리버스 엔지니어링

악성코드 분석 실무 과정

5일 교육과정 커리큘럼

INSEC security

리버스 엔지니어링

악성코드 분석 실무 과정 (5일)

교육일정	교육내용	교육시간
1일차	**리버스 엔지니어링 개요** - 리버스 엔지니어링의 개요 및 도구 설명 - 올리디버거 메뉴 및 기능 설명	10:00 ~ 10:50
	시스템 구조 - 프로세스(Process) 개요 - 가상 메모리 동작 방식 이해 - 레지스터 개요 - 악성코드 분석에 필요한 어셈블리어 종류	11:00 ~ 11:50
	리버싱 분석 도구 사용 방법 - OllyDBG - IDA Pro - Ghidra	13:00 ~ 13:50
	CrackMe 1 실습 - 어셈블리어 실습 - 어셈블리어의 이해 - 리버싱 방법 실습	14:00 ~ 14:50
	CrackMe 2 실습 (1) - 윈도우 API의 이해 - 윈도우 API 분석 방법 - 코드 및 레지스터 패치 기법 설명	15:00 ~ 15:50
	메모리 패치 - 치트 엔진 사용 방법 - 치트 엔진을 통한 메모리 패치 실습	16:00 ~ 16:50
	지뢰 찾기 크래킹 - IDA Pro 활용 - IDA Pro를 통한 지뢰 찾기 크래킹	17:00 ~ 17:50
	질문 & Review	17:50 ~ 18:00
	* 교육 진행 시 사용 툴 OllyDBG, IDA Pro, CheatEngine	

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

상담문의 : 02-851-5687

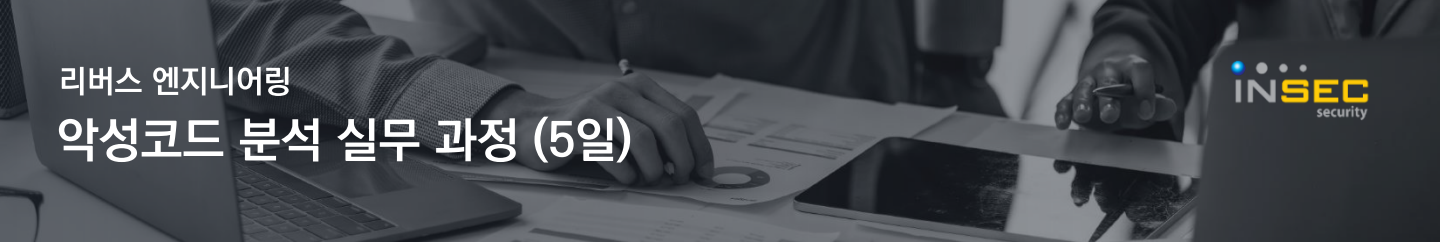
리버스 엔지니어링

악성코드 분석 실무 과정 (5일)

교육일정	교육내용	교육시간
2일차	**악성코드 분석 개요** - 악성코드 분석 절차	10:00 ~ 10:50
	기초분석 – 악성코드 패킹 유/무 확인 방법 - PEiD - Exeinfo - DiE	11:00 ~ 11:50
	기초분석 – 멀티 백신을 이용한 악성코드 판별 - Maestro CTIP를 활용한 악성코드 식별	13:00 ~ 13:50
	동적분석 – Process Monitor를 이용한 백도어 계열 악성코드 분석 실습 - Procmon 개요 - Procmon 사용 방법 - Procmon을 통한 백도어 계열 악성코드 동적 분석 실습	14:00 ~ 14:50
	동적분석 – 패킷 모니터링 도구를 이용한 네트워크 트래픽 분석 실습 - smsniff - Crowdinspect - Wireshark	15:00 ~ 15:50
	동적분석 – ProcDot을 이용한 그래프 도식화 실습 - ProcDot 이란? - Procmon 설정 및 데이터 추출 - ProcDot을 이용한 Procmon 데이터 그래프 도식화 실습	16:00 ~ 16:50
	동적 분석 – 스냅샷 분석 기법 및 샌드박스 - 스냅샷 분석을 통한 악성코드 감염 전/후 비교 - 조샌드박스를 통한 악성코드 자동화 분석 실습	17:00 ~ 17:50
	질문 & Review	17:50 ~ 18:00
	* 교육 진행 시 사용 툴 PEiD, Exeinfo, DiE Process Monitor, ProcDot, smsniff, CrowdInspect, Wireshark Process Explorer, Joe Sandbox, Metadefender	

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

상담문의 : 02-851-5687



리버스 엔지니어링

악성코드 분석 실무 과정 (5일)

교육일정	교육내용	교육시간
3일차	**디버거를 이용한 메인 함수 추적** - 메인 함수의 중요성 - StubCode - 메인 함수 추적 트릭 실습	10:00 ~ 10:50
	백도어 악성코드 분석 실습 – 파일 생성 및 서비스 생성 루틴 분석 실습 - 파일 생성 관련 Windows API 분석 - 파일 생성 API 기능 확인 - 서비스 생성 루틴 확인 - 서비스 생성 관련 Windows API 분석	11:00 ~ 11:50
	백도어 악성코드 분석 실습 – 서비스 분석 실습 - 서비스 프로세스 - 서비스 프로세스의 동작 루틴 - 서비스 프로세스 분석 방법론	13:00 ~ 13:50
	백도어 악성코드 분석 실습 – 네트워크 통신 루틴 분석 실습 - Windows 소켓 통신 - Windows 소켓 통신 관련 API 분석 - Windows 소켓 통신 루틴	14:00 ~ 14:50
	백도어 악성코드 분석 실습 – API 분석 실습 - 다양한 Windows API 분석 방법론 - 다양한 Windows API 분석 실습	15:00 ~ 15:50
	PE 구조 (1) - PE 개요 - PE 구조 - PE 헤더	16:00 ~ 16:50
	PE 구조 (2) - IAT & IDT 재구성의 이해 - .section 영역 분석 방법론	17:00 ~ 17:50
	질문 & Review	17:50 ~ 18:00
	*** 교육 진행 시 사용 툴** OllyDBG, IDA Pro, PEiD, Process Monitor, ProcDot, Hex Decompiler Joe Sandbox, Metadefender, Malzilla, SSView, Volatility, Response Pro	

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

상담문의 : 02-851-5687

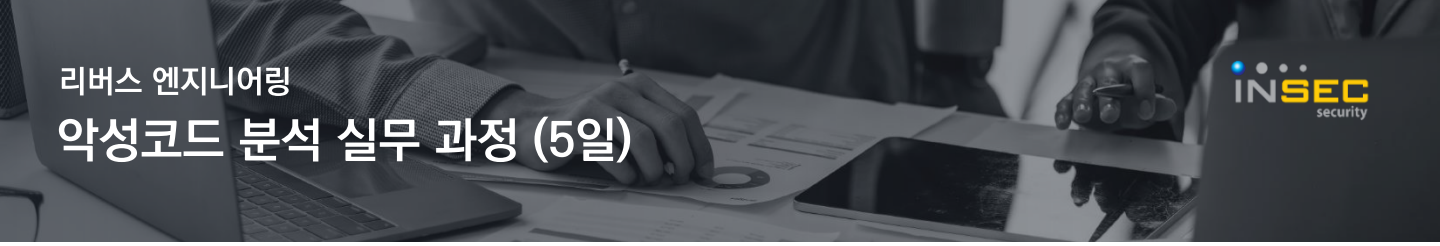
리버스 엔지니어링

악성코드 분석 실무 과정 (5일)

교육일정	교육내용	교육시간
4일차	**패킹 이란?** - 패킹 개요 - 패킹의 원리 - 패킹 전/후 비교	10:00 ~ 10:50
	패킹 실습 - UPX / ASPack / UPack 패킹 실습 - 각 패킹의 특징	11:00 ~ 11:50
	언패킹 - 언패킹 설명 - 언패킹 방법론 - 언패킹 실습	13:00 ~ 13:50
	링크 라이브러리 - 링크 라이브러리 - 명시적/묵시적 링크 라이브러리 - DLL 개요	14:00 ~ 14:50
	인젝션 - 인젝션 이란? - 다양한 인젝션 방법 - 인젝션 악성코드 - DLL 인젝션?	15:00 ~ 15:50
	인젝션 실습 - Windows OS별 레지스트리 인젝션 실습 - DLL 인젝션 실습 - CreateRemoteThread	16:00 ~ 16:50
	인젝션 악성코드 분석 실습 - PE 구조 리소스 영역 분석 - 권한 상승 코드 분석 - 인젝션 대상 프로세스 식별 코드 분석 - DLL Injection 루틴 분석 - DLL 파일 분석 방법론	17:00 ~ 17:50
	질문 & Review	17:50 ~ 18:00
	*** 교육 진행 시 사용 툴** Dex2jar, jd-gui, Metadefender, Maestro Android Analyzer, APKtool, ADB	

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

상담문의 : 02-851-5687



리버스 엔지니어링

악성코드 분석 실무 과정 (5일)

교육일정	교육내용	교육시간
5일차	**안드로이드 개요** – 안드로이드란 – 안드로이드 릴리즈 노트 – 안드로이드 아키텍처	10:00 ~ 10:50
	안드로이드 기본 개념 – 안드로이드 보안 기능 – 안드로이드 4대 컴포넌트 – 안드로이드 컴포넌트 라이프 사이클	11:00 ~ 11:50
	안드로이드 APK – 안드로이드 APK 개요 – 안드로이드 APK 생성 과정 – 안드로이드 APK 컴파일 방법 – 안드로이드 APK 구조	13:00 ~ 13:50
	안드로이드 악성코드 – 안드로이드 악성코드 개요 – 안드로이드 악성코드 종류 – 안드로이드 악성코드 트렌드	14:00 ~ 14:50
	안드로이드 악성코드 분석 방법론 – 정적 분석 vs 동적 분석 – Androidmanifest.xml 분석 – Android 디컴파일 방법	15:00 ~ 15:50
	실전 악성코드 분석 – 모바일 RAT 악성코드 – Androidmanifest.xml 분석 – 위험 권한 분석 – 컴포넌트 분석 – 디컴파일을 통한 코드 분석	16:00 ~ 16:50
	실전 악성코드 분석 – 모바일 Stalker / Ransomware 분석 – Stalker 악성코드 분석 – 랜섬웨어 악성코드 분석	17:00 ~ 17:50
	질문 & Review	17:50 ~ 18:00
	* 교육 진행 시 사용 툴 Maestro Android Analyzer, APKtool, ADB, Dex2jar, jd-gui, Metadefender 등	

* 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