

최정예 정보보호 전문인력 양성

2026 교육과정 안내



KISA 아카데미
교육신청 바로가기

국가인적자원개발컨소시엄 산업맞춤형 인력양성사업이란?

CHAMP : Consortium for HRD Ability Magnified Program

국가인적자원개발컨소시엄 사업은 고용보험법 제31조제1항, 시행령 제52조 제1항6호, 제2항 및 제3항에 따라 공동훈련센터가 협약기업 사업주와 협약을 체결하고 근로자의 니즈를 파악하여 수요자 중심의 맞춤형 교육 프로그램을 제공하는 대한민국의 대표적인 직업능력 개발 훈련 사업입니다. 특히 산업맞춤형 분야는 특정 산업이나 직종에 대한 체계적인 인력양성 및 근로자 직업능력개발을 목적으로 하며, 한국인터넷진흥원은 정보보호 분야에 특화된 전문교육을 제공합니다. 현재 국내 약 200여개 기업·기관 및 단체가 산업맞춤형 인력양성훈련기관으로 지정되어 있습니다.



사업 소개

1

사업운영 체계



2

교육훈련 지원 체계

재직근로자 맞춤형 교육 훈련 제공

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

수요자 중심의 맞춤형 교육훈련 제공

- 수요조사를 통하여 정보보호 산업계의 전략적 요구를 반영한 훈련과정 개발 및 제공

비용 부담 없는 교육훈련시스템

- 협약기업이 운영기관 교육훈련에 참여할 경우 정부에서 지원하여 기업의 인력양성 부담을 최소화
- 고용보험기금을 활용한 교육비 지원 (우선지원 대상기업 100%, 대규모기업 80% 지원)

간편한 교육훈련참여 등 편리한 행정서비스 제공

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

실전 중심의 훈련 환경 제공

- 고용노동부의 지원으로 최신 실습교육 시설을 갖추고, 보안관제·침해사고대응·디지털포렌식 등 현장 수요 기반의 전문 훈련과정을 제공하여 실질적인 역량 강화 지원

3

강사모집 관리 체계

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

» 강사POOL지원대상

- 최정에 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
- 최정에 정보보호 전문인력 양성과정 자문 활동 등
- ※ 강사로 등 제반 사항은 "국가인적자원 개발 컨소시엄 운영기준"에 의함

» 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 진행하여, 상위10%의 우수 강사진에게는 감사패 수여

최정에 정보보호 전문인력 양성 교육 참여방법



교육대상

- 한국인터넷진흥원과 산업맞춤형 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, 대규모기업의 경우 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.

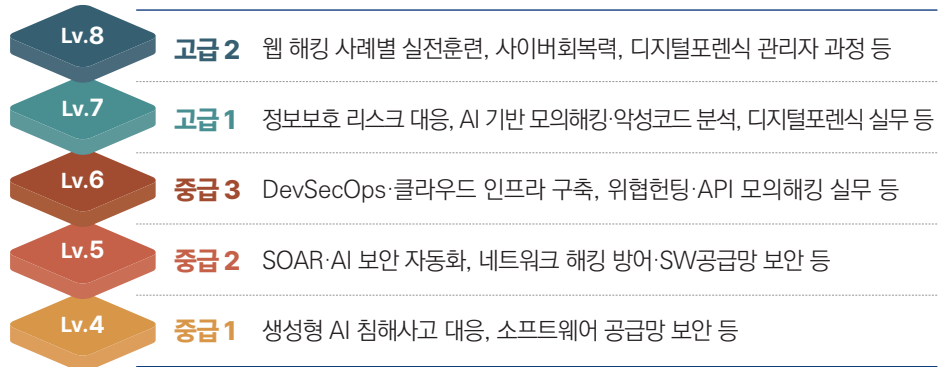
※ 소속기업의 우선지원 대상기업 해당 여부 확인: 근로복지공단(☎1588-0075) 또는 고용노동부 고객상담센터 (☎1350)



교육과정

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

K-Shield Program (중·고급 과정)



※ 위 그림은 KISA아카데미 초급(1~3)·중급(1~3)·고급(1~3) 단계 중 K-Shield 교육과정이 해당하는 등급을 표시한 것임



교육비

우선지원 대상기업

» 우선지원대상기업 재직자

- 협약 체결 시, 기업규모, 매출액, 직원 수에 따라 정기적으로 분류(고용노동부 HRD-Net 조회 기준).

» 교육비 전액 지원 (고용보험기금 적용)

- 우선지원대상기업 재직자는 교육비 납부 없음
- 전 과정 교육비 무료(기업이 직업능력개발 및 고용안정을 위하여 조성한 고용보험기금을 통하여 조달됩니다.).

» 교육비 환급절차 없음

- 협약기업의 재직자 여부 및 교육생 선발 확정
- 본 교육과정은 면세 과정으로 교육비 환급절차 없음.

대규모기업

» 대규모기업 재직자

- 협약 체결 시, 기업규모, 매출액, 직원 수에 따라
- 정기적으로 분류(고용노동부 HRD-Net 조회 기준).

» 교육비 자부담금 20% 납부

- 대규모기업 재직자의 경우, 교육비 자부담금 20% 납부 필수 (고용보험기금 80% 지원)
- 교육비는 과정별 상이하므로, KISA아카데미 누리집 교육과정 상세 안내 참조

» 교육비 환급절차 없음

- 협약기업의 재직자 여부 및 교육비 납부 확인 후 교육생 선발 확정
- 본 교육과정은 면세 과정으로 교육비 환급절차 없음

최정에 정보보호 전문인력 양성 교육수강 절차 및 인증과정

K-Shield는 최정에 사이버보안 전문가 양성 목적의 침해사고 예방·대응 기술 전문 교육과정으로 정보보호 산업계 재직자 대상 연간 교육 총 120시간 이상 및 단계별 교육과정 합산 이수 시간에 따라 모두 수료하는 경우에 한하여, 최종 인증서 평가를 거쳐 한국인터넷진흥원이 인정하는 최정에 사이버보안 전문가(K-Shield) 인증서를 발급하여 드립니다.

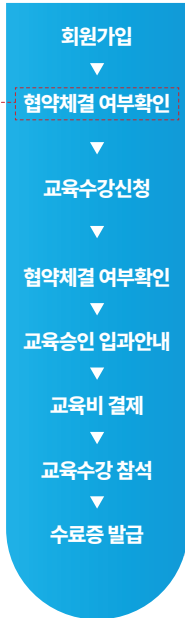


교육수강 절차

- KISA 아카데미 접속
- 양식 작성
- 첨부파일 등록
- 협약신청
- 협약승인(협약서 수신)
- 협약완료



NO



연중 상시	교육생 출결관리, 수료증 발급 등을 위하여 개별 회원가입 후 교육신청 가능
~ 2026. 9. 30	협약체결 예정 기업의 경우 협약체결이 완료된 후 교육신청 가능
상시모집	교육신청은 상시 모집 하며, 업무일 기준 교육시작 7일전 모집 마감 됩니다. • 선착순 모집으로 사전 마감 될 수 있음 • 교육접수 마감 후 신청자의 취소로 여석이 발생하는 경우에 한하여 추가모집 진행
~ 2026. 9. 30	협약체결 예정 기업의 경우 협약체결이 완료된 후 교육신청 가능
~7일	협약기업별 교육 참여횟수 및 교육과정별 참여 인원에 대한 제한 없음
~5일	교육 취소의 경우 교육수강 5일전까지 가능하며, 교육시작 후 환불은 되지 않음
당일	교육수강 전 사전이해도 조사 필수 제출
+3일	수료증 (출석 80%이상 참석) 발급은 교육 종료 3일 후, KISA 아카데미 누리집에서 출력 가능

- **협약체결 기간 : 2026. 2. 23.(월) ~ 2026. 9. 30 (수)**
※ 9월 30일(화)까지 협약체결이 완료된 기업에 한하여 2026년도에 실시하는 교육수강 신청가능
- **제출서류**
– 신청정보 입력 후, 전라분야 인력양성사업 **협약서 원본 1부** 및 **참여기업 일반현황 1부**를 작성하여 **파일 등록**
– 신규 협약기업대상 **최정에 정보보호 인력양성 교육 선호도 조사 온라인 설문 진행**
- **문의 : champ@kisa.or.kr**
※ 협약 시점은 고용노동부 HRD-Net 행정지원시스템에 협약정보가 등록된 날 부터로, KISA 아카데미 누리집 (https://academy.kisa.or.kr)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 전라분야는 타 컨소시엄 운영기관과 중복협약이 가능합니다.



인증서 발급 절차

K-Shield 2026년 전교육과정중 총 120시간 이상 수료시
최종 인증서 평가에 응시할 수 있으며, 평가 기준 점수(70점)에 따라
인증서 발급 여부가 결정됩니다.



**K-Shield
인증시험 기준**

연 120H 이상 수료 필수
 *전년도 수료했던 교육시간은 이월되지 않습니다.

FAST TRACK

K-Shield 교육은 KISA가 인증하는 교육과정 수료생을 위한 K-Shield 패스트트랙을
 운영합니다. 연 80시간 이상 수료 시 K-Shield 인증 시험에 빠르게 응시할 수 있습니다.

패스트트랙 대상 K-Shield 타 분야 인증서 보유자, K-Shield Jr.인증생, BOB 수료생, 사이버보안전문단원

Step01 ※ K-Shield 정규 교육과정 이수
교육수강

- 총 120시간 이상 이수 (K-Shield 인증서 취득분야 2과목 필수)
- 실전형 사이버훈련장(Security-Gym) 훈련과 혼합 수강 가능하며, 중·고급 과정 수강시간 (온·오프라인 모두 인정)은 최대 20시간까지 이수시간으로 인정
- 예시 : K-Shield 100h + 실전형 사이버훈련장 중·고급 과정 20h = 120h
- ※ 초급 과정은 인정 제외

Step02 ※ 시험 응시를 위한 검증
이수조건 확인

- 응시 대상 확인 (필수 이수 시간 조건 충족 여부 확인)
- 검증 요청 및 확인 (예외대상 관련 서류 제출)
- 응시 자격 부여 (최종평가 대상자 확정통보)

Step03
최종 평가 응시

- 평가 방식 : 필기시험 100%)
- 평가 시기 : 2026년 11월 중
- 합격 기준 : 70점 이상 득점 시 합격
- 기타사항 : 시험문제에 대한 사전 리뷰는 별도로 진행되지 않음

Step04
K-Shield 인증서 발급

- 한국인터넷진흥원장 명의 K-Shield 인증서 수여
- 발급시기 : 2026년 12월 중순 예정

최정에 정보보호 전문인력 양성 2026년 교육과정 소개



연번	분야	교육과정	훈련 일수	훈련 시간	훈련 인원	개설 횟수	대기업 자기부담금	훈련일정
2601	보안컨설팅	K-Shield 정보보호 입문자를 위한 보안컨설팅 시작하기	2	12	20	3	32,950	1차 4/2(목)-4/3(금) 2차 5/7(목)-5/8(금) 3차 10/1(목)-10/2(금)
2602	보안컨설팅	K-Shield 정보보호전문가에게 필요한 'SI와 정보보호'리스크 대응	2	12	20	3	32,950	1차 4/20(월)-4/21(화) 2차 6/8(월)-6/9(화) 3차 9/7(월)-9/8(화)
2603	보안컨설팅	K-Shield 정보보호 관리자를 위한 보안전략수립 및 관리 실무	2	12	20	3	32,950	1차 5/14(목)-5/15(금) 2차 8/3(월)-8/4(화) 3차 9/28(월)-9/29(화)
2604	보안컨설팅	K-Shield 팀장부터 정보보호 최고책임자(CISO)까지 알아야 할 정보보안	1	6	20	3	19,470	1차 6/5(금) 2차 7/1(수) 3차 10/13(화)
2605	침해사고대응	K-Shield 생성형 AI를 활용한 침해사고 대응 기초	3	18	20	2	46,400	1차 5/11(월)-5/13(수) 2차 6/29(월)-7/1(수)
2606	침해사고대응	K-Shield SOAR 및 AI 기반 워크플로우 엔진으로 하는 보안업무 자동화	3	21	20	2	52,850	1차 5/20(수)-5/22(금) 2차 8/5(수)-8/7(금)
2607	침해사고대응	K-Shield 오픈소스 활용 위협헌팅(보안관제)을 위한 시스템 구축 운영 실습	2	12	20	2	32,950	1차 4/9(목)-4/10(금) 2차 7/2(목)-7/3(금)
2608	침해사고대응	K-Shield 주요정보통신 기반시설 인프라 취약점 점검 툴 개발	3	18	20	2	46,430	1차 4/15(수)-4/17(금) 2차 7/14(화)-7/16(목)
2609	침해사고대응	K-Shield 정보보호 담당자가 알아야 할 암호의 기초와 블록체인 원리	2	14	20	2	42,480	1차 6/8(월)-6/9(화) 2차 8/20(목)-8/21(금)
2610	침해사고대응	K-Shield 기업 보안 관제를 위한 SIEM 구축 및 운영	3	18	20	2	46,430	1차 6/10(수)-6/12(금) 2차 7/20(월)-7/22(수)
2611	침해사고대응	K-Shield 침해사고 사례를 통해 배우는 사이버 회복력 전략 실무	2	14	20	2	38,040	1차 6/25(목)-6/26(금) 2차 10/22(목)-10/23(금)
2612	모의해킹	K-Shield HTTP Security A to Z	3	21	20	2	52,850	1차 4/15(수)-4/17(금) 2차 7/14(화)-7/16(목)
2613	모의해킹	K-Shield AI를 활용한 CTF 실습으로 배우는 시나리오 기반 웹 해킹 실무	3	21	20	2	82,620	1차 5/6(수)-5/8(금) 2차 7/29(수)-7/31(금)
2614	모의해킹	K-Shield 네트워크 해킹 기법과 방어 기술	3	21	20	2	52,850	1차 6/10(수)-6/12(금) 2차 8/12(수)-8/14(금)
2615	모의해킹	K-Shield 그레이박스 테스트와 연계한 웹 모의해킹 활용 및 API 모의해킹 활용	2	14	20	2	37,230	1차 7/27(월)-7/28(화) 2차 10/15(목)-15/16(금)
2616	모의해킹	K-Shield 모바일 애플리케이션 취약점 분석 및 공격과 보안	3	21	20	2	81,200	1차 5/20(수)-5/22(금) 2차 8/5(수)-8/7(금)
2617	모의해킹	K-Shield AI를 활용한 다양한 시스템의 Client-Server 프로그램 모의해킹	3	21	20	2	82,500	1차 6/17(수)-6/19(금) 2차 9/16(수)-9/18(금)
2618	모의해킹	K-Shield 웹 해킹 사례별 실전훈련 및 시큐어코딩 가이드	3	21	20	2	83,150	1차 4/28(화)-4/30(목) 2차 9/2(수)-9/4(금)
2619	모의해킹	K-Shield 종합 해킹 실무 훈련을 통한 침투테스트 레드팀 화이트해커 양성 과정	3	21	20	2	83,030	1차 8/19(수)-8/21(금) 2차 9/30(수)-10/2(금)
2620	악성코드분석	K-Shield 리버싱을 통한 프로그램 인증 우회 실습	2	12	20	2	32,950	1차 7/21(화)-7/22(수) 2차 9/14(월)-9/15(화)
2621	악성코드분석	K-Shield 딥러닝 모델을 이용한 스미싱 탐지 및 생성형 AI를 이용한 악성 사이트 탐지	2	12	20	3	32,950	1차 3/30(월)-3/31(화) 2차 5/14(목)-5/15(금) 3차 9/10(목)-9/11(금)
2622	악성코드분석	K-Shield RAG 기반 보안사고분석 보고서 자동화실무	3	18	20	2	46,430	1차 5/27(수)-5/29(금) 2차 10/6(화)-10/8(목)
2623	디지털포렌식	K-Shield 디지털포렌식을 활용한 보안사고 현장 대응 및 분석	3	21	20	2	70,500	1차 4/22(수)-4/24(금) 2차 8/12(수)-8/14(금)
2624	디지털포렌식	K-Shield 디지털포렌식을 활용한 기업 감사 내부진단	3	18	20	2	55,600	1차 4/6(월)-4/8(금) 2차 8/26(수)-8/28(금)
2625	디지털포렌식	K-Shield 디지털포렌식 내부 감사 책임자 과정	2	12	20	2	34,550	1차 5/11(월)-5/12(화) 2차 9/10(목)-9/11(금)
2626	디지털포렌식	K-Shield 외부 조사 대응을 위한 디지털포렌식 관리자 과정	2	12	20	2	34,550	1차 5/28(목)-5/29(금) 2차 10/12(월)-10/13(화)
2627	클라우드보안	K-Shield 클라우드 보안요구사항 이해	1	4	20	2	9,840	1차 5/19(화) 2차 8/19(수)
2628	클라우드보안	K-Shield 퍼블릭 클라우드 보안 인프라 서비스 구축 및 운영 실무	3	21	20	2	52,850	1차 4/8(수)-4/10(금) 2차 9/28(월)-9/30(수)
2629	클라우드보안	K-Shield 하이브리드 클라우드 보안 인프라 설계 및 구축 실무	3	21	20	2	52,850	1차 4/22(수)-4/24(금) 2차 10/14(수)-10/16(금)
2630	클라우드보안	K-Shield 클라우드 환경의 계층화된 보안 강화 방안	2	12	20	2	32,950	1차 6/4(목)-6/5(금) 2차 7/30(목)-7/31(금)
2631	클라우드보안	K-Shield 클라우드 환경의 계층화된 위협 탐지 및 생성형 AI 보호	2	12	20	2	34,550	1차 7/2(목)-7/3(금) 2차 9/7(월)-9/8(화)
2632	SW공급망보안	K-Shield 소프트웨어 공급망 보안	2	12	20	2	39,050	1차 4/27(월)-4/28(화) 2차 8/27(목)-8/28(금)
2633	SW공급망보안	K-Shield 디지털 혁신을 위한 DevSecOps 의 이해 및 K8S 와 AI 추론 서비스 구축	3	18	20	2	46,400	1차 6/17(수)-6/19(금) 2차 9/2(수)-9/4(금)
2634	SW공급망보안	K-ShieldAI 시대 LangChain과 Spring 기반 시큐어코딩	3	21	20	2	52,850	1차 6/24(수)-6/26(금) 2차 9/16(수)-9/18(금)
2635	SW공급망보안	K-Shield 산업제어시스템(ICS)보안	1	7	20	2	21,600	1차 5/27(수) 2차 10/14(수)

최정에 정보보호 전문인력 양성 직무별 교육과정



A | 정보보호기획자

조직의 핵심 비즈니스 목표와 밀접하게 관련된 **보안 솔루션/장비와 정보보안 대책을 설계하고 개발**합니다. 조직의 정보보안 요구사항을 정확히 이해하고, 이를 기반으로 효과적인 보안 아키텍처와 전략을 개발하여 **사이버 위협으로부터 조직을 보호하는 역할**을 합니다. 또한 최신 보안기술과 트렌드를 연구하고 이를 조직의 보안 설계에 통합하여 지속적으로 개선합니다. 조직의 정보보안 전략을 구체적으로 실현시키며, 보안이 비즈니스 프로세스와 기술 인프라에 통합되도록 보장합니다.



B | 정보보호최고책임자

조직의 정보보안 책임자로, 정보보안 전략을 주도하고 **실행**합니다. 기술적 역량과 전략적 지식을 활용하여 **조직의 정보보안 수준을 강화하고, 자산과 개인정보를 안전하게 관리**합니다. 또한 조직의 경영진과 소통을 통해 정보보안에 대한 자원 및 지원을 확보하고 조직 내 보안문화를 확산시켜 모든 직원이 정보보안을 실천할 수 있도록 노력합니다.



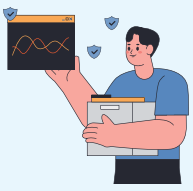
C | 정보보호연구원

정보보안 분야에서 깊이있는 연구와 분석을 수행하는 전문가로, **최신 사이버 위협, 취약점 및 방어기술에 대한 광범위한 연구를 진행**합니다. 지속적으로 변화하는 환경에 대응하기 위해 **새로운 위협, 취약점에 대한 심층적 이해를 바탕으로 혁신적인 보안 솔루션을 개발**합니다. 잠재적인 취약점을 예측하고 대비하기 위한 전략을 수립하는 역할을 하며, 연구 결과를 발표하여 정보보안 수준을 향상시키는데 기여합니다. 단순한 연구에 그치지 않고, 발견된 지식을 **실제 보안 전략과 정책에 적용**하여 조직의 사이버 방어 능력을 향상시키는데 핵심적인 역할을 합니다.



D | 정보보호엔지니어

정보보안에 필요한 **솔루션/장비를 개발**하거나 **구현**합니다. 조직의 보안요구 사항에 충족하기 위해 필요한 보안 인프라, 네트워크 구성, 시스템 관리 등을 통합적으로 수행합니다. **보안 시스템을 설계하고 구현하며, 운영에 이르기까지 모든 과정에 참여**하여 시스템 및 네트워크의 안정성을 보장합니다. 또한 시스템과 구성 요소의 유지관리, 지원을 담당하여 사이버 위협에 대응하면서도 조직의 정보 기술 인프라를 최적화합니다. **보안 기술의 선택부터 구축 및 관리까지 조직의 정보보안을 강화**하는데 중요한 역할을 합니다.



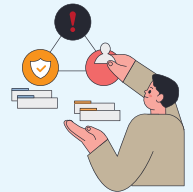
E | 보안관제 및 사고대응담당자

디지털 방어 체계를 중심으로 지속적인 모니터링과 데이터 분석을 통해 **잠재적인 사이버 위협을 조기에 발견**하고 분석합니다. 수집된 정보를 활용하여 사이버 공격에 신속하고 효과적으로 대응하며, 잠재적인 위협을 최소화합니다. 또한 **보안시스템을 안정적으로 운영**하여 변화하는 사이버 위협에 대비하고, 조직의 디지털 자산과 인프라를 보호합니다. 단순한 기술적 관리를 넘어, 조직의 정보보안 준비와 **전체 보안 생태계를 유지**하는 데 중요한 역할을 합니다.



F | 침해사고분석가

정보보안을 강화하기 위해 다양한 소스로부터 사이버위협 및 침해사고와 관련된 정보를 수집·분석·평가 합니다. 체계적인 정보 수집 및 분석 절차를 구축하고 실행하여 조직이 사이버 위협에 대응하기 위한 정보를 제공합니다. 또한 수집된 정보를 기반으로 조직의 보안 상태를 평가하고, 보안 취약점을 식별하기 위한 지표를 개발하고 관리합니다. 개발된 지표는 조직이 현재의 보안 상태를 정확하게 이해하고 잠재적인 위협에 대비하기 위한 전략을 수립하는데 중요한 역할을 합니다. 조직의 정보보안을 전략적으로 강화하고, 지속적인 위협 모니터링 및 분석을 통해 정보보안 위협을 최소화하는 핵심 역할을 수행합니다.



G | 취약점분석가

조직의 보안 체계를 테스트하여 시스템과 네트워크에 대한 취약점을 찾아내고 평가합니다. 공격자의 관점에서 조직을 공격하는 시뮬레이션을 수행하여 조직의 보안 대비 능력을 평가하며, 발견된 취약점에 대한 구체적인 개선 방안을 제공하여 조직의 보안 체계를 강화하는 데 중요한 역할을 합니다. 기술적 전문성을 기반으로 조직의 정보보안 능력을 향상시키며, 지속적인 보안 개선과 위험 관리에 핵심적인 역할을 수행합니다. 이들은 조직이 **사이버 위협에 효과적으로 대응**하고 필요한 보안 전략과 정책을 수립하는 데 중요한 인사이트를 제공합니다.



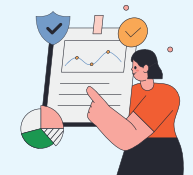
H | 디지털포렌식전문가

사이버 범죄사건과 관련된 디지털 증거를 전문적으로 처리합니다. 사건 발생 시, 중요한 디지털 증거를 식별·수집·분석하여 사건의 원인과 경로를 명확히 밝히는 데 중점을 둡니다. 수집된 증거를 철저히 검토하고 보존하여, 사이버 범죄 조사 및 법적 절차에 필요한 핵심 정보를 제공합니다. 또한 사이버 범죄와 관련된 복잡한 사건을 해결할 뿐 아니라, 기술적 전문성과 법적 지식을 결합하고 분석 결과를 활용하여 재발방지 권고안을 개발하는 등 조직의 정보보안을 강화하는데 필요한 통찰력을 제공합니다.



I | 정보보호컨설턴트

조직의 정보보안 위협을 전문적으로 **실행·평가·관리 및 완화**합니다. 효과적인 위험 관리 프로세스를 개발·실행하고 유지하며, 조직의 정보보안 위협을 조직적으로 관리하고, 위협에 대한 통찰력을 제공하여 조직이 **보안 관련 결정을 내릴 수 있도록 지원**합니다. 고객 및 조직의 요구사항을 면밀히 평가하고, 적절한 기술 솔루션과 정책을 제안합니다. 다양한 이해관계자와 긴밀히 협력하며, 위험 관리에 대한 커뮤니케이션과 교육을 제공하여 조직의 전반적인 정보보안 인식을 향상시킵니다. 조직의 보안 위협을 최소화하고, 지속 가능한 보안 전략과 정책을 수립하는 데 중요한 역할을 수행하며, 조직이 사이버 위협에 효과적으로 대응할 수 있도록 지원합니다.



최정에 정보보호 전문인력 양성 2026 훈련과정 로드맵



교육과정별 상호보완 연계

로드맵 사이버 보안 직무분류 + NCS NCS 직능 분류 수준

능력 단위별 체계적 개발

전문 분야별 전문 교육

심화 분야별 심화 교육

인증 인증취득 과정

	NCS	중급 - I	중급 - II	중급 - III	고급 - I	고급 - II	고급 - III	Special
보안컨설팅	8		K-Shield 정보보호 임문자를 위한 보안컨설팅 시작하기 A-B-C-D-E-F-G-H-I		K-Shield 정보보호 관리를 위한 보안전략수립 및 관리 실무 A-B-C-D-E-I	K-Shield 정보보호 책임자가 알아야 할 정보보안 A-B-D-I		K-Shield 인증서 취득과정 (보안컨설팅 분야)
	7				K-Shield 정보보호전문가에게 필요한 'SI와 정보보호' 리스크 대응 A-B-C-D-E-I			
침해사고대응	8	K-Shield 생성형 AI를 활용한 침해사고 대응 기초 E-F-G-H-I			K-Shield 기업 보안 관제를 위한 SIEM 구축 및 운영 C-D-E-F-I			
	7					K-Shield 침해사고 사례를 통해 배우는 사이버 회복력 전략 실무 A-B-D-F-G-I		
	6		K-Shield SOAR 및 AI 기반 워크플로우 편입으로 하는 보안업무 자동화 A-B-E-F K-Shield 오픈소스 활용 위협 헌팅(보안관제)을 위한 시스템 구축 운영 실습 A-B-C-D-E-F-G-I	K-Shield 주요정보통신 기밀시설 인프라 취약점 점검 툴 개발 A-B-C-D-E-F-G-I				K-Shield 인증서 취득과정 (침해사고대응 분야)
	5				K-Shield 정보보호 담당자가 알아야 할 암호의 기초와 블록체인 원리 A-C-D-E-F			
모의해킹	7					K-Shield 웹 해킹 사례별 실전 훈련 및 시큐어코딩 가이드 A-B-C-D-E-F-G-I K-Shield 종합 해킹 실무 훈련을 통한 침투테스트 레드팀 화이트해커 양성 과정 A-B-C-D-E-F-G-I		K-Shield 인증서 취득과정 (모의해킹 분야)
	5	K-Shield HTTP Security A to Z A-B-C-D-E-F-G-I	K-Shield AI를 활용한 CTF 실습으로 배우는 시나리오 기반 웹 해킹 실무 D-E-G-I K-Shield 네트워크 해킹 기법과 방어 기술 A-B-C-D-E-F-G-H-I	K-Shield 그레이박스 테스트와 연계한 웹 모의해킹 활용 및 API 모의해킹 활용 A-C-E-F-G-I	K-Shield 모바일 애플리케이션 취약점 분석 및 공격과 보안 A-B-C-D-E-F-G-I K-Shield AI를 활용한 다양한 시스템의 Client-Server 프로그램 모의해킹 A-B-C-D-E-F-G-I			
악성코드분석	5		K-Shield 리버싱을 통한 프로그램 인증 우회 실습 D-E-F-G-H		K-Shield 디러닝 모델을 이용한 스미싱 탐지 및 생성형 AI를 이용한 악성 사이트 탐지 A-C-D-F K-Shield RAG 기반 보안사고 분석 보고서 자동화 실무 C-E-F			K-Shield 인증서 취득과정 (악성코드분석 분야)
디지털포렌식	6				K-Shield 디지털포렌식을 활용한 보안사고 현장 대응 및 분석 F-H K-Shield 디지털포렌식을 활용한 기업 감사 내부진단 E-F-H	K-Shield 디지털포렌식 내부 감사 책임자 과정 F-H K-Shield 외부 조사 대응을 위한 디지털포렌식 관리자 과정 F-H		K-Shield 인증서 취득과정 (디지털포렌식 분야)
클라우드보안	7	K-Shield 클라우드 보안요구사항 이해 A-C-D-E-I						
	5			K-Shield 퍼블릭 클라우드 보안 인프라 서비스 구축 및 운영 실무 A-C-D-I K-Shield 하이브리드 클라우드 보안 인프라 설계 및 구축 실무 A-C-D-I	K-Shield 클라우드 환경의 계층화된 보안 강화 방안 A-C-D-E-F-G-I	K-Shield 클라우드 환경의 계층화된 위협 탐지 및 생성형 AI 보호 A-C-D-E-F-G-I		K-Shield 인증서 취득과정 (클라우드보안분야)
SW공급망보안	8		K-Shield 소프트웨어 공급망 보안 C-D-I					
	5			K-Shield 디지털 혁신을 위한 DevSecOps의 이해 및 K8S와 AI 추론 서비스 구축 A-C-D K-Shield AI 시대 LangChain과 Spring 기반 시큐어코딩 C-D-E-F-G-I	K-Shield 산업제어시스템 (ICS)보안 A-B-C-D-E-F-G-I			K-Shield 인증서 취득과정 (SW공급망보안분야)

A 정보보호 기획자

B 정보보호 최고책임자

C 정보보호 연구원

D 정보보호 엔지니어

E 보안관제 및 사고대응담당자

F 침해사고 분석가

G 취약점 분석가

H 디지털포렌식 전문가

I 정보보호 컨설턴트

미래를 연결하는 기술력과 지식으로 기업과 개인의 혁신과 성장을 이끄는 세계 최고 사이버보안 전문인력양성 기관 KISA 아카데미

찾아오시는 길

경기도 성남시 수정구 대왕판교로 815
판교제2테크노밸리
기업지원허브 정보보호클러스터 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, 기업지원허브, 서울기록관·코이카 정류장 하차

지하철+버스 이용 시

1. 신분당선 판교역 1번 출구(북편) → 101번 버스 탑승 → 판교 제2테크노밸리 하차
2. 신분당선 판교역 4번 출구(서편) → 66번 버스 탑승 → 판교 제2테크노밸리 하차
3. 신분당선 판교역 2번 출구(동편) → 370번, 310번 버스 탑승 → 판교 제2테크노밸리 하차
4. 신분당선 판교역 2번 출구(동편) → 55번, 누리2번 버스 탑승 → 기업지원허브 정류장 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

빠른 길 찾기



[주차안내]

※ 주차료를 지원하지 않으며, 기급적 대중교통 이용을 권장합니다.

※ 건물내 주차 시 최초 30분 무료 / 10분당 500원, 일 최대 20,000원