안드로이드 / iOS 모바일 악성코드

모바일 악성코드 분석 실무 과정

2일 교육과정 커리큘럼

INSEC security

안드로이드 / iOS 모바일 악성코드

모바일 악성코드 분석 실무 과정 (2일)

교육일정	교육내용	교육시간
1일차	**모바일 악성코드 개요** – 모바일 악성코드 개요 – 모바일 악성코드 종류 및 유형 별 특징 – 모바일 악성코드 분석 절차 – 분석 단계 별 활용 도구	10:00 ~ 10:50
	안드로이드 기본 개념 – 안드로이드 운영체제 구성 요소 이해 – 안드로이드 커널 구조 – 안드로이드 버전 별 특징 이해 – 달빅(Dalvik) 가상 머신의 이해 [DVM]	11:00 ~ 11:50
	분석 환경 구축 – 안드로이드 SDK 설치 – 안드로이드 에뮬레이터 구축 – 네트워크 패킷 분석 도구 설치 및 ADB 환경 설정	13:00 ~ 13:50
	실제 모바일 악성코드 샘플 분석 – 정보 유출(Smishing) 계열 – 디컴파일(Decompile) 분석 방법 – 퍼미션(Permission) 데이터 분석 – /data/data 디렉토리 데이터 분석 – 오픈 소스 도구를 활용한 바이너리 XML 분석	14:00 ~ 14:50
	실제 모바일 악성코드 샘플 분석 – 랜섬웨어(Ransomware) 계열 – 모바일 랜섬웨어 주요 특징 및 파일 암호화 코드 루틴 분석 – 디컴파일을 통한 안드로이드 내부 코드 정적 분석 실습 – 전문 상세 분석 도구를 활용한 랜섬웨어 샘플 분석 실습	15:00 ~ 15:50
	실제 모바일 악성코드 샘플 분석 – 스파이웨어(Spyware) 계열 – 문자 메시지, 통화 기록, 녹음 파일, GPS 정보, 주소록 정보 탈취 특징 이해 – 정보 유출 유형 코드 루틴 분석 – 정보 유출 유형 퍼미션 특징 이해 – 전문 상세 분석 도구를 활용한 스파이웨어 샘플 분석 실습	16:00 ~ 16:50
	실제 모바일 악성코드 샘플 분석 – 난독화 악성코드 계열 – 프로가드(Proguard)로 난독화 된 악성코드 유형 분석 – APKProtect로 난독화 된 악성코드 유형 분석 – 전문 상세 분석 도구를 활용한 난독화 악성코드 분석 실습	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

안드로이드 / iOS 모바일 악성코드

모바일 악성코드 분석 실무 과정 (2일)

교육일정	교육내용	교육시간
2일차	**실제 모바일 악성코드 샘플 분석 – 국내 마켓 앱 위장 악성코드(FakeApp)** – 리소스(src) 영역 분석을 통한 위장 앱 판별 방법 – 코드 분석을 통한 정보 유출 로직 상세 분석 – 전문 상세 분석 도구를 활용한 위장 앱 악성코드 분석 실습	10:00 ~ 10:50
	프리다(Frida) 활용 – 안드로이드 전문 분석 도구 프리다(Frida) 사용 방법 – 멀티 플랫폼 후킹 기술 이해 – 후킹 명령어 사용 방법 – 악성코드 분석에 활용 가능한 프리다 라이브러리 소개	11:00 ~ 11:50
	실제 모바일 악성코드 샘플 분석 – 백도어 계열 앱 계열 악성코드 – 프리다(Frida)를 활용한 백도어 앱 악성코드 분석 실습 – 악성코드 주요 핵심 기능 분석 – 메모리 내 dex 파일 추출을 통한 난독화 앱 분석 방법 – Dexdump 계열 라이브러리 활용 실습	13:00 ~ 13:50
	iOS 악성코드 분석 개요 – iOS 악성코드 특징 및 한계점 이해 – iOS 버전 별 특징 및 내부 적용 보안 기술 설명 – 전 세계 유명 iOS 악성코드 종류 파악 – 악성코드 감염 유입 경로 파악	13:00 ~ 13:50
	iOS 악성코드 분석 실습 – 정보 유출 계열 악성코드 – ipa 파일 구조 이해 – Ipa 상세 분석 방안 – 샌드박스 분석 도구를 활용한 iOS 악성코드 분석 실습	14:00 ~ 14:50
	Maestro CTIP(Cyber Threat Intellignece Platform) / Maestro iNSIGHT – Android Analyzer – 안드로이드 어플리케이션 자동화 분석 앱(Android Analyzer 소개) – Android Analyzer를 통한 앱 분석, 악성 앱 탐지, 자동화 분석 및 취약점 진단 실습 – Maestro CTIP 소개 – Maestro CTIP를 통한 통합 분석 체계 시연 – CTIP를 통한 통합 분석 실습 진행	16:00 ~ 16:50
	질문 & Review	17:50 ~ 18:00
	*** 교육 진행 시 사용 툴** Maestro Android Analyzer, APKtool, ADB, Dex2jar, jd-gui, Frida, Joe Sandbox 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