실전형 사이버훈련장 대학생 특별과정 운영계획(안)

□ 개요

○ **(추진배경)** 비수도권 정보보호학과 대상(약 150명) 실전형 사이버훈련장 훈련 제공을 통한 보안지식 및 역량 강화로 지역 사이버보안 인재 양성

○ **(추진일정)** '23년 7월 31일 ~ 8월 21일(온라인 3주), 8월 31일(오프라인 1일)

○ **(훈련과정)** 스피어피싱 대응 훈련(기본, 심화1(HWP), 심화2(MS Office))

○ **(협력방안)** 지역센터와 협력하여 비수도권 대학생 홍보 및 모집 추진

※ (6.21일 기준) 호원대, 우석대, 원광대, 전주대 4개학교 55명 섭외 완료

□ 주요내용

○ 대학생 특별과정 훈련 프로그램(안)

온라인 자율수강(7.31 ~ 8.21, 3주간)				오프라인 챌린지(8.31)
스피어피싱 기본 온라인 자율 수강	➡	스피어피싱 심화1 온라인 자율 수강	➡ 스피어피싱 심화2 온라인 자율 수강 ➡	판교 훈련장 미니챌린지 개최 * 우수 훈련생 30명 선발/참여

○ 대학생 특별과정 오프라인 미니챌린지(안)

구분	계(팀)	상금	평가방식
대상	1	50만원	CTF 기반 악성 문서 식별 및 분석 ※ 우수 훈련생 대상 6팀 구성
금상	1	40만원	
은상	1	30만원	
동상	3	각 20만원	
계	**6**	**180만원**	

□ 향후계획

○ 각 지역정보보호센터별 지역 대학생(15~20명) 모집(~07.14일)

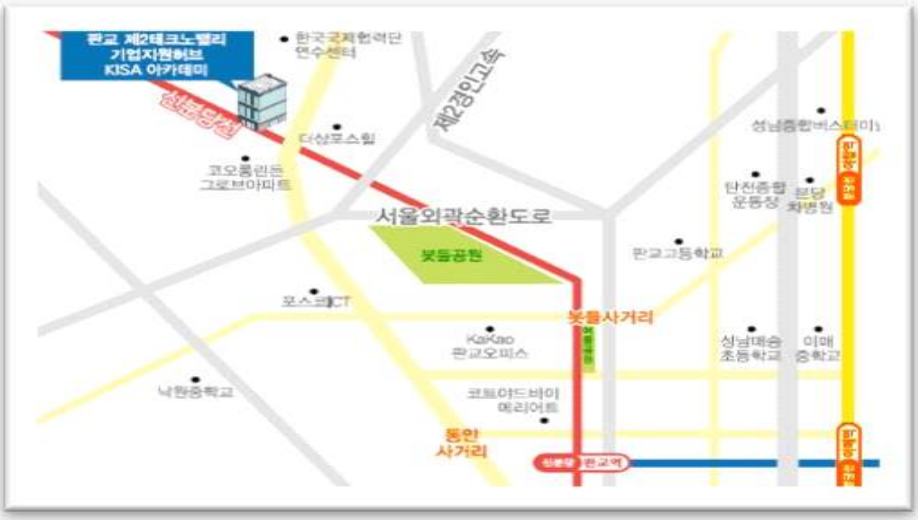
○ 실전형 사이버훈련장 대학생 특별과정 입과 안내(~07.26일)

참고1 실전형 사이버훈련장 대학생 특별과정 세부 운영 방안

□ 스피어피싱 온라인 과정 운영 방안

주제	세부내용	
수강 기간	- 총 21일(3주)간 3개 과정(기본, 심화1-HWP, 심화2-MS Office) 온라인 자율 수강	
수료 조건 (과정별 수료증 발급)	수강률	- 과정별 80% 이상 수강
	사후평가	- 사후평가 필수 참여
	사전/사후 설문	- 사전설문, 사후설문 필수 응답
오프라인 과정 선발 기준	- 3과목 모두 수료인원 기준 상위 30명 선발	

□ 오프라인 미니 챌린지 과정 운영 방안

주제	세부내용
일시 및 장소	- 8.31일(목) 13:00~17:00, KISA 판교 실전형 사이버훈련장 * 경기도 성남시 수정구 대왕판교로 815 기업지원허브 5층
 판교제2테크노밸리 정류장(구 한국도로공사) 하차 후 도보 약 5분 • 수서역 6번 출구 정류장 일반 101 광역 1007, 1007-1, 1009, 5600, 5700, 6900 • 잠실광역환승센터 일반 101 광역 1007, 1009 • 잠실역 4번 출구 정류장 광역 1007-1, 6900 • 잠실역 6, 7번 출구 중앙버스 정류장 광역 5600, 5700 • 판교역 동편 정류장 일반 101, 370, 55(기업지원허브 하차), 누리2(기업지원허브 하차 • 분당내곡간 고속화도로 이용시 내곡터널 통과 후 3차선 진입 → 판교방향 진입(시흥사거리에서 우회전) • 경부고속도로 이용시 판교IC → 세종연구소 방향(세곡동 방향) 진입 • 대왕판교로(23번 국도) 이용시 수서역사거리 → 세곡동사거리 → 서울공항 → 시흥사거리 직진	
운영 방식	- 팀 간 CTF 기반 악성 문서 식별 및 분석	
교통비	- 전원 지원(참석자에게 선불카드 제공 예정, 별도안내)	
식사	- 전원 중식 제공	

참고2 스피어피싱 대응 과정별 세부 훈련내용

□ 스피어피싱 대응 기본과정

연번	제목	훈련내용
1	**MITRE ATT&CK 프레임워크와 위협 탐지**	- MITRE ATT&CK 프레임워크 개요 - MITRE ATT&CK 지식 기반의 구성요소 - 위협에 대한 탐지, 차단, 대응 기술과 전략의 발전 방향
2	**파일리스(Fileless) 공격**	- 파일리스 공격의 개념 - LoL(Livin Off the land), LoL Binaries - 프로세스 인젝션
3	**스피어 피싱 이메일 분석**	- 이메일 기반 공격 기법과 유형 - 이메일 전송 과정과 헤더 구조 - 이메일 헤더 분석을 통한 이상징후 식별 방법
4	**악성 문서파일 분석을 위해 알아야할 필수 지식**	- PE-COFF 파일의 구본 구조 - 프로세스의 가상 주소 공간 - 악성 첨부파일 유형과 구성요소 - 악성 문서파일의 분석 절차
5	**쉘코드 분석**	- 쉘코드 개요와 분석 목표 - 쉘코드가 사용하는 주요 API - 쉘코드의 바인딩(Binding) API 해시 - 쉘코드에서 임포트하는 API 확인 방법 - 쉘 코드 분석 절차와 디버깅 방법
6	**악성 HWP 문서 분석**	- HWP 문서 개요와 기본 구조 - HWP 문서 파일 트리아지 (이상징후 식별) - HWP 문서 파일 분석 절차 - 포스트 스크립트 개요
7	**악성 MS 오피스 문서 분석**	- MS 오피스 문서파일 트리아지 (이상징후 식별) - VBA 매크로 개요와 특징 - DDE/DDEAUTO 개요와 특징

□ 스피어피싱 대응 심화1(HWP) 과정

연번	제목	훈련내용
1	악성 HWP 문서의 유형별 분석 전략	- 악성 HWP 문서의 공격 방식에 따른 유형 분류와 시나리오 - 악성 HWP 문서의 유형별 식별 방법
2	포스트스크립트 유형 악성 HWP 문서 파일 분석	- BAT 파일을 이용한 파워쉘 스크립트 실행 코드 패턴
3	익스플로잇 유형 악성 HWP 문서 파일 분석	- 한컴 오피스의 그라데이션 오버플로우 취약점 - 포스트 스크립트의 프로세스 인젝션 루틴 패턴
4	오브젝트 유형 악성 HWP 문서 파일 분석	- OLE 객체로 임베드된 오브젝트의 특징과 분석 방법
5	매크로 유형 악성 HWP 문서 파일 분석 #1	- 매크로 유형 HWP 파일의 특징과 분석 방법

□ 스피어피싱 대응 심화2(MS Office) 과정

연번	제목	훈련내용
1	악성 MS 오피스 문서의 유형별 분석 전략	- 악성 MS 오피스 문서의 공격 방식에 따른 유형 분류와 시나리오 - 악성 MS 오피스 문서의 유형별 식별 방법
2	VBA 스크립트 유형 악성 MS 오피스 문서 파일 분석	- 엑셀의 VHS(Very Hidden Sheet) 기능을 이용한 스크립트 은닉 - MSHTA와 자바스크립트를 이용한 공격 루틴 - 파워쉘을 이용한 쉘코드 로딩 루틴
3	DDE 유형 악성 MS 오피스 문서 파일 분석	- 파워쉘 스크립트 실행 루틴 - REGSVR32 및 VBA 스크립트를 이용한 프로세스 인젝션 루틴
4	OLE 오브젝트 유형 악성 MS 오피스 문서 파일 분석	- VBA 기반의 파워쉘 스크립트를 이용한 쉘코드 실행 루틴 - 윈도우 Startup Folder 대상 자바스크립트 모듈 생성 루틴
5	익스플로잇 유형 악성 MS 오피스 문서 파일 분석	- CVE-2017-11882 취약점을 이용한 원격코드 실행 - CVE-2021-40444 취약점을 이용한 자바스크립트 코드 실행