(주)인섹시큐리티 공인 교육센터

## 디지털 포렌식 / 자격증 과정

# AX310
# 자격증 과정

4일

2023.06

INSEC security

## ✓ AX310 자격증 과정

| 교육일정 | 교육내용 | 교육시간 |
|---|---|---|
| 1일차 | **MODULE 1**<br>– AX310 진행 절차 안내<br>– AXIOM Process / Examine 소개 | 10:00 ~ 10:50 |
| | **MODULE 2 – 악성코드 ( Malware ) 개요**<br>– 악성코드 행위<br>– 악성코드 종류<br>– 파워쉘 로드 분석 ( Powershell log ) | 11:00 ~ 11:50 |
| | **MODULE 3 – 패킷 분석 ( Packet )**<br>– 패킷 개요 및 패킷 주요 정보<br>– 패팃 수집 툴 활용<br>– PCAP 파일 분석 | 13:00 ~ 13:50 |
| | **MODULE 4 – 사고대응 분석**<br>– 휘발성 데이터 수집<br>– 기본 시스템 정보 수집<br>– 실행 프로세스 정보 수집 | 14:00 ~ 14:50 |
| | **MODULE 4 – 사고대응 분석**<br>– 서비스 항목 수집<br>– 예약된 프로세스 수집<br>– 네트워크 정보 수집 | 15:00 ~ 15:50 |
| | **MODULE 4 – 사고대응 분석**<br>– 방화벽 정보 수집<br>– 프리패치 ( Prefetch ) 정보 수집<br>– 무선 인터넷 ( Wi-fi ) 정보 수집<br>– MPC( Magnet Process Capture )를 통한 정보 수집<br>– 보조 기억장치 이미징 | 16:00 ~ 16:50 |
| | 질문 & Review | 16:50 ~ 17:00 |
| | *** 교육 진행 시 사용 툴**<br>MAGNET AXIOM | |

* 교육시간 및 교육 내용은 강의 내용 / 설명 / 질문에 따라 조금씩 변경 될 수 있습니다.

## ✓ AX310 자격증 과정

| 교육일정 | 교육내용 | 교육시간 |
|---|---|---|
| 2일차 | **MODULE 5 – 메모리 분석 ( RAM )**<br>– 메모리 분석 개요<br>– API 후크 ( API Hook )<br>– 파일 스캔 ( File Scan )<br>– 프로세스 리스트 ( pslist ) | 10:00 ~ 10:50 |
| | **MODULE 5 – 메모리 분석 ( RAM )**<br>– 숨김 프로세스 ( PSXVIEW )<br>– 네트워크 정보 분석 ( NETSCAN )<br>– 오픈핸들 ( HANDLE )<br>– 타임라인 분석 ( Timeline ) | 11:00 ~ 11:50 |
| | **MODULE 6 – 악성코드 정적 분석 ( Static Analysis )**<br>– Virtual Box 셋팅<br>– 가상머신 환경 설정 | 13:00 ~ 13:50 |
| | **MODULE 6 – 악성코드 정적 분석 ( Static Analysis )**<br>– 실행 파일 분석 (악성코드 Type 1 ) | 14:00 ~ 14:50 |
| | **MODULE 6 – 악성코드 정적 분석 ( Static Analysis )**<br>– 실행 파일 분석 (악성코드 Type 2 ) | 15:00 ~ 15:50 |
| | **MODULE 6 – 악성코드 정적 분석 ( Static Analysis )**<br>– 실행 파일 분석 (악성코드 Type 2 ) | 16:00 ~ 16:50 |
| | **질문 & Review** | 16:50 ~ 17:00 |
| | *** 교육 진행 시 사용 툴**<br>MAGNET AXIOM, Passware Kit Forensics, DB Browser for SQLite | |

* 교육시간 및 교육 내용은 강의 내용 / 설명 / 질문에 따라 조금씩 변경 될 수 있습니다.

## ✓ AX310 자격증 과정

| 교육일정 | 교육내용 | 교육시간 |
|---|---|---|
| 3일차 | MODULE 7 – 악성코드 동적 분석 ( Dynamic Analysis )<br>– 악성코드 동적 분석 개요<br>– 악성코드 감염 시나리오 시연 | 10:00 ~ 10:50 |
| | MODULE 7 – 악성코드 동적 분석 ( Dynamic Analysis )<br>– 동덕 분석 오픈소스 활용<br>– 프로세스 정보 수집 ( 모니터링 )<br>– 레지스트리 변조 여부 확인 ( 오픈소스 ) | 11:00 ~ 11:50 |
| | MODULE 7 – 악성코드 동적 분석 ( Dynamic Analysis )<br>– 네트워크 분리 ( 감염 시스템 수집 단계 )<br>– 방화벽 설정<br>– Burp suite을 이용한 프록시 설정 및 패킷 캡처 | 13:00 ~ 13:50 |
| | MODULE 7 – 악성코드 동적 분석 ( Dynamic Analysis )<br>– RAMMNUX 설정을 통한 학성코드 동적 분석 | 14:00 ~ 14:50 |
| | MODULE 7 – 악성코드 동적 분석 ( Dynamic Analysis )<br>– RAMMNUX 설정을 통한 학성코드 동적 분석 | 15:00 ~ 15:50 |
| | MODULE 7 – 악성코드 동적 분석 ( Dynamic Analysis )<br>– RAMMNUX 설정을 통한 학성코드 동적 분석 | 16:00 ~ 16:50 |
| | 질문 & Review | 16:50 ~ 17:00 |
| | * 교육 진행 시 사용 툴<br>MAGNET AXIOM, plist viewer, DB Browser for SQLite | |

* 교육시간 및 교육 내용은 강의 내용 / 설명 / 질문에 따라 조금씩 변경 될 수 있습니다.

## ✓ AX310 자격증 과정

| 교육일정 | 교육내용 | 교육시간 |
|---|---|---|
| 4일차 | **MODULE 8 – 조사 마무리 Artifacts 분석**<br>– 프리패치 분석 ( Prefetch )<br>– 유저 어시스트 분석 ( UserAssit )<br>– 레지스트리 탐색기를 통한 원본파일 확인 ( Rot13 Encording / Decording ) | 10:00 ~ 10:50 |
| | **MODULE 8 – 조사 마무리 Artifacts 분석**<br>– 캐시 기록 분석 ( shim, MUI, Amcache, BAM )<br>– 응용 프로그램 모니터링 ( Srum )<br>– 윈도우 타임라인 분석 ( Timeline )<br>– 윈도우 알림센터 분석 ( Notification Center ) | 11:00 ~ 11:50 |
| | **MODULE 9 – 시각화 분석을 이용한 증거 분석**<br>– 커넥션 빌드 개요 ( Connection Build )<br>– 커넥션 빌드를 이용한 소스 ( source ) 선정<br>– 데이터 시각화 해석<br>– 연관 분석 | 13:00 ~ 13:50 |
| | **MODULE 10 – 타임라인 ( Timeline ) 분석**<br>– 타임라인( Timeline ) 분석 개요<br>– 특정 이벤트 필터링 및 검색<br>– 악성코드 실행 흔적 조사 | 14:00 ~ 14:50 |
| | **MODULE 11 – 데이터 추출( Export )**<br>– 태그(TAG)를 홀용한 데이터 추출방안<br>– 증거테이블 ( Evidence Table ) 정보 내보내기<br>– 탐색기별 ( Explorer )별 데이터 내보내기<br>– 파일 타입별 ( Filetype ) 데이터 내보내기 | 15:00 ~ 15:50 |
| | **MODULE 12 – 리포트 ( Report ) 생성**<br>– 파일 타입별 리포트 생성<br>– 리포트 설정<br>– 리포트 템플릿 수정<br>– 리포트 확인 | 16:00 ~ 16:50 |
| | 질문 & Review | 16:50 ~ 17:00 |
| | *** 교육 진행 시 사용 툴**<br>MAGNET AXIOM, plist viewer, DB Browser for SQLite | |

* 교육시간 및 교육 내용은 강의 내용 / 설명 / 질문에 따라 조금씩 변경 될 수 있습니다.

# 감사합니다.


## INSEC Security

서울특별시 금천구 가산디지털 1로 19 대륭테크노타운 18차 4층

Email : insec@insec.co.kr  TEL : 02-851-5687  www.insec.co.kr