국가인적자원개발컨소시엄
CHAMP Consortium for HRD Ability Magnified Program

2019

최정예 사이버보안 및 산업보안 전문인력 양성

교육과정 안내

고용노동부
한국산업인력공단 HUMAN RESOURCES DEVELOPMENT SERVICE OF KOREA
한국인터넷진흥원

CONTENTS

한국인터넷진흥원 사이버보안인재센터는?

사이버보안인재센터는 일반인의 정보보호 인식 제고 및 지식정보보안 분야 산업체의 전문인력 양성을 위하여 다양한 교육 프로그램을 운영하고 있는 전문교육기관입니다. 사이버보안인재센터는 세계적인 정보보호 전문인력 양성 기관을 목표로 최정예 사이버보안 전문가(K-Shield) 양성 과정을 통해 우수보안인력을 양성하고 있으며, 정보보호 재직자 역량 강화를 위한 산업보안 전문인력 양성 교육을 제공하고 있습니다. 이외에도 정보보호에 관심 있는 학생, 일반인을 대상으로 미래 정보보호 인력을 육성하고, 재직근로자 등 산업계 수요맞춤형 교육과정을 운영하는 등 분야별 정보보호 인력의 수급차 해소에 기여하고 있습니다.

정보보호 인력 양성으로 국가의 안전한 정보보호 기반 확립에 기여

세계적인 정보보호 전문인력 양성 기관

1 정보보호 인력정책 수립 및 활성화 지원

2 미래 정보보호 인력 육성 및 수급 해소 지원

- 차세대 보안리더 양성(BOB) 프로그램 지원
- 대학정보보호동아리(KUCIS) 지원

3 산업계 수요에 대응한 정보보호 우수 인력 육성

- 정보보호 특성화 대학 지원
- 지역전략산업 융합보안 핵심인재 양성
- 정보보안 (산업)기사 국가기술자격 운영
- NCS 기반 실무형 정보보호 기술인력 양성(K-Shield Jr.)

4 정보보호 재직자 역량강화 지원

- 최정예 사이버보안 인력(K-Shield) 양성 교육
- 산업보안 전문인력 양성 교육

5 지능정보사회 도래에 따른 선제적 인력 육성 지원

- 공격/방어 콘텐츠 기반 양방향 실전형 사이버훈련장(Security Gym) 운영
- 융합보안 인력 양성 교육

[CHAMP : Consortium for HRD Ability Magnified Program]

국가인적자원개발컨소시엄 전략분야 인력양성사업이란?

국가인적자원개발컨소시엄 사업은 고용보험법 시행령 제52조 제1항6호, 제2항 및 제3항에 따라 공동훈련센터가 협약기업 사업주와 협약을 체결하고 근로자의 니즈를 파악하여 수요자 중심의 맞춤형 교육 프로그램을 제공하는 인력양성 사업입니다. 특히 전략분야는 특정 산업이나 직종에 대한 체계적인 인력양성 및 근로자 직업능력개발을 목적으로 하며, 한국인터넷진흥원은 국내 기업의 정보보호 분야에 특화된 전문교육을 제공합니다. 현재 국내 80여개 기업·기관 및 단체가 컨소시엄 전략분야 인력양성훈련기관으로 지정되어 있습니다.

사업운영체계

고용노동부
컨소시엄 제도 및 정책 마련, 사업 관리

한국산업인력공단
컨소시엄 공동훈련센터 지원 및 평가

한국인터넷진흥원
정보보호 직종 교육훈련을 제공하는 공동훈련센터

협약기업
협약체결을 통한 공동훈련센터 교육훈련참여

협약기업 지원

⊘ 수요자 중심의 맞춤형 교육훈련 제공
- 수요조사를 통하여 협약기업이 원하는 맞춤형 교육훈련 제공

⊘ 우수한 공동교육훈련환경 제공
- 고용노동부의 지원으로 실습교육시설과 양질의 훈련과정 등 우수한 교육환경 제공

⊘ 비용 부담 없는 교육 훈련시스템 제공
- 협약기업이 운영기관 교육훈련에 참여할 경우 정부에서 지원하여 기업의 인력양성 부담을 최소화
- 고용보험기금을 활용한 무료교육 진행

⊘ 간편한 교육훈련 참여 등 편리한 행정서비스 제공
- 운영기관과의 협약체결만으로 원하는 교육훈련과정에 참여할 수 있는 간편한 절차 제공
- 협약기업별 참여인원 제한 없음

훈련참여자 지원

⊘ 재직근로자 맞춤형 교육훈련 제공
- 중소기업 근로자들을 위하여 운영기관에서 지속적으로 협약기업 근로자의 교육체계 관리서비스를 제공하고 수요조사를 통하여 협약기업 근로자가 원하는 맞춤형 교육훈련 및 핵심 훈련을 제공

교육비

⊘ 무료(협약 관련 가입비·교육비 및 환급절차 없음)
- 기업이 직업능력개발 및 고용안정을 위하여 조성한 고용보험기금을 통해 조달

최정예 사이버보안 및 산업보안 전문인력 양성 교육 참여방법

교육대상

- 한국인터넷진흥원과 전략분야 인력양성사업 협약이 체결된 기업에 재직중이며, 고용보험을 납부하고 있는 재직자
  ※ 공무원, 학생, 기업대표 등은 본 교육 대상에서 제외됩니다.
- 정보보호 업무 담당자 및 관리자 대상으로, **우선지원기업만(대규모 기업 제외) 협약 체결 및 교육 수강이 가능**합니다.
  ※ 소속 기업의 기업 규모를 모르실 경우, 근로복지공단(☎1588-0075) 또는 고용노동부 상담센터(☎1350)를 통해 확인 바랍니다.

협약절차

협약서 다운로드 → 양식 작성 → 우편 제출 → 협약 체결

✓ 제출서류

- 전략분야 인력양성사업 협약서 원본 2부 및 참여기업 일반현황 1부를 작성하여 원본을 우편으로 제출
  [사이버보안인재센터 홈페이지(http://academy.kisa.or.kr/) 에서 협약서 다운로드]

✓ 제출처

- 경기도 성남시 수정구 대왕판교로 815 판교제2테크노밸리 기업지원허브 4층 493호 KISA 사이버보안인재센터 컨소시엄 협약담당자 앞
  ※ 협약 시점은 사이버보안인재센터 협약담당자 협약서 수령일로 간주하며, 사이버보안인재센터 홈페이지(http://academy.kisa.or.kr/) 좌측 하단 "협약체결안내"에서 기업명 검색을 통해 협약 체결 여부를 확인하실 수 있습니다.
  ※ 협약 완료 여부는 별도로 유선통보하지 않으며, 협약이 완결된 후 협약서 1부를 기업으로 발송 해 드립니다.
  ※ 국가인적자원개발컨소시엄 전략분야는 타 컨소시엄 운영기관과 중복협약이 가능합니다.

교육수강절차

홈페이지 회원가입 → 협약 체결 여부 확인 → 교육 수강 신청 → 교육 입과 안내 (수강자격 확인 후 교육 시작 7일 전) → 교육 수강 → 수료증 발급 (출석 80% 이상)

✓ 모든 교육은 사이버보안인재센터 홈페이지(http://academy.kisa.or.kr/)를 통해서만 신청할 수 있습니다.

- 교육생 출결관리, 수료증 발급 등을 위하여 개별 회원가입 후 교육신청 가능(단체수강 불가)
- 수료증 발급은 교육 종료 3일 후, 사이버보안인재센터 홈페이지 퀵메뉴에서 출력

✓ 교육 시작일 약 1개월 전부터 수강신청을 시작하며, 업무일 기준 교육시작 7일전 모집 마감됩니다.

- 선착순 모집으로 사전 마감 될 수 있음
  ※ 단, K-Shield 정규과정(K-Shield 1차, 2차 교육훈련)은 교육 신청 후 별도의 선발 평가 있음.
- 신청 마감 후 교육 취소자로 인한 여석 발생 시 추가 모집 실시할 수 있음
- 사이버보안인재센터 홈페이지 공지사항의 '연간교육일정' 참고

✓ 협약기업별 교육 참여횟수는 제한이 없습니다.

연간일정

구 분	과 정 명	교육시간	정원	교육 시작일	교육 종료일
K-Shield 단기과정	K-Shield 인젝션 공격대응 실습훈련	21(3일)	20	05-07(화)	05-09(목)
				07-09(화)	07-11(목)
				11-05(화)	11-07(목)
	K-Shield 악성코드를 이용한 공격대응 실습훈련	28(4일)	20	03-26(화)	03-29(금)
				06-25(화)	06-28(금)
				09-24(화)	09-27(금)
	K-Shield 산업제어 시스템 공격대응 실습훈련	28(4일)	20	11-11(월)	11-14(목)
	K-Shield 모의해킹 정문 실습훈련	28(4일)	20	09-17(화)	09-20(금)
				11-26(화)	11-29(금)
	K-Shield 보안제품군 활용 실습훈련	21(3일)	20	07-30(화)	08-01(목)
				11-19(화)	11-21(목)
	K-Shield IoT 보안 실습	32(5일)	20	04-15(월)	04-19(금)
				07-01(월)	07-05(금)
	K-Shield 소프트웨어 개발보안 실습[설계]	32(5일)	20	05-27(월)	05-31(금)
				10-14(월)	10-18(금)
	K-Shield 소프트웨어 개발보안 실습[테스트]	32(5일)	20	06-10(월)	06-14(금)
				10-28(월)	11-01(금)
	K-Shield 운영보안 실습	32(5일)	20	05-20(월)	05-24(금)
				09-02(월)	09-06(금)
K-Shield 정규과정 [장기교육] * 2차 교육은 1차 교육 이수자 대상 진행	K-Shield 1차 교육훈련 (주1회 교육)	105 (15일)	30	04-15(월)	07-29(월)
				04-16(화)	07-30(화)
				04-17(수)	07-31(수)
				04-18(목)	08-01(목)
				04-19(금)	08-02(금)
	K-Shield 1차 교육훈련 (주중 연속교육)	105 (15일)	30	05-13(월)	05-17(금)
				06-17(월)	06-21(금)
				07-15(월)	07-19(금)
	K-Shield 2차 교육훈련(디지털 포렌식)	70(10일)	30	09-16(월)	11-25(월)
	K-Shield 2차 교육훈련(악성코드 분석)	70(10일)	30	09-17(화)	11-26(화)
	K-Shield 2차 교육훈련(침해대응)	70(10일)	30	09-18(수)	11-27(수)
	K-Shield 2차 교육훈련(모의해킹)	70(10일)	30	09-19(목)	11-28(목)
	K-Shield 2차 교육훈련(보안컨설팅)	70(10일)	30	09-20(금)	11-29(금)

※ K-Shield 2차 교육훈련의 경우 1차 교육훈련 수료생 중 평가 통과자 대상
※ 모든 교육은 주간과정으로 운영됩니다.
※ 상기 교육일정 등은 변경될 수 있으며, 변경 시 홈페이지 공지사항을 통하여 안내 예정

연간일정

과 정 명	교육시간	정원	교육 시작일	교육 종료일
침해사고 분석대응 전문가	28(4일)	30	04-15(월)	04-18(목)
			05-21(화)	05-24(금)
			08-20(화)	08-23(금)
			11-26(화)	11-29(금)
해킹 방어를 위한 시큐어코딩	21(3일)	40	03-27(수)	03-29(금)
			04-22(월)	04-24(수)
			06-26(수)	06-28(금)
			07-17(수)	07-19(금)
			09-25(수)	09-27(금)
			11-20(수)	11-22(금)
기반시설 네트워크 보안	28(4일)	30	05-13(월)	05-16(목)
			06-10(월)	06-13(목)
			07-29(월)	08-01(목)
			10-14(월)	10-17(목)
			11-04(월)	11-07(목)
디지털 포렌식 실습	28(4일)	30	04-16(화)	04-19(금)
			05-21(화)	05-24(금)
			08-27(화)	08-30(금)
암호 및 인증의 이해와 실무 응용	28(4일)	30	06-25(화)	06-28(금)
			09-03(화)	09-06(금)
			11-18(월)	11-21(목)
웹 공격 및 대응 기법	21(3일)	25	03-25(월)	03-27(수)
			07-01(월)	07-03(수)
			10-28(월)	10-30(수)
정보통신 기반시설 정보보호 업무실무	28(4일)	30	06-10(월)	06-13(목)
			07-01(월)	07-04(목)
			09-23(월)	09-26(목)
			11-25(월)	11-28(목)
보안컨설팅 이론과 실제	21(3일)	30	07-10(수)	07-12(금)
			09-04(수)	09-06(금)
			11-20(수)	11-22(금)

※ 모든 교육은 주간과정으로 운영됩니다.
※ 상기 교육일정은 변경될 수 있으며, 변경 시 홈페이지 공지사항을 통하여 안내 예정

교육 과정 안내

01 K-Shield 인젝션 공격대응 실습훈련

인젝션 공격으로 인한 기밀정보 유출 피해발생, 시스템 탈취 사고발생 등을
방지하기 위한 인젝션 공격대응 전문역량 제고

훈련 시간
연 3회 3일(21시간) 과정
09:30~17:30

훈련 방법
집체 훈련

정원
20명

활용 교재
자체개발교재

훈련 내용

교과목	교육내용	
인젝션 취약성의 이해	• HTTP 프로토콜의 이해	• JavaScript 이해
인젝션 취약성 보안위협	• 인젝션 공격의 이해	• PHP 시큐어코딩
인젝션 취약점 대응방안	• 웹방화벽 운영	• MASS SQL 인젝션 이해
인젝션 공격대응 실습훈련	• 인젝션 공격 및 대응 실습	• K-Shield 실습훈련 콘텐츠

02 K-Shield 악성코드 공격대응 실습훈련

악성코드 분석 이론 및 실습 교육을 통해
악성코드 탐지, 분석, 공격 대응을 위한 전문역량 제고

훈련 시간
연 3회 4일(28시간) 과정
09:30~17:30

훈련 방법
집체 훈련

정원
20명

활용 교재
자체개발교재

훈련 내용

교과목	교육내용	
악성코드 개요 및 행위분석	• 악성코드의 특징	• 악성코드 행위분석
침해사고 대응 절차	• 주요 프로세스 분석 • 연관파일 및 유입경로 분석	• 주요 레지스트리 및 네트워크 분석 • 메모리 파일시스템 분석
시나리오 기반 탐지&분석	• 악성코드 탐지&분석	
악성코드를 이용한 공격대응 실습훈련	• K-Shield 실습훈련 콘텐츠	

03 K-Shield 산업제어시스템 공격대응 실습훈련

산업제어시스템 인프라에 대한 실무지식 및 사고분석 대응력 강화

훈련 내용

교과목	교육내용
산업제어시스템 인프라 및 Modbus	• SCADA 시스템 개요 • Modbus 프로토콜 이해
산업제어시스템 구성요소	• 주통신기술 기반의 산업제어시스템 • 제어콘트롤러 기반의 산업제어시스템
산업제어시스템 사고분석 기본	• 악성코드 흔적 분석 • 각종 아티팩트 수집 및 분석
산업제어시스템 사고분석 및 대응	• 악성코드 흔적 및 로그분석 • 문서기반 악성코드 분석 • Supply Chain Attack 이해
내부 업무망 사고분석 및 대응	• 디스크 볼륨 분석 및 복구 기법 • 난독화 코드 및 웹 로그 분석

훈련 시간
연 1회 4일(28시간) 과정
09:30~17:30

훈련 방법
집체 훈련

정원
20명

활용 교재
자체개발교재

04 K-Shield 모의해킹 전문 실습훈련

정보자산에 대한 점검 및 취약점 분석평가가 가능한 모의해킹 기술인력 양성

훈련 내용

교과목	교육내용
웹해킹 개요	• WEB / HTTP 프로토콜 이해 • 지원 언어에 대한 이해 • 인코딩에 대한 이해
웹해킹 실습 기초준비	• 웹해킹시 사용되는 도구 • 실습환경 구성 연습 • 웹해킹 공격항목에 대한 기본 이해
취약점 및 대응방안	• Cross Site Scripting • SQL Injection • FileUpload, Download • FileInclusion, Command Injection • 쿠키접속, URL 강제접속 등

훈련 시간
연 2회 4일(28시간) 과정
09:30~17:30

훈련 방법
집체 훈련

정원
20명

활용 교재
자체개발교재

05 K-Shield 보안제품군 활용 실습훈련

보안 제품군별 운용을 위한 실무 지식 및 사이버 공격 탐지/조치방법 습득

훈련 시간
연 2회 3일(21시간) 과정
09:30~17:30

훈련 방법
집체 훈련

정원
20명

활용 교재
자체개발교재

훈련 내용

교과목	교육내용
보안산업 및 제품 동향	• 정보보호 사고 사례 등 동향 • 정보보호 제품 트랜드
보안제품군 소개	• 정보보호 제품군 소개 - Firewall, IDS, IPS, WAF, UTM, NGFW, ESM, DLP, APT
방화벽	• DoS, DDoS, Flooding 공격 실습 • 방화벽을 이용한 공격 탐지 및 대응
정규표현식	• 정규표현식의 이해 • 정규표현식을 활용한 패턴 매칭 실습
웹 방화벽	• 웹 공격의 이해 • 웹 방화벽을 이용한 공격 탐지 및 차단 실습
침입 탐지/차단 시스템	• APT 공격 이해 • 침입탐지시스템을 이용한 공격 탐지 실습

06 K-Shield 1차 교육훈련

네트워크, 웹, 시스템 분야별 사이버공격 기법 분석을 통한
공격대응력 향상 및 악성코드 분석력 강화

훈련 시간
연 6회 15일(105시간) 과정
09:30~17:30

훈련 방법
집체 훈련

정원
30명

활용 교재
자체개발교재

훈련 내용

교과목	교육내용
보안 트랜드 및 이슈대응	• 주요 보안사고 사례 • 사이버보안 동향 및 이슈별 대응
표적공격(APT)	• 표적공격의 일반적인 절차 • 표적공격에 사용되는 기술 활용 기법
네트워크 패킷 및 트래픽 분석	• 네트워크 공격 탐지 • 취약점 공격 예방

교과목	교육내용	
웹 취약점 탐지 및 공격	• 웹 해킹 공격항목	• 주요 취약점별 대응방안
침해사고 대응 기법	• 리눅스 윈도우 현장 대응 및 데이터 분석 • 리눅스 Syslog 분석	• 윈도우 이벤트 로그 분석
악성코드 헌팅	• 물리메모리 분석	• 레지스트리 및 파일시스템 분석
악성코드 동적 분석	• 다양한 포맷의 악성코드 분석	
모바일 애플리케이션 취약점 분석	• 모바일 취약점 진단 • 앱 무결성 검증 진단	• 코드(모듈) 보호 진단
오픈소스 보안 솔루션 운용	• ModSecurity WAF, Snort IDS/IPS • 공격패턴 분석을 통한 룰셋 제작기법	
정보보호 컴플라이언스	• 정보보호 법률	• 국내외 정보보호 컴플라이언스

07 K-Shield 2차 교육훈련(디지털 포렌식)

정보유출 사고 발생 시 종합적인 대응절차 수행이 가능한 디지털 포렌식 전문가 양성
※ 훈련 대상 요건: K-Shield 1차 교육과정을 수료한 교육생 중 평가시험 상위자 등

훈련 내용

교과목	교육내용	
디지털포렌식 기본 실습	• 시나리오 기반 실습 - 레지스트리 포렌식 - 웹 포렌식	- 파일시스템 포렌식
디지털포렌식 실무 실습	• 시나리오 기반 실습 - 네트워크 포렌식 - 이메일 포렌식	- 로그 분석
디지털포렌식 심화 실습	• 시나리오 기반 실습 - 모바일 포렌식	- 데이터 복구

훈련 시간
연 1회 10일(70시간) 과정
09:30~17:30

훈련 방법
집체 훈련

정원
30명

활용 교재
자체개발교재

08 K-Shield 2차 교육훈련(악성코드 분석)

유형별 악성코드 분석 훈련을 통한 악성코드 분석 전문가 양성
※ 훈련 대상 요건: K-Shield 1차 교육과정을 수료한 교육생 중 평가시험 상위자 등

훈련 시간
연 1회 10일(70시간) 과정
09:30~17:30

훈련 방법
집체 훈련

정원
30명

활용 교재
자체개발교재

훈련 내용

교과목	교육내용
악성코드 판별 및 정보 수집	• 시나리오 기반 실습 - 악성코드 식별 및 기능 분석을 위한 악성코드 주요 기능 - 악성코드 기본 정보 분석
악성코드 분석 및 대응 기법	• 시나리오 기반 실습 - 악성코드 식별 - 기본정보 추출 - 악성코드 주요 기능 분석 - 시그니처 및 IoC 작성

09 K-Shield 2차 교육훈련(침해대응)

가상 환경에서의 사이버 공격 및 방어 훈련 수행을 통한 침해대응 고급 인력 양성
※ 훈련 대상 요건: K-Shield 1차 교육과정을 수료한 교육생 중 평가시험 상위자 등

훈련 시간
연 1회 10일(70시간) 과정
09:30~17:30

훈련 방법
집체 훈련

정원
30명

활용 교재
자체개발교재

훈련 내용

교과목	교육내용
침해사고 대응 실습	• 유형별 침해사고 대응 시나리오 실습 - 웹 어플리케이션 취약점, 웹쉘 및 공격도구 등을 활용한 정보유출 사고 대응 - 스피어 피싱 및 악성코드 공격 대응 등

10 K-Shield 2차 교육훈련(모의해킹)

IT 자산에 대한 취약점과 위협을 식별, 평가하고 발견된 취약점의
심층 분석이 가능한 모의해킹 전문인력 양성
※ 훈련 대상 요건: K-Shield 1차 교육과정을 수료한 교육생 중 평가시험 상위자 등

훈련 내용

교과목	교육내용
웹 및 시스템 모의해킹	• 웹 애플리케이션 및 시스템 모의해킹을 위한 단위기술 교육 • 모의해킹 시나리오 실습 • 보고서 작성
모의해킹 심화	• 모바일 어플리케이션 모의해킹 단위기술 교육 • 모바일 모의해킹 시나리오 실습
종합 실습	• 웹, 시스템, 모바일 모의해킹을 종합한 가상 시나리오 실습 • 취약점 진단 및 대책수립

훈련 시간
연 1회 10일(70시간) 과정
09:30~17:30

훈련 방법
집체 훈련

정원
30명

활용 교재
자체개발교재

11 K-Shield 2차 교육훈련(보안컨설팅)

정보자산에 대한 위협의 진단 및 제거를 통해
종합적인 정보보호 대책 수립이 가능한 컨설팅 전문인력 양성
※ 훈련 대상 요건: K-Shield 1차 교육과정을 수료한 교육생 중 평가시험 상위자 등

훈련 내용

교과목	교육내용
관리적 컨설팅 실무	• 시나리오 : 기업 보안수준 평가 - 보안환경 및 요구분석 - 정보보호 수준평가 - 위험분석/도출 - 대책수립
기술적 컨설팅 실무	• 시나리오 : 취약점 발견 및 이행 진단 - 취약점 진단 항목별 이해 - 인프라 자산에 대한 취약점 진단(서버, DBMS, 네트워크, 보안장비, 웹)
종합 컨설팅	• 시나리오 : 종합 컨설팅 실습 - ISMS 컨설팅 실무 - 관리적 컨설팅(수준진단, 취약점 도출, 대책 마련) - 기술적 컨설팅(인프라 진단, 취약점 발견, 대책 마련) - 마스터 플랜 수립 및 작성

훈련 시간
연 1회 10일(70시간) 과정
09:30~17:30

훈련 방법
집체 훈련

정원
30명

활용 교재
자체개발교재

12 K-Shield IoT보안 실습

IoT(사물인터넷) 환경의 보안이슈를 사전 예방하고 IoT 침해사고 대응 능력을 함양

훈련 시간
연 2회 5일(32시간) 과정
1~4일차 09:30~17:30
5일차 09:30~13:30

훈련 방법
집체 훈련

정원
20명

활용 교재
자체개발교재

훈련 내용

교과목	교육내용	
인터페이스	• PCB, IC 식별 • JTAG 식별, 연결	• UART 식별, 연결 • JTAG 디버깅, 메모리 조작
펌웨어	• 펌웨어 추출 • 펌웨어 취약점 분석	• 펌웨어 분석 • 펌웨어 수정
시큐어 부팅	• 시큐어 부팅	• 시큐어 부팅 우회
취약점 실습	• 취약점 실습(SDR)	

13 K-Shield 소프트웨어 개발보안 실습[설계]

정의된 보안요구사항에 따라 SW의 보안 아키텍처를 수립하고
이에 따라 SW에 대한 보안을 설계하는 능력 함양

훈련 시간
연 2회 5일(32시간) 과정
1~4일차 09:30~17:30
5일차 09:30~13:30

훈련 방법
집체 훈련

정원
20명

활용 교재
자체개발교재

훈련 내용

교과목	교육내용
SW 개발보안 이해	• SW개발 방법론이해 - SW개발보안 방법론 이해 - 분석/설계단계 산출물 이해 • RFP 분석과 보안요구 항목 식별 - RFP 분석 - 보안요구항목 식별 • 설계단계 고려해야 할 보안요구 항목 이해 - 입력값 검증, 인증, 인가 - 중요정보 처리, 세션 관리, 에러처리, 로깅
위협모델링	• 위협모델링 프로세스 이해 - 위협 도출 - 위험도 계산 - 대응기법 - 대응기술도출 - 위협모델링 WORKSHOP - 보안요구항목 적용 WORKSHOP

14 K-Shield 소프트웨어 개발보안 실습[테스트]

정의된 보안요구사항에 따라 SW의 보안 아키텍처를 수립하고
이에 따라 SW에 대한 보안을 테스트하는 능력 함양

훈련 내용

교과목	교육내용
SW테스트 이해	- SW테스트 개요 - SW테스트 프로세스 이해 - SW테스트와 SW보안 테스트 • SW보안성 테스트 준비 및 데이터 수집 단계 - 진단대상 및 방법 선정 - 요구사항 파악 - 정보수집 및 분석 - 테스트 준비 단계 WORKSHOP
SW보안성 테스트	- 동적분석도구 활용 방법 이해 - 진단 항목 식별 - 담당자 인터뷰, 자동점검, 수동점검을 통한 SW 보안성 테스트 - SW보안성 테스트 WORKSHOP - 보고서 작성 및 취약점 제거 권고안 작성 - 취약점 진단 및 보고서 작성

훈련 시간
연 2회 5일(32시간) 과정
1~4일차 09:30~17:30
5일차 09:30~13:30

훈련 방법
집체 훈련

정원
20명

활용 교재
자체개발교재

15 K-Shield 운영보안 실습

보안요구사항에 따라 정보 시스템을 안전하게 보호하기 위한 운영보안 전문역량 제고

훈련 내용

교과목	교육내용
운영 보안 개요	• 접근 제어 - 정보시스템 접근 제어 정책 및 지침 - 정보시스템 접근 제어 권한 설정 및 해제 - 정보시스템 접근 제어 이력관리
운영 보안 시나리오	• 시스템 운영 및 관리 - 정보시스템 운영 관리 정책 및 지침 - 정보시스템 운영 실무(장애 관리, 성능/용량 관리, 보안 관리, 패치 관리, 백업 관리등)
운영 보안 시나리오	• 정보시스템 보안 관리 - 침해시도 모니터링 - 정보시스템 취약점 점검 및 악성코드 관리 절차 실무
운영 보안 시나리오	• 정보시스템 보안 관리 - 시스템 보안솔루션 운영 - 정보시스템 보안성 검토 실습

훈련 시간
연 2회 5일(32시간) 과정
1~4일차 09:30~17:30
5일차 09:30~13:30

훈련 방법
집체 훈련

정원
20명

활용 교재
자체개발교재

교육 과정 안내

16 침해사고 분석대응 전문가

보안사고 발생 시 정보수집/분석/복구/대응 등의 활동을 전개하는 전문가 양성

훈련 시간
연 4회 4일(28시간) 과정
09:30~17:30

훈련 방법
집체 훈련

정원
30명

활용 교재
자체개발교재

훈련 내용

교과목	교육내용	
침해사고 분석개론	• 침해사고 분석의 정의와 사고유형 • 침해사고 대응주기 • 침해사고 분석 준비,탐지,분석,복구 등 • 악성코드 침해사고 시나리오	• 침해사고 분석 트렌드 • 침해사고 사후활동
침해사고 분석(Linux)	• 리눅스 시스템의 이해 • 리눅스 시스템 log evidence • 리눅스 증거분석방법론	• 리눅스 시스템 live evidence • 리눅스 루트킷 분석 • 리눅스 파일 복구 등
침해사고 분석(Windows)	• 윈도우 침해사고 분석 접근개념 • 윈도우 침해사고 증적분석 및 방법론	• 윈도우 침해사고 분석 사례 • 웹쉘 분석실무
악성코드 분석	• 침해사고 사례와 악성코드 • 악성코드 리버싱	• 악성코드 수집/탐지/분석

17 해킹방어를 위한 시큐어코딩

소프트웨어 보안 취약점의 이해를 토대로 진단취약점 도구를 활용한 개발보안 기법 습득

훈련 시간
연 6회 3일(21시간) 과정
09:30~17:30

훈련 방법
집체 훈련

정원
40명

활용 교재
자체개발교재

훈련 내용

교과목	교육내용	
시큐어코딩 개요 및 보안사례 위험한 코딩 스타일	• 시큐어코딩의 필요성	• 안전하지 않은 프로그래밍 습관
보안개발 방법론 정적 분석 및 위협모델링	• 보안개발 프로세스 단계별 활동 • 정적분석 결과 리포트 활용법 • 위협 모델링을 통한 소스코드 취약점 제거 활동	• 분석개발 단계의 보안활동
보안 취약점 DB활용 웹 어플리케이션 보안을 위한 기본 지식	• CVE/CWE, CERT, SANS 등 활용 • HTTP 구조, 인코딩, 정규식을 이용한 필터 작성기법 • 클라이언트 측 통제검사	• 서버 측 보안 메커니즘 검사
SW개발보안 기법	• 명령어, XPath, SOAP등의 인젝션 공격기법 및 취약점 제거 • 인증과 세션관리 취약점 • 크로스사이트요청위조 취약점 • 데이터암호화/접근제어/리다이렉트 취약점 • 디렉토리 리스팅, 에러 노출 등	• 크로스사이트스크림트 취약점 • 파일 업로드/다운로드 취약점

18 기반시설 네트워크 보안

정보통신 기반시설 네트워크 관리·운영 담당자의 침해사고 분석/대응 역량 강화

훈련 내용

교과목	교육내용
네트워크 보안	• 네트워크 프로토콜 기본 • 네트워크 해킹 접근방법의 이해 • 스니핑 및 스캐닝 기법 실습 • 계층별 스푸핑 취약점 공격 실습 • 세션하이재킹 공격 실습 • 보안 솔류션별 특징 • 인프라 장비 구성과 특성 • 네트워크 정보수집 도구들 • 와이파이 공격 및 암호해독 실습 • 분산(반사)서비스거부공격시스템 실습 • 취약점 진단 개요 및 위험평가 • 네트워크 인프라 보안 디자인
SCADA 보안	• 최신 사이버공격 트랜드 • 전력 SCADA 시스템 운영현황 • 침해사례 상세분석 (Stuxnet, Black Energy) • SCADA 시스템 보안 특성 • SCADA 시스템 공격 가능 시나리오 및 사용 취약점 정리(실습) • SCADA 망 침투 가능 시나리오 • SCADA 보안 국내외 추진현황(정책, 기술, 표준화 등) • SCADA 시스템 보안성 확보를 위한 대응책 서술(실습) • SCADA 시스템 보안성 확보 전략 • 정보통신기반보호법과 주요정보통신기반시설 취약점 분석·평가 • SCADA 보안기술 연구개발 현황 • 원자력 발전시스템 보안 • SCADA 시스템 개념 및 국내 SCADA 시스템 현황 • SCADA 시스템 보안위협 및 사이버 침해사례 • SCADA 취약점 분석 • 스마트그리드 보안 • IEC-62351 표준

훈련 시간
연 5회 4일(28시간) 과정
09:30~17:30

훈련 방법
집체 훈련

정원
30명

활용 교재
자체개발교재

19 디지털 포렌식 실습

정보유출, 침해사고 등에 대한 전자증거물을 수집/확보/분석하는 포렌식 전문기술인력 양성

훈련 내용

교과목	교육내용
디지털 포렌식 개론	- 디지털포렌식 개론(개념 및 법률이해) - 디지털포렌식 기초 실무(도구 및 사용법)
데이터베이스 포렌식	- 데이터베이스포렌식의 절차와 주의사항 - 데이터베이스 증거수집 실습 - 증거수집과분석과정
IoT 포렌식	- IoT와 드론 포렌식 사례 및 절차 - IoT 기기 데이터 수집 방법 및 분석 등 - IoT 포렌식 최신 동향 및 이슈
모바일 포렌식	- 모바일 포렌식 사례, 정의 및 원칙, 절차 - 최신 동향 및 이슈 - SQLite 카빙 및 실습 - 스마트폰 구조 및 저장 장치 - SQLite 소개 및 논리적·물리적 구조 - 모바일 앱 기반 암호화 및 리버스 엔지니어링

훈련 시간
연 3회 4일(28시간) 과정
09:30~17:30

훈련 방법
집체 훈련

정원
30명

활용 교재
자체개발교재

20 암호 및 인증의 이해와 실무 응용

암호알고리즘의 안전성과 구현 적합성을 검증하기 위해
분석 과정 및 결과 도출을 설계하는 능력 함양

훈련 시간
연 3회 4일(28시간) 과정
09:30~17:30

훈련 방법
집체 훈련

정원
30명

활용 교재
자체개발교재

훈련 내용

교과목	교육내용
암호 및 인증 기술	• 암호학 기초 및 최신 기술 동향 - 암호의 역사 - 암호 유형 별 알고리즘(대칭키/비대칭키/일방향 암호) - 암호 키 관리, 최신 암호 기술(WBC) - 온라인 인증서비스, OTP 인증기술, FIDO 인증기술, 블록체인기술 등 최신 기술 동향 개요 • 암호 알고리즘 보안요구사항 확인하기 - ASN.1, PKI표준 - 온라인 인증 서비스, 공인인증체계 • 알고리즘 개발하기 - PKCS이론/실습, PKI응용 • 암호 알고리즘 보안요구사항 확인하기 - 암호이론, 암호프로토콜의 이해 - E2E 암호기술, OTP 인증기술, FIDO 인증기술

21 웹 공격 및 대응 기법

웹 브라우저에 대한 지식을 갖고 정의된 보안요구사항에 따라
SW에 대한 보안을 구현, 테스트하는 능력 함양

훈련 시간
연 3회 3일(21시간) 과정
09:30~17:30

훈련 방법
집체 훈련

정원
25명

활용 교재
자체개발교재

훈련 내용

교과목	교육내용
웹 공격 및 대응 기법	• 웹 보안 기본 지식 - 실습 환경 구성 : Linux, Apache, Java, PHP, MySQL - HTTP 프로토콜의 구조와 특징 - 주요 브라우저 및 렌더링 엔진 비교 - 주요 인코딩 기법 이해 - 주요 취약점 DB 및 시큐어코딩 가이드 참조 - 웹 브라우저 보안 기능 이해 -HTML5 / SOP / CORS / CSP • 주요 웹 공격 및 대응 기법 - SQL Injection 공격 원리 및 유형 이해 - SQL Injection 대응 기법 이해 - Command Injection 공격 원리 이해 - Command Injection 대응 기법 이해 - XSS 공격 원리 및 유형 이해 - XSS 공격 대응 기법 이해 - CSRF 공격 원리 및 대응 기법 이해 - HTML5 신규 기능을 이용한 공격 및 대응 기법 이해 - 주요 JavaScript Framework 소개 - Angular, Vue.js, React 보안 이해

22 보안 컨설팅 이론과 실제

체계적인 보안컨설팅 이론 및 실습 교육을 통해 보안컨설팅 수행역량 및 프로젝트관리 역량 제고

훈련 내용

교과목	교육내용	
보안컨설팅 이해	• 정보보호 컨설팅의 이해 • 최근 보안컨설팅 트렌드	• 보안컨설팅 프로젝트 이해
보안컨설팅 실무이론 및 실습	• 보안컨설팅 수행 방법 • 위험분석 방법론 • 정보보호 대책 수립 • 실습	• 자산분석 • 위험 식별 및 위험평가 • 정보보호관리체계 이해
보안컨설팅 프로젝트관리 실무	• 프로젝트의 이해 • 프로젝트 단계별 관리활동	• 프로젝트 관리자 역할 및 책임 • WBS 및 보고자료 작성 실무
정보보호관리체계 인증	• 비즈니스 유형별 정보보호 관리체계 특성 • 정보보호 관련 법규 현황 • 정보보호관리체계 인증심사 주안점	• 정보보호관리체계 수립 준비

훈련 시간
연 3회 3일(21시간) 과정
09:30~17:30

훈련 방법
집체 훈련

정원
30명

활용 교재
자체개발교재

23 정보통신 기반시설 정보보호 업무실무

사이버침해로부터 정보통신 기반시설을 보호하고 대응하기 위하여
기반시설 정보보호 담당자의 사이버보안 전문역량 제고

훈련 내용

교과목	교육내용	
주요 정보통신 기반시설 보호의 이해	• 기반보호 제도 소개 • 기반시설 침해사고 동향 및 대응기술	• 관리기관 보호체계 가이드
위험관리 방법론	• 위험분석 개요 • 위험 분석 및 평가	• 위험분석 전략 및 계획 수립 • 정보보호 대책 선정 및 계획 수립
기반시설 보호를 위한 취약점 진단 및 분석	• 취약점 진단개요 • UNIX 취약점 분석 • Windows 취약점 분석 • 웹 취약점 진단	• 취약점 점검 실습 환경준비 • 네트워크 취약점 분석 • 취약점 위험 평가 • 제어시스템 보안
기반시설 보안관제의 이해 및 기반시설 관제방안	• 기반시설 보안관제의 이해와 특성 • 장비별 특징 및 보안설정 등 관제 방안	• 국내외 관제 동향 • 기반시설 통합보안관제 구성

훈련 시간
연 4회 4일(28시간) 과정
09:30~17:30

훈련 방법
집체 훈련

정원
30명

활용 교재
자체개발교재

한국인터넷진흥원 사이버보안인재센터
찾아 오시는 길

약도

경기도 성남시 수정구 대왕판교로 815 판교 제2테크노밸리 기업지원허브 4~5층
KISA 사이버보안인재센터

대중교통

판교제2테크노밸리 정류장(구 한국도로공사) 하차 후 도보 약 5분

- **수서역 6번 출구 정류장** 일반 B 101 광역 B 1007, 1007-1, 1009, 5600, 5700, 6900
- **잠실광역환승센터** 일반 B 101 광역 B 1007, 1009
- **잠실역 4번 출구 정류장** 광역 B 1007-1, 6900
- **잠실역 6, 7번 출구 중앙버스 정류장** 광역 B 5600, 5700
- **판교역 동편 정류장** 일반 B 55, 370

자가용

- **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

국가인적자원개발컨소시엄
CHAMP Consortium for HRD Ability Magnified Program