일)

| 교육일정 | 교육내용 | 교육시간 |
|---|---|---|
| 2일차 | **디지털 포렌식 조사 절차**<br>– 침해사고 관련 증거데이터 조사절차<br>– 주요 정보 유출 방식 | 10:00 ~ 10:50 |
| | **정보유출 사례별 사고 조사 기법**<br>– 외부 불법 침입에 의한 정보유출 사례<br>– 내부 직원에 의한 정보 유출 사례<br>– 원격지에서 내부 시스템 접속 중 정보 유출 사례<br>– USB, 외장 하드 등 이동식 저장매체에 의한 정보 유출 사례 | 11:00 ~ 11:50 |
| | **정보유출 사고 관련 아티팩트 분석 – 저장장치**<br>– 최근 검색내역 수집 및 분석<br>– Windows Event log 수집 및 분석<br>– 최근 실행된 응용프로그램 수집 및 분석<br>· UserAssist<br>· Prefetch<br>· ShimCache<br>· AmCache<br>· etc | 13:00 ~ 14:50 |
| | **정보유출 사고 관련 아티팩트 분석 – 저장장치**<br>– 최근 실행된 문서 리스트 확인<br>– 최근 사용한 이동식 저장장치 정보 수집 및 분석<br>– 인터넷 / SNS 등 접속 흔적 및 다운로드 파일 분석<br>– E-mail / Cloud Service 등 접속 흔적 및 첨부 파일 분석 | 15:00 ~ 15:50 |
| | **정보유출 사과 관련 아티팩트 분석 – 네트워크**<br>– 공유 폴더 운용 또는 접근 흔적 or 증거 수집 및 분석<br>– FTP 사이트 접근 흔적 or 증거 수집 및 분석<br>– File Server / Mail Server 접근 흔적 or 증거 수집 및 분석<br>– 개발 서버, 기타 중요 서버 접근 흔적 or 증거 수집 및 분석 | 16:00 ~ 16:50 |
| | **정보유출 사고 관련 아티팩트 분석 – 안티포렌식 기법**<br>– 볼륨 암호화 탐지 및 분석<br>– 문서 암호화 탐지 및 복호화<br>– 압축파일 암호화 탐지 및 복호화<br>– 시그니처 변조 파일 탐지 및 복호화<br>– Root kit을 이용한 프로세스 은닉 탐지<br>– Slacker를 이용한 파일 은닉 탐지<br>– ADS 영역을 이용한 파일 은닉 탐지 | 17:00 ~ 17:50 |
| | 질문 & Review | 17:50 ~ 18:00 |
| | * 교육 진행 시 사용 툴<br>EnCase, X-Ways Forensics, Responder Pro, MAGNET AXIOM, Volatility 등 | |

* 교육 시간 및 교육 내용은 사정에 따라 변동될 수 있으니 참고 바랍니다.

상담문의 : 02-851-5687

악성코드 / 해킹 / 정보 유출

# 침해사고 조사 및 대응 실무 과정 (5일)

| 교육일정 | 교육내용 | 교육시간 |
|---|---|---|
| 3일차 | **악성코드 개요**<br>– 악성코드 개요<br>– 악성코드 종류 및 유형 별 특징<br>– 악성코드 분석 절차 **(기초/동적/정적 분석 차이점 이해)**<br>– 분석 단계 별 활용 도구 | 10:00 ~ 10:50 |
| | **침해사고 관련 증거 데이터 수집**<br>– 바이너리 분석을 통한 패킹 여부 탐지<br>– 멀티 백신 검사 서비스를 이용한 악성코드 사전 식별<br>– 스트링 분석을 통한 가독성 문자열 추출 | 11:00 ~ 11:50 |
| | **실제 악성코드 샘플 분석 실습 – 백도어/봇넷 계열**<br>– 오픈 소스 도구를 활용한 동적 분석 **[ Procmon 활용 ]**<br>– 동적 분석 시 주의 깊게 봐야할 핵심 이벤트 설명<br>– 동적 분석 결과 그래픽 도식화를 통한 상세 분석 실습 | 13:00 ~ 13:50 |
| | **실제 악성코드 샘플 분석 실습 – 백도어/봇넷 계열**<br>– 디버깅 기술을 이용한 정적 분석<br>– 올리디버거(OllyDBG) 사용법 및 분석 가이드 | 14:00 ~ 14:50 |
| | **자동화 분석 도구를 활용한 악성코드 분석**<br>– 샌드박스 분석을 통한 악성코드 상세 분석 실습<br>– 주요 파일 / 네트워크 / 레지스트리 관련 악성 행위 판별 방법 | 15:00 ~ 15:50 |
| | **패킹(Packing) 기술**<br>– 패킹의 개념 및 사용 목적<br>– 패킹과 파일 압축의 차이점<br>– 악성코드가 패킹을 사용하는 이유<br>– 패커 종류 및 기능 설명 | 16:00 ~ 16:50 |
| | **매뉴얼 언패킹(Manual Unpacking)**<br>– 언패킹이란?<br>– 패킹 된 악성코드 분석 방법<br>– 다양한 방식의 언패킹 실습 | 17:00 ~ 17:50 |
| | 질문 & Review | 17:50 ~ 18:00 |
| | *** 교육 진행 시 사용 툴**<br>IDA Pro, Hex Decompiler, Process Monitor, PEid, OllyDBG, Metadefender, Joe Sandbox, Malzilla, SSView 등 | |

* 교육 시간 및 교육 내용은 사정에 따라 변동될 수 있으니 참고 바랍니다.

상담문의 : 02-851-5687

악성코드 / 해킹 / 정보 유출

# 침해사고 조사 및 대응 실무 과정 (5일)

| 교육일정 | 교육내용 | 교육시간 |
|---|---|---|
| 4일차 | **인젝션 계열 악성코드 분석**<br>– DLL 및 실행 코드 인젝션을 통한 악성코드 동작 방식 이해<br>– 레지스트리를 이용한 DLL 인젝션 실습 | 10:00 ~ 10:50 |
| | **인젝션 계열 악성코드 분석**<br>– 디버거를 활용한 랜섬웨어 정적 분석<br>– 인젝션 악성코드 API 루틴 분석 | 11:00 ~ 11:50 |
| | **문서 파일 계열 악성코드 분석 – MS오피스 파일 계열**<br>– MS오피스 파일 포맷 유형 및 OLE 파일 포맷 구조 이해<br>– 매크로 악용 / 하이퍼링크 / DDE 악용 특징 이해<br>– 오픈 소스 도구를 활용한 문서 파일 내부 구조 분석 | 13:00 ~ 13:50 |
| | **문서 파일 계열 악성코드 분석 – MS오피스 파일 계열**<br>– 오픈 소스 도구를 활용한 문서 파일 내부 구조 분석<br>– 매크로를 악용한 문서 파일 분석 방법 | 14:00 ~ 14:50 |
| | **문서 파일 계열 악성코드 분석 – 한컴오피스 파일 계열**<br>– 한컴오피스 문서 파일 포맷 유형 및 파일 포맷 구조 이해<br>– 매크로 악용 / 하이퍼링크 악용 사례 | 15:00 ~ 15:50 |
| | **문서 파일 계열 악성코드 분석 – 한컴오피스 파일 계열**<br>– 오픈 소스 도구를 활용한 문서 파일 내부 구조 분석<br>– 한글 파일(.hwp / hwpx) 계열 악성코드 분석 실습 | 16:00 ~ 16:50 |
| | **문서 파일 계열 악성코드 분석 – 한컴오피스 파일 계열**<br>– PostScript 악용 한글 악성코드 분석 실습 | 17:00 ~ 17:50 |
| | 질문 & Review | 17:50 ~ 18:00 |
| | * 교육 진행 시 사용 툴<br>OllyDBG, IDA Pro, OleVIewer, HwpScan, 등 | |

* 교육 시간 및 교육 내용은 사정에 따라 변동될 수 있으니 참고 바랍니다.

상담문의 : 02-851-5687

악성코드 / 해킹 / 정보 유출

# 침해사고 조사 및 대응 실무 과정 (5일)

| 교육일정 | 교육내용 | 교육시간 |
|---|---|---|
| 5일차 | **메모리 분석**<br>– 메모리 분석 개념 및 동작 원리 설명<br>– 악성코드 분석에서의 메모리 분석 필요성 이해<br>– 메모리 분석 절차 및 활용 도구 설명 | 10:00 ~ 10:50 |
| | **실제 악성코드 샘플 분석 실습 – 정보 탈취 악성코드 계열**<br>– 메모리 분석을 통한 정보 탈취 악성코드 분석 실습<br>– 메모리 내 의심되는 프로세스 식별 방법 | 11:00 ~ 11:50 |
| | **실제 악성코드 샘플 분석 실습 – 정보 탈취 악성코드 계열**<br>– 인젝션 공격 탐지 방법<br>– 메모리 내 바이너리 덤프 방법<br>– 멀티 백신 검사 서비스를 이용한 바이너리 판별 | 13:00 ~ 13:50 |
| | **EDR(Endpoint Detection & Response) 개념 이해**<br>– EDR이란?<br>– EDR 종류<br>– VMware Carbon Black EDR 소개<br>– EDR을 통한 침해사고 탐지 실습 – 랜섬웨어 악성코드<br>– EDR을 통한 침해사고 탐지 실습 – 백도어/봇넷 악성코드 | 13:00 ~ 13:50 |
| | **Sandbox 솔루션**<br>– 샌드박스(Sandbox) 란?<br>– 샌드박스(Sandbox) 종류<br>– 샌드박스를 통한 샘플 분석 실습 – Windows 악성코드<br>– 샌드박스를 통한 샘플 분석 실습 – Android 악성코드<br>– EDR 솔루션과 통합 실습 | 14:00 ~ 14:50 |
| | **MITRE ATT&CK 프레임 워크**<br>– MITRE ATT&CK 란?<br>– MITRE ATT&CK 구조<br>(Matrix, Tactics, Techniques, Mitigations, Groups)<br>– MITRE ATT&CK for Enterprise<br>– MITRE ATT&CK 활용 및 도식화<br>– JOE Sandbox & Carbon Black EDR과 통합 실습 | 16:00 ~ 16:50 |
| | **질문 & Review** | 17:50 ~ 18:00 |
| | *** 교육 진행 시 사용 툴**<br>VMware Carbon Black EDR, JOE Sandbox, Any.run,<br>Maestro CTIP 플랫폼, Maestro iNSIGHT – Android Analyzer | |

* 교육 시간 및 교육 내용은 사정에 따라 변동될 수 있으니 참고 바랍니다.

상담문의 : 02-851-5687

# (주)인섹시큐리티 공인 교육센터

교육센터 지점별 안내 [ 서울 독산 / 제주 함덕 ] 바로가기

교육일정 안내 바로가기

교육문의 : 02-851-5687


INSEC security