

실전형 사이버훈련장 서비스 대폭 확대된다!

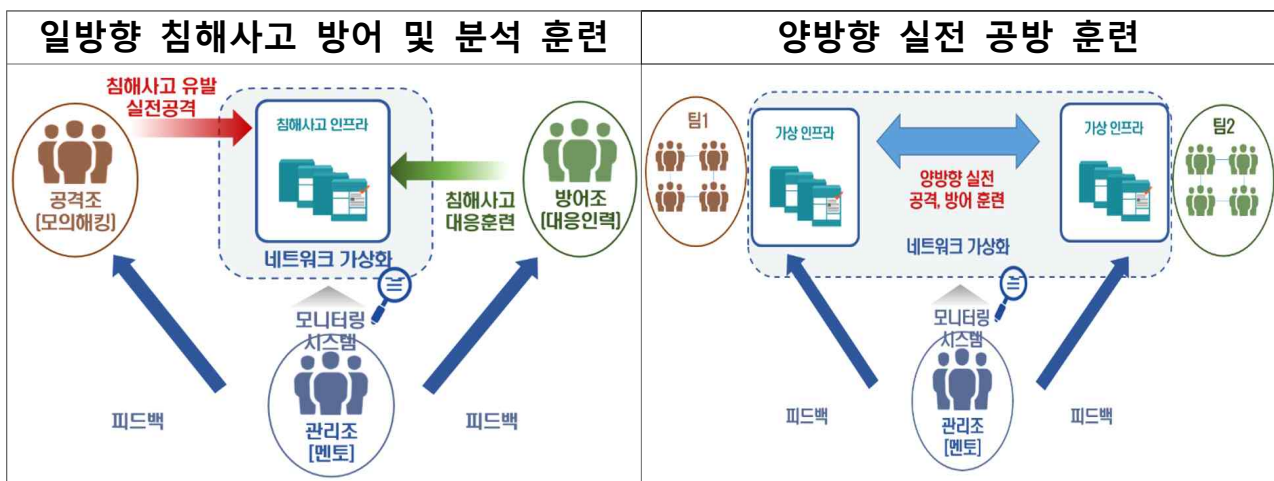
- 과기정통부, 실전형 사이버훈련장 교육생 2배 확대 지원 -
- 정보보호 지역 거점(부·울·경) 훈련장 '23년 하반기 개소 예정 -

과학기술정보통신부(장관 이종호, 이하 '과기정통부')는 한국인터넷진흥원(원장 이원태, 이하 'KISA')과 함께 판교에서 운영 중인 실전형 사이버훈련장 (Security-Gym)의 시설을 보완하여 교육과정을 추가 개설하고 교육생 수 (1,087명/'22년 → 2,820명/'23년)도 크게 확대하여 7월부터 신규 교육생을 모집한다고 밝혔다.

과기정통부와 KISA는 '사이버보안 10만 인재 양성' 목표 달성을 위해 전년도보다 2배 이상의 교육생을 수용할 수 있도록 실전형 훈련장의 교육 훈련 서버 증설(4대 → 10대), 실시간 해킹방어 훈련 등 교육과정을 확대 (7개 → 19개) 하고, 특히 다양한 정보보호 제품 실습을 위한 제품군을 추가 (2종 → 12종) 구비하였다.

본 사업은 구직자 및 재직자를 대상으로 최근 발생한 해킹 시나리오 기반으로 가상의 침해사고 환경을 구축하고, 침해사고 조사, 침해 공격·방어훈련, 상용 정보보호 제품에 대한 실습 등 수준별 교육 과정을 편성·지원한다.

< 실전형 사이버훈련장 교육 과정 사례 >



실전형 사이버 침해 대응 과정 중 ‘일방향 침해사고 방어 및 분석 훈련’은 가상의 기업 인프라 환경에 대한 침투를 방어하고, 침투 사례에 대한 취약점 정보수집·분석을 통한 대책을 수립할 수 있는 방향으로 훈련을 진행하고,

‘양방향 실전 공방 훈련 과정’은 가상의 기업환경에 접속하여 각 팀별로 할당된 인프라에 대한 방어와 동시에 상대 인프라를 공격하는 절차와 방법을 훈련하면서 실질적인 침투사고에 대응할 수 있는 능력을 배양한다.

실전형 사이버훈련장은 작년 7월 발표한 ‘사이버보안 10만 인재양성 계획’의 일환으로 확대 추진되고 있으며, 침해사고 상황에 대한 충분한 이해와 함께 실습 훈련을 할 수 있어서 구직자 및 재직자들로부터 매년 높은 교육 수요가 있다.

2016년 훈련장을 구축한 후 작년까지 4,093명의 교육생을 배출하였고, 매년 교육생 배출 목표를 초과 달성하고 있으며, 교육 훈련 기반 확충을 통한 교육생 규모 확대에 대한 요구가 계속 있어왔다.

< 실전형 사이버훈련장 연도별 교육 실적 >

구분	'16년	'17년	'18년	'19년	'20년	'21년	'22년	합계
목표	-	250명	350명	350명	750명	650명	650명	3,000명
실적	-	250명	357명	500명	1,016명	883명	1,087명	4,093명

그간의 경험과 교육 수요를 반영하고, 국제적 사이버보안 패러다임 변화를 수용하여 기존 7개 교육 과정을 총 19개 과정으로 확대 편성하여, 날로 지능화·다양화되는 사이버보안 위협에 체계적으로 대응할 수 있는 실전형 사이버 침해 대응 인재를 집중 양성할 계획이다.

< 교육과정 확대 현황 >

구분		22년	23년
훈련 과정 수	초급	-	5개 과정
	중급	5개 과정	9개 과정
	고급	2개 과정	5개 과정
합 계		총 7개 과정	총 19개 과정

또한, 지역별 특화된 사이버보안 인재 양성을 및 지역 산업 육성을 위한 핵심 거점으로 활용하여 수도권과 지역의 정보보호 수준 격차를 줄이기 위해 정보보호 지역 거점(부산·울산·경남)을 올해 신규 지정하였다.

부산 센텀시티 지역에 위치한 동남권 지역 거점 센터에는 교육훈련장, 기업 지원시설 등을 구축하고 있으며, 지역 거점 센터 내 사이버훈련장은 판교 센터의 교육 인프라를 공유하도록 하여 규모의 경제를 실현하고, 올 해 10월 부터 지역 거점에서도 실전형 교육을 시작할 수 있도록 노력하고 있다.

이를 통해 수도권에만 한정되어 있던 사이버보안 실전훈련 기반을 동남권까지 넓히는 한편, 지역 산업계에서 필요로 하는 역량 있는 사이버보안 인재를 지역에서 양성할 수 있게 되었고, 장기적으로는 스마트시티·공장·항만·조선 등 동남권 지역 특화산업에 최적화된 사이버 침해 대응인력을 양성해갈 계획이다.

과기정통부 정창립 정보보호네트워크정책관은 “공공과 민간을 가리지 않고 발생하는 사이버위협에 적시 대응 할 수 있는 실전형 사이버 침해 대응 전문인력의 양성이 매우 중요하다.”고 강조하면서,

“날로 지능화·고도화되는 사이버공격에 대한 대응 역량을 강화할 수 있도록 실전형 훈련과정의 확대와 함께 위협이벤트 식별훈련, 침해사고 조사 훈련 등 특화 훈련과정을 지속적으로 확대해나가겠다.” 고 말했다.

- 붙임 1. 23년도 7월 실전형 사이버 훈련과정 세부운영 계획 1부.
2. 실전형 사이버훈련장 훈련과정 개요 1부.
3. 23년도 훈련과정 세부운영 계획 1부. 끝.

담당 부서	정보보호산업과	책임자	과 장	정은수 (044-202-6450)
		담당자	사무관	김성환 (044-202-6451)
			사무관	박세진 (044-202-6455)
담당 부서	한국인터넷진흥원 보안인재정책팀	책임자	팀 장	이동화 (061-820-1102)
		담당자	선 임	김광복 (061-820-1321)

□ '23년 7월 훈련과정 세부 일정

○ (신청방법) KISA 아카데미(academy.kisa.or.kr) 홈페이지 신청

※ 각 차수별 훈련생은 선착순 신청으로 접수

구분	과정명	운영 방법	접수기간	훈련기간	정원
초급	MITRE ATT&CK 활용	온라인	6.26 ~ 7.17	7.26 ~ 8.01	50명
	정보보호제품군-기초1		6.19 ~ 6.30	7.05 ~ 7.11	50명
	YARA기반 정규 표현식 활용		6.12 ~ 7.03	7.12 ~ 7.18	50명
	YARA기반 정규 표현식 활용	오프라인 (판교)	6.13 ~ 6.28	7.05 ~ 7.07	30명
중급	정보보호제품군-기본2	온라인	7.10 ~ 7.21	7.26 ~ 8.01	50명
	정보보호제품군-활용1		7.03 ~ 7.14	7.19 ~ 7.25	50명
	정보보호제품군-활용2		7.10 ~ 7.21	7.26 ~ 8.01	50명
	스피어피싱대응-기본		6.19 ~ 7.10	7.19 ~ 7.25	50명
	스피어피싱대응-심화1		6.12 ~ 7.03	7.12 ~ 7.18	50명
	스피어피싱대응-심화2		6.05 ~ 6.26	7.05 ~ 7.11	50명
	멀웨어 식별 훈련		6.26 ~ 7.17	7.26 ~ 8.01	50명
	위협 이벤트 식별 훈련	오프라인 (판교)	6.19 ~ 7.10	7.17 ~ 7.21	30명
고급	CTF기반 공격 및 방어 훈련	오프라인 (판교)	6.26 ~ 7.17	7.24 ~ 7.26	20명

구분	과정명	훈련과정 운영 방향개요
초급	신규 MITRE ATT&CK 활용	MITRE ATT&CK 구성 요소 및 활용 사례를 설명, TTPs를 선정하여 분석하고 탐지 방법 실습
	신규 정보보호제품군-기초1	보안제품의 이해를 위한 네트워크 및 서버 기본 구조
	신규 정보보호제품군-기초2	시스템, 네트워크, 웹 어플리케이션 모의 해킹
	신규 YARA 기반 정규 표현식 활용	정규 표현식 문법 학습 및 sed, awk를 활용한 텍스트 가공 실습, YARA 룰 활용을 통한 위협 탐지
	신규 리버스 엔지니어링	IA-32/64, ARM 환경에서 실행 파일의 구조를 파악하고, 디스어셈블된 코드를 읽고 디버깅 실습
중급	신규 정보보호제품군-기본1	UTM, WAF, Webproxy, Web Filter, SSL/TLS 가시화 도구 실습
	신규 정보보호제품군-기본2	CDR, NAC, DLP로 확장된 제품군 활용 실습
	신규 정보보호제품군-활용1	EDR, SIEM, SOAR로 확장된 제품군 활용 실습
	신규 정보보호제품군-활용2	CTI, Threat Hunting로 확장된 제품군 활용 실습
	스피어피싱대응-기본	스피어피싱 과정을 이해하고 관련된 악성행위 분석
	스피어피싱대응-심화1	악성 HWP 파일 상세 분석
	스피어피싱대응-심화2	악성 MS-Office 파일 상세 분석
	신규 멀웨어 식별 훈련	악성스크립트, 파일, 프로세스에서 사용하는 함수 및 동작기법 분석, 난독화 기법 이해 및 해제 실습
	신규 위협 이벤트 식별 훈련	공격자의 위협 행위로 발생하는 시스템 이벤트를 식별하고 설명하는 실습 수행(30 ~ 50개 사례분석)
고급	신규 MITRE ATT&CK 기반 RedTeaming	사이버위협 인텔리전스 분석 및 TTPs 추출, 위협 에뮬레이션 플랜에 따른 공격 시나리오 구성 및 구현, 공격 인프라 구축 및 플랜에 따른 공격 수행
	신규 침해사고 조사 훈련	공격자의 위협 행위로 발생하는 시스템 이벤트(로그 및 아티팩트)를 MITRE ATT&CK TTPs 기반으로 분석, 침해사고 원인 및 경과 분석
	시나리오 기반 침해사고 조사 및 공격 훈련	실제 해킹사건 시나리오 기반의 침해사고 환경에서 원인 분석 및 조사, 공격자 입장에서 공격 수행
	CTF기반 공격 및 방어 훈련	팀별로 동일하게 주어진 인프라에서 상대 인프라의 취약점을 공격하고, 자신의 취약점은 패치하는 훈련
	신규 실시간 공격, 방어 훈련	실시간으로 발생하는 해킹(공격)을 방어하는 훈련

□ '23년 훈련과정 세부 운영 일정

○ 총 19개 과정, 온라인 62회, 오프라인 총 33회(판교 29회, 부산 4회) 운영

구분	과정명	시간	온라인	판교	부산
초급	신규 MITRE ATT&CK 활용	14H	5회	-	-
	신규 정보보호제품군-기초1	32H	8회	-	-
	신규 정보보호제품군-기초2	32H	7회	-	-
	신규 YARA기반 정규 표현식 활용	21H	6회	2회	-
	신규 리버스 엔지니어링1	35H	4회	2회	-
중급	신규 정보보호제품군-기본1	28H	5회	1회	1회
	신규 정보보호제품군-기본2	28H	2회	1회	-
	신규 정보보호제품군-활용1	28H	5회	1회	1회
	신규 정보보호제품군-활용2	21H	2회	1회	-
	스피어피싱대응-기본	21H	6회	2회	-
	스피어피싱대응-심화1	21H	4회	2회	-
	스피어피싱대응-심화2	21H	4회	2회	-
	신규 멀웨어 식별 훈련	35H	4회	2회	-
	신규 위협 이벤트 식별 훈련	35H	-	3회	1회
고급	신규 MITRE ATT&CK 기반 RedTeaming	35H	-	2회	-
	신규 침해사고 조사 훈련	35H	-	2회	-
	시나리오 기반 침해사고 조사 및 공격 훈련	35H	-	3회	-
	CTF기반 공격 및 방어 훈련	35H	-	2회	-
	신규 실시간 공격, 방어 훈련	21H	-	1회	1회
합계	19개 과정		62회	29회	4회
			95회		

※ '23년 부산 훈련장은 '23년 4분기부터 운영 예정