국가인적자원개발컨소시엄
Consortium for HRD Ability Magnified Program

2023

최정예 정보보호 전문인력 양성(K-Shield) 교육과정 안내

고용노동부
Ministry of Employment and Labor

HRDK 한국산업인력공단
Human Resources Development Service of Korea

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

2023

최정예 정보보호 전문인력 양성(K-Shield) 교육과정 안내

CONTENTS

한국인터넷진흥원 KISA 아카데미는?

KISA 아카데미는 정보보호 분야 전문인력 양성을 위하여 다양한 교육 프로그램을 운영하고 있는 전문교육기관입니다. KISA 아카데미는 세계 최고의 사이버보안 전문인력 양성 기관을 목표로 최정예 정보보호 전문인력 양성 과정(K-Shield, 케이쉴드)을 통해 우수보안인력을 양성하고 있으며, 정보보호 재직자 역량 강화를 위한 산업보안 전문인력 양성 교육을 제공하고 있습니다. 이외에도 정보보호 인력양성을 위한 정책수립 및 활성화를 위한 지원과, 산업계 양적/질적 수요에 대응한 사이버보안 우수 인력을 양성하는 등 분야별 정보보호 인력의 수급차 해소에 기여하고 있습니다.

KISA 아카데미 **비전 및 목표**

한국판 뉴딜을 이끌 사이버보안 인재 육성으로
국가 디지털 트랜스포메이션 기반 확립

사이버보안 인력의 양적&질적 성장 지원으로 정보보호 산업 성장 주도

정보보호 인력양성 정책수립 및 활성화 지원

- 사이버보안 인력 수급차 현황조사 및 각종 양성정책 연구

정보보호 인력양성 정책수립 및 활성화 지원

- 온/오프라인 실전형 사이버훈련장 (Security Gym)운영
- 온택트 기반 인력양성

산업계 양적/질적 수요에 대응한 사이버보안 우수 인력 양성

- 정보보호 특성화 대학 지원
- 지역전략산업 융합보안 핵심인재양성(융합보안대학원)
- 구직자 정보보호 전문인력 양성(K-Shield Jr)

사이버보안 재직자 경력개발 및 역량강화 지원

- **최정예 정보보호 전문인력 양성(K-Shield)**
- 전자정부 정보보호 전문교육

국가인적자원개발컨소시엄 전략분야 인력양성사업이란?

CHAMP : Consortium for HRD Ability Magnified Program

국가인적자원개발컨소시엄
Consortium for HRD Ability Magnified Program

국가인적자원개발컨소시엄 사업은 고용보험법 시행령 제52조 제1항6호, 제2항 및 제3항에 따라 공동훈련센터가 협약기업사업주와 협약을 체결하고 근로자의 니즈를 파악하여 수요자 중심의 맞춤형 교육 프로그램을 제공하는 대한민국의 대표적인 직업능력개발훈련 사업입니다. 특히 전략분야는 특정 산업이나 직종에 대한 체계적인 인력양성 및 근로자 직업능력개발을 목적으로 하며, 한국인터넷진흥원은 정보보호 분야에 특화된 전문교육을 제공합니다. 현재 국내 72개 기업·기관 및 단체가 전략분야 인력양성 훈련기관으로 지정되어 있습니다.

사업운영체계

협약기업 지원

수요자 중심의 맞춤형 교육훈련 제공

- 수요조사를 통하여 정보보호 산업계의 전략적 요구를 반영한 훈련과정 개발 및 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 교육비 지원(우선지원 대상기업 100%, 대규모기업 80% 지원)

간편한 교육훈련 참여 등 편리한 행정서비스 제공

- 공동훈련센터와의 협약 체결만으로 원하는 교육훈련과정에 참여할 수 있는 간편한 절차 제공
- 협약기업별 참여인원 제한 없음

훈련참여자 지원

재직근로자 맞춤형 교육훈련 제공

- 공동훈련센터는 협약기업 재직자 대상 직무 향상교육을 제공하고 수요조사를 통하여 협약기업 근로자가 원하는 맞춤형 교육훈련을 지속적으로 개발

교육비

우선지원 대상기업 재직자 교육비 전액 무료, 대규모기업 재직자의 경우 80% 지원

- 교육비는 교육과정별 상이하므로, 누리집 및 교육과정 안내 참고

별도의 협약 관련 가입비 및 교육비 환급절차 없음

- 기업이 직업능력개발 및 고용안정을 위하여 조성한 고용보험기금을 통해 조달

최정예 정보보호 전문인력 양성(K-Shield) 교육 참여방법

교육대상

- 한국인터넷진흥원과 전략분야 인력양성사업 협약이 체결된 기업에 재직 중이며, 고용보험을 납부하고 있는 재직자

※ 공무원, 학생, 기업대표 등은 본 교육 대상에서 제외됩니다.

협약기업의 정보보호 유관업무 담당자 및 관리자를 대상으로 하며, 21년부터 대규모기업도 협약 체결 및 교육 수강은 가능하나, 20%의 교육비 부담이 발생합니다.

우선지원 대상기업이란

고용안정 사업 및 직업능력개발 사업을 실시할 때 우선적으로 고려해야 하는 기업을 말합니다.
제조업의 경우 상시 근로자 수가 500명 이하일 때 우선지원 대상기업에 해당하며, **"출판, 영상, 방송통신 및 정보 서비스업", "전문, 과학 및 기술 서비스업"**은 상시 근로자 수 300명 이하, 금융 및 보험업은 상시 근로자 수 200명 이하 등 업종별로 기준이 상이합니다.

※ 소속기업의 우선지원 대상기업 해당 여부는 **근로복지공단(☎1588-0075)** 또는 **고용노동부 고객상담센터(☎1350)**를 통해 확인하시기 바랍니다.

협약절차

2023년 협약체결 기간 : 2023년 2월 1일(수) ~ 2023년 9월 29일(금)

※ 9월 29일(금)까지 협약체결이 완료된 기업에 한하여 2023년도에 실시하는 교육수강신청 가능

제출서류

- 전략분야 인력양성사업 **협약서 원본 1부** 및 **참여기업 일반현황 1부**를 작성하여 **메일로 제출**
- 신규 협약기업대상 **최정예 정보보호 인력양성 교육 선호도 조사 온라인 설문 진행**

제출처

- champ@kisa.or.kr

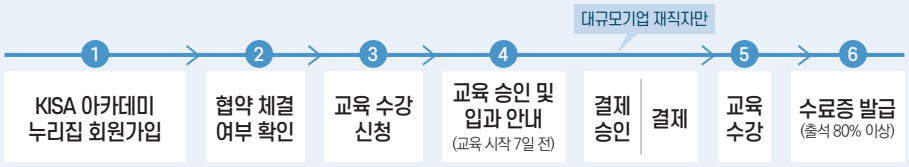
※ 협약 시점은 고용노동부 HRD-Net 행정지원시스템에 협약정보가 등록된 날 부터로, KISA 아카데미 누리집(https://academy.kisa.or.kr) 좌측 하단 "협약체결안내"에서 기업명 검색을 통해 협약 체결 여부를 확인하실 수 있습니다.

※ 협약 완료 여부는 별도로 유선 통보하지 않으며, 협약체결 완료 후 협약서를 메일로 회신해 드립니다.

※ 국가인적자원개발컨소시엄 전략분야는 타 컨소시엄 운영기관과 중복협약이 가능합니다.

협약서 다운로드
KISA 아카데미 누리집
https://academy.kisa.or.kr

교육수강절차



모든 교육은 KISA 아카데미 누리집(https://academy.kisa.or.kr)를 통해서만 신청할 수 있습니다.

- 교육생 출결관리, 수료증 발급 등을 위하여 **개별 회원가입 후 교육신청 가능(단체수강 불가)**
- 협약체결 예정 기업의 경우 협약체결이 완료된 후 교육신청 가능
- 수료증 발급은 교육 종료 3일 후, KISA 아카데미 누리집 퀵메뉴에서 출력

교육 시작일 약 1개월 전부터 교육신청 접수를 받으며, 업무일 기준 교육시작 7일전 모집 마감됩니다.

- 선착순 모집으로 사전 마감 될 수 있음
- 교육접수 마감 후 신청자의 취소로 여석이 발생하는 경우에 한하여 추가모집 진행
- **KISA 아카데미 누리집 공지사항의 '연간교육일정' 참고**

협약기업별 교육 참여횟수 및 교육과정별 참여 인원에 대한 제한은 없습니다.

최정예 정보보호 전문인력 양성(K-Shield) 교육 강사 POOL제 운영 안내

한국인터넷진흥원 KISA 아카데미는 국가인적자원개발컨소시엄 사업의 효율적인 운영을 위해 「최정예 정보보호 인력양성 교육」에 참여할 강사를 상시적으로 모집함으로써, 우수한 강사를 체계적으로 확보하고, 교육의 질적 향상을 도모하고자 합니다.
지원서를 제출하신 강사분들은 강사 POOL에 등록되며, KISA 아카데미에서 검토 후 필요한 과정 개설 시 해당 강사 중 개별적으로 연락하여 진행합니다.

강사POOL 지원대상

- 최정예 정보보호 인력양성 과정 중 강사 지원 분야에 관련된 전문성이 있으며 강의 수행 능력이 뛰어난 사람
- 정보보호 관련 기업인, 대학교수, 일반인 등

강사역할

- 정보보호 관련 분야 강의 및 평가
- 온·오프라인 과정 교재 제작
- 최정예 정보보호 전문인력 양성과정 자문 활동 등

※ 강사료 등 제반 수당은 '국가인적자원개발 컨소시엄 운영기준'에 의함

강사POOL 지원방법

제출 자료 : [첨부] KISA 아카데미 강사 POOL 등록 신청서
제출 방법 : champ@kisa.or.kr(전자우편으로 접수)
제출 기한 : 상시
문　　의 : 한국인터넷진흥원 KISA 아카데미 박유리 수석연구원(Tel. 02-405-6506)
지원 분야 : 자세한 내용은 KISA아카데미 누리집을 참고(https://academy.kisa.or.kr)

강사선정 및 포상제도

- 교육과정 개설 시 컨소시엄 운영위원회의 선정 절차를 거쳐 강사 선정

※ 강사 POOL 지원만으로 강의를 위촉하지 않음

- 강사로 선정 시 훈련생들에게 만족도 평가를 진행하며, 상위10%의 우수 강사진에게는 감사패 수여

※ 2년 연속 우수 강사로 전정 시 KISA 아카데미 누리집 '명예의 전당'에 등재

[우수포상]

교육 품질 향상을 위해
강사의 훈련 준비에 대한 평가와
훈련생 만족도 평가 점수를
합산하여 최종 평가

※ 필요시 가점/감점 항목을 추가할 수 있음

최정예 정보보호 전문인력 양성(K-Shield) 인증 과정 안내

K-Shield 인증과정

• K-Shield는 최정예 사이버보안 전문가 양성 목적의 침해사고 예방·대응 기술 전문 교육과정으로 정보보호 산업계 재직자 대상 연간 교육 총 150시간 이상 및 단계별 교육과정 합산 이수 시간에 따라 모두 수료하는 경우에 한하여, 최종 인증서 평가를 거쳐 한국인터넷진흥원장이 인정하는 최정예 사이버보안 전문가(K-Shield) 인증서를 발급하여 드립니다.

K-Shield 인증서 발급 절차

• **K-Shield 인증 과정** 으로 별도 표기된 과정 중 총 150시간 이상 수료 시, 최종 인증서 평가에 응시할 수 있으며, 평가 기준 점수에 따라 인증서 발급 여부가 결정됩니다.

인증 과정 교육 수강

K-Shield 인증 과정 표기된 과정 교육 수강

교육과정 최소 수료 기준 충족

K-Shield 인증 과정 총 150시간 이상 수료

※ Pro 과정 60시간 이상 수료 필수

최종 인증생 평가

K-Shield 인증서 발급을 위한 최종 평가

최종 인증서 발급

K-Shield 인증서 수여 ('23.12월 경)

K-Shield 교육내용

교육과정 통합 브랜드 K-Shield

• 기존 산업계 맞춤형 전문인력 양성 교육(산업보안)과 최정예 정보보호 전문인력 양성교육(K-Shield)으로 이원화되어 운영하였던 교육과정을 K-Shield 교육으로 통합하여, 브랜드 이미지를 강화하고 수준별로 교육과정을 다양화 하였습니다.

K-Shield 교육과정

• 정보보호 초급 담당자부터 전문가급 고급 기술자까지 필요한 다양한 수준의 맞춤형 교육을 제공합니다.

K-Shield Pro+(최고급) 실전형사이버훈련장

• 전문가급 심화과정, 고급 기술자, Pro과정 이수자, 실전형 훈련 연계 과정, 최대 5일

K-Shield Pro(고급)

• 전문가급 심화과정, 고급 기술자, Advanced 과정 수료 연계 과정, 최대 5일

K-Shield Advanced(중급)

• 정보보호 관리자, 상급 실무자, Basic과정 수료 연계 과정, 최대 5일

K-Shield Basic(초·중급)

• 정보보호 실무자, 초·중급 실무자, 기본 과정, 최대 3일

K-Shield Start(초급)

• 정보보호 담당자, 초급 실무자, 지역 연계 과정, 최대 1일

2023년 최정예 정보보호 전문인력 양성(K-Shield) 교육 연간 일정

	훈련과정명	과정종류	훈련시간	훈련인원	교육비(대규모기업)	훈련일정(안)
1	K-Shield 클라우드 보안 인프라스트럭쳐 서비스 구축 실무		18H (3일)	18명	62,630원	1차 : 08.16(수)~08.18(금) 2차 : 08.23(수)~08.25(금) 3차 : 09.13(수)~09.15(금) 4차 : 11.08(수)~11.10(금)
2	K-Shield 보안컨설팅 이론과 실무	-	18H (3일)	18명	62,690원	1차 : 05.24(수)~05.26(금) 2차 : 07.05(수)~07.07(금) 3차 : 10.11(수)~10.13(금)
3	K-Shield Spring 프레임워크 시큐어코딩		18H (3일)	20명	66,950원	1차 : 04.05(수)~04.07(금) 2차 : 06.28(수)~06.30(금) 3차 : 08.30(수)~09.01(금)
4	K-Shield 네트워크 보안 위협 대응 실무	-	24H (4일)	18명	93,080원	1차 : 04.04(화)~04.07(금) 2차 : 05.09(화)~05.12(금) 3차 : 09.12(화)~09.15(금)
5	K-Shield 포렌식을 활용한 기업보안사고 대응		21H (3일)	20명	72,080원	1차 : 04.24(월)~04.26(수) 2차 : 07.05(수)~07.07(금)
6	K-Shield 웹 공격 및 대응 기법	-	21H (3일)	18명	71,600원	1차 : 04.26(수)~04.28(금) 2차 : 09.20(수)~09.22(금) 3차 : 11.01(수)~11.03(금)
7	K-Shield 제어시스템 보안	-	18H (3일)	20명	67,060원	1차 : 06.07(수)~06.09(금) 2차 : 06.14(수)~06.16(금)
8	K-Shield 데브옵스 환경의 컨테이너 보안	-	21H (3일)	18명	71,600원	1차 : 08.23(수)~08.25(금) 2차 : 09.04(월)~09.06(수) 3차 : 10.04(수)~10.06(금)
9	K-Shield IT/OT 프로토콜 취약점 분석과 증거수집 기법	-	28H (4일)	18명	95,730원	1차 : 06.27(화)~06.30(금) 2차 : 08.29(화)~09.01(금) 3차 : 10.10(화)~10.13(금)
10	K-Shield 침해사고 기반환경 구성과 보안점검		18H (3일)	18명	66,430원	1차 : 05.17(수)~05.19(금) 2차 : 09.20(수)~09.22(금) 3차 : 11.01(수)~11.03(금)
11	K-Shield 산업 무선 시스템 해킹과 보안	-	14H (2일)	20명	54,360원	1차 : 05.15(월)~05.16(화) 2차 : 09.18(월)~09.19(화) 3차 : 10.30(월)~10.31(화)

[과정 수준]

- Pro+ (최고급)
- Pro (고급)
- Advanced (중급)
- Basic (초·중급)
- Start (초급)

	훈련과정명	과정종류	훈련시간	훈련인원	교육비(대규모기업)	훈련일정(안)
12	K-Shield KT Cloud 및 Naver Cloud 보안 실무(국내)		14H (2일)	20명	46,570원	1차 : 09.18(월)~09.19(화) 2차 : 10.30(월)~10.31(화)
13	K-Shield Microsoft Azure 및 Google Cloud 보안 인프라 구축(국외)		14H (2일)	20명	46,570원	1차 : 08.28(월)~08.19(화) 2차 : 10.05(월)~10.06(화)
14	K-Shield 그레이박스 테스팅을 통한 웹 모의해킹		14H (2일)	18명	42,500원	1차 : 05.30(화)~05.31(수) 2차 : 미정
15	K-Shield 제어시스템 보안(심화)	-	6H (1일)	20명	20,750원	1차 : 05.10(수) 2차 : 05.31(수) 3차 : 09.06(수)
16	K-Shield 사이버전 실전 훈련 (실전형 훈련장 연계과정)		30H (5일)	18명	81,400원	1차 : 06.26(월)~06.30(금) 2차 : 09.04(월)~09.08(금)
17	K-Shield 모의해킹 실습 훈련 전문가 과정		24H (4일)	18명	89,430원	1차 : 08.01(화)~08.04(금) 2차 : 11.27(월)~11.30(목)
18	K-Shield 보안 취약점 분석 화이트해커 전문가 과정		35H (5일)	18명	153,470원	1차 : 05.22(월)~05.26(금) 2차 : 07.03(월)~07.07(금) 3차 : 10.23(월)~10.27(금)
19	K-Shield 안티바이러스 엔진 개발		30H (5일)	18명	110,290원	1차 : 08.07(월)~08.11(금)
20	K-Shield 침투테스트 종합 훈련		35H (5일)	18명	131,410원	1차 : 07.24(월)~07.28(금) 2차 : 11.13(월)~11.17(금)
21	K-Shield 위협탐지를 위한 네트워크 패킷 및 트래픽 분석		30H (5일)	18명	117,970원	1차 : 04.03(월)~04.07(금)
22	K-Shield 악성코드 문서파일 분석 (MS 오피스, 한글, RTF 등)		30H (5일)	18명	117,970원	1차 : 09.18(월)~09.22(금)
23	K-Shield 악성코드 쉘코드 분석		30H (5일)	18명	117,970원	1차 : 05.15(월)~05.19(금)
24	K-Shield 침해사고 시나리오 기반 위협상황 실전 대응 훈련		30H (5일)	18명	117,970원	1차 : 10.30(월)~11.3(금)

	훈련과정명	과정종류	훈련시간	훈련인원	교육비(대규모기업)	훈련일정(안)
25	K-Shield 중소기업 보안역량 강화 (with.보호나라)	-	18H (3일)	20명	63,230원	1차 : 06.28(수)~06.30(금)
26	K-Shield 시큐리티 모니터링을 위한 SIEM구축 및 활용		18H (3일)	20명	56,190원	1차 : 07.26(수)~07.28(금) 2차 : 09.13(수)~09.15(금)
27	K-Shield 주요 정보통신 기반시설(리눅스) 취약점 진단 스크립트 개발 및 실무 적용사례 분석		18H (3일)	20명	63,250원	1차 : 07.10(월)~07.12(수)
28	K-Shield 보안제품군 훈련		18H (3일)	20명	62,930원	1차 : 05.31(수)~06.02(금) 2차 : 10.11(수)~10.13(금)
29	K-Shield 시큐리티 컨설턴트 트레이닝		18H (3일)	20명	63,250원	1차 : 05.02(화)~05.04(목)
30	K-Shield 모바일 디지털 증거능력 활용		18H (3일)	20명	62,930원	1차 : 05.17(수)~05.19(금) 2차 : 10.16(월)~10.18(수)
31	K-Shield 사이버 위협 보안 기술 동향 및 위협 탐지 프로세스 설계		12H (2일)	20명	37,990원	1차 : 06.08(목)~06.09(금) 2차 : 08.24(목)~08.25(금)
32	K-Shield 웹 애플리케이션 취약점 진단 분석		18H (3일)	20명	65,190원	1차 : 07.03(월)~07.05(수) 2차 : 08.30(수)~09.01(금)
33	K-Shield HTTP Security A to Z		21H (3일)	20명	74,510원	1차 : 05.02(화)~05.04(목) 2차 : 07.10(월)~07.21(수)
34	K-Shield DevSecOps환경 구축을 위한 코드 파이프라인 디자인		18H (3일)	20명	68,960원	1차 : 05.31(수)~06.02(금) 2차 : 11.01(수)~11.03(금)
35	K-Shield 모바일 애플리케이션 취약점 분석 및 공격과 보안		35H (5일)	20명	131,140원	1차 : 04.24(월)~04.28(금) 2차 : 11.20(월)~11.24(금)
36	K-Shield 클라우드 인프라 환경에서의 지능형 보안 위협 방어 (AWS)		18H (3일)	18명	65,270원	1차 : 04.12(수)~04.14(금)
37	K-Shield 클라우드 인프라 환경에서의 지능형 보안 위협 방어 (Google)		18H (3일)	18명	64,930원	1차 : 07.17(월)~07.19(수) 2차 : 08.16(수)~08.18(금)
38	K-Shield 클라우드 인프라 환경에서의 지능형 보안 위협 방어 (MS)		18H (3일)	18명	58,580원	1차 : 08.21(월)~08.23(수)
39	K-Shield IoT 환경을 위한 리눅스 포렌식		30H (5일)	18명	117,260원	1차 : 05.08(월)~05.12(금) 2차 : 09.18(월)~09.22(금)

	훈련과정명	과정종류	훈련시간	훈련인원	교육비(대규모기업)	훈련일정(안)
40	K-Shield 디지털 포렌식 단위기술 분석도구 활용		18H (3일)	18명	70,140원	1차 : 06.12(월)~06.14(수) 2차 : 08.16(수)~08.18(금)
41	K-Shield 리버싱을 통한 프로그램 인증 우회 및 악성코드 구조분석		18H (3일)	18명	68,810원	1차 : 04.05(수)~04.07(금) 2차 : 06.12(월)~06.14(수) 3차 : 09.13(수)~09.15(금)
42	K-Shield 버그바운티를 위한 Fuzzing & Exploit 개발 과정		35H (5일)	18명	126,490원	1차 : 06.19(월)~06.23(금) 2차 : 11.06(월)~11.10(금)
43	K-Shield 정보시스템 운영 보안 관리 실습		12H (2일)	18명	44,300원	1차 : 04.20(목)~04.21(금) 2차 : 06.15(목)~06.16(금) 3차 : 07.13(목)~07.14(금)
44	K-Shield 주요 취약점 공격 실습을 통한 모의 침투테스트		35H (5일)	18명	130,260원	1차 : 08.21(월)~08.25(금)
45	K-Shield 침투 시나리오를 활용한 웹, 모바일 환경 모의해킹 실습		35H (5일)	18명	117,530원	1차 : 06.19(월)~06.23(금) 2차 : 08.07(월)~08.11(금)
46	K-Shield 침해사고 현장대응 감사 기법		18H (3일)	20명	65,190원	1차 : 06.07(수)~06.09(금) 2차 : 09.04(월)~09.06(수)
47	K-Shield 사이버 회복력, 데이터 분석		18H (3일)	20명	64,560원	1차 : 09.25(월)~09.27(수) 2차 : 11.06(월)~11.08(수)
48	K-Shield 악성코드 기초 및 리버싱 없는 기본 분석		6H (1일)	20명	23,650원	1차 : 06.27(화) 2차 : 09.07(목)
49	K-Shield 포렌식을 활용한 침해사고 로그 분석 기법		18H (3일)	18명	70,140원	1차 : 05.02(화)~05.04(목) 2차 : 08.02(수)~08.04(금)
50	K-Shield MITRE ATT&CK 기반 위협 분석		30H (5일)	18명	110,290원	1차 : 08.28(월)~09.01(금)
51	K-Shield 악성코드 공격대응		18H (3일)	20명	65,190원	1차 : 05.22(월)~05.24(수) 2차 : 07.17(월)~07.19(수)
52	(부산) K-Shield 정보보안 담당자를 위한 사례 중심의 컨설팅 실습	-	6H (1일)	20명	23,650원	1차 : 07.21(금) 2차 : 11.17(금)

※ 교육일정 및 인원은 추후 변경될 수 있으며, 보다 자세한 사항은 KISA 아카데미 누리집(https://academy.kisa.or.kr)을 참고하여 주시기 바랍니다.

2023년 최정예 정보보호 전문인력 양성(K-Shield) 교육과정 안내

1 K-Shield 클라우드 보안 인프라 스트럭쳐 서비스 구축 실무

- 주 요 내 용 : 클라우드 시스템 환경에 대한 보안요소가 구축·운영이 이루어지도록 보안요소를 구현하는 능력 향상
- 훈련대상 요건 : 정보보호 직무 분야 재직자 및 보안 담당자, 클라우드 시스템 관리자 등

교과목	교육내용
AWS 클라우드 인프라 구축	• AWS 클라우드 이해 • AWS 계정생성 및 EC2 서비스 요금 관리 • EBS 데이터 암호화 볼륨생성 및 보안 원격 액세스 • ELB와 Autoscaling을 활용한 고가용성, 내결함성 구현 • VPC 네트워크 구축 및 피어링 설정 등 • Cloudformation을 활용한 클라우드 인프라 구축
AWS 클라우드 서비스 보안	• S3 버킷 보안 정책과 데이터 보호 • IAM 사용자, 그룹, 다중인증 설정, 키 유출 대책 • AWS CLI 설치 및 보안자격 증명 설정 • ACM을 이용한 공인인증서 발급 및 HTTPS 보안연결 • Cloudwatch, CloudTrail, Config 모니터링 • 아마존 Inspector를 이용한 애플리케이션 보안분석 등
AWS 클라우드 네트워크 보안	• AWS보안 공동책임 모델 이해 • AWS WAF 구축 및 DVWA 도커 컨테이너 취약점 진단 • NAT 게이트웨이를 이용한 격리 네트워크 구축 • 보안 그룹과 NACL 설정 • 네트워크 보안을 위한 AWS와 온-프레미스 IPsec VPN 연결 • 클라우드 보안이 강화된 워드프로세스 설계 및 구축 프로젝트 수행

교육 과정 : K-Shield Basic(초·중급)
훈련 방법 : 집체훈련
훈련 일수 : 3일
훈련 시간 : 18시간
훈련 인원 : 회당 18명
대규모기업 교육비 : 62,630원

2 K-Shield 보안컨설팅 이론과 실무

K-Shield 인증 과정 아님

- 주 요 내 용 : 조직의 보안현황을 분석하고 보안위험을 식별하며 보안위험 평가를 통해 정보보호 대책을 수립하는 보안 컨설팅 수행 능력을 함양
- 훈련대상 요건 : 정보보호 직무 분야 재직자 및 보안 담당자

교과목	교육내용
보안컨설팅 이해	• 보안컨설팅 이해 • 최신 보안컨설팅 트렌드
보안현황 분석	• 보안현황 조사방법 • 보안컨설팅 수행 방법 • 보호 대상의 정보자산 도출방법 • 법률 요구사항 분석
보안 위험분석 및 평가	• 보안 위험분석 방법론 • 정보자산 식별 및 취약점 진단 • 위험식별 및 위험평가
보안통제 설계하기	• 보안통제 적용전략 수립 • 보호대책 선정 및 이행계획 수립
보안컨설팅 프로젝트 관리 실무	• 프로젝트 이해 • 프로젝트 관리자 역할과 책임 • 프로젝트 관리활동
정보보호 관리체계 컨설팅 주안점	• 정보보호 관리체계 이해 • 정보보호 인증제도 이해 • 정보보호 관리체계 컨설팅 준비사항 • 정보보호 관리체계 컨설팅 수행 시 주안점

교육 과정 : K-Shield Basic(초·중급)
훈련 방법 : 집체훈련
훈련 일수 : 3일
훈련 시간 : 18시간
훈련 인원 : 회당 18명
대규모기업 교육비 : 62,690원

3 K-Shield Spring 프레임워크 기반 시큐어코딩

- 주 요 내 용 : 정의된 보안요구사항에 따라 SW의 보안 아키텍처를 수립하고 이에 따라 SW에 대한 보안을 설계하는 능력을 함양
- 훈련대상 요건 : 정보보호 직무 분야 재직자 및 보안 담당자, 소프트웨어 개발 설계자, 소프트웨어 보안약점 진단원 등

교과목	교육내용
시큐어코딩 개요	• 사고 사례 기반 시큐어코딩 이해
SW개발보안 방법론	• SW개발보안 방법론 이해 및 성공사례 • 제로트러스트 보안 모델을 적용한 보안성 강화 • DevSecOps 환경 구축으로 개발보안 구현
웹해킹 대응을 위한 기본지식	• HTTP, Session, Cookie 취약점 이해
취약점 대응을 위한 시큐어코딩 기법	• 인젝션(SQL/Command) 대응 시큐어코딩 기법 • 크로스사이트 스크립트(XSS) 대응을 위한 시큐어코딩 기법 • 크로스사이트 요청위조(CSRF) 대응을 위한 시큐어코딩 기법 • XXE 대응을 위한 시큐어코딩 기법 • 역직렬화 취약점 대응을 위한 시큐어코딩 기법
취약점 대응을 위한 시큐어코딩 기법	• 파일 업로드 취약점 대응을 위한 시큐어코딩 기법 • Log4j 취약점 대응을 위한 시큐어코딩 기법
SW보안성 강화를 위한 SW개발보안	• 중요 정보 암호화를 위한 설계 및 구현단계 보안 강화 • 인증 강화를 위한 설계 및 구현단계 보안 강화 • 접근제어 강화를 위한 설계 및 구현단계 보안 강화
SW보안약점 진단도구 활용	• 오픈소스를 이용한 시큐어코딩 진단 • 오픈소스 진단도구 커스터 마이징

교육 과정 : K-Shield Advanced(중급)
훈련 방법 : 집체훈련
훈련 일수 : 3일
훈련 시간 : 18시간
훈련 인원 : 회당 20명
대규모기업 교육비 : 66,950원

4 K-Shield 네트워크 보안 위협 대응 실무

K-Shield 인증 과정 아님

- 주 요 내 용 : 네트워크 구조 및 보안기반 이론을 토대로 보안 위협 및 대응방안, 솔루션 운영기법 등 안정적인 네트워크 운영을 위한 실무 적용기법 학습
- 훈련대상 요건 : 정보보호 직무 분야 재직자 및 보안 담당자, 네트워크 장비 운영자 등

교과목	교육내용
네트워크 보안원리	• 보안의 3요소 • 계층별 프로토콜 보안
네트워크 정보수집 및 공격기법	• 계층별 정보 수집 방법론 • 네트워크 파괴
라우터, 스위치, 무선랜 보안강화	• 인프라 장비 보안 • 무선랜 인증 과 암호화 보안
방화벽, 주소변환기술	• 접근제어목록을 이용한 패킷필터 • 신뢰성 기반 정책 방화벽
가상사설망 (VPN) 연결	• 암호학 서비스 • IPSec 과 TLS VPN 연결
네트워크 침입방지 구현	• 침입 탐지 엔진 기술 • 시그니처 스트링 튜닝
네트워크 접근제어	• NAC 장비 연결과 인증 구현 • NAC 사용자 접속 방식
웹 어플리케이션 방화벽	• WAF 모듈 기술 • 웹 서버 연동과 웹 보안 로그 감사

교육 과정 : K-Shield Advanced(중급)
훈련 방법 : 집체훈련
훈련 일수 : 4일
훈련 시간 : 24시간
훈련 인원 : 회당 18명
대규모기업 교육비 : 93,080원

5 K-Shield 포렌식을 활용한 기업보안 사고 대응

- 주 요 내 용 : 디지털 디바이스를 매개체로 하여 발생된 특정 행위의 사실 관계를 규명하고, 법정에서 증거자료로 사용될 수 있도록 요건을 갖추어 증거물을 수집, 이동, 복제, 분석, 제출, 검증하는 능력을 함양
- 훈련대상 요건 : 정보보호 직무 분야 재직자 및 보안 담당자, 침해사고 분석업무 관련 실무자 등

교과목	교육내용
디지털 포렌식 개론	• 디지털포렌식 개념, 디지털포렌식 기초 실무 (도구 및 사용법)
현장 분석 이론 및 실습	• 메모리 포렌식 분석 • 현장분석 방법론, 증거획득 실습
윈도우 시스템의 이해	• 운영체제 이론 • 파일 시스템 이론
윈도우 아티팩츠	• 시스템파일 이론 • 로그파일 이론 • 레지스트리 이론
포렌식을 통한 보안대응 실습	• 시스템 정보 확인 • 애플리케이션 설치 이력 분석, 실행프로그램 설치 이력 분석 • 비인가 웹 접속 이력 분석 • 파일 분석 및 복구, 파일 메타데이터 분석 • 개인정보파일 분석
포렌식을 통한 유출사고 대응 실습	• 웹 히스토리 분석, 웹 검색 프로파일링 분석 • 클라우드 유출 분석, 파일 시그니처 분석 • 무선랜/외장형 저장장치 분석 • 사용자 계정 분석, 파일 사용이력 분석 • 삭제 행위 분석, 안티포렌식 행위 분석 • 실전 분석 및 보고서 제출 실습

교육 과정 : K-Shield Advanced(중급)
훈련 방법 : 집체훈련
훈련 일수 : 3일
훈련 시간 : 21시간
훈련 인원 : 회당 20명
대규모기업 교육비 : 72,080원

6 K-Shield 웹 공격 및 대응 기법

K-Shield 인증 과정 아님

- 주 요 내 용 : 웹 브라우저에 대한 지식을 갖고 정의된 보안요구사항에 따라 SW에 대한 보안을 구현, 테스트하는 능력을 함양
- 훈련대상 요건 : 정보보호 직무 분야 재직자 및 보안 담당자, 웹 브라우저 개발자 등

교과목	교육내용
웹 공격 및 대응 기법	• 최근 해킹사고 사례에 대한 이해 • HTTP 프로토콜의 구조와 특징 • 주요 인코딩 기법 이해 및 활용 • 주요 취약점 DB 및 시큐어코딩 가이드 • 웹 서비스 관련 보안 • 실습 환경 구성 • 주요 취약점 (SQL Injection) • 주요 취약점 (Command Injection) • 주요 취약점 (XSS, Cross-site Script) • 주요 취약점 (CSRF, Cross-site Request Forgery) • 주요 취약점 (파일 업로드, 파일 다운로드) • 주요 취약점 (민감한 데이터 노출) • 주요 취약점 (XXE, XML External Entity) • 주요 취약점 (안전하지 않은 역직렬화)

교육 과정 : K-Shield Advanced(중급)
훈련 방법 : 집체훈련
훈련 일수 : 3일
훈련 시간 : 21시간
훈련 인원 : 회당 18명
대규모기업 교육비 : 71,600원

7 K-Shield 제어시스템 보안

K-Shield 인증 과정 아님

- 주 요 내 용 : 제어시스템의 구성요소, 사고사례 및 취약점 현황, 국내외 보안 추진 현황 및 기술, 표준동향 등 제어시스템 보안 실무지식 함양 및 보안인식 제고
- 훈련대상 요건 : 정보보호 직무 분야 재직자, 기반시설 보안 담당자, 정보보호 컨설턴트 등

교과목	교육내용
제어시스템의 이해 및 보안 동향	• 사이버보안 및 제어시스템 보안 현황 분석 • 제어시스템 개념 및 구성요소 • 제어시스템 현황, 특성 및 주요기능 • 제어시스템과 일반IT시스템 비교분석
제어시스템 사고사례 및 취약점 현황	• 제어시스템 사고사례 분석 • 제어시스템 취약점 현황 및 모의해킹 결과 분석
제어시스템 공격 시나리오 분석	• 제어시스템 보안 이슈 및 침투 가능 시나리오 • 제어시스템 보안 가이드라인
국내·외 제어시스템 보안 추진현황 및 기술	• 국내·외 제어시스템 보안 정책 및 기술 • 테스트베드 구축 및 취약점 분석 현황
원자력발전 및 스마트그리드 분야 보안 추진현황	• 원자력발전 및 스마트그리드 분야 보안 추진현황 분석
제어시스템 보안 평가	• 제어시스템 취약성 분석 및 모의해킹 기술 • 제어시스템 프로토콜 대상 취약점 분석 시연 및 실습
제어시스템 보안 표준	• 제어시스템 보안 표준 동향 및 세부 내용
제어시스템 보안 시험 평가	• 제어시스템 보안 시험 평가 기술 및 추진현황

교육 과정 : K-Shield Advanced(중급)
훈련 방법 : 집체훈련
훈련 일수 : 3일
훈련 시간 : 18시간
훈련 인원 : 회당 20명
대규모기업 교육비 : 67,060원

8 K-Shield 데브옵스 환경의 컨테이너 보안

K-Shield 인증 과정 아님

- 주 요 내 용 : 기업에서 사용하는 오픈소스 Docker와 Kubernetes의 보안설정 실습을 통해 안전한 컨테이너 환경을 유지하기 위한 실무 기술 학습
- 훈련대상 요건 : 정보보호 직무 분야 재직자 및 보안 담당자, SW개발자, SW아키텍쳐 등

교과목	교육내용
컨테이너 가상 환경 이해	• 최근 침해사고 사례에 대한 이해 • DevOps에 대한 이해 • 컨테이너에 대한 이해 • 실습을 위한 기본 환경 구성 • Docker 기본 사용법 실습
Docker 이해 및 취약점 점검	• Docker 취약점 점검 및 대응 • Docker 이미지 취약점 점검 및 대응 • Docker Swarm에 대한 이해 • Docker Swarm 취약점 점검 및 대응
Kubernetes 이해 및 취약점 점검	• Kubernetes 설치 및 활용 • Master Node 취약점 점검 및 대응 • Worker Node 취약점 점검 및 대응
참고자료	• Kubernetes 모니터링 시스템과 아키텍처 • 애플리케이션 로그 관리 • 큐브 대시보드 설치와 사용 • 취약점 진단 도구

교육 과정 : K-Shield Advanced(중급)
훈련 방법 : 집체훈련
훈련 일수 : 3일
훈련 시간 : 21시간
훈련 인원 : 회당 18명
대규모기업 교육비 : 71,600원

9 K-Shield IT/OT 프로토콜 취약점 분석 및 증거수집 기법

K-Shield 인증 과정 아님

- 주 요 내 용 : 정보통신기술과 산업운영시스템 융합 과정에서 발생하는 보안문제에 대하여 취약점 분석을 통한 증거자료 취합 능력 함양
- 훈련대상 요건 : 정보보호 직무 분야 재직자 및 보안 담당자, 스마트 제조·에너지·의료 산업계 IT/OT 기술 담당자 및 운영 보안 관리자 등

교과목	교육내용
계층별 IT 프로토콜	• OSI 7 참조 모델 과 IT 프로토콜 표준 기관 • 2계층 프레임 / 3계층 패킷 헤더 분석 • 4계층 세그먼트 / 7계층 메시지 헤더 분석
IT 프로토콜 취약점 분석과 증거수집 분석기법	• 증거 수집과 프로토콜 분석방법론 • BPF 캡처 필터 문법과 Wireshark 디스플레이 필터 문법 • Ethernet, WiFi, IPv4/IPv6, TCP/UDP, Application 취약점 분석
산업별 OT 프로토콜	• 스마트 제조/공장 프로토콜 특징 • 스마트 그리드/에너지 프로토콜 특징 • 스마트 의료/헬스케어 프로토콜 특징 • 스마트 홈/가전/IoT 프로토콜 특징 • 스마트 자동차/선박/드론 프로토콜 특징
OT 프로토콜 취약점 분석과 증거수집 분석기법	• OT 프로토콜에 캡처 필터 와 디스플레이 필터 적용 방법 • 산업별 FieldBus, EtherNet/IndustrialProtocol 프로토콜 취약점 분석 • Serial, RF, CPwE 통신 증거수집 분석방법론

교육 과정 : K-Shield Advanced(중급)
훈련 방법 : 집체훈련
훈련 일수 : 4일
훈련 시간 : 28시간
훈련 인원 : 회당 18명
대규모기업 교육비 : 95,730원

10 K-Shield 침해사고 기반환경 구성과 보안 점검

- 주 요 내 용 : 보안사고 발생 시 정보수집/분석/복구/대응을 위한 선제환경 실습
- 훈련대상 요건 : 정보보호 직무 분야 재직자 및 보안 담당자, 침해사고 분석 및 대응 관련 실무자 등

교과목	교육내용
가상 환경 구축 1	• VM, Docker, Sandbox 이해 • 운영체제에 따른 실험 환경 구축 소프트웨어 • 모의 환경 네트워크 아키텍처 구축
가상 환경 구축 2	• MS Windows, Linux, MacOS 가상화 • 라우터, 스위치, 무선망, 방화벽 가상화 • 애플리케이션과 서버 가상화
침해사고 대응 보고서 작성	• 공격 벡터 설정과 우회 방법 설계 • 시스템 및 장치 평가 전략 • 침해사고 보고서 작성

교육 과정 : K-Shield Advanced(중급)
훈련 방법 : 집체훈련
훈련 일수 : 3일
훈련 시간 : 18시간
훈련 인원 : 회당 18명
대규모기업 교육비 : 66,430원

11 K-Shield 산업 무선 시스템 해킹과 보안

K-Shield 인증 과정 아님

- **교육 과정 :** K-Shield Advanced(중급)
- **훈련 방법 :** 집체훈련
- **훈련 일수 :** 2일
- **훈련 시간 :** 14시간
- **훈련 인원 :** 회당 20명
- **대규모기업 교육비 :** 54,360원

- 주 요 내 용 : 산업계 표준 WiFi, Bluetooth, ZigBee, IrDA, RFID 등 무선 시스템 해킹과 방어 실습
- 훈련대상 요건 : 정보보호 직무 분야 재직자 및 보안 담당자, 산업계 IT/OT 기술 담당자 및 운영 보안 관리자 등

교과목	교육내용
무선 프로토콜 이해	• 802.11 Wi-Fi 프로토콜 구현 • 802.15 Bluetooth, ZigBee 프로토콜 구현 • RF/광파 통신 프로토콜 구현
무선 프로토콜 공격과 방어	• 무선 LAN 프로토콜 취약점 공격과 방어 • 무선 PAN 프로토콜 취약점 공격과 방어 • 드론 통신 프로토콜 보안

12 K-Shield KT Cloud 및 Naver Cloud 매니지드 보안 서비스 활용 (국내)

- **교육 과정 :** K-Shield Basic(초·중급)
- **훈련 방법 :** 집체훈련
- **훈련 일수 :** 2일
- **훈련 시간 :** 14시간
- **훈련 인원 :** 회당 20명
- **대규모기업 교육비 :** 46,570원

- 주 요 내 용 : 클라우드 시스템 환경에 대한 보안요소가 구축·운영이 이루어지도록 보안 요소를 구현하는 능력 향상
- 훈련대상 요건 : 정보보호 직무 분야 재직자 및 보안 담당자, 클라우드 시스템 관리자 등

교과목	교육내용
KT Cloud	• VM 구성 및 관리 • VM 별 방화벽 서비스 활용 • HTTP/HTTPS 공격 탐지 및 차단 • APT 실시간 탐지 및 검역 • 악성메일 모의훈련 • SSL VPN 서비스 연결
Naver Cloud	• SSD Server 구축 및 관리 • 서버 그룹에 대한 보안 정책 일괄 관리 • 보안 위협 대응을 위한 웹취약점 진단 • Global DNS 관리 • SSL 인증서 등록 및 관리 • 고가용성을 위한 GSLB 구성

13 K-Shield Microsoft Azure 및 Google Cloud 보안 인프라 구축(국외)

- 주 요 내 용 : 클라우드 시스템 환경에 대한 보안요소가 구축 · 운영이 이루어지도록 보안 요소를 구현하는 능력 향상
- 훈련대상 요건 : 정보보호 직무 분야 재직자 및 보안 담당자, 클라우드 시스템 관리자 등

교과목	교육내용
Microsoft Azure	• Windows 가상 머신 생성 및 관리 • VM 보안을 위한 Firewall 설정 • 데이터 보안 및 스토리지 암호화 • 네트워크 보안 액세스 제어 • Bastion 호스트 생성 • S2S VPN 연결에 대한 IPsec/IKE 구성
Google Cloud	• VM 인스턴스 생성 및 관리 • 프로젝트 및 계정 생성 • GCE VM 보안 관리 • 방화벽 정책 및 규칙 생성 • GCP 네트워크 피어링 연결 • VPC 격리된 네트워크 구축

교육 과정 : K-Shield Basic(초·중급)
훈련 방법 : 집체훈련
훈련 일수 : 2일
훈련 시간 : 14시간
훈련 인원 : 회당 20명
대규모기업 교육비 : 46,570원

14 K-Shield 그레이 박스 테스팅을 통한 웹 모의해킹

- 주 요 내 용 : 웹 브라우저에 대한 지식 및 그레이 박스 테스팅을 통해 정의된 보안요구 사항에 따라 SW에 대한 보안을 구현, 테스트하는 능력을 함양
- 훈련대상 요건 : 정보보호 직무 분야 재직자 및 보안 담당자, 웹 브라우저 개발자 등

교과목	교육내용
그레이 박스 테스팅을 통한 웹 모의해킹	• 실습 환경 이해 및 구축 • OWASP 10 취약점 설명, 공격 및 대응 • 소스코드 트레이싱 방법 / 설명 • 그레이 박스 테스팅을 통해 OWASP 10 취약점 실습 • 동일 포인트 발생 취약점 식별, 공격 및 대응

교육 과정 : K-Shield Pro(고급)
훈련 방법 : 집체훈련
훈련 일수 : 2일
훈련 시간 : 14시간
훈련 인원 : 회당 18명
대규모기업 교육비 : 42,500원

15 K-Shield 제어시스템 보안(심화)

K-Shield 인증 과정 아님

교육 과정 : K-Shield Pro(고급)
훈련 방법 : 집체훈련
훈련 일수 : 1일
훈련 시간 : 6시간
훈련 인원 : 회당 20명
대규모기업 교육비 : 20,750원

- 주 요 내 용 : 제어시스템의 구성요소, 사고사례 및 취약점 현황, 국내외 보안 추진 현황 및 기술, 표준동향 등 제어시스템 보안 실무지식 함양 및 보안인식 제고
- 훈련대상 요건 : 정보보호 직무 분야 재직자, 기반시설(국가/민간) 보안 담당자, 정보보호 컨설턴트 등

교과목	교육내용
제어시스템 보안	• 제어시스템의 이해 및 보안 동향 – 제어시스템 현황, 특성 및 주요기능 – 제어시스템과 일반IT시스템 비교분석 • 제어시스템 사고사례 및 취약점 분석 • 제어시스템 보안 표준 • 제어시스템 보안 정책, 기술 및 시험 · 인증

16 K-Shield 사이버전 실전 훈련

교육 과정 : K-Shield Pro+(최고급)
훈련 방법 : 집체훈련
훈련 일수 : 5일
훈련 시간 : 30시간
훈련 인원 : 회당 18명
대규모기업 교육비 : 81,400원

- 주 요 내 용 : APT 공격 및 침해사고 분석 심화 훈련을 통한 고급 수준의 실전형 사이버전 훈련 전문가 양성
- 훈련대상 요건 : 정보보호 직무 분야 재직자

교과목	교육내용
APT 공격과 침해사고대응 이해 / 침해사고대응 – Windows 시스템	• APT 공격과 침해사고대응 이해 • 침해사고대응 – Windows 시스템 • Windows Artifacts 분석
침해사고대응 – Windows 시스템 / Linux 시스템 **실습을 통한 APT 공격 절차 이해**	• 침해사고대응 – Windows 시스템 • 실습을 통한 APT 공격 절차 이해
실습을 통한 APT 공격 절차 이해	• Escalate Privileges 단계 개념 및 기술 요소 • Interal Reconnaissance 단계 개념 및 기술 요소 • Move Laterally 단계 개념 및 기술 요소
APT 기술 요소 실습 및 아티팩트 분석	• APT 기술 요소 실습 및 아티팩트 분석 실습
시나리오를 통한 공격 절차 및 기술 요소 분석	• Artifacts 및 로그를 분석하여 APT 공격 절차와 기술요소 분석 실습

17 K-Shield 모의해킹 실습훈련 전문가과정

- 주 요 내 용 : 정보시스템 보안성을 향상시키기 위하여 침투 테스트 대상시스템의 보안 취약점을 분석하여 공격을 수행할 수 있는 능력을 함양
- 훈련대상 요건 : 정보보호 직무 분야 재직자

교과목	교육내용
모의해킹 수행 I (NCS) – 웹해킹 –	• 모의해킹 기본지식 이해 • WEB / HTTP 프로토콜 이해 • 지원 언어에 대한 이해 • 인코딩에 대한 이해 • 웹해킹시 사용되는 도구 • 실습환경 구성 연습 • 웹해킹 공격에 대한 기본 이해
모의해킹 수행 I (NCS) – 취약점 및 대응 –	• 모의해킹 대상 시스템 정보 수집 진단, 취약점 분석, 모의해킹 유형, 대응 – Cross Site Scripting – SQL Injection
모의해킹 수행 I (NCS) – 취약점 및 대응 –	• 모의해킹 대상 시스템 정보 수집 진단, 취약점 분석, 모의해킹 유형, 대응 – FileUpload, Download – FileInclusion, Command Injection
모의해킹 수행II	• 쿠키접속, URL 강제접속 등 • 어드밴스드 모의해킹 기법 훈련(Node.JS, (Un)Serialize 등)

교육 과정 : K-Shield Pro(고급)
훈련 방법 : 집체훈련
훈련 일수 : 4일
훈련 시간 : 24시간
훈련 인원 : 회당 18명
대규모기업 교육비 : 89,430원

18 K-Shield 보안 취약점 분석 화이트해커 전문가 과정

- 주 요 내 용 : 모의침투 정의 및 프로세스의 이해, 취약점과 위협의 식별, 평가 및 취약점의 심층 분석이 가능한 침투테스트를 통하여 레드팀을 구성하고, 정보보호 전략 조직의 구성 실습
- 훈련대상 요건 : 침해사고 대응, 보안 컨설팅, 레드팀 등

교과목	교육내용
모의침투 개요 / 화이트 해커의 조직 전략 수립 및 역할	• 모의침투 정의 • 모의침투 프로세스 이해 • 해커그룹 공격 프로세스, 미션, 목표 이해 및 설계 • 레드팀 전술, 전략 이해 • 모의침투 환경 구축, 레드팀 조직 구성하기 • 정보수집 프로세스 이해
Information Gathering	• Google Hacking, Whois, Recon-ng, Shodan, Social Media 등
Vulnerability Scanning	• NMAP, OpenVAS, OWASP-ZAP, Nikto, Dirb, Web Vulnerabilities 등
Buffer Overflows	• x86 아키텍처 이해 • DEP, ASLR, Canaries, SEH 이해 • Buffer Overflows 흐름 이해 • Fuzzing 및 EIP 조작 • Windows Stack Over Flow 실습
Privilege Escalation	• Password Attacks • File Transfers • Antivirus Evasion • Active Directory Attacks • Windows Privilege Escalation • Linux Privilege Escalation • Metasploit Framework

교육 과정 : K-Shield Pro(고급)
훈련 방법 : 집체훈련
훈련 일수 : 5일
훈련 시간 : 35시간
훈련 인원 : 회당 18명
대규모기업 교육비 : 153,470원

19 K-Shield 안티바이러스 엔진 개발

- 주 요 내 용 : 컴퓨터에 악영향을 끼칠 수 있는 바이러스를 식별하고 그 기능을 정지시키거나 제어하는 프로세스를 분석하고 개발하는 능력을 함양
- 훈련대상 요건 : 정보보호 직무 분야 재직자

교과목	교육내용
안티바이러스 엔진 개발	• 백신(국내 백신의 역사) • 악성코드의 역사, 악성코드의 분류 동향 심화 • 악성코드 분석 • 16 비트 악성코드의 분석 및 백신 제작 • 개발환경 구축(파이썬의 이해, 파이썬 설치, 파이썬 문법) • 백신의 구조와 원리 • 암호화(파이썬 컴파일, 파이썬 디컴파일러 등) • 동적 모듈 로딩(파일을 통한 모듈 로딩) • 백신 엔진의 구조
안티바이러스 엔진 개발 실습	• 플러그인 구조의 백신 엔진 모듈 개발 실습 • 백신 엔진 커널 개발 실습 • 압축파일 엔진 개발 • PE 엔진 분석 개발 실습 • OLE 엔진 분석 개발 실습

교육 과정 : K-Shield Pro(고급)
훈련 방법 : 집체훈련
훈련 일수 : 5일
훈련 시간 : 30시간
훈련 인원 : 회당 18명
대규모기업 교육비 : 110,290원

20 K-Shield 침투테스트 종합훈련

- 주 요 내 용 : IT 자산에 대한 취약점과 위협의 식별, 평가 및 취약점의 심층 분석이 가능한 정보보안 전문인력 양성
- 훈련대상 요건 : 침해사고 대응, 보안 컨설팅 업무종사자 등

교과목	교육내용
침투테스트 개요	• 침투테스트 프로세스 이해 • 레드팀 업무 이해 • MITRE ATT&CK , TIBER-EU 및 OST Map 이해 • 환경 셋팅 및 도구 소개 • Powershell 이해
웹 취약점 공격 실습	• 웹 공격 이해 • 시나리오 기반 웹 취약점 활용 실습 • 피싱 공격 이해 • VBA를 통한 MS OFFICE MACRO 개발
Fuzzing 및 시스템 취약점 공격 실습	• Fuzzing 및 애플리케이션 취약점 이해 • 환경구축 및 도구 실습 • Fuzzing Code 작성 • 취약점 확인 및 Exploit Code 작성 • Stack OverFlow 실습 1 • Stack OverFlow 실습 2 • 시나리오 기반 시스템 해킹 • 윈도우 애플리케이션 우회 실습
리눅스 Buffer over Flow 취약점 이해	• 도구사용 실습 • 취약한 ELF 분석 • Exploit 작성
네트워크 우회 실습	• 네트워크 간 파일전송 이해 • Port knocking 및 Pivoting 실습

교육 과정 : K-Shield Pro(고급)
훈련 방법 : 집체훈련
훈련 일수 : 5일
훈련 시간 : 35시간
훈련 인원 : 회당 18명
대규모기업 교육비 : 131,410원

21 K-Shield 위협탐지를 위한 네트워크 패킷 및 트래픽 분석

- **교육 과정 :** K-Shield Pro(고급)
- **훈련 방법 :** 집체훈련
- **훈련 일수 :** 5일
- **훈련 시간 :** 30시간
- **훈련 인원 :** 회당 18명
- **대규모기업 교육비 :** 117,970원

- 주 요 내 용 : 비정상 네트워크 세션 식별, zeek 및 ELK 등의 도구와 플랫폼을 활용한 네트워크 패킷 및 트래픽 분석, C2 및 DoS 공격 등 주요 악성 행위 식별
- 훈련대상 요건 : 침해사고 대응, 정보보호기획관리 업무 종사자 등

교과목	교육내용
네트워크 위협 이벤트 이해	• 네트워크 패킷, 트래픽, 로그를 통해 확인 가능한 주요 위협 이벤트 학습
네트워크 세션 분석 실습	• 공격 에뮬레이션을 통해 수집된 패킷 트레이스를 활용해 네트워크 세션 분석 기법 실습
zeek를 활용한 위협 탐지	• zeek를 활용하여 공격 에뮬레이션을 통해 수집된 패킷 트레이스를 분석하고 다양한 위협을 탐지
ELK를 활용한 네트워크 트래픽 분석	• ELK를 활용한 네트워 트래픽 분석 및 위협 탐지
시나리오 기반 위협 분석 종합 실습	• 패킷 및 트래픽 분석을 통한 위협 탐지 종합 실습

22 K-Shield 악성코드 문서파일 분석

- **교육 과정 :** K-Shield Pro(고급)
- **훈련 방법 :** 집체훈련
- **훈련 일수 :** 5일
- **훈련 시간 :** 30시간
- **훈련 인원 :** 회당 18명
- **대규모기업 교육비 :** 117,970원

- 주 요 내 용 : 악성코드 탐지 및 분석 심화 훈련을 통한 고급 수준의 악성코드 분석 전문가 양성
- 훈련대상 요건 : 침해사고 대응, 정보보호기획관리 업무 종사자 등

교과목	교육내용
표적공격 (Targeting Attack)	• 표적공격의 의미와 주요 사례 분석 • MITRE ATT&CK 모델 개요와 지식기반 구성요소 • TTP(Tactics, Techniques, Procedures) • MITRE ATT&CK 모델을 활용한 시나리오 예시 분석 • 고통의 피라미드(Pyramid of pain)
Fileless 공격	• Fileless 공격의 개념 • LoL(Living off the Land) and LoL Bins • Process Injection • Process Injection API Example
악성문서 분석을 위해 알아야할 필수 지식	• PE 파일의 기본 구조와 운영 개념 • 악성 첨부파일 유형과 구성 요소 • 악성 문서파일 분석 절차
악성 MS 오피스 문서 분석	• 악성 MS 오피스 문서의 이상 징후 • 매크로 유형의 악성 MS 오피스 문서 분석 • DDE 유형의 악성 MS 오피스 문서 분석 • 오브젝트 임베드 유형의 악성 MS 오피스 문서 분석 • 익스플로잇 유형의 악성 MS 오피스 문서 분석
악성 HWP 문서 분석	• 악성 HWP 문서의 이상 징후 • 포스트 스크립트 유형의 악성 HWP 문서 분석 • 익스플로잇 유형의 악성 HWP 문서 분석 • 오브젝트 유형의 악성 HWP 문서 분석 • 매크로 유형의 악성 HWP 문서 분석
악성 PDF 문서 분석	• 악성 PDF 문서의 이상징후 • 난독화된 자바스크립트 코드 분석

23 K-Shield 악성코드 쉘코드 분석

- 주 요 내 용 : 악성코드 탐지 및 분석 심화 훈련을 통한 고급 수준의 악성코드 분석 전문가 양성
- 훈련대상 요건 : 침해사고 대응, 정보보호기획관리 업무 종사자 등

교과목	교육내용
윈도우 실행파일의 내부 구조 및 동작방법 이해	• 윈도우 실행파일 생성 • 가상 주소공간 • 윈도우 실행 파일의 기본 구조
악성코드 분석을 위한 리버스 엔지니어링	• 주요 레지스트리 및 기본 명령어 • 메모리 구조 • 스크립트 기본 문법
악성코드 판별 및 기본정보 분석	• 실행파일 구조 분석을 통한 악성코드 판별 • 악성코드가 사용하는 기능 및 API
악성코드 주요기능 식별 및 분석	• 다양한 포맷, 알 수 없는 회피 기술, 쉘코드 함수
쉘코드 분석	• 동작방식 및 파일 구조 • PE파일 (임포트 매커니즘, 익스포트 매커니즘)
악성 쉘코드 분석	• jnlp파일 분석 • jar파일 분석 • 인젝션 코드추출 • 스크립트 추출

교육 과정 : K-Shield Pro(고급)
훈련 방법 : 집체훈련
훈련 일수 : 5일
훈련 시간 : 30시간
훈련 인원 : 회당 18명
대규모기업 교육비 : 117,970원

24 K-Shield 침해사고 시나리오 기반 위협상황 실전 대응 훈련

- 주 요 내 용 : 가상환경에서의 사이버 공격 및 방어 훈련 수행을 통한 침해사고 대응 전문 인력 양성
- 훈련대상 요건 : 침해사고 대응, 정보보호기획관리 업무 종사자 등

교과목	교육내용
침해사고 대응 시나리오 실습(1)	• 웹 어플리케이션 취약점, 웹쉘 및 공격도구 등을 활용한 기업 정보유출 사고 대응
침해사고 대응 시나리오 실습(2)	• 스피어 피싱 및 악성코드 공격 대응
침해사고 대응 시나리오 실습(3)	• 보안 유출사고 조사 및 대응 (익스플로잇, 네트워크 인프라스트럭처, 악성코드 분석 대응)
침해사고 대응 실전 (1)	• (실습) 침해사고에 대한 사고 발생 원인규명 분석
침해사고 대응 실전 (2)	• (실습) 침해사고에 대한 공격자의 침투행위 분석

교육 과정 : K-Shield Pro(고급)
훈련 방법 : 집체훈련
훈련 일수 : 5일
훈련 시간 : 30시간
훈련 인원 : 회당 18명
대규모기업 교육비 : 117,970원

25 K-Shield 중소기업 침해 대응 역량 강화 (with. 보호나라)

K-Shield 인증 과정 아님

- **교육 과정 :** K-Shield Basic(초·중급)
- **훈련 방법 :** 집체훈련
- **훈련 일수 :** 3일
- **훈련 시간 :** 18시간
- **훈련 인원 :** 회당 20명
- **대규모기업 교육비 :** 63,230원

• 주 요 내 용 : 중소기업 침해사고 피해예방 및 보안역량 강화
• 훈련대상 요건 : 정보보호 직무 분야 재직자

교과목	교육내용
서버 취약점 진단	• 국내 중소기업 서버취약점 현황 • KISA 서버취약점 진단도구 소개 • 취약점 진단 방법론 • CCE기반 취약점 점검 및 조치방안 • CVE기반 취약점 점검 및 조치방안 • 침해사고 흔적조사 및 조치방안
클라우드 인프라 취약점 진단	• 클라우드 소개(클라우드 장단점, 이용 현황, 취약 사례) • 클라우드 점검 방법론 • 클라우드 환경에서의 인프라 취약점 진단
침해사고사례 / 침해사고 분석·대응	• 침해사고 사고사례 • 공격도구를 이용한 침해대응 실습훈련 • 시나리오 기반의 실습 모의훈련 • 공격도구에서 나타나는 공격자 흔적 분석 • Windows Artifacts(프로세스, 레지스트리, 이벤트 로그 등) 분석을 통해 침해사고 탐지 및 대응 훈련

26 K-Shield 시큐리티 모니터링을 위한 SIEM 구축 및 활용

- **교육 과정 :** K-Shield Basic(초·중급)
- **훈련 방법 :** 집체훈련
- **훈련 일수 :** 3일
- **훈련 시간 :** 18시간
- **훈련 인원 :** 회당 20명
- **대규모기업 교육비 :** 56,190원

• 주 요 내 용 : 시큐리티 모니터링 관점에서의 정보시스템 취약점 진단 및 침해사고 분석·대응
• 훈련대상 요건 : 정보보호 직무 분야 재직자

교과목	교육내용
공격 패러다임 변화와 Splunk 워크플로우	• Splunk 소개와 최신 공격 동향 • (실습) 환경 구축 – 수강생별 실습 환경 구축, SIEM 예제 데이터 import • Splunk 기본 검색 – 데이터 나열, 통계, 차드, 비교 분석 – 다중 문자열과 시간, 검색어 작성 및 검색 효율 극대화 • 보고서와 대시보드
공격 패러다임 변화와 Splunk 워크플로우	• SIEM 이해(SIEM 구축 전략 및 방안) • 로그 수집(네트워크, 엔드포인트, 스캐너 등 로그 특성 이해하기) • 네트워크 및 엔드포인트 로그 분석
SIEM구축 실습	• SIEM 앱 설계 및 구축 • 메뉴구성 및 인사이트 • 패널 시각화 • 대시보드 강화 실습

27 K-Shield 주요 정보통신 기반시설 (리눅스) 취약점 진단 스크립트 개발

- **교육 과정 :** K-Shield Basic(초·중급)
- **훈련 방법 :** 집체훈련
- **훈련 일수 :** 3일
- **훈련 시간 :** 18시간
- **훈련 인원 :** 회당 20명
- **대규모기업 교육비 :** 63,250원

- 주 요 내 용 : 주요통신 기반시설 정보보호 실무 취약점 진단 분석을 통한 네트워크 보안 침해사고 예방 및 대응력 향상
- 훈련대상 요건 : 침해사고 대응, 정보보호기획관리 업무 종사자 등

교과목	교육내용
KISA 기반시설(리눅스) 취약점 진단 가이드 분석	• KISA 리눅스 취약점 조치 가이드 분석 • 취약점 미 조치로 발생할 수 있는 사례 연구 • 리눅스 서버 주요 취약점에 대한 자동화 진단 스크립트 개발환경 구축
리눅스 서버 취약점 진단 스크립트 개발	• 리눅스 서버 주요 취약점에 대한 자동화 진단 스크립트 개발 • 진단결과 검증 및 정/오탐 분석
진단결과 분석 및 적용 사례 연구	• 리눅스 서버 주요 취약점에 대한 자동화 진단 스크립트 개발 • 진단결과 검증 및 정/오탐 분석 • 스크립트 진단결과 분석 및 실전 적용사례 소개 • 애플리케이션 영향도에 따른 취약점 관리 방법 연구

28 K-Shield 보안제품군 훈련

- **교육 과정 :** K-Shield Basic(초·중급)
- **훈련 방법 :** 집체훈련
- **훈련 일수 :** 3일
- **훈련 시간 :** 18시간
- **훈련 인원 :** 회당 20명
- **대규모기업 교육비 :** 62,930원

- 주 요 내 용 : 보안제품군을 활용해 정보시스템의 침투 공격을 탐지하고 대응할 수 있는 능력을 함양
- 훈련대상 요건 : 정보보호 직무 분야 재직자

교과목	교육내용
CERT 구축	• 침해대응 활동계획 수립 (CERT 구축을 위한 보안장비 도입계획 등) • 정보보호 사고사례 동향 • 정보보호 제품군을 활용한 공격대응 이해 등
보안시스템 로그 분석 (방화벽)	• 보안시스템 로그분석(보안로그, 오탐유무, 패킷확인) • DoS, DDoS, Flooding 공격 실습 • 방화벽을 이용한 공격 탐지 및 대응
보안시스템 로그 분석 (정규표현식)	• 보안시스템 로그분석(보안로그, 오탐유무, 패킷확인) • 정규표현식의 이해 • 정규표현식을 활용한 패턴 매칭 실습
보안시스템 로그 분석 (웹 방화벽)	• 보안시스템 로그분석(보안로그, 오탐유무, 패킷확인) • 웹 공격의 이해 • 웹 방화벽을 이용한 공격 탐지 및 차단 실습

29 K-Shield 시큐리티 컨설턴트 트레이닝

- 주 요 내 용 : 정보자산에 대한 위협의 진단 및 제거 등 종합적인 정보보호 대책 수립이 가능한 컨설팅 전문인력 양성
- 훈련대상 요건 : 시니어(관리자급) 이상 정보보호 직무 분야 재직자

교과목	교육내용
컨설팅 기본 이해	• 인증 컨설팅 이해 • 정보보호 관리체계 구축 방안 • 정보보호 관리체계 인증(ISMS-P) 통제항목 분석 • 정보자산의 식별/자산등급 부여 (작성 실습)
기술적/물리적/개인정보 분석	• 외부자 및 물리 보안 • 인증, 접근관리, 접근통제 • 암호화, 정보시스템 도입 및 개발 보안 • 시스템 및 서비스 운영관리 • 시스템 및 서비스 보안관리 • 침해사고 대응 및 재해복구 (침해사고 대응 실습) • 개인정보 수집 및 보호조치 (개인정보 처리방침 작성 실습)
종합실습	• 제안서 작성 실습 (목차 및 중요 포인트) • (보안전략 수립) 위험평가 보고서 작성과 실제 • (보안전략 수립) 정보보호 대책 선택 • (보안전략 수립) 정보보호 실행 계획(마스터플랜) 수립

교육 과정 : K-Shield Basic(초·중급)
훈련 방법 : 집체훈련
훈련 일수 : 3일
훈련 시간 : 18시간
훈련 인원 : 회당 20명
대규모기업 교육비 : 63,250원

30 K-Shield 모바일 디지털 증거능력 활용

- 주 요 내 용 : 정보유출 사고 발생 시 종합적인 대응절차 수행이 가능한 디지털 포렌식 전문가 양성
- 훈련대상 요건 : 악성코드 분석, 침해사고 대응 업무 종사자 등

교과목	교육내용
모바일 포렌식 개요	• 절차 이해 , 안드로이드 포렌식 이해, iOS 포렌식 이해 • 안드로이드 구조, iOS 구조 이해, 모바일 포렌식 도구 이해
모바일 포렌식 실습 분석	• 메시지, 연락처, 이메일 인터넷기록 분석 • 저장데이터 분석, 와이어리스 분석
실습	• 메시지, 연락처, 이메일 인터넷기록, App 분석 – 포렌식 실습 , SQLite3 DB복구

교육 과정 : K-Shield Basic(초·중급)
훈련 방법 : 집체훈련
훈련 일수 : 3일
훈련 시간 : 18시간
훈련 인원 : 회당 20명
대규모기업 교육비 : 62,930원

31 K-Shield 사이버 위협 보안 기술 동향 및 위협탐지 프로세스 설계

- **주 요 내 용 :** 정보보호 실무 전문교육을 통한 최신 동향 정보를 공유하고, 탐지 분석 및 대응 리포트 실습을 통한 XDR활용하여 보안위협 리포트를 설계
- **훈련대상 요건 :** 정보보호 직무 분야 재직자

교과목	교육내용
사이버보안 윤리 및 보안위협 트렌드	• 4대 혁신기술과 사회변화 – AI/VR/AR/3D 프린팅/바이오 기술로 인한 사회변화 • 인공지능(AI)과 사이버보안 윤리 – 기존 윤리의 한계, 정보격차 – 데이터 윤리 – 개발자, 사용자, 공급자 윤리 • 모럴머신(Moral Machine) 실습
보안트렌드 및 이슈대응	• 사이버보안 위협기술 트렌드 – 국내외 사이버보안 이슈 • 사이버보안 위협기술 대응방법 • 보안위협 관리 및 감지, 대응을 통한 보안관리 체계 설계 실습 – 취약점 분석 및 유형자산관리 체크리스트 – 정보보호 관리체계 구성 실습

교육 과정 : K-Shield Basic(초·중급)
훈련 방법 : 집체훈련
훈련 일수 : 2일
훈련 시간 : 12시간
훈련 인원 : 회당 20명
대규모기업 교육비 : 37,990원

32 K-Shield 웹 애플리케이션 취약점 진단 분석

- **주 요 내 용 :** 웹 애플리케이션 취약점을 분석하고, 모바일 환경에서의 사이버 공격 및 방어 훈련 수행을 통한 침해사고 대응 전문인력 양성
- **훈련대상 요건 :** 정보보호 직무 분야 재직자
  – 웹 애플리케이션 취약점 분석 업무를 수행하려는 자
  – 침해사고 대응, 악성코드 분석 등의 업무를 수행하는 자 등

교과목	교육내용
웹 취약점 분석을 위한 기본 지식 이해	• 웹의 기본 구조 • 웹의 주요 취약점(OWASP Top 10)
웹 취약점 분석 환경 구축	• 실습 환경 구축 • 로컬 웹 프록시 도구 사용 법 이해
주요 취약점 분석 및 대응 I	• SQL 삽입 취약점 • 세션 가로채기 • 통신 구간 취약점
주요 취약점 분석 및 대응 II	• XSS, CSRF • 악성 파일 업로드 및 실행

교육 과정 : K-Shield Basic(초·중급)
훈련 방법 : 집체훈련
훈련 일수 : 3일
훈련 시간 : 18시간
훈련 인원 : 회당 20명
대규모기업 교육비 : 65,190원

33 K-Shield HTTP Security A to Z

- 주 요 내 용 : 웹 애플리케이션의 주요 보안약점을 이해하고 웹 보안 가이드라인에 준수하여 침해사고 대응능력을 함양
- 훈련대상 요건 : 악성코드 분석, 침해사고 대응 업무 종사자 등

교과목	교육내용
실습 환경 구성 및 HTTP 개요	• 실습 환경 구성(JDK, STS, MySQL, curl, wget, netcat) • HTTP 개요(웹 클라이언트와 웹 서버, 리소스와 URI 등)
웹 애플리케이션의 주요 보안약점 이해	• HTTP 응답분할 • 사용자 하드디스크에 저장되는 쿠키를 통한 정보 노출 • 신뢰되지 않는 URL 주소로 자동접속 연결 • 암호화되지 않은 중요 정보 • 위험한 형식 파일 업로드 • 잘못된 세션에 의한 데이터 정보 노출 • 크로스사이트 스크립트(XSS) • 크로스사이트 요청 위조(CSRF)
HTTP 보안 및 웹 보안 가이드라인	• Transport Layer Security • HTTP Strict Transport Security • Content Security Policy • contribute.json • Cookies • Cross-origin Resource Sharing • CSRF Prevention 등

교육 과정 : K-Shield Basic(초·중급)
훈련 방법 : 집체훈련
훈련 일수 : 3일
훈련 시간 : 21시간
훈련 인원 : 회당 20명
대규모기업 교육비 : 74,510원

34 K-Shield DevSecOps 환경 구축을 위한 코드 파이프라인 디자인

- 주 요 내 용 : 정의된 보안요구사항에 따라 소프트웨어(SW)의 보안 아키텍처를 수립하고 이에 따라 SW에 대한 보안을 설계하는 능력을 함양
- 훈련대상 요건 : 소프트웨어 개발 설계자 등

교과목	교육내용
SW개발 방법론	• 클라우드 네이티브 소프트웨어 개발 • DevOps 환경
SW개발보안 방법론	• Security By Desing • SW개발보안 방법론 • DevSecOps 환경
설계단계에 고려해야할 보안 요구항목	• 입력값 검증, 인증, 인가 • 중요정보 처리, 세션 관리, 에러처리, 로깅
AWS 클라우드 기반의 DevSecOps 파이프라인 구축	• IAM설정과 통합개발환경(IDE) 구축 • 코드저장소 구축(CodeCommit) • 웹애플리케이션 및 서비스 배포 환경구축(Elastic BeanStalk) • SAST/DAST 구축 • Security Hub 구축 • Code Pipeline 배포
소프트웨어 보안 강화 기법	• 정적진단(SAST) 결과 점검 및 대응 • 동적진단(DAST) 결과 검점 및 대응

교육 과정 : K-Shield Advanced(중급)
훈련 방법 : 집체훈련
훈련 일수 : 3일
훈련 시간 : 18시간
훈련 인원 : 회당 20명
대규모기업 교육비 : 68,960원

35 K-Shield 모바일 애플리케이션 취약점 분석 및 공격과 보안

- 주 요 내 용 : 모바일 기기의 의존이 높아짐에 따라 증가하는 모바일 애플리케이션 취약점을 분석하고, 모바일 환경에서의 사이버 공격 및 방어 훈련 수행을 통한 침해사고 대응 전문인력 양성
- 훈련대상 요건 : 정보보호 직무 분야 재직자
  - 모바일 애플리케이션 취약점 분석 업무를 수행하려는 자
  - 침해사고 대응, 악성코드 분석 등의 업무를 수행하는 자 등

교과목	교육내용
모바일 애플리케이션 취약점 분석 및 공격과 보안 총론	• 모바일 애플리케이션 취약점 분석 및 공격 • 모바일 애플리케이션 보안 • 실무 설명
안드로이드의 애플리케이션 취약점 분석 및 공격과 보안	• 안드로이드 구조 • APK 파일 구조 • 안드로이드 루팅 //ARM 64bit 이상 필요, 예)갤럭시 S6 중고폰
안드로이드의 애플리케이션 취약점 분석 및 공격과 보안	• 모바일 애플리케이션 취약점 항목 • 취약점 항목별로 취약한 앱 개발 후 취약점 분석 및 공격
iOS 애플리케이션 취약점 분석 및 공격과 보안	• iOS 구조 • IPA 파일 구조 • iOS 탈옥 //ARM 64bit 이상 필요, 예)iOS 6S 중고폰 • 모바일 애플리케이션 취약점 항목 • iOS 애플리케이션 취약점 분석 및 공격 • 취약한 앱 시큐어코딩

교육 과정 : K-Shield Advanced(중급)
훈련 방법 : 집체훈련
훈련 일수 : 5일
훈련 시간 : 35시간
훈련 인원 : 회당 20명
대규모기업 교육비 : 131,140원

36 K-Shield 클라우드 인프라 환경에서의 지능형 보안 위협 방어 (AWS)

- 주 요 내 용 : AWS 클라우드 시스템 환경에 대한 보안요소가 구축·운영이 이루어지도록 보안요소를 구현하는 능력 향상
- 훈련대상 요건 : 정보보호 직무 분야 재직자, 클라우드 시스템 관리자 등

교과목	교육내용
AWS 클라우드 서비스 (클라우드 인트라스트럭처 서비스 구성)	• AWS Virtual Private Cloud(VPC) • 클라우드 네트워킹 및 부하 분산 • EC2 인스턴스 및 컴퓨팅 서비스 • 네트워크 보안 액세스 제어 • 계정 및 권한 관리 • API 사용 이력에 대한 추적 및 분석 • AWS IAM 구성 실습
아마존 웹서비스(AWS 입문)	• 웹 애플리케이션 보호를 위한 웹방화벽 • DDoS 공격 방어를 위한 구성 모범 사례 • 데이터 암호화를 위한 키 관리 서비스 • 클라우드 자산에 대한 변경 이력 추적 • 주요 자원에 대한 규정 준수 확인 및 미준수 자원에 대한 대응 • AWS WAF 구성 실습
아마존 웹서비스(AWS 활용)	• 취약점 탐지를 위한 Inspector 활용 • GuardDuty 를 통한 위협 탐지 및 대응 • S3 에 저정된 개인 정보 및 민감 정보의 탐지 • 멀티 계정 환경에서의 탐지 내역 통합 관리 • 다중 계정에서의 보안 서비스 배포 및 관리 • AWS 환경에서의 침입 탐지 및 대응 실습

교육 과정 : K-Shield Advanced(중급)
훈련 방법 : 집체훈련
훈련 일수 : 3일
훈련 시간 : 18시간
훈련 인원 : 회당 18명
대규모기업 교육비 : 65,270원

37 K-Shield 클라우드 인프라 환경에서의 지능형 보안 위협 방어 (Google)

- 주 요 내 용 : Google 클라우드 시스템 환경에 대한 보안요소가 구축·운영이 이루어지도록 보안요소를 구현하는 능력 향상
- 훈련대상 요건 : 정보보호 직무 분야 재직자, 클라우드 시스템 관리자 등

교과목	교육내용
Google 클라우드 서비스 (클라우드 인트라스트럭처 서비스 구성)	• Windows 가상 머신 생성 및 관리 • VM 보안을 위한 Firewall 설정 • 데이터 보안 및 스토리지 암호화 • 네트워크 보안 액세스 제어 • Bastion 호스트 생성 • S2S VPN 연결에 대한 IPsec/IKE 구성
Google 웹서비스	• 클라우드와 아마존 웹서비스, 서버, 스토리지 네트워크 구성 • VM 인스턴스 생성 및 관리 • 프로젝트 및 계정 생성 • GCE VM 보안 관리 • 방화벽 정책 및 규칙 생성 • GCP 네트워크 피어링 연결 • VPC 격리된 네트워크 구축
Google 웹서비스 (활용 실습)	• 로드밸런싱, DB데이터 만들기, 인프라 구성하기, CDN활용, 자원 리소스 관리, DNS 연결 • VM 인스턴스 생성 및 관리 • 프로젝트 및 계정 생성 • GCE VM 보안 관리 • 방화벽 정책 및 규칙 생성 • GCP 네트워크 피어링 연결 • VPC 격리된 네트워크 구축

교육 과정 : K-Shield Advanced(중급)
훈련 방법 : 집체훈련
훈련 일수 : 3일
훈련 시간 : 18시간
훈련 인원 : 회당 18명
대규모기업 교육비 : 64,930원

38 K-Shield 클라우드 인프라 환경에서의 지능형 보안 위협 방어 (MS)

- 주 요 내 용 : MS 클라우드 시스템 환경에 대한 보안요소가 구축·운영이 이루어지도록 보안요소를 구현하는 능력 향상
- 훈련대상 요건 : 정보보호 직무 분야 재직자, 클라우드 시스템 관리자 등

교과목	교육내용
MS클라우드 서비스 (클라우드 인트라스트럭처 서비스 구성)	• Windows 가상 머신 생성 및 관리 • VM 보안을 위한 Firewall 설정 • 데이터 보안 및 스토리지 암호화 • 네트워크 보안 액세스 제어 • Bastion 호스트 생성 • S2S VPN 연결에 대한 IPsec/IKE 구성
MS웹서비스	• 클라우드와 아마존 웹서비스, 서버, 스토리지 네트워크 구성 • VM 인스턴스 생성 및 관리 • 프로젝트 및 계정 생성 • GCE VM 보안 관리 • 방화벽 정책 및 규칙 생성 • GCP 네트워크 피어링 연결 • VPC 격리된 네트워크 구축
MS웹서비스 (활용 실습)	• 로드밸런싱, DB데이터 만들기, 인프라 구성하기, CDN활용, 자원 리소스 관리, DNS 연결 • VM 인스턴스 생성 및 관리 • 프로젝트 및 계정 생성 • GCE VM 보안 관리 • 방화벽 정책 및 규칙 생성 • GCP 네트워크 피어링 연결 • VPC 격리된 네트워크 구축

교육 과정 : K-Shield Advanced(중급)
훈련 방법 : 집체훈련
훈련 일수 : 3일
훈련 시간 : 18시간
훈련 인원 : 회당 18명
대규모기업 교육비 : 58,580원

39 K-Shield IoT환경을 위한 리눅스 포렌식

- **주 요 내 용 :** IoT 환경을 위한 보안사고 분석 대응 교육을 통한 보안 침해사고 예방 및 대응력 향상
- **훈련대상 요건 :** 정보보호 직무 분야 재직자

교과목	교육내용
보안사고 분석 대응	• IoT 환경 이해 • 리눅스 및 서버 포렌식 이해 • 리눅스 환경에서의 악성코드 동작 이해 • 휘발성 데이터 수집 • 데드 분석이 정당한지 판단하기 위한 데이터 수집 • Sleuth Kit 사용법 이해 • RAM 덤프 • 메모리 이미지 분석 • 파일시스템 이미지 덤프 • 파일 시스템 이미지 분석 • 타임라인 분석(시스템 설치, 업그레이드, 부팅 등의 시기 등) • 네트워크 분석(tcpstat 사용, tcpflow로 대화 분리 등) • 파일 포렌식 • Linux 악성코드 분석(ELF 정적 분석, 맬웨어 실행) • 시나리오 기반 리눅스 서버 포렌식 실습 • 악성코드가 심어진 IoT 펌웨어 포렌식 실습

교육 과정 : K-Shield Advanced(중급)
훈련 방법 : 집체훈련
훈련 일수 : 5일
훈련 시간 : 30시간
훈련 인원 : 회당 18명
대규모기업 교육비 : 117,260원

40 K-Shield 디지털 포렌식 단위기술 분석도구 활용

- **주 요 내 용 :** 디지털 포렌식 분석을 위해 관련 지식을 습득하고, 관련 프로그램과 장비를 이해하며, 최종적으로 법정에서 사용할 수 있는 효력의 증거자료 습득능력 등을 통한 침해사고 대응 전문인력 양성
- **훈련대상 요건 :** 정보보호 직무 분야 재직자
  - 기업의 정보 감사 업무를 수행하려는 자
  - 침해사고 대응, 악성코드 분석 등의 업무를 수행하는 자 등

교과목	교육내용
디지털 포렌식 도구 개요	• Magnet AXIOM 소개 • AXIOM Process – 기본 설정 – 증거 추가 및 이미징 – 처리 세부 설정 – 아티팩트 설정
디지털 포렌식 도구 활용	• AXIOM Examine – 기본 설정 – 인터페이스 – 아티팩트, 연결, 파일시스템, 미디어, 레지스트리, 타임라인 탐색기 – 운영체제, 브라우저, 문서, 미디어, 모바일, 채팅, 클라우드 아티팩트 분석
디지털 포렌식 도구 실습	• AXIOM을 활용한 케이스 분석 – 사용자 및 시스템 정보 분석 – 사용자 행위 분석 – 타임라인 분석

교육 과정 : K-Shield Advanced(중급)
훈련 방법 : 집체훈련
훈련 일수 : 3일
훈련 시간 : 18시간
훈련 인원 : 회당 18명
대규모기업 교육비 : 70,140원

41 K-Shield 리버싱을 통한 프로그램 인증 우회 및 악성코드 구조분석

- 주 요 내 용 : 윈도우 애플리케이션 구조 분석 기법과 인증로직의 이해, 우회기법을 학습
- 훈련대상 요건 : 정보보호 직무 분야 재직자

교과목	교육내용
윈도우 애플리케이션 구조 분석기법	• 윈도우 PE 파일 구조 및 실행 로직 분석 • C코드(변수 선언, 반복문, 조건문, 연산자 등)와 어셈블리어 비교 및 변환 • ollydbg를 이용한 윈도우 프로그램 인증로직 분석 • 인증로직 분석을 통한 인증 우회/key 파일 생성/ 레지스트리 변조 실습
인증로직의 이해 및 우회기법 실습	• ollydbg를 이용한 윈도우 프로그램 인증로직 분석 • 인증로직 분석을 통한 인증 우회/key 파일 생성/ 레지스트리 변조 실습 • Anti debugging/Code unpacking and Decoding/ Data Recovery 기법 실습
악성코드 동적/정적 분석 실습	• IDA를 이용한 악성코드 정적분석(레지스트리, 네트워크, API 호출 등) 실습 • vmware 환경에서 악성코드 동적분석 및 정적분석과의 결과 비교 • 주요 악성코드(WannaCry, Sony Pictures) 정적/동적 분석

교육 과정 : K-Shield Advanced(중급)
훈련 방법 : 집체훈련
훈련 일수 : 3일
훈련 시간 : 18시간
훈련 인원 : 회당 18명
대규모기업 교육비 : 68,810원

42 K-Shield 버그바운티를 위한 Fuzzing & Exploit 개발 과정

- 주 요 내 용 : 애플리케이션에 대한 취약점을 테스트하고 식별된 취약점을 활용
- 훈련대상 요건 : 악성코드 분석, 침해사고 대응 업무 종사자 등

교과목	교육내용
취약점 개요	• 버그바운티 및 애플리케이션 취약점 이해 • 메모리 구조 이해 • 어셈블리어 이해 및 실습 • 환경구축 및 분석도구 실습 • Fuzzing 과정 이해
Fuzzing & Exploit 기초	• 파일 입출력 기반 Fuzzing Code 작성 • 네트워크 기반 Fuzzing Code 작성 • 로컬 기반 Exploit Code 작성 • 네트워크 기반 Exploit Code작성 • Fuzzing & Exploit Code 분석 • Stack 기반 Fuzzing 및 Exploit 실습
Fuzzing & Exploit 중급	• 윈도우 보호 매커니즘 이해 • SEH 우회 이해 및 실습
Fuzzing & Exploit 고급	• ROP Chain 이해 • DEP 우회 이해 • DEP 우회 실습 • ASLR 우회 이해 및 실습 • DEP + ASLR 우회 실습

교육 과정 : K-Shield Advanced(중급)
훈련 방법 : 집체훈련
훈련 일수 : 5일
훈련 시간 : 35시간
훈련 인원 : 회당 18명
대규모기업 교육비 : 126,490원

43 K-Shield 정보시스템 운영 보안 관리 실습

- 주 요 내 용 : 정보시스템을 안전하게 운영하기 위해 정의된 보안요구사항에 따라 기업정보 시스템을 안정적으로 운영할 수 있는 전문능력을 함양
- 훈련대상 요건 : 정보보호 직무 분야 재직자

교과목	교육내용
접근제어	• 정보시스템 접근 제어 정책 및 지침 • 정보시스템 접근 제어 권한 설정 및 해제 • 정보시스템 접근 제어 이력관리
시스템 운영 및 관리	• 시스템 보안솔루션 운영(시스템 보안 요구사항, 시스템 구조, 솔루션 현황 파악 및 운영) • 정보시스템 운영 관리 정책 및 지침 • 정보시스템 운영 실무(장애 관리, 성능/용량 관리, 보안 관리, 패치 관리, 백업 관리 등)
정보시스템 보안 관리	• 침해시도 모니터링(로그 및 악성코드 탐지 프로세스 활용) • 정보시스템 취약점 점검 및 악성코드 관리 절차 실무 • 정보시스템 보안성 검토 실습

교육 과정 : K-Shield Advanced(중급)
훈련 방법 : 집체훈련
훈련 일수 : 2일
훈련 시간 : 12시간
훈련 인원 : 회당 18명
대규모기업 교육비 : 44,300원

44 K-Shield 주요 취약점 공격 실습을 통한 모의 침투테스트

- 주 요 내 용 : 모의침투 정의 및 프로세스의 이해, 취약점과 위협의 식별, 평가 및 취약점의 심층 분석이 가능한 침투테스트 전문가 양성
- 훈련대상 요건 : 정보보호 직무 분야 재직자

교과목	교육내용
최근 위협 개요	• 최근 취약점 개요 및 사례 • 주요 취약점 식별을 위한 방법 이해 • 취약점 정보수집 프로세스 이해
주요 취약점 정보수집	• 네트워크 정보 수집 이해 • 시스템 취약점 정보 수집 이해 • 애플리케이션 내 취약점 정보 수집 이해
웹 취약점 이해	• 웹 주요 취약점 이해 • 웹 취약점 식별을 위한 도구 이해 • 시나리오 기반 웹 취약점활용
최근 취약점 분석	• Log4j 취약점 이해 및 실습 • Dirty Pipe 취약점 이해 및 실습 • Pwnkit 취약점 이해 및 실습 • PrintSpool 취약점 이해 및 실습 • 시나리오 기반 서버 취약점 분석 실습

교육 과정 : K-Shield Advanced(중급)
훈련 방법 : 집체훈련
훈련 일수 : 5일
훈련 시간 : 35시간
훈련 인원 : 회당 18명
대규모기업 교육비 : 130,260원

45 K-Shield 침투 시나리오를 활용한 웹, 모바일 환경 모의해킹 실습

- 주 요 내 용 : 침투 시나리오를 기반한 웹, 모바일 환경에서의 모의해킹 실습을 통해 침해사고 대응 전문인력을 양성
- 훈련대상 요건 : 정보보호 직무 분야 재직자

교과목	교육내용
웹 모의해킹 총론 / SQL Injection	• 웹, 모바일 모의해킹 총론 • 환경 구축(Burpsuite, VSCode, OracleDB, Python) • 진단 도구 사용(Burpsuite 기본 사용법, Repeater와 Intruder) • DB 개요(Query문의 이해 • SQL Injection 개요 • Out of Band Exploitation(OOB)
Python을 이용한 SQL Injection 자동화 공격 / XSS	• Python • Blind SQL Injection Python Script • XSS(Cross-site Scripting)
CSRF, SSRF / 파일 업로드, 파일 다운로드	• CSRF(Cross-site request forgery) • SSRF(Server-side request forgery) • 파일 업로드 • 파일 다운로드
Session/Cookie, 파라미터 변조, 기타 취약점	• 션/쿠키 • 파라미터 변조 • 기타 취약점
Javascript 분석과 E2E 암호화 / 웹 테마 모의해킹	• 자바스크립트 분석 • E2E 암호화 • 쇼핑몰 모의해킹 • 인터넷 뱅킹 모의해킹

교육 과정 : K-Shield Pro(고급)
훈련 방법 : 집체훈련
훈련 일수 : 5일
훈련 시간 : 35시간
훈련 인원 : 회당 18명
대규모기업 교육비 : 117,530원

46 K-Shield 침해사고 현장대응 감사 기법

- 주 요 내 용 : 디지털 디바이스를 매개체로 하여 발생된 사이버상 불법 행위의 사실 관계를 법적으로 증명하여 범죄를 포착하고, 침해사고 현장대응 감사 능력을 갖춘 전문인력 양성
- 훈련대상 요건 : 정보보호 직무 분야 재직자
  - 기업의 정보 감사 업무를 수행하려는 자
  - 침해사고 대응, 악성코드 분석 등의 업무를 수행하는 자 등

교과목	교육내용
현장대응 전략	• 디지털 포렌식 및 침해사고 최신 동향 • 현장 대응을 위한 데이터 수집방안 • 수집된 데이터를 활용한 현장 대응 전략 수립
시스템 흔적 분석	• 현장대응 사례 분석 • 데이터 상세 분석 – 프로그램 실행 • 데이터 상세 분석 – 침투 흔적
사용자 행위 분석	• 데이터 상세 분석 – 문서 열람 및 생성 흔적 분석 • 랜섬웨어 현장대응 실습(사례 기반)

교육 과정 : K-Shield Advanced(중급)
훈련 방법 : 집체훈련
훈련 일수 : 3일
훈련 시간 : 18시간
훈련 인원 : 회당 20명
대규모기업 교육비 : 65,190원

47 K-Shield 사이버 회복력, 데이터 분석

- 주 요 내 용 : 사이버 회복력에 대해 이해하고, 사이버 침해사고 위협 탐지 평가 등을 실습하여 침해사고 대응 전문가를 양성
- 훈련대상 요건 : 정보보호 직무 분야 재직자

교과목	교육내용
사이버 회복력 평가 컨설팅	• 사이버 회복력 개요 • 사이버 침해사고 위협 탐지 평가 • NIST Cyber Security Framework • MITRE Cyber Resilience Metrics • CISA Cyber Resilience Review • EU Cyber Resilience Act • 사이버 회복력 컨설팅 방법론 • 자산관리 요구사항 점검 • 시스템 및 네트워크 제어 요구사항 점검 • 형상 관리 요구사항 점검 • 취약점 관리 요구사항 점검 • 침해사고 예방 및 대응 요구사항 점검 • 서비스 연속성 요구사항 점검 • 위험 관리 요구사항 점검 • 외부 의존성 요구사항 점검 • 사이버 회복력 강화 조치 가이드 • 사이버 회복력 강화 아키텍처 • 가상 환경 기반 사이버 회복력 컨설팅 실습

교육 과정 : K-Shield Basic(초·중급)
훈련 방법 : 집체훈련
훈련 일수 : 3일
훈련 시간 : 18시간
훈련 인원 : 회당 20명
대규모기업 교육비 : 64,560원

48 K-Shield 악성코드 기초 및 리버싱 없는 기본 분석

- 주 요 내 용 : 최신 악성코드 동향 및 기법 등의 실습을 통해 침해사고 대응 전문가 역량을 강화
- 훈련대상 요건 : 침해사고 대응 , 악성코드 분석 등의 업무를 수행하는 자

교과목	교육내용
악성코드 개요 및 기법	• 악성코드 종류 및 특징 • 최신 악성코드 동향 및 기법
리버싱 없는 기본 악성코드 분석	• 의심 샘플 분석 과정 • Hex 에디터 등을 이용한 의심 기능 유추 • Sandbox 결과 검토
실습	• 의심 샘플 기본 분석

교육 과정 : K-Shield Basic(초·중급)
훈련 방법 : 집체훈련
훈련 일수 : 1일
훈련 시간 : 6시간
훈련 인원 : 회당 20명
대규모기업 교육비 : 23,650원

49 K-Shield 포렌식을 활용한 침해사고 로그분석 기법

- 주 요 내 용 : 디지털 디바이스를 매개체로 하여 발생된 침해사고 로그 분석 기법을 통해 침해사고 대응 전문가 양성
- 훈련대상 요건 : 침해사고 대응 , 악성코드 분석 등의 업무를 수행하는 자

교과목	교육내용
로그 분석 개요 및 리눅스 로그 분석	• 로그의 개념과 종류 • 로그 분석을 위환 환경 준비 • 분석을 위한 로그 수집 • 리눅스 명령어를 활용한 로그 분석 • GUI 도구를 활용한 로그 분석
윈도우 로그 분석	• 로그 분석을 위한 환경 준비 • 악성코드 실행 로그 분석 • 인터넷을 통한 침해 유입 로그 분석
윈도우/웹 로그 분석 및 사례 실습	• 윈도우 운영체제로 유입 후 거점 확보 시 발생하는 로그 분석 • 웹 서비스 환경의 구성 요소 및 구조 • 웹 로그 처리 및 분석 • 로그 분석 위주의 침해사고 사례 실습

교육 과정 : K-Shield Advanced(중급)
훈련 방법 : 집체훈련
훈련 일수 : 3일
훈련 시간 : 18시간
훈련 인원 : 회당 18명
대규모기업 교육비 : 70,140원

50 K-Shield MITRE ATT&CK 기반 위협 분석

- 주 요 내 용 : MITRE ATT&CK 프레임워크를 분석하여 기업 보안역량진단을 수행하고 결과에 따른 침해사고 대응전략을 수립
- 훈련대상 요건 : 정보보호 기획, 침해사고 대응 업무 종사자 등

교과목	교육내용
MITRE ATT&CK	• MITRE ATT&CK 프레임워크 구성 및 활용 학습 • 위협 행위자들의 핵심 TTP 학습 • 시스템 바이너리 프록시 실행, 프로세스 인젝션
핵심 TTP	• 로그의 이해 • 웹 로그와 데이터베이스 로그 분석
TTP별 주요 위협 행위 이벤트	• 이벤트 로그 이해 • 이벤트 로그 분석
데이터 모델 / 위협 행위 식별 훈련	• 위협 탐지를 위한 데이터 모델 학습 • 주요 TTP별 위협 행위 식별 훈련 (로그 및 아티팩트 분석)
TTP별 주요 위협 행위 이벤트 / 시나리오 기반 위협 분석 종합 실습	• 이벤트 로그 이해 • 이벤트 로그 분석 • 아티팩트 및 로그 분석을 통한 위협 식별 및 분석 (시나리오 기반)

교육 과정 : K-Shield Pro(고급)
훈련 방법 : 집체훈련
훈련 일수 : 5일
훈련 시간 : 30시간
훈련 인원 : 회당 18명
대규모기업 교육비 : 110,290원

51 K-Shield 악성코드 공격대응

- **교육 과정 :** K-Shield Basic(초·중급)
- **훈련 방법 :** 집체훈련
- **훈련 일수 :** 3일
- **훈련 시간 :** 18시간
- **훈련 인원 :** 회당 20명
- **대규모기업 교육비 :** 65,190원

• 주 요 내 용 : 컴퓨터에 악영향을 끼칠 수 있는 소프트웨어를 실행하지 않고 분석하거나, 통제된 상황에서 실행한 후 분석하여 판별하는 능력을 함양

• 훈련대상 요건 : 정보보호 직무 분야 재직자

교과목	교육내용
시나리오 기반 유형별 악성코드 분석	• 악성코드 개요 및 행위분석 • 침해사고 대응 절차 – 연관파일 및 유입경로 분석 – 메모리 및 파일시스템 분석 – 주요 프로세스 분석 – 주요 레지스트리 및 네트워크 분석 • 시나리오 기반 탐지 & 분석
악성코드 대응	• 네트워크 및 시스템에 대한 악성코드 영향파악 • 악성코드 분석 • 악성코드와 일반코드 구분 및 대응

52 (부산) K-Shield 정보보안 담당자를 위한 사례 중심의 컨설팅 실습

K-Shield 인증 과정 아님

- **교육 과정 :** K-Shield Start(초급)
- **훈련 방법 :** 집체훈련
- **훈련 일수 :** 1일
- **훈련 시간 :** 6시간
- **훈련 인원 :** 회당 20명
- **대규모기업 교육비 :** 23,650원

• 주 요 내 용 : 조직의 보안현황을 분석하고 보안위험을 식별하며 보안위험 평가를 통해 정보보호 대책을 수립하는 보안 컨설팅 수행 능력을 함양

• 훈련대상 요건 : 정보보호 직무 분야 재직자

※ 본 과정은 부산에서 진행됩니다.

교과목	교육내용
정보보안 컨설팅 개요	• 정보보안 컨설팅 개요
정보보안 컨설팅 : 관리 과정	• 정보보안 컨설팅 인증 준비 • 주요결함 사례 • 정보보호정책 수립 및 범위 설정 • 경영진 책임 및 조직 구성 • 위험관리 • 정보보호대책 구현 • 사후관리
정보보안 컨설팅 : 정보보호 대책	• 정보보호 정책 • 정보보호 조직 • 외부자 보안 • 정보자산 분류 • 인적, 물리적, 시스템 개발 보안 등 • 암호 통제 • 접근 통제 • 운영 보안 • 침해사고 관리 • IT 재해복구
모의 컨설팅	• 실제 사례 중심의 컨설팅 실습


CHAMP
Consortium for HRD Ability Magnified Program

한국인터넷진흥원 KISA 아카데미 찾아오시는 길

경기도 성남시 수정구 대왕판교로 815 판교제2테크노밸리 기업지원허브 5층
KISA 아카데미 교육장

대중교통

• 버스 이용 시

지선버스 55번, 66번, 101번, 231번, 310번, 315번, 357번, 370번, 382번, 누리 2번, 73-2번, 87번

광역버스 1007번, 1007-1번, 1009번, 5600번, 5700A번, 5700B번, 6900번, 3100번, 9409번

→ 판교제2테크노밸리 또는 기업지원허브 정류장 하차

• 지하철+버스 이용 시

1. 신분당선 판교역 1번 출구(북편) → 66번, 101번, 3100번 버스 탑승 → 판교 제2테크노벨리 하차
3. 신분당선 판교역 2번 출구(동편) → 370번, 310번 버스 탑승 → 판교 제2테크노벨리 하차
4. 신분당선 판교역 2번 출구(동편) → 55번, 누리2번 버스 탑승 → 기업지원허브역 하차

자가용

• 대왕판교TG 이용 시

대왕판교TG → 분당/수지 방면 좌회전 → 금토동 삼거리에서 성남시청 방향 좌회전

• 판교TG 이용 시

판교TG → 삼평동 방향 좌회전 → 대왕판교로 2.3km 이동 좌회전

• 분당 – 내곡간도시고속화도로 이용 시

분당-내곡간도시고속화도로 → 시흥사거리 우회전 → 1.2km 이동 후 우회전

• 분당 – 수서간도시고속화도로 이용 시

분당-수서간도시고속화도로 → 고속화도로 출구 → 사송교삼거리 좌회전 → 여수교차로 좌회전 → 시흥사거리 좌회전 → 기업지원허브 방면 우회전

국가인적자원개발컨소시엄
Consortium for HRD Ability Magnified Program